

# 무한히 큰 냅킨

<https://web.evanchen.cc/napkin.html>

Evan Chen

버전: v1.6.19800101

이 문서는 Evan Chen과 기여자들의 *An Infinitely Large Napkin*을 기계 번역 후 검토한 비공식 한국어 번역본입니다. 한국어 번역이라는 변경 사항이 적용되었으며, 원문과 마찬가지로 CC BY-SA 4.0에 따라 이용할 수 있습니다.



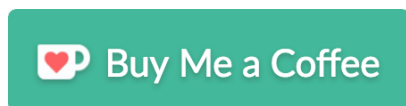


새로운 아이디어를 접했을 때는 항상 왜 신경 써야 하는지 물어보십시오.  
답을 당장 기대하지는 말되, 결국에는 요구하십시오.

— Ravi Vakil [Va17]

---

이 책이 마음에 드셔서 저를 후원하고 싶으시다면,  
커피 한 잔 사주시는 것을 고려해 주십시오!



<https://ko-fi.com/evanchen/>

결국 저에게 이 책을 쓰게 만든 *Brian*과 *Lisa*를 위하여.

© 1980 Evan Chen.

본문은 CC-by-SA-4.0에 따라 라이선스가 부여됩니다. 소스 파일은 GNU GPL v3에 따라 라이선스가 부여됩니다.

이것은 (아직도!) **미완성 초안**입니다. 수정 사항, 의견, 새끼 고양이 사진 등을 [evan@evanchen.cc](mailto:evan@evanchen.cc)로 보내주시거나, <https://github.com/vEnhance/napkin>에서 풀 리퀘스트를 보내주십시오.

마지막 수정: January 1, 1980.



# 서문

”냅킨”이라는 이름의 유래는 저의 다음과 같은 말에서 비롯됩니다.

저는 아직 고등학생인 친구들 몇 명과 간단히 점심을 먹곤 합니다. 친구들은 제게 지난 몇 주 동안 무엇을 하고 지냈는지 물어보고, 저는 범주론을 공부하고 있었다고 말합니다. 친구들은 범주론이 무엇에 관한 것인지 물어봅니다. 저는 대상 자체가 아니라 그것들 사이의 구조를 보존하는 사상만을 살펴봄으로써 사물을 추상화하는 것에 관한 것이라고 설명합니다. 저는 표준적인 예시인 Grp를 들어 설명하려 하지만, 그때 친구들이 준동형 사상이 무엇인지 모른다는 것을 깨닫습니다. 그래서 준동형사상이 무엇인지 설명하기 시작하지만, 그때 친구들이 군이 무엇인지 배운 적이 없다는 것이 떠오릅니다. 그래서 군이 무엇인지 설명하기 시작하지만, 냅킨에 군의 공리를 다 적을 즈음에는 친구들은 애초에 제가 왜 군에 관해 이야기하고 있었는지 이미 잊어버립니다. 그리고 어느새 오후 1시가 되고, 사람들은 각자 갈 곳이 있으니, 저는 이렇게 생각할 수밖에 없습니다:

”이런, 40분이 아니라 40시간이 있었다면, 정말로 이 모든 것을 설명할 수 있었을 텐데.”

이 책은 처음에는 그 40시간을 채우려는 저의 시도였지만, 그 이후로 상당히 성장했습니다.

## 이 책에 대하여

무한히 큰 냅킨은 방대한 고등 수학에 대한, 가볍지만 대체로 자체 완결적인 입문서입니다.

저는 이 책이 전문 서적이나 강의를 대체하기 위한 것이 아니라는 점을 먼저 말씀드려야 합니다. 깊이의 정도는 비교할 수 없습니다. 반면, 이러한 ”가벼운” 접근법의 이점은 목표가 온전한 한 학기 강의를 모방하는 것이 아니라 단지 독자에게 특정 주제에 대한 느낌을 주는 것이기 때문에 더 많은 독자층이 접근할 수 있게 된다는 점입니다.

저는 처음에 재능 있는 고등학생들, 특히 수학 올림피아드 배경을 가진 학생들을 염두에 두고 이 책을 썼습니다. 그러한 문화적 편향의 흔적은 책 전반에 걸쳐, 특히 수학 경시대회에서 가져온 다양한 도전 문제들에서 여전히 느껴질 수 있습니다. 하지만 일반적으로 저는 이 책이 어느 정도의 수학적 성숙도와 호기심을 가진 누구에게나 좋은 참고서가 될 것이라고 생각합니다. 그 예로는 다음과 같은 이들이 포함되지만 이에 국한되지는 않습니다: 수학 학부 전공자, 물리학/컴퓨터공학 전공자, 자신의 전공이 아닌 분야에 대해 조금이라도 듣고 싶어 하는 수학 박사과정 학생, 수학 경시대회는 좋아하지 않지만 수학 자체는 좋아하는 상급 고등학생, 그리고 영어에 유창한 남달리 영리한 새끼 고양이들.

## 소스 코드

이 프로젝트는 <https://github.com/vEnhance/napkin>에서 GitHub를 통해 호스팅되고 있습니다. 풀 리퀘스트는 언제나 환영합니다! 저는 또한 이메일을 통한 제안과 수정 사항도 기쁘게 받겠습니다.

## Napkin 접근법의 배경 철학

제가 아는 한, 고등학생을 위한 고등 수학은 두 가지 형태로 존재합니다.

- 누군가가 ”구형 고양이의 털은 빗질할 수 없다”는 형태로 털 있는 공 정리에 대해 이야기해 주지만, 그것이 왜 참이어야 하는지, 실제로 ”빗질한다”는 것이 무엇을 의미하는지, 혹은 그 기저에 있는 이론에 대해서는 아무것도 알려주지 않아서, 당신의 머릿속에는 그저 막연한 개념만 남게 됩니다.
- 당신은 수업을 듣고 모든 결과를 세세하게 증명하지만, 어느 순간부터는 교수가 무슨 말을 하는지 더 이상 신경 쓰지 않게 됩니다.

아마도 당신은 첫 번째 접근법이 얼마나 만족스럽지 못한지 이미 알고 있을 것입니다. 그래서 두 번째 접근법이 기본값처럼 보이지만, 저는 정말로 이 둘 사이에 어떤 중간 지점이 있어야 한다고 생각합니다.

대학과 달리, 이 책의 목적은 당신에게 연습 문제를 풀거나 증명을 작성하도록 훈련시키는 것이<sup>1</sup> 아니며, 혹은 그 분야의 연구를 준비시키는 것도 아닙니다. 대신 저는 그저 흥미로운 수학을 보여드리고 싶을 뿐입니다. 제시되는 내용들은 기억할 만하고 마음에 담아둘 가치가 있어야 합니다. 그런 이유로, 증명 안에 눈여겨볼 만한 아이디어가 있다고 생각되지 않는 한, 일반적인 교과서에서라면 완결성을 위해 포함되었을 증명들은 여기서는 흔히 생략됩니다. 특히, 저는 정리의 증명을 적어내는 것보다 그 정리가 왜 참이어야 하는지를 설명하는 데 강한 중점을 둡니다. 이는 이 책에서 반복되는 주제입니다:

**자연스러운 설명이 증명보다 우선합니다.**

Napkin의 특정 장을 읽고 난 후, 다음과 같은 것을 얻을 수 있기를 바랍니다:

- 주요 등장 개념들의 정확한 정의가 무엇인지 아는 것,
- 정말로 중요한 몇 가지 예시들에 익숙해지는 것,
- 유명한 정리들의 정확한 서술을 알고, 그것들이 왜 참이어야 하는지에 대한 감각을 갖는 것.

무언가가 왜 참인지 이해하는 데에는 여러 형태가 있을 수 있습니다. 이는 때로는 완전하고 엄밀한 증명으로 이루어지고, 다른 경우에는 증명의 아이디어로 주어지며, 또 다른 경우에는 몇 가지 핵심 예시와 함께 열렬한 응원으로 이루어지기도 합니다.

물론 어떤 분야에서 연구를 하고 싶다면 이것만으로는 전혀 충분하지 않습니다. 하지만 당신이 그저 호기심 많은 국외자라면, 저는 이것이 엘리베이터 피치나 위키백과 문서보다 더 만족스럽기를 바랍니다. 설령 어떤 주제를 진지하게 깊이 있게 배우고 싶다 하더라도, 저는 이것이 본격적으로 뛰어들기 전에 좋은 조망적 개관이 될 수 있기를 바랍니다. 왜냐하면 여러 의미에서 다루는 자료의 선택 기준은 "누군가 내가 시작하기 전에 알려주었으면 했던 것"이기 때문입니다.

## 더 많은 교육적 논평과 참고 문헌

저의 교육적 결정 중 일부에 대해 장별로 이야기한다면 서문이 너무 길어질 것이므로, 그러한 논평은 대신 [장 A](#)에 담았습니다.

특히 저는 종종 구체적인 참고문헌을 언급하는데, 그 부록의 끝부분에는 더 많은 참고문헌이 있습니다. 따라서 더 읽을거리를 원하신다면 이곳을 살펴보시기 좋습니다.

## 역사적 및 개인적 소회

저는 하버드 학부 첫 학기를 마친 뒤인 2014년 12월에 이 책을 쓰기 시작했습니다. 그 후 약 18개월 동안 이것이 저의 주된 관심사가 되었으며, 그 시기에 저는 고등 수학에 깊이 몰두하게 되었습니다. 저는 사실상 수학 수업만 들었고(다른 졸업 요건들은 즐겁게 무시하면서), 그것을 최대한 많이(제가 여가 시간에 배운 다른 많은 수학과 함께) Napkin에 합쳤습니다.

하지만 2016년 8월 무렵, 저는 결국 힘이 다 빠졌습니다. 그때 최초의 공개 초고가 온라인에 올라갔고, 저는 한 발 물러서기로 결정했습니다. 약간 지친 상태로, 저는 고등 수학에서

<sup>1</sup>이것이 문제 해결이 가치 없다는 뜻은 아닙니다. 저 자신도 본질적으로는 수학 올림피아드 코치입니다. 다만 그것이 이 책의 요점은 아니라는 것입니다.

잠시 손을 떼고, 남은 학부 2년<sup>2</sup> 동안 미국 수학 올림피아드 팀의 코치로 열심히 활동하며, 친구들이 졸업하여 각자의 길로 떠나기 전에 그들과 가능한 한 많은 시간을 보내려 애썼습니다.

그 2년 동안, 독자들은 제게 많은 감사의 따뜻한 말과 많은 오류 제보, 그리고 많은 추가 제안을 보내주었습니다. 그래서 수학 박사과정 첫 학기가 시작된 지 몇 주 지난 2018년 11월, 저는 제가 시작한 것을 끝내야겠다고 결심했습니다. 몇 달 후, 지금 이것이 그 결과물입니다.

## 감사의 말

저는 이 작업에 대해 헤아릴 수 없이 많은 분들께 빚을 지고 있습니다. 다음은 그 일부(분명 불완전한) 목록입니다.

- 이 노트에서 다룬 내용의 많은 부분을 가르쳐주신 모든 선생님과 교수님들께, 그리고 제가 여기서 인용한 모든 참고문헌의 저자분들께 감사드립니다. 특히 큰 영향을 준 [Ga14], [Le14], [Sj05], [Ga03], [Ll15], [Et11], [Ko14], [Va17], [Pu02], [Go18]에 특별히 감사드립니다.
- 또한 제 초고의 미리보기 사본을 읽고 오류를 지적하고 다른 제안을 해준 수십 명의 친구들과 낯선 분들께도 감사드립니다. 함께 천 개가 넘는 오류를 찾아준 Andrej Vuković과 Alexander Chua에게 특별히 언급하고자 합니다. 또한 많은 수정 사항을 알려준 Brian Gu와 Tom Tseng에게도 감사드립니다. (만약 여러분께서 직접 실수를 발견하시거나 제안이 있으시다면, 저는 그것을 듣고 싶습니다!) 또한 이 문서에 게스트 장을 기고해준 Royce Yao와 user202729에게도 감사드립니다.
- 표지 작품을 만들어준 Jenny Chu와 Lanie Deng에게 감사드립니다.
- 저는 또한 이 프로젝트가 진행되는 동안 받은 아주 많은, 정말 많은 따뜻한 말씀에 감사를 표하고 싶습니다. 이러한 너그러운 논평들 덕분에 저는 이 작업을 계속할 수 있었으며, 2018년 11월에 Napkin을 다시 업데이트하기로 한 저의 결정도 대체로 그 덕분이었습니다.

마지막으로, 냅킨(그리고 저)의 뿌리가 된 수학 올림피아드 커뮤니티에 큰 감사를 전합니다. 지난 세월 동안 받은 모든 열정과 격려, 감사의 메시지들이 애초에 제가 이 글을 쓰기 시작하게 만들었습니다. 그렇지 않았다면 저는 이런 프로젝트가 조금이라도 가능하리라고 감히 꿈꾸지 못했을 것입니다. 그리고 물론, IMO를 향해 제 꿈을 좇으며 겪었던 인생을 바꾼 여정이 없었다면 저는 오늘날의 이 자리에 결코 이르지 못했을 것입니다. 영원한 TWN2!

<sup>2</sup>다르게 말하면: "... 그리고 애써 배운 모든 것을 잊어버리며 다음 2년을 보냈다". 이는 Napkin에 남긴 과거의 노트들에 감사하게 만들었습니다!



# 독자를 위한 조언

## §1 선행 지식

서문에서 설명했듯이, 주된 선행 지식은 어느 정도의 수학적 성숙도입니다. 이는 독자가 증명을 읽고 쓸 줄 알고, 논리적 논증을 따라갈 줄 아는 등의 능력을 갖추고 있기를 기대한다는 뜻입니다.

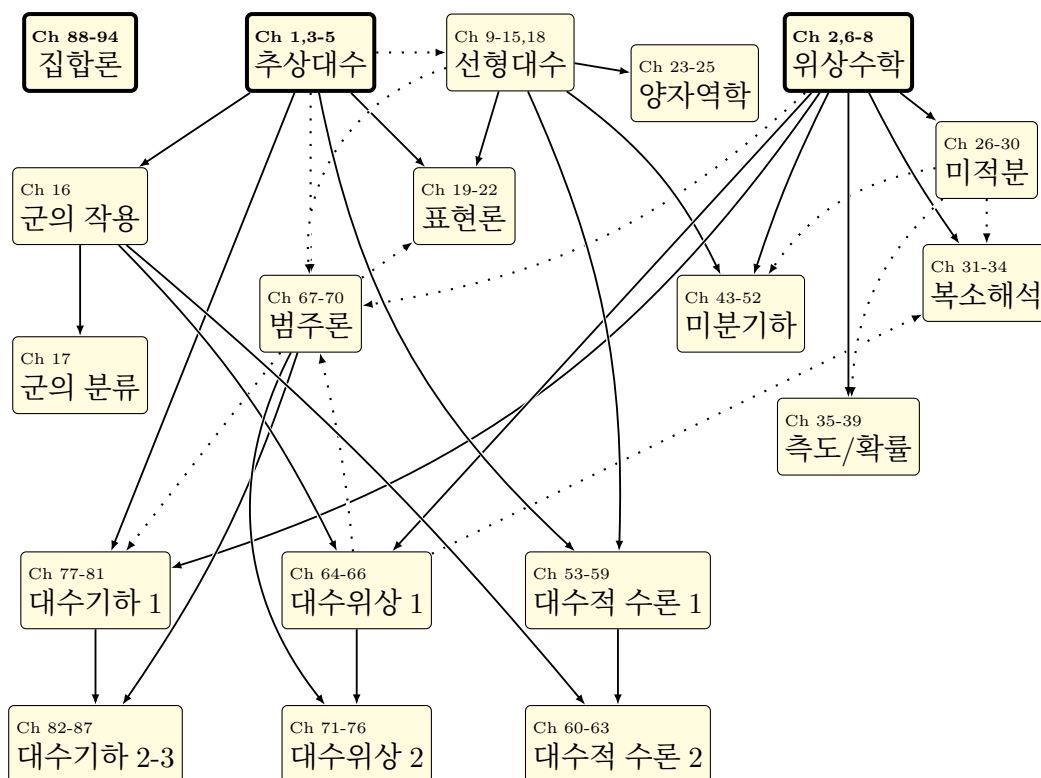
또한 독자가 집합과 함수에 관한 기본 용어(예를 들어 “전단사란 무엇인가?”)에 익숙하다고 가정합니다. 그렇지 않다면 [장 E](#)를 참고하십시오.

## §2 무엇을 읽을지 정하기

이 책을 순서대로 읽을 필요는 없습니다. 이 책은 수학의 온갖 분야를 다루고 있으며, 여러분이 택할 수 있는 경로도 다양합니다. [장 0](#)에서는 각 부에 대해 무엇을 기대할 수 있을지 간략히 개관합니다.

일단 여기서는 각 장이 서로 어떻게 의존하는지를 보여주는 간단한 도표를 제시합니다. 자세한 내용은 다시 [장 0](#)를 참고하십시오. 의존 관계는 화살표로 표시되며, 점선은 선택적 의존 관계입니다. 저는 여러분이 그저 흥미로워 보이는 장을 하나 고른 다음, 가장 짧은 경로를 찾아보기를 제안합니다. 이를 염두에 두면, 전체 PDF의 분량이 위압적으로 느껴지지 않기를 바랍니다.

(아래 도식의 텍스트는 클릭 가능하며, 해당 부분으로 연결되어야 합니다.)



### §3 질문, 연습문제, 문제

이 책에는 세 가지 위계가 있습니다:

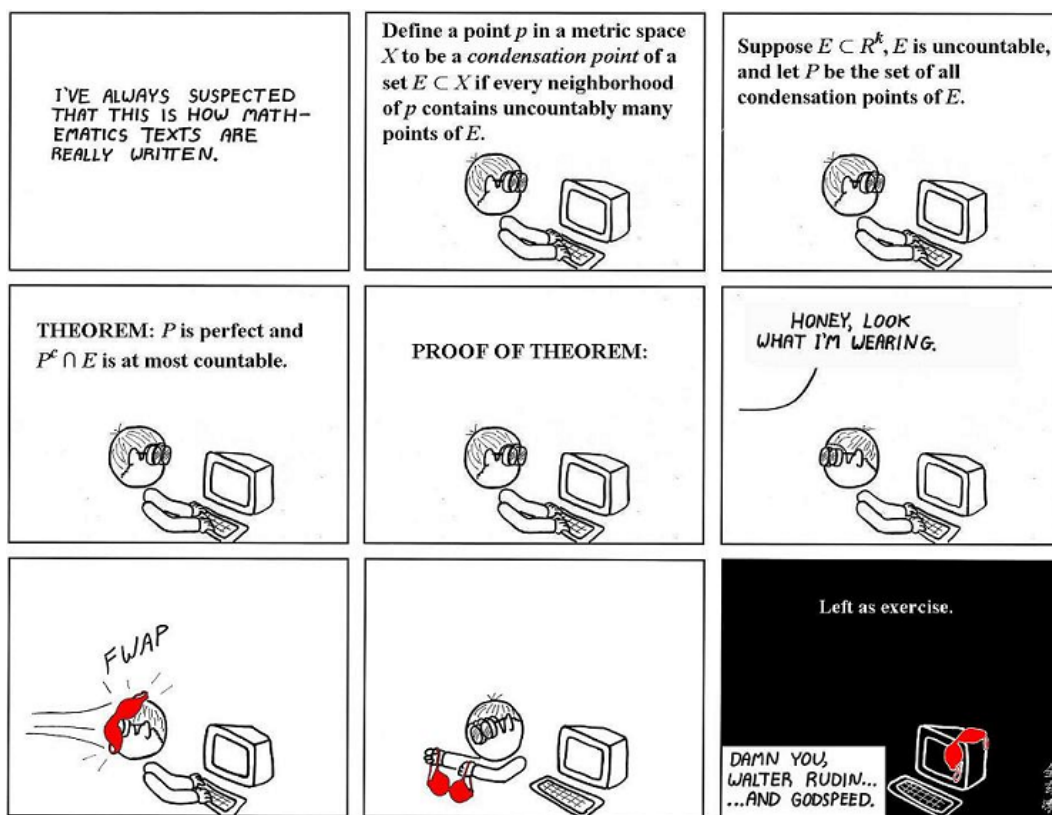
- 본문 중의 **질문(question)**은 어이없을 정도로 쉽게 만들어졌으며, 대체로 정의를 내면화하는 데 도움을 주기 위한 기회입니다. 만약 한두 개를 답할 수 없다면, 아마도 제가 설명을 잘못된 것이니 저에게 불만을 제기해야 합니다. 하지만 여러 개를 답할 수 없다면, 아마도 중요한 것을 놓쳤을 가능성이 크니 앞으로 돌아가 다시 읽으십시오.
- 본문 중의 **연습문제(exercise)**는 질문보다는 내용이 더 있지만, “까다로운” 단계는 없어야 합니다. 종종 저는 정리와 명제의 증명이 유익하고 어느 정도 흥미롭다면 이를 연습문제로 남겨둡니다.
- 각 장의 끝에는 좀 더 까다로운 **문제**들이 몇 개 실려 있습니다. 어떤 것은 적당하지만, 다른 것들은 정말로 어려운 올림피아드 스타일의 문제들입니다. 더 어려운 문제들은 이 문단처럼 최대 세 개의 칠리 고추(🌶️)로 표시됩니다.



난이도 표시 외에도, 문제들은 전체적인 그림에서 얼마나 중요한지에 따라서도 표시 됩니다.

- **일반 문제**는 재미있기를 바라지만 핵심적이지는 않은 문제입니다.
- **단검(dagger) 표시 문제**는 (대체로 흥미로운) 결과로서 알아두어야 하지만, 이후에 직접 사용되지는 않는 문제입니다.
- **별표 문제**는 이 책의 이후 부분에서 사용될 결과입니다.<sup>1</sup>

여러 힌트와 풀이는 **장 B and C**에서 찾아볼 수 있습니다.



이미지 출처: [Go08]

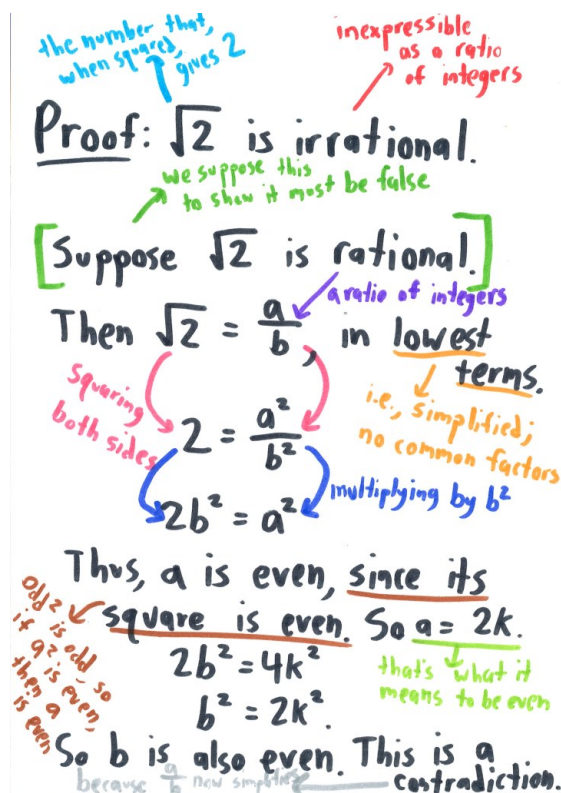
<sup>1</sup>이는 대학에서 종종 벌어지는 그 전형적인 “PSet 4 문제 8에서 끝난 것으로 한다”는 상황을 피하기 위해서인데, 마치 제가 그게 뭔지 기억이라도 하는 것처럼 말입니다.

## §4 종이

무뚝뚝하게 말할 위험을 무릅쓰고,

이 책은 연필과 종이를 가지고 읽으십시오.

그 이유는 다음과 같습니다:



[Or]에서 가져온 이미지

여러분은 신이 아닙니다. 모든 것을 머릿속에 담아둘 수는 없습니다.<sup>2</sup> 인쇄본을 출력했다면 여백에 메모를 하십시오. 종이를 아끼고 싶다면 공책 같은 것을 챙겨서 함께 가지고 다니십시오. 어쨌든, 무슨 방법으로든 필기를 할 수 있도록 하십시오. 감사합니다.

## §5 예시의 중요성에 대하여

저는 병적으로 예시에 집착합니다. 이 책에서는 모든 예시를 큰 박스에 넣어 강조하는데, 그 때문에 이 책의 어떤 페이지들은 그저 박스가 연이어 나오는 것으로만 이루어져 있습니다. 독자께서 이를 언짢게 여기지 않으시길 바랍니다.

또한 저는 일부 절에서 "전형적인 예시"를 강조하는 경우가 많으며, 이러한 표시에는 빨간색을 따로 사용합니다. 그 철학은, 독자가 그러한 대상에 관한 정의나 정리를 볼 때마다 전형적인 예시에 견주어 검증해 보아야 한다는 것입니다. 만약 그 예시가 좋은 전형이라면, 왜 그 정의가 직관적인지, 왜 그 정리가 참이어야 하는지, 왜 그 정리가 흥미로운지 등이 즉시 명확해질 것입니다.

비밀 하나를 말씀드리겠습니다. 이 책에서 정의나 정리를 쓸 때마다, 저는 (꽤 형편없는) 기억력에서 정확한 서술을 떠올려야 했습니다. 그래서 저는 대신 전형적인 예시를 먼저 떠올리고, 그런 다음에야 비로소 그 정의나 정리가 무엇이었는지 기억해 내는 경우가 많습니다.

<sup>2</sup><https://blog.evanchen.cc/writing/>와 위의 출처도 참고하십시오.

그런데 이것은 애초에 제가 모든 정의를 배웠던 방식이기도 합니다. 독자 여러분께도 이 방법이 유용하기를 바랍니다.

## §6 관례와 표기법

이 부분에서는 다소 낮은 표기법과 정의 몇 가지를 설명하고, 성가신 문제들("0은 자연수인가?")을 이번 기회에 확실히 정리합니다. 이들 대부분은 "전문가를 위한 참고 사항"이므로, 이해가 되지 않는다면 지금 당장은 걱정하지 않아도 될 것입니다.

사용된 표기법의 전체 용어집은 부록에서 찾아보실 수 있습니다.

### §6.i 자연수는 양수입니다

집합  $\mathbb{N}$ 은 양의 정수의 집합이며, 0은 포함하지 않습니다. 집합론 장들에서는 책의 나머지 부분과의 일관성을 위해 대신  $\omega = \{0, 1, \dots\}$ 를 사용합니다.

### §6.ii 집합과 동치 관계

이는 전문가를 위한 상기용으로 간략히 서술한 것입니다. 자세한 내용은 [장 E](#)를 참고하십시오.

집합  $X$  위의 **동치 관계**란 대칭적, 반사적, 추이적인 관계  $\sim$ 를 말합니다. 동치 관계는  $X$ 를 여러 개의 **동치류**로 분할합니다. 이를  $X/\sim$ 로 표기하겠습니다. 그러한 동치류의 원소를 그 동치류의 **대표원**이라고 합니다.

저는 "동형사상" 유형의 관계(formally: 어떤 적절한 범주에서 동형사상인 관계)에는 항상  $\cong$ 를 사용합니다. 냅킨에서  $\sim$ 가 쓰이는 유일한 경우는 호모토픽 경로에 대해서입니다.

저는 일반적으로  $\subseteq$ 와  $\subsetneq$ 를 사용하는데,  $\subset$ 와 달리 이들은 모호하지 않기 때문입니다.  $\subset$ 는 등호가 성립하지 않는다는 것이 명백하지만 이를 굳이 밝히면 오히려 산만해지는 드문 경우에만 사용합니다. 예를 들어, " $\mathbb{Q} \subset \mathbb{R}$ "는 산만하기 때문에 저는  $\mathbb{Q} \subsetneq \mathbb{R}$ 로 씁니다.

저는  $S - T$ 보다  $S \setminus T$ 를 선호합니다.

$S$ 의 멱집합(즉,  $S$ 의 부분집합들의 집합)은  $2^S$  또는  $\mathcal{P}(S)$ 로 표기됩니다.

### §6.iii 함수

이는 전문가를 위한 상기용으로 간략히 서술한 것입니다. 자세한 내용은 [장 E](#)를 참고하십시오.

$X \xrightarrow{f} Y$ 를 함수라고 합시다:

- $f^{\text{pre}}(T)$ 란 **원상**을 의미합니다

$$f^{\text{pre}}(T) := \{x \in X \mid f(x) \in T\}.$$

이는 세상 다른 곳에서 쓰이는  $f^{-1}(T)$ 와 대조되는데, 저는  $f^{-1}$ 를 오직 역함수에만 사용합니다.

표기의 남용으로,  $f^{\text{pre}}(\{y\})$ 를  $f^{\text{pre}}(y)$ 로 줄여 쓸 수 있습니다.  $f^{\text{pre}}(y)$ 를 **올**이라고 부릅니다.

- $f^{\text{img}}(S)$ 란 **상**(image)을 의미합니다

$$f^{\text{img}}(S) := \{f(x) \mid x \in S\}.$$

세상의 거의 모든 사람들은  $f(S)$ 를 사용합니다(다만  $f[S]$ 도 어느 정도 쓰이며, 논리학에서는  $f''(S)$ 가 자주 사용됩니다). 하지만 이는 표기법의 남용이며, 저는 강조를 위해  $f^{\text{img}}(S)$ 를 선호합니다. 이 상(image) 표기법은 표준이 아닙니다.

- $S \subseteq X$ 라면,  $f$ 의  $S$ 로의 **제한**은  $f|_S$ 로 표기하며, 즉 이것은 함수  $f|_S: S \rightarrow Y$ 입니다.
- 때로는 함수  $f: X \rightarrow Y$ 가 단사이거나 전사일 수 있습니다. 이를 강조하기 위해 각각  $f: X \hookrightarrow Y$  또는  $f: X \twoheadrightarrow Y$ 로 쓰기도 합니다.

### §6.iv 순열의 순환 표기법

또한 유한 집합 위의 순열은 [https://en.wikipedia.org/wiki/Permutation#Cycle\\_notation](https://en.wikipedia.org/wiki/Permutation#Cycle_notation)에 설명된 것과 같은 순환 표기법으로 나타낼 수 있습니다. 예를 들어 표기  $(1\ 2\ 3\ 4)(5\ 6\ 7)$ 은  $1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 4, 4 \mapsto 1, 5 \mapsto 6, 6 \mapsto 7, 7 \mapsto 5$ 인 순열을 가리킵니다. 이 표기법의 사용은 대체로 문맥상 명확할 것입니다.

### §6.v 환

별도로 명시하지 않는 한 모든 환은 곱셈 항등원 1을 가집니다. 일반적인 환에서는  $0 = 1$ 을 허용하지만, 정역에서는 허용하지 않습니다.

**별도의 언급이 없는 한 모든 환은 가환환입니다.** 코호몰로지 환을 다루는 장에서만 사용되는, 가환이 아닌 환에 이름을 붙이기 위한 정교한 스킴이 있습니다:

|                 | 등급      | 등급이 없음 |
|-----------------|---------|--------|
| 1이 필요하지 않음      | 등급 유사환  | 유사환    |
| 반가환, 1이 필요하지 않음 | 반가환 유사환 | 해당 없음  |
| 1을 가짐           | 등급환     | 해당 없음  |
| 1을 갖는 반가환       | 반가환환    | 해당 없음  |
| 1을 갖는 가환        | 가환 등급환  | 환      |

반면 대수는 항상 1을 가지지만, 가환일 필요는 없습니다.

### §6.vi 선택

저희는 선택 공리를 받아들이며, 이를 자유롭게 사용합니다.

## §7 더 읽을거리

부록 **장 A**에는 제가 좋아하는 자료 목록과 각 장에 대해 제가 내린 교육학적 선택에 대한 설명이 담겨 있습니다. 꼭 한번 살펴보시기를 권합니다.

특히, 이곳이 바로 여러분이 더 읽을거리를 찾아야 할 곳입니다! Napkin에서 다루어져야 하지만 저의 무지나 게으름으로 인해 다루어지지 않은 주제들이 있습니다. 이 부록에 제공된 참고 문헌들이 저의 누락을 부분적으로나마 만회하는 데 도움이 되기를 바랍니다.



# 목차

|                          |           |
|--------------------------|-----------|
| <b>서문</b>                | <b>v</b>  |
| <b>독자를 위한 조언</b>         | <b>ix</b> |
| 1 선행 지식                  | ix        |
| 2 무엇을 읽을지 정하기            | ix        |
| 3 질문, 연습문제, 문제           | x         |
| 4 종이                     | xi        |
| 5 예시의 중요성에 대하여           | xi        |
| 6 관례와 표기법                | xii       |
| 7 더 읽을거리                 | xiii      |
| <br>                     |           |
| <b>I 시작하기</b>            | <b>35</b> |
| <b>0 세일즈 피치</b>          | <b>37</b> |
| 0.1 기초                   | 37        |
| 0.2 추상대수학                | 38        |
| 0.3 실해석학과 복소해석학          | 39        |
| 0.4 대수적 수론               | 40        |
| 0.5 대수적 위상수학             | 40        |
| 0.6 대수기하학                | 41        |
| 0.7 집합론                  | 42        |
| <br>                     |           |
| <b>1 군</b>               | <b>43</b> |
| 1.1 군의 정의와 예시            | 43        |
| 1.2 군의 성질                | 46        |
| 1.3 동형사상                 | 48        |
| 1.4 군의 위수와 라그랑주 정리       | 50        |
| 1.5 부분군                  | 51        |
| 1.6 작은 위수의 군             | 52        |
| 1.7 중요하지 않은 긴 여담         | 53        |
| 1.8 생각해 볼 만한 조금 더 어려운 문제 | 53        |
| <br>                     |           |
| <b>2 거리 공간</b>           | <b>55</b> |
| 2.1 거리 공간의 정의와 예시        | 55        |
| 2.2 거리 공간에서의 수렴          | 57        |
| 2.3 연속 사상                | 58        |
| 2.4 위상동형사상               | 59        |
| 2.5 확장된 예시/정의: 곱 거리함수    | 60        |
| 2.6 열린집합                 | 61        |
| 2.7 닫힌집합                 | 64        |
| 2.8 생각해 볼 만한 조금 더 어려운 문제 | 65        |
| <br>                     |           |
| <b>II 기본 추상대수학</b>       | <b>67</b> |
| <b>3 준동형사상과 몫군</b>       | <b>69</b> |
| 3.1 생성원과 군 표시            | 69        |

|            |                                 |            |
|------------|---------------------------------|------------|
| 3.2        | 준동형사상                           | 70         |
| 3.3        | 잉여류와 잉여류로 나누기(모딩 아웃)            | 72         |
| 3.4        | (선택) 라그랑주 정리의 증명                | 75         |
| 3.5        | 준동형사상 없애기                       | 76         |
| 3.6        | (여담) 첫 번째 동형사상 정리               | 78         |
| 3.7        | 생각해 볼 만한 조금 더 어려운 문제            | 79         |
| <b>4</b>   | <b>환과 아이디얼</b>                  | <b>81</b>  |
| 4.1        | 환과 군에 관한 몇 가지 동기 부여용 비유         | 81         |
| 4.2        | (선택) 동기 부여에 관한 교육적 참고사항         | 81         |
| 4.3        | 환의 정의와 예시                       | 81         |
| 4.4        | 체                               | 84         |
| 4.5        | 준동형사상                           | 84         |
| 4.6        | 아이디얼                            | 85         |
| 4.7        | 아이디얼 생성하기                       | 87         |
| 4.8        | 주 아이디얼 정역                       | 89         |
| 4.9        | 뇌터 환                            | 90         |
| 4.10       | 생각해 볼 만한 조금 더 어려운 문제            | 91         |
| <b>5</b>   | <b>환의 종류</b>                    | <b>93</b>  |
| 5.1        | 체                               | 93         |
| 5.2        | 정역                              | 93         |
| 5.3        | 소 아이디얼                          | 94         |
| 5.4        | 극대 아이디얼                         | 95         |
| 5.5        | 분수체                             | 97         |
| 5.6        | 유일 인수분해 정역 (UFD)                | 97         |
| 5.7        | 추가: 유클리드 정역                     | 99         |
| 5.8        | 생각해 볼 만한 조금 더 어려운 문제            | 104        |
| <b>III</b> | <b>기본 위상수학</b>                  | <b>107</b> |
| <b>6</b>   | <b>거리 공간의 성질</b>                | <b>109</b> |
| 6.1        | 유계성                             | 109        |
| 6.2        | 완비성                             | 110        |
| 6.3        | 구매자는 조심하십시오                     | 111        |
| 6.4        | 부분공간, 그리고 (미리 말해두는) 헛갈리는 언어적 요점 | 112        |
| 6.5        | 생각해 볼 만한 조금 더 어려운 문제            | 113        |
| <b>7</b>   | <b>위상 공간</b>                    | <b>115</b> |
| 7.1        | 거리를 잊기                          | 115        |
| 7.2        | 재정의                             | 116        |
| 7.3        | 하우스도르프 공간                       | 117        |
| 7.4        | 부분공간                            | 118        |
| 7.5        | 연결 공간                           | 118        |
| 7.6        | 경로 연결 공간                        | 119        |
| 7.7        | 호모토피와 단순 연결 공간                  | 120        |
| 7.8        | 공간의 기저                          | 122        |
| 7.9        | 생각해 볼 만한 조금 더 어려운 문제            | 122        |

|           |                                                 |            |
|-----------|-------------------------------------------------|------------|
| <b>8</b>  | <b>콤팩트성</b>                                     | <b>125</b> |
| 8.1       | 점렬 콤팩트성의 정의                                     | 125        |
| 8.2       | 콤팩트성의 판정 기준                                     | 126        |
| 8.3       | 열린 덮개를 이용한 콤팩트성                                 | 127        |
| 8.4       | 콤팩트성의 응용                                        | 129        |
| 8.5       | (선택) 콤팩트성 정의들의 동치성                              | 131        |
| 8.6       | 생각해 볼 만한 조금 더 어려운 문제                            | 132        |
| <br>      |                                                 |            |
| <b>IV</b> | <b>선형대수학</b>                                    | <b>135</b> |
| <br>      |                                                 |            |
| <b>9</b>  | <b>벡터 공간</b>                                    | <b>139</b> |
| 9.1       | 환과 체의 정의                                        | 139        |
| 9.2       | 가군과 벡터 공간                                       | 139        |
| 9.3       | 직합                                              | 141        |
| 9.4       | 선형 독립, 생성, 그리고 기저                               | 143        |
| 9.5       | 선형 사상                                           | 145        |
| 9.6       | 행렬이란 무엇인가?                                      | 147        |
| 9.7       | 부분공간과 편리한 기저 선택하기                               | 151        |
| 9.8       | 재미있는 응용: 라그랑주 보간법                               | 153        |
| 9.9       | 교육학적 여담: 숫자 배열은 사악하다                            | 153        |
| 9.10      | 일반적인 가군에 관한 한마디                                 | 154        |
| 9.11      | 생각해 볼 만한 조금 더 어려운 문제                            | 155        |
| <br>      |                                                 |            |
| <b>10</b> | <b>고유한 것들</b>                                   | <b>157</b> |
| 10.1      | 관심을 가져야 하는 이유                                   | 157        |
| 10.2      | 가정에 관한 주의사항                                     | 158        |
| 10.3      | 고유벡터와 고유값                                       | 158        |
| 10.4      | 조르당 형식                                          | 159        |
| 10.5      | 몫영 사상                                           | 161        |
| 10.6      | 몫영인 경우로의 환원                                     | 162        |
| 10.7      | (선택 사항) 몫영 조르당 정리의 증명                           | 163        |
| 10.8      | 대수적 중복도와 기하적 중복도                                | 164        |
| 10.9      | 생각해 볼 만한 조금 더 어려운 문제                            | 165        |
| <br>      |                                                 |            |
| <b>11</b> | <b>쌍대 공간과 대각합</b>                               | <b>167</b> |
| 11.1      | 텐서곱                                             | 167        |
| 11.2      | 쌍대 공간                                           | 170        |
| 11.3      | $V^{\vee} \otimes W$ 는 $V$ 에서 $W$ 로 가는 행렬들을 줍니다 | 172        |
| 11.4      | 대각합                                             | 173        |
| 11.5      | 생각해 볼 만한 조금 더 어려운 문제                            | 174        |
| <br>      |                                                 |            |
| <b>12</b> | <b>행렬식</b>                                      | <b>175</b> |
| 12.1      | 췌기곱                                             | 175        |
| 12.2      | 행렬식                                             | 178        |
| 12.3      | 특성다항식과 케일리-해밀턴                                  | 179        |
| 12.4      | 생각해 볼 만한 조금 더 어려운 문제                            | 181        |
| <br>      |                                                 |            |
| <b>13</b> | <b>내적 공간</b>                                    | <b>183</b> |
| 13.1      | 내적                                              | 183        |
| 13.2      | 노름                                              | 185        |

|           |                                                                              |            |
|-----------|------------------------------------------------------------------------------|------------|
| 13.3      | 직교성 . . . . .                                                                | 187        |
| 13.4      | 힐베르트 공간 . . . . .                                                            | 188        |
| 13.5      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                               | 190        |
| <b>14</b> | <b>보너스: 푸리에 해석</b>                                                           | <b>191</b> |
| 14.1      | 개요 . . . . .                                                                 | 191        |
| 14.2      | 힐베르트 공간에 대한 상기 . . . . .                                                     | 191        |
| 14.3      | 흔한 예시들 . . . . .                                                             | 192        |
| 14.4      | 요약, 그리고 또 다른 예고편 . . . . .                                                   | 196        |
| 14.5      | Parseval과 그 친구들 . . . . .                                                    | 196        |
| 14.6      | 응용: 바젤 문제 . . . . .                                                          | 197        |
| 14.7      | 응용: Arrow의 불가능성 정리 . . . . .                                                 | 198        |
| 14.8      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                               | 200        |
| <b>15</b> | <b>쌍대, 수반, 그리고 전치</b>                                                        | <b>201</b> |
| 15.1      | 사상의 쌍대 . . . . .                                                             | 201        |
| 15.2      | (선택) 자연스러운 동형사상 $V \cong V^V$ 가 없을 때 무엇이 잘못될 수 있는지에<br>대한 교훈적인 이야기 . . . . . | 202        |
| 15.3      | 쌍대 공간과의 동일시 . . . . .                                                        | 204        |
| 15.4      | 딸림사상 (켈레 전치) . . . . .                                                       | 205        |
| 15.5      | 정규 사상의 고윳값 . . . . .                                                         | 206        |
| 15.6      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                               | 208        |
| <b>V</b>  | <b>군에 대하여 더 알아보기</b>                                                         | <b>211</b> |
| <b>16</b> | <b>군의 작용으로 AIME 문제를 압도적으로 풀어내기</b>                                           | <b>213</b> |
| 16.1      | 군의 작용의 정의 . . . . .                                                          | 213        |
| 16.2      | 안정자군과 궤도 . . . . .                                                           | 214        |
| 16.3      | 번사이드 보조정리 . . . . .                                                          | 215        |
| 16.4      | 원소의 켈레화 . . . . .                                                            | 216        |
| 16.5      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                               | 217        |
| <b>17</b> | <b>모든 군을 찾으시오</b>                                                            | <b>219</b> |
| 17.1      | 실로우 정리 . . . . .                                                             | 219        |
| 17.2      | (선택) 실로우 정리 증명하기 . . . . .                                                   | 220        |
| 17.3      | (선택) 단순군과 Jordan-Hölder . . . . .                                            | 222        |
| 17.4      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                               | 224        |
| <b>18</b> | <b>PID 구조 정리</b>                                                             | <b>225</b> |
| 18.1      | 유한 생성 아벨 군 . . . . .                                                         | 225        |
| 18.2      | 환론의 몇 가지 선행 지식 . . . . .                                                     | 226        |
| 18.3      | 구조 정리 . . . . .                                                              | 227        |
| 18.4      | 자유 $R$ -가군 사이의 사상으로서의 환원 . . . . .                                           | 228        |
| 18.5      | 준소 형식의 유일성 . . . . .                                                         | 229        |
| 18.6      | 스미스 표준형 . . . . .                                                            | 231        |
| 18.7      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                               | 234        |

|            |                             |            |
|------------|-----------------------------|------------|
| <b>VI</b>  | <b>표현론</b>                  | <b>235</b> |
| <b>19</b>  | <b>대수의 표현</b>               | <b>237</b> |
| 19.1       | 대수                          | 237        |
| 19.2       | 표현                          | 238        |
| 19.3       | 직합                          | 240        |
| 19.4       | 기약 표현과 분해불가능 표현             | 242        |
| 19.5       | 표현의 사상                      | 243        |
| 19.6       | $\text{Mat}_d(k)$ 의 표현들     | 245        |
| 19.7       | 생각해 볼 만한 조금 더 어려운 문제        | 246        |
| <b>20</b>  | <b>반단순 대수</b>               | <b>249</b> |
| 20.1       | 슈어의 보조정리 (계속)               | 249        |
| 20.2       | 조밀성 정리                      | 251        |
| 20.3       | 반단순 대수                      | 253        |
| 20.4       | 마슈케 정리                      | 254        |
| 20.5       | 예시: $\mathbb{C}[S_3]$ 의 표현들 | 255        |
| 20.6       | 생각해 볼 만한 조금 더 어려운 문제        | 256        |
| <b>21</b>  | <b>지표</b>                   | <b>257</b> |
| 21.1       | 정의                          | 257        |
| 21.2       | 교환자로 나눈 쌍대 공간               | 258        |
| 21.3       | 지표의 직교성                     | 259        |
| 21.4       | 지표표의 예                      | 261        |
| 21.5       | 생각해 볼 만한 조금 더 어려운 문제        | 262        |
| <b>22</b>  | <b>몇 가지 응용</b>              | <b>265</b> |
| 22.1       | 프로베니우스 나눗셈성                 | 265        |
| 22.2       | 번사이드의 정리                    | 266        |
| 22.3       | 프로베니우스 행렬식                  | 267        |
| <b>VII</b> | <b>양자 알고리즘</b>              | <b>269</b> |
| <b>23</b>  | <b>양자 상태와 측정</b>            | <b>271</b> |
| 23.1       | 브라-켓 표기법                    | 271        |
| 23.2       | 상태 공간                       | 272        |
| 23.3       | 관찰                          | 272        |
| 23.4       | 얽힘                          | 275        |
| 23.5       | 생각해 볼 만한 조금 더 어려운 문제        | 278        |
| <b>24</b>  | <b>양자 회로</b>                | <b>279</b> |
| 24.1       | 고전 논리 게이트                   | 279        |
| 24.2       | 가역 고전 논리                    | 280        |
| 24.3       | 양자 논리 게이트                   | 282        |
| 24.4       | 도이치-조사 알고리즘                 | 284        |
| 24.5       | 생각해 볼 만한 조금 더 어려운 문제        | 285        |
| <b>25</b>  | <b>쇼어 알고리즘</b>              | <b>287</b> |
| 25.1       | 고전적인 (역) 푸리에 변환             | 287        |
| 25.2       | 양자 푸리에 변환                   | 288        |
| 25.3       | 쇼어 알고리즘                     | 290        |

|             |                                                                   |            |
|-------------|-------------------------------------------------------------------|------------|
| <b>VIII</b> | <b>미적분학 101</b>                                                   | <b>293</b> |
| <b>26</b>   | <b>극한과 급수</b>                                                     | <b>295</b> |
| 26.1        | 완비성과 $\inf/\sup$ . . . . .                                        | 295        |
| 26.2        | $\mathbb{R}$ 의 두 가지 핵심 완비성 성질의 증명 . . . . .                       | 296        |
| 26.3        | 단조수열 . . . . .                                                    | 298        |
| 26.4        | 무한급수 . . . . .                                                    | 299        |
| 26.5        | 급수의 덧셈은 교환법칙이 성립하지 않습니다: 공포 이야기 . . . . .                         | 302        |
| 26.6        | 점에서의 함수의 극한 . . . . .                                             | 303        |
| 26.7        | 무한대에서의 함수의 극한 . . . . .                                           | 305        |
| 26.8        | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                    | 305        |
| <b>27</b>   | <b>Bonus: A hint of p-adic numbers</b>                            | <b>307</b> |
| 27.1        | 동기 . . . . .                                                      | 307        |
| 27.2        | 대수적 관점 . . . . .                                                  | 308        |
| 27.3        | 해석적 관점 . . . . .                                                  | 312        |
| 27.4        | Mahler 계수 . . . . .                                               | 315        |
| 27.5        | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                    | 317        |
| <b>28</b>   | <b>미분</b>                                                         | <b>319</b> |
| 28.1        | 정의 . . . . .                                                      | 319        |
| 28.2        | 계산하는 방법 . . . . .                                                 | 320        |
| 28.3        | 극소 (및 극대) 최댓값 . . . . .                                           | 323        |
| 28.4        | 롤과 그 동료들 . . . . .                                                | 325        |
| 28.5        | 매끄러운 함수 . . . . .                                                 | 328        |
| 28.6        | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                    | 328        |
| <b>29</b>   | <b>먹급수와 테일러 급수</b>                                                | <b>331</b> |
| 29.1        | 동기 . . . . .                                                      | 331        |
| 29.2        | 먹급수 . . . . .                                                     | 332        |
| 29.3        | 먹급수의 미분 . . . . .                                                 | 333        |
| 29.4        | 해석적 함수 . . . . .                                                  | 334        |
| 29.5        | 오일러 상수와 지수화의 정의 . . . . .                                         | 335        |
| 29.6        | 이는 복소수에 대해서도 마찬가지로 성립하는데, 다만 복소해석학 또한 천<br>국이라는 점만 다릅니다 . . . . . | 336        |
| 29.7        | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                    | 337        |
| <b>30</b>   | <b>리만 적분</b>                                                      | <b>339</b> |
| 30.1        | 균등 연속 . . . . .                                                   | 339        |
| 30.2        | 조밀 집합과 확장 . . . . .                                               | 340        |
| 30.3        | 리만 적분의 정의 . . . . .                                               | 341        |
| 30.4        | 메시(Mesh) . . . . .                                                | 342        |
| 30.5        | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                    | 344        |
| <b>IX</b>   | <b>복소해석학</b>                                                      | <b>347</b> |
| <b>31</b>   | <b>정칙 함수</b>                                                      | <b>349</b> |
| 31.1        | 세상에서 가장 훌륭한 함수들 . . . . .                                         | 349        |
| 31.2        | 복소 미분 . . . . .                                                   | 351        |
| 31.3        | 경로 적분 . . . . .                                                   | 352        |

|           |                                 |            |
|-----------|---------------------------------|------------|
| 31.4      | 코시-구르사 정리                       | 354        |
| 31.5      | 코시의 적분 정리                       | 355        |
| 31.6      | 정칙 함수는 해석적입니다                   | 357        |
| 31.7      | 선택: 정칙 함수가 해석적임을 증명하기           | 359        |
| 31.8      | 생각해 볼 만한 조금 더 어려운 문제            | 362        |
| <b>32</b> | <b>유리형 함수</b>                   | <b>365</b> |
| 32.1      | 세상에서 두 번째로 멋진 함수들               | 365        |
| 32.2      | 유리형 함수                          | 365        |
| 32.3      | 회전수와 유수 정리                      | 369        |
| 32.4      | 편각 원리                           | 371        |
| 32.5      | 여담: 기하학적으로 바라본 편각 원리            | 372        |
| 32.6      | 철학: 정칙 함수는 왜 그렇게 좋은 성질을 가지는가?   | 373        |
| 32.7      | 생각해 볼 만한 조금 더 어려운 문제            | 374        |
| <b>33</b> | <b>정칙 제곱근과 로그</b>               | <b>375</b> |
| 33.1      | 동기 부여: 복소수의 제곱근                 | 375        |
| 33.2      | 정칙 함수의 제곱근                      | 377        |
| 33.3      | 피복 사영                           | 378        |
| 33.4      | 복소 로그                           | 378        |
| 33.5      | 몇 가지 특수한 경우                     | 379        |
| 33.6      | 생각해 볼 만한 조금 더 어려운 문제            | 380        |
| <b>34</b> | <b>보너스: 위상수학적 아벨-루피니 정리</b>     | <b>381</b> |
| 34.1      | 진행 계획                           | 381        |
| 34.2      | 단계 1: 가장 단순한 경우                 | 381        |
| 34.3      | 단계 2: 중첩된 근호                    | 382        |
| 34.4      | 3단계: 정규 군                       | 383        |
| 34.5      | 요약                              | 384        |
| 34.6      | 생각해 볼 만한 조금 더 어려운 문제            | 384        |
| <b>X</b>  | <b>측도론</b>                      | <b>385</b> |
| <b>35</b> | <b>측도 공간</b>                    | <b>387</b> |
| 35.1      | 문자 연상                           | 387        |
| 35.2      | 확률 변수를 통해 측도 공간의 동기 부여하기        | 387        |
| 35.3      | 측도 공간을 기하학적으로 동기 부여하기           | 388        |
| 35.4      | $\sigma$ -대수와 가측 공간             | 388        |
| 35.5      | 측도 공간                           | 389        |
| 35.6      | 바나흐-타르스키의 힌트                    | 391        |
| 35.7      | 가측 함수                           | 391        |
| 35.8      | “거의”라는 단어에 대하여                  | 392        |
| 35.9      | 생각해 볼 만한 조금 더 어려운 문제            | 393        |
| <b>36</b> | <b>보렐 측도와 르베그 측도 구성하기</b>       | <b>395</b> |
| 36.1      | 사전측도                            | 395        |
| 36.2      | 외측도                             | 396        |
| 36.3      | 외측도에 대한 Carathéodory 확장         | 398        |
| 36.4      | 르베그 측도 정의하기                     | 399        |
| 36.5      | 네 번째 행: 준측도에 대한 Carathéodory 정리 | 401        |

|           |                                            |            |
|-----------|--------------------------------------------|------------|
| 36.6      | 지금부터, 우리는 보렐 측도를 가정합니다 . . . . .           | 403        |
| 36.7      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .             | 403        |
| <b>37</b> | <b>르베그 적분</b>                              | <b>405</b> |
| 37.1      | 정의 . . . . .                               | 405        |
| 37.2      | 동치인 정의 . . . . .                           | 408        |
| 37.3      | 리만 적분과의 관계 (또는: 실제로 르베그 적분 계산하기) . . . . . | 409        |
| 37.4      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .             | 410        |
| <b>38</b> | <b>르베그 적분과 순서 교환하기</b>                     | <b>411</b> |
| 38.1      | 극한 교환의 동기 . . . . .                        | 411        |
| 38.2      | 개요 . . . . .                               | 412        |
| 38.3      | 파투 보조정리 . . . . .                          | 413        |
| 38.4      | 그 외 모든 것 . . . . .                         | 413        |
| 38.5      | 푸비니와 토넬리 . . . . .                         | 417        |
| 38.6      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .             | 417        |
| <b>39</b> | <b>보너스: 폰트라긴 쌍대성에 대한 힌트</b>                | <b>419</b> |
| 39.1      | LCA 군 . . . . .                            | 419        |
| 39.2      | 폰트라긴 쌍대 . . . . .                          | 420        |
| 39.3      | 컴팩트한 경우의 정규직교 기저 . . . . .                 | 421        |
| 39.4      | 비컴팩트한 경우의 푸리에 변환 . . . . .                 | 422        |
| 39.5      | 요약 . . . . .                               | 422        |
| 39.6      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .             | 423        |
| <b>XI</b> | <b>확률 (작성 예정)</b>                          | <b>425</b> |
| <b>40</b> | <b>확률 변수 (작성 예정)</b>                       | <b>427</b> |
| 40.1      | 확률 변수 . . . . .                            | 427        |
| 40.2      | 분포 함수 . . . . .                            | 428        |
| 40.3      | 확률 변수의 예 . . . . .                         | 428        |
| 40.4      | 특성 함수 . . . . .                            | 428        |
| 40.5      | 독립 확률 변수 . . . . .                         | 428        |
| 40.6      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .             | 428        |
| <b>41</b> | <b>큰 수의 법칙 (작성 예정)</b>                     | <b>429</b> |
| 41.1      | 수렴의 개념들 . . . . .                          | 429        |
| 41.2      | 약한 큰 수의 법칙 . . . . .                       | 430        |
| 41.3      | 강한 큰 수의 법칙 . . . . .                       | 430        |
| 41.4      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .             | 435        |
| <b>42</b> | <b>정지된 마팅게일 (작성 예정)</b>                    | <b>437</b> |
| 42.1      | 거의 확실하게 돈을 버는 방법 . . . . .                 | 437        |
| 42.2      | 부분 $\sigma$ -대수와 여과 . . . . .              | 437        |
| 42.3      | 조건부 기댓값 . . . . .                          | 439        |
| 42.4      | 슈퍼마팅게일 . . . . .                           | 442        |
| 42.5      | 선택적 정지(Optional stopping) . . . . .        | 444        |
| 42.6      | 최적 정지의 재미있는 응용 (작성 예정) . . . . .           | 446        |
| 42.7      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .             | 449        |

|             |                                               |            |
|-------------|-----------------------------------------------|------------|
| <b>XII</b>  | <b>미분기하학</b>                                  | <b>451</b> |
| <b>43</b>   | <b>올바르게 하는 다변수 미적분학</b>                       | <b>453</b> |
| 43.1        | 전미분                                           | 453        |
| 43.2        | 사영 원리                                         | 455        |
| 43.3        | 전미분과 편미분                                      | 456        |
| 43.4        | (선택) 고계 도함수에 관한 소고                            | 458        |
| 43.5        | 미분 형식을 향하여                                    | 459        |
| 43.6        | 생각해 볼 만한 조금 더 어려운 문제                          | 459        |
| <b>44</b>   | <b>미분 형식</b>                                  | <b>461</b> |
| 44.1        | 미분 형식의 그림                                     | 461        |
| 44.2        | 외미분의 그림                                       | 463        |
| 44.3        | 미분 형식                                         | 464        |
| 44.4        | 외미분                                           | 466        |
| 44.5        | 여담: $\wedge^k(V^\vee)$ 대 $(\wedge^k(V))^\vee$ | 467        |
| 44.6        | 결가지 언급: 호의 길이 $ds$ 는 1-형식이 아닙니다               | 470        |
| 44.7        | 닫힌 형식과 완전 형식                                  | 471        |
| 44.8        | 생각해 볼 만한 조금 더 어려운 문제                          | 472        |
| <b>45</b>   | <b>미분 형식 적분하기</b>                             | <b>473</b> |
| 45.1        | 동기: 선적분                                       | 473        |
| 45.2        | 당겨오기                                          | 474        |
| 45.3        | 세포                                            | 475        |
| 45.4        | 경계                                            | 477        |
| 45.5        | 스토크스 정리                                       | 479        |
| 45.6        | 다시 현실로: 벡터 미적분학에서 배운 내용과의 비교                  | 479        |
| 45.7        | 생각해 볼 만한 조금 더 어려운 문제                          | 483        |
| <b>46</b>   | <b>다양체에 대한 약간의 이야기</b>                        | <b>485</b> |
| 46.1        | 위상 다양체                                        | 485        |
| 46.2        | 매끄러운 다양체                                      | 486        |
| 46.3        | 정칙값 정리                                        | 487        |
| 46.4        | 다양체 위의 미분 형식                                  | 488        |
| 46.5        | 방향                                            | 488        |
| 46.6        | 다양체에 대한 스토크스 정리                               | 489        |
| 46.7        | (선택) 접공간과 여접공간                                | 490        |
| 46.8        | 생각해 볼 만한 조금 더 어려운 문제                          | 492        |
| <b>XIII</b> | <b>리만 곡면</b>                                  | <b>493</b> |
| <b>47</b>   | <b>리만 곡면의 기본 정의</b>                           | <b>495</b> |
| 47.1        | 복소 구조                                         | 495        |
| 47.2        | 리만 곡면                                         | 497        |
| 47.3        | 복소 다양체                                        | 498        |
| 47.4        | 리만 곡면의 예                                      | 498        |
| <b>48</b>   | <b>리만 곡면 사이의 사상</b>                           | <b>501</b> |
| 48.1        | 정의                                            | 501        |
| 48.2        | 리만 구면으로 가는 함수                                 | 501        |

|            |                                |            |
|------------|--------------------------------|------------|
| 48.3       | 그 밖의 몇 가지 좋은 성질들               | 502        |
| 48.4       | 사상의 중복도                        | 504        |
| 48.5       | 유리형 함수의 위수의 합                  | 505        |
| 48.6       | 후르비츠 공식                        | 505        |
| 48.7       | 항등 정리                          | 505        |
| <b>49</b>  | <b>아핀 평면 곡선과 사영 평면 곡선</b>      | <b>507</b> |
| 49.1       | 아핀 평면 곡선                       | 507        |
| 49.2       | 사영직선 $\mathbb{CP}^1$           | 512        |
| 49.3       | 사영 평면 곡선                       | 513        |
| 49.4       | 구멍 메우기                         | 514        |
| 49.5       | 평면 곡선의 마디점                     | 515        |
| <b>50</b>  | <b>미분 형식</b>                   | <b>517</b> |
| 50.1       | $\mathbb{C}$ 위의 미분 형식          | 517        |
| 50.2       | 미분 형식의 시각화                     | 517        |
| <b>51</b>  | <b>리만-로흐 정리</b>                | <b>521</b> |
| 51.1       | 동기                             | 521        |
| 51.2       | 인자                             | 523        |
| 51.3       | 제수의 차수                         | 524        |
| 51.4       | 유리형 함수의 주인자(principal divisor) | 524        |
| 51.5       | 리만-로흐 정리                       | 525        |
| <b>52</b>  | <b>선다발</b>                     | <b>527</b> |
| 52.1       | 개요                             | 527        |
| 52.2       | 정의                             | 527        |
| 52.3       | 선다발 시각화하기                      | 528        |
| 52.4       | 선다발 사이의 사상                     | 534        |
| 52.5       | 가역층과의 관계                       | 534        |
| <b>XIV</b> | <b>대수적 정수론 I: 정수환</b>          | <b>535</b> |
| <b>53</b>  | <b>대수적 정수</b>                  | <b>537</b> |
| 53.1       | 고등학교 대수학으로부터의 동기               | 537        |
| 53.2       | 대수적 수와 대수적 정수                  | 538        |
| 53.3       | 수체                             | 540        |
| 53.4       | 원시원소 정리, 그리고 단생성 확대            | 540        |
| 53.5       | 생각해 볼 만한 조금 더 어려운 문제           | 541        |
| <b>54</b>  | <b>정수환</b>                     | <b>543</b> |
| 54.1       | 노름과 자취                         | 543        |
| 54.2       | 정수 환                           | 547        |
| 54.3       | 단생성 확대에 대하여                    | 550        |
| 54.4       | 생각해 볼 만한 조금 더 어려운 문제           | 551        |
| <b>55</b>  | <b>유일 인수분해 (드디어!)</b>          | <b>553</b> |
| 55.1       | 동기                             | 553        |
| 55.2       | 아이디얼 산술                        | 554        |
| 55.3       | 데데킨트 정역                        | 555        |
| 55.4       | 유일 인수분해가 성립합니다                 | 557        |

|           |                                                |            |
|-----------|------------------------------------------------|------------|
| 55.5      | 인수분해 알고리즘                                      | 559        |
| 55.6      | 분수 아이디얼                                        | 562        |
| 55.7      | 아이디얼 노름                                        | 563        |
| 55.8      | 생각해 볼 만한 조금 더 어려운 문제                           | 564        |
| <b>56</b> | <b>민코프스키 경계와 유상군</b>                           | <b>567</b> |
| 56.1      | 유상군                                            | 567        |
| 56.2      | 수체의 판별식                                        | 568        |
| 56.3      | 수체의 시그니처                                       | 571        |
| 56.4      | 민코프스키 정리                                       | 573        |
| 56.5      | 함정 상자                                          | 574        |
| 56.6      | 민코프스키 경계                                       | 575        |
| 56.7      | 유수군은 유한합니다                                     | 576        |
| 56.8      | 유수의 계산                                         | 577        |
| 56.9      | 선택: $\mathcal{O}_K$ 가 자유 $\mathbb{Z}$ -가군임을 증명 | 580        |
| 56.10     | 생각해 볼 만한 조금 더 어려운 문제                           | 585        |
| <b>57</b> | <b>판별식의 추가 성질</b>                              | <b>587</b> |
| 57.1      | 생각해 볼 만한 조금 더 어려운 문제                           | 587        |
| <b>58</b> | <b>보너스: 펠 방정식을 풀어봅시다!</b>                      | <b>589</b> |
| 58.1      | 단위                                             | 589        |
| 58.2      | 디리클레 단위 정리                                     | 590        |
| 58.3      | 기본 단위 찾기                                       | 591        |
| 58.4      | 펠 방정식                                          | 592        |
| 58.5      | 생각해 볼 만한 조금 더 어려운 문제                           | 593        |
| <b>XV</b> | <b>대수적 정수론 II: 갈루아 이론과 분기 이론</b>               | <b>595</b> |
| <b>59</b> | <b>갈루아에 관한 것들</b>                              | <b>597</b> |
| 59.1      | 동기                                             | 597        |
| 59.2      | 체 확대, 대수적 확대, 분해체                              | 598        |
| 59.3      | 수체의 대수적 폐포로의 매장                                | 599        |
| 59.4      | 모두가 표수 2를 싫어하는 이유: 분리 가능 대 기약                  | 600        |
| 59.5      | 자기동형사상군과 갈루아 확대                                | 602        |
| 59.6      | 갈루아 이론의 기본 정리                                  | 605        |
| 59.7      | 생각해 볼 만한 조금 더 어려운 문제                           | 606        |
| 59.8      | (선택) 갈루아 확장이 분해체임의 증명                          | 607        |
| <b>60</b> | <b>유한체</b>                                     | <b>609</b> |
| 60.1      | 유한체의 예                                         | 609        |
| 60.2      | 유한체는 소수의 거듭제곱 위수를 가짐                           | 610        |
| 60.3      | 모든 유한체는 동형입니다                                  | 611        |
| 60.4      | 유한체의 갈루아 이론                                    | 612        |
| 60.5      | 추가: 유한체의 곱셈군                                   | 613        |
| 60.6      | 생각해 볼 만한 조금 더 어려운 문제                           | 614        |
| <b>61</b> | <b>분지 이론</b>                                   | <b>615</b> |
| 61.1      | 분지된 / 비활성 / 분할 소수                              | 615        |
| 61.2      | 소수는 $\Delta_K$ 를 나눌 때에만 분지됩니다                  | 616        |

|            |                                                         |            |
|------------|---------------------------------------------------------|------------|
| 61.3       | 관성차수 . . . . .                                          | 616        |
| 61.4       | 갈루아 확장의 마법 . . . . .                                    | 617        |
| 61.5       | (선택) 분해군과 관성군 . . . . .                                 | 620        |
| 61.6       | 결가지 소견: 더 일반적인 갈루아 확장 . . . . .                         | 622        |
| 61.7       | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                          | 623        |
| <b>62</b>  | <b>프로베니우스 원소</b>                                        | <b>625</b> |
| 62.1       | 프로베니우스 원소들 . . . . .                                    | 625        |
| 62.2       | 컬레류 . . . . .                                           | 627        |
| 62.3       | 체보타레프 밀도 정리 . . . . .                                   | 628        |
| 62.4       | 예시: 원분체의 프로베니우스 원소 . . . . .                            | 629        |
| 62.5       | 프로베니우스 원소는 제한 사상과 잘 어울립니다 . . . . .                     | 629        |
| 62.6       | 응용: 이차 상호법칙 . . . . .                                   | 630        |
| 62.7       | 프로베니우스 원소는 인수분해를 통제합니다 . . . . .                        | 632        |
| 62.8       | 응용 예시: IMO 2003 문제 6 . . . . .                          | 635        |
| 62.9       | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                          | 636        |
| <b>63</b>  | <b>보너스: 아르틴 상호법칙에 대하여</b>                               | <b>639</b> |
| 63.1       | 개요 . . . . .                                            | 639        |
| 63.2       | 무한 소수 . . . . .                                         | 640        |
| 63.3       | 무한 소수를 이용한 모듈러 산술 . . . . .                             | 640        |
| 63.4       | 확장에서 무한 소수 . . . . .                                    | 642        |
| 63.5       | 프로베니우스 원소와 아르틴 기호 . . . . .                             | 643        |
| 63.6       | 아르틴 상호법칙 . . . . .                                      | 645        |
| 63.7       | 응용: 두 제곱수의 합의 일반화 . . . . .                             | 648        |
| 63.8       | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                          | 652        |
| <b>XVI</b> | <b>대수적 위상수학 I: 호모토피</b>                                 | <b>653</b> |
| <b>64</b>  | <b>몇 가지 위상수학적 구성</b>                                    | <b>655</b> |
| 64.1       | 구 . . . . .                                             | 655        |
| 64.2       | 몫위상 . . . . .                                           | 655        |
| 64.3       | 곱위상 . . . . .                                           | 657        |
| 64.4       | 분리합집합과 켤레 . . . . .                                     | 658        |
| 64.5       | CW 복합체 . . . . .                                        | 659        |
| 64.6       | 원환면, 클라인 병, $\mathbb{RP}^n$ , $\mathbb{CP}^n$ . . . . . | 660        |
| 64.7       | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                          | 666        |
| <b>65</b>  | <b>기본군</b>                                              | <b>667</b> |
| 65.1       | 경로를 융합하기 . . . . .                                      | 667        |
| 65.2       | 기본군 . . . . .                                           | 668        |
| 65.3       | 기본군은 위상동형사상에 대해 불변입니다 . . . . .                         | 673        |
| 65.4       | 고차 호모토피 군 . . . . .                                     | 673        |
| 65.5       | 호모토피 동치인 공간 . . . . .                                   | 674        |
| 65.6       | 점을 가진 호모토피 범주 . . . . .                                 | 676        |
| 65.7       | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                          | 677        |
| <b>66</b>  | <b>피복 사영</b>                                            | <b>679</b> |
| 66.1       | 균등 피복과 피복 사영 . . . . .                                  | 679        |
| 66.2       | 올림 정리 . . . . .                                         | 681        |

|              |                                    |            |
|--------------|------------------------------------|------------|
| 66.3         | 들어올리기 대응 . . . . .                 | 684        |
| 66.4         | 정칙 피복(Regular coverings) . . . . . | 685        |
| 66.5         | 기본군의 대수 . . . . .                  | 687        |
| 66.6         | 생각해 볼 만한 조금 더 어려운 문제 . . . . .     | 688        |
| <b>XVII</b>  | <b>범주론</b>                         | <b>689</b> |
| <b>67</b>    | <b>대상과 사상</b>                      | <b>691</b> |
| 67.1         | 동기: 동형사상 . . . . .                 | 691        |
| 67.2         | 범주, 그리고 그 예시들 . . . . .            | 691        |
| 67.3         | 범주 안의 특별한 대상들 . . . . .            | 695        |
| 67.4         | 이항 곱 . . . . .                     | 696        |
| 67.5         | 단사 사상과 전사 사상 . . . . .             | 699        |
| 67.6         | 생각해 볼 만한 조금 더 어려운 문제 . . . . .     | 701        |
| <b>68</b>    | <b>함자와 자연 변환</b>                   | <b>703</b> |
| 68.1         | 함자의 여러 예 . . . . .                 | 703        |
| 68.2         | 공변 함자 . . . . .                    | 704        |
| 68.3         | 대상의 색인 족으로서의 공변 함자 . . . . .       | 707        |
| 68.4         | 반변 함자 . . . . .                    | 708        |
| 68.5         | 범주의 동치 . . . . .                   | 709        |
| 68.6         | (선택) 자연 변환 . . . . .               | 709        |
| 68.7         | (선택) 요네다 보조정리 . . . . .            | 711        |
| 68.8         | 생각해 볼 만한 조금 더 어려운 문제 . . . . .     | 713        |
| <b>69</b>    | <b>범주에서의 극한 (작성 예정)</b>            | <b>715</b> |
| 69.1         | 등화자 . . . . .                      | 715        |
| 69.2         | 당겨오기 사각형 (작성 예정) . . . . .         | 716        |
| 69.3         | 극한 . . . . .                       | 716        |
| 69.4         | 생각해 볼 만한 조금 더 어려운 문제 . . . . .     | 716        |
| <b>70</b>    | <b>아벨 범주</b>                       | <b>717</b> |
| 70.1         | 영 대상, 핵, 여핵, 그리고 상 . . . . .       | 717        |
| 70.2         | 가법 범주와 아벨 범주 . . . . .             | 718        |
| 70.3         | 완전열 . . . . .                      | 720        |
| 70.4         | 프레이드-미첼 매장 정리 . . . . .            | 721        |
| 70.5         | 긴 완전열 쪼개기 . . . . .                | 723        |
| 70.6         | 생각해 볼 만한 조금 더 어려운 문제 . . . . .     | 723        |
| <b>XVIII</b> | <b>대수적 위상수학 II: 호몰로지</b>           | <b>725</b> |
| <b>71</b>    | <b>특이 호몰로지</b>                     | <b>727</b> |
| 71.1         | 단체와 경계 . . . . .                   | 727        |
| 71.2         | 특이 호몰로지 군 . . . . .                | 728        |
| 71.3         | 호몰로지 함자와 사슬 복합체 . . . . .          | 733        |
| 71.4         | 사슬 복합체의 더 많은 예시 . . . . .          | 737        |
| 71.5         | 생각해 볼 만한 조금 더 어려운 문제 . . . . .     | 739        |
| <b>72</b>    | <b>긴 완전열</b>                       | <b>741</b> |
| 72.1         | 짧은 완전열과 네 가지 예시 . . . . .          | 741        |

|            |                                       |            |
|------------|---------------------------------------|------------|
| 72.2       | 호몰로지 군의 긴 완전열 . . . . .               | 743        |
| 72.3       | 마이어-피토리스 완전열 . . . . .                | 745        |
| 72.4       | 생각해 볼 만한 조금 더 어려운 문제 . . . . .        | 751        |
| <b>73</b>  | <b>절제와 상대 호몰로지</b>                    | <b>753</b> |
| 73.1       | 동기 . . . . .                          | 753        |
| 73.2       | 긴 완전열 . . . . .                       | 754        |
| 73.3       | 쌍의 범주 . . . . .                       | 755        |
| 73.4       | 절단 . . . . .                          | 757        |
| 73.5       | 몇 가지 응용 . . . . .                     | 758        |
| 73.6       | 차원의 불변성 . . . . .                     | 759        |
| 73.7       | 생각해 볼 만한 조금 더 어려운 문제 . . . . .        | 760        |
| <b>74</b>  | <b>보너스: 세포 호몰로지</b>                   | <b>761</b> |
| 74.1       | 차수 . . . . .                          | 761        |
| 74.2       | 세포 사슬 복합체 . . . . .                   | 762        |
| 74.3       | 여담: 왜 호몰로지 군들이 같은가? . . . . .         | 764        |
| 74.4       | 응용: 베티 수를 통한 오일러 지표 . . . . .         | 766        |
| 74.5       | 세포 경계 공식 . . . . .                    | 767        |
| 74.6       | 생각해 볼 만한 조금 더 어려운 문제 . . . . .        | 770        |
| <b>75</b>  | <b>특이 코호몰로지</b>                       | <b>773</b> |
| 75.1       | 코사슬 복합체 . . . . .                     | 773        |
| 75.2       | 공간의 코호몰로지 . . . . .                   | 774        |
| 75.3       | 공간들의 코호몰로지는 함자적입니다 . . . . .          | 775        |
| 75.4       | 보편 계수 정리 . . . . .                    | 776        |
| 75.5       | 보편 계수 정리에 대한 설명 . . . . .             | 777        |
| 75.6       | 코호몰로지 군 계산 예시 . . . . .               | 778        |
| 75.7       | 코호몰로지 군의 시각화 . . . . .                | 780        |
| 75.8       | 상대 코호몰로지 군 . . . . .                  | 783        |
| 75.9       | 생각해 볼 만한 조금 더 어려운 문제 . . . . .        | 784        |
| <b>76</b>  | <b>코호몰로지의 응용</b>                      | <b>785</b> |
| 76.1       | Poincaré 쌍대성 . . . . .                | 785        |
| 76.2       | 드람 코호몰로지 . . . . .                    | 785        |
| 76.3       | 등급 환 . . . . .                        | 787        |
| 76.4       | 컵곱 . . . . .                          | 789        |
| 76.5       | 상대 코호몰로지 유사환 . . . . .                | 792        |
| 76.6       | 췌기합 . . . . .                         | 793        |
| 76.7       | 교차곱 . . . . .                         | 795        |
| 76.8       | Künneth 공식 . . . . .                  | 799        |
| 76.9       | 생각해 볼 만한 조금 더 어려운 문제 . . . . .        | 801        |
| <b>XIX</b> | <b>대수기하학 I: 고전적 다양체</b>               | <b>803</b> |
| <b>77</b>  | <b>아핀 다양체</b>                         | <b>805</b> |
| 77.1       | 아핀 다양체 . . . . .                      | 805        |
| 77.2       | 아이디얼을 통한 아핀 다양체의 명명 . . . . .         | 806        |
| 77.3       | 근 아이디얼과 힐베르트의 영점 정리 . . . . .         | 807        |
| 77.4       | $\mathbb{A}^1$ 에서 대수다양체의 그림 . . . . . | 808        |

|           |                                                  |            |
|-----------|--------------------------------------------------|------------|
| 77.5      | 소 아이디얼은 기약 아핀 다양체에 대응합니다 . . . . .               | 810        |
| 77.6      | $\mathbb{A}^2$ 와 $\mathbb{A}^3$ 에서의 그림 . . . . . | 810        |
| 77.7      | 극대 아이디얼 . . . . .                                | 811        |
| 77.8      | 비근호(non-radical) 아이디얼을 통해 스킴을 동기 부여하기 . . . . .  | 812        |
| 77.9      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                   | 813        |
| <b>78</b> | <b>환 달린 공간으로서의 아핀 다양체</b>                        | <b>815</b> |
| 78.1      | 개요 . . . . .                                     | 815        |
| 78.2      | $\mathbb{A}^n$ 위의 자리스키 위상 . . . . .              | 815        |
| 78.3      | 아핀 다양체 위의 자리스키 위상 . . . . .                      | 817        |
| 78.4      | 좌표환 . . . . .                                    | 818        |
| 78.5      | 정칙 함수의 층 . . . . .                               | 819        |
| 78.6      | 특수 열린집합 위의 정칙 함수 . . . . .                       | 821        |
| 78.7      | 베이비 환달린 공간 . . . . .                             | 822        |
| 78.8      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                   | 823        |
| <b>79</b> | <b>사영 다양체</b>                                    | <b>825</b> |
| 79.1      | 등급환 . . . . .                                    | 825        |
| 79.2      | 주변 공간 . . . . .                                  | 826        |
| 79.3      | 동차 아이디얼 . . . . .                                | 828        |
| 79.4      | 환달린 공간으로서 . . . . .                              | 829        |
| 79.5      | 정칙함수의 예시 . . . . .                               | 830        |
| 79.6      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                   | 832        |
| <b>80</b> | <b>보너스: 베주 정리(Bézout's theorem)</b>              | <b>833</b> |
| 80.1      | 근기가 아닌 아이디얼 . . . . .                            | 833        |
| 80.2      | 유한개 점들의 힐베르트 함수 . . . . .                        | 834        |
| 80.3      | 힐베르트 다항식 . . . . .                               | 836        |
| 80.4      | Bézout의 정리 . . . . .                             | 838        |
| 80.5      | 응용 . . . . .                                     | 839        |
| 80.6      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                   | 840        |
| <b>81</b> | <b>대수다양체의 사상</b>                                 | <b>843</b> |
| 81.1      | 초급 유유평간의 사상 정의하기 . . . . .                       | 843        |
| 81.2      | 가장 단순한 예시 분류 . . . . .                           | 844        |
| 81.3      | 몇 가지 추가 응용과 예시 . . . . .                         | 846        |
| 81.4      | 쌍곡선 효과 . . . . .                                 | 847        |
| 81.5      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                   | 849        |
| <b>XX</b> | <b>대수기하학 II: 아핀 스킴</b>                           | <b>851</b> |
| <b>82</b> | <b>층과 환 달린 공간</b>                                | <b>855</b> |
| 82.1      | 동기와 주의사항 . . . . .                               | 855        |
| 82.2      | 준층 . . . . .                                     | 855        |
| 82.3      | 줄기와 짝 . . . . .                                  | 857        |
| 82.4      | 층 . . . . .                                      | 861        |
| 82.5      | 층에서 단면은 짝의 수열"입니다" . . . . .                     | 862        |
| 82.6      | 층화(선택) . . . . .                                 | 864        |
| 82.7      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                   | 865        |

|           |                                                                              |            |
|-----------|------------------------------------------------------------------------------|------------|
| <b>83</b> | <b>국소화</b>                                                                   | <b>867</b> |
| 83.1      | 스포일러 . . . . .                                                               | 867        |
| 83.2      | 정의 . . . . .                                                                 | 868        |
| 83.3      | 원소를 제외한 국소화 . . . . .                                                        | 869        |
| 83.4      | 소 아이디얼에서의 국소화 . . . . .                                                      | 870        |
| 83.5      | 국소화의 소 아이디얼 . . . . .                                                        | 872        |
| 83.6      | 몫환의 소 아이디얼 . . . . .                                                         | 873        |
| 83.7      | 국소화는 몫과 교환됩니다 . . . . .                                                      | 874        |
| 83.8      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                               | 876        |
| <b>84</b> | <b>아핀 스킴: 자리스키 위상</b>                                                        | <b>877</b> |
| 84.1      | 조금 더 예고하자면 . . . . .                                                         | 877        |
| 84.2      | 점들의 집합 . . . . .                                                             | 878        |
| 84.3      | 스펙트럼 위의 자리스키 위상 . . . . .                                                    | 879        |
| 84.4      | 크를 차원 . . . . .                                                              | 882        |
| 84.5      | 근기에 관하여 . . . . .                                                            | 883        |
| 84.6      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                               | 885        |
| <b>85</b> | <b>아핀 스킴: 층</b>                                                              | <b>887</b> |
| 85.1      | 구조층의 쓸모없는 정의 . . . . .                                                       | 887        |
| 85.2      | 특별 열린집합의 가치 (또는: 실제로 절편을 계산하는 방법) . . . . .                                  | 888        |
| 85.3      | 구조층의 줄기 . . . . .                                                            | 890        |
| 85.4      | 국소환과 잉여체: 싹과 값을 잇는 다리 . . . . .                                              | 891        |
| 85.5      | 요약 . . . . .                                                                 | 894        |
| 85.6      | 함수는 값이 아니라 싹에 의해 결정됩니다 . . . . .                                             | 894        |
| 85.7      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                               | 895        |
| <b>86</b> | <b>막간: 아핀 스킴의 열여덟 가지 예시</b>                                                  | <b>897</b> |
| 86.1      | 예시: $\text{Spec } k$ , 하나의 점 . . . . .                                       | 897        |
| 86.2      | $\text{Spec } \mathbb{C}[x]$ , 일차원 직선 . . . . .                              | 897        |
| 86.3      | $\text{Spec } \mathbb{R}[x]$ , 복소 켈레가 붙은 일차원 직선(영점 정리를 두려워하지 마십시오) . . . . . | 898        |
| 86.4      | $\text{Spec } k[x]$ , 임의의 바탕체 위에서 . . . . .                                  | 899        |
| 86.5      | $\text{Spec } \mathbb{Z}$ , 1차원 스킴 . . . . .                                 | 899        |
| 86.6      | $\text{Spec } k[x]/(x^2 - 7x + 12)$ , 두 점 . . . . .                          | 900        |
| 86.7      | $\text{Spec } k[x]/(x^2)$ , 이중점 . . . . .                                    | 900        |
| 86.8      | $\text{Spec } k[x]/(x^3 - 5x^2)$ , 이중점과 단일점 . . . . .                        | 901        |
| 86.9      | $\text{Spec } \mathbb{Z}/60\mathbb{Z}$ , 세 점을 가진 스킴 . . . . .                | 901        |
| 86.10     | $\text{Spec } k[x, y]$ , 즉 이차원 평면 . . . . .                                  | 902        |
| 86.11     | $\text{Spec } \mathbb{Z}[x]$ , 이차원 스킴, 그리고 멤퍼드의 그림 . . . . .                 | 903        |
| 86.12     | $\text{Spec } k[x, y]/(y - x^2)$ , 포물선 . . . . .                             | 904        |
| 86.13     | $\text{Spec } \mathbb{Z}[i]$ , 가우스 정수 (일차원) . . . . .                        | 905        |
| 86.14     | 긴 예제: $\text{Spec } k[x, y]/(xy)$ , 두 축 . . . . .                            | 906        |
| 86.15     | $\text{Spec } k[x, x^{-1}]$ , 구멍 뚫린 직선(또는 쌍곡선) . . . . .                     | 908        |
| 86.16     | $\text{Spec } k[x]_{(x)}$ , 직선의 원점을 확대한 모습 . . . . .                         | 909        |
| 86.17     | $\text{Spec } k[x, y]_{(x, y)}$ , 평면의 원점을 확대한 모습 . . . . .                   | 910        |
| 86.18     | $\text{Spec } k[x, y]_{(0)} = \text{Spec } k(x, y)$ , 일반점 위의 줄기 . . . . .    | 910        |
| 86.19     | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                               | 910        |
| <b>87</b> | <b>국소 환 달린 공간의 사상</b>                                                        | <b>911</b> |
| 87.1      | 단면을 통한 환 달린 공간의 사상 . . . . .                                                 | 911        |
| 87.2      | 줄기를 통한 환 달린 공간의 사상 . . . . .                                                 | 912        |

|            |                                 |            |
|------------|---------------------------------|------------|
| 87.3       | 국소 환 달린 공간의 사상                  | 913        |
| 87.4       | 아핀 스킴 사이의 사상의 몇 가지 예            | 914        |
| 87.5       | 큰 정리                            | 917        |
| 87.6       | 스킴 사상의 추가 예시                    | 919        |
| 87.7       | 비아핀 스킴에 관하여 조금                  | 920        |
| 87.8       | 여기서 어디로 갈 것인가                   | 922        |
| 87.9       | 생각해 볼 만한 조금 더 어려운 문제            | 922        |
| <b>XXI</b> | <b>집합론 I: ZFC, 순서수, 그리고 기수</b>  | <b>923</b> |
| <b>88</b>  | <b>막간: 코시의 함수 방정식과 초른의 보조정리</b> | <b>925</b> |
| 88.1       | 괴물을 하나 만들어 봅시다                  | 925        |
| 88.2       | 유한 귀납법 복습                       | 926        |
| 88.3       | 초한 귀납법                          | 926        |
| 88.4       | 함수 방정식 마무리하기                    | 928        |
| 88.5       | 초른의 보조정리                        | 929        |
| 88.6       | 생각해 볼 만한 조금 더 어려운 문제            | 931        |
| <b>89</b>  | <b>선택공리를 포함한 체르멜로-프렝켈</b>       | <b>933</b> |
| 89.1       | 궁극의 함수방정식                       | 933        |
| 89.2       | 칸토어의 역설                         | 933        |
| 89.3       | 집합론의 언어                         | 934        |
| 89.4       | ZFC의 공리들                        | 935        |
| 89.5       | 부호화                             | 937        |
| 89.6       | 선택과 정렬순서                        | 938        |
| 89.7       | 집합 대 클래스                        | 938        |
| 89.8       | 생각해 볼 만한 조금 더 어려운 문제            | 939        |
| <b>90</b>  | <b>순서수</b>                      | <b>941</b> |
| 90.1       | 미취학 아동을 위한 세기                   | 941        |
| 90.2       | 집합론자를 위한 세기                     | 941        |
| 90.3       | 순서수의 정의                         | 944        |
| 90.4       | 순서수는 “높습니다”                     | 945        |
| 90.5       | 초한 귀납법과 초한 재귀법                  | 946        |
| 90.6       | 순서수 산술                          | 947        |
| 90.7       | 집합의 계층                          | 949        |
| 90.8       | 생각해 볼 만한 조금 더 어려운 문제            | 951        |
| <b>91</b>  | <b>기수</b>                       | <b>953</b> |
| 91.1       | 등수인 집합과 기수                      | 953        |
| 91.2       | 기수성                             | 954        |
| 91.3       | 알레프 수                           | 954        |
| 91.4       | 기수 산술                           | 955        |
| 91.5       | 기수 지수 연산                        | 957        |
| 91.6       | 공종성                             | 957        |
| 91.7       | 비가측 기수                          | 959        |
| 91.8       | 생각해 볼 만한 조금 더 어려운 문제            | 960        |

|              |                                |             |
|--------------|--------------------------------|-------------|
| <b>XXII</b>  | <b>집합론 II: 모형 이론과 강제법</b>      | <b>961</b>  |
| <b>92</b>    | <b>내부 모형 이론</b>                | <b>963</b>  |
| 92.1         | 모형 . . . . .                   | 963         |
| 92.2         | 문장과 만족 . . . . .               | 964         |
| 92.3         | 레비 계층 . . . . .                | 966         |
| 92.4         | 부분구조와 타르스키-보트 정리 . . . . .     | 967         |
| 92.5         | ZFC의 공리 얻기 . . . . .           | 968         |
| 92.6         | Mostowski 붕괴 . . . . .         | 969         |
| 92.7         | 비가측 기수 추가하기 . . . . .          | 970         |
| 92.8         | 가산 모형에 관한 자주 묻는 질문 . . . . .   | 972         |
| 92.9         | 내부 모형 그려 보기 . . . . .          | 972         |
| 92.10        | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 974         |
| <b>93</b>    | <b>강제법(Forcing)</b>            | <b>975</b>  |
| 93.1         | 순서집합 설정하기 . . . . .            | 976         |
| 93.2         | 부분 순서 집합의 추가 성질 . . . . .      | 978         |
| 93.3         | 이름과 제네릭 확장 . . . . .           | 979         |
| 93.4         | 강제법의 기본 정리 . . . . .           | 982         |
| 93.5         | (선택적) 관계 정의하기 . . . . .        | 982         |
| 93.6         | 나머지 공리들 . . . . .              | 984         |
| 93.7         | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 985         |
| <b>94</b>    | <b>연속체 가설 깨뜨리기</b>             | <b>987</b>  |
| 94.1         | 실수 추가하기 . . . . .              | 987         |
| 94.2         | 가산 사슬 조건 . . . . .             | 988         |
| 94.3         | 기수의 보존 . . . . .               | 989         |
| 94.4         | 무한 조합론 . . . . .               | 990         |
| 94.5         | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 991         |
| <b>XXIII</b> | <b>부록</b>                      | <b>993</b>  |
| <b>A</b>     | <b>교육적 논평과 참고 문헌</b>           | <b>995</b>  |
| A.1          | 기초 대수학과 위상수학 . . . . .         | 995         |
| A.2          | 2학년 주제 . . . . .               | 996         |
| A.3          | 고급 주제 . . . . .                | 997         |
| A.4          | Napkin에 없는 주제들 . . . . .       | 998         |
| <b>B</b>     | <b>선정된 문제들에 대한 힌트</b>          | <b>999</b>  |
| <b>C</b>     | <b>선정된 풀이의 개요</b>              | <b>1011</b> |
| <b>D</b>     | <b>표기법 용어집</b>                 | <b>1037</b> |
| D.1          | 일반 . . . . .                   | 1037        |
| D.2          | 함수와 집합 . . . . .               | 1037        |
| D.3          | 추상대수학과 선형대수학 . . . . .         | 1038        |
| D.4          | 양자 계산 . . . . .                | 1039        |
| D.5          | 위상수학과 실/복소 해석학 . . . . .       | 1039        |
| D.6          | 측도론과 확률론 . . . . .             | 1040        |
| D.7          | 대수적 위상수학 . . . . .             | 1040        |
| D.8          | 범주론 . . . . .                  | 1041        |

|          |                      |             |
|----------|----------------------|-------------|
| D.9      | 미분기하학                | 1042        |
| D.10     | 대수적 수론               | 1042        |
| D.11     | 표현론                  | 1043        |
| D.12     | 대수기하학                | 1044        |
| D.13     | 집합론                  | 1045        |
| <b>E</b> | <b>집합과 함수에 관한 용어</b> | <b>1047</b> |
| E.1      | 집합                   | 1047        |
| E.2      | 함수                   | 1048        |
| E.3      | 동치 관계                | 1050        |



# I

## 시작하기

## 제I부: 목차

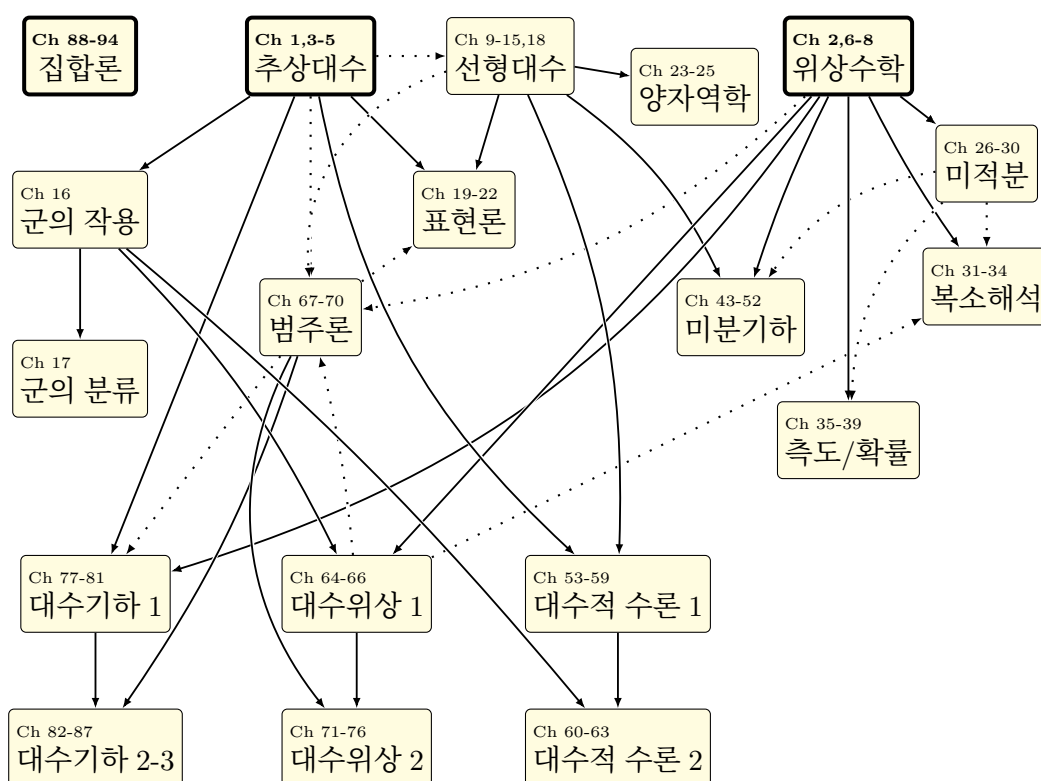
---

|          |                                |           |
|----------|--------------------------------|-----------|
| <b>0</b> | <b>세일즈 피치</b>                  | <b>37</b> |
| 0.1      | 기초 . . . . .                   | 37        |
| 0.2      | 추상대수학 . . . . .                | 38        |
| 0.3      | 실해석학과 복소해석학 . . . . .          | 39        |
| 0.4      | 대수적 수론 . . . . .               | 40        |
| 0.5      | 대수적 위상수학 . . . . .             | 40        |
| 0.6      | 대수기하학 . . . . .                | 41        |
| 0.7      | 집합론 . . . . .                  | 42        |
| <br>     |                                |           |
| <b>1</b> | <b>군</b>                       | <b>43</b> |
| 1.1      | 군의 정의와 예시 . . . . .            | 43        |
| 1.2      | 군의 성질 . . . . .                | 46        |
| 1.3      | 동형사상 . . . . .                 | 48        |
| 1.4      | 군의 위수와 라그랑주 정리 . . . . .       | 50        |
| 1.5      | 부분군 . . . . .                  | 51        |
| 1.6      | 작은 위수의 군 . . . . .             | 52        |
| 1.7      | 중요하지 않은 긴 여담 . . . . .         | 53        |
| 1.8      | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 53        |
| <br>     |                                |           |
| <b>2</b> | <b>거리 공간</b>                   | <b>55</b> |
| 2.1      | 거리 공간의 정의와 예시 . . . . .        | 55        |
| 2.2      | 거리 공간에서의 수렴 . . . . .          | 57        |
| 2.3      | 연속 사상 . . . . .                | 58        |
| 2.4      | 위상동형사상 . . . . .               | 59        |
| 2.5      | 확장된 예시/정의: 곱 거리함수 . . . . .    | 60        |
| 2.6      | 열린집합 . . . . .                 | 61        |
| 2.7      | 닫힌집합 . . . . .                 | 64        |
| 2.8      | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 65        |

---

# 0 세일즈 피치

이 장에는 각 부에 대한 소개가 담겨 있으며, 무엇을 읽고 싶은지 결정하는 데 도움을 주고 이들이 어떻게 서로 연결되어 있는지 더 자세히 설명합니다.  
편의를 위해, 프론트매터에 나왔던 의존성 도표를 다시 보여드립니다.



## §0.1 기초

### I. 시작하기.

첫 번째 부에는 대수학과 위상수학이 조금씩 다 들어가야 한다는 설계상의 결정을 내렸습니다: 그래서 이 첫 번째 장은 **군**을 정의하는 것으로 시작하고, 두 번째 장은 **거리 공간**을 정의하는 것으로 시작합니다. 그 의도는 초심자들이 다소 다른 맥락에서 "추가 구조를 가진 집합"의 두 가지 다른 예시를 보게 하고, 이러한 종류의 정의가 계속해서 반복해서 등장할 때를 대비해 최소한의 소양을 갖추게 하려는 것입니다.<sup>1</sup>

### II. 기본 추상대수학.

대수학에 더 마음이 끌리는 사람은 그다음 더 다양한 종류의 대수적 구조로 파고들 수 있습니다: **군**에 대한 몇 가지 추가 세부 사항, 그다음  $\mathbb{Z}$ ,  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ 를 일반화할 수 있게 해줄 **환**과 **체**입니다. 그렇게 하여 대수학에 등장하는 온갖 다른 명사들에 익숙해지는 법을 배우게 되며, 전에는 이야기할 수 없었던 온갖 대상들의 세계가 열리게 됩니다.

우리는 또한 여러분이 알고 있을 법한  $\mathbb{Z}$ 에서의 최대공약수를 일반화하는 **아이디얼**에 이르게 될 것입니다. 예를 들어,  $\gcd(3, 5) = 1$ 이므로  $\mathbb{Z}$ 에서 모든 정수는  $a, b \in \mathbb{Z}$ 에

<sup>1</sup>특히, 군 동형사상을 본 뒤에 위상동형사상이 무엇인지 배우는 것이, 그리고 연속 사상을 본 뒤에 준동형사상이 무엇인지 배우는 것이 더 쉽다고 생각합니다.

대해  $3a + 5b$ 의 형태로 쓸 수 있다는 것을 알고 있을 것입니다. 우리는 이 진술이 실제로는 아이디얼에 대한 진술, 즉 " $\mathbb{Z}$ 에서  $(3, 5) = 1$ "이라는 것을 보게 될 것이고, 따라서 어떤 상황에서 이것이 일반화될 수 있는지, 예컨대 다항식으로 일반화될 수 있는지 이해하게 될 것입니다.

### III. 기본 위상수학.

더 해석학적으로 마음이 끌리는 사람은 대신 위상수학으로 넘어가 공간에 대해 더 배울 수 있습니다. 우리는 "거리 공간"이 실제로는 너무 특수하며, 이른바 **열린집합**에 기반한 **위상 공간**을 다루는 것이 더 낫다는 것을 알게 될 것입니다. 그런 다음 여러분은 몇 가지 기하학적 아이디어의 싹이 트는 것을 보게 되고, 실해석학을 작동하게 만드는 강력한 개념인 **콤팩트성**이라는 정말 훌륭한 개념으로 마무리하게 됩니다.

지금 여러분을 유혹할 콤팩트성 응용의 한 예시입니다: 연속 함수  $f: [0, 1] \rightarrow \mathbb{R}$ 는 항상 최댓값을 달성합니다. (반면,  $x \mapsto 1/x$ 로 정의된  $f: (0, 1) \rightarrow \mathbb{R}$ 는 그렇지 않습니다.) 우리는 그 이유가  $[0, 1]$ 이 콤팩트하기 때문이라는 것을 보게 될 것입니다.

## §0.2 추상대수학

### IV. 선형대수학.

고등학교에서 선형대수학은 종종 정말 만족스럽지 않습니다. 여러분은 이 숫자들의 배열을 받고, 그것들은 별로 말이 되지 않는 방식으로 다루어집니다. 예를 들어, 행렬식은 마치 허공에서 나온 것처럼 보이는 여러 곱의 합으로 이루어진 이상하게 생긴 식으로 정의됩니다. 그것은 어디서 오는 것일까요? 왜  $\det(AB) = \det A \det B$ 가 그토록 기이한 공식으로 성립할까요?

자, 이 모든 것을 설명할 수 있다는 것이 밝혀집니다! 그 비결은 선형대수학을 행렬의 학문으로 생각하지 않고, 대신 선형 사상의 학문으로 생각하는 것입니다. 앞선 장들에서 우리는 "풍부한 구조를 가진 집합"과 "그 사이의 사상"을 이야기함으로써 훌륭한 일반화를 얻었다는 것을 보았습니다. 이번에 우리의 집합은 **벡터 공간**이고 우리의 사상은 **선형 사상**입니다. 우리는 행렬이 실제로는 선형 사상을 숫자의 배열로 적어 내는 하나의 방법일 뿐이라는 것을 알게 될 것이지만, "본질적인" 정의를 사용함으로써 고등학교에서 배운 모든 이상한 공식들의 신비를 벗겨내고 그것들이 어디서 오는지 보여드리겠습니다.

특히, 우리는 열 계수가 행 계수와 같다는 것, 행렬식이 곱셈적이라는 것, 대각합이 대각 원소들의 합이라는 것의 쉬운 증명들을 보게 될 것입니다. 우리는 내적이 어떻게 작동하는지 보고, "고유-"로 시작하는 모든 단어들을 배우게 될 것입니다. 벡터 공간에 익숙해지는 것만으로도 모든 큰 유행어들을 설명할 수 있음을 보여주는 푸리에 해석에 대한 보너스 장까지 있을 것입니다.

### V. 군에 대하여 더 알아보기.

여러분 중 몇몇은 군에 대해 더 관심이 있을 수 있는데, 이 장은 여러분에게 더 나아가 탐구할 방법을 제공할 것입니다. 이는 **군의 작용**에 대한 탐구로 시작하여, 모든 군을 분류하려는 시도를 가능하게 해주는 도구인 **실로우 정리**에 대해 조금 다룹니다.

### VI. 표현론.

$G$ 가 군이라면, 우리는 그것을 행렬로 구현함으로써, 즉 매입  $G \hookrightarrow \mathrm{GL}_n(\mathbb{C})$ 을 고려함으로써 이해하려고 시도할 수 있습니다. 이것들은  $G$ 의 **표현**이라고 불립니다; 이것들은 **기약** 표현으로 분해될 수 있다는 것이 밝혀집니다. 놀랍게도 우리는 그것들 전부를 기본적으로 특징지을 수 있다는 것을 알게 될 것입니다: 그 결과는 짧으면서도 완전히 예상치 못한 것으로 밝혀집니다.

예를 들어, 우리는 주어진 유한군  $G$ 의 기약 표현이 유한개만 존재한다는 것을 알게 될 것입니다; 그것들을  $V_1, V_2, \dots, V_r$ 이라고 표시하면, 우리는  $r$ 이  $G$ 의 켈레류의 개수라는 것을, 그리고 더 나아가 다음이 성립한다는 것을 알게 될 것입니다

$$|G| = (\dim V_1)^2 + \dots + (\dim V_r)^2$$

이는 난데없이 튀어나옵니다!

이 부의 마지막 장은 여러분에게 몇 가지 예상치 못한 따름정리를 보여드릴 것입니다. 그중 하나는 다음과 같습니다:  $G$ 를 유한군이라 하고 각  $g \in G$ 에 대해 변수  $x_g$ 를 만듭니다.  $|G| \times |G|$  행렬  $M$ 은  $(g, h)$ 번째 원소를 변수  $x_{g \cdot h}$ 로 설정하여 정의됩니다. 그러면 이 행렬식은 인수분해된다는 것이 밝혀지며, 그 인수들은 위에서 설명한  $V_i$ 에 대응됩니다:  $\dim V_i$ 번 나타나는 차수  $\dim V_i$ 의 기약 인수가 존재하게 됩니다. **프로베니우스 행렬식**이라 불리는 이 결과는 표현론을 탄생시켰다고 전해집니다.

## VII. 양자 알고리즘.

**쇼어 알고리즘**이 무엇인지 궁금했던 적이 있다면, 이 장에서는 지금까지 쌓아온 선형 대수를 이용해 그것을 알려드립니다!

## §0.3 실해석학과 복소해석학

### VIII. 미적분학 101.

이 부에서는 거리 공간과 위상 공간에 대해 쌓아온 지식을 이용하여, 고등학교 미적분학에서 전형적으로 다루는 정의와 정리들을 짧고 엄밀하게 제시합니다. 즉, **극한**, **급수**, **도함수**, **적분**에 관해 여러분이 이미 보아온 거의 모든 것을 실제로 정의하고 증명합니다.

이것이 다소 벅차 보일 수 있지만, 사실 이 장을 시작할 즈음이면 어려운 작업은 이미 끝나 있습니다: 극한, 열린집합, 콤팩트성이라는 개념이 있으면 AP 미적분학에서 대충 넘어갔던 부분들을 손쉽게 처리할 수 있습니다. 따라서 대부분의 증명은 실제로 상당히 짧을 것입니다. 우리는 뒤로 물러앉아, 앞서 위상수학을 꼼꼼히 공부한 것에 대한 보상으로 모든 조각들이 서서히 맞춰지는 것을 지켜보게 됩니다.

그렇긴 하지만, 만약 잠시 의구심을 접어들 의향이 있다면, 여기 나오는 미적분학의 정확한 세부 사항을 몰라도 다른 부의 대부분을 실제로 읽을 수 있으므로, 어떤 의미에서 이 부는 "선택 사항"입니다.

## IX. 복소해석학.

**정칙 함수**(복소미분가능 함수)는 지금까지 나온 것 중 거의 가장 좋은 것에 가깝다는 것이 밝혀집니다: 이들은 테일러 급수로 주어진다는 것이(즉, 본질적으로 다항식이라는 것이) 밝혀집니다. 이는 정칙 함수  $\mathbb{C} \rightarrow \mathbb{C}$ 에 대해 비합리적일 만큼 좋은 결과들을 증명할 수 있게 해준다는 것을 의미합니다. 예를 들면

- 이들은 단 몇 개의 입력값만으로 결정되고,
- 이들의 등고선 적분은 모두 영이며,
- 상수가 아닌 한 유계일 수 없다는 것 등입니다,
- ....

이어서 정칙 함수의 몫과 같은 **유리형 함수**를 소개하고, 평면에 단순히 고리를 그려 그 위에서 적분함으로써 그 영점을 검출할 수 있음을 알게 됩니다: 여기서 유명한 **유수 정리**가 등장합니다. (연습 문제에서, 이것이 다른 방법으로는 계산할 수 없는 실적분을 계산하는 방법까지도 제공한다는 것을 보게 됩니다.)

## X. 측도론.

측도론은 적분의 업그레이드 버전입니다. 리만 적분은 여러 용도에서 실제로 충분하지 않습니다; 예를 들어,  $f$ 가 유리수에서는 1이고 무리수에서는 0인 함수라면, 우리는  $\int_0^1 f(x) dx = 0$ 이기를 바라겠지만, 리만 적분은 이 함수  $f$ 를 다룰 수 없습니다.

**르베그 적분**은 일반적인 공간  $\Omega$ 에 측도를 부여하여 이를 **측도 공간**으로 만듦으로써 이러한 문제들을 해결할 것입니다. 이를 통해 위 적분이 "유리수는 측도가 0이다"라는 사실 때문에 실제로 0이 되는 더 풍부한 적분 이론을 전개할 수 있게 됩니다. 측도의 개발 자체도 하나의 성취인데, 왜냐하면 이는 넓이와 부피 같은 개념이 의미하는 바를  $\mathbb{R}^n$ 뿐 아니라 어떤 공간에서든—엄밀하고 완전하게 논할 방법을 개발했다는 뜻이기 때문입니다! 따라서 예를 들어 르베그 적분은 우리가 어떤 **측도 공간** 위에서든 함수를 적분할 수 있게 해줄 것입니다.

## XI. 확률 (작성 예정).

측도론의 도구들을 이용하여, 우리는 **확률**에 대해서도 엄밀한 정의를 제시하기 시작할 수 있습니다. 우리는 **확률 변수**가 실제로는 세계들의 측도 공간에서  $\mathbb{R}$ 로 가는 함수임을 알게 되며, 이는 그 확률에 대해 엄밀하게 이야기할 방법을 제공합니다. 그런 다음 우리는 **큰 수의 법칙**과 **중심 극한 정리** 같은 결과들을 진술하기도 쉽고 증명하기도 간단한 방식으로 실제로 서술하기 시작할 수 있습니다.

## XII. 미분기하학.

다변수 미적분학은 온갖 편도함수 때문에 종종 혼란스럽습니다. 하지만 선형대수에 대한 좋은 이해로 무장하면, 우리가 실제로 보고 있는 것은 **전미분**이라는 것을 알게 됩니다: 함수  $f: \mathbb{R}^n \rightarrow \mathbb{R}$ 의 모든 점에서 우리는 편도함수라는 개념을 하나의 대상으로 담아내는 선형 사상  $Df$ 를 대응시킬 수 있습니다. 이렇게 설정하면, **미분 형식**과 **스토크스 정리**의 버전들을 보게 될 것이며, 마침내 표기법  $dx$ 가 실제로 무엇을 의미하는지 알게 될 것입니다. 마지막으로, 다양체 일반에 대해서도 조금 이야기하겠습니다.

# §0.4 대수적 수론

## XIV. 대수적 정수론 I: 정수환.

왜  $3+\sqrt{5}$ 는  $3-\sqrt{5}$ 의 켤레일까요? 펠 방정식에서 사용되는 노름  $\|a+b\sqrt{5}\| = a^2-5b^2$ 이 왜 하필 곱셈적일까요? 왜  $\mathbb{Z}[i]$ 에서는 소수로의 인수분해를 할 수 있는데  $\mathbb{Z}[\sqrt{-5}]$ 에서는 할 수 없을까요? 이 모든 질문과 그 이상이 이 부에서 답을 얻게 되는데, 이때 우리는  $\mathbb{Q}$ 와  $\mathbb{Z}$ 를  $\mathbb{Q}(\sqrt{5})$ 와  $\mathbb{Z}[\sqrt{5}]$  같은 것들로 일반화한 **수체**에 대해 배우게 됩니다. 우리는 소 아이디얼의 유일 인수분해가 성립함을, 여기에 실제로 곱셈적 노름이 관여하고 있음을, 그리고 그 밖의 것들을 알게 됩니다. 또한 펠 방정식이 이 이론으로부터 자연스럽게 도출됨을 보게 됩니다.

## XV. 대수적 정수론 II: 갈루아 이론과 분기 이론.

이제 거창한 유행어들이 모두 등장합니다: **갈루아 군**, **프로베니우스**, 그리고 그 친구들 말입니다. 이차 상호법칙이 프로베니우스 원소의 거동이 드리우는 그림자에 불과함을 보게 될 것이고,  $a \pmod{n}$  꼴인 소수의 무한성에 관한 디리클레 정리를 크게 일반화하는 **체보타레프 밀도 정리**를 만나게 됩니다. 마지막 부분에서는 **유체론**의 위대한 결과 중 하나인 **아르틴 상호법칙**을 서술하고, 이것이 이차 상호법칙과 삼차 상호법칙을 어떻게 일반화하는지도 다룰 것입니다.

# §0.5 대수적 위상수학

## XVI. 대수적 위상수학 I: 호모토피.

환형(annulus)과 원판의 차이는 무엇일까요? 물론 둘 중 하나에는 "구멍"이 있지만, 순수하게 내재적인 위상 공간만 주어졌을 때 이 개념을 정확히 규정하기는 어렵습니다. **기본군**  $\pi_1(X)$ 와 더 일반적인 **호모토피 군**은 이를 정확하게 만들어 줍니다 — 공간 안에 올라가기를 던져 넣고 그것을 다시 감아 들일 수 있는지를 살펴봄으로써, 공간에 구멍이 있다는 발상을 포착하는 아벨 군  $\pi_1(X)$ 를 모든 위상 공간  $X$ 에 대해 정의하는 방법을 찾아낼 것입니다.

놀랍게도 기본군  $\pi_1(X)$ 는 온건한 조건 하에서 소위 **피복 사영**이라는 방식으로  $X$ 를 덮는 방법들을 알려줍니다. 하나의 그림은 실직선  $\mathbb{R}$ 을 나선 모양으로 감아서 원  $S^1$  위로 사영하는 것입니다. 이는  $\pi_1(S^1) = \mathbb{Z}$ 라는 사실에 대응함이 밝혀질 것입니다. 더 일반적으로  $\pi_1(X)$ 의 부분군들은 공간  $X$ 를 덮는 방법들과 전단사 관계에 있게 됩니다!

## XVII. 범주론.

체, 군, 다양체, 거리 공간, 측도 공간, 가군, 표현, 환, 위상 공간, 벡터 공간은 서로 무슨 공통점이 있을까요? 답: 이들은 모두 "추가 구조를 지닌 대상"이며, 그 사이에 사상들이 있다는 것입니다.

**범주**라는 개념은 이 모든 것을 적절하게 일반화합니다. 온갖 종류의 구성과 발상이 범주라는 틀 안으로 추상화될 수 있음을 보게 될 것인데, 이 틀에서는 대상들이 정확히 무엇인지를 굳이 깊이 파고들지 않고, 오직 대상들과 그 사이의 화살표들만을 생각합니다. 그 결과로 많은 **가환 도식**을 그리게 됩니다.

예를 들어, 한 범주의 대상을 취해 다른 범주의 대상을 얻는 방법(예컨대 위에서 나온  $\pi_1$ 처럼, 공간의 범주에서 군의 범주로 가는 경우)은 대개 **함자**일 것입니다.  $G \times H$ ,  $X \times Y$ ,  $R \times S$ , 그리고  $\times$  기호가 들어간 그 무엇이든 곱의 개념으로 통합하고, 그런 다음 훨씬 더 일반적으로 **극한**으로 통합할 것입니다. 마지막 부분에서는 **아벨 범주**에 관해 이야기하고, 유명한 **뱀 보조정리**, **다섯 보조정리** 등에 대해서도 다룹니다.

## XVIII. 대수적 위상수학 II: 호몰로지.

범주론의 언어를 사용하여, 우리는 대수적 위상수학에서의 모험을 다시 이어가는데, 여기서 정의를 내리는 데는 더 오래 걸리지만 실제로 계산하기는 더 쉬운 방식으로 공간의 구멍을 알아채는 또 다른 방법을 주는 **호몰로지 군**을 정의합니다. 그런 다음 이 구성을 뒤집어서, 공간을 구별하는 데 훨씬 더 섬세한 불변량을 주는 소위 **코호몰로지 환**을 얻을 것입니다.

## §0.6 대수기하학

### XIX. 대수기하학 I: 고전적 다양체.

우리는 고전적인 **복소 다양체**에 대한 고전적인 연구, 즉  $\mathbb{C}$  위에서 다항 방정식들의 교집합에 대한 연구로부터 시작합니다. 이는 자연스럽게 우리를 환의 기하학으로 이끌어, 아이디얼을 그림으로 그리는 방법을 제공하고 **힐베르트 영점정리**에 동기를 부여합니다. **자리스키 위상**이 그 모습을 드러낼 것이며, 그 후 우리는 **사영 다양체**와 **유사사영 다양체**를 가지고 놀아볼 것이고, 덤으로 **Bézout의 정리**로 잠시 우회할 것입니다. 이 모든 것이 스킴으로의 여정을 위한 준비가 됩니다.

### XX. 대수기하학 II: 아핀 스킴.

이제 우리는 진지하게 그로텐디크의 **아핀 스킴** 정의로 파고듭니다: 이는 우리의 고전적인 다양체를 일반화한 것으로, 임의의 환  $A$ 에서 시작하여 그 위에 공간  $\text{Spec } A$ 를 구성할 수 있게 해 줍니다. 우리는 여기에 자체의 자리스키 위상을 부여한 다음 그 위에 함수들의 층을 부여하여 **국소 환 달린 공간**으로 만들 것이며, 이 층이 그 위의 **국소화**의 관점에서 효과적으로 이해될 수 있음을 알게 될 것입니다. 우리는 가환대수학의 언어가 기하학적으로 벌어지는 일을 우아하게 일반화해 줌을 알게 될 것입니다.

소 아이디얼은 기약 닫힌집합에, 근기 아이디얼은 닫힌집합에, 극대 아이디얼은 닫힌 점에 대응하는 식입니다. 이를 뒷받침하기 위해 공간과 예시들의 그림을 많이 그릴 것입니다.

## §0.7 집합론

### XXI. 집합론 I: ZFC, 순서수, 그리고 기수.

**러셀의 역설**은 왜 그렇게 큰 문제이며 어떻게 해결될까요? 다들 계속 이야기하는 **이 초론의 보조정리**란 무엇일까요? 이 부분에서는 **체르멜로-프렝켈** 공리와 **선택 공리**를 실제로 서술함으로써, 수학이 맨 밑바닥 토대에서부터 공리적으로 어떻게 세워지는지 그 세부 사항으로 파고들어 이러한 질문들에 대한 답을 배울 것입니다. **순서수**와 **기수**를 만나고, 이들을 가지고 **초한 귀납법**을 수행하는 법을 배울 것입니다.

### XXII. 집합론 II: 모형 이론과 강제법.

**연속체 가설**은 자연수의 크기와 실수의 크기 사이에 어떤 기수도 존재하지 않는다는 것을 말합니다. 이는 공리들과 독립적임이 증명되었습니다 — 증명할 수도 반증할 수도 없습니다. 그런 결과가 대체 어떻게 증명될 수 있었을까요? ZF 공리에 대한 이해를 바탕으로, 약간의 **모델 이론**을 전개한 다음 **강제법**을 사용하여 연속체 가설이 참인 우주의 모델과 거짓인 우주의 모델을 통째로 구성하는 방법을 보이겠습니다.

# 1 군

군은 고등 수학에서 가장 기본적인 구조 중 하나입니다. 이 장에서는 최소한의 내용만 다룰 것입니다: 군이 무엇인지, 그리고 두 군이 언제 같은지에 대해서만 설명하겠습니다.

## §1.1 군의 정의와 예시

**이 절의 대표적인 예:** 정수의 덧셈군  $(\mathbb{Z}, +)$ 과 순환군  $\mathbb{Z}/n\mathbb{Z}$ . 대부분의 군이 비가환적이라는 사실을 잊지 마십시오.

군은 두 가지 데이터로 구성됩니다: 집합  $G$ 와, 몇 가지 성질을 만족하는 결합적 이항 연산  $\star$ 입니다. 군의 정의를 적기 전에, 먼저 두 가지 예시를 들어 보겠습니다.

### 예제 1.1.1 (덧셈 정수)

순서쌍  $(\mathbb{Z}, +)$ 는 군입니다:  $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ 가 집합이고 결합적 연산은 덧셈입니다. 다음을 주목하십시오.

- 원소  $0 \in \mathbb{Z}$ 는 항등원입니다: 임의의  $a$ 에 대해  $a + 0 = 0 + a = a$ 입니다.
- 모든  $a \in \mathbb{Z}$ 는 덧셈에 대한 역원을 가집니다:  $a + (-a) = (-a) + a = 0$ .

이 군을  $\mathbb{Z}$ 라고 부릅니다.

### 예제 1.1.2 (0이 아닌 유리수)

$\mathbb{Q}^\times$ 를 0이 아닌 유리수의 집합이라고 합시다. 순서쌍  $(\mathbb{Q}^\times, \cdot)$ 는 군입니다: 집합은  $\mathbb{Q}^\times$ 이고 결합적 연산은 곱셈입니다. 여기서도 같은 두 가지 좋은 성질을 볼 수 있습니다.

- 원소  $1 \in \mathbb{Q}^\times$ 는 항등원입니다: 임의의 유리수에 대해  $a \cdot 1 = 1 \cdot a = a$ 입니다.
- 임의의 유리수  $x \in \mathbb{Q}^\times$ 에 대해, 다음을 만족하는 역원  $x^{-1}$ 가 존재합니다

$$x \cdot x^{-1} = x^{-1} \cdot x = 1.$$

이로부터 여러분은 이미 군의 정의가 무엇인지 짐작하셨을 수도 있습니다.

**정의 1.1.3.** 군은 원소들의 집합  $G$ 와  $G$  위의 이항 연산  $\star$ 로 이루어진 순서쌍  $G = (G, \star)$ 이며, 다음을 만족합니다:

- $G$ 는 **항등원**을 가지며, 보통  $1_G$  또는 그냥 1로 표기하고, 다음 성질을 가집니다

$$1_G \star g = g \star 1_G = g \text{ 모든 } g \in G \text{에 대하여.}$$

- 이 연산은 **결합적**입니다, 즉 임의의  $a, b, c \in G$ 에 대해  $(a \star b) \star c = a \star (b \star c)$ 입니다. 따라서 일반적으로 괄호를 생략하고 씁니다.
- 각 원소  $g \in G$ 는 **역원**을 가지는데, 즉 다음을 만족하는 원소  $h \in G$ 가 존재합니다

$$g \star h = h \star g = 1_G.$$

**비고 1.1.4 (중요하지 않은 세부 사항)** — 일부 저자는 "단함" 공리를 추가하여, 즉  $g \star h \in G$ 임을 명시적으로 언급하기도 합니다. 이는  $\star$ 가  $G$  위의 이항연산이라는 사실에서 이미 함축되지만, 아래의 예시들을 위해 유념할 가치가 있습니다.

**비고 1.1.5** —  $\star$ 가 가환적일 것( $a \star b = b \star a$ )은 요구되지 않습니다. 그래서 연산이 가환적이면 군이 **아벨적**이라고 하고, 그렇지 않으면 **비아벨적**이라고 합니다.

**예제 1.1.6 (군이 아닌 예시)**

- 순서쌍  $(\mathbb{Q}, \cdot)$ 는 군이 아닙니다. (여기서  $\mathbb{Q}$ 는 유리수입니다.) 항등원은 존재하지만, 원소  $0 \in \mathbb{Q}$ 는 역원을 가지지 않습니다.
- 쌍  $(\mathbb{Z}, \cdot)$  또한 군이 아닙니다. (왜일까요?)
- $\text{Mat}_{2 \times 2}(\mathbb{R})$ 을  $2 \times 2$  실수 행렬의 집합이라 합시다. 그러면  $(\text{Mat}_{2 \times 2}(\mathbb{R}), \cdot)$  (여기서  $\cdot$ 은 행렬 곱셈)는 군이 아닙니다. 실제로, 항등 행렬이 있음에도 불구하고

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

우리는 여전히 이전과 같은 문제에 부딪힙니다: 영행렬은 곱셈에 대한 역원을 가지지 않습니다.

(집합에서 영행렬을 제거하더라도, 그 결과 구조는 여전히 군이 아닙니다: 선형 대수학을 조금 아는 분들은 행렬식이 0인 행렬은 역원을 가질 수 없다는 사실을 기억하실 것입니다.)

예시를 계속 적어봅시다. 다음은 군의 **아벨 예시**를 더 든 것입니다:

**예제 1.1.7 (복소수 단위원)**

$S^1$ 을 절댓값이 1인 복소수  $z$ 의 집합이라 합시다; 즉

$$S^1 := \{z \in \mathbb{C} \mid |z| = 1\}.$$

그러면  $(S^1, \times)$ 는 군입니다. 왜냐하면

- 복소수  $1 \in S^1$ 이 항등원의 역할을 하고,
- 각 복소수  $z \in S^1$ 은  $S^1$ 에 속하는 역원  $\frac{1}{z}$ 을 가지는데, 이는  $|z^{-1}| = |z|^{-1} = 1$ 이기 때문입니다.

한 가지 더 확인해야 할 것이 있습니다:  $z_1 \times z_2$ 가 실제로 여전히  $S^1$ 에 속한다는 것입니다. 하지만 이는  $|z_1 z_2| = |z_1| |z_2| = 1$ 이라는 사실로부터 따라옵니다.

**예제 1.1.8 ( $n$ 을 법으로 하는 덧셈)**

정수론에서 나오는 예시가 하나 있습니다:  $n > 1$ 을 정수라 하고,  $n$ 을 법으로 하는 잉여(나머지)를 생각합시다. 이들은 덧셈에 대해 군을 이룹니다. 이를 **위수  $n$ 의 순환**

군이라 부르고,  $\mathbb{Z}/n\mathbb{Z}$ 으로 표기하며, 원소는  $\bar{0}, \bar{1}, \dots$ 입니다. 항등원은  $\bar{0}$ 입니다.

### 예제 1.1.9 ( $p$ 를 법으로 하는 곱셈)

$p$ 를 소수라 합시다.  $p$ 를 법으로 하는  $\theta$ 이 아닌 잉여를 생각하고, 이를  $(\mathbb{Z}/p\mathbb{Z})^\times$ 로 표기합니다. 그러면  $((\mathbb{Z}/p\mathbb{Z})^\times, \times)$ 는 군입니다.

**질문 1.1.10.** 왜  $p$ 가 소수라는 사실이 필요할까요?

(여담:  $\mathbb{Z}/n\mathbb{Z}$ 과  $(\mathbb{Z}/p\mathbb{Z})^\times$ 라는 표기법이 이상해 보일 수 있지만, 나중에 환과 아이디얼을 다룰 때 이해가 될 것입니다. 지금은 걱정하지 마십시오.)

다음은 **비아벨 예시**입니다:

### 예제 1.1.11 (일반 선형군)

$n$ 을 양의 정수라 합시다. 그러면  $GL_n(\mathbb{R})$ 은 행렬식이 0이 아닌  $n \times n$  실수 행렬의 집합으로 정의됩니다. 이 조건 하에서는 실제로 모든 행렬이 역원을 가진다는 것이 밝혀지므로,  $(GL_n(\mathbb{R}), \times)$ 는 군이 되며, 이를 **일반 선형군**이라 부릅니다.  $(GL_n(\mathbb{R}))$ 이  $\times$ 에 대해 닫혀 있다는 사실은 이후 장에서 증명될  $\det(AB) = \det A \det B$ 라는 선형대수학의 사실로부터 따라옵니다.)

### 예제 1.1.12 (특수 선형군)

위 예시에 이어서,  $SL_n(\mathbb{R})$ 을 행렬식이 정확히 1인  $n \times n$  행렬의 집합이라 합시다. 다시금, 선형대수학적 이유로  $(SL_n(\mathbb{R}), \times)$  또한 군이 됨이 밝혀지며, 이를 **특수 선형군**이라 부릅니다.

### 예제 1.1.13 (대칭군)

$S_n$ 을  $\{1, \dots, n\}$ 의 순열들의 집합이라 합시다. 이 순열들을  $\{1, \dots, n\}$ 에서 자기 자신으로 가는 함수로 봄으로써, 순열의 합성을 생각할 수 있습니다. 그러면 쌍  $(S_n, \circ)$  (여기서  $\circ$ 는 함수 합성)도 군인데, 그 이유는

- 항등 순열이 존재하고,
- 각 순열은 역원을 가지기 때문입니다.

군  $S_n$ 은  $n$ 개 원소 위의 **대칭군**이라 불립니다.

### 예제 1.1.14 (이면체군)

$D_{2n}$ 으로 표기되는 **위수  $2n$ 의 이면체군**은 정  $n$ 각형  $A_1 A_2 \dots A_n$ 의 대칭군으로, 회전과 반사를 포함합니다. 이는 다음  $2n$ 개의 원소로 이루어집니다

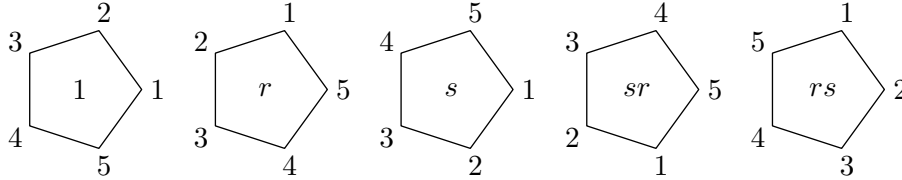
$$\{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}.$$

원소  $r$ 은  $n$ 각형을  $\frac{2\pi}{n}$ 만큼 회전시키는 것에 해당하고,  $s$ 는 직선  $OA_1$ 을 기준으로 반

사시키는 것에 해당합니다 (여기서  $O$ 는 다각형의 중심입니다). 따라서  $rs$ 는 "반사한 다음 회전한다"는 것을 뜻합니다 (함수 합성과 마찬가지로, 오른쪽에서 왼쪽으로 읽습니다).

특히,  $r^n = s^2 = 1$ 입니다. 또한  $r^k s = s r^{-k}$ 임을 알 수 있습니다.

다음은  $D_{10}$ 의 원소 몇 개를 그림으로 나타낸 것입니다.



여담: 이면체군  $D_{12}$ 는 제가 가장 좋아하는 비아벨 군의 예시이며, “예시를 찾으시오...”와 같은 형태의 시험 문제에서 제가 가장 먼저 시도하는 군입니다.

더 많은 예시:

### 예제 1.1.15 (군의 곱)

$(G, \star)$ 와  $(H, *)$ 를 군이라 합시다. 다음과 같이 **곱군**(product group)  $(G \times H, \cdot)$ 을 정의할 수 있습니다. 이 군의 원소는 순서쌍  $(g, h) \in G \times H$ 가 됩니다. 그러면

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \star g_2, h_1 * h_2) \in G \times H$$

이 군의 연산입니다.

**질문 1.1.16.** 곱군의 항등원과 역원은 무엇입니까?

### 예제 1.1.17 (자명군)

흔히 0 또는 1로 표기되는 **자명군**(trivial group)은 항등원만을 가지는 군입니다. 저는  $\{1\}$ 이라는 표기를 사용하겠습니다.

**연습문제 1.1.18.** 다음 중 어느 것이 군입니까?

- (a) 홀수 분모를 가지는 (기약분수 형태의) 유리수 전체로, 연산은 덧셈입니다. (이는  $n/1$ 로 쓰이는 정수와  $0 = 0/1$ 을 포함합니다.)
- (b) 분모가 2 이하인 유리수 전체의 집합으로, 연산은 덧셈입니다.
- (c) 분모가 2 이하인 유리수 전체의 집합으로, 연산은 곱셈입니다.
- (d) 음이 아닌 정수 전체의 집합으로, 연산은 덧셈입니다.

## §1.2 군의 성질

**이 절의 대표적인 예:**  $(\mathbb{Z}/p\mathbb{Z})^\times$ 가 아마도 가장 좋을 것입니다.

**표기의 남용 1.2.1.** 이제부터는 군  $(G, \star)$ 를 그냥  $G$ 라고 지칭하는 경우가 많을 것입니다. 또한  $a \star b$ 를 그냥  $ab$ 로 줄여 쓰겠습니다. 아울러 연산  $\star$ 가 결합법칙을 만족하므로 불필요한 괄호는 생략하겠습니다:  $(ab)c = a(bc) = abc$ .

**표기의 남용 1.2.2.** 이제부터 임의의  $g \in G$ 와  $n \in \mathbb{N}$ 에 대해 다음과 같이 줄여 씁니다

$$g^n = \underbrace{g \star \cdots \star g}_{n\text{번}}.$$

또한  $g^{-1}$ 가  $g$ 의 역원을 나타내도록 하고,  $g^{-n} = (g^{-1})^n$ 으로 둡니다.

수학에서 흔한 주제 중 하나는, 특정 예시들을 염두에 두면서도 어떤 대상이 최소한의 성질만을 만족하도록 요구한 다음, 종이 위에서는 그 예시들을 잊어버리고 오직 그 성질만으로부터 최대한 많은 것을 유도해 보려 하는 것입니다. (수학 올림피아드 경험자라면 함수의 단 하나의 성질만 알아도 그 함수 전체가 결정되는 “함수 방정식”에 익숙할 것입니다.) 이제 여기서도 이를 시도해 보면서, **정의 1.1.3**만을 알고서 우리가 무엇을 결론지을 수 있는지 살펴봅시다.

관과 그 밖의 37개 주에서는 제가 이제 다음 명제를 진술하는 것이 법으로 정해져 있습니다.

**사실 1.2.3.**  $G$ 를 군이라 합시다.

- (a) 군의 항등원은 유일합니다.
- (b) 임의의 원소의 역원은 유일합니다.
- (c) 임의의  $g \in G$ 에 대해,  $(g^{-1})^{-1} = g$ 입니다.

증명. 이는 대체로 형식적인 조작에 불과하므로, 처음 읽을 때 건너뛰어도 괜찮습니다.

- (a) 1과 1'이 항등원이라면,  $1 = 1 \star 1' = 1'$ 입니다.
- (b)  $h$ 와  $h'$ 이  $g$ 의 역원이라면,  $1_G = g \star h \implies h' = (h' \star g) \star h = 1_G \star h = h$ 입니다.
- (c) 자명하므로 생략합니다. □

이제 조금 더 유용한 명제를 서술합니다.

**명제 1.2.4 (곱의 역원)**

$G$ 가 군이고,  $a, b \in G$ 라고 합시다. 그러면  $(ab)^{-1} = b^{-1}a^{-1}$ 입니다.

증명. 직접 계산합니다. 다음이 성립합니다

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1_G.$$

마찬가지로,  $(b^{-1}a^{-1})(ab) = 1_G$  또한 성립합니다. 따라서  $(ab)^{-1} = b^{-1}a^{-1}$ 입니다. □

마지막으로, 역원을 갖는다는 것이 왜 그토록 유용한지를 잘 보여주는 군에 관한 매우 중요한 보조정리를 서술하겠습니다.

**보조정리 1.2.5 (왼쪽 곱셈은 전단사입니다)**

$G$ 를 군이라 하고,  $g \in G$ 를 하나 고릅니다. 그러면  $x \mapsto gx$ 로 주어지는 사상  $G \rightarrow G$ 는 전단사입니다.

**연습문제 1.2.6.** 단사성과 전사성을 직접 보임으로써 이를 확인하십시오. (이 단어들의 뜻을 모른다면 **장 E**를 참고하십시오.)

**예제 1.2.7**

$G = (\mathbb{Z}/7\mathbb{Z})^\times$  (예제 1.1.9에서와 같이)라 하고  $g = 3$ 을 곱시다. 위의 보조정리는 사상  $x \mapsto 3 \cdot x$ 가 전단사임을 말해주며, 이를 명시적으로 확인할 수 있습니다:

$$\begin{aligned} 1 &\xrightarrow{\times 3} 3 \pmod{7} \\ 2 &\xrightarrow{\times 3} 6 \pmod{7} \\ 3 &\xrightarrow{\times 3} 2 \pmod{7} \\ 4 &\xrightarrow{\times 3} 5 \pmod{7} \\ 5 &\xrightarrow{\times 3} 1 \pmod{7} \\ 6 &\xrightarrow{\times 3} 4 \pmod{7}. \end{aligned}$$

이 사상이 단사라는 사실은 종종 **소거 법칙**이라 불립니다. (왜 그렇게 불리는지 생각해 보십시오.)

**표기의 남용 1.2.8** (이후로는 항등원을 1 대신 0으로 표기하는 경우가 있습니다). 앞으로 몇 개의 장 동안은 이를 신경 쓰지 않아도 되지만, 지금 미리 언급해 두겠습니다. 지금까지의 예시 대부분에서는 연산  $\star$ 을 일종의 곱셈처럼 여겼으며, 그렇기 때문에  $1 = 1_G$ 가 항등원에 대한 자연스러운 표기였습니다.

그러나  $\mathbb{Z} = (\mathbb{Z}, +)$ 처럼 연산  $\star$ 을 덧셈으로 여기는 군도 있는데, 이 경우에는  $0 = 0_G$ 라는 표기가 오히려 더 자연스러울 수 있습니다. (일반적으로 연산이  $+$ 로 표기될 때는 그 연산이 거의 항상 가환입니다.) 나중에 환과 선형대수를 다룰 때 우리도 결국 이런 표기를 사용하기 시작할 것입니다.

**§1.3 동형사상**

**이 절의 대표적인 예:**  $\mathbb{Z} \cong 10\mathbb{Z}$ .

먼저, 두 군이 동형이라는 것이 무엇을 의미하는지 이야기해 보겠습니다. 다음 두 군을 생각해 봅시다

- $\mathbb{Z} = (\{\dots, -2, -1, 0, 1, 2, \dots\}, +)$ .
- $10\mathbb{Z} = (\{\dots, -20, -10, 0, 10, 20, \dots\}, +)$ .

이 두 군은 겉보기에는 "다르지만", 오직 표면적으로만 그러합니다 – 원소들의 이름만 다를 뿐이라고 말할 수도 있을 것입니다. 이것이 형식적으로 무엇을 의미할 수 있는지 잠시 생각해 보십시오.

구체적으로, 다음 사상은

$$\phi: \mathbb{Z} \rightarrow 10\mathbb{Z} \text{에 의해 } x \mapsto 10x$$

군 연산을 보존하는, 바탕 집합들 사이의 전단사입니다. 기호로 표현하면,

$$\phi(x + y) = \phi(x) + \phi(y).$$

다시 말해,  $\phi$ 는 군의 구조를 바꾸지 않으면서 원소들의 이름을 재배정하는 방식입니다. 이는  $(\mathbb{Z}, +)$ 와  $(10\mathbb{Z}, +)$ 가 사실상 같은 것이라는 명백한 사실을 포착하기 위한 형식화에 지나지 않습니다.

이제 일반적인 정의를 내려 봅시다.

**정의 1.3.1.**  $G = (G, \star)$ 와  $H = (H, *)$ 를 군이라 합시다. 전단사  $\phi: G \rightarrow H$ 는 다음을 만족할 때 **동형사상**이라 불립니다

$$\phi(g_1 \star g_2) = \phi(g_1) * \phi(g_2) \quad \text{모든 } g_1, g_2 \in G \text{에 대하여.}$$

$G$ 에서  $H$ 로의 동형사상이 존재하면,  $G$ 와  $H$ 가 **동형**이라고 말하며  $G \cong H$ 라고 씁니다.

이 정의에서 좌변  $\phi(g_1 \star g_2)$ 는  $G$ 의 연산을 사용하는 반면 우변  $\phi(g_1) * \phi(g_2)$ 는  $H$ 의 연산을 사용한다는 점에 유의하십시오.

**예제 1.3.2 (동형사상의 예)**

$G$ 와  $H$ 를 군이라 합시다. 다음과 같은 동형사상들이 있습니다.

(a) 위에서와 같이  $\mathbb{Z} \cong 10\mathbb{Z}$ 입니다.

(b) 다음과 같은 동형사상이 있습니다

$$G \times H \cong H \times G$$

사상  $(g, h) \mapsto (h, g)$ 에 의해서입니다.

(c) 항등사상  $\text{id}: G \rightarrow G$ 는 동형사상이므로,  $G \cong G$ 입니다.

(d)  $\mathbb{Z}$  자기 자신으로의 또 다른 동형사상이 있습니다: 모든  $x$ 를  $-x$ 로 보내는 것입니다.

**예제 1.3.3 (7을 법으로 하는 원시근)**

자명하지 않은 예로,  $\mathbb{Z}/6\mathbb{Z} \cong (\mathbb{Z}/7\mathbb{Z})^\times$ 임을 주장합니다. 전단사는

$$\phi(a \bmod 6) = 3^a \bmod 7.$$

- 이 사상이 전단사임을 명시적 계산으로 확인됩니다:

$$(3^0, 3^1, 3^2, 3^3, 3^4, 3^5) \equiv (1, 3, 2, 6, 4, 5) \pmod{7}.$$

(엄밀히 말하면, 좀 더 정확하게는  $3^{0 \bmod 6} = 1$  등으로 써야 할 것입니다.)

- 마지막으로, 이 사상이 군 연산을 보존함을 확인해야 합니다. 다시 말해,  $\mathbb{Z}/6\mathbb{Z}$ 의 연산은 덧셈인 반면  $(\mathbb{Z}/7\mathbb{Z})^\times$ 의 연산은 곱셈이므로,  $\phi(a+b) = \phi(a)\phi(b)$ 임을 보이고자 합니다. 이는 단지  $3^{a+b \bmod 6} \equiv 3^{a \bmod 6} 3^{b \bmod 6} \pmod{7}$ 이라는 것이며, 이는 참입니다.

**예제 1.3.4 (원시근)**

더 일반적으로, 임의의 소수  $p$ 에 대해,  $p$ 를 법으로 하는 **원시근**이라 불리는 원소  $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ 가 존재하여  $1, g, g^2, \dots, g^{p-2}$ 가  $p$ 를 법으로 모두 서로 다릅니다. 위의 증명을 그대로 따라 하면 다음을 보일 수 있습니다

$$\mathbb{Z}/(p-1)\mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z})^\times \text{ 모든 소수 } p \text{에 대하여.}$$

위의 예는  $p = 7$ 이고  $g = 3$ 인 특수한 경우였습니다.

**연습문제 1.3.5.** 원시근의 존재성을 가정하고, 위와 같이 동형사상  $\mathbb{Z}/(p-1)\mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z})^\times$ 를 확립하십시오.

$\cong$ 가 동치 관계임을 보이는 것은 어렵지 않습니다(왜일까요?). 게다가, 우리는 실제로 군의 구조에만 관심이 있으므로, 두 군이 동형일 때 보통 같은 것으로 간주할 것입니다. 그래서 "모든 군을 찾아라"와 같은 문구는 실제로는 "동형사상까지 고려하여 모든 군을 찾아라"를 의미합니다.

## §1.4 군의 위수와 라그랑주 정리

이 절의 대표적인 예:  $(\mathbb{Z}/p\mathbb{Z})^\times$ .

수학에서 흔히 그렇듯이, 우리는 "위수(order)"라는 단어를 너무 많은 것에 사용합니다. 군에서는 위수에 대한 두 가지 개념이 있습니다.

**정의 1.4.1.**  $G$ 의 **군의 위수**는  $G$ 의 원소 개수입니다. 이를  $|G|$ 로 표시합니다. 위수는  $\mathbb{Z}$ 에서처럼 유한하지 않을 수도 있다는 점에 유의하십시오.  $|G|$ 가 유한할 때  $G$ 를 **유한군**이라고 말합니다.

### 예제 1.4.2 (군의 위수)

소수  $p$ 에 대해,  $|\mathbb{Z}/p\mathbb{Z}| = p$ 입니다. 다시 말해,  $(\mathbb{Z}/p\mathbb{Z})^\times$ 의 위수는  $p-1$ 입니다. 또 다른 예로, 대칭군  $S_n$ 의 위수는  $n!$ 이고 이면군  $D_{2n}$ 의 위수는  $2n$ 입니다.

**정의 1.4.3.** 원소  $g \in G$ 의 **원소의 위수**는  $g^n = 1_G$ 를 만족하는 가장 작은 양의 정수  $n$ 이며, 그러한  $n$ 이 존재하지 않으면  $\infty$ 입니다. 이를  $\text{ord } g$ 로 표시합니다.

### 예제 1.4.4 (위수의 예)

$\mathbb{Q}^\times$ 에서  $-1$ 의 위수는 2인 반면,  $\mathbb{Z}$ 에서 1의 위수는 무한합니다.

**질문 1.4.5.** 원소가 여섯 개인 순환군  $\mathbb{Z}/6\mathbb{Z}$ 의 여섯 원소 각각의 위수를 구하십시오. ( $\mathbb{Z}/6\mathbb{Z}$ 이 무엇을 뜻하는지 잊었다면 [예제 1.1.8](#)을 참고하십시오.)

### 예제 1.4.6 (원시근)

올림피아드 정수론을 알고 있다면, 이는 법  $p$ 에 대한 나머지의 위수 정의와 일치합니다. 그래서 여기에서도 "위수"라는 용어를 사용합니다. 특히, 원시근은 정확히  $\text{ord } g = p-1$ 을 만족하는 원소  $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ 입니다.

$x^n \equiv 1 \pmod{p}$ 이면  $x \pmod{p}$ 의 위수가 반드시  $n$ 을 나눈다는 사실도 알고 있을 것입니다. 정확히 같은 이유로 일반적인 군에서도 이와 같은 사실이 성립합니다.

**사실 1.4.7.**  $g^n = 1_G$ 이면  $\text{ord } g$ 는  $n$ 을 나눕니다.

또한, 유한군의 모든 원소가 유한한 위수를 가짐을 보일 수 있습니다. 증명은 올림피아드식 비둘기집 논법에 불과합니다. 무한 수열  $1_G, g, g^2, \dots$ 를 생각하고, 같은 두 원소를 찾으십시오.

**사실 1.4.8.**  $G$ 를 유한군이라 합시다. 임의의  $g \in G$ 에 대하여,  $\text{ord } g$ 는 유한합니다.

올림피아드 수학에서 알고 있는  $(\mathbb{Z}/p\mathbb{Z})^\times$ 의 마지막 성질은 무엇입니까? 페르마의 소정리가 있습니다: 임의의  $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ 에 대하여,  $a^{p-1} \equiv 1 \pmod{p}$ 입니다. 이는 우연이 아닙니다: 더 일반적인 설정에서도 정확히 같은 사실이 성립합니다.

**정리 1.4.9** (위수에 대한 라그랑주 정리)

$G$ 를 임의의 유한군이라 합시다. 그러면 임의의  $x \in G$ 에 대하여  $x^{|G|} = 1_G$ 입니다.

이 결과를 기억해 두십시오! 나중에 정리 3.4.1의 일반적인 형태로 증명하겠습니다.

## §1.5 부분군

**이 절의 대표적인 예:**  $SL_n(\mathbb{R})$ 은  $GL_n(\mathbb{R})$ 의 부분군입니다.

앞서 우리는 행렬식이 0이 아닌  $n \times n$  행렬들인  $GL_n(\mathbb{R})$ 이 행렬 곱셈 아래 군을 이룸을 보았습니다. 그런데  $GL_n(\mathbb{R})$ 의 부분집합인  $SL_n(\mathbb{R})$  또한 같은 연산으로 군을 이룸도 보았습니다. 이러한 이유로 우리는  $SL_n(\mathbb{R})$ 이  $GL_n(\mathbb{R})$ 의 부분군이라고 말합니다. 그리고 이 정의는 여러분이 예상하는 바로 그 방식으로 일반화됩니다.

**정의 1.5.1.**  $G = (G, \star)$ 를 군이라 합시다.  $G$ 의 **부분군**은 정확히 여러분이 예상하는 그대로입니다:  $H$ 가  $G$ 의 부분집합인 군  $H = (H, \star)$ 입니다.  $H \neq G$ 이면 이를 **진부분군**이라 합니다.

**비고 1.5.2** — 군  $G$ 를 명시하려면, 집합  $G$ 가 무엇인지와 연산  $\star$ 가 무엇인지를 모두 알려드려야 했습니다. 그러나 주어진 군  $G$ 의 부분군  $H$ 를 명시하려면, 그 원소들이 무엇인지만 알려드리면 됩니다:  $H$ 의 연산은 그저  $G$ 의 연산으로부터 물려받은 것이기 때문입니다.

**예제 1.5.3** (부분군의 예)

- (a)  $2\mathbb{Z}$ 는  $\mathbb{Z}$ 의 부분군이며, 이는  $\mathbb{Z}$  자신과 동형입니다!
- (b)  $n$ 개의 원소에 대한 대칭군  $S_n$ 을 다시 생각해 봅시다.  $T$ 를  $\tau(n) = n$ 을 만족하는 순열  $\tau: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ 들의 집합이라 합시다. 그러면  $T$ 는  $S_n$ 의 부분군입니다; 실제로, 이는  $S_{n-1}$ 과 동형입니다.
- (c) 군  $G \times H$ (**예제 1.1.15**)와 원소들  $\{(g, 1_H) \mid g \in G\}$ 를 생각해 봅시다. 이는  $G \times H$ 의 부분군입니다(왜 그럴까요?). 실제로, 이는 동형사상  $(g, 1_H) \mapsto g$ 에 의해  $G$ 와 동형입니다.

**예제 1.5.4** (부분군의 뻘한 예)

임의의 군  $G$ 에 대하여, 자명군  $\{1_G\}$ 와 군 전체  $G$ 는  $G$ 의 부분군입니다.

다음은 이후 장들에서 더 다룰 특히 중요한 예입니다.

**예제 1.5.5** (한 원소로 생성되는 부분군)

$x$ 를 군  $G$ 의 한 원소라 합시다. 다음 집합을 생각해 봅시다

$$\langle x \rangle = \{ \dots, x^{-2}, x^{-1}, 1, x, x^2, \dots \}.$$

이 역시  $G$ 의 부분군이며,  $x$ 로 생성되는 부분군이라고 합니다.

**연습문제 1.5.6.**  $\text{ord } x = 2015$ 이면, 위 부분군은 무엇과 같습니까?  $\text{ord } x = \infty$ 이면 어떻습니까?

마지막으로, 부분군이 아닌 몇 가지 예를 제시합니다.

**예제 1.5.7 (부분군이 아닌 예)**

군  $\mathbb{Z} = (\mathbb{Z}, +)$ 을 생각해 봅시다.

- (a) 집합  $\{0, 1, 2, \dots\}$ 은 역원을 포함하지 않기 때문에  $\mathbb{Z}$ 의 부분군이 아닙니다.
- (b) 집합  $\{n^3 \mid n \in \mathbb{Z}\} = \{\dots, -8, -1, 0, 1, 8, \dots\}$ 은 덧셈에 대해 닫혀 있지 않기 때문에 부분군이 아닙니다. 두 세제곱수의 합은 일반적으로 세제곱수가 아닙니다.
- (c) 공집합  $\emptyset$ 은 항등원이 없기 때문에  $\mathbb{Z}$ 의 부분군이 아닙니다.

## §1.6 작은 위수의 군

그냥 재미로, 위수가 10 이하인 모든 군의 목록을 (물론 동형사상 아래에서) 여기 제시합니다.

1. 위수 1인 유일한 군은 자명군입니다.
2. 위수 2인 유일한 군은  $\mathbb{Z}/2\mathbb{Z}$ 입니다.
3. 위수 3인 유일한 군은  $\mathbb{Z}/3\mathbb{Z}$ 입니다.
4. 위수 4인 유일한 군들은 다음과 같습니다
  - $\mathbb{Z}/4\mathbb{Z}$ , 네 개의 원소로 이루어진 순환군,
  - 클라인 4원군이라 불리는  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 입니다.
5. 위수 5인 유일한 군은  $\mathbb{Z}/5\mathbb{Z}$ 입니다.
6. 위수 6인 군들은 다음과 같습니다
  - $\mathbb{Z}/6\mathbb{Z}$ , 여섯 개의 원소로 이루어진 순환군입니다.
  - $S_3$ , 세 원소의 치환군입니다. 이는 최초의 비아벨 군입니다.

여러분 중 일부는  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ 은 어디 있는지 궁금해할지도 모릅니다. 제가 할 말은 이것뿐입니다: 중국인의 나머지 정리입니다!

$D_6$ 은 이 목록에서 어디에 있는지 궁금하실 수도 있습니다. 사실 이는  $S_3$ 과 동형입니다.

7. 위수 7인 유일한 군은  $\mathbb{Z}/7\mathbb{Z}$ 입니다.
8. 위수 8인 군들은 더 많습니다.

- $\mathbb{Z}/8\mathbb{Z}$ , 여덟 개의 원소로 이루어진 순환군입니다.
- $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ .
- $D_8$ , 원소가 8개인 이면군이며, 아벨 군이 아닙니다.
- 비아벨 군  $Q_8$ 은 사원수군이라 불립니다. 이 군은  $i^2 = j^2 = k^2 = ijk = -1$ 을 만족하는 여덟 개의 원소  $\pm 1, \pm i, \pm j, \pm k$ 로 이루어져 있습니다.

9. 위수가 9인 군들은 다음과 같습니다.

- $\mathbb{Z}/9\mathbb{Z}$ , 원소가 9개인 순환군입니다.
- $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ .

10. 위수가 10인 군들은 다음과 같습니다.

- $\mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  (역시 중국인의 나머지 정리에 의합니다).
- $D_{10}$ , 원소가 10개인 이면군입니다. 이 군은 비아벨입니다.

## §1.7 중요하지 않은 긴 여담

흔히 나오는 질문은 다음과 같습니다: 왜 하필 이런 공리들일까요? 예를 들어, 왜 결합법칙은 요구하면서 교환법칙은 요구하지 않을까요? 이 답은 이후에나 이해가 될 것 같지만, 도움이 될 만한 몇 가지 설명을 남겨 둡니다.

하나의 일반적인 발견법은 다음과 같습니다: 새로운 종류의 일반적 대상을 정의할 때마다 항상 균형을 맞추는 작업이 벌어집니다. 한편으로는 대상이 "좋은" 성질을 갖도록 충분한 제약을 포함시키고 싶어 합니다. 다른 한편으로는, 제약을 너무 많이 포함시키면 정의가 너무 적은 대상에만 적용되게 됩니다.

그래서, 예를 들어, "결합법칙"을 포함시키는 이유는 그렇게 하면 우리 삶이 편해지고, 우리가 마주치는 대부분의 연산이 결합법칙을 만족하기 때문입니다. 특히, 원소의 역원이 반드시 유일하려면 결합법칙이 필요합니다. 하지만 "교환법칙"은 포함시키지 않는데, 이는 아래의 예시들이 우리가 관심을 갖는 비아벨 군이 많다는 것을 보여주기 때문입니다. (그러나 여전히 이를 추적하고 싶기 때문에 "아벨"이라는 또 다른 이름을 도입합니다.)

또 다른 설명: 역원 공리에 대한 좋은 동기는 상당한 양의 대칭성을 얻을 수 있다는 것입니다. 예를 들어, 덧셈을 갖춘 양의 정수 집합은 군이 아닌데, 이는 3에서 6을 뺄 수 없기 때문입니다: 어떤 원소들은 다른 원소들보다 "더 큼니다". 역원이 존재하도록 요구함으로써 이 문제를 없앨 수 있습니다. (이를 위해서는 항등원도 필요합니다. 항등원 없이는 역원을 정의하기 어렵습니다.)

더욱 난해한 설명: 문제 1F<sup>†</sup>은 군이 실은 대칭군의 그림자임을 보여줍니다. 이는 "군은 매우 대칭적이다"라는 관념을 엄밀하게 만들어 줍니다.

## §1.8 생각해 볼 만한 조금 더 어려운 문제

문제 1A. 다음 그림에서 농담은 무엇일까요? (출처: [Ge].)



**문제 1B.**  $G$ 가 유한 아벨 군인 특수한 경우에 대해 위수에 관한 라그랑주 정리를 증명하십시오.

**문제 1C.**  $D_6 \cong S_3$ 이지만  $D_{24} \not\cong S_4$ 임을 보이십시오.

**문제 1D\*.**  $p$ 를 소수라고 합시다.  $G$ 가 위수  $p$ 인 군이면  $G \cong \mathbb{Z}/p\mathbb{Z}$ 임을 보이십시오.

**문제 1E** (케일리 정리에 대한 힌트).  $D_8$ 과 동형인  $S_8$ 의 부분군  $H$ 를 찾고, 그 동형사상을 명시적으로 쓰십시오.

 **문제 1F†.**  $G$ 를 유한군이라 합시다.<sup>1</sup> 다음을 만족하는 양의 정수  $n$ 이 존재함을 보이십시오.

(a) (케일리 정리)  $G$ 는 대칭군  $S_n$ 의 어떤 부분군과 동형입니다.

(b) (표현론)  $G$ 는 일반선형군  $GL_n(\mathbb{R})$ 의 어떤 부분군과 동형입니다. (이는 가역  $n \times n$  행렬들로 이루어진 군입니다.)

 **문제 1G.** 대칭군  $S_n$ 이 위수 2018인 이면군  $D_{2018}$ 과 동형인 부분군을 갖도록 하는 가장 작은 정수  $n$ 을 찾으십시오.

  **문제 1H** (IMO SL 2005 C5).  $n$ 개의 마커가 있으며, 각각 한쪽 면은 흰색이고 다른 쪽 면은 검은색입니다. 처음에 이  $n$ 개의 마커는 흰색 면이 모두 위를 향하도록 한 줄로 정렬되어 있습니다. 각 단계에서 가능하다면, 흰색 면이 위를 향한 마커(단, 가장 바깥쪽 마커는 제외) 하나를 선택하여 제거하고, 그 왼쪽에 가장 가까운 마커와 오른쪽에 가장 가까운 마커를 뒤집습니다.

$n \equiv 1 \pmod{3}$ 이면 마커가 두 개만 남는 상태에 도달하는 것이 불가능함을 증명하십시오. (실제로 그 역도 성립합니다.)

 **문제 1I.**  $p$ 를 소수라 하고  $F_1 = F_2 = 1$ ,  $F_{n+2} = F_{n+1} + F_n$ 을 피보나치 수열이라 하십시오.  $F_{2p(p^2-1)}$ 가  $p$ 로 나누어짐을 보이십시오.

<sup>1</sup>다시 말해, 순열군은 임의로 이상해질 수 있습니다. 저는 이 정리를 처음 들었을 때 매우 당혹스러웠던 것으로 기억하지만, 돌아해보면 그리 놀라운 일은 아닙니다.

## 2 거리 공간

이 글을 쓰는 시점에서, 저는 거리 위상이 점집합 위상을 동기부여하는 데 있어서나 일반적인 미적분학을 일반화하는 데 있어서나 도덕적으로 올바른 방법이라고 확신합니다.<sup>1</sup> 그러니 여기 제 최선의 시도를 소개합니다.

거리 공간의 개념은 매우 "구체적"이어서 시각화하기가 쉽습니다. 따라서 이 장 전체에 걸쳐 여러분은 수렴하는 수열, 열린집합, 닫힌집합 등과 같은 새로운 대상들을 배우면서 많은 그림을 그려야 합니다.

### §2.1 거리 공간의 정의와 예시

**이 절의 대표적인 예:** 유클리드 거리를 가진  $\mathbb{R}^2$ 입니다.

**정의 2.1.1.** **거리 공간**은 점들의 집합  $M$ 과 **거리**  $d: M \times M \rightarrow \mathbb{R}_{\geq 0}$ 로 이루어진 순서쌍  $(M, d)$ 입니다. 이 거리 함수는 다음을 만족해야 합니다:

- 임의의  $x, y \in M$ 에 대해,  $d(x, y) = d(y, x)$ 가 성립합니다. 즉,  $d$ 는 대칭입니다.
- 함수  $d$ 는 **양의 정부호**여야 하는데, 이는  $d(x, y) \geq 0$ 이며 등호는  $x = y$ 일 때에만 성립함을 의미합니다.
- 함수  $d$ 는 **삼각 부등식**을 만족해야 합니다: 모든  $x, y, z \in M$ 에 대해,

$$d(x, z) + d(z, y) \geq d(x, y).$$

**표기의 남용 2.1.2.** 군의 경우와 마찬가지로, 우리는  $(M, d)$ 를 그냥  $M$ 으로 줄여 쓰겠습니다.

#### 예제 2.1.3 ( $\mathbb{R}$ 의 거리 공간)

- (a) 실수직선  $\mathbb{R}$ 은 거리  $d(x, y) = |x - y|$  아래에서 거리 공간을 이룹니다.
- (b) 구간  $[0, 1]$  또한 동일한 거리 함수를 가진 거리 공간입니다.
- (c) 실제로,  $\mathbb{R}$ 의 임의의 부분집합  $S$ 는 이러한 방식으로 거리 공간이 될 수 있습니다.

#### 예제 2.1.4 ( $\mathbb{R}^2$ 의 거리 공간)

- (a) 우리는 유클리드 거리 함수를 부여함으로써  $\mathbb{R}^2$ 를 거리 공간으로 만들 수 있습니다

$$d((x_1, y_1), (x_2, y_2)) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}.$$

- (b) 첫 번째 예시와 마찬가지로,  $\mathbb{R}^2$ 의 임의의 부분집합도 이를 물려받은 후에는 거리 공간이 됩니다. 단위 원판, 단위 원, 그리고 단위 정사각형  $[0, 1]^2$ 이 특별한 경우들입니다.

<sup>1</sup>또한, "거리"는 발음하기 재미있는 단어이기도 합니다.

**예제 2.1.5** ( $\mathbb{R}^2$  위의 택시 거리)

$\mathbb{R}^2$  위에 **택시 거리**를 부여하는 것도 가능합니다:

$$d((x_1, y_1), (x_2, y_2)) = |x_1 - x_2| + |y_1 - y_2|.$$

지금으로서는, 우리는 더 자연스러운 유클리드 거리를 사용하겠습니다.

**예제 2.1.6** ( $\mathbb{R}^n$ 의 거리 공간)

위의 예시들을 쉽게 일반화할 수 있습니다.  $n$ 을 양의 정수라고 합시다.

- (a) 점들이  $n$ 차원 유클리드 공간의 점들이고, 거리가 유클리드 거리인 거리 공간을  $\mathbb{R}^n$ 이라고 하겠습니다

$$d((a_1, \dots, a_n), (b_1, \dots, b_n)) = \sqrt{(a_1 - b_1)^2 + \dots + (a_n - b_n)^2}.$$

이것이 바로  $n$ 차원 **유클리드 공간**입니다.

- (b) 열린 **단위 공구**  $B^n$ 은  $x_1^2 + \dots + x_n^2 < 1$ 을 만족하는 점  $(x_1, \dots, x_n)$ 들로 이루어진  $\mathbb{R}^n$ 의 부분집합입니다.

- (c) **단위 구면**  $S^{n-1}$ 은  $x_1^2 + \dots + x_n^2 = 1$ 을 만족하는 점  $(x_1, \dots, x_n)$ 들로 이루어진  $\mathbb{R}^n$ 의 부분집합이며, 유도된 거리를 갖습니다. (위첨자  $n-1$ 은  $S^{n-1}$ 이  $n$ 차원 공간 안에 있음에도 불구하고  $n-1$ 차원 공간임을 나타냅니다.) 예를 들어,  $S^1 \subseteq \mathbb{R}^2$ 는 단위원이며, 두 점 사이의 거리는 그 두 점을 잇는 현의 길이입니다. 이를 단위 공구  $B^n$ 의 “경계”로 생각할 수도 있습니다.

**예제 2.1.7** (함수 공간)

$M$ 을 연속함수  $f: [0, 1] \rightarrow \mathbb{R}$ 의 공간으로 두고, 거리를  $d(f, g) = \int_0^1 |f - g| \, dx$ 로 정의할 수 있습니다. ( $d(f, g) = 0$ 이  $f = g$ 를 함의함을 확인하는 데는 다소 작업이 필요하지만, 지금은 그것을 걱정하지 않겠습니다.)

다소 더 병적인 예를 하나 살펴보겠습니다.

**예제 2.1.8** (이산 공간)

$S$ 를 (유한이든 무한이든) 임의의 점들의 집합이라 합시다. 다음과 같이 선언함으로써  $S$ 를 **이산 공간**으로 만들 수 있습니다

$$d(x, y) = \begin{cases} 1 & x \neq y \text{ 일 때} \\ 0 & x = y \text{ 일 때.} \end{cases}$$

$|S| = 4$ 이면 이 공간을  $\mathbb{R}^3$  안에 있는 정사면체의 꼭짓점들로 생각할 수 있습니다. 하지만  $S$ 가 더 커지면 시각화하기가 그리 쉽지 않습니다...

**예제 2.1.9** (그래프는 거리 공간입니다)

임의의 연결된 단순 그래프  $G$ 는 두 정점 사이의 거리를 그 둘 사이의 그래프 이론적 거리로 정의함으로써 거리 공간으로 만들 수 있습니다. (이산 거리는  $G$ 가  $S$  위의 완전 그래프인 특수한 경우입니다.)

**질문 2.1.10.** 이산 공간에서의 거리와 연결된 그래프에서의 거리에 대해 거리 공간의 조건을 확인해 보십시오.

**표기의 남용 2.1.11.** 이제부터는 유클리드 거리를 갖는  $\mathbb{R}^n$ 을 그냥  $\mathbb{R}^n$ 이라고 부르겠습니다. 또한, 유도된 거리를 갖는 부분집합  $S \subseteq \mathbb{R}^n$ 에 대해 거리 공간을 취하고자 할 때는 그냥  $S$ 라고 쓰겠습니다.

**§2.2 거리 공간에서의 수렴**

**이 절의 대표적인 예:**  $\mathbb{R}$ 에서의 수열  $\frac{1}{n}$  ( $n = 1, 2, \dots$ 에 대해).

두 점 사이의 거리를 말할 수 있으므로, 점들의 수열이 수렴한다는 것이 무엇을 의미하는지도 말할 수 있습니다. 이는 절댓값을 거리 함수로 대체한 전형적인 엡실론-델타 정의와 동일합니다.

**정의 2.2.1.**  $(x_n)_{n \geq 1}$ 을 거리 공간  $M$  안의 점들의 수열이라 합시다. 다음 조건이 성립하면  $x_n$ 이  $x$ 로 **수렴한다**고 말합니다: 모든  $\varepsilon > 0$ 에 대해, ( $\varepsilon$ 에 의존하는) 정수  $N$ 이 존재하여  $n \geq N$ 인 모든  $n$ 에 대해  $d(x_n, x) < \varepsilon$ 가 성립합니다. 이는

$$x_n \rightarrow x$$

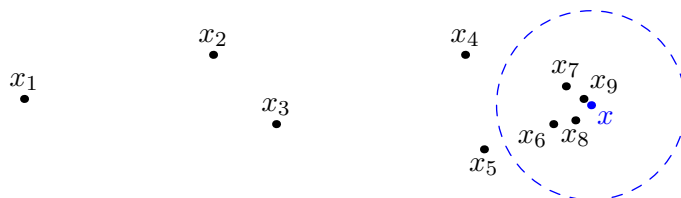
로 쓰거나, 더 풀어서

$$\lim_{n \rightarrow \infty} x_n = x.$$

로 씁니다. 수열이  $M$  안의 한 점으로 수렴하면 그 수열이  $M$ 에서 **수렴한다**고 말합니다.

이 정의가 여러분이 직관적으로 갖고 있는 “수렴한다”는 개념과 일치하는지 확인해 보아야 합니다.

**표기의 남용 2.2.2.** 모(母)공간  $M$ 이 명확한 경우, “ $M$ 에서 수렴한다”를 그냥 “수렴한다”로 줄여 쓰도록 하겠습니다. 하지만 수렴은 모공간에 상대적으로 정의된다는 점을 명심해야 합니다. 즉, 수열이 수렴하려면 공간의 “극한”이 실제로  $M$  안의 한 점이어야 합니다.

**예제 2.2.3**

수열  $x_1 = 1, x_2 = 1.4, x_3 = 1.41, x_4 = 1.414, \dots$ 을 생각해 봅시다.

(a) 이를  $\mathbb{R}$ 에서의 수열로 보면,  $\sqrt{2}$ 로 수렴합니다.

(b) 하지만 각  $x_i$ 가  $\mathbb{Q}$  안에 있음에도 불구하고, 이 수열을  $\mathbb{Q}$ 에서의 수열로 볼 때는

수렴하지 않습니다!

질문 2.2.4. 이산 거리 공간에서 수렴하는 수열은 무엇입니까?

## §2.3 연속 사상

미적분학에서 함수가 연속이라는 것이 무엇을 의미하는지 배운 적이 있을 것입니다(적어도 들어는 보았을 것입니다). 아마 다음과 같은 형태였을 것입니다

함수  $f: \mathbb{R} \rightarrow \mathbb{R}$ 가 점  $p \in \mathbb{R}$ 에서 연속이라는 것은, 모든  $\varepsilon > 0$ 에 대해  $|x - p| < \delta \implies |f(x) - f(p)| < \varepsilon$ 를 만족하는  $\delta > 0$ 가 존재함을 의미합니다.

질문 2.3.1. 거리 공간에 대한 대응되는 정의가 무엇일지 짐작할 수 있습니까?

우리가 해야 할 일은 절댓값을 더 일반적인 거리 함수로 바꾸는 것뿐입니다. 이렇게 하면 임의의 함수  $M \rightarrow N$ 에 대한 연속성의 정의를 얻게 됩니다.

**정의 2.3.2.**  $M = (M, d_M)$ 과  $N = (N, d_N)$ 을 거리 공간이라고 합시다. 함수  $f: M \rightarrow N$ 이 점  $p \in M$ 에서 **연속**이라는 것은, 모든  $\varepsilon > 0$ 에 대해 다음을 만족하는  $\delta > 0$ 가 존재함을 의미합니다.

$$d_M(x, p) < \delta \implies d_N(f(x), f(p)) < \varepsilon.$$

더 나아가, 함수  $f$  전체가 연속이라는 것은 모든 점  $p \in M$ 에서 연속임을 의미합니다.

군의 동형사상을 정의할 때와 마찬가지로, 한 조건에는  $M$ 의 거리를, 다른 조건에는  $N$ 의 거리를 사용한다는 점에 주목하십시오.

이러한 일반화가 좋은 이유는  $\mathbb{R}$ 에서의 연속성 논증을  $\mathbb{C}$ 와 같은 더 일반적인 공간으로 어떻게 옮길 수 있는지를 즉시 알려주기 때문입니다. 그럼에도 불구하고 이 정의는 실수 (엡실론과 델타)를 광범위하게 사용하기 때문에 다루기에 다소 번거롭습니다. 다음은 이와 동치인 조건입니다.

### 정리 2.3.3 (점렬 연속성)

거리 공간의 함수  $f: M \rightarrow N$ 이 점  $p \in M$ 에서 연속인 것은 다음 성질이 성립하는 것과 동치입니다:  $M$ 에서  $p$ 로 수렴하는 모든 수열  $x_1, x_2, \dots$ 에 대해,  $N$ 에서 수열  $f(x_1), f(x_2), \dots$ 가  $f(p)$ 로 수렴합니다.

증명. 한쪽 방향은 그리 어렵지 않습니다:

**연습문제 2.3.4.**  $\varepsilon$ - $\delta$  연속성이 각 점에서의 점렬 연속성을 함의함을 보이십시오.

역으로,  $f$ 가  $p$ 에서  $\varepsilon$ - $\delta$  연속이 아니면 수렴을 보존하지 않음을 증명하겠습니다.

$f$ 가  $p$ 에서 연속이 아니라면, "나쁜"  $\varepsilon > 0$ 이 존재하며, 이를 이제 고정된 것으로 간주합니다. 그러면  $\delta = 1/n$ 을 선택할 때마다,  $p$ 로부터  $\delta$  이내에 있지만  $f(p)$ 로부터  $\varepsilon$ 보다 더 멀리 사상되는 어떤 점  $x_n$ 이 존재해야 합니다. 그러나 그러면 수열  $x_n$ 은  $p$ 로 수렴하는데,  $f(x_n)$ 은 항상  $f(p)$ 로부터 적어도  $\varepsilon$ 만큼 떨어져 있으므로 모순입니다.  $\square$

순차 연속성의 유용함을 보여주는 응용 예시입니다:

**명제 2.3.5 (연속함수의 합성은 연속입니다)**

$f: M \rightarrow N$ 과  $g: N \rightarrow L$ 을 거리 공간 사이의 연속 사상이라고 합시다. 그러면 이들의 합성  $g \circ f$ 는 연속입니다.

증명. 수열을 사용하면 정말 간단합니다:  $p \in M$ 을 임의로 잡고  $M$ 에서  $x_n \rightarrow p$ 라고 합시다. 그러면  $N$ 에서  $f(x_n) \rightarrow f(p)$ 이고,  $L$ 에서  $g(f(x_n)) \rightarrow g(f(p))$ 이므로, 증명 완료입니다.  $\square$

**질문 2.3.6.**  $M$ 을 임의의 거리 공간,  $D$ 를 이산 공간이라고 합시다. 사상  $f: D \rightarrow M$ 은 언제 연속입니까?

## §2.4 위상동형사상

**이 절의 대표적인 예:** 단위원  $S^1$ 은 단위정사각형의 경계와 위상동형입니다.

우리는 언제 두 군을 같다고 여깁니까? 답: 그 사이에 구조를 보존하면서 전단사이기도 한 사상이 존재할 때입니다. 거리 공간에서도 정확히 같은 방식으로 하되, "구조를 보존한다"를 "연속이다"로 바꿉니다.

**정의 2.4.1.**  $M$ 과  $N$ 을 거리 공간이라고 합시다. 함수  $f: M \rightarrow N$ 이 **위상동형사상**이라는 것은, 이것이 전단사이고  $f: M \rightarrow N$ 과 그 역사상  $f^{-1}: N \rightarrow M$ 이 모두 연속임을 의미합니다. 이때  $M$ 과  $N$ 은 **위상동형**이라고 합니다.

말할 필요도 없이, 위상동형은 동치 관계입니다.

$f^{-1}$ 도 연속이어야 한다는 조건이 요구되는 것에 놀랄 수도 있습니다. 이유는 다음과 같습니다:  $\phi$ 가 군의 동형사상이면  $\phi^{-1}$ 도 군 연산을 보존하므로  $\phi^{-1}$  자체가 동형사상임을 보일 수 있습니다. 연속 전단사에 대해서는 이것이 성립하지 않으며, 바로 이 때문에 새로운 조건이 필요합니다.

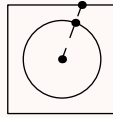
**예제 2.4.2 (위상동형사상  $\neq$  연속 전단사)**

- (a)  $[0, 1)$ 에서 원으로 가는 연속 전단사, 이 존재하지만, 이것은 연속인 역사상을 갖지 않습니다.
- (b)  $M$ 을 크기가  $|\mathbb{R}|$ 인 이산 공간이라고 합시다. 그러면 연속 함수  $M \rightarrow \mathbb{R}$ 이 존재하지만, 이는 확실히 연속인 역사상을 갖지 않습니다.

이것이 위상수학자의 "같음"에 대한 정의라는 점에 유의하십시오 – 위상동형사상은 "연속적인 변형"입니다. 몇 가지 예시가 있습니다.

**예제 2.4.3 (위상동형사상의 예시)**

- (a) 임의의 공간  $M$ 은 항등 사상을 통해 자기 자신과 위상동형입니다.
- (b) 옛말에 이르길: 도넛(원환면)은 커피잔과 위상동형입니다. (들어본 적이 없다면 찾아보십시오.)
- (c) 단위원  $S^1$ 은 단위 정사각형의 경계와 위상동형입니다. 적절한 스케일링을 거친 후, 둘 사이의 전단사 하나는 다음과 같습니다:



#### 예제 2.4.4 (단위원 위의 거리함수)

$S^1$  위의 우리의 거리함수가  $\mathbb{R}^2$ 로부터 물려받은 것, 즉 원 위의 두 점 사이의 거리가 현의 길이로 정의된 것이었다는 사실이 이상하게 느껴졌을 수 있습니다. 두 점을 잇는 더 짧은 호의 길이를 사용하는 것이 더 합리적이지 않았을까요?

사실 어느 쪽이든 상관없습니다:  $S^1$ 에 "현" 거리함수와 "호" 거리함수를 부여하여 생각하면, 둘 사이의 사상이 연속이므로 서로 위상동형인 두 공간을 얻습니다. 일반적인  $n$ 에 대한  $S^{n-1}$ 에 대해서도 마찬가지입니다.

#### 예제 2.4.5 (위상동형사상은 실제로 크기를 보존하지 않는다)

놀랍게도, 열린 구간  $(-1, 1)$ 은 실수선  $\mathbb{R}$ 과 위상동형입니다! 전단사 하나는 다음과 같이 주어집니다

$$x \mapsto \tan(x\pi/2)$$

그 역함수는  $t \mapsto \frac{2}{\pi} \arctan(t)$ 로 주어집니다.

$(-1, 1)$ 은  $\mathbb{R}$ 과 그다지 닮아 보이지 않으므로 이는 놀랍게 느껴질 수 있습니다; 전자는 "유계"인 반면 후자는 "비유계"입니다.

## §2.5 확장된 예시/정의: 곱 거리함수

이 절의 대표적인 예:  $\mathbb{R} \times \mathbb{R}$ 은  $\mathbb{R}^2$ 입니다.

이후에 등장할 확장된 예시가 여기 있습니다.  $M = (M, d_M)$ 과  $N = (N, d_N)$ 을 거리 공간이라 합시다 (예를 들어  $M = N = \mathbb{R}$ ). 우리의 목표는  $M \times N$  위에 거리 공간을 정의하는 것입니다.

$i = 1, 2$ 에 대해  $p_i = (x_i, y_i) \in M \times N$ 이라 합시다. 점들의 집합  $M \times N$  위에서 다음 거리함수들을 생각해 봅시다:

$$d_{\text{최대값}}(p_1, p_2) := \max \{d_M(x_1, x_2), d_N(y_1, y_2)\}$$

$$d_{\text{유클리드}}(p_1, p_2) := \sqrt{d_M(x_1, x_2)^2 + d_N(y_1, y_2)^2}$$

$$d_{\text{택시}}(p_1, p_2) := d_M(x_1, x_2) + d_N(y_1, y_2).$$

이들 모두 좋은 후보입니다. 우리가 어느 것을 사용하든 상관없다는 것을 곧 확인할 것입니다:

#### 연습문제 2.5.1. 다음을 확인하십시오

$$d_{\text{최대값}}(p_1, p_2) \leq d_{\text{유클리드}}(p_1, p_2) \leq d_{\text{택시}}(p_1, p_2) \leq 2d_{\text{최대값}}(p_1, p_2).$$

이를 이용하여, 세 거리함수 중 어느 것을 부여하더라도 얻어지는 거리 공간들이 위상동형이며, 그 위상동형사상은 단지 항등 사상임을 보이십시오.

**정의 2.5.2.** 따라서 우리는 보통  $M \times N$  위의 거리함수를 그냥 그 거리함수라 부르며, 이를 **곱 거리함수**라 합니다. 세 거리함수 중 어느 것을 선택하는지는 중요하지 않을 것입니다.

**예제 2.5.3** ( $\mathbb{R}^2$ )

$M = N = \mathbb{R}$ 이면, 우리는 유클리드 평면인  $\mathbb{R}^2$ 를 얻습니다. 거리함수  $d_{\text{유클리드}}$ 는 우리가 처음 시작한 것이지만, 나머지 두 거리함수 중 어느 것을 사용해도 마찬가지로 잘 작동합니다.

곱 거리함수는 수열의 수렴과 잘 어울립니다.

**명제 2.5.4** (곱 거리함수에서의 수렴은 성분별로 이루어진다)

$(x_n, y_n) \rightarrow (x, y)$ 인 것과  $x_n \rightarrow x$ 이고  $y_n \rightarrow y$ 인 것은 동치입니다.

증명.  $d_{\text{곱}}((x, y), (x_n, y_n)) = \max\{d_M(x, x_n), d_N(y, y_n)\}$ 이며,  $n \rightarrow \infty$ 일 때 이 값이 0에 수렴하는 것은  $d_M(x, x_n) \rightarrow 0$ 이고  $d_N(y, y_n) \rightarrow 0$ 인 것과 동치입니다.  $\square$

이것의 응용 하나를 살펴봅시다:

**명제 2.5.5** (덧셈과 곱셈은 연속입니다)

덧셈과 곱셈 사상은 연속 사상  $\mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ 입니다.

증명. 곱셈의 경우: 임의의  $n$ 에 대해 다음이 성립합니다

$$\begin{aligned} x_n y_n &= (x + (x_n - x))(y + (y_n - y)) \\ &= xy + y(x_n - x) + x(y_n - y) + (x_n - x)(y_n - y) \\ \implies |x_n y_n - xy| &\leq |y| |x_n - x| + |x| |y_n - y| + |x_n - x| |y_n - y|. \end{aligned}$$

$n \rightarrow \infty$ 일 때, 우변의 세 항은 모두 0으로 수렴합니다.  $+: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ 가 연속이라는 증명도 비슷합니다(그리고 더 쉽습니다): 임의의  $n$ 에 대해 다음이 성립함을 확인하면 됩니다

$$|(x_n + y_n) - (x + y)| \leq |x_n - x| + |y_n - y|$$

그리고  $n \rightarrow \infty$ 일 때 우변의 두 항은 모두 0으로 수렴합니다.  $\square$

**문제 2C**에서는 나머지 두 연산인 뺄셈과 나눗셈을 다룹니다. 이로부터 얻는 결론은, 합성 또한 연속이므로 자연스럽게 등장하는 대부분의 실숫값 함수들이 자동으로 연속이 된다는 것입니다. 예를 들어 함수  $\frac{3x}{x^2+1}$ 는  $+$ ,  $\times$ ,  $\div$ 를 합성하여 얻을 수 있으므로  $\mathbb{R} \rightarrow \mathbb{R}$ 의 연속 함수가 됩니다.

## §2.6 열린집합

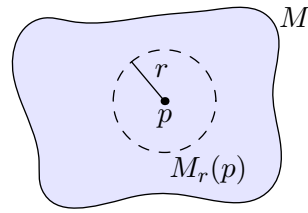
**이 절의 대표적인 예:**  $\mathbb{R}^2$ 에서의 열린 원판  $x^2 + y^2 < r^2$ .

연속성은 사실 "국소적으로" 무슨 일이 일어나는지에 관한 것입니다: 즉 함수가 "특정한 점  $p$  근처에서" 어떻게 행동하는지에 관한 것입니다. 이러한 "가까움"의 개념을 포착하는 한 가지 방법은 위에서 했던 것처럼 거리를 사용하는 것입니다. 이런 방식으로 점의  $r$ -근방을 정의할 수 있습니다.

**정의 2.6.1.**  $M$ 을 거리 공간이라 합시다. 각 실수  $r > 0$ 과 점  $p \in M$ 에 대해, 다음과 같이 정의합니다

$$M_r(p) := \{x \in M : d(x, p) < r\}.$$

집합  $M_r(p)$ 는  $p$ 의  $r$ -근방이라 불립니다.



$r$ -근방을 이용하면 수렴을 더 간결하게 다시 표현할 수 있습니다. 구체적으로, 수열  $(x_n)$  이  $x$ 로 수렴한다는 것은  $x$ 의 모든  $r$ -근방에 대해  $x_n$ 의 모든 항이 결국 그  $r$ -근방 안에 머무른다는 것을 의미합니다.

함수에 대해서도 같은 것을 해봅시다.

**질문 2.6.2.**  $r$ -근방의 관점에서, 함수  $f: M \rightarrow N$ 이 점  $p \in M$ 에서 연속이라는 것은 무엇을 의미할까요?

본질적으로, 우리는 모든  $\varepsilon$ -근방의 원상이 그 안에 어떤  $\delta$ -근방이 존재한다는 성질을 갖기를 요구합니다. 이는 다음을 동기로 제시합니다:

**정의 2.6.3.** 집합  $U \subseteq M$ 이  $M$ 에서 **열린**(open) 집합이라는 것은, 각  $p \in U$ 에 대해  $p$ 의 어떤  $r$ -근방이  $U$  안에 포함된다는 것을 의미합니다. 다시 말해,  $M_r(p) \subseteq U$ 인  $r > 0$ 가 존재합니다.

**표기의 남용 2.6.4.** 어떤 집합이 열려 있다는 것은 모(母)공간  $M$ 에 상대적으로 정의된다는 점에 유의하십시오. 다만  $M$ 이 자명하게 이해되는 경우에는 " $M$ 에서 열린"을 그냥 "열린"으로 줄여 부를 수 있습니다.

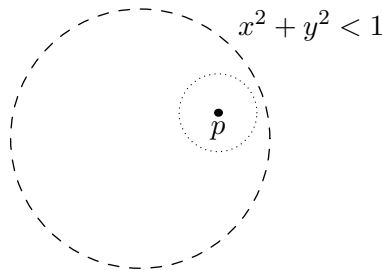


그림 2.1:  $\mathbb{R}^2$ 에서 점  $x^2 + y^2 < 1$ 의 집합은  $\mathbb{R}^2$ 에서 열려 있습니다.

#### 예제 2.6.5 (열린집합의 예)

- (a) 점의 임의의  $r$ -근방은 열려 있습니다.
- (b)  $\mathbb{R}$ 의 열린 구간은  $\mathbb{R}$ 에서 열려 있으며, 바로 이 때문에 그런 이름이 붙었습니다! 이것이 엄두에 두어야 할 전형적인 예시입니다.
- (c) 열린 단위 공  $B^n$ 도 같은 이유로  $\mathbb{R}^n$ 에서 열려 있습니다.
- (d) 특히, 열린 구간  $(0, 1)$ 은  $\mathbb{R}$ 에서 열려 있습니다. 하지만 이를  $\mathbb{R}^2$ 에 매장하면 더 이상 열려 있지 않습니다!
- (e) 공집합  $\emptyset$ 과 전체 점의 집합  $M$ 은  $M$ 에서 열려 있습니다.

**예제 2.6.6 (열린집합이 아닌 예시들)**

- (a) 닫힌 구간  $[0, 1]$ 은  $\mathbb{R}$ 에서 열려 있지 않습니다. 점 0의  $\varepsilon$ -근방 중  $[0, 1]$ 에 포함되는 것은 없습니다.
- (b) 단위원  $S^1$ 은  $\mathbb{R}^2$ 에서 열려 있지 않습니다.

**질문 2.6.7.** 이산 공간의 열린집합은 무엇입니까?

열린집합의 매우 중요한 두 가지 성질을 소개합니다.

**명제 2.6.8 (열린집합의 교집합과 합집합)**

- (a) 유한 개의 열린집합의 교집합은 열려 있습니다.
- (b) 무한히 많더라도, 열린집합들의 합집합은 열려 있습니다.

**질문 2.6.9.** 이것이 참임을 스스로 확인해 보십시오.

**연습문제 2.6.10.**  $\mathbb{R}$ 에서 교집합이  $\{0\}$ 이 되는 열린집합의 무한 모임을 하나 제시하십시오. 이는 열린집합들의 무한 교집합이 반드시 열려 있는 것은 아님을 함의합니다.

이것의 요점을 정리하면 다음과 같습니다.

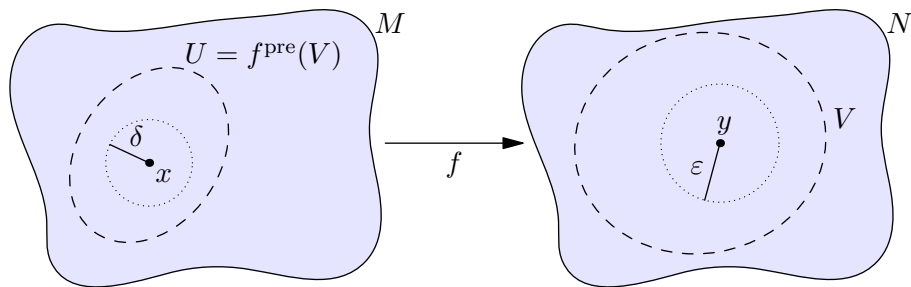
**정리 2.6.11 (열린집합 조건)**

거리 공간 사이의 함수  $f: M \rightarrow N$ 이 연속인 것과,  $N$ 의 모든 열린집합의 원상이  $M$ 에서 열려 있는 것은 동치입니다.

증명. 한쪽 방향만 증명하겠습니다...

**연습문제 2.6.12.**  $\delta$ - $\varepsilon$  연속성이 열린집합 조건으로부터 따라 나옴을 보이십시오.

이제  $f$ 가 연속이라고 가정합시다. 먼저  $V$ 가 거리 공간  $N$ 의 열린 부분집합이라 하고,  $U = f^{\text{pre}}(V)$ 라 둡시다.  $x \in U$ 를 하나 택하면  $y = f(x) \in V$ 이므로,  $U$  내부에서  $x$ 의 열린 근방을 찾고자 합니다.



$V$ 가 열려 있으므로  $y$  주위에는  $V$ 에 포함되는 작은  $\varepsilon$ -근방이 존재합니다.  $f$ 의 연속성에 의해,  $x$ 의  $\delta$ -근방이  $f$ 에 의해  $N$ 의  $\varepsilon$ -근방 안으로 대응되도록 하는  $\delta$ 를 찾을 수 있으며, 이

$\varepsilon$ -근방은 특히  $V$  안에 있습니다. 따라서 원하는 대로  $\delta$ -근방은  $U$  안에 있습니다.  $\square$

## §2.7 닫힌집합

**이 절의 대표적인 예:**  $\mathbb{R}^2$ 에서의 닫힌 단위원판  $x^2 + y^2 \leq r^2$ .

닫힌집합을 이야기하지 않은 채 열린집합을 논하는 것은 부당할 것입니다. “닫혀 있다”라는 이름은 거리 공간에서의 정의에서 비롯됩니다.

**정의 2.7.1.**  $M$ 을 거리 공간이라 합시다. 부분집합  $S \subseteq M$ 이  $M$ 에서 **닫혀** 있다는 것은 다음 성질이 성립함을 뜻합니다:  $x_1, x_2, \dots$ 를  $S$  안의 점들로 이루어진 수열이라 하고,  $x_n$ 이  $M$ 에서  $x$ 로 수렴한다고 가정합니다. 그러면  $x \in S$ 이기도 합니다.

**표기의 남용 2.7.2.** 같은 주의사항입니다: 모 공간  $M$ 이 문맥상 명확하면 “ $M$ 에서 닫혀 있다”를 그냥 “닫혀 있다”로 줄여 씁니다.

이를 표현하는 또 다른 방법이 있습니다. 부분집합  $S \subseteq M$ 의 **극한점**은 다음과 같이 정의됩니다.

$$\lim S := \{p \in M : \exists (x_n) \in S \text{ 이도록 } x_n \rightarrow p\}.$$

따라서  $S$ 가 닫혀 있는 것과  $S = \lim S$ 인 것은 동치입니다.

**연습문제 2.7.3.**  $S$ 가 닫힌집합이 아니더라도  $\lim S$ 는 닫힌집합임을 증명하십시오. (그림을 그려 보십시오.)

이러한 이유로,  $\lim S$ 는  $M$ 에서  $S$ 의 **폐포**라고도 불리며,  $\bar{S}$ 로 표기합니다. 이는 단순히  $S$ 를 포함하는 가장 작은 닫힌집합입니다.

### 예제 2.7.4 (닫힌집합의 예시)

- (a) 공집합  $\emptyset$ 은 자명한 이유로  $M$ 에서 닫힌집합입니다:  $\emptyset$ 의 원소로 이루어진 점들의 수열이 존재하지 않기 때문입니다.
- (b) 전체 공간  $M$ 은 동어반복적인 이유로  $M$ 에서 닫힌집합입니다. (이를 확인해 보십시오!)
- (c)  $\mathbb{R}$ 에서의 닫힌구간  $[0, 1]$ 은  $\mathbb{R}$ 에서 닫힌집합이며, 이 때문에 이러한 이름이 붙었습니다. 열린집합의 경우와 마찬가지로, 이는 닫힌집합의 전형적인 예시로 기억해 두어야 합니다!
- (d) 실제로, 닫힌구간  $[0, 1]$ 은  $\mathbb{R}^2$ 에서도 닫힌집합입니다.

### 예제 2.7.5 (닫힌집합이 아닌 예시)

$S = (0, 1)$ 을 열린구간이라 합시다. 그러면  $S$ 는  $\mathbb{R}$ 에서 닫힌집합이 아닌데, 왜냐하면 다음과 같은 점들의 수열이

$$\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \dots$$

$0 \in \mathbb{R}$ 로 수렴하지만,  $0 \notin (0, 1)$ 이기 때문입니다.

이제 이 용어의 혼란스러운 부분에 대해 주의를 드려야 합니다. 첫째, “대부분의” 집합은 열린집합도 닫힌집합도 아닙니다.

**예제 2.7.6 (열린집합도 닫힌집합도 아닌 집합)**

반열린구간  $[0, 1)$  은  $\mathbb{R}$ 에서 열린집합도 닫힌집합도 아닙니다.

둘째, 어떤 집합이 열린집합이면서 동시에 닫힌집합일 수도 있습니다; 이는 [장 7](#)에서 다룰 것입니다.

이렇게 상반되는 용어를 사용하는 이유는 다음 정리 때문입니다:

**정리 2.7.7 (닫힌집합은 열린집합의 여집합입니다)**

$M$ 을 거리 공간이라 하고,  $S \subseteq M$ 을 임의의 부분집합이라 합시다. 그러면 다음은 동치입니다:

- 집합  $S$ 는  $M$ 에서 닫힌집합입니다.
- 여집합  $M \setminus S$ 는  $M$ 에서 열린집합입니다.

**연습문제 2.7.8 (홀름함).** 이 정리를 증명하십시오! 무슨 일이 일어나는지 명확히 하기 위해 그림을 그려 보는 것이 좋습니다: 예를 들어,  $M = \mathbb{R}^2$ 이고  $S$ 를 닫힌 단위원판으로 택할 수 있습니다.

**§2.8 생각해 볼 만한 조금 더 어려운 문제**

**문제 2A.**  $M = (M, d)$ 를 거리 공간이라 합시다.

$$d: M \times M \rightarrow \mathbb{R}$$

가 그 자체로 연속함수임을 보이십시오 (단,  $M \times M$ 에는 곱 거리가 주어져 있습니다).

**문제 2B.**  $\mathbb{Q}$ 와  $\mathbb{N}$ 을 거리 공간으로 생각합시다 (각각 자명한 거리  $d(x, y) = |x - y|$ 를 갖습니다). 이 공간들은 위상동형입니까?

**문제 2C (산술 연산의 연속성, 계속).** 뺄셈이 연속 사상  $-: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ 이고, 나눗셈이 연속 사상  $\div: \mathbb{R} \times \mathbb{R}_{>0} \rightarrow \mathbb{R}$ 임을 보이십시오.

**문제 2D.**  $x \in \mathbb{R}$ 에서  $f$ 가 연속인 것이  $x = 0$ 인 것과 동치가 되는 함수  $f: \mathbb{R} \rightarrow \mathbb{R}$ 를 제시하십시오.



**문제 2E.** 강증가 함수  $f: \mathbb{R} \rightarrow \mathbb{R}$ 는 어떤 점에서 반드시 연속임을 증명하십시오.

**문제 2F.** 인터넷에서 누군가가 "1/x는 연속 함수인가?"라는 질문을 올려서 트위터에서 큰 논쟁이 벌어졌습니다. 이에 어떻게 답해야 할까요?



# II

## 기본 추상대수학

## 제II부: 목차

---

|          |                         |           |
|----------|-------------------------|-----------|
| <b>3</b> | <b>준동형사상과 몫군</b>        | <b>69</b> |
| 3.1      | 생성원과 군 표시               | 69        |
| 3.2      | 준동형사상                   | 70        |
| 3.3      | 잉여류와 잉여류로 나누기(모딩 아웃)    | 72        |
| 3.4      | (선택) 라그랑주 정리의 증명        | 75        |
| 3.5      | 준동형사상 없애기               | 76        |
| 3.6      | (여담) 첫 번째 동형사상 정리       | 78        |
| 3.7      | 생각해 볼 만한 조금 더 어려운 문제    | 79        |
| <br>     |                         |           |
| <b>4</b> | <b>환과 아이디얼</b>          | <b>81</b> |
| 4.1      | 환과 군에 관한 몇 가지 동기 부여용 비유 | 81        |
| 4.2      | (선택) 동기 부여에 관한 교육적 참고사항 | 81        |
| 4.3      | 환의 정의와 예시               | 81        |
| 4.4      | 체                       | 84        |
| 4.5      | 준동형사상                   | 84        |
| 4.6      | 아이디얼                    | 85        |
| 4.7      | 아이디얼 생성하기               | 87        |
| 4.8      | 주 아이디얼 정역               | 89        |
| 4.9      | 뇌터 환                    | 90        |
| 4.10     | 생각해 볼 만한 조금 더 어려운 문제    | 91        |
| <br>     |                         |           |
| <b>5</b> | <b>환의 종류</b>            | <b>93</b> |
| 5.1      | 체                       | 93        |
| 5.2      | 정역                      | 93        |
| 5.3      | 소 아이디얼                  | 94        |
| 5.4      | 극대 아이디얼                 | 95        |
| 5.5      | 분수체                     | 97        |
| 5.6      | 유일 인수분해 정역 (UFD)        | 97        |
| 5.7      | 추가: 유클리드 정역             | 99        |
| 5.8      | 생각해 볼 만한 조금 더 어려운 문제    | 104       |

---

# 3 준동형사상과 몫군

## §3.1 생성원과 군 표시

**이 절의 대표적인 예:**  $D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$

$G$ 를 군이라고 합시다. 어떤 원소  $x \in G$ 에 대해, 우리는 다음 부분군을 고려할 수 있었음을 상기하십시오.

$$\{\dots, x^{-2}, x^{-1}, 1, x, x^2, \dots\}$$

$G$ 의. 우리가 한 것을 좀 더 그림적으로 표현하면 다음과 같습니다:  $x$ 를 상자에 넣고, 단단히 밀봉한 다음, 세계 흔듭니다. 원소  $x$ 만을 사용해서, 우리는 위의 부분군을 만들어내는 멋진 폭발을 얻습니다.

상자에 두 원소  $x, y$ 를 넣으면 어떻게 될까요? 만들어지는 원소 중에는 다음과 같은 것들이 있습니다.

$$xyxyx, \quad x^2y^9x^{-5}y^3, \quad y^{-2015}, \quad \dots$$

본질적으로, 저는  $x, y, x^{-1}, y^{-1}$ 의 임의의 유한 곱을 만들어낼 수 있습니다. 이는 다음과 같이 정의하도록 이끕니다:

**정의 3.1.1.**  $S$ 를  $G$ 의 부분집합이라고 합시다.  $S$ 에 의해 **생성된** 부분군은  $\langle S \rangle$ 로 표기하며,  $S$ 의 원소들(및 그 역원들)의 유한 곱으로 쓸 수 있는 원소들의 집합입니다. 만약  $\langle S \rangle = G$ 이면  $S$ 의 원소들이 함께  $G$  전체를 만들어내므로,  $S$ 를  $G$ 의 **생성원** 집합이라고 부릅니다.

**연습문제 3.1.2.**  $G$ 가 유한군인 경우 "및 그 역원들"이라는 조건이 필요하지 않은 이유는 무엇입니까? (평소와 같이, 라그랑주 정리를 가정하십시오.)

**예제 3.1.3** ( $\mathbb{Z}$ 는 무한 순환군입니다)

1을  $\mathbb{Z} = (\mathbb{Z}, +)$ 의 원소로 생각해 봅시다.  $\langle 1 \rangle = \mathbb{Z}$ 임을 알 수 있으며, 이는  $\{1\}$ 이  $\mathbb{Z}$ 를 생성함을 의미합니다. 1의 역원인  $-1$ 도 허용된다는 점이 중요합니다: 모든 정수를 1과  $-1$ 의 합으로 쓰기 위해서는 이것이 필요합니다.

이는 군을 압축적으로 표현하려는 방법에 대한 아이디어를 줍니다. 그냥 군의 생성원 목록을 적어보는 것은 어떨까요? 예를 들어, 우리는 다음과 같이 쓸 수 있습니다

$$\mathbb{Z} \cong \langle a \rangle$$

이는  $\mathbb{Z}$ 가 단지 하나의 원소에 의해 생성되는 군임을 의미합니다.

한 가지 문제가 있습니다: 생성원들은 보통 특정 성질을 만족합니다. 예를 들어,  $\mathbb{Z}/100\mathbb{Z}$ 를 생각해 봅시다. 이것 역시 단일 원소  $x$ 에 의해 생성되지만, 이  $x$ 는  $x^{100} = 1$ 이라는 추가적인 성질을 가집니다. 이는 우리로 하여금 다음과 같이 쓰도록 동기를 부여합니다

$$\mathbb{Z}/100\mathbb{Z} = \langle x \mid x^{100} = 1 \rangle.$$

이것이 어디로 향하는지 여러분은 분명 알 수 있을 것입니다. 우리가 해야 할 일은 생성원들의 집합과 생성원들 사이의 **관계**를 명시하고, 두 원소가 서로 관계를 통해 도달할 수 있을 때에만 서로 같다고 말하는 것뿐입니다. 이러한 표현은 적절하게도 **군 표시**라고 불립니다.

**예제 3.1.4 (이면체군)**

위수  $2n$ 의 이면체군은 다음 표시를 가집니다

$$D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle.$$

따라서  $D_{2n}$ 의 각 원소는  $r^\alpha$  또는  $sr^\alpha$ 의 형태로 유일하게 쓸 수 있으며, 여기서  $\alpha = 0, 1, \dots, n-1$ 입니다.

**예제 3.1.5 (클라인 사원군)**

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 와 동형인 **클라인 사원군**은 다음 표시로 주어집니다

$$\langle a, b \mid a^2 = b^2 = 1, ab = ba \rangle.$$

**예제 3.1.6 (자유군)**

$n$ 개 원소 위의 **자유군**은 표시가  $n$ 개의 생성원을 가지고 관계는 전혀 없는 군입니다. 이는  $F_n$ 으로 표기되며, 따라서

$$F_n = \langle x_1, x_2, \dots, x_n \rangle.$$

다시 말해,  $F_2 = \langle a, b \rangle$ 는  $a, b, a^{-1}, b^{-1}$ 의 유한 개의 복사본을 이어 붙여서 형성된 문자열들의 집합입니다.

**질문 3.1.7.**  $F_1 \cong \mathbb{Z}$ 임에 유의하십시오.

**표기의 남용 3.1.8.** 안타깝게도 어떤 사람은 " $a$ 와  $b$ 에 의해 생성된 부분군"이 자유군  $\langle a, b \rangle$ 와 정확히 같은 표기법을 가진다는 것을 알아챌 수 있습니다. 우리는 문맥에 따라 어느 쪽을 의미하는지 명확히 하고자 노력할 것입니다.

표시(presentation)는 군을 콤팩트하게 적어 내려가는 방법을 제공하므로 유용합니다. 하지만 몇 가지 단점도 있습니다.<sup>1</sup>

**예제 3.1.9 (표시(presentation)는 매우 다르게 보일 수 있습니다)**

같은 군이라도 매우 다른 표시를 가질 수 있습니다. 예를 들어 다음을 생각해 봅시다:

$$D_{2n} = \langle x, y \mid x^2 = y^2 = 1, (xy)^n = 1 \rangle.$$

(이것이 동치임을 확인하려면  $x = s, y = rs$ 로 놓으십시오.)

## §3.2 준동형사상

**이 절의 대표적인 예:** "100으로 나머지를 취하는" 사상,  $\mathbb{Z} \rightarrow \mathbb{Z}/100\mathbb{Z}$ .

군들은 서로 어떻게 대화할 수 있을까요?

<sup>1</sup>사실, 표시의 두 원소가 같은지 판정하는 문제는 결정 불가능합니다. 심지어 표시로부터 군이 유한한지 판정하는 것조차 결정 불가능합니다.

두 군 사이에 동형사상을 쓸 수 있다면 두 군은 "같다"고 합니다. 그리고 앞서 보았듯이, 두 거리 공간 사이에 위상동형사상을 쓸 수 있다면 두 거리 공간은 "같다"고 합니다. 그런데 연속 사상에 대응하는 군의 유사 개념은 무엇일까요? 그저 "전단사" 조건을 빼면 됩니다.

**정의 3.2.1.**  $G = (G, \star)$ 와  $H = (H, *)$ 를 군이라 합시다. **군 준동형사상**이란 임의의  $g_1, g_2 \in G$ 에 대해 다음을 만족하는 사상  $\phi: G \rightarrow H$ 입니다

$$\phi(g_1 \star g_2) = \phi(g_1) * \phi(g_2).$$

(지난 장의 "위상동형사상"과 혼동하지 마십시오: 철자에 유의하십시오.)

### 예제 3.2.2 (준동형사상의 예시)

$G$ 와  $H$ 를 군이라 합시다.

- (a) 임의의 동형사상  $G \rightarrow H$ 는 준동형사상입니다. 특히 항등 사상  $G \rightarrow G$ 는 준동형사상입니다.
- (b) **자명한 준동형사상**  $G \rightarrow H$ 는 모든 것을  $1_H$ 로 보냅니다.
- (c) 각 정수를 100으로 나눈 나머지로 보내는 방식으로  $\mathbb{Z}$ 에서  $\mathbb{Z}/100\mathbb{Z}$ 으로 가는 준동형사상이 있습니다.
- (d)  $x \mapsto 10x$ 에 의한,  $\mathbb{Z}$ 에서 자기 자신으로 가는 준동형사상이 있으며, 이는 단사이지만 전사는 아닙니다.
- (e) "매장(embedding)"에 의해  $S_n$ 에서  $S_{n+1}$ 로 가는 준동형사상이 있습니다:  $\{1, \dots, n\}$  위의 모든 치환은,  $n+1$ 을 그저 고정점으로 두면  $\{1, \dots, n+1\}$  위의 치환으로 생각할 수 있습니다.
- (f)  $s_{12} \mapsto s_6$ 과  $r_{12} \mapsto r_6$ 에 의해 준동형사상  $\phi: D_{12} \rightarrow D_6$ 이 주어집니다.
- (g)  $\mathbb{Z} \rightarrow G$ 인 준동형사상을 명시하는 것은 오직 원소  $1 \in \mathbb{Z}$ 의 상만을 명시하는 것과 같습니다. 왜 그럴까요?

앞의 두 예시는 어떤 사실을 보여줍니다:  $G$ 의 표시가 하나 주어졌다고 합시다. 준동형사상  $G \rightarrow H$ 를 명시하려면, 관계식들이 모두 성립하는 방식으로  $G$ 의 각 생성원이 어디로 가는지만 명시하면 됩니다.

중요한 언급: 동형사상을 생각하는 올바른 방식은 "전단사 준동형사상"으로 보는 것입니다. 구체적으로 말하면,

**연습문제 3.2.3.**  $\phi \circ \psi = \text{id}_H$ 이고  $\psi \circ \phi = \text{id}_G$ 인 준동형사상  $\phi: G \rightarrow H$ 와  $\psi: H \rightarrow G$ 가 존재할 때, 오직 그때만  $G \cong H$ 임을 보이십시오.

그러므로 거리 공간의 위상동형사상과 군의 동형사상의 정의는 그다지 다르지 않습니다. 준동형사상의 자명한 성질 몇 가지를 살펴봅시다.

**사실 3.2.4.**  $\phi: G \rightarrow H$ 를 준동형사상이라 합시다. 그러면  $\phi(1_G) = 1_H$ 이고  $\phi(g^{-1}) = \phi(g)^{-1}$ 입니다.

증명. 지루하지만, 원한다면 직접 해낼 수 있으리라 확신합니다. □

이제 준동형사상의 매우 중요한 성질 하나를 정의해 봅시다.

**정의 3.2.5.** 준동형사상  $\phi: G \rightarrow H$ 의 **핵**은 다음과 같이 정의됩니다.

$$\ker \phi := \{g \in G : \phi(g) = 1_H\}.$$

이는  $G$ 의 부분군입니다(특히, 자명한 이유로  $1_G \in \ker \phi$ 입니다).

**질문 3.2.6.**  $\ker \phi$ 가 실제로  $G$ 의 부분군임을 확인하십시오.

또한 다음과 같은 중요한 사실이 있으며, 독자께서도 이를 확인해 보시기를 권장합니다.

**명제 3.2.7 (핵이 단사성을 결정함)**

사상  $\phi$ 는  $\ker \phi = \{1_G\}$ 일 때 그리고 오직 그때만 단사입니다.

이를 구체적으로 보이기 위해, 우리 예시들 각각의 핵을 계산해 봅시다.

**예제 3.2.8 (핵의 예시들)**

(a) 임의의 동형사상  $G \rightarrow H$ 의 핵은 자명한데, 동형사상은 단사이기 때문입니다. 특히 항등 사상  $G \rightarrow G$ 의 핵은  $\{1_G\}$ 입니다.

(b) 자명한 준동형사상  $G \rightarrow H$  ( $g \mapsto 1_H$ 로 주어짐)의 핵은  $G$  전체입니다.

(c)  $n \mapsto \bar{n}$ 으로 주어지는 준동형사상  $\mathbb{Z} \rightarrow \mathbb{Z}/100\mathbb{Z}$ 의 핵은 정확히

$$100\mathbb{Z} = \{\dots, -200, -100, 0, 100, 200, \dots\}$$

입니다.

(d)  $x \mapsto 10x$ 로 주어지는 사상  $\mathbb{Z} \rightarrow \mathbb{Z}$ 의 핵은 자명합니다:  $\{0\}$ 입니다.

(e) “임베딩”을 통한  $S_n$ 에서  $S_{n+1}$ 로의 준동형사상이 존재하지만, 이 역시 단사이므로 핵이 자명합니다.

(f) 준동형사상  $\phi: D_{12} \rightarrow D_6$ 는  $s_{12} \mapsto s_6$  및  $r_{12} \mapsto r_6$ 로 주어집니다. 다음을 확인할 수 있습니다

$$\ker \phi = \{1, r_{12}^3\} \cong \mathbb{Z}/2\mathbb{Z}.$$

(g) 아래 연습문제.

**연습문제 3.2.9.** 임의의  $g \in G$ 를 고정하십시오.  $n \mapsto g^n$ 으로 주어지는 준동형사상  $\mathbb{Z} \rightarrow G$ 가 있다고 합시다. 핵은 무엇입니까?

**질문 3.2.10.** 임의의 준동형사상  $\phi: G \rightarrow H$ 에 대해, 상  $\phi^{\text{img}}(G)$ 가  $H$ 의 부분군임을 보이십시오. 따라서 우리는  $\phi$ 가 전사인 경우에 특히 관심을 가질 것입니다.

### §3.3 잉여류와 잉여류로 나누기(모딩 아웃)

이 절의 대표적인 예:  $n$ 으로 모딩 아웃하기:  $\mathbb{Z}/(n \cdot \mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$ .

다음 몇 절은 다소 밀도가 높습니다. 이 설명이 여러분에게 잘 맞지 않는다면, [Go11]를 시도해 보십시오.

$G$ 와  $Q$ 를 군이라 하고, 전사 준동형사상

$$\phi: G \twoheadrightarrow Q.$$

가 존재한다고 합시다. 다시 말해,  $\phi$ 가 단사라면  $\phi: G \rightarrow Q$ 는 전단사이고, 따라서 동형사상입니다. 하지만 우리가 그렇게 운이 좋지 않아서  $\ker \phi$ 가  $\{1_G\}$ 보다 크다고 합시다. 더 일반적인 준동형사상의 올바른 해석은 무엇입니까?

$\phi: \mathbb{Z} \rightarrow \mathbb{Z}/100\mathbb{Z}$ 이 “100으로 나눈 나머지를 취하는” 특수한 경우를 살펴봅시다. 우리는 이미 이 사상의 핵이

$$\ker \phi = 100\mathbb{Z} = \{\dots, -200, -100, 0, 100, 200, \dots\}.$$

이제  $\ker \phi$ 가  $G$ 의 부분군임을 상기하십시오. 이것이 의미하는 바는  $\phi$ 가  $\mathbb{Z}$ 의 부분군  $100\mathbb{Z}$ 에 대해 무관심하다는 것입니다:

$$\phi(15) = \phi(2000 + 15) = \phi(-300 + 15) = \phi(700 + 15) = \dots$$

따라서  $\mathbb{Z}/100\mathbb{Z}$ 은 우리가 “100으로 모딩 아웃”할 때 얻는 것입니다. 멋지지 않습니까?

다시 말해,  $G$ 를 군이라 하고  $\phi: G \twoheadrightarrow Q$ 를 핵이  $N \subseteq G$ 인 전사 준동형사상이라 합시다.

$Q$ 는  $G$ 를  $N$ 으로 나눈 몫으로 생각해야 한다고 주장합니다.

이를 형식화하기 위해,  $Q$ 를 참조하지 않고 오직  $G$ 와  $N$ 만으로 소위 몫군(quotient group)  $G/N$ 을 정의할 것이며, 이는  $Q$ 와 자연스럽게 동형사상을 이룰 것입니다.

동기 부여를 위해,  $\phi$ 와  $G$ 만을 사용하여  $Q$ 의 구체적인 서술을 제시해 봅시다. 앞의 예를 계속 사용하여,  $N = 100\mathbb{Z}$ 를  $G$ 의 부분군으로 둡니다. 다음 집합들을 생각해 봅시다

$$\begin{aligned} N &= \{\dots, -200, -100, 0, 100, 200, \dots\} \\ 1 + N &= \{\dots, -199, -99, 1, 101, 201, \dots\} \\ 2 + N &= \{\dots, -198, -98, 2, 102, 202, \dots\} \\ &\vdots \\ 99 + N &= \{\dots, -101, -1, 99, 199, 299, \dots\}. \end{aligned}$$

각 집합의 원소들은  $\phi$ 를 적용했을 때 모두 같은 상을 가지며, 나아가 서로 다른 집합에 속한 임의의 두 원소는 서로 다른 상을 가집니다. 그러면 핵심 아이디어는 다음을 알아차리는 것입니다

$Q$ 를 위 집합들을 원소로 갖는 군으로 생각할 수 있습니다.

따라서  $\phi$ 가 주어지면,  $\phi(x) = \phi(y)$ 일 때  $x \sim_N y$ 라고 함으로써  $G$  위에 동치 관계  $\sim_N$ 을 정의합니다. 이  $\sim_N$ 은  $G$ 를 몇 개의 동치류로 나누는데, 이 동치류들은  $G$  안에서 위에서와 같이  $Q$ 와 자명하게 전단사 대응됩니다. 이제 우리는 이 동치류들을 매우 명시적으로 쓸 수 있음을 주장합니다.

**연습문제 3.3.1.**  $x \sim_N y$ 인 것과 어떤  $n \in N$ 에 대해  $x = yn$ 인 것이 동치임을 보이십시오 (mod 100 예시에서, 이는 두 수가 “100의 어떤 배수만큼 차이가 난다”는 것을 의미합니다). 따라서

임의의  $g \in G$ 에 대해,  $g$ 를 포함하는  $\sim_N$ 의 동치류는 다음과 같이 명시적으로 주어집니다

$$gN := \{gn \mid n \in N\}.$$

지금 우리가 마주하고 있는 유형의 집합들을 나타내는 용어가 있습니다.

**정의 3.3.2.**  $H$ 를 (반드시 어떤 준동형사상의 핵일 필요는 없는)  $G$ 의 임의의 부분군이라 합시다.  $gH$  형태의 집합을  $H$ 의 **좌잉여류**라고 부릅니다.

**비고 3.3.3** — 표기법이 그렇게 보이지 않을 수도 있지만,  $g_1 \neq g_2$ 이더라도  $g_1N$ 이  $g_2N$ 과 같은 경우가 흔하다는 점을 기억하십시오. “mod 100” 예시에서는  $3 + N = 103 + N$ 입니다. 다시 말해, 이 잉여류들은 집합입니다.

이는 만약 제가  $g$ 가 무엇인지 알려주지 않고 “ $gH$ 를 하나의 잉여류라 하자”라고 쓴다면, 잉여류 자체만 보고서는 제가 어떤  $g$ 를 선택했는지 알아낼 수 없다는 것을 의미합니다. 만약 이 말을 믿지 못하겠다면, 제가 의미하는 바의 예를 들어 보겠습니다

$$x + 100\mathbb{Z} = \{\dots, -97, 3, 103, 203, \dots\} \implies x = ?.$$

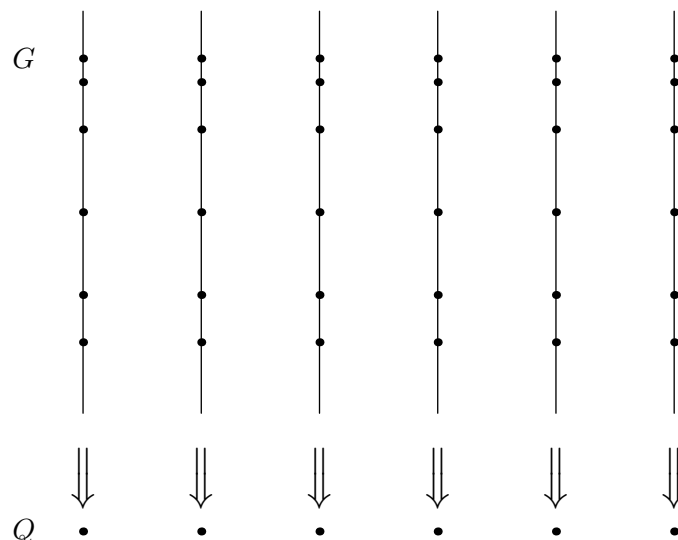
제가  $x = 3$ 을 골랐다고 생각할 이유는 없습니다. (실제로 저는  $x = -13597$ 을 골랐습니다.)

**비고 3.3.4** — 잉여류  $g_1H$ 와  $g_2H$ 가 주어졌을 때, 사상  $x \mapsto g_2g_1^{-1}x$ 가 이 둘 사이의 전단사임을 확인할 수 있습니다. 따라서 실제로 모든 잉여류는 같은 크기를 가집니다.

그러니까, 간단히 말하면,

**군  $Q$ 의 원소들은  $N$ 의 좌잉여류들과 자연스럽게 동일시됩니다.**

실제로는, 사람들이 여전히  $Q$ 의 원소를 하나의 점으로 그리는 것을 선호하는 경우가 많습니다 (예를 들어  $\mathbb{Z}/2\mathbb{Z}$ 를  $\{\{\dots, -2, 0, 2, \dots\}, \{\dots, -1, 1, 3, \dots\}\}$ 보다는  $\{0, 1\}$ 로 생각하는 것이 더 쉽습니다). 이런 그림이 마음에 든다면,  $G$ 를 (잉여류인) 높이가 모두 같은 여러 개의 올(fiber)들로 그린 다음, 이를  $Q$  위로 “붕개는(collapse)” 방식으로 나타낼 수 있습니다.



이제 이 작업을 마쳤으니, 앞서 언급했던 몫군에 대한 내재적인(intrinsic) 정의를 제시할 수 있습니다.

**정의 3.3.5.**  $G$ 의 부분군  $N$ 이 어떤 준동형사상의 핵일 때 이를 **정규**라고 부릅니다. 이는  $N \trianglelefteq G$ 로 씁니다.

**정의 3.3.6.**  $N \trianglelefteq G$ 라고 합시다. 그러면  $G/N$ 으로 표기하고 (“ $G \bmod N$ ”이라고 읽는) **몫군**은 다음과 같이 정의되는 군입니다.

- $G/N$ 의 원소들은  $N$ 의 좌잉여류들이 될 것입니다.
- $G/N$ 에서 두 잉여류  $C_1$ 과  $C_2$ 의 곱을 정의하고자 합니다. 잉여류들이  $Q$ 의 원소들과 전단사 관계에 있음을 기억하십시오. 따라서  $q_1$ 을 잉여류  $C_1$ 에 대응하는 값이라 하고,  $q_2$ 를  $C_2$ 에 대응하는 값이라 합시다. 그러면 그 곱을  $q_1q_2$ 에 대응하는 잉여류로 취할 수 있습니다.

매우 중요한 점으로, 이를 **잉여류의 대표원(representative)**을 이용하여 정의할 수도 있습니다.  $g_1 \in C_1$ 이고  $g_2 \in C_2$ 라 하면,  $C_1 = g_1N$ 이고  $C_2 = g_2N$ 입니다. 그러면  $C_1 \cdot C_2$ 는  $g_1g_2$ 를 포함하는 잉여류가 되어야 합니다. 이는  $\phi(g_1g_2) = \phi(g_1)\phi(g_2) = q_1q_2$ 이므로 위의 정의와 동일합니다. 즉, 우리가 한 일은 곱을  $H$ 의 값이 아니라  $G$ 의 원소들을 이용하여 정의한 것뿐입니다.

$gN$  표기법을 사용하고 **비고 3.3.3**을 옆두에 두면, 이를 훨씬 더 간결하게 쓸 수 있습니다

$$(g_1N) \cdot (g_2N) := (g_1g_2)N.$$

그리고 이제 정수를  $n$ 으로 나눈 나머지의 집합이 왜 흔히  $\mathbb{Z}/n\mathbb{Z}$ 로 표기되는지 아셨을 것입니다!

**질문 3.3.7.** 위 정의를 잠시 곱씹어 보십시오.

우리가 구성한 방식 때문에, 결과로 나오는 군  $G/N$ 은  $Q$ 와 동형입니다. 어떤 의미에서 우리는  $G/N$ 을 “모든  $n \in N$ 에 대해  $n = 1$ 이라는 조건을 준  $G$ ”로 생각합니다.

### §3.4 (선택) 라그랑주 정리의 증명

여담으로, 잉여류의 언어를 이용하면 이제 일반적인 경우에 대해 라그랑주 정리를 보일 수 있습니다.

#### 정리 3.4.1 (라그랑주 정리)

$G$ 를 유한군이라 하고,  $H$ 를 임의의 부분군이라 합시다. 그러면  $|H|$ 는  $|G|$ 를 나눕니다.

증명은 매우 간단합니다:  $H$ 의 잉여류들은 모두 크기가 같으며  $G$ 의 분할을 이룬다는 점에 주목하십시오 ( $H$ 가 정규가 아니더라도 성립합니다). 따라서 잉여류의 개수를  $n$ 이라 하면,  $n \cdot |H| = |G|$ 입니다.

**질문 3.4.2.**  $H = \langle x \rangle \subseteq G$ 로 놓아  $x^{|G|} = 1$ 임을 결론지으십시오.

**비고 3.4.3** — 이 시점에서 언급해 둘 것은, 일반적으로  $G$ 가 유한군이고  $N$ 이 정규라면  $|G/N| = |G|/|N|$ 이라는 사실입니다.

### §3.5 준동형사상 없애기

이 절의 대표적인 예: 다시 한번,  $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z}$ 입니다.

앞서 제시한  $G/N$ 의 마지막 정의를 살펴봅시다. 요약하면 다음과 같습니다:

- $G/N$ 의 원소는 잉여류  $gN$ 이며, 이는 관계  $\sim_N$ 의 동치류로 생각할 수 있습니다 (여기서  $g_1 \sim_N g_2$ 는 어떤  $n \in N$ 에 대해  $g_1 = g_2n$ 일 때 성립합니다).
- 잉여류  $g_1N$ 과  $g_2N$ 이 주어졌을 때, 군 연산은 다음과 같습니다

$$g_1N \cdot g_2N := (g_1g_2)N.$$

질문: 실제로  $N$ 이 정규라는 사실을 어디에서 사용합니까? 이 정의 어디에서도  $\phi$ 나  $Q$ 에 대해 이야기하지 않았습시다.

답은 **비고 3.3.3**에 있습니다. 군 연산은 두 개의 잉여류를 입력받으므로,  $g_1$ 과  $g_2$ 가 무엇인지는 알지 못합니다. 하지만 그 이면에서, **정규 조건은 군 연산이 원하는 어떤  $g_1$ 과  $g_2$ 를 선택하더라도 결국 같은 잉여류에 도달함을 보장합니다.** 만약 이 성질이 없었다면, 두 잉여류  $C_1$ 과  $C_2$ 의 곱을 정의하기가 어려웠을 것인데, 왜냐하면  $g_1 \in C_1$ 과  $g_2 \in C_2$  중 어떤 것을 선택했는지에 따라 결과가 달라질 수 있기 때문입니다.  $N$ 이 준동형사상으로부터 나왔다는 사실은, 원하는 잉여류의 대표원  $g_1$ 과  $g_2$ 를 아무렇게나 선택할 수 있음을 의미했는데, 왜냐하면 그것들은 모두 같은  $\phi$ -값을 가졌기 때문입니다.

우리는  $\phi$ 를 전혀 참조하지 않고도 이것이 성립하도록 강제하는 조건을 원합니다.  $\phi: G \rightarrow K$ 가  $H = \ker \phi$ 를 만족하는 군의 준동형사상이라 합시다.  $H$ 가 군이라는 사실 외에도, 우리는 “당연한” 성질을 얻을 수 있습니다:

**질문 3.5.1.**  $h \in H$ ,  $g \in G$ 이면  $ghg^{-1} \in H$ 임을 보이십시오. ( $\phi(ghg^{-1}) = 1_K$ 임을 확인하십시오.)

#### 예제 3.5.2 (정규가 아닌 부분군의 예)

$D_{12} = \langle r, s \mid r^6 = s^2 = 1, rs = sr^{-1} \rangle$ 라 합시다. 위수가 2인 부분군  $H = \{1, s\}$ 를 생각하면

$$rsr^{-1} = r(sr^{-1}) = r(rs) = r^2s \notin H$$

임을 알 수 있습니다. 따라서  $H$ 는 정규가 아니며, 어떤 준동형사상의 핵도 될 수 없습니다.

뭐, 당연한 얘기죠 – 그래서 어쨌다는 걸까요? 놀랍게도 이것이 바로 우리가 원하는 충분 조건임이 밝혀집니다. 구체적으로, 이 조건은 우리가 원했던 멋진 “잉여류 곱셈”이 잘 작동하도록 만듭니다.

**비고 3.5.3 (수학 경시대회 애호가를 위해)** — 이 우연의 일치는 IMO의 함수 방정식과 정말 비슷합니다. 정규 부분군  $H$ 가  $ghg^{-1} \in H$ 를 만족한다는 것은 누구나 알고 있습니다; 놀라운 점은 겉보기에 더 약해 보이는 후자의 조건으로부터  $H$ 가 정규임을 유도할 수 있다는 것입니다.

따라서 우리는  $\phi$ 를 외부적으로 참조하지 않는, “정규” 부분군에 대한 새로운 판정 기준을 얻었습니다.

**정리 3.5.4** (정규 부분군에 대한 대수적 조건)

$H$ 를  $G$ 의 부분군이라 합시다. 그러면 다음이 동치입니다:

- $H \trianglelefteq G$ .
- 모든  $g \in G$ 와  $h \in H$ 에 대해,  $ghg^{-1} \in H$ 입니다.

증명. 한쪽 방향은 이미 보였습니다.

반대 방향을 위해서는, 핵이  $H$ 인 준동형사상을 구성해야 합니다. 그래서 우리는 단순히 잉여류들의 집합으로 군  $G/H$ 를 정의합니다. 군의 연산을 부여하려면 다음을 확인해야 합니다.

**주장 3.5.5.**  $g'_1 \sim_H g_1$ 이고  $g'_2 \sim_H g_2$ 이면  $g'_1 g'_2 \sim_H g_1 g_2$ 입니다.

증명. 지루한 대수적 조작입니다(다시 함수방정식 스타일입니다).  $g'_1 = g_1 h_1$ 이고  $g'_2 = g_2 h_2$ 라 하면,  $g_1 h_1 g_2 h_2 \sim_H g_1 g_2$ 임을 보이고자 합니다.  $H$ 가 그 성질을 가지므로,  $g_2^{-1} h_1 g_2$ 는  $H$ 의 어떤 원소이며, 이를  $h_3$ 라 합시다. 따라서  $h_1 g_2 = g_2 h_3$ 이고, 좌변은  $g_1 g_2 (h_3 h_2)$ 가 되는데,  $h_3 h_2 \in H$ 이므로 문제없습니다. ■

이것이 정리되었으니 우리는 그냥 (정규 부분군의) 두 코셋의 곱을

$$(g_1 H) \cdot (g_2 H) = (g_1 g_2) H.$$

로 정의할 수 있습니다.

따라서 위의 주장은 이 곱셈이 잘 정의됨을 보여줍니다(이 검증이 정리의 "핵심 내용"입니다). 그러므로  $G/H$ 는 실제로 군입니다! 또한  $g \mapsto gH$ 에 의해 정의되는, 명백한 "사영" 준동형사상  $G \rightarrow G/H$ (핵  $H$ 를 가지는)가 존재합니다. □

**예제 3.5.6** (곱군에서 몫을 취하기)

다시 곱군  $G \times H$ 를 생각해 봅시다. 앞서 우리는 부분군

$$G' = \{(g, 1_H) \mid g \in G\} \cong G.$$

$G' \trianglelefteq G \times H$ 임을 쉽게 알 수 있습니다. (쉬운 계산입니다.) 게다가, 다음을 확인할 수 있습니다

$$(G \times H)/(G') \cong H.$$

실제로, 모든  $g \in G$ 와  $h \in H$ 에 대해  $(g, h) \sim_{G'} (1_G, h)$ 입니다.

**예제 3.5.7** (몫과 곱은 반드시 상쇄되지는 않습니다)

$(G/H) \times H \cong G$ 가 반드시 성립하는 것은 아닙니다. 예를 들어,  $G = \mathbb{Z}/4\mathbb{Z}$ 와 정규 부분군  $H = \{0, 2\} \cong \mathbb{Z}/2\mathbb{Z}$ 를 생각해 봅시다. 그러면  $G/H \cong \mathbb{Z}/2\mathbb{Z}$ 이지만,  $\mathbb{Z}/4\mathbb{Z} \not\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 입니다. (각주: 이러한 "상쇄"에 대한 정확한 조건은 슈어-잔젠 하우스 보조정리라 불립니다.)

**예제 3.5.8** (또 다른 명시적 계산)

$$r \mapsto \bar{2}, \quad s \mapsto \bar{2}$$

로 정의되는 사상  $\phi: D_8 \rightarrow \mathbb{Z}/4\mathbb{Z}$ 를 생각합시다. 이 사상의 핵은  $N = \{1, r^2, sr, sr^3\}$ 입니다.

$D_8$ 의 모든 원소에 대해 빠르게 계산해 보면 다음을 얻을 수 있습니다

$$\phi(1) = \phi(r^2) = \phi(sr) = \phi(sr^3) = \bar{0} \text{ 그리고 } \phi(r) = \phi(r^3) = \phi(s) = \phi(sr^2) = \bar{2}.$$

관련된 두 올은

$$\phi^{\text{pre}}(\bar{0}) = 1N = r^2N = srN = sr^3N = \{1, r^2, sr, sr^3\}$$

그리고

$$\phi^{\text{pre}}(\bar{2}) = rN = r^3N = sN = sr^2N = \{r, r^3, s, sr^2\}.$$

따라서  $|D_8/N| = 2$ 는 위수 2인 군, 즉  $\mathbb{Z}/2\mathbb{Z}$ 임을 알 수 있습니다. 실제로,  $\phi$ 의 상은

$$\{\bar{0}, \bar{2}\} \cong \mathbb{Z}/2\mathbb{Z}.$$

입니다.

**질문 3.5.9.**  $G$ 가 아벨 군이라고 합시다.  $G$ 의 임의의 부분군이 정규 부분군이 된다는 것이 왜 성립합니까?

마지막으로 생각해 볼 거리입니다:  $n$ 개의 생성원을 사용하는 군  $G$ 의 군 표시가 있다고 합시다. 이를  $F_n/N$  형태의 몫으로 쓸 수 있습니까? 여기서  $N$ 은  $F_n$ 의 정규 부분군입니다.

### §3.6 (여담) 첫 번째 동형사상 정리

다른 문헌들이 보통 무엇을 말하는지에 대해 간단히 언급하겠습니다.

대부분의 교과서는 실제로  $ghg^{-1} \in H$  성질을 이용하여 정규를 정의합니다. 그런 다음 위에서 제가 한 것처럼 잉여류 정의를 사용하여 정규인  $H$ 에 대해  $G/H$ 를 정의합니다

$$(g_1H) \cdot (g_2H) = g_1g_2H.$$

(제가 한 것처럼) 순수하게 대수적인 조작을 사용하면 이것이 잘 정의되며, 이제 이 군  $G/H$  인지 뭔지를 갖게 됩니다. 근처에 있는 준동형사상은 전혀 언급되지 않거나 그저 지나가듯 언급될 뿐입니다.

저는 이것이 대단히 어리석다고 생각합니다. 정규 조건은 마치 허공에서 튀어나온 것처럼 보이고 아무도 무슨 일이 벌어지고 있는지 전혀 알지 못하는데, 왜냐하면 정규 부분군이 실제로 어떤 모습이어야 하는지 아무도 감을 잡지 못하기 때문입니다.

다른 문헌들은 소위 제1 동형사상 정리도 함께 써두기를 좋아합니다.<sup>2</sup> 이는 다음과 같습니다.

#### 정리 3.6.1 (제1 동형사상 정리)

$\phi: G \rightarrow H$ 를 준동형사상이라 합시다. 그러면  $G/\ker \phi$ 는  $\phi^{\text{img}}(G)$ 와 동형입니다.

<sup>2</sup>제2, 제3 동형사상 정리도 있습니다. 하지만 그것들을 배운 지 4년이 지난 지금도 저는 여전히 그것들이 무엇인지 기억하지 못합니다. 그러니 별로 중요하지 않았던 모양이라고 짐작합니다.

제가 보기에 이는 같은 발상을 더 서투르게 서술하는 방식일 뿐입니다.

이 주장이 가진 거의 유일한 장점은,  $\phi$ 가 단사일 경우 상  $\phi^{\text{img}}(G)$ 가 군  $H$  안에 있는  $G$ 의 동형 복사본이라는 것입니다. (직접 확인해 보십시오!) 이는 우리가 수학의 다른 분야에서 도 종종 보게 될 패턴입니다: 단사인 구조 보존 사상을 가질 때마다, 종종 이 사상의 상은  $G$ 의 어떤 "복사본"이 됩니다. (여기서 "구조"란 군의 곱셈을 가리키지만, 나중에 "대상의 종류"에 대한 다른 예시들도 좀 더 보게 될 것입니다!)

그런 의미에서 단사 준동형사상  $\phi: G \hookrightarrow H$ 는  $G$ 를  $H$  안으로 매장하는 것입니다.

### §3.7 생각해 볼 만한 조금 더 어려운 문제

**문제 3A** (MIT 18.701).

$$\phi(g) = g^2$$

로 정의된 사상  $\phi: G \rightarrow G$ 가 준동형사상이 되는 모든 군  $G$ 를 구하십시오.

**문제 3B.** 이면군  $G = D_{10}$ 을 생각해 봅시다.

- (a)  $H = \langle r \rangle$ 는  $G$ 의 정규 부분군입니까? 만약 그렇다면, 동형사상까지  $G/H$ 를 계산하십시오.
- (b)  $H = \langle s \rangle$ 는  $G$ 의 정규 부분군입니까? 만약 그렇다면, 동형사상까지  $G/H$ 를 계산하십시오.

**문제 3C.**  $S_4$ 는 위수 3인 정규 부분군을 갖습니까?

**문제 3D.**  $G$ 와  $H$ 를 유한군이라 하고,  $|G| = 1000$ 이고  $|H| = 999$ 라 합시다. 준동형사상  $G \rightarrow H$ 는 반드시 자명함을 보이십시오.

**문제 3E.**  $\mathbb{C}^\times$ 가 곱셈에 대한 0이 아닌 복소수들을 나타낸다고 합시다.  $\mathbb{Z}/5\mathbb{Z}$ 가  $D_{10}$ 의 부분군임에도 불구하고,  $\mathbb{Z}/5\mathbb{Z} \rightarrow \mathbb{C}^\times$ 인 준동형사상은 다섯 개 존재하지만  $D_{10} \rightarrow \mathbb{C}^\times$ 인 준동형사상은 두 개뿐임을 보이십시오.



**문제 3F.**  $G$ 의 모든 부분군이 정규가 되는 비아벨 군  $G$ 를 찾으십시오. (이러한 군들은 **해밀턴 군**이라 불립니다.)



**문제 3G** (PRIMES 입학 시험, 2018).  $G$ 를 다음과 같은 표시(presentation)로 주어진 군이라 합시다.

$$G = \langle a, b, c \mid ab = c^2a^4, bc = ca^6, ac = ca^8, c^{2018} = b^{2019} \rangle.$$

$G$ 의 위수를 구하십시오.



**문제 3H** (동음이의어군). (영어의) 동음이의어군은 26개의 생성원  $a, b, \dots, z$ 를 가지며, 발음이 같은 모든 영어 단어 쌍에 대해 하나의 관계를 갖는 군입니다. 예를 들어  $knight = night$ 입니다 (따라서  $k = 1$ ). 이 군이 자명군임을 증명하십시오.



# 4 환과 아이디얼

## §4.1 환과 군에 관한 몇 가지 동기 부여용 비유

이 장에서는 **가환환**  $R$ 의 개념을 소개하겠습니다. 이는 군보다 더 큰 구조입니다: 하나가 아니라 덧셈과 곱셈이라는 두 개의 연산을 가지게 됩니다. 그런 다음 곧바로 환들의 쌍 사이의 **환 준동형사상**  $R \rightarrow S$ 를 정의하겠습니다.

이번에는 정규 부분군  $H \trianglelefteq G$ 를 갖는 대신, 환은 **아이디얼**이라 불리는 부분집합  $I \subseteq R$ 을 갖게 되는데, 이는 그 자체로는 환이 아니지만 몇 가지 좋은 조건들을 만족합니다. 그런 다음 앞서와 마찬가지로  $G/H$ 에 대응하여  $R/I$ 를 어떻게 정의하는지 보여드리겠습니다. 마지막으로, 군의 경우처럼 아이디얼을 생성하는 방법에 대해서도 조금 다루겠습니다.

기억하는 데 도움이 될 만한 비유 표를 아래에 제시합니다:

|       | 군                         | 환                         |
|-------|---------------------------|---------------------------|
| 표기법   | $G$                       | $R$                       |
| 연산    | $\cdot$                   | $+, \times$               |
| 가환성   | 아벨 군일 때만                  | 우리에게는 항상<br>(다루지 않음)      |
| 부분 구조 | 부분군                       |                           |
| 준동형사상 | 군 준동형사상 $G \rightarrow H$ | 환 준동형사상 $R \rightarrow S$ |
| 핵     | 정규 부분군                    | 아이디얼                      |
| 몫     | $G/H$                     | $R/I$                     |

## §4.2 (선택) 동기 부여에 관한 교육적 참고사항

이 예시들 대부분은 정수론적 관점을 염두에 두고 작성하였습니다; 따라서 초등 정수론을 좋아하셨다면 여러분의 직관 상당 부분이 그대로 이어질 것입니다. 기본적으로 우리는 환  $\mathbb{Z}$ 의 성질들을 곱셈도 가능한 임의의 아벨 구조로 일반화하려 시도할 것입니다. 그렇기 때문에, 예를 들어 “ $\mathbb{Z}$ 에서의 소수”를 이야기하듯 “ $\mathbb{Q}[x]$ 에서의 기약다항식”을 이야기할 수 있고, “ $\mathbb{Z}$ 에서의 유일 인수분해”를 이야기하듯 “법  $p$ 에 대한 다항식 인수분해”를 이야기할 수 있는 것입니다. 여러분이 오직  $\mathbb{Z}$ 에만 관심이 있더라도(예컨대 정수론자라면), 이는 상당한 가치가 있습니다: 장담컨대  $x^n + y^n = z^n$  ( $n > 2$ 인 경우)을 풀려면  $\mathbb{Z}$ 가 아닌 다른 환으로 들어가야만 합니다!

따라서 이어지는 모든 절에서,  $\mathbb{Z}$ 를 여러분의 원형으로 염두에 두시기 바랍니다.

여기서 이를 언급하는 이유는 가환대수학이 대수기하학과도 역시 밀접하게 연관되어 있기 때문입니다. 가환대수학의 많은 아이디어들은 정의에 동기를 부여하는 좋은 “기하학적” 해석을 가지고 있으며, 이러한 연관성들은 나중에 해당 파트에서 탐구됩니다. 그러므로 이것이 앞으로 다룰 내용에 동기를 부여하는 유일하게 좋은 방법은 아니라는(어쩌면 가장 자연스러운 방법조차 아닐 수 있다는) 점을 솔직히 인정하고 싶습니다.

## §4.3 환의 정의와 예시

**이 절의 대표적인 예:**  $\mathbb{Z}$ 가 시종일관 등장합니다!  $R[x]$ 와 다양한 체들도 마찬가지입니다(다음 절).

자, 환을 정의해 보겠습니다<sup>1</sup>.

<sup>1</sup>또는 일부 저자에 따르면 “항등원을 갖는 환”이라고도 합니다; 일부 저자는 환이 곱셈 항등원을 가질 것을 요구하지 않습니다. 우리에게 “환”이 항상 “1을 갖는 환”을 의미합니다.

**정의 4.3.1.** **환**은 세 쌍  $(R, +, \times)$ 이며, 두 연산은 보통 덧셈과 곱셈이라 불리고, 다음을 만족합니다

- (i)  $(R, +)$ 는 항등원  $0_R$ , 또는 그냥 0을 갖는 아벨 군입니다.
- (ii)  $\times$ 는  $R$  위의 결합적인 이항 연산으로,  $1_R$  또는 그냥 1이라 쓰이는 어떤 항등원을 갖습니다.
- (iii) 곱셈은 덧셈에 대해 분배됩니다.

환  $R$ 은  $\times$ 가 가환적이면 **가환적**이라 합니다.

**표기의 남용 4.3.2.** 평소처럼  $(R, +, \times)$ 를  $R$ 로 줄여 쓰겠습니다.

**표기의 남용 4.3.3.** 간단히 하기 위해, 이 장의 나머지 부분에서는 모든 환이 가환적이라고 가정하겠습니다. 결국 비가환환들도 마주치게 되겠지만, 그러한 환에 대해서는 어차피 이 장의 완전한 이론이 필요하지 않을 것입니다.

이 정의들은 완전성을 위해 여기 있을 뿐입니다. 예시들이 훨씬 더 중요합니다.

**예제 4.3.4 (전형적인 환들)**

- (a) 집합  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ 는 모두 통상의 덧셈과 곱셈에 대해 환입니다.
- (b) 법  $n$ 에 대한 정수들 역시 통상의 덧셈과 곱셈에 대해 환입니다. 이를  $\mathbb{Z}/n\mathbb{Z}$ 이라고도 표기합니다.

여기 자명한 예시도 하나 있습니다.

**정의 4.3.5.** **영환**은 원소가 하나뿐인 환  $R$ 입니다. 영환은 0으로 표기합니다. 환이 영환이 아니면 **자명하지 않다**고 합니다.

**연습문제 4.3.6 (코믹).** 환이 자명하지 않은 것과  $0_R \neq 1_R$ 인 것이 동치임을 보이십시오.

이 구조를 정의했으니, 이에 관한 필수적인 사실들도 함께 서술하겠습니다.

**사실 4.3.7.** 임의의 환  $R$ 과  $r \in R$ 에 대해,  $r \cdot 0_R = 0_R$ 입니다. 또한  $r \cdot (-1_R) = -r$ 입니다.

환의 예시를 몇 가지 더 살펴보겠습니다.

**예제 4.3.8 (곱환)**

두 환  $R$ 과  $S$ 가 주어졌을 때,  $R \times S$ 로 표기하는 **곱환**은 순서쌍  $(r, s)$ 로 정의되며 두 연산 모두 성분별로 이루어집니다. 예를 들어 중국인의 나머지 정리는

$$\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$

임을 말해주며, 이때 동형사상은  $n \bmod 15 \mapsto (n \bmod 3, n \bmod 5)$ 입니다.

**비고 4.3.9 —** 동등하게,  $R \times S$ 를 아벨 군  $R \oplus S$ 로 정의하고,  $r \in R, s \in S$ 에 대해  $r \cdot s = 0$ 인 곱셈을 부여한 것으로 정의할 수도 있습니다.

**질문 4.3.10.** 곱환  $R \times S$ 의 항등원은 어떤  $(r, s)$ 입니까?

**예제 4.3.11 (다항식환)**

임의의 환  $R$ 이 주어졌을 때, **다항식환**  $R[x]$ 는 계수가  $R$ 에 속하는 다항식들의 집합으로 정의됩니다:

$$R[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \mid a_0, \dots, a_n \in R\}.$$

이는 “ $R$ 에  $x$ 를 첨가한다”라고 읽습니다. 덧셈과 곱셈은 여러분이 예상하는 방식 그대로 이루어집니다.

**비고 4.3.12 (나눗셈에 관한 여담)** — 다행히도 다항식 나눗셈 역시 우리가 예상하는 대로 작동합니다:  $p \in R[x]$ 가 다항식이고  $p(a) = 0$ 이면, 어떤 다항식  $q$ 에 대해  $(x - a)q(x) = p(x)$ 입니다. 증명: 다항식 장제법을 수행하십시오. 이와 함께, 다음과 같은 주의사항에 유의하십시오

$$x^2 - 1 \equiv (x - 1)(x + 1) \pmod{8}$$

$\mathbb{Z}/8\mathbb{Z}$ 에서 근이 네 개, 즉 1, 3, 5, 7을 가집니다.

문제는 2와 4가 영이 아님에도  $2 \cdot 4 = 0$ 이라는 점입니다. 이런 이유로 2와 4를 영인자라고 부릅니다. 정역(영인자가 없는 환)에서는 이러한 병리적 현상이 사라지며, 여러분이 다항식에 대해 알고 있는 거의 모든 것이 그대로 적용됩니다. (이 내용은 다음 절에서 다시 말씀드리겠습니다.)

**예제 4.3.13 (다변수 다항식환)**

$R$ 을 계수로 하는  $n$ 개의 변수를 가진 다항식을 생각할 수 있으며, 이는  $R[x_1, \dots, x_n]$ 으로 표기합니다. (원한다면 무한히 많은  $x$ 를 첨가할 수도 있습니다!)

**예제 4.3.14 (가우스 정수는 환이다)**

**가우스 정수**는 실수부와 허수부가 모두 정수인 복소수들의 집합이며, 즉

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

**표기의 남용 4.3.15 (첨가의 자유로운 사용).** 주의 깊은 독자라면 여기서 표기법의 남용을 발견할 것입니다.  $\mathbb{Z}[i]$ 는 공식적으로는 “변수  $i$ 에 대한 정수 계수 다항식”이어야 합니다. 그러나 문맥상  $i^2 = -1$ 임이 이해되며,  $i = \sqrt{-1}$ 에 대한 다항식은 가우스 정수“인 것으로” 취급됩니다.

**예제 4.3.16 (2의 세제곱근)**

또 다른 예로 (같은 표기법 남용을 사용하면):

$$\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\}.$$

## §4.4 체

**이 절의 대표적인 예:**  $\mathbb{Q}$ 는 체이지만  $\mathbb{Z}$ 는 체가 아닙니다.

체가 무엇인지는 다음 장까지 알 필요가 없지만, 예시를 들 때 매우 편리하므로 지금 미리 소개하겠습니다.

이미 알고 계실 수도 있듯이, 곱셈이 가역이면 그 환을 체라고 부릅니다. 명확히 하기 위해 관련 정의들을 적어보겠습니다.

**정의 4.4.1.** 환  $R$ 의 **단원**은 가역인 원소  $u \in R$ 입니다: 즉 어떤  $x \in R$ 에 대해  $ux = 1_R$ 이 성립합니다.

### 예제 4.4.2 (단원의 예시)

- (a)  $\mathbb{Z}$ 의 단원은  $\pm 1$ 인데, 이는 이것들이 “1을 나누는” 유일한 것들이기 때문입니다 (이것이 “단원”이라는 이름의 이유입니다).
- (b) 반면,  $\mathbb{Q}$ 에서는 (0을 제외한) 모든 원소가 단원입니다. 예를 들어,  $\frac{3}{5} \cdot \frac{5}{3} = 1$ 이므로  $\frac{3}{5}$ 는 단원입니다.
- (c) 가우스 정수  $\mathbb{Z}[i]$ 는 네 개의 단원  $\pm 1$ 과  $\pm i$ 를 갖습니다.

**정의 4.4.3.** 자명하지 않은 (가환) 환에서 모든 영이 아닌 원소가 단원일 때, 이를 **체**라고 합니다.

구어체로는 다음과 같이 말합니다.

**체는 덧셈, 뺄셈, 곱셈, 나눗셈을 할 수 있는 구조입니다.**

문맥에 따라, 이들은 흔히  $k$ ,  $K$ ,  $F$  중 하나로 표기됩니다.

### 예제 4.4.4 (체의 첫 예시들)

- (a)  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ 는 체인데, 이는 이들 안에서  $\frac{1}{c}$ 라는 개념이 성립하기 때문입니다.
  - (b)  $p$ 가 소수이면,  $\mathbb{Z}/p\mathbb{Z}$ 는 체이며, 이를 보통  $\mathbb{F}_p$ 로 표기합니다.
- 자명한 0은 체로 간주되지 않는데, 이는 체가 자명하지 않을 것을 요구하기 때문입니다.

## §4.5 준동형사상

**이 절의 대표적인 예:** 5로 나머지를 취해  $\mathbb{Z} \rightarrow \mathbb{Z}/5\mathbb{Z}$ 로 가는 사상.

이 절은 빠르게 진행될 것입니다 – 이는 뭇군에서 다룬 모든 내용의 명백한 일반화이기 때문입니다.<sup>2</sup>

먼저, 준동형사상과 동형사상을 정의합니다.

<sup>2</sup>예전에 군보다 환을 먼저 가르치는 추상대수학 교재를 본 적이 있습니다. 그때는 왜 그런지 이해하지 못했지만, 지금은 그 이유를 알 것 같습니다 – 가환환에서 어떤 것으로 나머지를 취하는 것이 훨씬 더 자연스러우며, 그렇게 하면 환과 체의 다양한 종류들에 대해 곧바로 이야기를 시작할 수 있습니다. 또한 (제 생각에는) 군보다 환에 대해 더 생생한 첫 예시들을 갖게 됩니다. 저는 사실 이러한 접근 방식에 상당히 공감하며 – 언젠가는 Napkin을 이 방식을 따르도록 바꿀지도 모르겠습니다.

**정의 4.5.1.**  $R = (R, +_R, \times_R)$ 와  $S = (S, +_S, \times_S)$ 를 환이라 합시다. **환 준동형사상**이란 다음을 만족하는 사상  $\phi: R \rightarrow S$ 입니다.

- (i) 모든  $x, y \in R$ 에 대해  $\phi(x +_R y) = \phi(x) +_S \phi(y)$ 가 성립합니다.
- (ii) 모든  $x, y \in R$ 에 대해  $\phi(x \times_R y) = \phi(x) \times_S \phi(y)$ 가 성립합니다.
- (iii)  $\phi(1_R) = 1_S$ .

$\phi$ 가 전단사이면  $\phi$ 는 **동형사상**이며, 이때 환  $R$ 과  $S$ 는 **동형**이라고 말합니다.

정확히 예상하신 그대로입니다. 유일한 놀라운 점은  $\phi(1_R)$ 이  $1_S$ 로 가는 것도 요구한다는 것입니다. 이 조건은 불필요한 것이 아닙니다: “0을 곱하기”라고 불리는 사상  $\mathbb{Z} \rightarrow \mathbb{Z}$ 를 생각해 보십시오.

#### 예제 4.5.2 (준동형사상의 예시)

- (a) 언제나처럼, 항등 사상.
- (b) 5로 나눈 나머지를 취하는 사상  $\mathbb{Z} \rightarrow \mathbb{Z}/5\mathbb{Z}$ 입니다.
- (c) 상수항을 취함으로써  $p(x) \mapsto p(0)$ 로 정의되는 사상  $\mathbb{R}[x] \rightarrow \mathbb{R}$ 입니다.
- (d) 임의의 환  $R$ 에 대해, 자명한 환 준동형사상  $R \rightarrow 0$ 이 존재합니다.

#### 예제 4.5.3 (준동형사상이 아닌 예시들)

$1_R$ 이  $1_S$ 로 대응되어야 한다는 조건 때문에, 준동형사상이라고 생각했을 법한 몇몇 사상들은 성립하지 않습니다.

- (a)  $x \mapsto 2x$ 로 정의되는 사상  $\mathbb{Z} \rightarrow \mathbb{Z}$ 는 환 준동형사상이 아닙니다. 1을 2로 보낸다는 사실은 차치하더라도, 이 사상은 곱셈을 보존하지 않습니다.
- (b)  $S$ 가 자명하지 않은 환이라면,  $x \mapsto 0$ 으로 정의되는 사상  $R \rightarrow S$ 는 곱셈을 보존함에도 불구하고 환 준동형사상이 아닙니다.
- (c) 환 준동형사상  $\mathbb{Z}/2016\mathbb{Z} \rightarrow \mathbb{Z}$ 은 애초에 존재하지 않습니다.

특히, 군  $G$ 와  $H$ 에 대해서는  $G$ 의 모든 원소를  $1_H$ 로 보내는 자명한 군 준동형사상이 항상 존재했던 것과 달리, 환의 경우에는 그렇지 않습니다.

## §4.6 아이디얼

**이 절의 대표적인 예:** 5의 배수들은  $\mathbb{Z}$ 의 아이디얼입니다.

이제, 군을 몫으로 나눌 수 있었던 것처럼, 몫환도 정의하고 싶습니다. 그러므로 다시 한번,

**정의 4.6.1.** 환 준동형사상  $\phi: R \rightarrow S$ 의 **핵**은  $\ker \phi$ 로 표기하며,  $\phi(r) = 0$ 을 만족하는  $r \in R$ 의 집합입니다.

군론에서는 몇 가지 명백히 필요한 조건들(즉,  $gHg^{-1} = H$ )로 “정규” 부분군을 특징지을 수 있었습니다. 환에 대해서도 같은 일을 할 수 있으며, 사실 연산이 가환적이기 때문에 오히려 더 쉽습니다.

먼저, 두 가지 자명한 사실에 주목하십시오.

- $\phi(x) = \phi(y) = 0$ 이면,  $\phi(x + y) = 0$  역시 성립합니다. 따라서  $\ker \phi$ 는 덧셈에 대해 닫혀 있어야 합니다.
- $\phi(x) = 0$ 이면, 임의의  $r \in R$ 에 대해  $\phi(rx) = \phi(r)\phi(x) = 0$  역시 성립합니다. 따라서  $x \in \ker \phi$ 이고  $r \in R$ 이 어떤 것이든,  $rx \in \ker \phi$ 입니다.

공집합이 아닌 부분집합  $I \subseteq R$ 이 이러한 성질들을 만족하면 아이디얼이라고 부릅니다. 즉,

**정의 4.6.2.** 공집합이 아닌 부분집합  $I \subseteq R$ 이 덧셈에 대해 닫혀 있고, 각  $x \in I$ 와 모든  $r \in R$ 에 대해  $rx \in I$ 이면,  $I$ 를 **아이디얼**이라고 합니다.  $I \neq R$ 이면 **진**이라고 합니다.

두 번째 조건에서  $r$ 이  $I$ 에 속할 필요는 없다는 점에 주목하십시오! 따라서 이는 단순히  $I$ 가 곱셈에 대해 닫혀 있다는 것보다 더 강한 조건입니다.

**비고 4.6.3** —  $R$ 이 가환환이 아니라면,  $xr \in I$ 라는 조건도 필요합니다. 즉, 이 아이디얼은 양쪽에서 곱셈을 흡수합니다: 왼쪽과 오른쪽 모두에서 말입니다. 하지만 Napkin에서 다루는 환은 가환적이므로 이러한 구별에 대해 걱정할 필요가 없습니다.

#### 예제 4.6.4 (아이디얼의 전형적인 예)

집합  $I = 5\mathbb{Z} = \{\dots, -10, -5, 0, 5, 10, \dots\}$ 을  $\mathbb{Z}$  안의 아이디얼로 생각해 봅시다. 실제로  $I$ 가 "mod 5를 취하는" 준동형사상의 핵임을 알 수 있습니다:

$$\mathbb{Z} \rightarrow \mathbb{Z}/5\mathbb{Z}.$$

이는 덧셈에 대해 명백히 닫혀 있을 뿐 아니라,  $\mathbb{Z}$ 의 모든 원소로부터의 곱셈을 흡수합니다:  $15 \in I$ ,  $999 \in \mathbb{Z}$ 가 주어지면,  $15 \cdot 999 \in I$ 를 얻습니다.

**연습문제 4.6.5** (필수 문제: 체는 두 개의 아이디얼을 갖는다).  $K$ 가 체라면,  $K$ 가 정확히 두 개의 아이디얼을 가짐을 보이십시오. 그것들은 무엇입니까?

이제 우리는 이러한 조건들이 충분함을 주장합니다. 더 명시적으로 말하면,

#### 정리 4.6.6 (정규 부분군의 환 유사물)

$R$ 을 환이라 하고  $I \subseteq R$ 이라 합시다. 그러면  $I$ 가 어떤 준동형사상의 핵인 것과 아이디얼인 것은 동치입니다.

증명. 이는 정규 부분군에 대한 증명과 상당히 유사하므로, 연습 삼아 직접 시도해 보실 수 있습니다.

조건들이 필요조건임은 명백합니다. 이 조건들이 충분조건임을 확인하기 위해, “잉여류”를 이용해 환을 정의하겠습니다

$$S = \{r + I \mid r \in R\}.$$

이는  $r_1 \sim r_2$ 가  $r_1 - r_2 \in I$ 와 동치일 때의 동치류입니다(이를 “ $I$ 로 나눈 나머지를 취하는 것”으로 생각하십시오). 이들이 환을 이룬다는 것을 확인하려면, 우리가 이들 위에 정의한 덧셈과 곱셈이 잘 정의되어 있는지 확인해야 합니다. 구체적으로,  $r_1 \sim s_1$ 이고  $r_2 \sim s_2$ 이면  $r_1 + r_2 \sim s_1 + s_2$ 이고  $r_1 r_2 \sim s_1 s_2$ 임을 확인하고자 합니다. 첫 번째 부분은 사실 이미 다루었습니다 —  $R$ 과  $S$ 를 아벨 군으로 생각하고, 잠시 곱셈이 가능하다는 사실은 잊으십시오. 곱셈이 더 흥미롭습니다.

**연습문제 4.6.7 (권장).**  $r_1 \sim s_1$ 이고  $r_2 \sim s_2$ 이면  $r_1 r_2 \sim s_1 s_2$ 임을 보이십시오.  $I$ 에 속한 원 소뿐 아니라  $R$ 의 임의의 원소로부터의 곱셈도  $I$ 가 흡수한다는 사실을 사용해야 할 것입니다.

어쨌든 이 덧셈과 곱셈이 잘 정의되므로, 이제 핵이 정확히  $I$ 인 전사 준동형사상  $R \rightarrow S$ 가 존재합니다.  $\square$

**정의 4.6.8.** 아이디얼  $I$ 가 주어지면, 위와 같이 **몫환**을 정의합니다

$$R/I := \{r + I \mid r \in R\}.$$

이는 이러한 동치류들의 환입니다. 이 환은 “ $R$  모드  $I$ ”라고 읽습니다.

#### 예제 4.6.9 ( $\mathbb{Z}/5\mathbb{Z}$ )

“5로 덧셈적으로 나머지를 취하여” 만들어지는 정수 모듈로 5는 우리가 이미 만난  $\mathbb{Z}/5\mathbb{Z}$ 입니다.

하지만 여기서 중요한 점이 있습니다:  $\mathbb{Z}/5\mathbb{Z}$ 를  $k = 0, \dots, 4$ 에 대한  $k + 5\mathbb{Z}$ 들로 이루어진 것으로 실제로 생각하지 않는 것과 마찬가지로,  $R/I$  역시 원소  $r + I$ 로 생각하고 싶지 않습니다. 더 나은 사고방식은 다음과 같습니다

$R/I$ 는  $I$ 의 원소들을 모두 영으로 선언할 때 얻어지는 결과입니다. 즉, “ $I$ 의 원소들로 나머지를 취하는 것”입니다.

예를 들어, 5로 나머지를 취한다는 것은  $\mathbb{Z}$ 에서 5로 나누어떨어지는 모든 원소를 영으로 간주한다는 것을 의미합니다. 이것이 바로 우리가 익히 아는 모듈러 산술을 줍니다!

**연습문제 4.6.10.** 앞서 우리는 가우스 정수를  $\mathbb{Z}[i]$ 로 표기했는데, 이는 약간의 표기 남용이었 습니다. 완전히 형식적으로 표현하고자 한다면 이 환을 대신  $\mathbb{Z}[x]/(x^2 + 1)$ 로 쓸 수 있음을 스스로 확인해 보십시오. (다만 우리는 계속  $\mathbb{Z}[i]$ 를 사용할 것입니다 — 그것이 더 자연스럽게 때문입니다.) 여기서 축약 표기  $(x^2 + 1) := (x^2 + 1)\mathbb{Z}[x] = \{(x^2 + 1)f \mid f \in \mathbb{Z}[x]\}$ 는  $\mathbb{Z}[x]$  내에서  $x^2 + 1$ 의 배수들로 이루어진 아이디얼을 나타냅니다.  $\mathbb{Z}[\sqrt{2}]$ 에 대한 유사한 형식화를 찾아보십시오.

## §4.7 아이디얼 생성하기

**이 절의 대표적인 예:**  $\mathbb{Z}$ 에서, 아이디얼들은 모두  $(n)$  꼴입니다.

아이디얼에 대한 연습을 좀 해 봅시다.

중요한 직관 하나는, 아이디얼이 단위원을 포함하는 순간 1을 포함하게 되고, 따라서 환 전체를 포함해야 한다는 것입니다. 이것이 바로 “진 아이디얼”이라는 개념이 유용한 용어인 이유입니다. 이를 좀 더 부연하면:

#### 명제 4.7.1 (진 아이디얼 $\iff$ 단위원 없음)

$R$ 을 환이라 하고  $I \subseteq R$ 을 아이디얼이라 합시다. 그러면  $I$ 가 진 아이디얼인 것(즉  $I \neq R$ 인 것)은  $I$ 가  $R$ 의 단위원을 하나도 포함하지 않는 것과 동치입니다.

증명.  $I$ 가 단위원  $u$ , 즉 역원  $u^{-1}$ 를 갖는 원소  $u$ 를 포함한다고 합시다. 그러면  $I$ 는  $u \cdot u^{-1} = 1$ 을 포함하게 되고, 따라서  $I = R$ 입니다. 역으로,  $I$ 가 단위원을 전혀 포함하지 않는다면  $I$ 는 명백히 진 아이디얼입니다.  $\square$

그 결과로,  $K$ 가 체이면 그것의 아이디얼은 오직  $(0)$ 과  $K$ 뿐입니다(이는 [연습문제 4.6.5](#)에서 다룬 내용입니다). 따라서 연습을 위한 목적으로는, 체가 아닌 환들을 다루도록 하겠습니다.

첫 번째 연습:  $\mathbb{Z}$ .

**연습문제 4.7.2.**  $\mathbb{Z}$ 의 아이디얼이 정확히  $n\mathbb{Z}$  꼴의 집합들뿐임을 보이십시오. 여기서  $n$ 은 음이 아닌 정수입니다.

따라서 체의 아이디얼들은 그다지 흥미롭지 않은 반면,  $\mathbb{Z}$ 의 아이디얼들은  $\mathbb{Z}$ 의 원소들과 묘하게 닮아 있습니다. 이를 좀 더 명확히 해 봅시다.

**정의 4.7.3.**  $R$ 을 환이라 합시다. 원소들의 집합  $x_1, \dots, x_n \in R$ 에 의해 **생성된 아이디얼**은  $I = (x_1, x_2, \dots, x_n)$ 으로 표기되며 다음과 같이 주어집니다

$$I = \{r_1x_1 + \dots + r_nx_n \mid r_i \in R\}.$$

이는 “모든  $x_i$ 를 포함하는 가장 작은 아이디얼”이라고 생각할 수 있습니다.

$\{x_i\}$ 를 밀폐된 상자에 넣고 세계 흔든다는 비유가 여기서도 어느 정도 통합니다.

**비고 4.7.4 (선형대수학 여담)** — 선형대수학을 알고 있다면 이를 다음과 같이 요약할 수 있습니다: 아이디얼은  $R$ -가군입니다. 아이디얼  $(x_1, \dots, x_n)$ 은  $x_1, \dots, x_n$ 에 의해 생성되는 부분가군입니다.

특히  $I = (x)$ 이면  $I$ 는 정확히 “ $x$ 의 배수”, 즉  $r \in R$ 에 대해  $rx$ 꼴의 수들로 이루어집니다.

**비고 4.7.5** — 이 정의는 무한 생성 집합에도 적용할 수 있는데, 다만  $r_i$  중 유한개만 0이 아니어야 합니다(일반적으로 무한합은 의미가 없기 때문입니다).

#### 예제 4.7.6 (생성된 아이디얼의 예)

- (a) 모든  $n \in \mathbb{Z}$ 에 대해  $(n) = n\mathbb{Z}$ 이므로,  $\mathbb{Z}$ 의 모든 아이디얼은  $(n)$ 의 꼴입니다.
- (b)  $\mathbb{Z}[i]$ 에서는  $(5) = \{5a + 5bi \mid a, b \in \mathbb{Z}\}$ 입니다.
- (c)  $\mathbb{Z}[x]$ 에서 아이디얼  $(x)$ 는 상수항이 0인 다항식들로 이루어집니다.
- (d)  $\mathbb{Z}[x, y]$ 에서 아이디얼  $(x, y)$  역시 상수항이 0인 다항식들로 이루어집니다.
- (e)  $\mathbb{Z}[x]$ 에서 아이디얼  $(x, 5)$ 는 상수항이 5로 나누어떨어지는 다항식들로 이루어집니다.

**질문 4.7.7.** 집합  $I = \{r_1x_1 + \dots + r_nx_n \mid r_i \in R\}$ 가 실제로 항상 아이디얼임(덧셈에 대해 닫혀 있고, 곱셈을 흡수함)을 확인해 보십시오.

이제  $I = (x_1, \dots, x_n)$ 이라 합시다.  $R/I$ 는 어떤 모습일까요? 지난 절 끝에서 말했듯이, 이는 각 원소  $x_i$ 에 대해 “나머지를 취하는(mod out)” 것에 해당합니다. 예를 들면...

#### 예제 4.7.8 (생성된 아이디얼로 나머지 취하기)

- (a)  $R = \mathbb{Z}$ 이고  $I = (5)$ 라 합시다. 그러면  $R/I$ 는 문자 그대로  $\mathbb{Z}/5\mathbb{Z}$ , 즉 “5를 법으로

한 정수”입니다: 이는  $5 = 0$ 이라고 선언한 결과입니다.

- (b)  $R = \mathbb{Z}[x]$ 이고  $I = (x)$ 라고 합시다. 그러면  $R/I$ 는  $x$ 를 영으로 보낸다는 것을 의미하며, 따라서 임의의 다항식  $p(x) \in R$ 이 주어졌을 때 우리는 단순히 그 상수항을 얻게 되므로  $R/I \cong \mathbb{Z}$ 입니다.
- (c) 다시  $R = \mathbb{Z}[x]$ 라 하고 이번에는  $I = (x-3)$ 이라 합시다. 그러면  $R/I$ 는  $x-3 \equiv 0$ , 즉  $x \equiv 3$ 일 때의 몫으로 생각해야 합니다. 그러므로 다항식  $p(x)$ 가 주어지면, 나머지를 취한 후의 그 상은  $p(3)$ 으로 생각해야 합니다. 이번에도  $R/I \cong \mathbb{Z}$ 이지만, 다른 방식으로 그렇습니다.
- (d) 마지막으로  $I = (x-3, 5)$ 라 합시다. 그러면  $R/I$ 는  $x$ 를 3으로 보낼 뿐만 아니라 5도 0으로 보냅니다. 그러므로  $p \in R$ 이 주어지면, 우리는  $p(3) \pmod{5}$ 를 얻습니다. 따라서  $R/I \cong \mathbb{Z}/5\mathbb{Z}$ 입니다.

**비고 4.7.9 (나머지 표기법)** — 그런데, 환  $R$ 의 아이디얼  $I$ 가 주어졌을 때, 다음과 같이 쓰는 것은 완전히 정당합니다

$$x \equiv y \pmod{I}$$

이는  $x - y \in I$ 를 의미합니다. 모듈러 산술에 대해 배운 모든 것이 그대로 적용됩니다.

## §4.8 주 아이디얼 정역

**이 절의 대표적인 예:**  $\mathbb{Z}$ 는 PID이지만,  $\mathbb{Z}[x]$ 는 아닙니다.  $\mathbb{C}[x]$ 는 PID이지만,  $\mathbb{C}[x, y]$ 는 아닙니다.

아이디얼에  $(10, 15) \subseteq \mathbb{Z}$ 처럼 여러 개의 생성원을 넣으면 어떻게 됩니까? 정의에 의하면,  $(10, 15)$ 는 집합으로서 다음과 같이 주어집니다

$$(10, 15) := \{10x + 15y \mid x, y \in \mathbb{Z}\}.$$

정수론에 능숙하다면 이것이  $5\mathbb{Z} = (5)$ 임을 즉시 알아볼 것입니다. 놀랍지 않습니까!  $\mathbb{Z}$ 에서 아이디얼  $(a, b)$ 는 정확히  $\gcd(a, b)\mathbb{Z}$ 입니다. 그리고 바로 이것이 두 수의 최대공약수를  $(a, b)$ 로 표기하는 것을 흔히 볼 수 있는 이유입니다.

이러한 아이디얼(단 하나의 원소로 생성되는 아이디얼)을 **주 아이디얼**이라고 부릅니다. 따라서  $\mathbb{Z}$ 에서는 모든 아이디얼이 주 아이디얼입니다. 하지만 더 일반적인 환에서는 이것이 성립하지 않습니다.

### 예제 4.8.1 (주 아이디얼이 아닌 예)

$\mathbb{Z}[x]$ 에서  $I = (x, 2015)$ 는 주 아이디얼이 아닙니다.

왜냐하면 만약  $I = (f)$ 가 어떤 다항식  $f \in I$ 에 대해 성립한다면,  $f$ 는  $x$ 와 2015를 모두 나누어야 하기 때문입니다. 이는  $f = \pm 1$ 인 경우에만 가능한데, 그렇다면  $I$ 는  $\pm 1$ 을 포함해야 하지만, 실제로는 그렇지 않습니다.

모든 아이디얼이 주 아이디얼인 성질을 가진 환을 **주 아이디얼 환**이라고 부릅니다. 이 성질을 좋아하는 이유는  $\mathbb{Z}$ 에서의 최대공약수와 비슷한 방식으로 사실상 "최대공약원"을 취할 수 있게 해주기 때문입니다.

실제로는 흔히 이른바 **주 아이디얼 정역(PID)**에 관심을 갖습니다. 하지만 아직 정역이 무엇인지는 정의하지 않았습니다. 그럼에도 불구하고 아래의 모든 예시는 실제로 PID이므로, 일단 이 용어를 사용하기로 하고 다음 장에서 추가 조건이 무엇인지 알려드리겠습니다.

#### 예제 4.8.2 (PID의 예시)

다시 한번 말씀드리면, 지금은 PID라는 단어를 사용하고는 있지만 그저 이들이 주 아이디얼 환임을 확인하시면 됩니다.

- (a) 앞서 보았듯이  $\mathbb{Z}$ 는 PID입니다.
- (b) 앞서 보았듯이  $\mathbb{Z}[x]$ 는 PID가 아닌데, 예를 들어  $I = (x, 2015)$ 가 주 아이디얼이 아니기 때문입니다.
- (c) 체  $k$ 에 대해 환  $k[x]$ 는 항상 PID임이 밝혀져 있습니다. 예를 들어  $\mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ 는 PID입니다.  
이를 증명해보고 싶다면, 먼저 이 결과를 함의하는 베주 보조정리(Bézout's lemma)의 유사한 형태를 증명해 보십시오.
- (d)  $\mathbb{C}[x, y]$ 는 PID가 아닌데,  $(x, y)$ 가 주 아이디얼이 아니기 때문입니다.

## §4.9 뇌터 환

**이 절의 대표적인 예:**  $\mathbb{Z}[x_1, x_2, \dots]$ 는 뇌터 환이 아니지만, 대부분의 합리적인 환은 뇌터 환입니다. 특히 다항식환은 뇌터 환입니다. (동치로, 괴짜들만이 비뇌터 환에 관심을 가집니다.)

아이디얼이 하나의 원소로 생성된다고 요구하는 것이 너무 과하다면, 적어도 아이디얼이 유한개의 원소로 생성된다고 요구할 수는 있을 것입니다. 안타깝게도, 특정한 이상한 환에서는 이것도 성립하지 않습니다.

#### 예제 4.9.1 (비뇌터 환)

무한히 많은 자유 변수를 갖는 환  $R = \mathbb{Z}[x_1, x_2, x_3, \dots]$ 를 생각해 봅시다. 그러면 아이디얼  $I = (x_1, x_2, \dots) \subseteq R$ 은 유한 생성 집합으로 나타낼 수 없습니다.

그럼에도 불구하고, 우리가 다루는 대부분의 "정상적인" 환은 그 아이디얼이 유한 생성된다는 성질을 실제로 가지고 있습니다. 이제 이러한 환에 이름을 붙이고 동치인 두 가지 정의를 제시하겠습니다:

**명제 4.9.2 (뇌터 환의 동치 정의)**

환  $R$ 에 대하여, 다음은 동치입니다:

- (a)  $R$ 의 모든 아이디얼  $I$ 는 유한 생성됩니다(즉, 유한 생성 집합으로 나타낼 수 있습니다).
- (b) 아이디얼들의 무한 오름차순 사슬이 존재하지 않습니다

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \dots$$

이러한 사슬이 존재하지 않는다는 것을 흔히 **오름차순 사슬 조건**이라고 부릅니다. 이러한 환을 **뇌터 환**이라고 부릅니다.

**예제 4.9.3 (비뇌터 환은 오름차순 사슬 조건을 만족하지 않음)**

환  $R = \mathbb{Z}[x_1, x_2, x_3, \dots]$ 에서 우리는 무한 오름차순 사슬을 갖습니다

$$(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \dots$$

이 예시로부터 이 명제가 참인 이유를 어느 정도 알 수 있습니다: 유한 생성되지 않은 아이디얼로부터 원소를 하나씩 던져 넣음으로써 오름차순 사슬을 뽑아낼 수 있습니다. 직접 해보고 싶으시다면 증명은 여러분께 맡기겠습니다.<sup>3</sup>

**질문 4.9.4.** 체는 왜 뇌터 환입니까? PID( $\mathbb{Z}$ 와 같은)는 왜 뇌터 환입니까?

여기서 다음과 같은 질문이 남습니다: PID가 아닌 대표적인 예시인  $\mathbb{Z}[x]$ 는 뇌터 환입니까? 유명한 힐베르트 기저 정리에 따르면, 대답은 영광스럽게도 그렇다입니다.

**정리 4.9.5 (힐베르트 기저 정리)**

뇌터 환  $R$ 이 주어지면, 환  $R[x]$  또한 뇌터 환입니다. 따라서 귀납법에 의해, 임의의 정수  $n$ 에 대해  $R[x_1, x_2, \dots, x_n]$ 은 뇌터 환입니다.

이 정리의 증명은 정말로 올림피아드스러운 흥미를 지니고 있어서, 도저히 미리 밝힐 수 없습니다 – 이 장의 끝에 문제로 남겨두었습니다.

뇌터 환은 대수기하학에서 진가를 발휘하는데, 지금 당장 그 동기를 설명하기는 다소 어려우니, "여러분이 마주치게 될 대부분의 환은 뇌터 환이다"라는 말씀만 드리겠습니다. 부디 조금만 참아주십시오!

**§4.10 생각해 볼 만한 조금 더 어려운 문제**

**문제 4A.** 환  $R = \mathbb{R}[x]/(x^2 + 1)$ 은 여러분이 전에 본 적이 있는 것입니다. 그 이름은 무엇입니까?

**문제 4B.**  $\mathbb{C}[x]/(x^2 - x) \cong \mathbb{C} \times \mathbb{C}$ 임을 보이십시오.

<sup>3</sup>한편, 제가 본 이 주제를 다루는 모든 학부 수업에서는 이것을 숙제로 시킵니다. 다만 제가 그런 수업을 그렇게 많이 들어본 것은 아닙니다.

**문제 4C.** 환  $\mathbb{Z}$ 에서,  $I = (2016)$ 이고  $J = (30)$ 이라 합시다.  $I \cap J$ 가  $\mathbb{Z}$ 의 아이디얼임을 보이고 그 원소들을 계산하십시오.

**문제 4D\*.**  $R$ 을 환,  $I$ 를 아이디얼이라 합시다. 다음 사이에 포함관계를 보존하는 전단사를 찾으십시오:

- $R/I$ 의 아이디얼들과,
- $I$ 를 포함하는  $R$ 의 아이디얼들.

**문제 4E.**  $R$ 을 환이라 합시다.

- (a) 환 준동형사상  $\mathbb{Z} \rightarrow R$ 이 정확히 하나 존재함을 증명하십시오.
- (b) 환 준동형사상  $\mathbb{Z}[x] \rightarrow R$ 의 개수가  $R$ 의 원소의 개수와 같음을 증명하십시오.



**문제 4F.** 힐베르트 기저 정리, 정리 4.9.5를 증명하십시오.

**문제 4G** (USA Team Selection Test 2016).  $\mathbb{F}_p$ 가 고정된 소수  $p$ 에 대한 정수의 나머지를 나타낸다고 합시다.  $\Psi: \mathbb{F}_p[x] \rightarrow \mathbb{F}_p[x]$ 를 다음과 같이 정의합니다

$$\Psi\left(\sum_{i=0}^n a_i x^i\right) = \sum_{i=0}^n a_i x^{p^i}.$$

$S$ 가  $\Psi$ 의 상을 나타낸다고 합시다.

- (a)  $S$ 가 다항식 덧셈으로 주어지는 덧셈과 함수 합성으로 주어지는 곱셈을 갖는 환임을 보이십시오.
- (b)  $\Psi: \mathbb{F}_p[x] \rightarrow S$ 가 그러면 환 동형사상임을 증명하십시오.



**문제 4H** (아키즈키의 정리). 환  $R$ 이 **하강 사슬 조건**을 만족시키면, 즉 아이디얼의 무한 하강 사슬  $I_1 \supsetneq I_2 \supsetneq I_3 \supsetneq \dots$ 이 존재하지 않으면,  $R$ 을 **아르틴 환**이라고 부릅니다. 환  $R$ 이 아르틴 환이면 뇌터 환임을 보이십시오.

(아르틴 환은 뇌터 환보다도 대수기하학의 맥락에서 더 잘 이해됩니다 — 즉, **문제 84C\***은 아르틴 환의 훨씬 더 나은 정의를 보여줍니다. 이 문제는 여기서는 오히려 맛보기로 실려 있습니다 — 상승 사슬 조건과 하강 사슬 조건이 둘 다 단순하고 비슷해 보이기 때문에 쉬워 보이지만, 실제로는 어렵다는 것이 드러납니다.)

# 5 환의 종류

환에 대한 탐구를 이어가면서, 환이나 아이디얼이 만족할 수 있는 몇 가지 좋은 성질들을 살펴보겠습니다. 이는 나중에 유용하게 쓰일 것입니다. 이전과 마찬가지로, 정수론이 동기 부여로서 함께 엮여 있습니다. 처음부터 완성된 표가 어떤 모습일지 미리 보여드려서, 무엇을 기대해야 할지 알 수 있도록 하겠습니다.

| 환 명사 | 아이디얼 형용사 | 관계                                             |
|------|----------|------------------------------------------------|
| PID  | 주        | $R$ 이 PID이다 $\iff R$ 은 정역이고, 모든 $I$ 가 주 아이디얼이다 |
| 뇌터 환 | 유한 생성    | $R$ 이 뇌터 환이다 $\iff$ 모든 $I$ 가 유한 생성입니다          |
| 체    | 극대       | $R/I$ 가 체이다 $\iff I$ 가 극대 아이디얼이다               |
| 정역   | 소        | $R/I$ 가 정역이다 $\iff I$ 가 소 아이디얼이다               |

## §5.1 체

**이 절의 대표적인 예:**  $\mathbb{Q}$ 는 체이지만,  $\mathbb{Z}$ 는 그렇지 않습니다.

이 정의는 지난 장에서 이미 살펴보았습니다: 체  $K$ 란 영이 아닌 모든 원소가 단원인 자명하지 않은 환입니다.

특히, 체에는 오직 두 개의 아이디얼만 존재합니다: 극대인 아이디얼  $(0)$ 과, 체 전체인  $K$ 입니다.

## §5.2 정역

**이 절의 대표적인 예:**  $\mathbb{Z}$ 는 정역입니다.

실제로는, 우리가 완전한 체를 갖는 행운을 누리지 못하는 경우가 많습니다. 그럼에도 영인자 곱 성질, 즉  $ab = 0$ 이면  $a = 0$ 이거나  $b = 0$ 이라는 결론을 여전히 내릴 수 있다면 좋을 것입니다. 우리의 환이 체라면 이는 참입니다:  $b \neq 0$ 이면,  $b^{-1}$ 를 곱하여  $a = 0$ 을 얻을 수 있습니다. 하지만  $\mathbb{Z}$ 와  $\mathbb{Z}[x]$ 처럼 우리가 다루는 다른 많은 환들도 나눗셈이 없음에도 불구하고 이 성질을 가지고 있습니다.

그러나 모든 환이 그런 것은 아닙니다:  $\mathbb{Z}/15\mathbb{Z}$ 에서는,

$$3 \cdot 5 \equiv 0 \pmod{15}.$$

$a, b \neq 0$ 이지만  $ab = 0$ 이면,  $a$ 와  $b$ 를 환  $R$ 의 **영인자**라고 부릅니다. 그래서 이러한 환들에 이름을 붙여줍니다.

**정의 5.2.1.** 영인자가 없는 자명하지 않은 환을 **정역**이라고 부릅니다.<sup>1</sup>

**질문 5.2.2.** 체가 정역임을 보이십시오.

**연습문제 5.2.3** (정역에서의 소거). 정역에서  $ac = bc$ 이고  $c \neq 0$ 이라고 합시다.  $a = b$ 임을 보이십시오. ( $c^{-1}$ 를 곱할 수는 없으므로, 정의를 사용해야 합니다.)

<sup>1</sup>일부 저자들은 이를 줄여서 "domain"이라고 부르는데, 특히 Artin이 그렇습니다.

**예제 5.2.4 (정역의 예시)**

모든 체는 정역이므로, 앞서 든 모든 예시가 적용됩니다. 이에 더하여:

- (a)  $\mathbb{Z}$ 는 정역이지만, 체는 아닙니다.
- (b)  $\mathbb{R}[x]$ 는 체가 아닙니다.  $xP(x) = 1$ 을 만족하는 다항식  $P(x)$ 가 존재하지 않기 때문입니다. 하지만  $\mathbb{R}[x]$ 는 정역입니다.  $P(x)Q(x) = 0$ 이면  $P$  또는  $Q$  중 하나는 영이기 때문입니다.
- (c)  $\mathbb{Z}[x]$  또한 정역의 예시입니다. 사실, 임의의 정역  $R$ 에 대해  $R[x]$ 는 정역입니다 (왜 그럴까요?).
- (d)  $\mathbb{Z}/n\mathbb{Z}$ 은  $n$ 이 소수일 때 정확히 체(따라서 정역)입니다.  $n$ 이 소수가 아닐 때는, 환이기는 하지만 정역은 아닙니다.

자명환 0은 정역으로 간주되지 않습니다.

이 지점에서, 다음과 같이 말하겠습니다:

**정의 5.2.5.** 모든 아이디얼이 주 아이디얼인 정역을 **주 아이디얼 정역(PID)**이라고 부릅니다.

아이디얼  $(a, b)$ 는 gcd 연산의 환 버전에 해당한다는 것을 기억하십시오. 그러므로 이 정의가 본질적으로 말하는 바는: 임의의 원소 모임  $\{a_i\}$ 를 취하면, 모든  $a_i$ 에 의해 생성되는 아이디얼이 실제로는 단 하나의 원소  $a$ 에 의해 생성된다는 것입니다.

다시 말해서,

**PID에서는 임의의 원소 모임의 gcd를 취할 수 있습니다.**

환  $\mathbb{Z}/6\mathbb{Z}$ 는 주 아이디얼 환이지만 정역은 아닌 환의 예입니다. 앞서 언급했듯이, 우리는 "주 아이디얼 환"을 실제로는 거의 사용하지 않을 것입니다: 일반적으로 이를 PID로 강화하고자 할 것입니다.

## §5.3 소 아이디얼

**이 절의 대표적인 예:**  $(5)$ 는  $\mathbb{Z}$ 의 소 아이디얼입니다.

모든 정수는 (부호를 제외하면) 소수들의 곱으로 유일하게 인수분해될 수 있음을 우리는 알고 있습니다. 예를 들어  $15 = 3 \cdot 5$ 이고  $-10 = -2 \cdot 5$ 입니다. 이 증명에는 소위 베주 보조정리가 관여한다는 것을 기억하실 수도 있는데, 이는 본질적으로  $(a, b) = (\gcd(a, b))$ 임을 말합니다. 다시 말해 우리는  $\mathbb{Z}$ 가 PID라는 사실을 조심스럽게 사용한 것입니다.

일반적인 환에서는 대부분의 환이 PID가 아니기 때문에 원소를 인수분해하는 상황이 그리 좋지 않다는 것이 밝혀졌습니다. 무언가 잘못되는 대표적인 예는

$$6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$$

$\mathbb{Z}[\sqrt{-5}]$ 에서입니다. 그럼에도 불구하고 우리는 이 문제를 우회하여 아이디얼을 인수분해하는 것에 대해 이야기할 수 있습니다: 어떻게든  $10 = 2 \cdot 5$ 라는 예는  $(10) = (2) \cdot (5)$ 가 되어야 하는데, 이는 "10의 모든 배수는 2의 배수와 5의 배수의 곱이다"라는 것을 말합니다. 그렇다면 두 아이디얼을 곱하는 방법을 말씀드려야 할 텐데, 이는 유일 인수분해에 관한 장에서 다루겠습니다.

소수가 무엇인지 적어도 알아봅시다.  $\mathbb{Z}$ 에서  $p \neq 1$ 이 소수라는 것은  $p \mid xy$ 일 때마다  $p \mid x$  또는  $p \mid y$ 가 성립한다는 것입니다. 우리는 이 정의를 아이디얼의 세계로 옮겨갑니다.

**정의 5.3.1.**  $I \subsetneq R$ 인 진아이디얼  $I$ 가 **소 아이디얼**이라는 것은  $xy \in I$ 일 때마다  $x \in I$  또는  $y \in I$ 가 성립한다는 것입니다.

$I$ 가 진아이디얼이어야 한다는 조건은 우리가 1을 소수로 간주하지 않는다는 사실과 유사합니다.

### 예제 5.3.2 (소 아이디얼의 예와 반례)

- (a)  $\mathbb{Z}$ 의 아이디얼 (7)은 소 아이디얼입니다.
- (b)  $\mathbb{Z}$ 의 아이디얼 (8)은 소 아이디얼이 아닌데,  $2 \cdot 4 = 8$ 이기 때문입니다.
- (c)  $\mathbb{Z}[x]$ 의 아이디얼  $(x)$ 는 소 아이디얼입니다.
- (d)  $\mathbb{Z}[x]$ 의 아이디얼  $(x^2)$ 는 소 아이디얼이 아닌데,  $x \cdot x = x^2$ 이기 때문입니다.
- (e)  $\mathbb{Z}[x]$ 의 아이디얼  $(3, x)$ 는 소 아이디얼입니다. 이는 사실 아래의 정리 5.3.5를 이용하면 가장 쉽게 알 수 있습니다.
- (f)  $\mathbb{Z}[i]$ 의 아이디얼  $(5) = 5\mathbb{Z} + 5i\mathbb{Z}$ 는 소 아이디얼이 아닌데, 원소  $3 + i$ 와  $3 - i$ 의 곱이  $10 \in (5)$ 이지만 둘 다 그 자체로는  $(5)$ 에 속하지 않기 때문입니다.

**비고 5.3.3** — 아이디얼은 "부호 문제"를 없애준다는 좋은 성질을 가지고 있습니다. 예를 들어,  $\mathbb{Z}$ 에서  $-3$ 을 소수로 간주해야 할까요? 아이디얼로 표현하면 이런 성가신 문제는 사라집니다:  $(-3) = (3)$ 입니다. 더 일반적으로, 환  $R$ 에 대해 아이디얼로 이야기하는 것은 단원과의 곱셈을 무시할 수 있게 해줍니다. ( $-1$ 이  $\mathbb{Z}$ 에서 단원이라는 점에 유의하십시오.)

**연습문제 5.3.4.** 영 아이디얼 (0)이 소 아이디얼인 환  $R$ 을 무엇이라고 부르겠습니까?

또한 다음이 성립합니다:

### 정리 5.3.5 (소 아이디얼 $\iff$ 몫이 정역)

아이디얼  $I$ 가 소 아이디얼인 것은  $R/I$ 가 정역인 것과 동치입니다.

**연습문제 5.3.6** (필수). 이 정리가 참임을 스스로 확인해 보십시오; 이는 단지 정의를 따라가는 것일 뿐입니다. (시작점으로  $R = \mathbb{Z}$ 이고  $I = (15)$ 인 경우를 고려해 보는 것도 좋습니다.)

이제 유감스럽게도 "소" 아이디얼이라는 개념이 있어도 유일 인수분해는 여전히 성립하지 않는다는 것을 말씀드려야 합니다(다시 말하지만 아직 두 아이디얼을 곱하는 방법도 말씀드리지 않았습시다). 하지만 대수적 정수론에서 등장할 몇 가지 추가 가정 하에서는 성립하게 될 것입니다(관련 용어: 데데킨트 정역).

## §5.4 극대 아이디얼

**이 절의 대표적인 예:** 아이디얼  $(x, 5)$ 는 몫을 취함으로써  $\mathbb{Z}[x]$ 에서 극대입니다.

여기 아이디얼의 또 다른 종류가 있습니다.

**정의 5.4.1.** 환  $R$ 의 진 아이디얼  $I$ 가 다른 어떤 진 아이디얼에도 포함되지 않으면 **극대**라고 합니다.

**예제 5.4.2 (극대 아이디얼의 예시)**

- (a)  $\mathbb{Z}$ 의 아이디얼  $I = (7)$ 은 극대인데, 만약 아이디얼  $J$ 가 7과  $I$ 에 속하지 않는 원소  $n$ 을 포함한다면  $\gcd(7, n) = 1$ 도 포함해야 하고, 따라서  $J = \mathbb{Z}$ 가 되기 때문입니다.
- (b) 아이디얼  $(x)$ 는  $\mathbb{Z}[x]$ 에서 극대가 아닌데,  $(x, 5)$ 에 포함되기 때문입니다 (그 밖에도 여러 아이디얼에 포함됩니다).
- (c) 반면에,  $(x, 5)$ 는  $\mathbb{Z}[x]$ 에서 실제로 극대입니다. 이는 아래의 **정리 5.4.4**를 이용하면 가장 쉽게 확인할 수 있습니다.
- (d) 또한  $(x)$ 는  $\mathbb{C}[x]$ 에서 극대인데, 이번에도 아래의 **정리 5.4.4**에 의거합니다.

**연습문제 5.4.3.** 영 아이디얼  $(0)$ 이 극대인 환  $R$ 를 무엇이라고 부르겠습니까?

소 아이디얼에 대한 것과 유사한 정리가 있습니다.

**정리 5.4.4 ( $I$ 가 극대  $\iff R/I$ 가 체)**

아이디얼  $I$ 가 극대인 것과  $R/I$ 가 체인 것은 동치입니다.

증명. 환이 체인 것과  $(0)$ 이 유일한 극대 아이디얼인 것은 동치입니다. 따라서 이는 **문제 4D\***에 의해 성립합니다.  $\square$

**따름정리 5.4.5 (극대 아이디얼은 소 아이디얼이다)**

만약  $I$ 가 환  $R$ 의 극대 아이디얼이면,  $I$ 는 소 아이디얼입니다.

증명. 만약  $I$ 가 극대이면,  $R/I$ 는 체이고, 따라서 정역이므로,  $I$ 는 소 아이디얼입니다.  $\square$

실제로는, 생성된 아이디얼로 몫을 취하는 것이 상당히 편리하기 때문에, 이것이 어떤 아이디얼이 극대인지 확인하는 매우 효율적인 방법입니다.

**예제 5.4.6 ( $\mathbb{Z}[x]$ 에서 몫을 취하기)**

- (a) 이는  $(x, 5)$ 가  $\mathbb{Z}[x]$ 에서 극대 아이디얼임을 즉시 함의하는데,  $\mathbb{Z}[x]$ 에서  $x$ 와 5로 몫을 취하면 단지  $\mathbb{F}_5$ 를 얻고, 이는 체이기 때문입니다.
- (b) 반면에,  $x$ 만으로 몫을 취하면  $\mathbb{Z}$ 를 얻는데, 이는 정역이지만 체는 아닙니다. 이것이  $(x)$ 가 소 아이디얼이지만 극대는 아닌 이유입니다.

우리가 본 바와 같이, 모든 극대 아이디얼은 소 아이디얼입니다. 그런데 이제  $\mathbb{Z}$ 가 그 모든 영이 아닌 소 아이디얼이 또한 극대이기도 한 특별한 성질을 가진다는 점에 주목합시다. 바로 이 조건과 몇 가지 다른 사소한 조건들을 통해 아이디얼의 소인수분해가 실제로 작동하는, 이른바 데데킨트 정역을 얻게 됩니다. 이에 대해서는 나중에 더 다루겠습니다.

## §5.5 분수체

이 절의 대표적인 예:  $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$ .

여기까지 온 김에, 임의의 정역을 체로 바꾸는 유용한 구성을 소개하는 시간을 가지겠습니다.

**정의 5.5.1.** 정역  $R$ 이 주어지면, 그 **분수체** 또는 **분수 체**  $\text{Frac}(R)$ 을 다음과 같이 정의합니다: 이는 원소  $a/b$ 들로 이루어지며, 여기서  $a, b \in R$ 이고  $b \neq 0$ 입니다.  $bc = ad$ 일 때 그리고 오직 그때만  $a/b \sim c/d$ 로 놓습니다. 덧셈과 곱셈은 다음과 같이 정의됩니다

$$\begin{aligned}\frac{a}{b} + \frac{c}{d} &= \frac{ad + bc}{bd} \\ \frac{a}{b} \cdot \frac{c}{d} &= \frac{ac}{bd}.\end{aligned}$$

사실  $\mathbb{Q}$ 에 대해 여러분이 알고 있는 모든 것은 기본적으로 유추를 통해 그대로 적용됩니다. 원한다면 이것이 실제로 체임을 증명할 수 있지만,  $\mathbb{Q}$ 가 잘 정의되어 있다는 것에 우리가 얼마나 익숙한지를 고려하면, 저는 그것에 대해 걱정하지 않겠습니다...

**정의 5.5.2.**  $k$ 를 체라고 합시다.  $k(x) = \text{Frac}(k[x])$ 로 정의하고 (“ $k$  of  $x$ ”라고 읽습니다), 이를 **유리 함수체**라고 부릅니다.

### 예제 5.5.3 (분수체의 예시)

(a) 정의에 의해,  $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$ 입니다.

(b) 체  $\mathbb{R}(x)$ 는  $x$ 에 대한 유리 함수로 이루어져 있습니다:

$$\mathbb{R}(x) = \left\{ \frac{f(x)}{g(x)} \mid f, g \in \mathbb{R}[x] \right\}.$$

예를 들어,  $\frac{2x}{x^2-3}$ 이 전형적인 원소가 될 수 있습니다.

### 예제 5.5.4 (가우스 유리수)

$\mathbb{Z}[i]$ 를 표기를 남용하여 정의했던 것과 마찬가지로,  $\mathbb{Q}(i) = \text{Frac}(\mathbb{Z}[i])$ 라고도 쓸 수 있습니다. 공식적으로는 다음과 같은 것들로 이루어져야 합니다

$$\mathbb{Q}(i) = \left\{ \frac{f(i)}{g(i)} \mid g(i) \neq 0 \right\}$$

유리 계수를 갖는 다항식  $f$ 와  $g$ 에 대해서 말입니다. 하지만  $i^2 = -1$ 이므로 이는 곧 다음으로 이어집니다

$$\mathbb{Q}(i) = \left\{ \frac{a + bi}{c + di} \mid a, b, c, d \in \mathbb{Q}, (c, d) \neq (0, 0) \right\}.$$

그리고  $\frac{1}{c+di} = \frac{c-di}{c^2+d^2}$ 이므로 우리는 다음에 이르게 됩니다

$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}.$$

## §5.6 유일 인수분해 정역 (UFD)

이 절의 대표적인 예:  $\mathbb{Z}$  및 일반적인 다항식환.

여기 정수론에 관심이 있는 분들에게 중요할 별도의 정의가 하나 있습니다. 양의 정수 위에서, 모든 정수가 소수의 곱으로 유일하게 표현된다는 산술의 기본 정리가 성립합니다.

$6 = (-2)(-3)$ 과 같은 표현을 허용한다면,  $\mathbb{Z}$ 나  $\mathbb{Z}[i]$ 에서도 유사한 진술을 할 수 있습니다. 요령은 모든 것을 단원의 차이를 무시하고 고려한다는 것입니다; 그래서  $6 = (-2)(-3) = 2 \cdot 3$ 은 같은 것으로 간주됩니다.

일반적인 정의는 다음과 같습니다.

**정의 5.6.1.** 정역  $R$ 의 영이 아닌 비단원은, 두 비단원의 곱으로 쓸 수 없는 경우 **기약**이라고 합니다.

정역  $R$ 의 모든 영이 아닌 비단원이 기약원의 곱으로 쓸 수 있고, 그 표현이 단원을 곱하는 것을 제외하면 유일할 때,  $R$ 을 **유일 인수분해 정역**이라고 합니다.

**질문 5.6.2.**  $\mathbb{Z}$ 가 UFD임을 확인하십시오.

### 예제 5.6.3 (UFD의 예시)

- (a) 체는 UFD의 “퇴화된” 예시입니다: 영이 아닌 모든 원소가 단원이므로, 확인할 것이 없습니다.
- (b)  $\mathbb{Z}$ 는 UFD입니다. 기약원은  $p$ 와  $-p$ 이며, 예를 들어 5나  $-17$ 입니다.
- (c)  $\mathbb{Q}[x]$ 는 UFD입니다: 유리 계수를 갖는 다항식은 상수배를 제외하면 유일하게 인수분해될 수 있습니다 ( $\mathbb{Q}[x]$ 의 단원은 그저 유리수이기 때문입니다).
- (d)  $\mathbb{Z}[x]$ 는 UFD입니다.
- (e) 가우스 정수  $\mathbb{Z}[i]$  역시 UFD임이 밝혀집니다 (이는 대수적 정수론을 다루는 장에서 증명될 것입니다).
- (f)  $\mathbb{Z}[\sqrt{-5}]$ 는 UFD가 아닌 대표적인 예시입니다. 다음과 같이 쓸 수 있습니다.

$$6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$$

하지만 2, 3,  $1 \pm \sqrt{-5}$  각각은 기약원입니다. (이를 바로잡는 올바른 방법은 대신 소 아이디얼을 고려하는 것으로 밝혀지는데, 이것이 **부 XIV**의 주요 동기 중 하나입니다.)

- (g) 증명하지 않을 정리:  $R$ 이 UFD이면  $R[x]$ 도 UFD입니다 (따라서 귀납적으로  $R[x, y]$ ,  $R[x, y, z]$ , ...도 마찬가지입니다).

다음과 같은 정리가 있습니다.

### 정리 5.6.4

$R$ 을 PID라고 합시다. 그러면  $R$ 은 UFD입니다.

위의 반례를 살펴보면 다음과 같습니다.

$$6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$$

여기서  $\mathbb{Z}[\sqrt{-5}]$ 가 UFD가 되지 못하는 것은 어떤 인수도 더 이상 기약인수로 분해할 수 없다는 사실에 반영되어 있으며, 실제로 다음 아이디얼

$$(2, 1 + \sqrt{-5})$$

은 주 아이디얼이 아닙니다 — 2와  $1 + \sqrt{-5}$ 의 gcd가 되는 원소는 존재하지 않습니다.

비슷한 방식으로, 기약인수로의 분해가 존재한다고 가정할 때 PID가 UFD임을 증명할 수 있습니다.

## §5.7 추가: 유클리드 정역

이 장은 이후에 사용되지 않지만, 역사적으로 흥미로운 내용입니다.

PID는 원소들의 임의의 족에 대해 gcd를 취할 수 있는 환이라는 것을 상기하십시오.

$\mathbb{Z}$ 에서 두 원소의 gcd를 계산하는 가장 널리 알려진 알고리즘이 유클리드 알고리즘이라는 것은 모두 알고 있습니다.

- 두 정수  $a$ 와  $b$ 로 시작합니다.
- $a$ 와  $b$  중 하나가 0이면 끝납니다. gcd는 0이 아닌 원소입니다.
- 그렇지 않으면,  $|a| \geq |b|$ 라고 가정하고,  $a$ 를  $b$ 로 나누어  $|r| < |b|$ 를 만족하는 나머지  $r$ 을 구한 다음,  $a$ 를  $r$ 로 바꾸고 알고리즘을 계속합니다.

이 알고리즘은 매우 효율적입니다 — 이 알고리즘은  $a$ 와  $b$ 의 크기에 대해 로그 개수의 단계만 필요하다는 것을 증명할 수 있습니다 — 예를 들어,  $a$ 와  $b$ 가  $10^{100}$  자릿수 정도라면, 최악의 경우에도 500단계면 충분합니다.

자연스럽게 다음과 같은 질문이 제기됩니다.

어떤 환에서 같은 알고리즘을 수행할 수 있을까요?

사실 여러 환에서 이를 수행할 수 있다는 것을 보게 될 것입니다! 예를 들어, 가우스 정수환  $\mathbb{Z}[i]$ , 아이젠슈타인 정수환  $\mathbb{Z}[\omega]$  등이 있습니다.

위의 알고리즘 설명을 살펴보면, 이 알고리즘이 작동하게 하는 것은 무엇일까요? 그것은 두 수의 크기를 비교하는 데 사용되는 절댓값  $|\cdot|$ 이며, 이 절댓값은 두 가지 조건을 만족합니다.

- 이 함수는 음이 아닌 정수값을 출력합니다 — 그래야 알고리즘이 결국 종료됩니다.
- $b \neq 0$ 인 임의의 두 환 원소  $a$ 와  $b$ 에 대해,  $r = a - qb$ 가  $b$ 보다 작은 절댓값을 갖도록 하는 어떤  $q$ 가 존재합니다.

그러므로 자연스럽게, 이와 비슷한 정수 값을 갖는 함수가 있는 임의의 환에서 이 알고리즘을 수행할 수 있습니다. 위의 두 조건을 만족하는 함수  $N: R \rightarrow \mathbb{Z}_{\geq 0}$ 을 **유클리드 노름**이라고 부르며, 노름을 갖는 정역  $R$ 을 **유클리드 정역**이라고 부릅니다.

### 예제 5.7.1 (가우스 정수환은 유클리드 정역입니다)

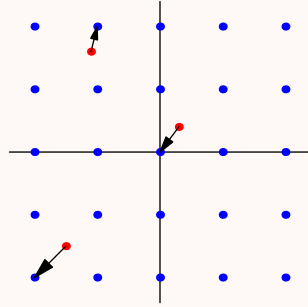
$\mathbb{Z}[i]$ 에서 통상적인 노름은

$$|a + bi| = a^2 + b^2$$

유클리드 노름입니다.

실제로,  $b \neq 0$ 인 임의의 원소  $a$ 와  $b$ 에 대해,  $a$ 를  $b$ 로 나누어 나머지  $r$ 을 계산할 수 있습니다.  $q$ 를  $\frac{a}{b}$ 에 가장 가까운 가우스 정수라 하고(즉,  $|\frac{a}{b} - q|$ 가 최소가 되도록 하고)  $r = a - bq$ 라 하면,  $|r| < |b|$ 임을 증명할 수 있습니다.

이 증명은  $|\frac{a}{b} - q| < 1$ 임을 보임으로써 이루어집니다 — 복소평면에 임베딩된  $\mathbb{Z}[i]$ 에 속한 점들의 격자를 살펴보면,  $\frac{a}{b} \in \mathbb{C}$ 의 어떤 값에 대해서도 가장 가까운 정수로 반올림하면 최대  $\frac{\sqrt{2}}{2} < 1$ 만큼 이동하게 됩니다.



### 예제 5.7.2 (아이젠슈타인 정수환은 유클리드 정역입니다)

마찬가지로  $\omega = \frac{1+\sqrt{3}i}{2}$  라 하면(즉  $\omega^3 = -1$ ),  $\mathbb{Z}[\omega]$ 는 통상적인 노름에 대해 유클리드 정역이 됩니다

$$|a + bi| = a^2 + b^2$$

또는 동등하게

$$|a + b\omega| = a^2 + ab + b^2.$$

### 예제 5.7.3 (환 $\mathbb{Z}[\sqrt{11}]$ 는 유클리드 정역입니다)

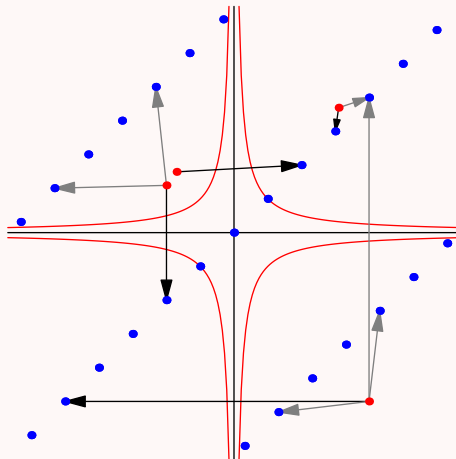
앞서와 마찬가지로입니다. 이번에는 자연스러운 노름<sup>a</sup>이 다음과 같습니다:

$$N_{\mathbb{Q}(\sqrt{11})/\mathbb{Q}}(a + b\sqrt{11}) = (a + b\sqrt{11})(a - b\sqrt{11}) = a^2 - 11b^2.$$

유클리드 노름이 필요하므로, 우리는  $N(a + b\sqrt{11}) = |a^2 - 11b^2|$  로 두겠습니다.

$\mathbb{Z}[\sqrt{11}]$ 의 두 원소  $a$ 와  $b$ 가 주어지고  $b \neq 0$ 일 때, 앞서와 마찬가지로  $r = a - qb$ 로 하여  $N(r) < N(b)$ 를 만족하는  $r$ 을 계산해 보겠습니다.

이번에는  $\mathbb{Z}[\sqrt{11}]$ 을 점들의 격자로 그릴 수 없습니다 —  $\mathbb{R}$  안에서 조밀하기 때문입니다 — 따라서 각 점  $a + b\sqrt{11}$ 을 좌표  $(a + b\sqrt{11}, a - b\sqrt{11})$ 에 그리도록 하겠습니다. 노름이  $< 1$ 인 점들의 집합은 아래와 같이 그려집니다.



(허수 이차체, 즉 정수  $d$ 에 대한  $\mathbb{Q}(\sqrt{-d})$ 의 경우와 같은) 공 모양 대신, 노름이 1인 점들의 집합은 쌍곡선을 이룹니다.

이 때문에 가장 가까운 점으로 반올림하는 것이 항상 최선의 방법은 아닙니다 — 그럼에도  $(\mathbb{Z}[i]$ 의 경우와 마찬가지로) 전수 조사를 통해  $\frac{a}{b} \in \mathbb{Q}(\sqrt{11})$ 의 모든 값에 대해

$N(\frac{a}{b} - q) < 1$ 을 만족하는  $q \in \mathbb{Z}[\sqrt{11}]$ 이 존재함을 증명할 수 있습니다. 따라서  $N$ 은 유클리드 노름입니다.

<sup>a</sup>이 노름이 왜 자연스러운 것인지에 대한 설명은 [절 54.1](#)를 참고하십시오.

그렇긴 하지만, 유클리드 정역의 자연스러운 노름이 항상 유클리드 노름일 필요는 없습니다.  $\mathbb{Z}[\frac{1+\sqrt{69}}{2}]$ 가 그 첫 번째 예시입니다.

#### 예제 5.7.4 ( $\mathbb{Q}[x]$ 는 유클리드 정역입니다)

마찬가지로  $\mathbb{Q}[x]$ 에서는 노름을 다항식의 차수로 잡을 수 있습니다 — 나머지가 있는 다항식 나눗셈 알고리즘이 gcd의 계산을 처리해 줄 것입니다.

다시 PID 주제로 돌아가겠습니다. 유클리드 정역에서는 임의의 두 원소의 gcd를 계산할 수 있습니다. 그렇다면 무한히 많은 원소들의 모임에 대해서는 어떨까요? 상황이 매우 좋은 것으로 밝혀집니다:

#### 명제 5.7.5

유클리드 정역은 PID입니다.

사실, 무한히 많은 원소들의 모임의 gcd를 계산하는 명시적인 알고리즘을 제시할 필요는 없습니다 — 물론 그러한 알고리즘은 유한한 시간 안에 끝날 수 없습니다! — 다만 gcd가 존재함을 보이기만 하면 되므로, 우회하는 방법을 쓸 수 있습니다.

유클리드 알고리즘에서는 원소들 중 하나가 0이 될 때까지 원소들의 노름이 계속 감소한다는 점에 주목하십시오. 그러므로 임의의 원소들의 모임이 주어졌을 때, 이 원소들이 생성하는 아이디얼을 취하면 — 분명 gcd는 그 아이디얼 안에 있습니다 — 노름이 가장 작은 0이 아닌 원소를 취합니다. 이것이 바로 gcd입니다.

이러한 직관을 염두에 두고, 우리의 증명을 형식화합니다:

증명.  $I$ 를 임의의 아이디얼이라 합시다.  $I$ 가 주 아이디얼임을 보여야 합니다.

$a$ 를  $I$ 에서 노름이 가장 작은 0이 아닌 원소라 합시다 —  $\mathbb{Z}_{\geq 0}$ 이 정렬순서집합이므로 이러한 원소가 존재합니다.

**질문 5.7.6.**  $I$ 의 다른 모든 원소  $b \in I$ 에 대해  $a \mid b$ 임을 보이십시오.

따라서  $I = (a)$ 이며, 증명이 끝났습니다. □

#### 예제 5.7.7 (환 $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ 는 유클리드 정역이 아닙니다)

$R = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ 라 합시다.

위 예를 염두에 두면, 이 환에 대해 무엇을 말할 수 있습니까?

이는 사실 주 아이디얼 정역이지만(여기서는 증명하지 않겠습니다), 사실 이 환에는 유클리드 노름이 존재하지 않습니다.

위 주장을 증명하겠습니다. 전체적인 계획은 다음과 같습니다:

- 유클리드 노름이 존재하면 우리가 **보편 준약수**(universal side divisor)라 부르는 것이 존재함을 보이십시오.

- $R$ 에는 보편 준약수가 존재하지 않음을 보이십시오.
- 따라서  $R$ 은 유클리드 노름을 가질 수 없습니다.

먼저, 위의  $\mathbb{Z}[i]$ 와  $\mathbb{Z}[\omega]$  예시를 살펴봅시다. 단위원들이 노름이 가장 작은 원소들임을 알 수 있습니다.

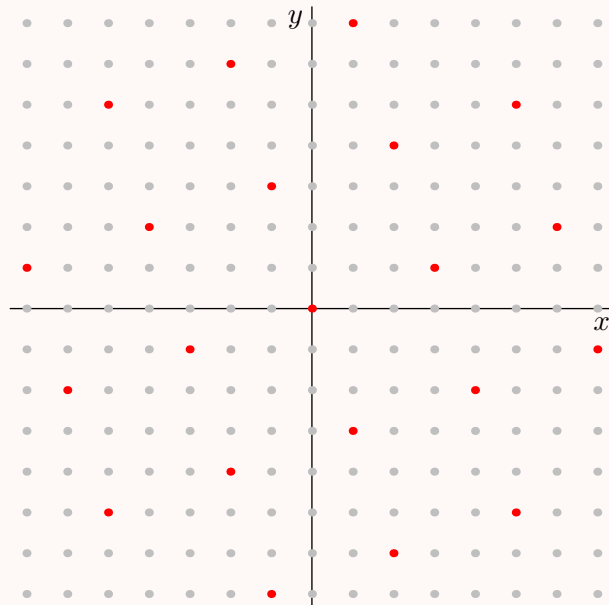
지금까지는 유용한 것이 없습니다 — 모든 환은 단위원 1을 가집니다. 다음으로, 그다음으로 노름이 작은 원소들을 살펴봅시다:

- $\mathbb{Z}[i]$ 에서, 원소  $1 + i$ 는 노름이 2이며, 0도 단위원도 아니면서 노름이 가장 작은 원소입니다. (다른 원소들은  $\pm 1 \pm i$ 입니다.)
- $\mathbb{Z}[\omega]$ 에서, 단위원들은 노름이 1인  $\{\pm 1, \pm \omega, \pm(\omega - 1)\}$ 입니다. 그다음으로 노름이 작은 원소는 노름이 3인  $1 + \omega$ 입니다.

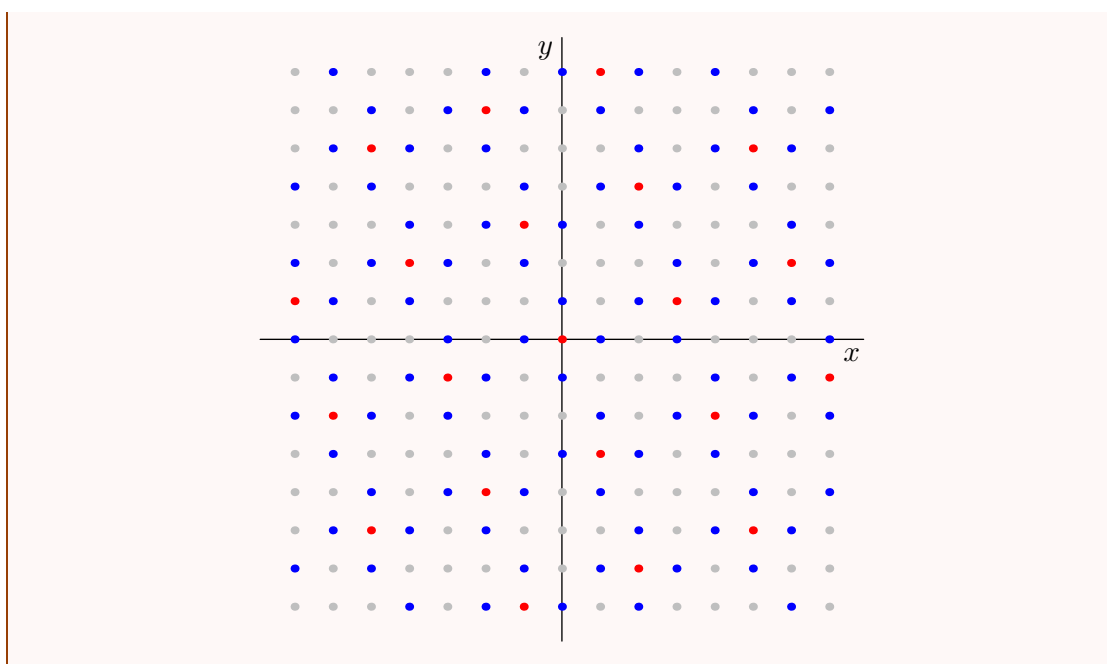
이제 증명을 계속 진행하기 위해, 준약수(side divisor)를 정의해야 합니다.  $a = bq$ 인 어떤  $q$ 가 존재하면  $b$ 가  $a$ 의 약수라는 것을 기억하십시오. 나머지  $a - bq$ 가 0이거나 단위원인 어떤  $q$ 가 존재하면,  $b$ 를  $a$ 의 **준약수**(읽는 법: "거의 약수")라고 합니다.

#### 예제 5.7.8

$\mathbb{Z}[i]$ 에서,  $b = 3 + i$ 를 생각해 봅시다.  $b \mid a$ 를 만족하는 수  $a$ 들의 집합을 아래에 빨간색으로 그렸습니다.



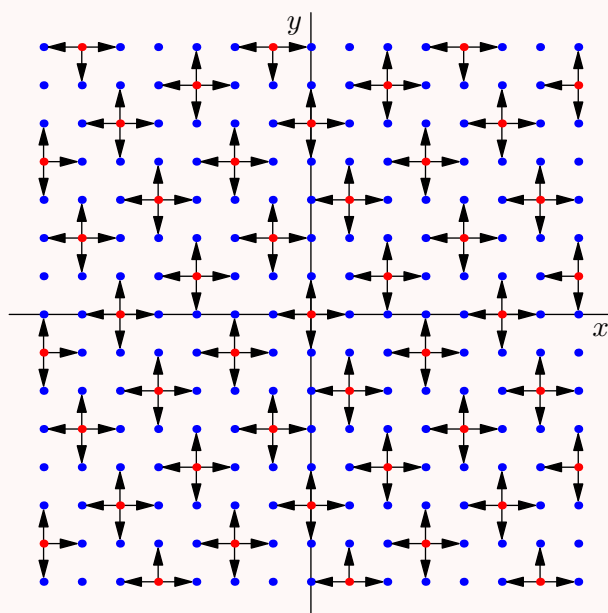
이러한  $a$ 의 값들에 단위원을 더하면,  $b$ 가  $a$ 의 준약수가 되는 수  $a$ 들의 집합을 얻게 되며, 이로써 "거의 약수"라는 개념에 그림을 부여할 수 있습니다.  $b$ 가  $a$ 의 준약수가 되는 점  $a$ 들이 아래에 빨간색과 파란색으로 표시되어 있습니다.



마지막으로, **보편 준약수**란 모든 원소  $a \in R$ 에 대해  $b$ 가 준약수가 되는 수  $b$ 로 정의합니다.

#### 예제 5.7.9

위와 비슷한 그림을 그려 보면,  $\mathbb{Z}[i]$ 에서  $2+i$ 와  $1+i$ 가 준약수임을 알 수 있습니다.



이제, 위에서 살펴본 두 개념 사이의 연관성을 살펴봅시다.

#### 보조정리 5.7.10

유클리드 정역에서, 단원이 아니면서 노름이 가장 작은 0이 아닌 원소  $b$ 는 보편 준제수입니다.

증명. 임의의 수와  $b$  사이에서 유클리드 호제법을 한 단계만 수행하면, 나머지는 0이거나 단원이어야 합니다.  $\square$

그리고 마지막으로,

### 명제 5.7.11

$R$ 에는 보편 준제수가 존재하지 않습니다.

증명. 모든 수는  $\frac{a}{2} + \frac{b\sqrt{-19}}{2}$  형태이며, 여기서  $a$ 와  $b$ 는 홀짝성이 같습니다.  $\frac{a^2}{4} + \frac{19b^2}{4}$ 로 정의되는 복소수의 절댓값은 곱셈적이며,  $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ 의 모든 수에 대해 1보다 크지만,  $-1, 0, 1$ 은 예외로서 각각 절댓값이 1, 0, 1입니다. 이 환에는 절댓값이 0보다 크고 1보다 작은 수가 존재하지 않으므로, 절댓값이 1보다 큰 환의 모든 수는 환 안에서 곱셈에 대한 역원을 갖지 않습니다. 따라서 단원은 1과  $-1$ 뿐입니다.

환의 모든 원소에  $x$ 를 곱하면, 복소평면에서 원소 쌍 사이의 거리는  $|x|$ 배가 됩니다. 처음에 원소 쌍 사이의 거리는 최소 1이었습니니다.

- $x$ 가 실수이고  $|x| \geq 2$ 이면,  $xR$ 은  $a + \frac{\sqrt{-19}}{2}$  형태의 원소를 전혀 포함하지 않으므로,  $x$ 는 보편 준제수가 아닙니다.
- $x$ 가 실수가 아니고  $|x| \geq 2$ 이면,  $xR$ 의 원소가 실수가 되려면 곱해지기 전 원소가 실수가 아니었어야 합니다. 이는  $xR$ 에서 실수축 위에 있는 원소들의 절댓값이 최소  $2|\frac{1+\sqrt{-19}}{2}| = 2\sqrt{5} \geq 4$ 임을 의미합니다. 따라서  $x$ 는 2의 준제수가 아니므로,  $x$ 는 보편 준제수가 아닙니다.

$R$ 은 보편 준제수를 갖지 않으므로,  $R$ 은 유클리드 정역이 아닙니다.  $\square$

## §5.8 생각해 볼 만한 조금 더 어려운 문제

올림피아드 문제는 아니지만, 그 취지는 올림피아드에서 볼 법한 것과 매우 유사합니다.

문제 5A. 다음 환을 생각해 봅시다

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

이것은 체입니까?

문제 5B (체로부터의 준동형사상은 단사입니다).  $K$ 를 체,  $R$ 을 자명하지 않은 환이라 합시다. 임의의 준동형사상  $\psi: K \rightarrow R$ 이 단사임을 증명하십시오.<sup>2</sup>

문제 5C\* (소 아이디얼의 원상).  $\phi: R \rightarrow S$ 가 환 준동형사상이고,  $I \subseteq S$ 가 소 아이디얼이라고 합시다.  $\phi^{\text{pre}}(I)$  또한 소 아이디얼임을 증명하십시오.



문제 5D\*.  $R$ 을 원소가 유한 개인 정역이라 합시다.  $R$ 이 체임을 증명하십시오.

문제 5E\* (크룰 정리).  $R$ 을 환,  $J$ 를 진 아이디얼이라 하겠습니다.

(a)  $R$ 이 뇌터 환이면  $J$ 가 극대 아이디얼  $I$ 에 포함됨을 증명하십시오.

(b)  $R$ 이 뇌터 환이 아니더라도 이 결과를 증명하기 위해 초른의 보조정리(장 88)를 사용하십시오.

<sup>2</sup> $\psi(1_K) = 1_R$ 을 요구하기 때문에, 우리에게  $\psi$ 는 영사상이 될 수 없다는 점에 유의하십시오. 문헌에서는 때때로 다른 서술을 찾아볼 수 있습니다.

**문제 5F** ( $\text{Spec } k[x]$ ).  $\mathbb{C}[x]$ 와  $\mathbb{R}[x]$ 의 소 아이디얼을 설명하십시오.

**문제 5G<sup>†</sup>**.  $\mathbb{Z}[\sqrt{2017}]$ 의 소 아이디얼 중 극대 아이디얼이 아닌 것은 몇 개입니까?

**문제 5H**.  $R$ 을 유리수  $q$  중에서,  $q$ 를 기약분수로 나타냈을 때 분모가 5의 배수가 아닌 것들의 집합이라 하겠습니다. 그러면  $R$ 은 (보통의 덧셈과 곱셈에 대해) 환입니다.  $R$ 의 모든 아이디얼을 분류하십시오. 이 아이디얼들 중 어느 것이 소 아이디얼/극대 아이디얼입니까?

**문제 5I**. **문제 4H**에서 환  $R$ 이 **하강 사슬 조건**을 만족시키면 **아르틴**이라 함을 상기하십시오. 즉, 아이디얼의 무한 하강 사슬은 존재하지 않습니다:  $I_1 \supsetneq I_2 \supsetneq I_3 \supsetneq \dots$ .

(a)  $R$ 이 아르틴이고 정역이면 체임을 보이십시오.

(b) 더 일반적으로, 아르틴 환의 모든 소 아이디얼이 극대 아이디얼임을 보이십시오.



# III

## 기본 위상수학

## 제III부: 목차

---

|          |                                           |            |
|----------|-------------------------------------------|------------|
| <b>6</b> | <b>거리 공간의 성질</b>                          | <b>109</b> |
| 6.1      | 유계성 . . . . .                             | 109        |
| 6.2      | 완비성 . . . . .                             | 110        |
| 6.3      | 구매자는 조심하십시오 . . . . .                     | 111        |
| 6.4      | 부분공간, 그리고 (미리 말해두는) 헛갈리는 언어적 요점 . . . . . | 112        |
| 6.5      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .            | 113        |
| <br>     |                                           |            |
| <b>7</b> | <b>위상 공간</b>                              | <b>115</b> |
| 7.1      | 거리를 잊기 . . . . .                          | 115        |
| 7.2      | 재정의 . . . . .                             | 116        |
| 7.3      | 하우스도르프 공간 . . . . .                       | 117        |
| 7.4      | 부분공간 . . . . .                            | 118        |
| 7.5      | 연결 공간 . . . . .                           | 118        |
| 7.6      | 경로 연결 공간 . . . . .                        | 119        |
| 7.7      | 호모토피와 단순 연결 공간 . . . . .                  | 120        |
| 7.8      | 공간의 기저 . . . . .                          | 122        |
| 7.9      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .            | 122        |
| <br>     |                                           |            |
| <b>8</b> | <b>콤팩트성</b>                               | <b>125</b> |
| 8.1      | 접렬 콤팩트성의 정의 . . . . .                     | 125        |
| 8.2      | 콤팩트성의 판정 기준 . . . . .                     | 126        |
| 8.3      | 열린 덮개를 이용한 콤팩트성 . . . . .                 | 127        |
| 8.4      | 콤팩트성의 응용 . . . . .                        | 129        |
| 8.5      | (선택) 콤팩트성 정의들의 동치성 . . . . .              | 131        |
| 8.6      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .            | 132        |

---

# 6 거리 공간의 성질

거리 공간에 관한 지난 장의 마지막에서, 우리는 “열린”과 “닫힌”이라는 두 형용사를 소개했습니다. 이것들이 중요한 이유는, 거리 공간을 졸업하고 나면 일반적인 위상 공간의 정의로 성장하게 되기 때문입니다.

앞으로 나아가기 위해, 모(母) 공간에 상대적인 하나의 집합이 아니라 거리 공간 전체에 적용되는 몇 가지 좋은 성질을 나타내는 형용사를 제공할 것입니다. 그것은 “(전) 유계”와 “완비”입니다. 이 형용사들은 거리 공간에 특유한 것이지만, 콤팩트성이라는 개념으로 성장하게 되는데, 이는 [Pu02]의 표현을 빌리면 “실해석학에서 단연 가장 중요한 개념”입니다. 이 장의 끝에 이르면, 우리는 위상동형사상의 정의에 뭔가 미심쩍은 부분이 있음을 깨달을 만큼 충분히 알게 될 것이며, 이것이 완전히 일반적인 위상 공간을 정의하게 될 다음 장의 출발점 역할을 하게 됩니다.

## §6.1 유계성

**이 절의 대표적인 예:**  $[0, 1]$ 은 유계이지만  $\mathbb{R}$ 은 그렇지 않습니다.

다음은 거리 공간이 지나치게 커지는 것을 막는 하나의 개념입니다.

**정의 6.1.1.** 거리 공간  $M$ 은,  $d(p, q) \leq D$ 가 모든  $p, q \in M$ 에 대해 성립하는 상수  $D$ 가 존재하면 **유계**라고 합니다.

한정사의 순서를 바꿀 수도 있습니다:

### 명제 6.1.2 (지름 대신 반지름을 이용한 유계성)

거리 공간  $M$ 이 유계인 것은, 모든 점  $p \in M$ 에 대해 (아마도  $p$ 에 따라 달라질 수 있는) 반지름  $R$ 이 존재하여 모든  $q \in M$ 에 대해  $d(p, q) \leq R$ 이 성립하는 것과 동치입니다.

**연습문제 6.1.3.** 삼각부등식을 이용하여 이것들이 동치임을 보이십시오. (“반지름”과 “지름”이라는 이름이 큰 힌트입니다!)

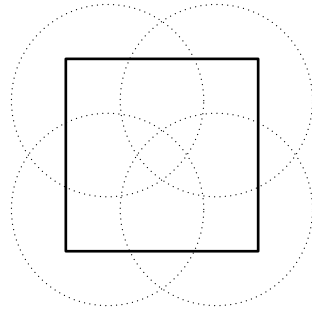
### 예제 6.1.4 (유계 공간의 예)

- (a)  $[0, 1]$ 이나  $(a, b)$ 와 같은 유한 구간은 유계입니다.
- (b) 단위 정사각형  $[0, 1]^2$ 은 유계입니다.
- (c)  $\mathbb{R}^n$ 은 어떤  $n \geq 1$ 에 대해서도 유계가 아닙니다.
- (d) 무한 집합 위의 이산 공간은 유계입니다.
- (e)  $\mathbb{N}$ 은 이산 공간과 위상동형임에도 불구하고 유계가 아닙니다!

무한 집합 위의 이산 공간이 “유계”라는 사실이 당신을 불편하게 만들 수도 있으므로, 여기 사용할 수 있는 다소 더 강한 조건을 소개합니다:

**정의 6.1.5.** 거리 공간이, 임의의  $\varepsilon > 0$ 에 대해 유한히 많은  $\varepsilon$ -근방들로  $M$ 을 덮을 수 있으면 **전유계**라고 합니다.

예를 들어,  $\varepsilon = 1/2$ 이면  $[0, 1]^2$ 을  $\varepsilon$ -근방들로 덮을 수 있습니다.



**연습문제 6.1.6.** “전유계”가 “유계”를 함의함을 보이십시오.

### 예제 6.1.7 (전유계 공간의 예)

(a)  $\mathbb{R}^n$ 의 부분집합이 유계인 것은 그것이 전유계인 것과 동치입니다.

이는 유클리드 기하학적인 이유 때문입니다: 예를 들어  $\mathbb{R}^2$ 에서 반지름 2인 원판 하나로 어떤 집합을 덮을 수 있다면, 반지름 1/2인 유한히 많은 원판들로도 분명히 덮을 수 있습니다. (이것을 엄밀하게 증명하지는 않겠습니다.)

(b) 그래서 예를 들어  $[0, 1]$ 이나  $[0, 2] \times [0, 3]$ 은 전유계입니다.

(c) 반면, 무한 집합 위의 이산 공간은 전유계가 아닙니다.

## §6.2 완비성

**이 절의 대표적인 예:**  $\mathbb{R}$ 은 완비이지만,  $\mathbb{Q}$ 와  $(0, 1)$ 은 그렇지 않습니다.

지금까지는 극한을 가지는 경우에만 수열이 수렴한다고 말할 수 있었습니다. 하지만 다음 수열을 생각해봅시다

$$x_1 = 1, x_2 = 1.4, x_3 = 1.41, x_4 = 1.414, \dots$$

물론 이 수열은  $\mathbb{R}$ 에서  $\sqrt{2}$ 로 수렴합니다. 하지만  $\mathbb{Q}$ 에서는 수렴하지 못합니다. 이 수열이 수렴하는 유리수는 존재하지 않습니다. 그러니 만약 우리가  $\mathbb{R}$ 의 존재를 몰랐다면, 어떤지 수열  $(x_n)$ 이 무언가로 “다가가고” 있다는 것을 전혀 알 수 없었을 것입니다.

그것은 아쉬운 일인 것 같습니다. 항들이 공간 안의 어떤 특정한 점으로 다가가지 않더라도, 항들끼리 서로 가까워지는 이런 수열들을 기술하기 위한 새로운 정의를 세워봅시다. 따라서 우리는 정의에서 주어진 점들만을 언급하고자 합니다.

**정의 6.2.1.**  $x_1, x_2, \dots$ 를 거리 공간  $M = (M, d_M)$  안에 있는 수열이라고 합시다. 임의의  $\varepsilon > 0$ 에 대해 다음이 성립하면 이 수열을 **코시** 수열이라고 부릅니다

$$d_M(x_m, x_n) < \varepsilon$$

충분히 큰 모든  $m$ 과  $n$ 에 대해.

**질문 6.2.2.** 수렴하는 수열은 자동으로 코시 수열임을 보이십시오. (그림을 그려보십시오.)

이제 다음과 같이 정의할 수 있습니다:

**정의 6.2.3.** 모든 코시 수열이 수렴하면 거리 공간  $M$ 을 **완비**라고 합니다.

**예제 6.2.4 (완비 공간의 예)**

- (a)  $\mathbb{R}$ 은 완비입니다. ( $\mathbb{R}$ 의 정의에 따라, 이는 정의에 의해 바로 성립하거나 약간의 작업이 필요합니다. 여기서는 이를 다루지 않겠습니다.)
- (b) 이산 공간은 완비입니다. 유일한 코시 수열은 결국 상수 수열이기 때문입니다.
- (c) 닫힌 구간  $[0, 1]$ 은 완비입니다.
- (d)  $\mathbb{R}^n$  또한 완비입니다. ( $n$ 에 대한 귀납법으로 이를 증명해보셔도 좋습니다.)

**예제 6.2.5 (완비 공간이 아닌 예)**

- (a) 유리수  $\mathbb{Q}$ 는 완비가 아닙니다.
- (b) 열린 구간  $(0, 1)$ 은 완비가 아닙니다. 수열  $0.9, 0.99, 0.999, 0.9999, \dots$ 는 코시 수열이지만 수렴하지 않기 때문입니다.

그러므로  $\mathbb{Q}$ 처럼 거리 공간이 반드시 완비일 필요는 없습니다. 하지만 우리는 분명히 그것들이 완비이기를 바라며, 다음 정리에 비추어 보면 이는 무리한 바람이 아닙니다.

**정리 6.2.6 (완비화)**

모든 거리 공간은 몇몇 점들을 추가함으로써 "완비화"될 수 있습니다. 즉, 완비 공간으로 만들 수 있습니다.

우리는 이 구성을 전혀 필요로 하지 않으므로, 이는 **문제 6C†**로 남겨두겠습니다.

**예제 6.2.7 ( $\mathbb{Q}$ 는  $\mathbb{R}$ 로 완비화됩니다)**

$\mathbb{Q}$ 의 완비화는  $\mathbb{R}$ 입니다.

(사실, 실수에 의존하지 않는 수정된 완비화의 정의를 사용하여, 다른 저자들은 종종 이를  $\mathbb{R}$ 의 정의로 삼기도 합니다.)

## §6.3 구매자는 조심하십시오

이 두 개념 모두에는 뭔가 미심쩍은 점이 있습니다: 둘 다 위상동형사상 하에서 보존되지 않습니다!

**예제 6.3.1 (여기서 뭔가 수상한 일이 벌어지고 있습니다)**

$M = (0, 1)$ 이고  $N = \mathbb{R}$ 이라고 합시다. 훨씬 앞서 보았듯이  $M$ 과  $N$ 은 위상동형입니다. 그러나:

- $(0, 1)$ 은 전유계이지만 완비는 아닙니다.
- $\mathbb{R}$ 은 완비이지만 유계는 아닙니다.

이는 거리에 뭔가 잘못되어 가고 있다는 첫 번째 힌트입니다. 위상수학 공부를 더 진행해

나가면서, 사실 (거리를 이용해 동기를 부여했던) 열린집합과 닫힌집합이야말로 나중에 진정으로 빛을 발할 개념임을 보게 될 것입니다. 열린집합과 닫힌집합에 대한 표준적인 그림이 이해되도록 하기 위해 거리를 먼저 도입할 것을 고집했지만, 결국에는 보조 바퀴를 뺄 때가 옵니다.

## §6.4 부분공간, 그리고 (미리 말해두는) 헛갈리는 언어적 요점

**이 절의 대표적인 예:** 원은  $\mathbb{R}^2$ 의 부분공간으로 얻어집니다.

우리가 예제들에서 이미 암묵적으로 해 왔듯이, 이제 다음과 같이 말하겠습니다:

**정의 6.4.1.** 모든 부분집합  $S \subseteq M$ 은  $M$  위의 거리 함수를 재사용함으로써 그 자체로 하나의 거리 공간이 됩니다. 우리는  $S$ 가  $M$ 의 **부분공간**이라고 말합니다.

예를 들어, 우리는 원  $S^1$ 이 그저  $\mathbb{R}^2$ 의 부분공간임을 보았습니다.

따라서 다음을 구별하는 것이 중요해집니다

- (i) "완비"나 "유계"와 같은 "**절대적**" 형용사는 공간에도 적용될 수 있고, 따라서 (부분 공간을 취함으로써) 공간의 부분집합에도 적용될 수 있으며,
- (ii) "( $M$ 에서) 열려 있다"나 "( $M$ 에서) 닫혀 있다"와 같은 "**상대적**" 형용사는 공간과 관련해서만 의미를 가지지만, 사람들은 종종 부주의하게 이를 생략합니다.

따라서 "[0, 1]은 완비이다"는 의미가 통하며, "[0, 1]은  $\mathbb{R}$ 의 완비 부분집합이다"도 마찬가지로 의미가 통하는데, 우리는 이를 "[0, 1]은  $\mathbb{R}$ 의 완비 부분공간이다"를 뜻하는 것으로 받아들이고 있습니다. 이는 "완비"가 절대적 형용사이기 때문입니다.

그러나 상대적 형용사가 조금 더 주의를 요하는 방식의 몇 가지 예가 여기 있습니다:

- 수열 1, 1.4, 1.41, 1.414, ...를 생각해 봅시다.  $\mathbb{R}$  안의 수열로 보면  $\sqrt{2}$ 로 수렴합니다. 하지만  $\mathbb{Q}$  안의 수열로 보면 이 수열은 수렴하지 않습니다! 마찬가지로, 수열 0.9, 0.99, 0.999, 0.9999는 공간  $(0, 1)$ 에서는 수렴하지 않지만,  $[0, 1]$ 에서는 수렴합니다. 이 수열들이 "마땅히 그래야 함에도" 수렴하지 못한다는 사실은 이상하고 나쁜 것이며, 이것이 바로 우리가 애초에 완비 공간을 정의한 이유였습니다.
- 일반적으로, "[0, 1]은 열려 있는가?"와 같은 질문을 던지는 것은 의미가 없습니다. 그러나 "[0, 1]은  $\mathbb{R}$ 에서 열려 있는가?"와 "[0, 1]은  $[0, 1]$ 에서 열려 있는가?"라는 질문은 의미가 통합니다. 첫 번째 질문에 대한 답은 "아니오"이지만 두 번째 질문에 대한 답은 "예"입니다; 실제로, 모든 공간은 그 자신 안에서 열려 있습니다. 마찬가지로,  $[0, \frac{1}{2})$ 는 공간  $M = [0, 1]$ 에서 열린집합 인데, 이는 그것이  $M$  안에서 0을 중심으로 하는 반지름  $\frac{1}{2}$ 의 공입니다.
- 쌍대적으로, "[0, 1]은 닫혀 있는가?"라고 묻는 것도 의미가 없습니다. 그것은  $\mathbb{R}$ 에서 그리고 그 자신 안에서 닫혀 있습니다(하지만 어차피 모든 공간은 그 자신 안에서 닫혀 있습니다).

위 내용을 제대로 이해했는지 확인하기 위해, 상대적 형용사를 연습해 볼 수 있는 두 가지 연습문제가 여기 있습니다.

**연습문제 6.4.2.**  $M$ 을 완비 거리 공간이라 하고  $S \subseteq M$ 이라고 합시다.  $S$ 가 완비인 것과  $S$ 가  $M$ 에서 닫혀 있는 것이 동치임을 증명하십시오. 특히,  $[0, 1]$ 은 완비입니다.

**연습문제 6.4.3.**  $M = [0, 1] \cup (2, 3)$ 이라 합시다.  $[0, 1]$ 과  $(2, 3)$ 이  $M$ 에서 모두 열려 있으면서 닫혀 있음을 보이십시오.

이는 세 번째 요점을 보여줍니다: 자명하지 않은 집합이 열려 있으면서 동시에 닫혀 있을 수 있습니다.<sup>1</sup> **장 7**에서 보게 되듯이, 이는 공간이 비연결임을 함의합니다. 즉, 위에서 든 예와 상당히 비슷한 경우들만 존재합니다.

## §6.5 생각해 볼 만한 조금 더 어려운 문제

**문제 6A<sup>†</sup>** (바나흐 부동점 정리).  $M = (M, d)$ 를 완비 거리 공간이라 합시다.  $T: M \rightarrow M$ 이 다음과 같은 연속 사상이라고 가정합시다. 즉, 임의의  $p, q \in M$ 에 대해,

$$d(T(p), T(q)) \leq 0.999d(p, q).$$

( $T$ 를 **축약사상**이라 부릅니다.)  $T$ 가 유일한 부동점을 가짐을 보이십시오.

**문제 6B** (Henning Makhholm, [math.SE](https://math.stackexchange.com)에서).  $\mathbb{R}$ 에 다음 두 거리를 부여하여 얻은 거리 공간을 각각  $M$ 과  $N$ 이라 합시다:

$$\begin{aligned} d_M(x, y) &= \min \{1, |x - y|\} \\ d_N(x, y) &= |e^x - e^y|. \end{aligned}$$

(a) 다음  $2 \times 3$  표의 각 칸을 "예" 또는 "아니오"로 채우십시오.

|     | 완비인가? | 유계입니까? | 전유계입니까? |
|-----|-------|--------|---------|
| $M$ |       |        |         |
| $N$ |       |        |         |

(b)  $M$ 과  $N$ 은 위상동형입니까?



**문제 6C<sup>†</sup>** (거리 공간의 완비화).  $M$ 을 거리 공간이라 합시다.  $M$ 이  $\overline{M}$ 의 부분공간이 되고,  $\overline{M}$ 의 공집합이 아닌 모든 열린집합이  $M$ 의 점을 포함하도록(즉  $M$ 이  $\overline{M}$ 에서 **조밀**하도록) 완비 거리 공간  $\overline{M}$ 을 구성하십시오.

**문제 6D.** 거리 공간이 전유계인 것과 임의의 수열이 코시 부분수열을 가지는 것이 동치임을 보이십시오.



**문제 6E.**  $\mathbb{Q}$ 가 어떤 완비 거리 공간과도 위상동형이 아님을 증명하십시오.

<sup>1</sup>언제나 놀림받는 사실입니다.



# 7 위상 공간

장 2에서 우리는 공간 위에 거리를 정의함으로써 공간이라는 개념을 소개했습니다. 이는 여러분에게 많은 예시와 좋은 직관을 제공하며, 열린집합과 닫힌집합의 그림을 어떻게 그려야 하는지 알려줍니다.

하지만 앞으로 나아가면서, 위상 공간을 오직 그것의 열린집합만으로 생각하기 시작하는 것이 유용할 것입니다. (한 가지 동기는, 우리의 수상쩍은 예제 6.3.1가 어떤 면에서는 위상 동형사상 개념이 실제로는 거리가 아니라 열린집합의 관점에서 서술되기를 원한다는 것을 보여준다는 점입니다.) 앞으로 보게 되겠지만, 열린집합은 우리가 필요로 하는 정보의 거의 전부를 실제로 유지하면서도 더 단순합니다.<sup>1</sup> 이는 단 몇 개의 절에서 이루어질 것이며, 그 후 우리는 위상 공간(따라서 거리 공간)에 적용할 수 있는 더 많은 형용사들을 서술하기 시작할 것입니다.

이 장에는 가장 중요한 위상 개념이 빠져 있습니다: 바로 콤팩트 공간이라는 개념입니다. 이는 너무나 중요해서 저는 이를 위해 별도의 장을 하나 할애했습니다.

관심 있는 분들을 위한 간단한 참고 사항: "하우스도르프", "연결", 그리고 나중에 나올 "콤팩트"라는 형용사들은 모두 절대 형용사입니다.

## §7.1 거리를 잊기

정리 2.6.11을 상기해 봅시다:

거리 공간 사이의 함수  $f: M \rightarrow N$ 이 연속이라는 것은  $N$ 의 모든 열린집합의 원상이  $M$ 에서 열려 있다는 것과 동치입니다.

우리가 이를 거리 공간이라는 맥락에서 정의했음에도 불구하고, 이는 흥미롭게도 거리를 전혀 언급하지 않고 오직 열린집합만을 언급합니다. 이 장의 시작 부분에서 암시했듯이, 이는 우리가 애초에 거리를 가지고 있었다는 사실을 어떻게 잊어버리고, 대신 열린집합에서부터 시작할 수 있는지에 대한 훌륭한 동기가 됩니다.

**정의 7.1.1. 위상 공간**은 순서쌍  $(X, \mathcal{T})$ 이며, 여기서  $X$ 는 점들의 집합이고,  $\mathcal{T}$ 는 **위상**으로서  $X$ 의 여러 부분집합들로 이루어져 있으며, 이들은  $X$ 의 **열린집합**이라고 불립니다. 위상은 다음 공리들을 만족해야 합니다.

- $\emptyset$ 과  $X$ 는 모두  $\mathcal{T}$ 에 속합니다.
- 열린집합들의 유한 교집합도  $\mathcal{T}$ 에 속합니다.
- 열린집합들의 임의의 (아마도 무한한) 합집합도  $\mathcal{T}$ 에 속합니다.

그래서 이번에는 열린집합이 주어집니다. 거리를 정의하고 그 거리로부터 열린집합을 얻는 대신, 우리는 오직 열린집합에서부터 시작합니다.

**표기의 남용 7.1.2.** 우리는  $(X, \mathcal{T})$ 를 그냥  $X$ 로 줄여 쓰며, 위상  $\mathcal{T}$ 는 암묵적으로 남겨둡니다. (여기서 어떤 패턴이 보이십니까?)

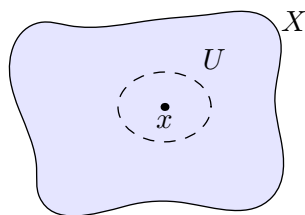
<sup>1</sup>제가 거리 공간을 먼저 고집스럽게 소개하는 이유는, 그렇지 않으면 예시들이 훨씬 덜 이해될 것이라고 생각하기 때문입니다.

**예제 7.1.3** (위상의 예시)

- (a) 거리 공간  $M$ 이 주어지면, 우리는  $\mathcal{T}$ 를 거리적 의미에서의 열린집합들로 둘 수 있습니다. 요점은 공리들이 만족된다는 것입니다.
- (b) 특히, **이산 공간**은 모든 집합이 열려 있는 위상 공간입니다. (왜 그럴까요?)
- (c)  $X$ 가 주어지면, 우리는  $\mathcal{T} = \{\emptyset, X\}$ 로 둘 수 있으며, 이는 이산 공간과 정반대의 극단입니다.

이제 우리는 거리에 대한 정의들을 옮겨올 수 있습니다.

**정의 7.1.4.** 점  $x \in X$ 의 **열린 근방**<sup>2</sup>은  $x$ 를 포함하는 열린집합  $U$ 입니다 (그림 참조).



**표기의 남용 7.1.5.** 완전히 명확히 하자면: "열린 근방"이라고 할 때 저는  $x$ 를 포함하는 임의의 열린집합을 의미합니다. 하지만 " $r$ -근방"이라고 할 때 저는 항상  $x$ 로부터 거리가  $r$ 보다 작은 점들을 의미하며, 따라서 이 용어는 제 공간이 거리 공간일 때만 사용할 수 있습니다.

## §7.2 재정의

이제 우리가 위상 공간을 정의했으므로, 거의 모든 거리 개념들에 대해 오직 열린집합만을 필요로 하는 정의를 적어낼 수 있습니다 (이는 물론 우리가 거리 공간을 다룰 때 기존의 정의들과 일치할 것입니다).

### §7.2.i 연속성

우리의 동기가 된 예시는 연속성이었습니다:

**정의 7.2.1.** 위상 공간  $f: X \rightarrow Y$ 가 점  $p \in X$ 에서 **연속**이라는 것은  $f(p)$ 의 임의의 열린 근방의 원상이  $p$ 의 열린 근방을 포함할 때를 말합니다. 함수가 모든 점에서 연속이면 그 함수는 연속입니다.

따라서 동형사상의 개념도 옮겨집니다: 양방향으로 연속인 전단사입니다.

**정의 7.2.2.** 위상 공간  $(X, \tau_X)$ 와  $(Y, \tau_Y)$ 의 **동형사상**(homeomorphism)이란  $\tau_X$ 에서  $\tau_Y$ 로의 전단사를 유도하는 전단사  $f: X \rightarrow Y$ 입니다: 즉 이 전단사가 열린집합을 보존합니다.

**질문 7.2.3.** 이것이  $f$ 와 그 역함수가 둘 다 연속인 것과 동치임을 보이십시오.

따라서 열린집합만으로 정의된 성질은 모두 동형사상에 의해 보존됩니다. 이러한 성질을 **위상적 성질**(topological property)이라고 부릅니다. 이후 우리가 정의할 형용사들("연결"(connected), "하우스도르프"(Hausdorff), "콤팩트"(compact))은 모두 열린집합만으로 정의될 것이므로, 위상적 성질이 될 것입니다.

<sup>2</sup>문헌에서 "근방"은  $x$  주위의 어떤 열린집합을 포함하는 집합을 가리킵니다. 우리는 이 용어를 사용하지 않고, 오로지 "열린 근방"만을 사용하겠습니다.

### §7.2.ii 닫힌집합

지난 시간에 닫힌집합에 대한 동치인 두 정의가 있음을 보았는데, 그중 하나는 오직 열린집합에만 의존하며, 우리는 그것을 사용합니다:

**정의 7.2.4.** 일반적인 위상 공간  $X$ 에서,  $S \subseteq X$ 가  $X$ 에서 **닫혀 있다**(closed)고 하는 것은 여집합  $X \setminus S$ 가  $X$ 에서 열려 있을 때를 말합니다.

$S \subseteq X$ 가 임의의 집합일 때,  $S$ 의 **폐포**(closure),  $\bar{S}$ 로 표기하는 것은  $S$ 를 포함하는 가장 작은 닫힌집합으로 정의됩니다.

따라서 일반적인 위상 공간에서 열린집합과 닫힌집합은 같은 정보를 담고 있으며, 모든 것을 열린집합으로 정의하든 닫힌집합으로 정의하든 전적으로 취향의 문제입니다. 특히 열린집합의 공리와 성질들을 닫힌집합의 것으로 옮길 수 있습니다:

**질문 7.2.5.** 닫힌집합들의 (무한할 수도 있는) 교집합은 닫혀 있는 반면, 유한 개의 닫힌집합들의 합집합도 닫혀 있음을 보이십시오. (여집합을 살펴보십시오.)

**연습문제 7.2.6.** 함수가 연속인 것과 모든 닫힌집합의 원상이 닫혀 있는 것이 동치임을 보이십시오.

수학자들은 열린집합을 더 좋아하기로 합의한 듯합니다.

### §7.2.iii 옮겨지지 않는 성질들

모든 것이 통하지는 않습니다:

**비고 7.2.7 (완비성과 (전)유계성은 거리 공간의 성질입니다)** — 우리가 살펴본 두 가지 거리 공간의 성질, “완비”(complete)와 “(전)유계”(totally bounded)는 위상적 성질이 아닙니다. 이것들은 거리에 의존하므로, 쓰인 그대로는 위상 공간에 적용할 수 없습니다. 어쩌면 (“연속 함수”에서 본 것처럼) 순전히 열린집합에 기반한 대체 정의가 있지 않을까 기대할 수도 있습니다. 하지만  $(0, 1) \cong \mathbb{R}$ 임을 보이는 **예제 6.3.1**는 그것이 가망 없음을 말해줍니다.

**비고 7.2.8 (수열은 잘 통하지 않습니다)** — 수열과 수렴하는 수열의 개념도 옮겨보려 시도할 수 있을 것입니다. 그러나 이는 여러 바람직한 성질들을 깨뜨리는 것으로 드러납니다. 따라서 저는 굳이 그렇게 하지 않을 것이며, 수열에 대해 논의할 때는 우리가 거리 공간을 다루고 있다고 가정해야 합니다.

## §7.3 하우스도르프 공간

**이 절의 대표적인 예:** 자리스키 위상(훨씬 나중에 정의됨)이 아닌 모든 공간.

예상하셨을 수도 있듯이, 거리 공간으로 실현될 수 없는(다시 말해, **거리화 가능**(metrizable)하지 않은) 위상 공간이 존재합니다. 한 예는 그저  $X = \{a, b, c\}$ 와 위상  $\tau_X = \{\emptyset, \{a, b, c\}\}$ 를 취하는 것입니다. 이 위상은 상당히 “어리석습니다”: 점  $a, b, c$  중 어느 것도 구별할 수 없습니다! 하지만 어떤 거리 공간이든 그 점들을 구별할 수 있습니다 ( $x \neq y$ 일 때  $d(x, y) > 0$ 이기 때문입니다).

덜 사소한 예들은 나중에 살펴보겠지만, 지금은 우리의 공간에 약간의 건전성 조건을 더 추가하고자 합니다. 정수  $n$ 에 대해  $T_n$ 이라 표기되는 (여기서  $n = 0$ 이 가장 약하고  $n = 6$

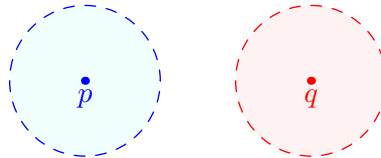
이 가장 강한) 이러한 공리들의 전체 위계가 있습니다; 이 공리들을 **분리 공리**(separation axioms)라고 부릅니다.

단연 가장 흔한 가정은  $T_2$  공리이며, 이는 특별한 이름을 갖고 있습니다.

**정의 7.3.1.** 위상 공간  $X$ 의 서로 다른 두 점  $p, q$ 에 대해,  $p$ 의 열린 근방  $U$ 와  $q$ 의 열린 근방  $V$ 가 존재하여 다음을 만족할 때,  $X$ 를 **하우스도르프** 공간이라고 합니다.

$$U \cap V = \emptyset.$$

다시 말해, 서로 다른 임의의 두 점 주위에 서로소인 열린 근방을 그릴 수 있어야 합니다. 위 내용에 맞는 그림이 여기 있지만, 별다른 내용은 없습니다.



**질문 7.3.2.** 모든 거리 공간이 하우스도르프임을 보이십시오.

나중에 이 단어를 사용할 수 있도록 여기서 정의해 두고자 합니다. 어쨌든, 자리스키 위상을 제외하면 우리가 마주칠 거의 모든 공간은 하우스도르프입니다.

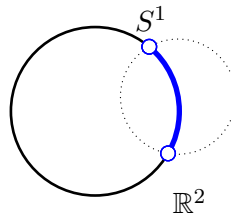
## §7.4 부분공간

**이 절의 대표적인 예:**  $S^1$ 은  $\mathbb{R}^2$ 의 부분공간입니다.

일반적인 위상 공간에 대해서도 부분공간을 취할 수 있습니다.

**정의 7.4.1.** 위상 공간  $X$ 와 부분집합  $S \subseteq X$ 가 주어졌을 때,  $S$ 의 열린 부분집합을 열린집합  $U \subseteq X$ 에 대한  $U \cap S$ 로 선언함으로써  $S$ 를 위상 공간으로 만들 수 있습니다. 이를 **부분공간 위상**이라고 합니다.

예를 들어  $S^1$ 을  $\mathbb{R}^2$ 의 부분공간으로 볼 경우, 임의의 열린 호는 열린집합이 되는데, 이는 그것을 열린 원판과  $S^1$ 의 교집합으로 볼 수 있기 때문입니다.



말할 필요도 없이, 거리 공간의 경우 이 정의들 중 어느 것을 선택하든 상관없습니다. (이를 증명하는 것은 뜻밖에 상당히 번거로운 일이므로, 여기서는 하지 않겠습니다.)

## §7.5 연결 공간

**이 절의 대표적인 예:**  $[0, 1] \cup [2, 3]$ 은 비연결입니다.

거리 공간에서도 하나의 집합이 열려 있으면서 동시에 닫혀 있을 수 있습니다.

**정의 7.5.1.** 위상 공간  $X$ 의 부분집합  $S$ 가  $X$ 에서 닫혀 있으면서 동시에 열려 있을 때,  $S$ 를 **닫힌열린집합**이라고 합니다. (동치로,  $S$ 와 그 여집합이 모두 열려 있다는 것입니다.)

예를 들어  $\emptyset$ 과 전체 공간은 닫힌열린집합의 예입니다. 사실, 이 둘 이외의 자명하지 않은 닫힌열린집합이 존재하면 이른바 비연결 공간이 됩니다.

**질문 7.5.2.** 공간  $X$ 가 자명하지 않은 닫힌열린집합( $\emptyset$ 과  $X$ 가 아닌 것)을 가지는 것과,  $X$ 가 두 개의 공집합이 아닌 열린집합의 서로소 합집합으로 쓸 수 있는 것이 동치임을 보이십시오.

자명하지 않은 닫힌열린집합이 존재하면  $X$ 가 **비연결**이라고 하고, 그렇지 않으면 **연결**이라고 합니다. 이것이 왜 타당한 정의인지 알아보려면, **문제 7A†**를 풀어보는 것이 도움이 될 것입니다.

### 예제 7.5.3 (비연결 공간과 연결 공간)

(a) 거리 공간

$$\{(x, y) \mid x^2 + y^2 \leq 1\} \cup \{(x, y) \mid (x - 4)^2 + y^2 \leq 1\} \subseteq \mathbb{R}^2$$

은 비연결입니다 (두 개의 원판으로 이루어져 있습니다).

(b) 공간  $[0, 1] \cup [2, 3]$ 은 비연결입니다: 이는 각각이 닫힌열린집합인 두 개의 선분으로 이루어져 있습니다.

(c) 두 개 이상의 점을 가진 이산 공간은 비연결인데, 이산 공간에서는 모든 집합이 닫힌열린집합이기 때문입니다.

(d) 다음 집합이

$$\{x \in \mathbb{Q} \mid x^2 < 2014\}$$

$\mathbb{Q}$ 의 닫힌열린 부분집합임을 스스로 확인해 보십시오. 따라서  $\mathbb{Q}$  역시 비연결입니다 – 틈이 있기 때문입니다.

(e)  $[0, 1]$ 은 연결되어 있습니다.

## §7.6 경로 연결 공간

**이 절의 대표적인 예:**  $\mathbb{C}$ 에서 돌아다니기.

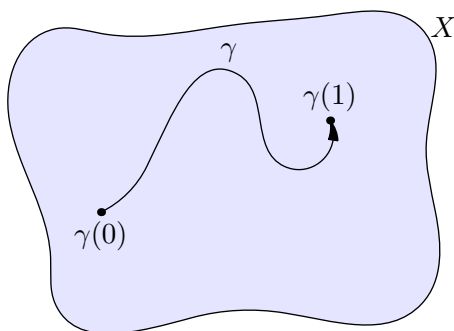
연결 공간이라는 개념보다 더 강력하고 아마도 더 직관적인 개념은 경로 연결 공간입니다. 짧게 설명하자면: "공간 안을 걸어 다니기"입니다.

**정의 7.6.1.** 공간  $X$ 에서의 **경로**란 다음과 같은 연속 함수입니다

$$\gamma: [0, 1] \rightarrow X.$$

이 경로의 **끝점**은 두 점  $\gamma(0)$ 과  $\gamma(1)$ 입니다.

$[0, 1]$ 을 "시간"을 재는 것으로 생각할 수 있으므로,  $t \in [0, 1]$ 에 대해  $\gamma(t)$ 라고 자주 쓰겠습니다 ( $t$ 가 "시간"을 나타냅니다). 다음은 경로를 나타낸 그림입니다.



**질문 7.6.2.** 이것이 "경로"에 대한 여러분의 직관적인 개념과 왜 일치할까요?

**정의 7.6.3.** 공간  $X$ 의 임의의 두 점이 어떤 경로로 연결되어 있으면,  $X$ 는 **경로 연결**이라고 합니다.

**연습문제 7.6.4** (경로 연결은 연결을 함의함).  $X = U \sqcup V$ 가 비연결 공간이라고 합시다.  $U$ 의 한 점에서  $V$ 의 한 점으로 가는 경로가 없음을 보이십시오. ( $\gamma: [0, 1] \rightarrow X$ 라면  $[0, 1] = \gamma^{\text{pre}}(U) \sqcup \gamma^{\text{pre}}(V)$ 를 얻게 되지만,  $[0, 1]$ 은 연결되어 있습니다.)

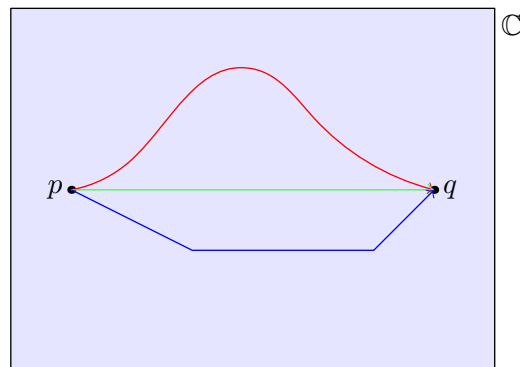
**예제 7.6.5** (경로 연결 공간의 예)

- $\mathbb{R}^2$ 는 경로 연결입니다. 임의의 두 점을 직선으로 "연결"할 수 있기 때문입니다.
- 단위원  $S^1$ 은 경로 연결입니다. 두 점을 연결하는 우호나 열호를 그리기만 하면 되기 때문입니다.

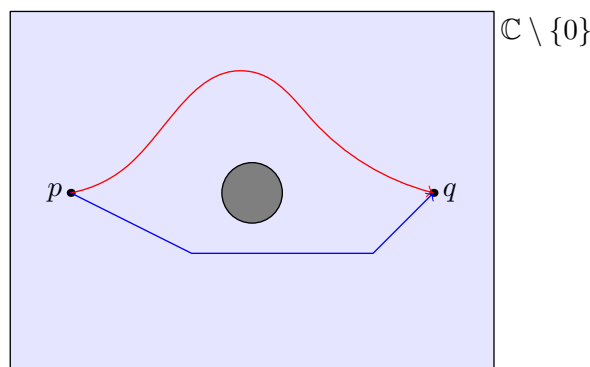
## §7.7 호모토피와 단순 연결 공간

이 절의 대표적인 예:  $\mathbb{C}$ 와  $\mathbb{C} \setminus \{0\}$ .

이제 호모토피라는 개념의 동기를 살펴봅시다. 두 점  $p$ 와  $q$ 가 있는 복소평면  $\mathbb{C}$ (그냥  $\mathbb{R}^2$ 로 생각해도 됩니다)의 예를 생각해 봅시다.  $p$ 에서  $q$ 로 가는 경로는 무수히 많지만, 어쨌든 그것들은 서로 크게 다르지 않습니다. 누군가 여러분에게 "p에서 q로 걸어가십시오"라고 말한다면, 여러분은 그다지 많은 질문을 하지 않을 것입니다.



그렇게 우리가  $\mathbb{C}$ 에서 행복하게 살던 중, 유성이 원점에 떨어져 원점을 소멸시켜 버렸다고 합시다. 그러면 갑자기  $p$ 에서  $q$ 로 가려면, 사람들은 서로 다른 두 가지를 말할지도 모릅니다: "유성 왼쪽으로 도십시오" 또는 "유성 오른쪽으로 도십시오".



그렇다면 무슨 일이 벌어지는 것일까요? 첫 번째 그림에서는 빨간색, 초록색, 파란색 경로가 어쩐지 모두 똑같아 보였습니다. 이들을  $p$ 와  $q$ 에 고정된 고무줄 조각으로 상상해 보면, 각각을 다른 것으로 자유롭게 늘릴 수 있습니다.

하지만 두 번째 그림에서는 빨간 줄을 파란 줄과 일치하도록 옮길 수 없습니다. 유성이 가로막고 있기 때문입니다. 이 경로들은 실제로 서로 다릅니다.<sup>3</sup>

이를 포착하기 위해 사용할 형식적 개념은 호모토피 동치입니다. 우리는 첫 번째 그림에서 세 경로가 모두 호모토픽하지만, 두 번째 그림의 두 경로는 어쩐지 호모토픽하지 않게 되는 정의를 쓰고자 합니다. 그리고 그 아이디어는 단지 연속적인 변형입니다.

**정의 7.7.1.**  $\alpha$ 와  $\beta$ 를  $X$ 에서의 경로로서 끝점이 서로 일치한다고 합시다.  $\alpha$ 에서  $\beta$ 로 가는 (경로) **호모토피**란 연속 함수  $F: [0, 1]^2 \rightarrow X$ 로서,  $s, t \in [0, 1]$ 에 대해  $F_s(t)$ 라고 쓰며, 다음을 만족합니다

$$F_0(t) = \alpha(t) \text{ 그리고 } F_1(t) = \beta(t) \text{ 모든 } t \in [0, 1] \text{에 대하여}$$

그리고 나아가

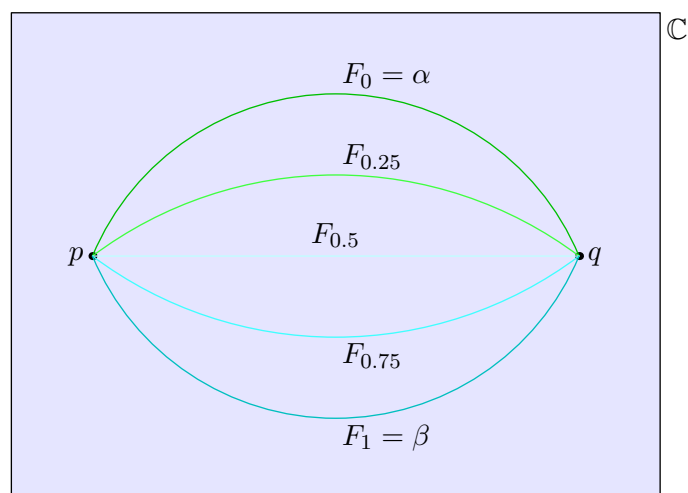
$$\alpha(0) = \beta(0) = F_s(0) \text{ 그리고 } \alpha(1) = \beta(1) = F_s(1) \text{ 모든 } s \in [0, 1] \text{에 대해.}$$

경로 호모토피가 존재하면,  $\alpha$ 와  $\beta$ 가 경로 **호모토픽**하다고 하며  $\alpha \simeq \beta$ 라고 씁니다.

**표기의 남용 7.7.2.** 엄밀히 말하면 두 경로 사이의 이 관계를 설명할 때 "경로 호모토피"라고 해야 하지만, 저는 이를 줄여서 그냥 "호모토피"라고 하겠습니다. 마찬가지로 "경로 호모토픽"도 줄여서 "호모토픽"이라고 하겠습니다.

애니메이션 그림: <https://commons.wikimedia.org/wiki/File:HomotopySmall.gif>. 말할 필요도 없이,  $\simeq$ 는 동치 관계입니다.

이 정의가 하는 일은  $\alpha$ 를  $\beta$ 로 "연속적으로 변형"시키되, 끝점은 고정된 채로 유지하는 것입니다. 특정한 각  $s$ 에 대해,  $F_s$  자체가 하나의 함수임에 주목하십시오. 그래서  $s$ 는  $\alpha$ 를  $\beta$ 로 변형해 나가는 시간을 나타냅니다: 0에서 1까지 진행하며,  $\alpha$ 에서 시작하여  $\beta$ 에서 끝납니다.



**질문 7.7.3.** 위의 정의가 옳다는 것을 스스로 납득해 보십시오. 유성이 충돌하면 무엇이 잘못 되는지 생각해 보십시오.

이제  $\mathbb{C}$ 를 특별하게 만드는 것이 무엇인지 말씀드릴 수 있습니다:

<sup>3</sup>감김수에 대해 알고 있다면 이것이 익숙하게 느껴질 것입니다. 이에 대해서는 기본군을 다루는 장에서 더 이야기하겠습니다.

**정의 7.7.4.** 공간  $X$ 가 경로 연결이고 임의의 두 점  $p$ 와  $q$ 에 대해  $p$ 에서  $q$ 로 가는 모든 경로가 호모토픽하다면,  $X$ 는 **단순 연결**이라고 합니다.

이것이 바로  $\mathbb{C}$ 에서  $p$ 에서  $q$ 로 걸어갈 때 아무런 질문도 하지 않는 이유입니다: 걷는 방법이 정말로 오직 하나뿐이기 때문입니다. 그래서 "단순" 연결이라는 용어가 붙습니다.

**질문 7.7.5.**  $\mathbb{R}^n$ 이 모든  $n$ 에 대해 단순 연결임을 스스로 납득해 보십시오.

## §7.8 공간의 기저

**이 절의 대표적인 예:**  $\mathbb{R}$ 은 열린 구간으로 이루어진 기저를 가지며,  $\mathbb{R}^2$ 는 열린 원판으로 이루어진 기저를 갖습니다.

$\mathbb{R}$ 의 열린집합을 기술하는 것이 다소 성가시다는 것을 눈치채셨을지도 모릅니다: 열린집합의 전형적인 예는  $(0, 1)$ 이지만, 다음과 같은 다른 열린집합들도 있습니다

$$(0, 1) \cup \left(1, \frac{3}{2}\right) \cup \left(2, \frac{7}{3}\right) \cup (2014, 2015).$$

**질문 7.8.1.** 이것이 열린집합임을 확인해 보십시오.

하지만 괜찮습니다, 이것이 그렇게 많이 다른 것은 아닙니다. 제가 한 일은 그저 제 전형적인 예시들을 잔뜩 모아 놓고  $\cup$  기호를 잔뜩 던져 넣은 것뿐입니다. 그리고 그것이 바로 기저의 개념입니다.

**정의 7.8.2.** 위상 공간  $X$ 에 대한 **기저**란,  $X$ 의 모든 열린집합이  $\mathcal{B}$ 의 원소들 중 (아마도 무한히 많은) 일부의 합집합이 되도록 하는, 열린집합들의 부분집합  $\mathcal{B}$ 를 말합니다.

그리고 우리가 하고 있는 일은 결국 이렇게 말하는 것입니다:

**예제 7.8.3** ( $\mathbb{R}$ 의 기저)

열린 구간들은  $\mathbb{R}$ 의 기저를 이룹니다.

사실, 더 일반적으로 다음이 성립합니다:

**정리 7.8.4** (거리 공간의 기저)

$r$ -근방들은 임의의 거리 공간  $M$ 의 기저를 이룹니다.

증명. 다소 뻔한 이야기입니다 – 열린집합  $U$ 가 주어졌을 때,  $U$  내부의 모든 점  $p$ 에 대해,  $U$  안에 완전히 포함되는  $r_p$ -근방  $U_p$ 를 그리십시오. 그러면  $\bigcup_p U_p$ 는  $U$ 에 포함되며 그 안의 모든 점을 덮습니다.  $\square$

따라서  $\mathbb{R}^2$ 의 열린집합은 결국 여러 열린 원판들의 합집합에 지나지 않으며, 다른 경우도 마찬가지입니다. 요점은, 거리 공간에서 정말로 신경 써야 할 열린집합은 오직  $r$ -근방뿐이라는 것입니다.

## §7.9 생각해 볼 만한 조금 더 어려운 문제

**문제 7A<sup>†</sup>.**  $X$ 를 위상 공간이라 합시다.  $X \rightarrow \{0, 1\}$ 인 상수가 아닌 연속함수가 존재하는 것과  $X$ 가 비연결인 것이 동치임을 보이십시오(여기서  $\{0, 1\}$ 에는 이산 위상이 주어집니다).

**문제 7B\*.**  $X$ 와  $Y$ 를 위상 공간이라 하고  $f: X \rightarrow Y$ 를 연속함수라 합시다.

- (a)  $X$ 가 연결이면  $f^{\text{img}}(X)$ 도 연결임을 보이십시오.
- (b)  $X$ 가 경로 연결(path-connected)이면  $f^{\text{img}}(X)$ 도 그러함을 보이십시오.

**문제 7C** (하우스도르프 공간이면  $T_1$  공리를 만족함).  $X$ 를 하우스도르프 위상 공간이라 합시다. 임의의 점  $p \in X$ 에 대해 집합  $\{p\}$ 가 닫혀 있음을 증명하십시오.

**문제 7D** ([Pu02], 연습문제 2.56).  $M$ 을 점이 하나보다 많지만 많아야 가산 무한 개인 거리 공간이라 합시다.  $M$ 이 비연결임을 보이십시오.

**문제 7E.**  $X$ 를 위상 공간이라 합시다. 점  $p \in X$ 의 연결 성분은 연결이면서  $p$ 를 포함하는 모든 부분공간  $S \subseteq X$ 의 합집합입니다.

- (a) 점의 연결 성분은 그 자체로 연결이어야 합니까?
- (b) 점의 연결 성분은  $X$ 의 열린집합이어야 합니까?

**문제 7F** (퍼스텐버그).  $\mathbb{Z}$ 의 부분집합이 등차수열  $\{a + nd \mid n \in \mathbb{Z}\}$ (단,  $a$ 와  $d$ 는 양의 정수)들의 합집합(공집합이거나 무한할 수 있음)일 때 이를 열려 있다고 선언합니다.

- (a) 이것이  $\mathbb{Z}$  위에 위상을 이룸을 확인하십시오. 이 위상을 **등간격 정수 위상**이라 부릅니다.
- (b) 소수  $p$ 에 대해  $\bigcup_p p\mathbb{Z}$ 를 고려하여 소수가 무한히 많음을 증명하십시오.



**문제 7G.**  $\mathbb{Z}$  위의 등간격 정수 위상이 거리화 가능함을 증명하십시오. 다시 말해, 위에서 기술한 열린집합들을 갖는 거리 공간으로  $\mathbb{Z}$ 를 만드는 거리함수  $d: \mathbb{Z}^2 \rightarrow \mathbb{R}$ 를 부여할 수 있음을 보이십시오.



**문제 7H.** 임의의 열린집합  $U \subseteq \mathbb{R}$ 은 열린 구간(끝점으로  $\pm\infty$ 를 허용)들의 합집합임을 우리는 알고 있습니다. 실제로  $U$ 를 서로소인 열린 구간들의 합집합으로 쓰는 것이 가능함을 보일 수 있습니다.<sup>4</sup> 이러한 서로소인 합집합이 많아야 가산 개의 구간으로 존재함을 증명하십시오.

<sup>4</sup>직접 증명해 보시기 바랍니다만, 저 개인적으로는 이 증명이 상당히 지루하다고 느꼈습니다.



# 8 콤팩트성

위상 공간의 가장 중요한 개념 중 하나는 콤팩트성입니다. 이는 유클리드 공간에서의 "닫혀 있고 유계"라는 개념을 임의의 위상 공간으로 일반화한 것입니다(예를 들어 **문제 8F†**를 참고하십시오).

거리 공간의 경우, 콤팩트성을 정식화하는 동치인 두 가지 방법이 있습니다:

- 수열을 사용하는 "자연스러운" 정의로, 점렬 콤팩트성이라고 불립니다.
- 열린 덮개를 사용하는 덜 자연스러운 정의입니다.

앞서 언급했듯이, 거리 공간에서의 수열은 매우 훌륭하지만, 일반적인 위상 공간에서의 수열은 형편없습니다(일반적인 수열의 수렴을 정의하는 수고조차 하지 않을 정도로 말입니다). 따라서 일반적인 공간에는 두 번째 정의가 사용될 것입니다.

## §8.1 점렬 콤팩트성의 정의

**이 절의 대표적인 예:**  $[0, 1]$ 은 콤팩트하지만,  $(0, 1)$ 은 그렇지 않습니다.

강조하자면, 콤팩트성은 거리 공간이 가질 수 있는 최상의 성질 중 하나입니다.

**정의 8.1.1.** 무한 수열  $x_1, x_2, \dots$ 의 **부분수열**은 그 이름 그대로입니다:  $i_1 < i_2 < \dots$ 가 양의 정수인 수열  $x_{i_1}, x_{i_2}, \dots$ 를 말합니다. 이 수열은 무한해야 함에 유의하십시오.

이를 생각하는 또 다른 방법은, 여러분의 관점이 부정적이나 긍정적이나에 따라 수열에서 "무한히 많은 항을 선택하는 것" 또는 "일부 항을 삭제하는 것"이라고 볼 수 있습니다.

**정의 8.1.2.** 거리 공간  $M$ 은 모든 수열이 수렴하는 부분수열을 가질 때 **점렬 콤팩트**하다고 합니다.

이번에는 예시를 들기 전에 반례부터 몇 가지 제시해 보겠습니다.

### 예제 8.1.3 (콤팩트 거리 공간이 아닌 예시들)

- (a) 공간  $\mathbb{R}$ 은 콤팩트하지 않습니다: 수열  $1, 2, 3, 4, \dots$ 를 생각해 보십시오. 어떤 부분 수열도 발산하므로,  $\mathbb{R}$ 은 결코 콤팩트할 수 없습니다.
- (b) 더 일반적으로, 어떤 공간이 유계가 아니라면 그 공간은 콤팩트할 수 없습니다. (원한다면 이를 증명해 보십시오.)
- (c) 열린 구간  $(0, 1)$ 은 유계이지만 콤팩트하지 않습니다: 수열  $\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots$ 를 생각해 보십시오. 이 수열은 "0으로 수렴"하기 때문에, 어떤 부분수열도  $(0, 1)$  안의 한 점으로 수렴할 수 없습니다.
- (d) 더 일반적으로, 완비가 아닌 공간은 어떤 것도 콤팩트할 수 없습니다.

이제 예시를 살펴봅시다!

**질문 8.1.4.** 유한 집합이 콤팩트함을 보이십시오. (비둘기집 원리.)

**예제 8.1.5 (콤팩트 공간의 예시)**

콤팩트 공간의 예시를 몇 가지 더 들어보겠습니다. 잠시 후 이들이 콤팩트함을 증명할 것이니, 지금은 그저 스스로 확신해 보십시오.

- (a)  $[0, 1]$ 은 콤팩트합니다. 스스로 확신해 보십시오! 단위 구간 안에 수많은 점이 있다고 상상해 보십시오...
- (b) 구의 표면,  $S^2 = \{(x, y, z) \mid x^2 + y^2 + z^2 = 1\}$ 은 콤팩트합니다.
- (c) 단위 공  $B^2 = \{(x, y) \mid x^2 + y^2 \leq 1\}$ 은 콤팩트합니다.
- (d)  $\mathbb{R}^2$ 에 존재하는 **하와이 귀걸이**는 콤팩트합니다: 이는 **그림 8.1**에서와 같이 각  $n$ 에 대해 반지름  $\frac{1}{n}$ 을 가지며 서로 접하는 원들로 구성됩니다.

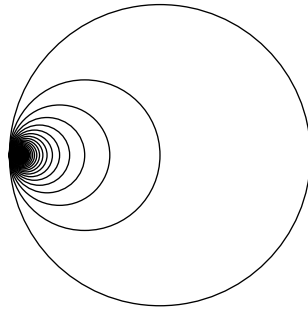


그림 8.1: 하와이 귀걸이.

더 많은 예를 생성하는 데 도움이 되도록, 다음을 언급합니다:

**명제 8.1.6 (콤팩트 집합의 닫힌 부분집합)**

점열 콤팩트 집합의 닫힌 부분집합은 콤팩트합니다.

**질문 8.1.7.** 이를 증명하십시오. (정의로부터 쉽게 따라와야 합니다.)

이러한 예시에 대해서는 좀 더 작업이 필요하며, 이는 다음 절에서 다룹니다.

## §8.2 콤팩트성의 판정 기준

**정리 8.2.1 (티호노프 정리)**

$X$ 와  $Y$ 가 콤팩트 공간이면,  $X \times Y$ 도 콤팩트합니다.

증명. 문제 8E.

□

또한 다음이 성립합니다:

**정리 8.2.2 (구간은 콤팩트합니다)**

$[0, 1]$ 은 콤팩트합니다.

증명. **문제 8F<sup>†</sup>**에 의해 이미 처리되지만, 직접 증명의 개요를 소개합니다.  $[0, 1]$ 을  $[0, \frac{1}{2}] \cup [\frac{1}{2}, 1]$ 로 나눕니다. 비둘기집 원리에 의해, 수열의 무한히 많은 항이 (예를 들어) 왼쪽 절반에 있으므로,  $x_1$ 을 그 첫 항으로 두고  $x_1$  이후 왼쪽 절반에 있는 항들만 남깁니다. 이제  $[0, \frac{1}{2}]$ 을  $[0, \frac{1}{4}] \cup [\frac{1}{4}, \frac{1}{2}]$ 로 나눕니다. 다시 비둘기집 원리에 의해, 무한히 많은 항이 어느 한 절반에 떨어지므로, 그중 하나를 골라  $x_2$ 라고 부릅니다. 이 과정을 반복합니다. 이런 방식으로 코시 수열인  $x_1, x_2, \dots$ 를 생성하며,  $[0, 1]$ 이 완비적이므로 이 수열이 수렴함을 의미합니다.  $\square$

이제 유클리드 공간에 관한 주요 정리를 증명할 수 있습니다:  $\mathbb{R}^n$ 에서 콤팩트성은 "닫혀 있고 유계"인 것과 동치입니다.

**정리 8.2.3 (볼차노-바이어슈트라스)**

$\mathbb{R}^n$ 의 부분집합은 닫혀 있고 유계인 경우에만 콤팩트합니다.

**질문 8.2.4.** 이것이 왜 우리 예시의 공간들이 콤팩트함을 함의합니까?

증명. 자, 닫혀 있고 유계인  $S \subseteq \mathbb{R}^n$ 을 살펴봅시다. 유계이므로, 이는 어떤 상자  $[a_1, b_1] \times [a_2, b_2] \times \dots \times [a_n, b_n]$  안에 존재합니다. 티호노프 정리에 의해, 각  $[a_i, b_i]$ 가 콤팩트하므로 전체 상자도 콤팩트합니다.  $S$ 가 이 콤팩트한 상자의 닫힌 부분집합이므로, 증명이 완료됩니다.  $\square$

이것이 성립하려면 정말로  $\mathbb{R}^n$ 에서 작업해야 합니다! 다른 공간에서는 이 판정 기준이 쉽게 성립하지 않을 수 있습니다.

**예제 8.2.5 (닫혀 있고 유계이지만 콤팩트하지 않은 경우)**

$S = \{s_1, s_2, \dots\}$ 를 이산 거리를 갖춘 임의의 무한 집합이라고 합시다. 그러면  $S$ 는 닫혀 있고 (모든 수렴 수열이 상수 수열이므로)  $S$ 는 유계이지만 (모든 점이 서로 거리 1만큼 떨어져 있으므로) 수열  $s_1, s_2, \dots$ 가 수렴하지 않으므로 분명히 콤팩트하지 않습니다.

**문제 8F<sup>†</sup>**인 볼차노-바이어슈트라스 정리는 거리 공간에서 어떤 집합이 콤팩트한지를 기하학적인 방식으로 정확히 알려줍니다.

**§8.3 열린 덮개를 이용한 콤팩트성**

이 절의 대표적인 예:  $[0, 1]$ 은 콤팩트합니다.

이제 정의할, 콤팩트성과 관련된 두 번째 개념이 있습니다. 다음 정의들은 매우 동기가 없어 보일 수 있지만, 조금만 참아 주십시오.

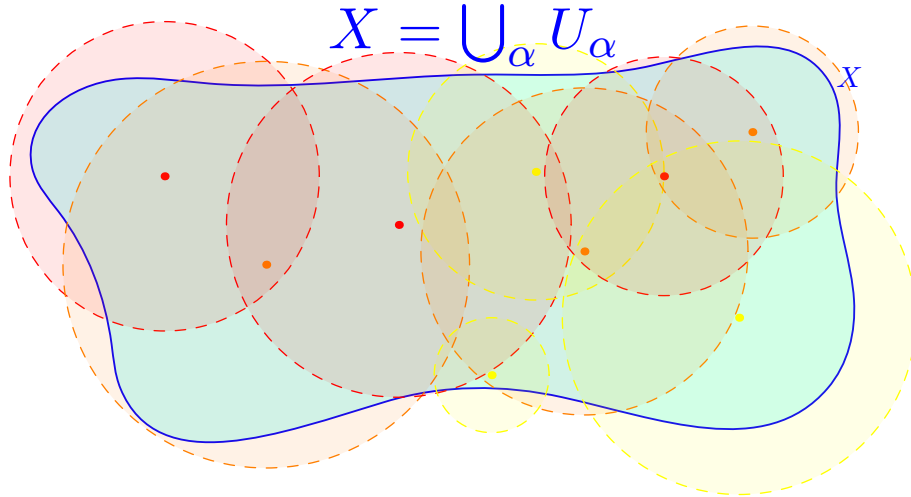
**정의 8.3.1.** 위상 공간  $X$ 의 **열린 덮개**란  $X$ 를 덮는 열린집합들의 모임  $\{U_\alpha\}$  (무한이거나 비가산일 수도 있음)를 말합니다:  $X$ 의 모든 점이 적어도 하나의  $U_\alpha$ 에 속하여,

$$X = \bigcup U_\alpha.$$

가 성립합니다.

**부분덮개**란 말 그대로의 뜻입니다:  $U_\alpha$  중 일부만을 취하면서도  $X$ 가 여전히 덮이도록 하는 것입니다.

그림을 하나 보겠습니다:



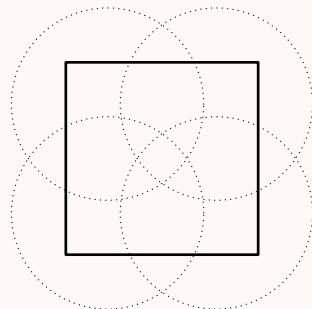
**정의 8.3.2.** 위상 공간  $X$ 는 모든 열린 덮개가 유한 부분덮개를 가질 때 **준콤팩트**하다고 합니다. 이것이 또한 하우스도르프이면 **콤팩트**하다고 합니다.

**비고 8.3.3** — 제가 슬쩍 끼워 넣은 "하우스도르프" 가정은 일종의 정합성 조건으로서, 대수기하학 장을 다루는 것이 아니라면 신경 쓸 필요가 없습니다. 왜냐하면 여러분이 다루게 될 공간은 모두 하우스도르프이기 때문입니다. (실제로 일부 저자들은 이를 굳이 언급조차 하지 않습니다.) 예를 들어 모든 거리 공간은 하우스도르프이므로, 거리 공간을 다루는 경우 이 조건은 안심하고 무시해도 됩니다.

이것이 무슨 뜻일까요? 예를 하나 들어 보겠습니다:

**예제 8.3.4 (유한 부분덮개의 예)**

단위 정사각형  $M = [0, 1]^2$ 을 모든 점을 중심으로 지름 1인 열린 원판을 놓아 (넘치는 부분은 잘라내면서) 덮는다고 합시다. 모든 점이 많은 열린집합에 속하며, 특히 그중 하나의 중심이기도 하므로, 이것이 열린 덮개임은 분명합니다. 하지만 이는 지나치게 과합니다 – 정사각형 전체를 덮는 데는 대략 네 개의 원이면 충분합니다. 이것이 바로 "유한 부분덮개"가 뜻하는 바입니다.



왜 이것이 중요할까요? 다음과 같은 이유에서입니다:

**정리 8.3.5** (점열 콤팩트  $\iff$  콤팩트)

거리 공간  $M$ 은 점열 콤팩트인 것과 콤팩트인 것이 동치입니다.

증명은 마지막 절로 미루겠습니다.

이로써 우리가 원했던 정의에 대한 동기를 얻었습니다. 점열 콤팩트성은 이해가 되는 조건이었습니다. 열린 덮개를 이용한 정의는 이상해 보였지만, 결국 동치임이 밝혀졌습니다. 그러나 우리는 이제 이 정의를 더 선호합니다. 왜냐하면 가능한 한 열린집합만을 이용한 정의에 의존하고 싶다는 것을 보아 왔기 때문입니다: 예를 들어 그러한 정의는 위상동형사상 아래에서 보존됩니다.

**예제 8.3.6** (비콤팩트성의 예)

공간  $X = [0, 1)$ 은 두 가지 의미 모두에서 콤팩트하지 않습니다. 이것이 심지어 완비적이지도 않으므로 ( $x_n = 1 - \frac{1}{n}$ 을 보십시오), 점열 콤팩트하지 않다는 것은 이미 알 수 있습니다. 덮개를 이용한 정의 아래에서 콤팩트하지 않음을 보이려면, 집합

$$U_m = \left[0, 1 - \frac{1}{m+1}\right)$$

( $m = 1, 2, \dots$ )을 생각해 봅시다. 그러면  $X = \bigcup U_i$ 이므로,  $U_i$ 는 실제로 덮개입니다. 그러나  $U_i$  중 유한개의 모임으로는  $X$ 를 덮을 수 없습니다.

**질문 8.3.7.**  $[0, 1]$ 이 실제로 콤팩트함을 스스로 확인해 보십시오; 이는 점열 콤팩트라는 것보다 조금 덜 직관적입니다.

**표기의 남용 8.3.8.** 따라서 우리는 이제부터 거리 공간을 "점열 콤팩트"하다고 부르지 않고 - 그냥 "콤팩트"하다고 부르겠습니다. (실제로 앞의 몇 절에서 이미 그렇게 해 왔습니다.)

## §8.4 콤팩트성의 응용

콤팩트성은 무한한 열린 덮개를 유한한 덮개로 줄일 수 있게 해 줍니다. 사실, 열린 덮개가 터무니없이 어리석은 것이라 하더라도 이렇게 할 수 있게 해 줍니다. 매우 흔히, 공간의 모든 점  $x$  하나하나에 대해  $x \in X$ 의 열린 근방으로 이루어진 열린 덮개를 취하곤 합니다; 이는 엄청나게 많은 수의 열린집합이지만, 콤팩트성은 이를 유한 집합으로 줄일 수 있게 해 줍니다.

전형적인 사용례를 하나 들자면:

**명제 8.4.1** (콤팩트  $\implies$  전유계)

$M$ 이 콤팩트라고 합시다. 그러면  $M$ 은 전유계입니다.

덮개를 이용한 증명. 모든 점  $p \in M$ 에 대해,  $p$ 의  $\varepsilon$ -근방을 취하고 이를  $U_p$ 라 합시다. 이들은 각 점  $p$ 가 적어도 그 열린 근방  $U_p$ 에는 덮인다는 지극히 당연한 이유로  $M$ 을 덮습니다. 그러면 콤팩트성에 의해 유한 부분덮개를 취할 수 있습니다.  $\square$

다음으로, 콤팩트 공간 사이의 사상에 관한 중요한 결과를 살펴봅시다.

**정리 8.4.2 (콤팩트 집합의 상은 콤팩트합니다)**

$f: X \rightarrow Y$ 를 연속 함수라 하고,  $X$ 는 콤팩트하다고 합시다. 그러면

$$f^{\text{img}}(X) \subseteq Y$$

는 콤팩트합니다.

덮개를 이용한 증명.  $f^{\text{img}}(X)$ 에 대한  $Y$ 의 임의의 열린 덮개  $\{V_\alpha\}$ 를 취합시다.  $f$ 의 연속성에 의해, 이는  $X$ 의 열린 덮개  $\{U_\alpha\}$ 로 당겨옵니다. 따라서 이것의 어떤 유한 부분덮개가  $X$ 를 덮습니다. 대응하는  $V$ 들이  $f^{\text{img}}(X)$ 를 덮습니다.  $\square$

**질문 8.4.3.** 연속성과 콤팩트성의 수열적 정의를 이용해 또 다른 증명을 제시하십시오. (이쪽이 훨씬 더 쉽습니다.)

이로부터 얻어지는 몇 가지 멋진 따름정리들:

**따름정리 8.4.4 (최댓값·최솟값 정리)**

$X$ 가 콤팩트하고 연속 함수  $f: X \rightarrow \mathbb{R}$ 를 생각합시다. 그러면  $f$ 는 어떤 점에서 최댓값을 달성합니다. 즉, 다른 모든  $q \in X$ 에 대해  $f(p) \geq f(q)$ 가 성립하는 점  $p \in X$ 가 존재합니다.

**따름정리 8.4.5 (중간값 정리)**

연속 함수  $f: [0, 1] \rightarrow \mathbb{R}$ 를 생각합시다. 그러면  $f$ 의 상은 어떤 실수  $a \leq b$ 에 대해  $[a, b]$ 를 포함합니다.

증명 개요. 핵심은  $f$ 의 상이  $\mathbb{R}$ 에서 콤팩트하므로 닫혀 있고 유계라는 점입니다. 닫힌집합들이 단지 닫힌구간들의 합집합일 뿐임을 스스로 확인해 볼 수 있습니다. 이로부터 최댓값·최솟값 정리가 따라옵니다.

$X = [0, 1]$ 일 때, 상은 또한 연결되어 있으므로  $f^{\text{img}}([0, 1])$ 에는 오직 하나의 닫힌구간만 있어야 합니다. 상이 유계이므로, 이제 그것이  $[a, b]$  꼴임을 압니다. (완전한 증명을 제시하려면 이른바 상한 성질을 이용해야 하겠지만, 그것은 잠자리에서 들려주는 이야기치고는 조금 복잡합니다. 게다가 저는  $\mathbb{R}$ 이 지루하다고 생각합니다.)  $\square$

**예제 8.4.6 ( $1/x$ )**

여기서 콤팩트성 가정은 정말로 중요합니다. 그렇지 않다면, 다음 함수를 생각해 봅시다

$$(0, 1) \rightarrow \mathbb{R} \quad \text{에 의해} \quad x \mapsto \frac{1}{x}.$$

(쌍곡선으로 그려지는) 이 함수는 유계가 아닙니다. 본질적으로, 문제는  $x = 0$  근처에서 함수가 발산하기 때문에 이를  $[0, 1]$  위의 함수로 확장할 수 없다는 것을 그래프로 확인할 수 있습니다.

마지막 응용으로,  $M$ 이 콤팩트 거리 공간이면 연속 함수  $f: M \rightarrow \mathbb{R}$ 은 특히 "좋은" 방식으로 연속입니다:

**정의 8.4.7.** 거리 공간 사이의 함수  $f: M \rightarrow N$ 은, 임의의  $\varepsilon > 0$ 에 대해 (오직  $\varepsilon$ 에만 의존하는)  $\delta > 0$ 이 존재하여  $d_M(x, y) < \delta$ 일 때마다  $d_N(f(x), f(y)) < \varepsilon$ 도 성립하면 **균등연속**이라 부릅니다.

이 이름은  $\varepsilon > 0$ 에 대해  $M$ 의 모든 점에서 통하는  $\delta$ 가 필요하다는 것을 의미합니다.

#### 예제 8.4.8 (균등연속)

- (a)  $x \mapsto ax + b$  꼴의  $\mathbb{R}$ 에서  $\mathbb{R}$ 로 가는 함수들은 모두 균등연속입니다. 항상  $\delta = \varepsilon/|a|$ 를 취할 수 있기 때문입니다 (또는  $a = 0$ 이면  $\delta = 1$ ).
- (b) 실제로, 유계인 도함수를 갖는 미분가능 함수  $\mathbb{R} \rightarrow \mathbb{R}$ 는 균등연속이라는 것이 참입니다. (역은 성립하지 않는데, 균등연속이 미분가능성을 전혀 함의하지 않기 때문입니다.)
- (c)  $x \mapsto x^2$ 에 의한 함수  $f: \mathbb{R} \rightarrow \mathbb{R}$ 는 균등연속이 아닙니다. 큰  $x$ 에 대해서는,  $x$ 의 아주 작은  $\delta$  변화가  $x^2$ 에서는 상당히 큰 변화로 이어지기 때문입니다. (원한다면 지금 이를 형식적으로 증명해 볼 수 있습니다.)  
 $f(2017.01) - f(2017) > 40$ 을 생각해 보십시오.  $\delta = 0.01$ 일 때조차,  $f$ 에서 큰 변화를 일으킬 수 있습니다.
- (d) 그러나  $(0, 1)$  또는  $[0, 1]$ 로 제한하면 함수  $x \mapsto x^2$ 는 균등연속이 됩니다. (이제  $\varepsilon > 0$ 에 대해 예를 들어  $\delta = \min\{1, \varepsilon\}/3$ 을 택할 수 있습니다.)
- (e)  $(0, 1) \rightarrow \mathbb{R}$ 로 정의된 함수  $x \mapsto 1/x$ 는 균등연속이 아닙니다 (앞서와 같은 이유입니다).

이제 약속했던 대로:

#### 명제 8.4.9 (콤팩트 집합 위에서 연속 $\implies$ 균등 연속)

$M$ 이 콤팩트이고  $f: M \rightarrow N$ 이 연속이면,  $f$ 는 균등 연속입니다.

수열을 이용한 증명.  $\varepsilon > 0$ 을 고정하고, 모순을 유도하기 위해 모든  $\delta = 1/k$ 에 대해 서로  $\delta$  이내에 있지만 그 상들은  $\varepsilon > 0$ 만큼 떨어져 있는 점  $x_k$ 와  $y_k$ 가 존재한다고 가정합니다. 콤팩트성에 의해 수렴하는 부분수열  $x_{i_k} \rightarrow p$ 를 취합니다. 그러면  $x_k$ 들과  $y_k$ 들이 서로 가깝기 때문에  $y_{i_k} \rightarrow p$  역시 성립합니다. 따라서 수열적 연속성에 의해 두 수열  $f(x_{i_k})$ 와  $f(y_{i_k})$  모두  $f(p)$ 로 수렴해야 하지만, 두 수열은 항상  $\varepsilon$ 만큼 떨어져 있으므로 이는 참일 수 없습니다.  $\square$

## §8.5 (선택) 콤팩트성 정의들의 동치성

다음을 증명하겠습니다:

#### 정리 8.5.1 (일반 거리 공간에 대한 하이네-보렐 정리)

거리 공간  $M$ 에 대해 다음은 동치입니다:

- (i) 모든 수열은 수렴하는 부분수열을 가진다,
- (ii) 공간  $M$ 은 완비이고 전유계이다, 그리고
- (iii) 모든 열린 덮개는 유한 부분덮개를 가집니다.

(i)  $\iff$  (ii)의 증명은 **문제 8F<sup>†</sup>**로 남겨둡니다; 증명의 아이디어는 **정리 8.2.2**의 정신과 매우 흡사합니다.

(i)와 (ii)  $\implies$  (iii)의 증명. 다음 보조정리를 증명하겠는데, 이는 그 자체로도 흥미롭습니다.

#### 보조정리 8.5.2 (르베그 수 보조정리)

$M$ 을 콤팩트 거리 공간이라 하고  $\{U_\alpha\}$ 를 열린 덮개라 합시다. 그러면 그 덮개에 대한 **르베그 수**라 불리는 실수  $\delta > 0$ 이 존재하여, 임의의 점  $p$ 의  $\delta$ -근방이 어떤  $U_\alpha$ 에 완전히 포함됩니다.

보조정리의 증명. 모순을 유도하기 위해, 모든  $\delta = 1/k$ 에 대해 그  $1/k$ -근방이 어떤  $U_\alpha$ 에도 포함되지 않는 점  $x_k \in M$ 이 존재한다고 가정합시다. 이렇게 하여 수열  $x_1, x_2, \dots$ 를 구성합니다; 따라서 어떤  $x$ 로 수렴하는 부분수열을 취할 수 있습니다. 그러면 모든  $\varepsilon > 0$ 에 대해  $d(x_n, x) + 1/n < \varepsilon$ 를 만족하는 정수  $n$ 을 찾을 수 있습니다; 따라서 모든  $\varepsilon > 0$ 에 대해  $x$ 에서의  $\varepsilon$ -근방은 어떤  $U_\alpha$ 에도 포함되지 않습니다. 이는 불가능한데, 우리가  $x$ 가 어떤 열린집합에 덮여 있다고 가정했기 때문입니다. ■

이제 그 덮개에 대한 르베그 수  $\delta$ 를 취합니다.  $M$ 이 전유계이므로, 유한히 많은  $\delta$ -근방이 공간을 덮으며, 따라서 유한히 많은  $U_\alpha$  역시 그러합니다. □

(iii)  $\implies$  (ii)의 증명. 한 단계는 자명합니다:

**질문 8.5.3.** 덮개 조건  $\implies$  전유계임을 보이십시오.

까다로운 부분은  $M$ 이 완비임을 보이는 것입니다. 모순을 유도하기 위해 그렇지 않다고 가정하고, 따라서 수열  $(x_k)$ 가 코시 수열이지만 어떤 특정한 점으로도 수렴하지 않는다고 가정합시다.

**질문 8.5.4.** 이것이 각  $p \in M$ 에 대해, 수열  $(x_k)$ 의 점들 중 많아야 유한히 많은 점만을 포함하는  $\varepsilon_p$ -근방  $U_p$ 가 존재함을 함의함을 보이십시오. ( $x_k \not\rightarrow p$ 이고  $(x_k)$ 가 코시 수열이라는 사실을 사용해야 할 것입니다.)

이제  $M = \bigcup_p U_p$ 를 고려하면 이 열린 근방들의 유한 부분덮개를 얻습니다; 하지만 이 유한 부분덮개는 그 수열의 유한히 많은 점만을 덮을 수 있으므로, 모순입니다. □

## §8.6 생각해 볼 만한 조금 더 어려운 문제

이후의 문제들은 꽤 어렵습니다; 일부는 IMO 3/6번 스타일의 구성 문제의 성격을 띠니다. 무슨 일이 일어나고 있는지 파악할 수 있도록 그림을 많이 그려보는 것이 중요합니다. 이 중에서 **문제 8F<sup>†</sup>**가 단연 제가 가장 좋아하는 것입니다.

**문제 8A.** 닫힌구간  $[0, 1]$ 과 열린구간  $(0, 1)$ 이 동형사상이 아님을 보이십시오.

**문제 8B.**  $X$ 를 이산 위상을 갖는 위상 공간이라 합시다. 어떤 조건에서  $X$ 가 콤팩트합니까?

**문제 8C** (여유한 위상은 준콤팩트할 뿐).  $X$ 를 무한 집합이라 하고 **여유한 위상**을 부여합시다: 열린집합은 공집합과 유한 집합의 여집합입니다. 이로써  $X$ 는 위상 공간이 됩니다.  $X$ 가 준콤팩트하지만 하우스도르프는 아님을 보이십시오.

**문제 8D** (칸토어의 교집합 정리).  $X$ 를 콤팩트 위상 공간이라 하고, 다음을 가정합시다

$$X = K_0 \supseteq K_1 \supseteq K_2 \supseteq \dots$$

는 포함관계로 중첩된 공집합이 아닌 닫힌 부분집합들의 무한 수열입니다.  $\bigcap_{n \geq 0} K_n \neq \emptyset$ 임을 보이십시오.

**문제 8E** (티호노프 정리).  $X$ 와  $Y$ 를 콤팩트 거리 공간이라 합시다.  $X \times Y$ 가 콤팩트함을 보이십시오. (이는 일반적인 위상 공간에 대해서도 참이지만, 증명이 뜻밖에 어렵고, 아직 일반적인  $X \times Y$ 조차 정의하지 않았습니다.)



**문제 8F<sup>†</sup>** (일반 거리 공간에 대한 볼차노-바이어슈트라스 정리). 거리 공간  $M$ 이 완비이고 전유계일 때, 그리고 오직 그때만 수열콤팩트임을 증명하십시오.



**문제 8G** (거의 Arzelà-Ascoli 정리).  $f_1, f_2, \dots : [0, 1] \rightarrow [-100, 100]$ 을 **동등연속**인 함수열이라 합시다. 이는 다음을 의미합니다

$$\forall \varepsilon > 0 \quad \exists \delta > 0 \quad \forall n \quad \forall x, y \quad (|x - y| < \delta \implies |f_n(x) - f_n(y)| < \varepsilon)$$

이 함수들의 부분수열  $f_{i_1}, f_{i_2}, \dots$ 를 뽑아낼 수 있음을 보이십시오. 이때 모든  $x \in [0, 1]$ 에 대해 수열  $f_{i_1}(x), f_{i_2}(x), \dots$ 이 수렴합니다.



**문제 8H.**  $M = (M, d)$ 를 유계 거리 공간이라 합시다.  $(M, d)$ 와  $(M, d')$ 가 동형사상이 되게 하는 (즉 같은 열린집합을 갖는)  $M$  위의 또 다른 거리  $d'$ 가 있을 때마다  $d'$  역시 유계라고 가정합시다.  $M$ 이 콤팩트함을 증명하십시오.



**문제 8I.** 이 문제에서 "원"이란 반지름이  $\theta$ 이 아닌 원판의 경계를 가리킵니다.

(a) 평면  $\mathbb{R}^2$ 를 서로소인 원들로 분할하는 것이 가능합니까?

(b) 평면  $\mathbb{R}^2$ 에서 서로 다른 두 점  $p$ 와  $q$ 를 제거합니다. 남은 점들을 서로소인 원들로 분할하는 것이 가능합니까?



# IV

## 선형대수학

## 제IV부: 목차

|           |                                               |            |
|-----------|-----------------------------------------------|------------|
| <b>9</b>  | <b>벡터 공간</b>                                  | <b>139</b> |
| 9.1       | 환과 체의 정의                                      | 139        |
| 9.2       | 가군과 벡터 공간                                     | 139        |
| 9.3       | 직합                                            | 141        |
| 9.4       | 선형 독립, 생성, 그리고 기저                             | 143        |
| 9.5       | 선형 사상                                         | 145        |
| 9.6       | 행렬이란 무엇인가?                                    | 147        |
| 9.7       | 부분공간과 편리한 기저 선택하기                             | 151        |
| 9.8       | 재미있는 응용: 라그랑주 보간법                             | 153        |
| 9.9       | 교육학적 여담: 숫자 배열은 사악하다                          | 153        |
| 9.10      | 일반적인 가군에 관한 한마디                               | 154        |
| 9.11      | 생각해 볼 만한 조금 더 어려운 문제                          | 155        |
| <b>10</b> | <b>고유한 것들</b>                                 | <b>157</b> |
| 10.1      | 관심을 가져야 하는 이유                                 | 157        |
| 10.2      | 가정에 관한 주의사항                                   | 158        |
| 10.3      | 고유벡터와 고윳값                                     | 158        |
| 10.4      | 조르당 형식                                        | 159        |
| 10.5      | 떡영 사상                                         | 161        |
| 10.6      | 떡영인 경우로의 환원                                   | 162        |
| 10.7      | (선택 사항) 떡영 조르당 정리의 증명                         | 163        |
| 10.8      | 대수적 중복도와 기하적 중복도                              | 164        |
| 10.9      | 생각해 볼 만한 조금 더 어려운 문제                          | 165        |
| <b>11</b> | <b>쌍대 공간과 대각합</b>                             | <b>167</b> |
| 11.1      | 텐서곱                                           | 167        |
| 11.2      | 쌍대 공간                                         | 170        |
| 11.3      | $V^\vee \otimes W$ 는 $V$ 에서 $W$ 로 가는 행렬들을 줍니다 | 172        |
| 11.4      | 대각합                                           | 173        |
| 11.5      | 생각해 볼 만한 조금 더 어려운 문제                          | 174        |
| <b>12</b> | <b>행렬식</b>                                    | <b>175</b> |
| 12.1      | 썰기곱                                           | 175        |
| 12.2      | 행렬식                                           | 178        |
| 12.3      | 특성다항식과 케일리-해밀턴                                | 179        |
| 12.4      | 생각해 볼 만한 조금 더 어려운 문제                          | 181        |
| <b>13</b> | <b>내적 공간</b>                                  | <b>183</b> |
| 13.1      | 내적                                            | 183        |
| 13.2      | 노름                                            | 185        |
| 13.3      | 직교성                                           | 187        |
| 13.4      | 힐베르트 공간                                       | 188        |
| 13.5      | 생각해 볼 만한 조금 더 어려운 문제                          | 190        |
| <b>14</b> | <b>보너스: 푸리에 해석</b>                            | <b>191</b> |
| 14.1      | 개요                                            | 191        |
| 14.2      | 힐베르트 공간에 대한 상기                                | 191        |
| 14.3      | 흔한 예시들                                        | 192        |
| 14.4      | 요약, 그리고 또 다른 예고편                              | 196        |
| 14.5      | Parseval과 그 친구들                               | 196        |
| 14.6      | 응용: 바젤 문제                                     | 197        |
| 14.7      | 응용: Arrow의 불가능성 정리                            | 198        |
| 14.8      | 생각해 볼 만한 조금 더 어려운 문제                          | 200        |
| <b>15</b> | <b>쌍대, 수반, 그리고 전치</b>                         | <b>201</b> |
| 15.1      | 사상의 쌍대                                        | 201        |

---

|      |                                                                           |     |
|------|---------------------------------------------------------------------------|-----|
| 15.2 | (선택) 자연스러운 동형사상 $V \cong V^V$ 가 없을 때 무엇이 잘못될 수 있는지에 대한 교훈적인 이야기 . . . . . | 202 |
| 15.3 | 쌍대 공간과의 동일시 . . . . .                                                     | 204 |
| 15.4 | 딸림사상 (컬레 전치) . . . . .                                                    | 205 |
| 15.5 | 정규 사상의 고윳값 . . . . .                                                      | 206 |
| 15.6 | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                            | 208 |

---



# 9 벡터 공간

이 장은 상당히 가볍습니다. 이 장의 목적은 벡터 공간과 기저가 무엇인지 정의하는 것입니다. 이는 여러분이 이미 알고 있을 법한 직관적인 개념들입니다.

## §9.1 환과 체의 정의

**이 절의 대표적인 예:**  $\mathbb{Z}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ 는 환이며, 뒤의 둘은 체입니다.

앞 장을 건너뛰었을 경우를 대비하여, 여기서 환/체를 매우 비형식적으로 정의하겠습니다.

- **환**은  $\mathbb{Z}$ 처럼 교환법칙이 성립하는 덧셈과 곱셈, 그리고 뺄셈을 갖춘 구조입니다. 또한 덧셈 항등원 0과 곱셈 항등원 1을 가집니다.
- $\mathbb{R}$ 이나  $\mathbb{C}$ 에서처럼 곱셈이 가역적이면(즉,  $x \neq 0$ 인 모든  $x$ 에 대해  $\frac{1}{x}$ 가 의미를 가지면), 그 환을 **체**라고 부릅니다.

사실, 이어지는 내용에서 "체"를 어디서나 " $\mathbb{R}$ "로 바꾸어 읽어도 별문제가 없을 것입니다. 관례적으로 환에는 문자  $R$ 을, 체에는  $k$  또는  $K$ 를 사용합니다.

마지막으로, 군에 대한 장을 건너뛰었을 경우를 대비하여 다음도 언급해야겠습니다.

- **덧셈적 아벨 군**은 교환법칙이 성립하는 덧셈과 뺄셈, 그리고 덧셈 항등원 0을 갖춘 구조입니다. 곱셈을 가질 필요는 없습니다. 좋은 예로는  $\mathbb{R}^3$ (성분별 덧셈을 갖춘)이 있습니다.

## §9.2 가군과 벡터 공간

**이 절의 대표적인 예:** 차수가  $n$  이하인 다항식들.

여러분은 이미  $\mathbb{R}^n$ 이 "벡터 공간"이라는 것을 직관적으로 알고 있습니다: 그 원소들은 서로 더할 수 있고, 실수에 의한 스칼라배가 존재합니다. 이를 더 일반적으로 전개해 봅시다. 가환환  $R$ 을 고정합시다. 그러면 비형식적으로,

**$R$ -가군이란 두 원소를 더할 수 있고  $R$ 의 원소로 스칼라배를 할 수 있는 임의의 구조입니다.**

나아가, **벡터 공간**은 가환환이 실제로 체인 가군일 뿐입니다. 완전한 정의는 잠시 후에 드리겠지만, 우선 예시부터 보겠습니다...

### 예제 9.2.1 (이차다항식, 일명 제가 가장 좋아하는 예시)

제가 가장 좋아하는  $\mathbb{R}$ -벡터 공간의 예시는 차수가 2 이하인 다항식들의 집합입니다, 즉

$$\{ax^2 + bx + c \mid a, b, c \in \mathbb{R}\}.$$

실제로, 임의의 두 이차식을 더할 수 있고 상수를 곱할 수 있습니다. 두 이차식을 곱해서 이차식을 얻을 수는 없지만, 이는 무관합니다 – 벡터 공간에서는 두 벡터를 서로 곱한다는 개념이 반드시 있을 필요가 없습니다.

나중에 정의할 의미에서, 이 벡터 공간은 (예상대로!) 차원이 3입니다.

### 예제 9.2.2 (모든 다항식)

실수 계수를 갖는 모든 다항식의 집합은  $\mathbb{R}$ -벡터 공간입니다, 왜냐하면 임의의 두 다항식을 더할 수 있고 상수를 곱할 수 있기 때문입니다.

### 예제 9.2.3 (유클리드 공간)

(a) 복소수는

$$\{a + bi \mid a, b \in \mathbb{R}\}$$

실수 벡터 공간을 이룹니다. 나중에 보겠지만, 이는 "차원 2"를 가집니다.

(b) 실수  $\mathbb{R}$ 은 차원 1의 실수 벡터 공간을 이룹니다.

(c) 3차원 벡터의 집합

$$\{(x, y, z) \mid x, y, z \in \mathbb{R}\}$$

임의의 두 순서쌍을 성분별로 더할 수 있으므로 이는 실수 벡터 공간을 이룹니다. 이것이 왜 "차원 3"을 갖는지는 나중에 다시 설명하겠습니다.

### 예제 9.2.4 (벡터 공간의 더 많은 예시)

(a) 집합

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

은 자명한 방식으로  $\mathbb{Q}$ -벡터 공간의 구조를 가집니다: 임의의 두 원소를 더할 수 있고, 유리수로 스칼라배할 수 있습니다. (이것은  $\mathbb{R}$ -벡터 공간이 아닙니다 — 왜 그럴까요?)

(b) 집합

$$\{(x, y, z) \mid x + y + z = 0 \text{ 그리고 } x, y, z \in \mathbb{R}\}$$

은 2차원 실수 벡터 공간입니다.

(c) 모든 함수  $f: \mathbb{R} \rightarrow \mathbb{R}$ 의 집합 또한 실수 벡터 공간입니다 ( $c \in \mathbb{R}$ 에 대해  $f + g$ 와  $c \cdot f$ 라는 개념이 모두 성립하기 때문입니다).

이제 이 곱셈이 어떻게 작동하는지에 대한 실제 규칙을 적어보겠습니다.

**정의 9.2.5.**  $R$ 을 가환환이라 합시다.  $R$ -**가군**은 항등원이  $0 = 0_M$ 으로 표기되는 덧셈 아벨 군  $M = (M, +)$ 에서 시작합니다. 여기에 추가로  $R$ 의 원소에 의한 좌측 곱셈을 지정합니다. 이 곱셈은  $r, r_1, r_2 \in R$ 과  $m, m_1, m_2 \in M$ 에 대해 다음 성질들을 만족해야 합니다:

(i)  $r_1 \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m$ .

(ii) 곱셈은 분배법칙을 만족하며, 이는 다음을 의미합니다

$$(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m \text{ 그리고 } r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2.$$

(iii)  $1_R \cdot m = m$ .

(iv)  $0_R \cdot m = 0_M$ 입니다. (사실 이는 불필요한 조건입니다; 앞의 세 가지로부터 유도할 수 있습니다.)

$R$ 이 체이면  $M$ 을  $R$ -**벡터 공간**이라 하며, 그 원소들을 **벡터**라 하고  $R$ 의 원소들을 **스칼라**라 합니다.

**표기의 남용 9.2.6.** 위에서는  $M$ 의 덧셈과  $R$ 의 덧셈에 같은 기호  $+$ 를 사용하고 있습니다. 죄송하지만 이는 피하기가 다소 어렵고, 공리의 요점은 이 두 덧셈이 서로 관련되어야 한다는 것입니다. 가군의 곱셈에는  $r \cdot m$ 을,  $R$ 의 곱셈에는  $r_1 r_2$ 를 쓰도록 기억해 보겠습니다.

**질문 9.2.7. 예제 9.2.1**에서 저는 "차수 2" 대신 "차수 2 이하"라고 신중하게 표현했습니다. 그 이유는 무엇일까요? 다시 말해, 왜

$$\{ax^2 + bx + c \mid a, b, c \in \mathbb{R}, a \neq 0\}$$

는  $\mathbb{R}$ -벡터 공간이 아닐까요?

덜 직관적이지만 다소 중요한 몇 가지 예시...

### 예제 9.2.8 (아벨 군은 $\mathbb{Z}$ -가군입니다)

(군에 익숙하지 않다면 이 예시는 건너뛰어도 좋습니다.)

(a) 실수 다항식의 예시

$$\{ax^2 + bx + c \mid a, b, c \in \mathbb{R}\}$$

또한  $\mathbb{Z}$ -가군입니다! 실제로 우리는 이러한 다항식을 임의로 두 개 더할 수 있고, 정수로 스칼라배할 수 있습니다.

(b) 100을 법으로 하는 정수의 집합, 즉  $\mathbb{Z}/100\mathbb{Z}$  역시  $\mathbb{Z}$ -가군입니다. 어떻게 그런지 알 수 있겠습니까?

(c) 사실, 임의의 아벨 군  $G = (G, +)$ 는  $\mathbb{Z}$ -가군입니다. 곱셈은 다음과 같이 정의될 수 있습니다

$$n \cdot g = \underbrace{g + \cdots + g}_{n\text{번}} \quad (-n) \cdot g = n \cdot (-g)$$

$n \geq 0$ 에 대해. (여기서  $-g$ 는  $g$ 의 덧셈에 대한 역원입니다.)

### 예제 9.2.9 (모든 환은 자기 자신의 가군입니다)

(a)  $\mathbb{R}$ 은 그 자신 위의  $\mathbb{R}$ -벡터 공간으로 생각할 수 있습니다. 왜 그런지 아시겠습니까?

(b) 같은 논리로, 임의의 가환환  $R$ 은 그 자신 위의  $R$ -가군으로 생각할 수 있음을 알 수 있습니다.

## §9.3 직합

**이 절의 대표적인 예:**  $\{ax^2 + bx + c\} = \mathbb{R} \oplus \mathbb{R}x \oplus \mathbb{R}x^2$ 이고,  $\mathbb{R}^3$ 은 자신의 좌표축들의 합입니다.

**예제 9.2.1**로 돌아가서, 다음을 생각해봅시다

$$V = \{ax^2 + bx + c \mid a, b, c \in \mathbb{R}\}.$$

차원이 무엇인지 아직 말씀드리지 않았지만, 이 벡터 공간이 "가져야 할" 차원이 3이라는 것을 아마 알아차리셨을 것입니다. 이에 대해서는 곧 다루겠습니다.

눈치채셨을 또 다른 점은,  $x^2$ ,  $x$ ,  $1$  항이 어쩐지 서로 "연관되지 않는다"는 것입니다. 이들은 완전히 무관합니다. 다시 말해, 다음 세 집합을 생각할 수 있습니다

$$\begin{aligned}\mathbb{R}x^2 &:= \{ax^2 \mid a \in \mathbb{R}\} \\ \mathbb{R}x &:= \{bx \mid b \in \mathbb{R}\} \\ \mathbb{R} &:= \{c \mid c \in \mathbb{R}\}.\end{aligned}$$

명백한 방식으로, 이들 각각은  $\mathbb{R}$ 의 "복사본"으로 생각할 수 있습니다.

그러면  $V$ 는 말 그대로 "이 집합들의 합"으로 이루어져 있습니다. 구체적으로,  $V$ 의 모든 원소는 이 집합들 각각에서 하나씩 뽑은 원소들의 합으로 유일하게 쓸 수 있습니다. 이는 다음과 같이 쓰도록 동기를 부여합니다

$$V = \mathbb{R}x^2 \oplus \mathbb{R}x \oplus \mathbb{R}.$$

이를 형식적으로 포착하는 개념이 바로 **직합**입니다.

**정의 9.3.1.**  $M$ 을  $R$ -가군이라 합시다.  $M_1$ 과  $M_2$ 를 그 자체로  $R$ -가군인  $M$ 의 부분집합이라 합시다. 그러면  $M$ 의 모든 원소가  $M_1$ 의 원소와  $M_2$ 의 원소의 합으로 유일하게 쓸 수 있을 때,  $M = M_1 \oplus M_2$ 라 쓰고  $M$ 을  $M_1$ 과  $M_2$ 의 **직합**이라고 말합니다.

#### 예제 9.3.2 (유클리드 평면)

벡터 공간  $\mathbb{R}^2 = \{(x, y) \mid x \in \mathbb{R}, y \in \mathbb{R}\}$ 을 생각해봅시다. 이를  $x$ 축과  $y$ 축의 직합으로 생각할 수 있습니다:

$$X = \{(x, 0) \mid x \in \mathbb{R}\} \text{ 그리고 } Y = \{(0, y) \mid y \in \mathbb{R}\}.$$

그러면  $\mathbb{R}^2 = X \oplus Y$ 입니다.

이는 가군을 몇 개의 서로 연결되지 않은 성분으로 분해하는 "하향식" 방법을 제공합니다.

이 발상을 거꾸로 적용하여, 새로운 벡터 공간을 다음과 같이 구성할 수도 있습니다. 매우 불운한 우연으로, 기술적으로는 서로 다른 두 대상의 이름과 표기가 정확히 똑같습니다.

**정의 9.3.3.**  $M$ 과  $N$ 을  $R$ -가군이라 합시다. **직합**  $M \oplus N$ 을, 그 원소가  $(m, n) \in M \times N$ 인 쌍들로 이루어진  $R$ -가군으로 정의합니다. 연산은 다음과 같이 주어집니다

$$(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2).$$

그리고

$$r \cdot (m, n) = (r \cdot m, r \cdot n).$$

예를 들어, 기술적으로는  $\mathbb{R}^2 = X \oplus Y$ 라고 썼지만,  $X$ 와  $Y$  각각이  $\mathbb{R}$ 의 복사본이므로,  $\mathbb{R}^2 \cong \mathbb{R} \oplus \mathbb{R}$ 이라고 써도 무방했을 것입니다.

**표기의 남용 9.3.4.** 위 내용은 직합을 표기하는 방식에 있어 표기법의 남용을 보여줍니다. 기호  $\oplus$ 는 두 가지 의미를 가집니다.

- $V$ 가 주어진 공간이고  $W_1$ 과  $W_2$ 가 부분공간이라면,  $V = W_1 \oplus W_2$ 는 위에서 정의한 방식으로 " $V$ 가 직합  $W_1 \oplus W_2$ 로 분해된다"는 것을 의미합니다.
- $W_1$ 과  $W_2$ 가 서로 무관한 두 공간이라면,  $W_1 \oplus W_2$ 는 그 원소가  $(w_1, w_2) \in W_1 \times W_2$ 인 쌍들인 벡터 공간으로 정의됩니다.

이 두 정의가 “어느 정도” 일치함을 알 수 있습니다.

이런 방식으로,  $V$ 가  $\mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$ 와 동형이어야 함을 알 수 있습니다. 우리는  $V = \mathbb{R}x^2 \oplus \mathbb{R}x \oplus \mathbb{R}$ 을 얻었는데,  $1, x, x^2$ 은 사실 서로 관련이 없고 각 항의 항은 본질적으로 그저  $\mathbb{R}$ 의 복사본일 뿐이기 때문입니다.

**정의 9.3.5.** 또한 모든 양의 정수  $n$ 에 대해, 다음과 같은 가군을 정의할 수도 있습니다

$$M^{\oplus n} := \underbrace{M \oplus M \oplus \cdots \oplus M}_{n\text{번}}$$

## §9.4 선형 독립, 생성, 그리고 기저

**이 절의 대표적인 예:**  $\{1, x, x^2\}$ 는  $\{ax^2 + bx + c \mid a, b, c \in \mathbb{R}\}$ 의 기저입니다.

이 절의 주제인 기저라는 개념은 다음과 같은 발상을 포착하는 또 다른 방법을 제공합니다

$$V = \{ax^2 + bx + c \mid a, b, c \in \mathbb{R}\}$$

$\{1, x, x^2\}$ 의 사본들의 합이라는 것입니다. 이 절은 기술적이기는 하지만 매우 직관적이어야 합니다. 여기 나오는 정리들이 왜 “성립해야 하는지” 이해되지 않는다면, 무언가 잘못하고 있는 것입니다.

이제  $M$ 을  $R$ -가군이라 합시다. 이미 익숙할 가능성이 높은 세 가지 매우 고전적인 개념을 정의하겠습니다. 만약 익숙하지 않다면, 유클리드 공간이나 위의  $V$ 에 대한 감각에 의지하십시오.

**정의 9.4.1.** 벡터  $v_1, \dots, v_n$ 의 **선형 결합**이란  $r_1v_1 + \cdots + r_nv_n$  형태의 합을 말하며, 여기서  $r_1, \dots, r_n \in R$ 입니다. 이 선형 결합은  $r_1 = r_2 = \cdots = r_n = 0_R$ 일 때 **자명하다**고 하며, 그렇지 않으면 **비자명하다**고 합니다.

**정의 9.4.2.**  $v_1, \dots, v_n$ 을  $R$ -가군  $M$ 의 원소들이라 합시다.

- 값이  $0_M$ 인 비자명한 선형 결합이 존재하지 않으면 **선형 독립**이라고 합니다. ( $0_M = 0 \cdot v_1 + 0 \cdot v_2 + \cdots + 0 \cdot v_n$ 은 항상 성립함을 관찰하십시오 – 여기서 주장하는 바는  $0_M$ 을 이 형태로 표현하는 다른 방법이 없다는 것입니다.)
- 모든  $v \in M$ 이  $\{v_i\}$ 의 선형 결합으로 나타내어질 수 있으면 **생성 집합**이라고 합니다.  $M$ 이 벡터 공간인 경우에는 대신 **생성한다**고 표현합니다.
- 모든  $v \in M$ 이  $\{v_i\}$ 의 선형 결합으로 유일하게 나타내어질 수 있으면 **기저**(복수형 **기저들**)라고 합니다.

동일한 정의가 무한 집합에도 적용되며, 다만 모든 합은 유한해야 한다는 조건이 붙습니다.

따라서 정의에 의해  $\{1, x, x^2\}$ 는  $V$ 의 기저입니다. 이것이 유일한 것은 아닙니다:  $\{2, x, x^2\}$ 와  $\{x+4, x-2, x^2+x\}$ 도 기저의 다른 예시이지만, 그다지 자연스럽지는 않습니다. 하지만 집합  $S = \{3+x^2, x+1, 5+2x+x^2\}$ 는 기저가 아니며, 두 가지 이유로 실패합니다:

- $0 = (3+x^2) + 2(x+1) - (5+2x+x^2)$ 임에 주목하십시오. 따라서 집합  $S$ 는 선형 독립이 아닙니다.
- $x^2$ 을  $S$ 의 원소들의 합으로 나타내는 것은 불가능합니다. 따라서  $S$ 는 생성 집합이 되지 못합니다.

이 새로운 용어들을 사용하면, 기저는 선형 독립이면서 생성하는 집합이라고 말할 수 있습니다.

**예제 9.4.3 (기저의 더 많은 예시)**

- (a)  $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ 를  $\mathbb{Q}$ -벡터 공간으로 생각합시다. 그러면  $\{1, \sqrt{2}\}$ 는 기저입니다.
- (b)  $V$ 가 모든 실수 다항식의 집합이라면,  $\{1, x, x^2, \dots\}$ 라는 무한 기저가 존재합니다. 유한개의 항만 사용한다는 조건은 단지 다항식이 유한한 차수를 가져야 한다는 것을 의미할 뿐입니다(이는 바람직한 일입니다).
- (c)  $V = \{(x, y, z) \mid x + y + z = 0 \text{ 그리고 } x, y, z \in \mathbb{R}\}$ 라 합시다. 그러면 크기 2의 기저가 존재할 것으로 예상되지만, 이전 예시들과 달리 즉시 “명백한” 선택이 없습니다. 성립하는 예시들은 다음과 같습니다:
- $(1, -1, 0)$ 과  $(1, 0, -1)$ ,
  - $(0, 1, -1)$ 과  $(1, 0, -1)$ ,
  - $(5, 3, -8)$ 과  $(2, -1, -1)$ .

**연습문제 9.4.4.** 벡터들의 집합이 기저인 것은 선형 독립이면서 생성하는 것과 동치임을 보이십시오. (막힌다면 다항식 예시를 생각해 보십시오.)

이제 벡터 공간의 기저가 가능한 한 가장 좋은 방식으로 동작함을 주장하는 몇 가지 결과를 서술하겠습니다.

**정리 9.4.5 (기저의 극대성과 극소성)**

$V$ 를 어떤 체  $k$  위의 벡터 공간이라 하고  $e_1, \dots, e_n \in V$ 를 취합니다. 다음은 동치입니다:

- (a)  $e_i$ 가 기저를 이룹니다.
- (b)  $e_i$ 는 생성 집합이지만, 진부분집합은 어느 것도 생성 집합이 아닙니다.
- (c)  $e_i$ 는 선형독립이지만,  $V$ 의 다른 어떤 원소를 추가해도 더 이상 선형독립이 아니게 됩니다.

**비고 9.4.6** —  $V$ 를 가환환  $R$  위의 일반적인 가군  $M$ 으로 바꾸면, (a)  $\implies$  (b)와 (a)  $\implies$  (c)는 성립하지만 그 역은 성립하지 않습니다.

증명. 간단하므로, 원한다면 직접 해보십시오. 주목해야 할 핵심은 역방향을 위해서는 스칼라로 나누어야 한다는 점이며, 따라서 (b)  $\implies$  (a)와 (c)  $\implies$  (a)의 함의를 위해서는  $V$ 가 단순히 가군이 아니라 벡터 공간이어야 합니다.  $\square$

**정리 9.4.7 (벡터 공간에 대한 차원 정리)**

벡터 공간  $V$ 가 유한 기저를 가진다면, 다른 모든 기저도 같은 개수의 원소를 가집니다.

증명. 우리는 더 강한 사실을 증명합니다:  $v_1, \dots, v_n$ 이 생성 집합이고  $w_1, \dots, w_m$ 이 선형 독립이라고 가정합니다. 우리는  $n \geq m$ 임을 주장합니다.

**질문 9.4.8.** 이 주장이 정리를 함의하기에 충분함을 보이십시오.

$A_0 = \{v_1, \dots, v_n\}$ 을 생성 집합이라 합시다.  $w_1$ 을 집어넣습니다: 생성 조건에 의해,  $w_1 = c_1v_1 + \dots + c_nv_n$ 입니다. 어떤 0이 아닌 계수가 있는데, 이를  $c_n$ 이라 합시다. 따라서

$$v_n = \frac{1}{c_n}w_1 - \frac{c_1}{c_n}v_1 - \frac{c_2}{c_n}v_2 - \dots$$

이로써  $A_1 = \{v_1, \dots, v_{n-1}, w_1\}$ 은 생성 집합입니다. 이제 같은 과정을 반복하여  $w_2$ 를 집어 넣고, 앞서와 같이  $v_i$  중 하나를 제거하여  $A_2$ 를 얻습니다;  $w_i$ 가 선형독립이라는 조건은 어떤  $v_i$ 의 계수가 항상 0이 아니게 됨을 보장합니다. 결국  $A_m$ 에 도달할 수 있으므로,  $n \geq m$ 입니다.  $\square$

#### 비고 9.4.9 (일반화)

- "원소의 개수"를 "농도"로 해석하면 이 정리는 무한 기저에 대해서도 성립합니다. 이는 처음 읽을 때 혼란스러울 수 있으므로, 자세히 다루지는 않겠습니다.
- 사실, 이는 임의의 가환환 위의 가군에 대해서도 성립합니다. 흥미롭게도, 일반적인 경우의 증명은 벡터 공간의 경우로 환원하는 방식으로 진행됩니다.

차원 정리는 그 이름에 걸맞게, 벡터 공간의 **차원**을 유한 기저가 존재할 경우 그 크기로 정의할 수 있게 해줍니다. 그러한 기저가 존재할 때 우리는  $V$ 가 **유한 차원**이라고 말합니다. 예를 들어,

$$V = \{ax^2 + bx + c \mid a, b, c \in \mathbb{R}\}$$

는 차원이 3인데, 왜냐하면  $\{1, x, x^2\}$ 이 기저이기 때문입니다. 이것이 유일한 기저는 아닙니다: 우리는 다음과 같이 쓸 수도 있었습니다

$$\{a(x^2 - 4x) + b(x + 2) + c \mid a, b, c \in \mathbb{R}\}$$

그리고 완전히 동일한 벡터 공간을 얻었을 것입니다. 하지만 이 정리의 아름다움은, 우리가 생성 집합을 어떻게 고안하려 해도 항상 정확히 세 개의 원소를 얻는다는 데 있습니다. 그것이 바로  $V$ 가 차원 3이라고 말하는 것이 타당한 이유입니다.

반면에, 모든 다항식의 집합  $\mathbb{R}[x]$ 는 무한 차원입니다(이는 직관적으로 명백해야 합니다).

$V$ 의 기저  $e_1, \dots, e_n$ 이 정말 멋진 이유는,  $v \in V$ 를 명시하기 위해서  $a_1, \dots, a_n \in k$ 만 명시하면 되고, 그러면  $v = a_1e_1 + \dots + a_ne_n$ 이 되기 때문입니다. 심지어  $v$ 를  $(a_1, \dots, a_n)$ 으로 생각할 수도 있습니다. 다르게 말하면,  $V$ 가  $k$ -벡터 공간이라면 우리는 항상 다음을 얻습니다

$$V = e_1k \oplus e_2k \oplus \dots \oplus e_nk.$$

## §9.5 선형 사상

**이 절의 대표적인 예:**  $x = 3$ 에서  $\{ax^2 + bx + c\}$ 의 값 계산.

우리는 준동형사상과 연속 사상을 보았습니다. 이제 우리는 벡터 공간 사이의 구조 보존 사상인 선형 사상을 보려고 합니다. 그 정의를 짐작할 수 있습니까?

**정의 9.5.1.**  $V$ 와  $W$ 를 같은 체  $k$  위의 벡터 공간이라고 합시다. **선형 사상**이란 다음을 만족하는 사상  $T: V \rightarrow W$ 입니다:

- (i) 임의의  $v_1, v_2 \in V$ 에 대해  $T(v_1 + v_2) = T(v_1) + T(v_2)$ 가 성립합니다.<sup>1</sup>

<sup>1</sup>군의 언어로 말하면,  $T$ 는 준동형사상  $(V, +) \rightarrow (W, +)$ 입니다.

(ii) 임의의  $a \in k$ 와  $v \in V$ 에 대해  $T(a \cdot v) = a \cdot T(v)$ 가 성립합니다.

이 사상이 전단사(동등하게, 역사상을 가지면)라면 이는 **동형사상**입니다. 이때  $V$ 와  $W$ 를 **동형**인 벡터 공간이라고 하며  $V \cong W$ 라고 씁니다.

### 예제 9.5.2 (선형 사상의 예시)

- (a) 임의의 벡터 공간  $V$ 와  $W$ 에 대해, 모든 것을  $0_W \in W$ 로 보내는 자명한 선형 사상이 존재합니다.
- (b) 임의의 벡터 공간  $V$ 에 대해, 항등 동형사상  $\text{id}: V \rightarrow V$ 가 존재합니다.
- (c)  $(a, b, c) \mapsto 4a + 2b + c$ 로 정의되는 사상  $\mathbb{R}^3 \rightarrow \mathbb{R}$ 은 선형 사상입니다.
- (d)  $V$ 를 차수가 2 이하인 실수 다항식의 집합이라고 합시다.  $(a, b, c) \mapsto ax^2 + bx + c$ 로 정의되는 사상  $\mathbb{R}^3 \rightarrow V$ 는 동형사상입니다.
- (e)  $V$ 를 차수가 2 이하인 실수 다항식의 집합이라고 합시다.  $ax^2 + bx + c \mapsto 9a + 3b + c$ 로 정의되는 사상  $V \rightarrow \mathbb{R}$ 은 선형 사상이며, 이는 "3에서의 값매김"이라고 설명할 수 있습니다.
- (f)  $W$ 를  $\mathbb{R} \rightarrow \mathbb{R}$ 인 함수들의 집합이라고 합시다.  $f \mapsto f(0)$ 으로 정의되는 값매김 사상  $W \rightarrow \mathbb{R}$ 은 선형 사상입니다.
- (g) " $\sqrt{2}$ 를 곱하기"라고 불리는  $\mathbb{Q}$ -벡터 공간의 사상  $\mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}[\sqrt{2}]$ 이 있습니다. 이 사상은  $a + b\sqrt{2} \mapsto 2b + a\sqrt{2}$ 로 보냅니다. 이 사상은 역사상 " $1/\sqrt{2}$ 를 곱하기"를 가지므로 동형사상입니다.

$T(a \cdot v) = a \cdot T(v)$ 라는 표현에서, 첫 번째  $\cdot$ 은  $V$ 의 곱셈이고 두 번째  $\cdot$ 은  $W$ 의 곱셈임에 유의하십시오. 이 동형사상의 개념은 실제로는 기저의 크기에만 관심이 있다는 점에 유의하십시오:

### 명제 9.5.3 ( $n$ 차원 벡터 공간은 동형입니다)

$V$ 가  $n$ 차원 벡터 공간이면,  $V \cong k^{\oplus n}$ 입니다.

**질문 9.5.4.**  $e_1, \dots, e_n$ 을  $V$ 의 기저라고 합시다. 그 동형사상은 무엇일까요? (아마 여러분의 첫 번째 추측이 맞을 것입니다.)

**비고 9.5.5** — 엄밀히 말해, 모든 유한 차원 벡터 공간은 그저  $k^{\oplus n}$ 일 뿐이며 그 외 다른 공간은 신경 쓸 가치가 없다고 말할 수도 있습니다. 하지만 이는 다소 무례해 보입니다. 공간은 종종 단순한 삼중항 이상의 것입니다:  $ax^2 + bx + c$ 는 다항식이며, 따라서 그것을  $(a, b, c)$ 로 압축하면 잃게 되는 어떤 "본질"을 가지고 있습니다. 게다가,  $x + y + z = 0$ 을 만족하는 벡터  $(x, y, z)$ 의 집합처럼 많은 공간은 명백한 기저 선택이 없습니다. 따라서 그러한 공간을  $k^{\oplus n}$ 으로 옮기려면 임의의 결정을 내려야 할 것입니다.

## §9.6 행렬이란 무엇인가?

이제 드디어 행렬이 무엇인지 말씀드릴 수 있습니다! 이는 재미있는데, 왜냐하면 이제 저는 행렬 곱셈의 공식을 그저 전달받는 것이 아니라 어떻게 유도하는지 여러분께 마침내 설명할 수 있기 때문입니다.

이 절은 매우 중요하며, 또한 많은 학생들에게 깨달음을 주는 내용이므로, 저는 실제로 이를 두 번 다루려고 합니다. 첫 번째로, 저는 극도로 특수한 경우, 즉  $V = W = \mathbb{R}^2$ 인 경우에서 많은 숫자를 사용하여 작업할 것입니다. (이는 제가 증명 경험이 없는 대학 신입생들에게 이 개념을 가르쳤을 때 설명했던 방식입니다.) 그다음 두 번째로, 우리는 숫자를 전혀 사용하지 않고 현대적인 언어로 이를 다룰 것입니다.

### §9.6.i 일반 독자를 위한 $\mathbb{R}^2$ 의 확장된 예시

이 절 전체에서 저는 구체적으로  $\mathbb{R}^2$ 를 다룰 것이며, 그 원소들을  $(x, y)$ 가 아니라  $\begin{bmatrix} x \\ y \end{bmatrix}$ 로 표기하겠습니다(행렬 곱셈에 대해 이야기할 때 그 이유를 보시게 될 것입니다).

깜짝 퀴즈:

- **문제 1:** 선형 사상  $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ 가 주어졌는데  $T\left(\begin{bmatrix} 3 \\ 4 \end{bmatrix}\right) = \begin{bmatrix} \pi \\ 9 \end{bmatrix}$ 이고  $T\left(\begin{bmatrix} 100 \\ 100 \end{bmatrix}\right) = \begin{bmatrix} 0 \\ 12 \end{bmatrix}$ 라고 합시다.  $T\left(\begin{bmatrix} 103 \\ 104 \end{bmatrix}\right)$ 와  $T\left(\begin{bmatrix} 203 \\ 204 \end{bmatrix}\right)$ 는 무엇입니까?

**답 1:** 그냥 더하면 됩니다.

$$\begin{aligned} T\left(\begin{bmatrix} 103 \\ 104 \end{bmatrix}\right) &= \begin{bmatrix} \pi \\ 9 \end{bmatrix} + \begin{bmatrix} 0 \\ 12 \end{bmatrix} = \begin{bmatrix} \pi \\ 21 \end{bmatrix} \\ T\left(\begin{bmatrix} 203 \\ 204 \end{bmatrix}\right) &= \begin{bmatrix} \pi \\ 9 \end{bmatrix} + 2 \begin{bmatrix} 0 \\ 12 \end{bmatrix} = \begin{bmatrix} \pi \\ 33 \end{bmatrix}. \end{aligned}$$

- **문제 2:** 선형 사상  $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ 가 주어졌는데  $T\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) = \begin{bmatrix} 1 \\ 3 \end{bmatrix}$ 이고  $T\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right) = \begin{bmatrix} 2 \\ 4 \end{bmatrix}$ 라고 합시다.  $T\left(\begin{bmatrix} 50 \\ 70 \end{bmatrix}\right)$ 는 무엇입니까?

**답 2:**

$$T\left(\begin{bmatrix} 50 \\ 70 \end{bmatrix}\right) = 50 \begin{bmatrix} 1 \\ 3 \end{bmatrix} + 70 \begin{bmatrix} 2 \\ 4 \end{bmatrix} = \begin{bmatrix} 190 \\ 430 \end{bmatrix}.$$

이 예시가 보여주는 바는, 선형 사상  $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ 에 대한 요구 조건이 매우 강력해서,  $T\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right)$ 와  $T\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right)$ 만 알면 다른 어떤 점에서의  $T$  값도 계산할 수 있다는 것입니다. 이는 임의의 두 기저 벡터에 대해서도 성립합니다(즉, 문제 1은 일부러 고른  $\begin{bmatrix} 103 \\ 104 \end{bmatrix}$ 와  $\begin{bmatrix} 203 \\ 204 \end{bmatrix}$ 보다 훨씬 더 지저분한 입력에 대해서도 물어볼 수 있었을 것이고, 그래도 여전히 풀 수 있었을 것입니다), 하지만 물론  $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ 와  $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ 는 특히 편리한 선택입니다.

이제 다음과 같은 정의를 내릴 수 있습니다:

**정의 9.6.1.** 선형 변환  $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ 에 대해, 그 행렬은 열벡터들을 이어붙여 얻어지는  $T$ 의 인코딩입니다

$$T\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) \quad \text{그리고} \quad T\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right)$$

를 이어붙여  $2 \times 2$  숫자 배열을 얻음으로써 만들어지는  $T$ 의 부호화입니다.

예를 들어,

$$T\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) = \begin{bmatrix} 1 \\ 3 \end{bmatrix} \quad \text{그리고} \quad T\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right) = \begin{bmatrix} 2 \\ 4 \end{bmatrix} \iff T \text{다음과 같이 인코딩됨} \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}.$$

이제, 고등학교에서 배운 행렬 곱셈 규칙을 열벡터  $\begin{bmatrix} 50 \\ 70 \end{bmatrix}$ 에 적용하면 어떻게 될까요? 그러면 다음을 얻습니다

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 50 \\ 70 \end{bmatrix} = \begin{bmatrix} 1 \cdot 50 + 2 \cdot 70 \\ 3 \cdot 50 + 4 \cdot 70 \end{bmatrix} = \begin{bmatrix} 190 \\ 430 \end{bmatrix}$$

...그리고 우리가 실은 두 번째 깜짝 퀴즈 문제를 다시 풀고 있을 뿐임을 알 수 있습니다. 그러므로:

$T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ 가  $2 \times 2$  행렬  $M$ 로 부호화되어 있다면,  $M$ 와 (열)벡터  $v \in \mathbb{R}^2$ 의 곱셈은  $T(v)$ 와 일치하도록 정의됩니다.

**비고 9.6.2** (행렬이 그 이름값을 하는 이유) — 이는 또한 왜  $2 \times 2$  행렬이 고등학교에서 주는 설명(즉, "곱해 보면 같은 결과가 나온다는 것을 알 수 있습니다")보다 더 자연스러운 이유로  $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ 인지를 보여줍니다.  $\text{id}$ 가 항등함수라면,  $\text{id}(\begin{bmatrix} 1 \\ 0 \end{bmatrix}) = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ 이므로 이것이 행렬의 첫 번째 열이 되고, 마찬가지로  $\text{id}(\begin{bmatrix} 0 \\ 1 \end{bmatrix}) = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ 은 두 번째 열이 됩니다.

이제, 두 사상  $S$ 와  $T$ 를 함께 등장시켜 합성하면 어떻게 될까요?  $S \circ T$ 에 대해서도 같은 방식을 적용할 수 있습니다.

- **문제 3:** 선형 사상  $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ 가 주어졌는데  $T(\begin{bmatrix} 1 \\ 0 \end{bmatrix}) = \begin{bmatrix} 1 \\ 3 \end{bmatrix}$ 이고  $T(\begin{bmatrix} 0 \\ 1 \end{bmatrix}) = \begin{bmatrix} 2 \\ 4 \end{bmatrix}$ 라고 합시다. 그다음 두 번째 선형 사상  $S: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ 가 주어졌는데  $S(\begin{bmatrix} 1 \\ 0 \end{bmatrix}) = \begin{bmatrix} 5 \\ 7 \end{bmatrix}$ 이고  $S(\begin{bmatrix} 0 \\ 1 \end{bmatrix}) = \begin{bmatrix} 6 \\ 8 \end{bmatrix}$ 라고 합시다.  $S(T(\begin{bmatrix} 1 \\ 0 \end{bmatrix}))$ 와  $S(T(\begin{bmatrix} 0 \\ 1 \end{bmatrix}))$ 는 무엇입니까?

**답 3:**

$$\begin{aligned} S\left(T\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right)\right) &= S\left(\begin{bmatrix} 1 \\ 3 \end{bmatrix}\right) = 1 \begin{bmatrix} 5 \\ 7 \end{bmatrix} + 3 \begin{bmatrix} 6 \\ 8 \end{bmatrix} = \begin{bmatrix} 23 \\ 31 \end{bmatrix}. \\ S\left(T\left(\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right)\right) &= S\left(\begin{bmatrix} 2 \\ 4 \end{bmatrix}\right) = 2 \begin{bmatrix} 5 \\ 7 \end{bmatrix} + 4 \begin{bmatrix} 6 \\ 8 \end{bmatrix} = \begin{bmatrix} 34 \\ 46 \end{bmatrix}. \end{aligned}$$

$S \circ T$  자체도 선형 사상이므로, 이제 그 행렬 인코딩을 알 수 있습니다:

$$S \circ T = \begin{bmatrix} 23 & 34 \\ 31 & 46 \end{bmatrix}.$$

이제 여러분은 학교에서 행렬 곱셈 규칙을 정의로서 배웠을 수도 있습니다.  $S$ 와  $T$ 의 행렬에 그 정의를 적용하면 다음을 얻어야 합니다

$$\underbrace{\begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix}}_{S \text{의 인코딩}} \underbrace{\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}}_{T \text{의 인코딩}} = \begin{bmatrix} 5 \cdot 1 + 6 \cdot 3 & 5 \cdot 2 + 6 \cdot 4 \\ 7 \cdot 1 + 8 \cdot 3 & 7 \cdot 2 + 8 \cdot 4 \end{bmatrix} = \begin{bmatrix} 23 & 34 \\ 31 & 46 \end{bmatrix}$$

이것이 바로  $S \circ T$ 의 인코딩입니다 — 실제로 그 이유를 알 수 있는데, 답 3의 과정을 따라가 보면 사실 동일한 산술이 수행되고 있기 때문입니다.

이는 왜 행렬을 선형 함수의 부호화로 보는 우리 냅킨의 정의가 여러분이 봐 왔던 것보다 더 나은지를 보여줍니다. 고등학교에서는 행렬 곱셈의 절차가 부자연스러운 정의로서 제공되는데, 예를 들면 **그림 9.1**에 나오는 것 같은 귀여운 그림들이 그렇습니다. 하지만 우리에게 **그림 9.1**의 절차가 하나의 정리입니다: 즉  $S$ 와  $T$ 의 부호화가 주어졌을 때  $S \circ T$ 의 부호화를 얻는 방법을 유도할 수 있습니다.

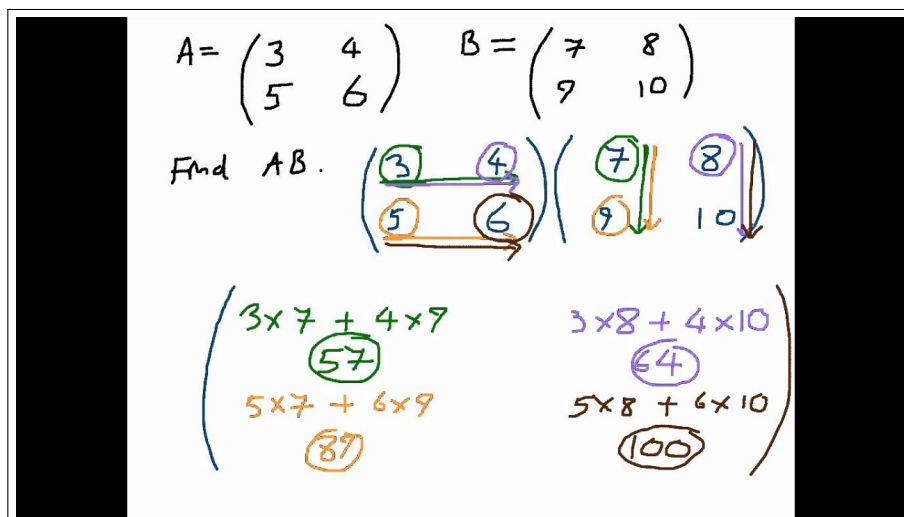


그림 9.1: 미국 고등학교에서 가르치는 행렬 곱셈: “이게 레시피야, 그냥 믿어”. [Ma12]에서 가져온 이미지.

### §9.6.ii 일반적인 논의, 다시 Napkin 수준의 추상화로

이제 현대적인 언어로 돌아가서, 이전 절에서처럼 고정된 기저가 아니라, 어떤 체 위의 유한 차원 공간과 그 공간의 임의의 기저를 다루도록 합시다.

기저  $e_1, \dots, e_m$ 을 가진 어떤 유한 차원 벡터 공간  $V$ 와 기저  $w_1, \dots, w_n$ 을 가진 벡터 공간  $W$ 를 하나 고릅시다. 사상  $T: V \rightarrow W$ 가 있고, 여러분에게  $T$ 가 무엇인지 알려주고 싶다고 합시다. 모든 점  $v$ 에서  $T(v)$ 가 무엇인지 알려주려 한다면 그것은 매우 배려 없는 일이 될 것입니다. 하지만 우리는  $T(e_1), \dots, T(e_m)$ 이 무엇인지만 알려주면 된다는 것을 보았는데, 그로부터 여러분 스스로  $T(a_1e_1 + \dots + a_me_m)$ 을 구할 수 있기 때문입니다:

$$T(a_1e_1 + \dots + a_me_m) = a_1T(e_1) + \dots + a_mT(e_m).$$

$e_i$ 들이 기저이므로, 이것으로  $T$ 에 대해 필요한 모든 것을 알 수 있습니다.

#### 예제 9.6.3 (선형 사상의 확장)

$V = \{ax^2 + bx + c \mid a, b, c \in \mathbb{R}\}$ 라고 합시다. 그러면  $T(ax^2 + bx + c) = aT(x^2) + bT(x) + cT(1)$ 입니다.

이제 저는 훨씬 더 구체적일 수 있습니다.  $T(e_1)$ 이 무엇인지 알려드릴 수도 있지만,  $W$ 의 기저를 가지고 있으므로 실제로는 이 기저를 기준으로  $T(e_1)$ 이 무엇인지만 알려드리면 됩니다. 구체적으로, 다음을 만족하는 유일한  $a_{11}, a_{21}, \dots, a_{n1} \in k$ 가 존재합니다

$$T(e_1) = a_{11}w_1 + a_{21}w_2 + \dots + a_{n1}w_n.$$

그러므로 추상적인 공간  $W$ 에서  $T(e_1)$ 의 값을 알려드리는 대신,  $a_{11}, a_{21}, \dots, a_{n1}$ 이 무엇인지만 알려드리면 됩니다. 그런 다음  $T(e_2)$ ,  $T(e_3)$ 에 대해서도,  $T(e_m)$ 까지 이 과정을 반복 하면 되고, 그것으로  $T$ 에 대해 필요한 모든 것을 알려드리는 셈이 됩니다.

바로 여기서 행렬  $T$ 가 나오는 것입니다! 이는 제가 알려드려야 할  $mn$ 개의 숫자 전부를 간결하게 적는 방법입니다.

명시적으로,  $T$ 에 대한 행렬은 다음 배열로 정의됩니다

$$T = \underbrace{\begin{bmatrix} | & | & \dots & | \\ T(e_1) & T(e_2) & \dots & T(e_m) \\ | & | & \dots & | \end{bmatrix}}_{m\text{개의 열}} \Bigg\} n\text{개의 행}$$

$$= \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{bmatrix}.$$

이 점을 확실히 하기 위해,

**행렬은  $V$ 에서  $W$ 로 가는 선형 사상을 지정하는 가장 게으른 방법입니다.**

#### 예제 9.6.4 (행렬의 예)

여기 기저를 이용한 구체적인 예가 있습니다.  $V = \mathbb{R}^3$ 에 기저  $e_1, e_2, e_3$ 가 있고  $W = \mathbb{R}^2$ 에 기저  $w_1, w_2$ 가 있다고 합시다.  $T: V \rightarrow W$ 가 있다면 이는 예를 들어 세 값에 의해 유일하게 결정됩니다:

$$T(e_1) = 4w_1 + 7w_2$$

$$T(e_2) = 2w_1 + 3w_2$$

$$T(e_3) = w_1$$

그러면 열들은  $T(e_1), T(e_2), T(e_3)$ 에 대응합니다:

$$T = \begin{bmatrix} 4 & 2 & 1 \\ 7 & 3 & 0 \end{bmatrix}$$

#### 예제 9.6.5 (기저를 선택한 후의 행렬 예)

다시  $V = \{ax^2 + bx + c\}$ 를 차수가 2 이하인 다항식들의 벡터 공간이라고 합시다. 이에 대해 기저  $1, x, x^2$ 를 고정합니다.

"3에서의 평가" 사상, 즉  $V \rightarrow \mathbb{R}$ 인 사상을 생각해 봅시다. 우변의 기저 원소로 1을 선택합니다; 그러면 이를  $1 \times 3$  행렬로 다음과 같이 쓸 수 있습니다

$$\begin{bmatrix} 1 & 3 & 9 \end{bmatrix}$$

여기서 열들은  $T(1), T(x), T(x^2)$ 에 대응합니다.

여기서부터 두 행렬을 곱한다는 것이 무엇을 의미하는지 스스로 도출해 낼 수 있습니다. 세 공간  $U, V, W$ 에 대해 기저를 선택했다고 합시다. 사상  $T: U \rightarrow V$ 와  $S: V \rightarrow W$ 가 주어졌을 때, 이들의 합성  $S \circ T$ 를 생각할 수 있습니다, 즉

$$U \xrightarrow{T} V \xrightarrow{S} W.$$

행렬 곱셈은 정확히, 지난 절에서 보았듯이 합성 함수  $S \circ T$ 를 행렬로 해석했을 때 얻는 것과 행렬  $ST$ 가 같은 것이 되도록 정의됩니다.

특히 함수 합성이 결합적이므로, 행렬 곱셈 역시 결합적임이 따라 나옵니다.

이는 행렬의 행렬식이나 대각합 같은 개념을, "내재적인" 사상  $T: V \rightarrow W$ 의 관점에서, 행렬의 성분의 관점에서 정의할 수 있음을 뜻합니다. 사상  $T$  자체는 어떤 기저도 참조하지 않으므로, 추상적 정의는 수치적 정의가 기저의 선택에 의존하지 않음을 함의할 것입니다.

## §9.7 부분공간과 편리한 기저 선택하기

**이 절의 대표적인 예:**  $\mathbb{R}^3$ 에서 임의의 선형독립인 두 벡터.

**정의 9.7.1.**  $M$ 을 왼쪽  $R$ -가군이라고 합시다.  $M$ 의 **부분가군**  $N$ 이란,  $N$ 의 모든 원소가 또한  $M$ 의 원소이기도 한 가군  $N$ 입니다.  $M$ 이 벡터 공간이면  $N$ 을 **부분공간**이라고 부릅니다.

### 예제 9.7.2 (핵)

사상  $T: V \rightarrow W$ 의 **핵**(kernel,  $\ker T$ 로 표기)은  $T(v) = 0_W$ 를 만족하는  $v \in V$ 의 집합입니다. 이는 덧셈과 스칼라배에 대해 닫혀 있으므로  $V$ 의 부분공간입니다(왜 그럴까요?).

### 예제 9.7.3 (생성 공간)

$V$ 를 벡터 공간이라고 하고  $v_1, \dots, v_m$ 을  $V$ 의 임의의 벡터들이라고 합시다. 이 벡터들의 **생성 공간**은 다음 집합으로 정의됩니다

$$\{a_1v_1 + \dots + a_mv_m \mid a_1, \dots, a_m \in k\}.$$

이 역시  $V$ 의 부분공간임에 유의하십시오!

**질문 9.7.4.** 왜 위의 각 예에서  $0_V$ 가 원소가 될까요? 일반적으로 왜 모든 부분공간은  $0_V$ 를 포함해야 할까요?

부분공간은 기저와 관련하여 좋은 성질을 가집니다.

### 정리 9.7.5 (기저 완성)

$V$ 를  $n$ 차원 공간이라 하고,  $V'$ 을  $V$ 의 부분공간이라고 합시다. 그러면

- (a)  $V'$  역시 유한차원입니다.
- (b)  $e_1, \dots, e_m$ 이  $V'$ 의 기저라면,  $V$  안에  $e_{m+1}, \dots, e_n$ 이 존재하여  $e_1, \dots, e_n$ 이  $V$ 의 기저가 됩니다.

증명. 직관적이며 증명이 그다지 유익하지 않으므로 생략합니다. (다만 이 결과를 이후 반복해서 사용할 것이므로, 지금 시간을 들여 내면화해 두십시오.)  $\square$

매우 흔한 사용 사례는 사상  $T$ 에 대해 편리한 기저를 고르는 것입니다.

**정리 9.7.6** (선형 사상에 대한 기저 고르기)

$T: V \rightarrow W$ 를 유한 차원 벡터 공간 사이의 사상이라 하고,  $n = \dim V$ ,  $m = \dim W$ 라 합시다. 그러면  $V$ 의 기저  $e_1, \dots, e_n$ 과  $W$ 의 기저  $f_1, \dots, f_m$ , 그리고 음이 아닌 정수  $k$ 가 존재하여 다음을 만족합니다

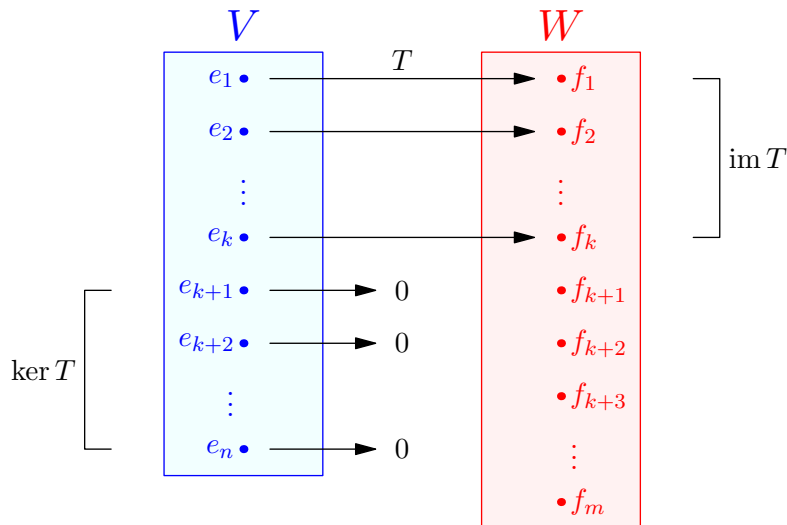
$$T(e_i) = \begin{cases} f_i & i \leq k \text{인 경우} \\ 0_W & i > k \text{인 경우.} \end{cases}$$

더욱이  $\dim \ker T = n - k$ 이고  $\dim T^{\text{img}}(V) = k$ 입니다.

증명 개요. 계속 읽기 전에 직접 시도해 보고 싶을 수도 있습니다: 이는 정리 9.7.5의 반복 적용입니다.

$\ker T$ 의 차원이  $n - k$ 라고 합시다.  $\ker T$ 의 기저로  $e_{k+1}, \dots, e_n$ 을 선택할 수 있습니다. 그런 다음 이를  $V$ 의 기저  $e_1, \dots, e_n$ 으로 확장합니다. 사상  $T$ 는  $e_1, \dots, e_k$ 의 생성 공간 위에서 단사입니다(핵에는 오직  $0_V$ 만 있으므로). 따라서  $W$ 에서의 그 상들은 선형독립입니다. 각  $i$ 에 대해  $f_i = T(e_i)$ 로 놓으면  $W$ 에서 어떤 선형독립인 집합을 얻습니다. 그런 다음 이를 다시  $W$ 의 기저로 확장합니다.  $\square$

이 정리는 응용 때문만이 아니라, 선형 사상이 어떤 모습이어야 하는지에 대한 올바른 그림을 여러분의 머릿속에 심어주기 때문에도 매우 중요합니다. 여러분이 확실히 기억하도록 이를 그림으로도 그려 보겠습니다:



특히  $T: V \rightarrow W$ 에 대해,  $V = \ker T \oplus V'$ 로 쓸 수 있으며, 이때  $T$ 는 자신의 핵을 소멸시키는 한편  $V'$ 는  $W$  안의 동형인 사본으로 보냅니다.

이것의 따름정리(어차피 예상했어야 할 내용입니다)는 이른바 계수-퇴화차수 정리(rank-nullity theorem)로, 이는 제1 동형사상 정리의 유사물입니다.

**정리 9.7.7** (계수-퇴화차수 정리)

$V$ 와  $W$ 를 유한 차원 벡터 공간이라 합시다.  $T: V \rightarrow W$ 이면 다음이 성립합니다

$$\dim V = \dim \ker T + \dim \text{im } T.$$

**질문 9.7.8.** 정리 9.7.6로부터 계수-퇴화차수 정리를 도출하십시오.

## §9.8 재미있는 응용: 라그랑주 보간법

고등학교 정리에 대한 선형대수학의 재미있는 응용<sup>2</sup>이 여기 있습니다.

### 정리 9.8.1 (라그랑주 보간법)

$x_1, \dots, x_{n+1}$ 을 서로 다른 실수라 하고,  $y_1, \dots, y_{n+1}$ 을 임의의 실수라 합시다. 그러면 모든  $i$ 에 대해

$$P(x_i) = y_i$$

를 만족하는 차수가  $n$  이하인 유일한 다항식  $P$ 가 존재합니다.

예를 들어  $n = 1$ 일 때, 이는 대략적으로 두 점을 잇는 직선이 유일하게 존재한다는 것을 말합니다.

증명. 아이디어는 차수가  $n$  이하인 다항식들의 벡터 공간  $V$ 와 벡터 공간  $W = \mathbb{R}^{n+1}$ 을 고려하는 것입니다.

**질문 9.8.2.**  $\dim V = n + 1 = \dim W$ 임을 확인하십시오. 이는  $V$ 에 대한 기저를 고르면 가장 쉽게 할 수 있지만, 이 연습문제를 마치고 나면 그 기저는 곧바로 잊어버려도 됩니다.

그런 다음 다음으로 주어지는 선형 사상  $T: V \rightarrow W$ 를 고려합니다

$$P \mapsto (P(x_1), \dots, P(x_{n+1})).$$

이것이 실제로 선형 사상인 이유는, 뒤,  $T(P+Q) = T(P) + T(Q)$ 이고  $T(cP) = cT(P)$ 이기 때문입니다. 이는 또한 단사이기도 합니다:  $P \in \ker T$ 이면  $P(x_1) = \dots = P(x_{n+1}) = 0$ 이지만,  $\deg P \leq n$ 이므로  $P$ 는 오직 영다항식일 수밖에 없습니다.

따라서  $T$ 는 같은 차원을 갖는 벡터 공간들 사이의 단사 사상입니다. 그러므로 문제 9B†에 의해 이는 실제로 전단사이며, 이것이 바로 우리가 원했던 것입니다.  $\square$

## §9.9 교육학적 여담: 숫자 배열은 사악하다

(이 절 전체는 선형대수학을 어떻게 가르칠지에 대한 예반의 수다이므로, 안심하고 건너뛰어도 됩니다.)

반복해서 강조하겠지만, 행렬은 두 벡터 공간 사이의 선형 사상을 나타냅니다. 그것을  $m \times n$  행렬의 형태로 쓰는 것은 그 사상을 구체적으로 보기 위한 매우 편리한 방법일 뿐입니다. 하지만 이는 이 사상이 실은 숫자들의 배열이 아니라 사상이라는 사실을 흐릿하게 만듭니다.

고등학교 미적분 예비 과정을 수강했다면, 모든 것이 행렬로 표현되는 것을 보게 됩니다. 전형적인 고등학생에게 행렬이란 숫자들의 배열입니다. 이 숫자들이 정확히 무엇을 나타내는지 아무도 확신하지 못하지만, 이 배열들을 마법처럼 곱해서 또 다른 배열을 얻는 방법을 배웁니다. 그들은 다음 행렬이

$$\begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

<sup>2</sup>출처: 첫 번째 하버드-MIT 학부생 수학 심포지엄에서 조 해리스가 저에게 전해준 것입니다.

다른 행렬과 곱해도 변하지 않기 때문에 "항등행렬"이라고 배웁니다. 그다음 행렬식이 이 기묘한 곱셈 규칙으로 만들어진 이 숫자들의 마법 같은 조합이라고 배웁니다.  $\det(AB) = \det A \det B$ 라는 사실과, 넓이와 행 연산 및 크라머 공식에 관한 무언가를 제외하고는, 이 행렬식이 무엇을 하는지 아무도 알지 못합니다.

그다음 대학에서 선형대수학을 배우게 되면, 이 숫자 배열들로 더 많은 마법을 부리게 됩니다. 두 행렬  $T_1$ 과  $T_2$ 가 어떤 가역행렬  $S$ 에 대해

$$T_2 = ST_1S^{-1}$$

를 만족하면 서로 닮음이라고 배웁니다. 행렬의 대각합  $\text{Tr } T$ 는 대각 성분들의 합이라고 배웁니다. 어떤 일인지 닮은 행렬을 보아도 이 값은 변하지 않지만, 왜 그런지는 확실히 알지 못합니다. 그다음 특성다항식을 다음과 같이 정의합니다

$$p_T(X) = \det(XI - T).$$

어떤 일인지 이것 역시 닮은 행렬을 취해도 변하지 않지만, 이제는 정말로 그 이유를 알지 못합니다. 그리고 온갖 흑마법 같은 케일리-해밀턴 정리를 만나게 됩니다:  $p_T(T)$ 는 영사상입니다. 호기심에 증명을 검색해 보면, 여전히 왜 참인지 전혀 알 수 없게 만드는 임기응변식 절차를 발견하게 됩니다.

이것은 끔찍합니다.  $T_2 = ST_1S^{-1}$ 의 무엇이 그리 특별합니까? 행렬이 선형 사상이라는 것을 알아야만 비로소 이것이 이해가 됩니다:  $T_2$ 는 그저 다른 기저 선택으로 다시 쓴  $T_1$ 일 뿐입니다.

저는 정말로 그 반대 관점을 밀어붙이고 싶습니다. 선형대수학은 선형 사상에 관한 학문이지만, 숫자 배열에 관한 학문으로 가르쳐지며, 이 숫자들이 무엇을 의미하는지 아무도 알지 못합니다. 그리고 그럴 만한 이유가 있습니다: 그 숫자들은 무의미하기 때문입니다. 그것들은 행렬을 부호화하는 매우 편리한 방법일 뿐, 역사에서 사건의 날짜가 주된 연구 대상이 아니듯이 주된 연구 대상은 아닙니다.

또 다른 큰 단점은 사람들이 존재하는 유일한 (실수) 벡터 공간이  $\mathbb{R}^{\oplus n}$ 이라는 인상을 받게 된다는 것입니다. **비고 9.5.5**에서 설명했듯이, 영혼 없는 로봇이라면 이런 방식으로 작업할 수는 있지만, 인간이 그렇게 하는 것은 매우 부자연스럽습니다.

제가 하버드 신입생 시절 Math 55a를 수강했을 때, 저는 정반대의 대우를 받았습니다: 우리는 행렬을 단 하나도 쓰지 않고 선형대수학 전체를 배웠습니다. 그 시간 내내 저는 상당히 혼란스러웠습니다. 기저가 뭐가 문제란 말입니까? 저는 나중에야 이 접근법이 이 주제를 다루는 도덕적으로 올바른 방식이었다는 것을 깨달았습니다: 그것은 무슨 일이 일어나고 있는지를 명확하게 해주었습니다.

Napkin 전체에 걸쳐, 저는 이 두 접근법 사이의 균형을 잡으려 노력했으며, 적절할 때는 행렬을 사용하여 사상을 예시하고 증명을 단순화하되, 궁극적으로는 정리와 정의를 도덕적으로 올바른 형태로 서술했습니다. 저는 이것이 "옳은" 정의를 제공하면서도 소화할 수 있을 만큼 구체적이라는 이점을 모두 갖추기를 바랍니다. 하지만 기록을 위해 말씀드리자면, 고등학교식 접근법과 55a식 접근법 중 하나를 골라야 한다면, 저는 망설임 없이 55a를 고르겠습니다.

## §9.10 일반적인 가군에 관한 한마디

**이 절의 대표적인 예:**  $\mathbb{Z}[\sqrt{2}]$ 는 계수 2인  $\mathbb{Z}$ -가군입니다.

저는 이 장에서 단순함을 위해 주로 벡터 공간(즉 체 위의 가군)에 초점을 맞추었으므로, 마무리하기 전에 일반적인 가환환  $R$  위의 가군에 관해 몇 가지 언급을 하고 싶습니다.

먼저, 일반적인 가군에서는 "펼침 집합" 대신 "생성 집합"이라고 부른다는 점을 기억하십시오. 어쩔 수 없는 일입니다.

환에서의 주된 문제는 우리의 핵심 정리인 **정리 9.4.5**가 극적으로 실패한다는 것입니다. 예를 들어,  $\mathbb{Z}$ 를 그 자신 위의  $\mathbb{Z}$ -가군으로 생각해 봅시다. 그러면  $\{2\}$ 는 선형독립이지만

기저로 확장될 수 없습니다. 마찬가지로  $\{2, 3\}$ 은 생성 집합이지만 기저로 줄일 수 없습니다. 차원을 정의하는 것이 왜 어려울지 알 수 있을 것입니다.

그럼에도 불구하고, 위의 정의들 중 몇 가지에 대한 유사한 개념은 여전히 존재합니다.

**정의 9.10.1.**  $R$ -가군  $M$ 은 유한한 생성 집합을 가질 때 **유한생성**이라고 불립니다.

**정의 9.10.2.**  $R$ -가군  $M$ 은 기저를 가질 때 **자유**롭다고 불립니다. 앞서 말했듯이 차원 정리의 유사한 결과가 성립하며, 우리는 기저의 크기를 나타내기 위해 **계수**라는 단어를 사용합니다. 앞에서와 마찬가지로,  $n$ 이 계수일 때 동형사상  $M \cong R^{\oplus n}$ 이 존재합니다.

### 예제 9.10.3 ( $\mathbb{Z}$ -가군의 예시)

$\mathbb{Z}$ -가군

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$$

$\{1, \sqrt{2}\}$ 을 기저로 가지므로, 이를 계수(rank) 2의 자유  $\mathbb{Z}$ -가군이라고 합니다.

**표기의 남용 9.10.4** (군에 대한 표기법). 아벨 군은  $\mathbb{Z}$ -가군으로 볼 수 있다는 것을 기억하십시오 (사실 그 역도 성립합니다!). 그러므로 우리는 이러한 용어들을 아벨 군에도 적용할 수 있습니다 (그리고 실제로 그렇게 할 것입니다). 우리는 두 아벨 군  $G$ 와  $H$ 의 데카르트 곱을 나타내기 위해  $G \oplus H$ 라는 표기법을 사용하여,  $G$ 와  $H$ 가 아벨 군이라는 사실을 강조할 것입니다. 이는 우리가 대수적 수론과 호몰로지 군을 공부할 때 일어날 것입니다.

## §9.11 생각해 볼 만한 조금 더 어려운 문제

일반적인 힌트: **정리 9.7.6**가 이러한 문제들 대부분에서 여러분의 가장 좋은 친구가 되어 줄 것입니다.

**문제 9A<sup>†</sup>.**  $V$ 와  $W$ 를 0이 아닌 차원을 갖는 유한차원 벡터 공간이라 하고, 선형 사상  $T: V \rightarrow W$ 를 생각합시다. 각 항목에 "때때로", "항상", "결코 아님" 중 하나를 적어 다음 표를 완성하십시오.

|                           | $T$ 단사 | $T$ 가 전사 | $T$ 가 동형사상 |
|---------------------------|--------|----------|------------|
| $\dim V > \dim W$ 인 경우... |        |          |            |
| $\dim V = \dim W$ 인 경우... |        |          |            |
| $\dim V < \dim W$ 인 경우... |        |          |            |

**문제 9B<sup>†</sup>** (차원이 같은 벡터 공간은 대개 동형사상입니다).  $\dim V = \dim W$ 인 유한 차원 벡터 공간  $V$ 와  $W$ 가 있다고 합시다. 사상  $T: V \rightarrow W$ 에 대해 다음이 동치임을 증명하십시오:

- $T$ 가 단사이다,
- $T$ 가 전사이다,
- $T$ 는 전단사입니다.

**문제 9C.** 마방진을 모든 대각선, 열, 행의 합이 같은  $3 \times 3$  실수 행렬이라고 합시다, 예를 들어  $\begin{bmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{bmatrix}$ . 덧셈에 대한 실수 벡터 공간으로서, 마방진들의 집합의 차원을 구하십시오.

**문제 9D** ( $\sqrt{5}$ 에 의한 곱셈).  $V = \mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5}\}$ 를 2차원  $\mathbb{Q}$ -벡터 공간이라 하고, 그 기저로  $\{1, \sqrt{5}\}$ 를 고정합시다.  $\sqrt{5}$ 에 의한 곱셈에 해당하는 유리수 계수의  $2 \times 2$  행렬을 적으십시오.

**문제 9E** (다변수 라그랑주 보간법).  $S \subset \mathbb{Z}^2$ 을  $n$ 개의 격자점으로 이루어진 집합이라 합시다. 차수가 최대  $\sqrt{2n}$ 이고 실수 계수를 갖는 영이 아닌 이변수 다항식  $p$ 가 존재하여, 모든  $(x, y) \in S$ 에 대해  $p(x, y) = 0$ 이 성립함을 증명하십시오.

**문제 9F** (Putnam 2003). 다음을 만족하는 다항식  $a(x)$ ,  $b(x)$ ,  $c(y)$ ,  $d(y)$ 가 존재합니까?

$$1 + xy + (xy)^2 = a(x)c(y) + b(x)d(y)$$

항등적으로 성립합니까?



**문제 9G** (TSTST 2014).  $P(x)$ 와  $Q(x)$ 를 실수 계수를 갖는 임의의 다항식이라 하고,  $d$ 를  $P(x)$ 의 차수라고 합시다.  $P(x)$ 가 영 다항식이 아니라고 가정합니다. 다음을 만족하는 다항식  $A(x)$ 와  $B(x)$ 가 존재함을 증명하십시오:

- (i)  $A$ 와  $B$  모두 차수가 최대  $d/2$ 이다,
- (ii)  $A$ 와  $B$  중 많아야 하나가 영 다항식이다,
- (iii)  $P$ 는  $A + Q \cdot B$ 를 나눕니다.

**문제 9H\*** (역등원은 사영 사상입니다).  $P: V \rightarrow V$ 가 선형 사상이라 하고,  $V$ 는 벡터 공간 (반드시 유한 차원일 필요는 없음)이라 합시다.  $P$ 가 **멱등**이라고 가정합니다. 즉 각  $v \in V$ 에 대해  $P(P(v)) = P(v)$ 이거나, 동등하게  $P$ 가 자신의 상 위에서 항등사상이라고 합시다. 다음을 증명하십시오.

$$V = \ker P \oplus \operatorname{im} P.$$

따라서  $P$ 를 부분공간  $\operatorname{im} P$  위로의 사영으로 생각할 수 있습니다.



**문제 9I\***.  $V$ 가 유한 차원 벡터 공간이라 합시다.  $T: V \rightarrow V$ 가 선형 사상이라 하고,  $T^n: V \rightarrow V$ 는  $T$ 를  $n$ 번 적용한 것을 나타낸다고 합시다. 다음을 만족하는 정수  $N$ 이 존재함을 증명하십시오.

$$V = \ker T^N \oplus \operatorname{im} T^N.$$

# 10 고유한 것들

이 장에서는 고윳값과 고유벡터의 이론, 이른바 "조르당 표준형(Jordan canonical form)"을 소개합니다. (이후에는 이를 이용하여 특성다항식을 정의할 것입니다.)

## §10.1 관심을 가져야 하는 이유

정사각행렬  $T$ 는 사실상  $V$ 에서  $V$ 로 가는 선형 사상일 뿐입니다. 가장 단순한 형태의 선형 사상은 무엇일까요? 그것은 단순히 어떤 스칼라  $\lambda$ 를 곱하는 것으로, 이는 (어떤 기저에서든!) 다음과 같은 행렬을 갖습니다

$$T = \begin{bmatrix} \lambda & 0 & \dots & 0 \\ 0 & \lambda & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda \end{bmatrix}.$$

하지만 이는 어쩌면 지나치게 단순합니다. 만약 고정된 기저  $e_1, \dots, e_n$ 가 있다면, 또 다른 매우 "단순한" 연산은 각 기저 원소  $e_i$ 를  $\lambda_i$ 로 스케일하는 것, 즉 다음과 같은 형태의 **대각 행렬(diagonal matrix)**일 것입니다

$$T = \begin{bmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{bmatrix}.$$

이러한 사상은 더 일반적입니다. 실제로 예를 들어  $T^{100}$ 을 순식간에 계산할 수 있습니다: 이 사상은  $e_i \mapsto \lambda_i^{100} e_i$ 로 보냅니다. (임의의  $n \times n$  행렬로 그렇게 해보십시오.)

물론 대부분의 선형 사상은 아마 그렇게 좋지 않을 것입니다. 정말 그럴까요?

### 예제 10.1.1 (운이 좋은 경우)

$V$ 를  $e_1$ 과  $e_2$ 를 기저 원소로 갖는 어떤 2차원 벡터 공간이라 합시다.  $e_1 \mapsto 2e_1$ 이고  $e_2 \mapsto e_1 + 3e_2$ 인 사상  $T: V \rightarrow V$ 를 생각해 봅시다. 이는 다음과 같이 구체적으로 쓸 수도 있습니다

$$T = \begin{bmatrix} 2 & 1 \\ 0 & 3 \end{bmatrix} \quad \text{기저 } e_1, e_2 \text{에서.}$$

이는 다음과 같이 다시 쓸 수 있음을 깨닫기 전까지는 전혀 좋아 보이지 않습니다

$$\begin{aligned} e_1 &\mapsto 2e_1 \\ e_1 + e_2 &\mapsto 3(e_1 + e_2). \end{aligned}$$

이제 기저를  $e_1$ 과  $e_1 + e_2$ 로 바꾼다고 합시다. 그러면 새로운 기저에서는

$$T = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix} \quad \text{기저 } e_1, e_1 + e_2 \text{에서.}$$

이렇게 우리의 완전히 무작위로 보이던 사상이, 적절한 기저 변환 아래에서는 앞서 설명한 매우 좋은 사상들처럼 보입니다!

이 장에서 우리는 그러한 운을 만들어낼 것이며, 행렬에 대한 더 나은 이해가 이를 생각하는 올바른 방법을 준다는 것을 보게 될 것입니다.

## §10.2 가정에 관한 주의사항

이 장의 대부분의 정리는 다음의 경우에만 성립합니다

- 유한 차원 벡터 공간  $V$ 에 대하여,
- 대수적으로 닫힌 체  $k$  위에서.

반면 정의는 이러한 가정 없이도 잘 성립합니다.

## §10.3 고유벡터와 고윳값

$k$ 를 체라 하고  $V$ 를 그 위의 벡터 공간이라 합시다. 위의 예에서 우리는  $V$ 에 대해 매우 단순한 작용을 하는 두 개의 매우 좋은 벡터,  $e_1$ 과  $e_1 + e_2$ 가 있음을 보았습니다. 당연히 이러한 벡터들에는 이름이 있습니다.

**정의 10.3.1.**  $T: V \rightarrow V$ 이고  $v \in V$ 를 영이 아닌 벡터라 합시다. 어떤  $\lambda \in k$ 에 대해  $T(v) = \lambda v$ 이면 (영일 수도 있지만,  $v \neq 0$ 임을 기억하십시오)  $v$ 를 **고유벡터(eigenvector)**라고 합니다. 값  $\lambda$ 는  $T$ 의 **고윳값(eigenvalue)**이라고 합니다.

때로는 " $v$ 는 고윳값  $\lambda$ 를 갖는 고유벡터이다"를 간단히 " $v$ 는  $\lambda$ -고유벡터이다"로 줄여 쓸 것입니다.

물론, 어디에도 기저에 대한 언급은 없습니다.

### 예제 10.3.2 (고유벡터와 고윳값의 예)

$T = \begin{bmatrix} 2 & 1 \\ 0 & 3 \end{bmatrix}$ 을 사용한 앞의 예를 생각해 봅시다.

- $e_1$ 과  $e_1 + e_2$ 는 각각 2-고유벡터와 3-고유벡터임에 유의하십시오.
- 물론  $5e_1$  또한 2-고유벡터입니다.
- 그리고  $7e_1 + 7e_2$  또한 3-고유벡터입니다.

그러므로 다음 관찰을 빠르게 확인할 수 있습니다.

**질문 10.3.3.**  $\lambda$ -고유벡터들이  $\{0\}$ 과 함께 부분공간을 이룸을 보이십시오.

**정의 10.3.4.** 임의의  $\lambda$ 에 대해,  $\lambda$ -**고유공간**을  $\lambda$ -고유벡터들과 0을 함께 모은 집합으로 정의합니다.

이를 통해 "2는  $T$ 의 고윳값이며 그 고유공간은  $e_1$ 이 생성하는 1차원 공간이다"라고 간결하게 서술할 수 있습니다.

안타깝게도, 고윳값이 항상 존재한다는 것은 정확히 참이 아닙니다.

### 예제 10.3.5 (고윳값은 존재하지 않을 수도 있습니다)

$V = \mathbb{R}^2$ 이라 하고,  $T$ 를 원점을 중심으로 벡터를  $90^\circ$  회전시키는 사상이라 합시다. 그

려면 자명한 경우인  $v = 0$ 을 제외하면, 어떠한  $v \in V$ 에 대해서도  $T(v)$ 는  $v$ 의 배수가 아닙니다.

그러나  $k$ 를 대수적으로 닫힌 체로 바꾸면 이는 참입니다.<sup>1</sup>

### 정리 10.3.6 (대수적으로 닫힌 체 위에서는 고윳값이 항상 존재합니다)

$k$ 가 대수적으로 닫힌 체라고 가정합시다.  $V$ 를 유한 차원  $k$ -벡터 공간이라고 합시다. 그러면  $T: V \rightarrow V$ 가 선형 사상이면, 고윳값  $\lambda \in k$ 가 존재합니다.

증명. ([Ax97]에서 인용) 이 증명의 핵심 아이디어는  $T$ 에 대한 “다항식”을 고려하는 것입니다. 예를 들어  $2T^2 - 4T + 5$ 는  $2T(T(v)) - 4T(v) + 5v$ 의 축약 표기입니다. 이런 식으로 “다항식”  $P(T)$ 를 고려할 수 있으며, 이를 통해 “대수적으로 닫혀 있다”라는 조건을 결부시킬 수 있습니다. 이 다항식들은 다음과 같이 잘 작동합니다:

**질문 10.3.7.**  $P(T) + Q(T) = (P + Q)(T)$ 이고  $P(T) \circ Q(T) = (P \cdot Q)(T)$ 임을 보이십시오.

$n = \dim V < \infty$ 라 하고 임의의 0이 아닌 벡터  $v \in V$ 를 고정한 다음, 벡터  $v, T(v), \dots, T^n(v)$ 를 생각해 봅시다. 이들은  $n + 1$ 개이므로 차원상의 이유로 선형독립일 수 없습니다. 따라서  $v$ 에 적용했을 때  $P(T)$ 가 0이 되는 0이 아닌 다항식  $P$ 가 존재합니다. 일반성을 잃지 않고  $P$ 가 모닉 다항식이라 하면,  $P(z) = (z - r_1) \dots (z - r_m)$ 이라 할 수 있습니다. 그러면 다음을 얻습니다

$$0 = (T - r_1 \text{id}) \circ (T - r_2 \text{id}) \circ \dots \circ (T - r_m \text{id})(v)$$

( $\text{id}$ 는 항등행렬입니다). 이는  $T - r_i \text{id}$  중 적어도 하나는 단사가 아니라는 것, 즉 자명하지 않은 핵을 가진다는 것을 의미하며, 이는 고유벡터를 가지는 것과 같습니다.  $\square$

그래서 일반적으로 우리는 대수적으로 닫힌 체를 고려하는 것을 선호합니다. 이는 큰 손실이 아닙니다: 예를 들어, 임의의 실행렬은 그 성분이 우연히 실수인 복소행렬로 해석할 수 있습니다.

## §10.4 조르당 형식

제가 어디로 향하는지 정확히 알 수 있도록, 여기 주요 정리를 소개합니다.

**정의 10.4.1.** **조르당 블록**은 다음과 같은 형태의  $n \times n$  행렬입니다.

$$\begin{bmatrix} \lambda & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & \lambda & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & \lambda & 1 & \dots & 0 & 0 \\ 0 & 0 & 0 & \lambda & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & \lambda & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 & \lambda \end{bmatrix}.$$

다시 말해, 대각선 위에는  $\lambda$ 가, 그 바로 위에는 1이 있습니다.  $n = 1$ 도 허용하므로,  $[\lambda]$ 도 조르당 블록입니다.

<sup>1</sup>체가 **대수적으로 닫혀 있다**는 것은 그 체의 모든 다항식이 근을 가짐을 뜻하며, 그 대표적인 예가  $\mathbb{C}$ 입니다.

**정리 10.4.2 (조르당 표준형)**

$T: V \rightarrow V$ 가 대수적으로 닫힌 체  $k$  위의 유한 차원 벡터 공간들 사이의 선형 사상이라고 합시다. 그러면  $V$ 의 기저를 적절히 선택하여, 각 블록이 조르당 블록이 되도록 행렬  $T$ 가 “블록 대각”이 되게 할 수 있습니다.

이러한 행렬을 **조르당 형식**이라고 합니다. 이 형식은 블록들의 순서를 재배열하는 것을 제외하면 유일합니다.

예를 들어, 이는 행렬이 다음과 같은 모습이어야 함을 의미합니다:

$$\begin{bmatrix} \lambda_1 & 1 & & & & \\ 0 & \lambda_1 & & & & \\ & & \lambda_2 & & & \\ & & & \lambda_3 & 1 & 0 \\ & & & 0 & \lambda_3 & 1 \\ & & & 0 & 0 & \lambda_3 \\ & & & & & \ddots \\ & & & & & & \lambda_m & 1 \\ & & & & & & 0 & \lambda_m \end{bmatrix}$$

**질문 10.4.3.** 각 블록이  $1 \times 1$ 일 때가 대각행렬의 특수한 경우임을 확인하십시오.

이것은 무엇을 의미할까요? 기본적으로, 이는 우리의 꿈이 거의 실현되었음을 의미합니다. 여기서 일어나는 일은  $V$ 가 다음과 같은 직합으로 분해될 수 있다는 것입니다

$$V = J_1 \oplus J_2 \oplus \cdots \oplus J_m$$

그리고  $T$ 는 이 부분공간들 각각에 독립적으로 작용합니다. 이 부분공간들은 위 행렬의 블록들에 대응됩니다. 가장 단순한 경우,  $\dim J_i = 1$ 이므로,  $J_i$ 는  $T(e) = \lambda_i e$ 를 만족하는 기저 원소  $e$ 를 가지게 됩니다. 다시 말해, 우리는 단순히 단순 고윳값을 가지는 것입니다. 하지만 때로는 상황이 그리 단순하지 않아서, 1보다 큰 크기의 블록을 가지게 되는데, 이는 대각선 바로 위에 1들이 나타나게 만듭니다.

1들을 어떻게 해석해야 하는지는, 제가 하강 계단이라는 단어를 만들 때 나중에 설명하겠습니다. 지금은  $\dim J_i \geq 2$ 이더라도, 우리는 여전히 고윳값  $\lambda_i$ 를 가지는 고유벡터인 기저 원소를 가진다는 점에 주목하십시오.

**예제 10.4.4 (조르당 표준형의 구체적인 예시)**

$T: k^6 \rightarrow k^6$ 이라 하고,  $T$ 가 다음 행렬로 주어진다고 합시다

$$T = \begin{bmatrix} 5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 7 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \end{bmatrix}.$$

행렬을 읽으면, 우리는 모든 고유벡터와 고윳값을 계산할 수 있습니다. 임의의 상수

$a, b \in k$ 에 대해 우리는 다음을 가집니다

$$T(a \cdot e_1) = 5a \cdot e_1$$

$$T(a \cdot e_2) = 2a \cdot e_2$$

$$T(a \cdot e_4) = 7a \cdot e_4$$

$$T(a \cdot e_5 + b \cdot e_6) = 3[a \cdot e_5 + b \cdot e_6].$$

반면 원소  $e_3$ 는  $T(e_3) = e_2 + 2e_3$ 이므로 고유벡터가 아닙니다.

## §10.5 멱영 사상

잠시만 참아 주십시오. 먼저, 다음과 같이 정의합니다:

**정의 10.5.1.** 사상  $T: V \rightarrow V$ 는, 어떤 정수  $m$ 에 대해  $T^m$ 이 영사상이면 **멱영**이라고 합니다. (여기서  $T^m$ 은 " $T$ 를  $m$ 번 적용한 것"을 의미합니다.)

멱영 사상의 예시는 무엇일까요?

### 예제 10.5.2 ("하강 계단")

$V = k^{\oplus 3}$ 이 기저  $e_1, e_2, e_3$ 을 가진다고 합시다. 그러면 다음을 보내는 사상  $T$ 는

$$e_3 \mapsto e_2 \mapsto e_1 \mapsto 0$$

$T(e_1) = T^2(e_2) = T^3(e_3) = 0$ 이므로 멱영이며, 따라서 모든  $v \in V$ 에 대해  $T^3(v) = 0$ 입니다.

$3 \times 3$  하강 계단은 다음과 같은 행렬 표현을 가집니다

$$T = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}.$$

이것이 조르당 블록임을 알아차리실 것입니다.

**연습문제 10.5.3.** 위의 하강 계단이 0을 유일한 고윳값으로 가짐을 보이십시오.

이것은 꽤 좋은 예시입니다. 또 다른 예시로, 우리는 이러한 계단을 여러 개 가질 수 있습니다.

### 예제 10.5.4 (이중 계단)

$V = k^{\oplus 5}$ 가 기저  $e_1, e_2, e_3, e_4, e_5$ 를 가진다고 합시다. 그러면 다음 사상은

$$e_3 \mapsto e_2 \mapsto e_1 \mapsto 0 \text{ 그리고 } e_5 \mapsto e_4 \mapsto 0$$

멱영입니다.

강조를 위해 일부 0을 생략한 그림입니다.

$$T = \begin{bmatrix} 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \\ 0 & 0 & 0 & & \\ & & & 0 & 1 \\ & & & 0 & 0 \end{bmatrix}$$

이것이 앞의 예와 실제로 그리 다르지 않다는 것을 알 수 있는데, 같은 아이디어가 여러 번 반복된 것에 불과합니다. 그리고 실제로 이제 우리는 모든 멱영 사상이 본질적으로 그러한 형태를 가진다고 주장합니다.

#### 정리 10.5.5 (멱영 조르당)

$V$ 가 대수적으로 닫힌 체  $k$  위의 유한 차원 벡터 공간이라고 합시다.  $T: V \rightarrow V$ 가 멱영 사상이라고 합시다. 그러면  $V = \bigoplus_{i=1}^m V_i$ 로 쓸 수 있는데, 여기서 각  $V_i$ 는 어떤  $v_i \in V_i$ 에 대해  $v_i, T(v_i), \dots, T^{\dim V_i - 1}(v_i)$  형태의 기저를 가지며,  $T^{\dim V_i}(v_i) = 0$ 을 만족합니다.

따라서:

**모든 멱영 사상은 독립적인 계단들로 볼 수 있습니다.**

각 사슬  $v_i, T(v_i), T(T(v_i)), \dots$  는 그저 하나의 계단일 뿐입니다. 증명은 나중에 제시하겠지만, 먼저 이것이 어디로 향하는지 짚어보겠습니다.

여기 핵심이 있습니다. 다시 이중 계단을 살펴봅시다. 이를 행렬로 나타내면, 예를 들어

$$S = \begin{bmatrix} 0 & 1 & 0 & & \\ 0 & 0 & 1 & & \\ 0 & 0 & 0 & & \\ & & & 0 & 1 \\ & & & 0 & 0 \end{bmatrix}.$$

그러면 다음을 계산할 수 있습니다

$$S + \lambda \text{id} = \begin{bmatrix} \lambda & 1 & 0 & & \\ 0 & \lambda & 1 & & \\ 0 & 0 & \lambda & & \\ & & & \lambda & 1 \\ & & & 0 & \lambda \end{bmatrix}.$$

$\lambda$  조르당 블록들이 잔뜩 나옵니다! 이는 우리에게 나아갈 방향을 제시해 줍니다:  $V$ 를 여러 부분공간으로 쪼개어 각 부분공간에서  $T - \lambda \text{id}$ 가 멱영이 되도록 해야 합니다. 그러면 멱영 조르당 정리가 나머지를 마무리해 줄 것입니다.

## §10.6 멱영인 경우로의 환원

**정의 10.6.1.**  $T: V \rightarrow V$ 라 합시다. 부분공간  $W \subseteq V$ 는 임의의  $w \in W$ 에 대해  $T(w) \in W$  일 때  $T$ -**불변**이라고 부릅니다. 이렇게 하면  $T$ 는 사상  $W \rightarrow W$ 로 생각할 수 있습니다.

이런 식으로, 조르당 표준형은  $V$ 를 불변 부분공간들로 분해한 것입니다.

이제 조금 편한 방법을 써서, 다음과 같이 정의하겠습니다:

**정의 10.6.2.** 사상  $T: V \rightarrow V$ 는,  $W_1$ 과  $W_2$ 가 모두 자명하지 않은  $T$ -불변 공간인  $V = W_1 \oplus W_2$ 를 쓰는 것이 불가능할 때 **분해 불가능**하다고 부릅니다.

분해 가능한 사상의 그림:

$$\left[ \begin{array}{c|ccc} W_1 & 0 & 0 & 0 \\ \hline 0 & 0 & & \\ 0 & 0 & & \\ 0 & 0 & & \end{array} \right] \begin{array}{c} \\ \\ W_2 \\ \end{array}$$

예상하시다시피, 공간을 "분해 불가능한" 부분들로 쪼갤 수 있습니다.

### 명제 10.6.3 (불변 부분공간 분해)

$V$ 를 유한 차원 벡터 공간이라 합시다. 임의의 사상  $T: V \rightarrow V$ 가 주어지면, 다음과 같이 쓸 수 있습니다

$$V = V_1 \oplus V_2 \oplus \cdots \oplus V_m$$

여기서 각  $V_i$ 는  $T$ -불변이며, 임의의  $i$ 에 대해 사상  $T: V_i \rightarrow V_i$ 는 분해 불가능합니다.

증명. 모든 정수가 소수의 곱이라는 증명과 같습니다.  $V$ 가 분해 가능하지 않다면 증명이 끝납니다. 그렇지 않다면, 정의에 따라  $V = W_1 \oplus W_2$ 로 쓰고  $W_1$ 과  $W_2$  각각에 대해 반복합니다.  $\square$

놀랍게도, 이것만으로도 거의 끝난 셈입니다! 위와 같은 분해를 생각해 봅시다. 즉  $T: V_1 \rightarrow V_1$ 이 분해 불가능한 사상이라고 합시다. 그러면  $T$ 는 고윳값  $\lambda_1$ 을 가지므로,  $S = T - \lambda_1 \text{id}$ 라 하면  $\ker S \neq \{0\}$ 입니다.

**질문 10.6.4.**  $V_1$ 이 또한  $S$ -불변임을 보이십시오. 따라서  $S: V_1 \rightarrow V_1$ 을 고려할 수 있습니다.

**문제 9I\***에 의해, 다음을 얻습니다

$$V_1 = \ker S^N \oplus \text{im } S^N$$

어떤  $N$ 에 대해서 말입니다. 그런데  $T$ 가 분해 불가능하다고 가정했으므로, 이는  $\text{im } S^N = \{0\}$ 이고  $\ker S^N = V_1$ 일 때만 일어날 수 있습니다( $\ker S^N$ 이 우리의 고유벡터를 포함하기 때문입니다). 따라서  $S$ 는 멱영이므로 계단들의 모임입니다. 사실,  $T$ 가 분해 불가능하므로 계단은 오직 하나뿐입니다. 따라서  $V_1$ 은 원하는 대로 조르당 블록입니다.

## §10.7 (선택 사항) 멱영 조르당 정리의 증명

증명은 그저  $\dim V$ 에 대한 귀납법입니다.  $\dim V \geq 1$ 이라 가정하고,  $W = T^{\text{img}}(V)$ 를  $V$ 의 상이라 합시다.  $T$ 가 멱영이므로  $W \subseteq V$ 일 수밖에 없습니다. 더욱이,  $W = \{0\}$ 이면(즉  $T$ 가 영사상이면) 이미 증명이 끝납니다. 따라서  $\{0\} \subsetneq W \subsetneq V$ 라 가정합니다.

귀납 가정에 의해,  $W$ 의 좋은 기저를 선택할 수 있습니다:

$$\mathcal{B}' = \left\{ \begin{array}{l} T(v_1), T(T(v_1)), T(T(T(v_1))), \dots \\ T(v_2), T(T(v_2)), T(T(T(v_2))), \dots \\ \dots, \\ T(v_\ell), T(T(v_\ell)), T(T(T(v_\ell))), \dots \end{array} \right\}$$

어떤  $T(v_i) \in W$ 에 대해서 말입니다(여기서  $W$ 의 각 원소가 그 자체로 어떤  $v$ 에 대해  $T(v)$ 의 형태라는 사실을 활용했습니다).

또한,  $B'$ 의 원소 중 정확히  $\ell$ 개가  $\ker T$ 에 속함을 주목하십시오(즉  $\ell$ 개의 계단 각각의 마지막 원소입니다). 따라서 이를 확장하여 기저  $v_{\ell+1}, \dots, v_m$ 을 만들 수 있습니다(여기서  $m = \dim \ker T$ 입니다). (다시 말해, 각 계단의 마지막 원소와 새로 추가된  $m - \ell$ 개의 원소가  $\ker T$ 의 기저를 이룹니다.)

이제 다음을 고려합시다

$$B = \left\{ v_1, T(v_1), T(T(v_1)), T(T(T(v_1))), \dots, v_2, T(v_2), T(T(v_2)), T(T(T(v_2))), \dots, \dots, v_\ell, T(v_\ell), T(T(v_\ell)), T(T(T(v_\ell))), \dots, v_{\ell+1}, v_{\ell+2}, \dots, v_m \right\}.$$

**질문 10.7.1.** 원소가 정확히  $\ell + \dim W + (\dim \ker T - \ell) = \dim V$ 개 있음을 확인하십시오.

**연습문제 10.7.2.** 모든 원소가 선형독립임을 보이십시오. (귀류법으로 어떤 선형종속 관계가 있다고 가정한 다음, 양변에  $T$ 를 취하십시오.)

따라서  $B$ 는 원하는 형태의 기저입니다.

## §10.8 대수적 중복도와 기하적 중복도

**이 절의 대표적인 예:** 아래의 행렬  $T$ .

이는 편리한 표기법입니다: 조르당 형식으로 된 행렬을 살펴봅시다

$$T = \begin{bmatrix} 7 & 1 & & & \\ 0 & 7 & & & \\ & & 9 & & \\ & & & 7 & 1 & 0 \\ & & & 0 & 7 & 1 \\ & & & 0 & 0 & 7 \end{bmatrix}.$$

여러 번 등장하는 고윳값 7에 주목합니다. 이는 분명히 "중복"됩니다. 하지만 이것이 중복된다고 말할 수 있는 서로 다른 두 가지 의미가 있습니다.

- 대수적: 대각선에 다섯 번 등장하므로 다섯 번 중복된다고 말할 수 있습니다.
- 기하적: 실제로는 두 번만 등장한다고 말할 수 있습니다. 고윳값 7을 갖는 고유벡터는  $e_1$ 과  $e_4$  단 두 개뿐이기 때문입니다.

실제로 예를 들어 벡터  $e_2$ 는  $T(e_2) = 7e_2 + e_1$ 을 만족하므로 진정한 고유벡터가 아닙니다! 하지만  $e_2$ 에  $T - 7\text{id}$ 를 두 번 적용하면 정말로 영이 됩니다.

**질문 10.8.1.** 이 예제에서  $e_6$ 에  $T - 7\text{id}$ 를 몇 번 적용해야 영이 되겠습니까?

두 개념 모두 타당하므로 둘 다 이름을 붙이겠습니다. 일반성을 유지하기 위해 먼저 "본질적인" 정의를 서술하겠습니다.

**정의 10.8.2.**  $T: V \rightarrow V$ 를 선형 사상이라 하고  $\lambda$ 를 스칼라라 합시다.

- $\lambda$ 의 **기하적 중복도**는  $\lambda$ -고유공간의 차원  $\dim V_\lambda$ 입니다.
- **일반화된 고유공간**  $V^\lambda$ 를 어떤  $n \geq 1$ 에 대해  $(T - \lambda \text{id})^n(v) = 0$ 을 만족하는  $V$ 의 부분공간으로 정의합니다.  $\lambda$ 의 **대수적 중복도**는 차원  $\dim V^\lambda$ 입니다.

(사소한 경계 사례:  $\lambda$ 가 애초에 고윳값이 아닌 경우 "중복도 영"을 허용합니다.)

하지만 실제로는 그저 조르당 블록의 개수를 세면 됩니다.

**예제 10.8.3** (조르당 형식을 통한 고유공간의 예)

앞서 언급한 행렬  $T$ 를 그대로 사용하고  $\lambda = 7$ 이라 합시다.

- 고유공간  $V_\lambda$ 는 기저  $e_1$ 과  $e_4$ 를 가지므로 기하적 중복도는 2입니다.
- 일반화된 고유공간  $V^\lambda$ 는 기저  $e_1, e_2, e_4, e_5, e_6$ 을 가지므로 대수적 중복도는 5입니다.

완전히 명시적으로 설명하자면, 실제로는 다음과 같이 생각하면 됩니다:

**명제 10.8.4** (조르당 블록에 대한 기하적 중복도와 대수적 중복도)

$T: V \rightarrow V$ 가 유한 차원 벡터공간 사이의 선형 사상이며 조르당 형식으로 쓰여 있다고 가정합니다.  $\lambda$ 를 스칼라라 합시다. 그러면

- $\lambda$ 의 기하적 중복도는 고윳값  $\lambda$ 를 갖는 조르당 블록의 개수이며, 고유공간은 각 조르당 블록마다 하나씩의 기저 원소를 가집니다.
- $\lambda$ 의 대수적 중복도는 고윳값  $\lambda$ 를 갖는 조르당 블록들의 차원의 합이며, 고유공간은 그 블록들에 대응하는 부분공간들의 직합입니다.

증명. 정의 10.8.2는 본질적으로 이 명제를 기저 없이 다시 서술한 것으로 선택되었습니다.  $\square$

**질문 10.8.5.** 기하적 중복도가 항상 대수적 중복도 이하임을 보이십시오.

이는 실제로 잠정적인 정의를 제공합니다:

- 대각합은 대수적 중복도를 고려하여 센 고윳값들의 합입니다.
- 행렬식은 대수적 중복도를 고려하여 센 고윳값들의 곱입니다.

이 정의는 괜찮지만, 기저체가 대수적으로 닫혀 있어야 한다는 단점이 있습니다. 또한 계산상 다루기 가장 쉬운 정의도 아닙니다. 다음 두 장에서 더 나은 정의를 제공할 것입니다.

## §10.9 생각해 볼 만한 조금 더 어려운 문제

**문제 10A** (대수적 중복도의 합). 2018차원 복소 벡터 공간  $V$ 와 사상  $T: V \rightarrow V$ 가 주어졌을 때,  $T$ 의 모든 고윳값의 대수적 중복도의 합은 얼마입니까?

**문제 10B** ("대각화 가능"이라는 단어). 선형 사상  $T: V \rightarrow V$  ( $\dim V$ 가 유한한 경우)는, 각  $e_i$ 가 고유벡터가 되는 기저  $e_1, \dots, e_n$ 을 가질 때 **대각화 가능**하다고 합니다.

(a) “대각화 가능”이라는 이름을 설명하십시오.

(b) 대수적으로 닫힌 체 위에서 작업한다고 합시다. 이때  $T$ 가 대각화 가능한 것은 임의의  $\lambda$ 에 대해  $\lambda$ 의 기하적 중복도가  $\lambda$ 의 대수적 중복도와 같은 것과 동치임을 보이십시오.

**문제 10C** (뒤바꾸기).  $V$ 를 기저  $e_1$ 과  $e_2$ 를 갖는  $\mathbb{C}$ -벡터 공간이라고 합시다. 사상  $T: V \rightarrow V$ 는  $T(e_1) = e_2$ 이고  $T(e_2) = e_1$ 입니다.  $T$ 의 고유공간을 구하십시오.

**문제 10D.**  $T: \mathbb{C}^{\oplus 2} \rightarrow \mathbb{C}^{\oplus 2}$ 가  $T^{2011} = \text{id}$ 를 만족하는  $\mathbb{C}$ -벡터 공간의 선형 사상이라고 합시다.  $T$ 는 반드시 대각화 가능합니까?

**문제 10E** (다항식을 거꾸로 쓰기). 차수가 2 이하인 다항식들의 복소 벡터 공간  $V$ 를, 즉  $V = \{ax^2 + bx + c \mid a, b, c \in \mathbb{C}\}$ 를 정의합시다.  $T: V \rightarrow V$ 를 다음과 같이 정의합니다

$$T(ax^2 + bx + c) = cx^2 + bx + a.$$

$T$ 의 고유공간을 구하십시오.

**문제 10F** (다항식의 미분).  $V = \mathbb{R}[x]$ 를 실수 계수를 갖는 모든 다항식으로 이루어진 무한차원 실수 벡터 공간이라고 합시다.  $\frac{d}{dx}: V \rightarrow V$ 가 선형 사상임에 유의하십시오 (예를 들어  $x^3$ 을  $3x^2$ 으로 보냅니다). 어떤 실수들이 이 사상의 고윳값입니까?

**문제 10G** (함수의 미분).  $V$ 를 무한히 미분 가능한 모든 함수  $\mathbb{R} \rightarrow \mathbb{R}$ 로 이루어진 무한차원 실수 벡터 공간이라고 합시다.  $\frac{d}{dx}: V \rightarrow V$ 가 선형 사상임에 유의하십시오 (예를 들어  $\cos x$ 를  $-\sin x$ 로 보냅니다). 어떤 실수들이 이 사상의 고윳값입니까?

# 11 쌍대 공간과 대각합

다음과 같은 행렬이 주어졌을 때

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

대각합은 대각선을 따라 더한 값  $a+d$ 이고 행렬식은  $ad-bc$ 라는 것을 고등학교에서 배웠을 수도 있습니다. 하지만 우리는 행렬이 어떤 의미에서는 기저의 선택을 이용하여 선형 사상을 인코딩한 것에 불과하다는 것을 알고 있습니다. 그렇다면 이 임의로 보이는 공식들이 어째서 기저의 선택에 의존하지 않는 것일까요?

이 장에서는  $T: V \rightarrow V$ 이고  $\dim V < \infty$ 일 때  $\text{Tr } T$ 에 대한 본질적인 정의를 제시하고자 합니다. 이는 좌표에 무관한 정의를 제공할 것이며, 특히 대각합  $a+d$ 가 다른 기저를 취하더라도 변하지 않음을 함의할 것입니다.

그 과정에서 우리는 두 가지 새로운 구성을 도입할 것입니다. 하나는 두 공간의 일종의 곱으로, 차원이  $\dim V \cdot \dim W$ 인 텐서곱  $V \otimes W$ 이고, 다른 하나는  $V \rightarrow k$ 인 선형 사상 ( $k$ -벡터 공간)들의 집합인 쌍대 공간  $V^\vee$ 입니다. 나중에 벡터 공간  $V$ 에서 내적 공간으로 업그레이드할 때, 쌍대 공간  $V^\vee$ 가 행렬의 "전치"에 대한 멋진 해석을 제공한다는 것을 보게 될 것입니다. 그중 일부는 여기서도 이미 엿볼 수 있습니다.

대각합은 유한 차원 벡터 공간에 대해서만 정의되므로, 원한다면 이 장에서는 관심을 유한 차원 벡터 공간으로 제한해도 됩니다. (반면 기저체가 대수적으로 닫혀 있을 필요는 없습니다.)

다음 장에서는 행렬식에 대해 같은 작업을 할 것입니다.

## §11.1 텐서곱

**이 절의 대표적인 예:**  $\mathbb{R}[x] \otimes \mathbb{R}[y] = \mathbb{R}[x, y]$ .

$V \oplus W$ 가 집합으로서는  $V \times W$ 처럼 보이더라도  $\dim(V \oplus W) = \dim V + \dim W$ 라는 것을 우리는 알고 있습니다. 만약 차원의 곱셈이 성립하는 진짜 "곱" 공간을 원한다면 어떻게 해야 할까요?

예를 들어, 제가 가장 좋아하는 실수 벡터 공간의 예를 꺼내보겠습니다. 즉

$$V = \{ax^2 + bx + c \mid a, b, c \in \mathbb{R}\}.$$

여기 조금 더 작은 또 다른 공간이 있습니다.

$$W = \{dy + e \mid d, e \in \mathbb{R}\}.$$

직합을 취한다면 원소들이 쌍  $(ax^2 + bx + c, dy + e)$ 로 생각될 수 있는, 다소 부자연스러운 5차원 벡터 공간을 얻게 될 것입니다. 하지만 만약 우리가 원소들이  $V$ 와  $W$ 의 다항식들의 곱인 벡터 공간을 원한다고 가정해봅시다. 이는  $4x^2y + 5xy + y + 3$ 과 같은 원소들을 포함할 것입니다. 특히 그 기저는 다음과 같을 것입니다.

$$\{x^2y, x^2, xy, x, y, 1\}$$

따라서 6차원을 가질 것입니다.

이를 위해 우리는 텐서곱에 의지합니다. 이는 정확히 이 작업을 하지만, "곱셈"이 무서운<sup>1</sup> 기호  $\otimes$ 에 의해 이루어진다는 점만 다릅니다. 이를 두 벡터 공간 사이의 원소들을 분리하는 "벽"이라고 생각하십시오. 예를 들어 위의 예시는 다음과 같이 쓸 수 있습니다.

$$4x^2 \otimes y + 5x \otimes y + 1 \otimes y + 3 \otimes 1.$$

(이는  $(4x^2 \otimes y) + (5x \otimes y) + \dots$ 로 읽혀야 합니다. 덧셈은  $\otimes$  뒤에 옵니다.) 물론  $4x^2 \otimes y$ 를 쓰는 것과  $x^2 \otimes 4y$ 를 쓰는 것, 심지어  $2x^2 \otimes 2y$ 를 쓰는 것 사이에는 아무런 구별이 없어야 합니다. 우리는  $x$ 와  $y$ 를 분리된 상태로 유지하고 싶지만, 스칼라는 자유롭게 오갈 수 있어야 합니다.

물론 모든 것을 단항식만으로 표현할 필요는 없습니다. 우리는 자유롭게 다음과 같이 쓸 수 있습니다.

$$(x+1) \otimes (y+1).$$

원한다면 이를 다음과 같이 전개할 수 있습니다.

$$x \otimes y + 1 \otimes y + x \otimes 1 + 1 \otimes 1.$$

같은 것입니다. 요점은 우리가 두 다항식을 임의로 취해 인위적으로 "텐서"할 수 있다는 것입니다.

텐서곱의 정의는 정확히 이 작업을 하며, 그 이상은 하지 않습니다.<sup>2</sup>

**정의 11.1.1.**  $V$ 와  $W$ 를 같은 체  $k$  위의 벡터 공간이라고 합시다. **텐서곱**  $V \otimes_k W$ 는  $v \otimes w$  형태의 원소들로 생성되는 아벨 군으로, 다음 관계를 만족합니다.

$$(v_1 + v_2) \otimes w = v_1 \otimes w + v_2 \otimes w$$

$$v \otimes (w_1 + w_2) = v \otimes w_1 + v \otimes w_2$$

$$(c \cdot v) \otimes w = v \otimes (c \cdot w).$$

벡터 공간으로서 그 작용은  $c \cdot (v \otimes w) = (c \cdot v) \otimes w = v \otimes (c \cdot w)$ 로 주어집니다.

같은 아이디어를 표현하는 또 다른 방법이 있습니다. 우리는  $v \in V$ 이고  $w \in W$ 인  $v \otimes w$  형태의 원소를 **순수 텐서**로 정의합니다. 하지만 우리는  $\otimes$  벽이 다음과 같은 의미에서 "투과성"을 갖도록 합니다.

$$(c \cdot v) \otimes w = v \otimes (c \cdot w) = c \cdot (v \otimes w)$$

그리고 곱셈과 덧셈이 우리가 예상하는 대로 분배되도록 합니다. 그러면  $V \otimes W$ 는 순수 텐서들의 합으로 이루어집니다.

#### 예제 11.1.2 (텐서곱의 무한 차원 예시: 두 변수 다항식)

이 장과는 관련이 없지만, 이 정의는 무한 차원 벡터 공간에서도 똑같이 잘 작동합니다. 가장 좋은 예시는 아마 다음과 같을 것입니다.

$$\mathbb{R}[x] \otimes_{\mathbb{R}} \mathbb{R}[y] = \mathbb{R}[x, y].$$

즉,  $x$ 에 대한 다항식과  $y$ 에 대한 실수 다항식의 텐서곱은 결국 이변수 다항식  $\mathbb{R}[x, y]$ 가 됩니다.

<sup>1</sup>정말로,  $\otimes$ 는 수학자가 아닌 사람들에게는 무시무시하게 보이며, 심지어 많은 수학 학부생들에게도 그렇습니다.

<sup>2</sup>단순화를 위해 저는 이를 벡터 공간에 대해서만 정의하겠습니다. 가환환  $R$  위의 가군에 대한 정의도 정확히 동일합니다.

**비고 11.1.3 (순수 텐서의 합에 대한 주의)** —  $V \otimes_k W$ 의 원소들이 실제로는 이러한 순수 텐서들의 합이라는 것을 기억하십시오! 앞의 예시가 마음에 들었다면, 이 사실은 멋진 해석을 갖습니다 —  $\mathbb{R}[x, y] = \mathbb{R}[x] \otimes_{\mathbb{R}} \mathbb{R}[y]$ 의 모든 다항식이  $x$ 에 대한 다항식과  $y$ 에 대한 다항식의 곱(즉 순수 텐서  $f(x) \otimes g(y)$ )으로 인수분해되는 것은 아닙니다. 하지만 그것들은 모두 순수 텐서  $x^a \otimes y^b$ 의 합으로 쓸 수 있습니다.

앞서 든 예시가 시사하듯이,  $V \otimes_k W$ 의 기저는 말 그대로  $V$ 와  $W$ 의 기저의 "곱"입니다. 특히 이는  $\dim(V \otimes_k W) = \dim V \cdot \dim W$ 이기를 바라는 우리의 바람을 충족시킵니다.

#### 명제 11.1.4 ( $V \otimes W$ 의 기저)

$V$ 와  $W$ 를 유한 차원  $k$ -벡터 공간이라 합시다.  $e_1, \dots, e_m$ 이  $V$ 의 기저이고  $f_1, \dots, f_n$ 이  $W$ 의 기저라면,  $V \otimes_k W$ 의 기저는 정확히  $e_i \otimes f_j$ 이며, 여기서  $i = 1, \dots, m$ 이고  $j = 1, \dots, n$ 입니다.

증명. 생략합니다. 적어도 이 기저가 생성 집합임을 확인하는 것은 쉽습니다. □

#### 예제 11.1.5 (구체적인 계산)

$V$ 가 기저  $e_1, e_2$ 를 가지고  $W$ 가 기저  $f_1, f_2$ 를 가진다고 합시다.  $v = 3e_1 + 4e_2 \in V$ 이고  $w = 5f_1 + 6f_2 \in W$ 라 합시다.  $V \otimes_k W$ 에 대한 이 기저로  $v \otimes w$ 를 써 봅시다:

$$\begin{aligned} v \otimes w &= (3e_1 + 4e_2) \otimes (5f_1 + 6f_2) \\ &= (3e_1) \otimes (5f_1) + (4e_2) \otimes (5f_1) + (3e_1) \otimes (6f_2) + (4e_2) \otimes (6f_2) \\ &= 15(e_1 \otimes f_1) + 20(e_2 \otimes f_1) + 18(e_1 \otimes f_2) + 24(e_2 \otimes f_2). \end{aligned}$$

그러므로 우리가 단순한 직합보다 더 긴밀한 방식으로 정말  $V \times W$ 에 관심이 있다면, 왜 텐서곱이 고려하기 좋은 "곱"인지 알 수 있습니다.

**표기의 남용 11.1.6.** 앞으로는  $k$ 가 대개 명확하므로  $\otimes_k$ 를 거의 항상 그냥  $\otimes$ 로 줄여 쓰겠습니다.

**비고 11.1.7** — 선형 사상  $V \otimes W \rightarrow X$ 를 정의하려면, 각 순수 텐서  $v \otimes w$ 가 어떻게 되는지만 말하면 된다는 것에 주목하십시오. 순수 텐서들이  $V \otimes W$ 를 생성하기 때문입니다. 하지만 다시 한번,  $V \otimes W$ 가 이러한 순수 텐서들의 합으로 이루어진다는 것을 명심하십시오! 다시 말해,  $V \otimes W$ 는 순수 텐서들에 의해 생성됩니다.

**비고 11.1.8** — 집합의 데카르트 곱  $A \times B$ 와 매우 비슷하게, 같은 체  $k$  위의 임의의 두 벡터 공간  $V$ 와  $W$ 를 텐서로 묶을 수 있습니다.  $V$ 와  $W$  사이의 관계는 전혀 상관 없습니다.  $\otimes$ 를  $k$ 의 스칼라는 통과시키지만 그 외에는  $V$ 와  $W$ 의 원소들을 분리된 채로 유지하는 일종의 "벽"으로 생각할 수 있습니다. 따라서  $\otimes$ 는 **내용에 무관합니다**. 이는 또한  $V$ 와  $W$ 가 서로 어떤 관계를 가지고 있더라도 텐서곱이 이를 기억하지 못한다는 것을 의미합니다. 예를 들어 군  $G \times G$ 에서  $(g, 1_G) \neq (1_G, g)$ 인 것과 마찬가지로  $v \otimes 1 \neq 1 \otimes v$ 입니다.

## §11.2 쌍대 공간

이 절의 대표적인 예: 열 행렬을 90도 회전시키십시오.

다음 벡터 공간을 생각해 봅시다:

### 예제 11.2.1 ( $\mathbb{R}^3 \rightarrow \mathbb{R}$ 로 가는 함수들)

실함수  $f(x, y, z)$ 들의 집합은 무한 차원 실수 벡터 공간입니다. 실제로 우리는 두 함수를 더하여  $f + g$ 를 얻을 수 있고,  $2f$ 와 같은 함수도 생각할 수 있습니다.

이는 무섭도록 큰 벡터 공간이지만, 몇 가지 합리적인 축소를 할 수 있습니다. 예를 들어,  $\mathbb{R}^3$ 에서  $\mathbb{R}$ 로 가는 선형 사상들에만 관심을 한정할 수 있습니다.

그것이 바로 우리가 지금 하려는 것입니다. 이 정의는 처음에는 이상하게 보일 수 있지만, 조금만 참아 주십시오.

**정의 11.2.2.**  $V$ 를  $k$ -벡터 공간이라 합시다. 그러면  $V$ 의 **쌍대 공간**인  $V^\vee$ 는  $V$ 에서  $k$ 로 가는 선형 사상들을 원소로 갖는 벡터 공간으로 정의됩니다.

덧셈과 곱셈은 점별로 이루어집니다. 이는  $cf + g$ 를  $c \cdot f(x) + g(x)$ 의 의미로 쓸 때 사용하는 것과 같은 표기법입니다. 쌍대 공간 자체는 생각하기가 그리 쉽지 않습니다.

$V^\vee$ 의 기저를 찾아봅시다. 먼저, 이 벡터 공간에 대한 매우 구체적인 해석을 살펴보겠습니다. 예를 들어  $V = \mathbb{R}^3$ 이라고 합시다.  $V$ 의 원소를 다음과 같이 열 행렬로 생각할 수 있습니다.

$$v = \begin{bmatrix} 2 \\ 5 \\ 9 \end{bmatrix} \in V.$$

그러면 선형 사상  $f: V \rightarrow k$ 는 행 행렬로 해석할 수 있습니다:

$$f = \begin{bmatrix} 3 & 4 & 5 \end{bmatrix} \in V^\vee.$$

그러면

$$f(v) = \begin{bmatrix} 3 & 4 & 5 \end{bmatrix} \begin{bmatrix} 2 \\ 5 \\ 9 \end{bmatrix} = 71.$$

더 정확히 말하면: 선형 사상  $V \rightarrow k$ 를 지정하려면,  $V$ 의 각 기저 원소가 어디로 가는지만 알려주면 됩니다. 위 예에서  $f$ 는  $e_1$ 을 3으로,  $e_2$ 를 4로,  $e_3$ 를 5로 보냅니다. 그러므로  $f$ 는 다음과 같이 보냅니다:

$$2e_1 + 5e_2 + 9e_3 \mapsto 2 \cdot 3 + 5 \cdot 4 + 9 \cdot 5 = 71.$$

이 모든 것을 정확하게 만들어 봅시다.

### 명제 11.2.3 ( $V^\vee$ 의 쌍대 기저)

$V$ 를 기저  $e_1, \dots, e_n$ 을 갖는 유한 차원 벡터 공간이라 합시다. 각  $i$ 에 대해 다음과 같이 정의되는 함수  $e_i^\vee: V \rightarrow k$ 를 생각해 봅시다

$$e_i^\vee(e_j) = \begin{cases} 1 & i = j \\ 0 & i \neq j. \end{cases}$$

좀 더 직관적으로 말하면,  $e_i^\vee(v)$ 는  $v$ 에서  $e_i$ 의 계수를 줍니다. 그러면  $e_1^\vee, e_2^\vee, \dots, e_n^\vee$ 는  $V^\vee$ 의 기저입니다.

**예제 11.2.4** ( $V^\vee$ 에 있는 원소의 구체적인 예)

이 표기법에서  $f = 3e_1^\vee + 4e_2^\vee + 5e_3^\vee$ 입니다. 여기서 "합" 표기법이 예상대로 작동하는 이유를 알겠습니까? 실제로

$$\begin{aligned} f(e_1) &= (3e_1^\vee + 4e_2^\vee + 5e_3^\vee)(e_1) \\ &= 3e_1^\vee(e_1) + 4e_2^\vee(e_1) + 5e_3^\vee(e_1) \\ &= 3 \cdot 1 + 4 \cdot 0 + 5 \cdot 0 = 3. \end{aligned}$$

이것이 바로 우리가 원했던 것입니다.

이 시점에서  $e_i \mapsto e_i^\vee$ 로 주어지는 동형사상과 함께  $V \cong V^\vee$ 라고 지적하고 싶어질 수 있습니다. 이것을 "열 행렬을  $90^\circ$  회전하는 것"이라고 부를 수도 있습니다.

이 진술은 기술적으로 참이지만, 추가 정보가 없는 일반적인 벡터 공간  $V$ 에 대해서는 이것을 그저  $\dim V = \dim V^\vee$ 라는 사실의 부산물로 생각할 수 있습니다(임의의 두 벡터 공간이 차원이 같으면 동형이기 때문입니다). 가장 중요한 점은, 위에서 주어진 동형사상이 어떤 기저를 선택했는지에 의존한다는 것입니다.

**비고 11.2.5** (위에서 주어진 동형사상  $V \rightarrow V^\vee$ 가 자연스럽게 **않음**을 보여주는 구체적인 예) 앨리스와 밥이 같은 2차원 실벡터 공간을 보고 있습니다

$$V = \{(x, y, z) \mid x + y + z = 0\}.$$

또한 구체성을 위해  $v_{\text{예시}} = (3, 5, -8)$ 을  $V$ 의 임의의 원소의 예로 둡시다. 앨리스가  $V$ 에 대해 다음 기저 벡터들을 선택한다고 합시다.

$$\begin{aligned} e_1 &= (1, 0, -1) \\ e_2 &= (0, 1, -1). \end{aligned}$$

앨리스는 이를 사용하여 위에서 설명한 대로 동형사상  $A: V \rightarrow V^\vee$ 를 구성하고,  $e_1^\vee = A(e_1)$ 을 생각합니다. 원소  $e_1^\vee \in V^\vee$ 는 함수  $e_1^\vee: V \rightarrow \mathbb{R}$ 이며, 이는 앨리스가  $V$ 의 임의의 벡터를 여기에 대입할 수 있음을 의미합니다. 예를 들어,  $v_{\text{예시}}$ 에 대해

$$e_1^\vee(v_{\text{예시}}) = e_1^\vee((3, 5, -8)) = e_1^\vee(3e_1 + 5e_2) = 3.$$

한편, 밥은 다음과 같이 다른 기저 벡터들을 선택합니다

$$\begin{aligned} f_1 &= (1, 0, -1) \\ f_2 &= (1, -1, 0). \end{aligned}$$

이는 밥에게 동형사상  $B: V \rightarrow V^\vee$ 와 그에 대응하는  $f_1^\vee = B(f_1)$ 을 줍니다. 밥도 이것을 어디서든 계산할 수 있습니다. 예를 들면

$$f_1^\vee(v_{\text{예시}}) = f_1^\vee((3, 5, -8)) = f_1^\vee(8f_1 - 5f_2) = 8.$$

따라서  $e_1^\vee = A((1, 0, -1))$ 와  $f_1^\vee = B((1, 0, -1))$ 는  $V^\vee$ 의 서로 다른 원소입니다. 다시 말해, 앨리스와 밥은 서로 다른 기저를 선택했기 때문에 서로 다른 동형사상을 얻은 것입니다.

### §11.3 $V^\vee \otimes W$ 는 $V$ 에서 $W$ 로 가는 행렬들을 줍니다

이 절의 목표:

$V$ 와  $W$ 가 유한 차원  $k$ -벡터 공간이면,  $V^\vee \otimes W$ 는 선형 사상  $V \rightarrow W$ 를 나타냅니다.

직관은 다음과 같습니다.  $V$ 가 3차원이고  $W$ 가 5차원이라면, 사상  $V \rightarrow W$ 를  $5 \times 3$  크기의 숫자 배열로 생각할 수 있습니다. 우리는 이 사상들을 벡터 공간으로 생각하고 싶습니다(행렬을 더하거나 스칼라배할 수 있기 때문입니다). 그러므로 이것은 차원이 15인 벡터 공간이어야 하겠지만, 그냥 " $k^{\oplus 15}$ "라고 말하는 것은 그다지 만족스럽지 않습니다(기저가 무엇입니까?).

더 잘하기 위해, 텐서곱을 생각해 봅시다

$$V^\vee \otimes W$$

이는 어떻게 보면  $V$ 에서 나가는 사상들과 목표 공간  $W$ 의 곱입니다. 우리는 이것이 실제로 우리가 원하는 공간이라고 주장합니다. 즉,  $V^\vee \otimes W$ 의 원소들과  $V$ 에서  $W$ 로 가는 선형 사상들 사이에는 자연스러운 전단사가 존재합니다.

먼저,  $V^\vee \otimes W$ 의 원소를 사상  $V \rightarrow W$ 로 어떻게 해석할까요? 구체성을 위해  $V$ 가 기저  $e_1, e_2, e_3$ 을 갖고,  $W$ 가 기저  $f_1, f_2, f_3, f_4, f_5$ 를 갖는다고 합시다.  $V^\vee \otimes W$ 의 원소를 생각해 봅시다, 예를 들면

$$e_1^\vee \otimes (f_2 + 2f_4) + 4e_2^\vee \otimes f_5.$$

우리는 이 원소를 함수  $V \rightarrow W$ 로 해석하고 싶습니다. 즉,  $v \in V$ 가 주어지면  $W$ 의 원소를 출력하고 싶습니다. 이를 하는 방법은 사실 하나뿐입니다.  $v \in V$ 를 왼쪽에 있는  $V^\vee$ 들에 대입하는 것입니다. 즉, 다음 사상을 취합니다

$$v \mapsto e_1^\vee(v) \cdot (f_2 + 2f_4) + 4e_2^\vee(v) \cdot f_5 \in W.$$

그러므로, 임의의 원소  $\xi_1 \otimes w_1 + \cdots + \xi_m \otimes w_m \in V^\vee \otimes W$ 를 선형 사상  $V \rightarrow W$ 로 해석하는 자연스러운 방법이 있습니다. 주장은 사실 모든 선형 사상  $V \rightarrow W$ 가 이러한 해석을 갖는다는 것입니다.

먼저, 표기의 편의를 위해,

**정의 11.3.1.**  $\text{Hom}(V, W)$ 가  $V$ 에서  $W$ 로의 선형 사상들의 집합(이는  $V$ 를  $W$ 로 보내는 행렬들로 해석할 수 있습니다)을 나타내며,  $k$  위의 벡터 공간으로 간주된다고 합시다. (“Hom”은 준동형사상을 뜻합니다.)

**질문 11.3.2.**  $\text{Hom}(V, k)$ 를 이름으로 식별하십시오.

이제 좀 더 일반적으로 성립하는 것을 적어볼 수 있습니다.

#### 정리 11.3.3 ( $V^\vee \otimes W \iff \text{선형 사상 } V \rightarrow W$ )

$V$ 와  $W$ 를 유한 차원 벡터 공간이라고 합시다. 우리는 다음과 같은 사상을 기술했습니다

$$\Psi: V^\vee \otimes W \rightarrow \text{Hom}(V, W)$$

$\xi_1 \otimes w_1 + \cdots + \xi_m \otimes w_m$ 을 다음 선형 사상으로 보냄으로써

$$v \mapsto \xi_1(v)w_1 + \cdots + \xi_m(v)w_m.$$

그러면  $\Psi$ 는 벡터 공간의 동형사상입니다, 즉 모든 선형 사상  $V \rightarrow W$ 는 이러한 방식으로  $V^\vee \otimes W$ 의 원소로서 유일하게 표현될 수 있습니다.

위 내용은 다소 난해할 수 있으므로, 구체적인 예시를 살펴보겠습니다.

**예제 11.3.4 (구체적인 예시)**

$V = \mathbb{R}^2$ 라 하고  $V$ 의 기저  $e_1, e_2$ 를 취합시다. 그러면  $T: V \rightarrow V$ 를 다음과 같이 정의합니다

$$T = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}.$$

그러면 다음을 얻습니다

$$\Psi(e_1^\vee \otimes e_1 + 2e_2^\vee \otimes e_1 + 3e_1^\vee \otimes e_2 + 4e_2^\vee \otimes e_2) = T.$$

아름다운 점은  $\Psi$ 의 정의가 기저에 무관하다는 것입니다. 따라서 기저를 바꾸더라도, 위 표현은 완전히 다르게 보이겠지만,  $V^\vee \otimes V$  안의 실제 원소는 변하지 않습니다.

그럼에도 불구하고, 증명을 위해서는 좌표를 사용하는 즐거움을 누리보겠습니다.

**정리 11.3.3**의 증명. 위협적으로 보이지만, 사실은 어렵지 않습니다. 두 단계로 진행합니다:

1. 먼저,  $\Psi$ 가 전사임을 확인합니다. 즉 모든 선형 사상은  $V^\vee \otimes W$ 에서 적어도 하나의 표현을 갖습니다. 이를 보이기 위해, 임의의  $T: V \rightarrow W$ 를 취합시다.  $V$ 가 기저  $e_1, e_2, e_3$ 를 가지고  $T(e_1) = w_1, T(e_2) = w_2, T(e_3) = w_3$ 라고 합시다. 그러면 다음 원소가

$$e_1^\vee \otimes w_1 + e_2^\vee \otimes w_2 + e_3^\vee \otimes w_3$$

작동합니다, 왜냐하면 이는 기저 원소  $e_i$ 에서  $T$ 와 일치하도록 고안되었기 때문입니다.

2. 따라서 이제  $\dim V^\vee \otimes W = \dim \text{Hom}(V, W)$ 임을 확인하는 것으로 충분합니다. 분명히,  $V^\vee \otimes W$ 는 차원  $\dim V \cdot \dim W$ 를 갖습니다. 그러나  $\text{Hom}(V, W)$ 를  $\dim V \cdot \dim W$  행렬로 봄으로써, 이 또한 차원  $\dim V \cdot \dim W$ 를 가짐을 알 수 있습니다.  $\square$

그러므로 **자연스러운 동형사상**  $V^\vee \otimes W \cong \text{Hom}(V, W)$ 가 존재합니다. 비록 그것이 작동한다는 증명에서 기저를 자유롭게 사용하긴 했지만, 이는 이 동형사상이 “신께서 주신 것”이며, 오직  $V$ 와  $W$  자체의 본질에만 의존하고 벡터 공간을 표현하기 위해 어떤 기저를 선택하는지에는 의존하지 않는다는 사실을 바꾸지 않습니다.

## §11.4 대각합

이제 대각합의 정의를 내릴 준비가 되었습니다. 정사각 행렬  $T$ 는 사상  $T: V \rightarrow V$ 로 생각할 수 있음을 상기하십시오. 위 정리에 따르면,

$$\text{Hom}(V, V) \cong V^\vee \otimes V$$

그러므로 모든 사상  $V \rightarrow V$ 는  $V^\vee \otimes V$ 의 원소로 생각할 수 있습니다. 그러나 우리는 각 순수 텐서를 “붕괴”시켜 평가 사상  $\text{ev}: V^\vee \otimes V \rightarrow k$ 를 정의할 수도 있습니다:  $f \otimes v \mapsto f(v)$ . 이는 우리에게 합성 사상을 제공합니다

$$\text{Hom}(V, V) \xrightarrow{\cong} V^\vee \otimes V \xrightarrow{\text{ev}} k.$$

이 결과를 행렬  $T$ 의 **대각합**이라고 부릅니다.

**예제 11.4.1 (대각합의 예시)**

앞의 예시를 계속하면,

$$\operatorname{Tr} T = e_1^\vee(e_1) + 2e_2^\vee(e_1) + 3e_1^\vee(e_2) + 4e_2^\vee(e_2) = 1 + 0 + 0 + 4 = 5.$$

그리고 이것이 대각합이 대각 성분들의 합인 이유입니다.

**§11.5 생각해 볼 만한 조금 더 어려운 문제**

**문제 11A** (대각합은 고윳값들의 합).  $V$ 를 대수적으로 닫힌 체  $k$  위의  $n$ 차원 벡터 공간이라 합시다.  $T: V \rightarrow V$ 를 고윳값  $\lambda_1, \lambda_2, \dots, \lambda_n$ 을 갖는 (대수적 중복도를 세어) 선형 사상이라 합시다.  $\operatorname{Tr} T = \lambda_1 + \dots + \lambda_n$ 임을 보이십시오.

**문제 11B<sup>†</sup>** (대각합의 곱).  $T: V \rightarrow V$ 와  $S: W \rightarrow W$ 를 유한 차원 벡터 공간  $V$ 와  $W$ 의 선형 사상이라 합시다.  $T \otimes S: V \otimes W \rightarrow V \otimes W$ 를  $v \otimes w \mapsto T(v) \otimes S(w)$ 로 정의합시다. 다음을 증명하십시오.

$$\operatorname{Tr}(T \otimes S) = \operatorname{Tr}(T) \operatorname{Tr}(S).$$



**문제 11C<sup>†</sup>** (대각합은 어느 정도 교환됩니다).  $T: V \rightarrow W$ 와  $S: W \rightarrow V$ 를 유한 차원 벡터 공간  $V$ 와  $W$  사이의 선형 사상이라 합시다. 다음을 보이십시오.

$$\operatorname{Tr}(T \circ S) = \operatorname{Tr}(S \circ T).$$



**문제 11D** (Putnam 1988).  $V$ 를  $n$ 차원 벡터 공간이라 합시다.  $T: V \rightarrow V$ 를 선형 사상이라 하고,  $n+1$ 개의 고유벡터가 존재하며 그중 임의의  $n$ 개가 선형독립이라고 가정합시다. 그러면  $T$ 가 항등원의 스칼라배임이 따라 나오니까?

# 12 행렬식

이 장의 목표는 행렬식의 기저 독립적인 정의를 제시하는 것입니다. 즉,  $T: V \rightarrow V$ 에 대해  $T$ 의 인코딩을 참조하지 않고  $\det T$ 를 정의할 것입니다. 이를 통해 행렬의 행렬식이 기저 선택에 의존하지 않는다는 것과, 몇몇 성질(예를 들어 행렬식이 곱셈적이라는 것)이 공허하게 참이라는 것이 명백해질 것입니다.

행렬식은 유한 차원 벡터 공간에 대해서만 정의되므로, 원한다면 이 장에서는 유한 차원 벡터 공간으로 관심을 국한해도 좋습니다. 반면 바탕체가 대수적으로 닫혀 있을 필요는 없습니다.

## §12.1 켤레곱

**이 절의 대표적인 예:**  $\wedge^2(\mathbb{R}^2)$ 는 평행사변형을 줍니다.

이제 켤레곱이라 불리는 것을 정의하려고 합니다. 처음에는 텐서곱  $V \otimes V$ 처럼 보이지만, 여기에 관계 하나가 추가로 있을 것입니다.

간단히 하기 위해, 먼저 켤레곱  $\wedge^2(V)$ 를 정의하겠습니다. 하지만 나중에 2를 임의의  $n$ 으로 대체할 것입니다.

**정의 12.1.1.**  $V$ 를  $k$ -벡터 공간이라 합시다. 2-켤레곱  $\wedge^2(V)$ 는  $v \wedge w$  ( $v, w \in V$ ) 형태의 원소들로 생성되는 아벨 군이며, 동일한 관계들을 만족합니다

$$\begin{aligned}(v_1 + v_2) \wedge w &= v_1 \wedge w + v_2 \wedge w \\ v \wedge (w_1 + w_2) &= v \wedge w_1 + v \wedge w_2 \\ (c \cdot v) \wedge w &= v \wedge (c \cdot w)\end{aligned}$$

여기에 두 가지 추가 관계가 더해집니다:

$$v \wedge v = 0 \quad \text{그리고} \quad v \wedge w = -w \wedge v.$$

벡터 공간으로서, 그 작용은  $c \cdot (v \wedge w) = (c \cdot v) \wedge w = v \wedge (c \cdot w)$ 로 주어집니다.

**연습문제 12.1.2.** 조건  $v \wedge w = -(w \wedge v)$ 가 사실은 불필요함을 보이십시오: 이는  $v \wedge v = 0$ 이라는 사실로부터 유도할 수 있습니다. (힌트:  $(v + w) \wedge (v + w) = 0$ 을 전개해 보십시오.)

이는 텐서곱의 정의와 거의 똑같아 보이지만, 두 가지 미묘한 차이가 있습니다. 첫째는 이제 텐서곱에서처럼  $V$ 와  $W$ 가 아니라  $V$  하나만 있다는 것입니다.<sup>1</sup> 둘째로, 새로운 수수끼리 같은 관계가 있습니다

$$v \wedge v = 0 \implies v \wedge w = -(w \wedge v).$$

저게 왜 저기 있는 걸까요? 좀 이상해 보입니다.

힌트를 하나 드리겠습니다.

### 예제 12.1.3 (켤레곱의 명시적 계산)

$V = \mathbb{R}^2$ 이고,  $v = ae_1 + be_2$ ,  $w = ce_1 + de_2$ 라고 합시다. 이제  $\wedge^2(V)$ 에서  $v \wedge w$ 를

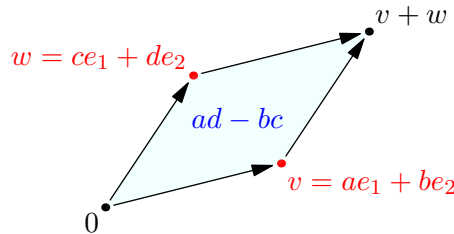
<sup>1</sup>그러니 어쩌면 켤레곱은 "켤레 거듭제곱"이라고 부르는 것이 더 정확할지도 모릅니다!

계산해 봅시다.

$$\begin{aligned}
 v \wedge w &= (ae_1 + be_2) \wedge (ce_1 + de_2) \\
 &= ac(e_1 \wedge e_1) + bd(e_2 \wedge e_2) + ad(e_1 \wedge e_2) + bc(e_2 \wedge e_1) \\
 &= ad(e_1 \wedge e_2) + bc(e_2 \wedge e_1) \\
 &= (ad - bc)(e_1 \wedge e_2).
 \end{aligned}$$

$ad - bc$ 는 무엇일까요? 이미 알아보셨을지도 모릅니다:

- $v$ 와  $w$ 로 이루어진 평행사변형의 넓이가  $ad - bc$ 라는 것을 알고 있을 것입니다.
- 이것이  $\begin{bmatrix} a & c \\ b & d \end{bmatrix}$ 의 행렬식이라는 것을 알아볼 수도 있습니다. 실제로, 행렬식이 초부피(hypervolume)를 해석하기 위한 것임을 이미 알고 있을 수도 있습니다.



이는 결코 우연이 아닙니다. 췌기곱(wedge product)은 부호 있는 넓이를 해석하도록 설계되어 있습니다. 즉,  $v \wedge w$ 는  $v$ 와  $w$ 로 이루어진 평행사변형의 넓이를 해석하기 위한 것입니다. 이제  $(cv) \wedge w = v \wedge (cw)$ 라는 조건이 왜 타당한지 알 수 있을 것입니다. 그리고 이제 물론  $v \wedge v$ 가 왜 0이 되어야 하는지도 알 수 있습니다: 그것은 넓이가 0인 평행사변형이기 때문입니다!

**췌기곱의 기적**은 텐서곱 공리에 추가로 필요한 조건이 오직  $v \wedge v = 0$ 뿐이라는 것입니다. 그러면 갑자기 췌기가 부피를 해석하는 우리의 모든 작업을 대신 해줄 것입니다.

**비고 12.1.4 (수학에서의 정의에 관한 부수적 여담)** 이 "성질 기반" 철학은 현대 수학에서 흔한 상투 수법입니다. 정의하고자 하는 대상에 대한 어떤 직관을 가지고 있고, 그로부터 "따라와야 할" 것 같은 성질들의 희망 목록을 적어 봅니다. 그런데 그 성질들만으로 다루기에 충분하다는 것이 밝혀지면, 정의를 위해서는 그저 희망 목록의 모든 성질을 만족하는 추상적 대상을 정의하기만 하면 됩니다. 그 이후로 직관은 어떤 "공식적인" 역할도 하지 않으며, 그저 희망 목록에 대한 응원 삼아 동기를 부여하는 역할만 할 뿐입니다.

췌기곱의 경우, 희망 목록에는 단 하나의 성질  $v \wedge v = 0$ 만 있습니다.

앞서와 유사하게:

#### 명제 12.1.5 ( $\wedge^2(V)$ 의 기저)

$V$ 를 기저  $e_1, \dots, e_n$ 을 갖는 벡터 공간이라고 합시다. 그러면  $\wedge^2(V)$ 의 기저는 다음과 같습니다.

$$e_i \wedge e_j$$

여기서  $i < j$ 입니다. 따라서  $\wedge^2(V)$ 는 차원  $\binom{n}{2}$ 를 가집니다.

증명. 놀랍도록 다루기 까다로우며, 이 역시 생략합니다. (텐서곱에 대한 해당 정리로부터 유도할 수 있습니다.)  $\square$

이제 다차원 켤레곱을 정의할 용기가 생겼습니다. 이것은 켤레가 더 많아진 것일 뿐, 동일한 것입니다.

**정의 12.1.6.**  $V$ 를 벡터 공간,  $m$ 을 양의 정수라고 합시다. 공간  $\wedge^m(V)$ 는 다음 형태의 켤레들로 생성됩니다.

$$v_1 \wedge v_2 \wedge \cdots \wedge v_m$$

다음 관계를 조건으로 합니다.

$$\begin{aligned} \cdots \wedge (v_1 + v_2) \wedge \cdots &= (\cdots \wedge v_1 \wedge \cdots) + (\cdots \wedge v_2 \wedge \cdots) \\ \cdots \wedge (cv_1) \wedge v_2 \wedge \cdots &= \cdots \wedge v_1 \wedge (cv_2) \wedge \cdots \\ \cdots \wedge v \wedge v \wedge \cdots &= 0 \\ \cdots \wedge v \wedge w \wedge \cdots &= -(\cdots \wedge w \wedge v \wedge \cdots) \end{aligned}$$

벡터 공간으로서

$$c \cdot (v_1 \wedge v_2 \wedge \cdots \wedge v_m) = (cv_1) \wedge v_2 \wedge \cdots \wedge v_m = v_1 \wedge (cv_2) \wedge \cdots \wedge v_m = \cdots$$

이 정의는 상당히 장황하지만, 세 가지 조건을 말로 풀면 다음과 같습니다.

- 이전처럼 곱을 더할 수 있어야 합니다.
- ("벡터 공간" 작용에서 직접 지적되었듯이)  $m$ 개의 성분 중 아무 곳이나 상수를 넣을 수 있으며, 그리고
- 임의의 두 인접한 켤레를 바꾸면 켤레 전체의 부호가 바뀝니다.

따라서 이것은  $\wedge^2(V)$ 의 자연스러운 일반화입니다. 다음 형태의 임의의 원소는

$$\cdots \wedge v \wedge \cdots \wedge v \wedge \cdots$$

여전히 0이어야 함을 스스로 확인할 수 있습니다.

앞서  $e_1 \wedge e_2$ 가 기저였던 것처럼, 일반적인  $m$ 과  $n$ 에 대해서도 기저를 찾을 수 있습니다.

#### 명제 12.1.7 (켤레곱의 기저)

$V$ 를 기저  $e_1, \dots, e_n$ 을 갖는 벡터 공간이라고 합시다.  $\wedge^m(V)$ 의 기저는 다음 원소들로 구성됩니다.

$$e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_m}$$

여기서

$$1 \leq i_1 < i_2 < \cdots < i_m \leq n.$$

따라서  $\wedge^m(V)$ 는 차원  $\binom{n}{m}$ 을 가집니다.

증명 개요. 우리는 앞서  $e_{i_1} \otimes \cdots \otimes e_{i_m}$ 이 텐서곱의 기저임을 알고 있었습니다. 여기서는 다음의 추가적인 성질이 있습니다: (a) 만약 두 기저 원소가 다시 나타나면 전체가 0이 되므로,  $i$ 들이 모두 서로 다르다고 가정해야 합니다. 그리고 (b) 원소들의 순서를 바꿀 수 있으므로, 임의로 기저 원소들을 증가하는 순서로 배치하기로 정합니다.  $\square$

## §12.2 행렬식

**이 절의 대표적인 예:**  $(ae_1 + be_2) \wedge (ce_1 + de_2) = (ad - bc)(e_1 \wedge e_2)$ .

이제 행렬식을 정의할 준비가 되었습니다.  $T: V \rightarrow V$ 가 정방행렬이라고 합시다. 췌기들에 대해 다음과 같이 주어지는 사상  $\wedge^m(V) \rightarrow \wedge^m(V)$ 가

$$v_1 \wedge v_2 \wedge \cdots \wedge v_m \mapsto T(v_1) \wedge T(v_2) \wedge \cdots \wedge T(v_m).$$

$\wedge^m(V)$  전체로 선형적으로 확장할 때 잘 정의된 선형 사상임을 주장합니다. (여기서 "잘 정의됨"이란 정의역의 동치인 원소들이 공역의 동치인 원소들로 대응됨을 의미합니다. 이는 선형성과 함께  $T$ 가 선형 사상이라는 사실로부터 따라 나옵니다.) 이 사상을  $\wedge^m(T)$ 라고 부릅니다.

### 예제 12.2.1 ( $\wedge^m(T)$ 의 예)

표준 기저  $e_1, e_2, e_3, e_4$ 를 갖는  $V = \mathbb{R}^4$ 에서,  $T(e_1) = e_2, T(e_2) = 2e_3, T(e_3) = e_3, T(e_4) = 2e_2 + e_3$ 라고 합시다. 그러면 예를 들어  $\wedge^2(T)$ 는 다음을 보냅니다.

$$\begin{aligned} (e_1 \wedge e_2) + (e_3 \wedge e_4) &\mapsto T(e_1) \wedge T(e_2) + T(e_3) \wedge T(e_4) \\ &= e_2 \wedge 2e_3 + e_3 \wedge (2e_2 + e_3) \\ &= 2(e_2 \wedge e_3 + e_3 \wedge e_2) \\ &= 0. \end{aligned}$$

이제 흥미로운 사실이 하나 있습니다.  $V$ 의 차원이  $n$ 이고,  $m = n$ 이라고 합시다. 그러면  $\wedge^n(V)$ 는 차원  $\binom{n}{n} = 1$ 을 가집니다 — 즉 1차원 공간입니다! 따라서  $\wedge^n(V) \cong k$ 입니다.

따라서  $\wedge^n(T)$ 는  $k$ 에서  $k$ 로 가는 선형 사상으로 생각할 수 있습니다. 그런데  $k$ 에서  $k$ 로 가는 선형 사상은 단순히 상수 곱셈이라는 것을 우리는 알고 있습니다. 따라서  $\wedge^n(T)$ 는 어떤 상수의 곱셈입니다.

**정의 12.2.2.**  $V$ 가  $n$ 차원 벡터 공간일 때,  $T: V \rightarrow V$ 라 합시다. 그러면  $\wedge^n(T)$ 는 상수  $c$ 의 곱셈이며, 이  $c = \det T$ 를  $T$ 의 **행렬식**으로 정의합니다.

### 예제 12.2.3 ( $2 \times 2$ 행렬의 행렬식)

다시  $V = \mathbb{R}^2$ 이고 기저가  $e_1$ 과  $e_2$ 라고 합시다. 다음과 같다고 합시다

$$T = \begin{bmatrix} a & c \\ b & d \end{bmatrix}.$$

다시 말해,  $T(e_1) = ae_1 + be_2$ 이고  $T(e_2) = ce_1 + de_2$ 입니다.

이제  $\wedge^2(V)$ 를 생각해 봅시다. 이는 기저  $e_1 \wedge e_2$ 를 가집니다. 이제  $\wedge^2(T)$ 는 이것을 다음으로 보냅니다

$$e_1 \wedge e_2 \xrightarrow{\wedge^2(T)} T(e_1) \wedge T(e_2) = (ae_1 + be_2) \wedge (ce_1 + de_2) = (ad - bc)(e_1 \wedge e_2).$$

따라서  $\wedge^2(T): \wedge^2(V) \rightarrow \wedge^2(V)$ 는  $\det T = ad - bc$ 의 곱셈인데, 이는  $e_1 \wedge e_2$ 를  $(ad - bc)(e_1 \wedge e_2)$ 로 보내기 때문입니다.

그리고 이것이 바로 행렬식의 정의입니다. 다시 한번 말하지만, 이를  $\wedge^n(T)$ 의 관점에서 정의했으므로, 이 정의는 기저의 선택과 완전히 무관합니다. 다시 말해, 행렬식은 행렬을 전혀 참조하지 않고  $T: V \rightarrow V$ 만으로 정의할 수 있습니다.

**질문 12.2.4.** 왜  $\wedge^n(S \circ T) = \wedge^n(S) \circ \wedge^n(T)$ 가 성립합니까?

이런 방식으로 우리는

$$\det(S \circ T) = \det(S) \det(T)$$

도 공짜로 얻습니다.

더 일반적으로 2를  $n$ 으로 바꾸고, 다음을 전개한 결과를 써보면

$$(a_{11}e_1 + a_{21}e_2 + \cdots) \wedge \cdots \wedge (a_{1n}e_1 + a_{2n}e_2 + \cdots + a_{nn}e_n)$$

다음 공식을 얻게 됩니다.

$$\det(A) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}$$

이는 행렬식에 대한 **라이프니츠 공식**이라 불립니다. 미국 고등학생이라면 이를 알아볼 텐데, (안타깝게도) 이것이 웨지곱을 이용한 더 나은 정의의 따름정리가 아니라 행렬식의 정의 자체로 가르쳐지고 있습니다.

**연습문제 12.2.5.** 웨지곱을 전개하면  $n = 3$ 에 대한 라이프니츠 공식이 나옴을 확인하십시오.

## §12.3 특성다항식과 케일리-해밀턴

고윳값 이론과 연결해 봅시다.  $V$ 가 대수적으로 닫힌 체 위에서  $n$ 차원일 때, 사상  $T: V \rightarrow V$ 를 생각하고, 그 고윳값을  $\lambda_1, \lambda_2, \dots, \lambda_n$ 이라 합시다(중복 포함). 그러면 **특성다항식**은 다음과 같이 주어집니다.

$$p_T(X) = (X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_n).$$

$T$ 를 조르당 표준형으로 썼다면, 즉

$$T = \begin{bmatrix} \lambda_1 & * & 0 & \cdots & 0 \\ 0 & \lambda_2 & * & \cdots & 0 \\ 0 & 0 & \lambda_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_n \end{bmatrix}$$

(여기서 각  $*$ 는 0 또는 1입니다) 다음과 같이 정의를 짜맞출 수 있습니다.

$$p_T(X) := \det(X \cdot \text{id}_n - T) = \det \begin{bmatrix} X - \lambda_1 & * & 0 & \cdots & 0 \\ 0 & X - \lambda_2 & * & \cdots & 0 \\ 0 & 0 & X - \lambda_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & X - \lambda_n \end{bmatrix}.$$

후자의 정의는 대부분의 선형대수학 책에서 볼 수 있는 것인데, 이는 "고윳값"이라는 단어를 언급하지 않고(즉, 전적으로 숫자 배열의 관점에서) 특성다항식을 정의할 수 있게 해주기 때문입니다. 어떤 행렬이 주어지든 특성다항식을 쉽게 계산할 수 있고 따라서 고윳값도 쉽게 계산할 수 있다는 점에서 이러한 정의가 장점을 가진다는 것은 인정합니다. 하지만 저는 여전히 정의는 애초에 고윳값의 관점에서 이루어져야 한다고 생각합니다. 예를 들어 행렬식을 이용한 정의는 다음 정리를 모호하게 만드는데, 사실 이 정리는 완전히 자명한 것입니다.

**정리 12.3.1 (케일리-해밀턴)**

$T: V \rightarrow V$ 가 대수적으로 닫힌 체 위의 유한 차원 벡터 공간들 사이의 사상이라 합시다. 그러면 사상  $p_T(T)$ 는 영사상입니다.

여기서  $p_T(T)$ 란, 만약

$$p_T(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_0$$

라면

$$p_T(T) = T^n + c_{n-1}T^{n-1} + \cdots + c_1T + c_0I$$

가 영사상임을 의미하며, 여기서  $T^k$ 는  $T$ 를  $k$ 번 적용한 것을 나타냅니다. 우리는  $T$ 가 적어도 하나의 영이 아닌 고유벡터를 가짐을 증명할 때 이미 이 개념을 본 적이 있습니다.

**예제 12.3.2 (행렬식 정의를 이용한 케일리-해밀턴 정리의 예)**

$T = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ 라고 합시다. 특성다항식의 행렬식 정의를 이용하면,  $p_T(X) = (X - 1)(X - 4) - (-2)(-3) = X^2 - 5X - 2$ 임을 알 수 있습니다. 실제로 다음을 확인할 수 있습니다

$$T^2 - 5T - 2 = \begin{bmatrix} 7 & 10 \\ 15 & 22 \end{bmatrix} - 5 \cdot \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} - 2 \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

만약 고윳값이라는 단어 없이  $p_T$ 를 정의하고, 행렬을 숫자들의 배열로 보는 사악한 관점을 취한다면, 이것은 완전한 기적처럼 보일 것입니다. (실제로 위키백과에 있는 끔찍한 증명들을 보십시오.)

하지만  $T$ 를 선형 사상으로 보는 추상적인 관점을 사용한다면, 이 정리는 거의 자명합니다.

케일리-해밀턴 정리의 증명.  $V$ 를 조르당 표준형으로 다음과 같이 쓴다고 합시다.

$$V = J_1 \oplus \cdots \oplus J_m$$

여기서  $J_i$ 는 고윳값  $\lambda_i$ 와 차원  $d_i$ 를 가집니다. 정의에 의해,

$$p_T(T) = (T - \lambda_1)^{d_1} (T - \lambda_2)^{d_2} \cdots (T - \lambda_m)^{d_m}.$$

정의에 의해,  $(T - \lambda_1)^{d_1}$ 은  $J_1$  위에서 영사상입니다. 따라서  $p_T(T)$ 는  $J_1$  위에서 영입니다. 마찬가지로 다른  $J_i$ 들 각각에 대해서도 영이며 — 이것으로 끝입니다.  $\square$

**비고 12.3.3 (텐서로 확장하기)** — 케일리-해밀턴 정리는  $k$ 가 대수적으로 닫혀 있다는 가정 없이도 성립합니다. 예를 들어 임의의 실수 행렬은 (앞서 언급한 트릭에 따라) 복소수 계수를 가진 행렬로 볼 수 있기 때문입니다. 이 아이디어를 텐서곱을 이용해 어떻게 형식화할 수 있는지 간략히 힌트를 드리겠습니다.

기저  $e_1, e_2, e_3$ 을 가지는 공간  $V = \mathbb{R}^3$ 을 생각해 봅시다. 그러면  $V$ 의 원소들은  $r_1, r_2, r_3$ 이 실수인  $r_1e_1 + r_2e_2 + r_3e_3$  형태를 가집니다. 우리는 본질적으로 동일한 벡터 공간을 고려하되, 실수 계수  $r_i$  대신 복소수 계수  $z_i$ 를 가지도록 하고자 합니다. 그래서 우리가 하는 일은 다음과 같습니다.  $\mathbb{C}$ 를 (예를 들어 기저  $\{1, i\}$ 를 가지는)  $\mathbb{R}$ -벡터 공간으로 보고, **복소화**를 고려합니다.

$$V_{\mathbb{C}} := \mathbb{C} \otimes_{\mathbb{R}} V.$$

그러면 우리의 원소들이 실제로 다음과 같은 형태를 가짐을 확인할 수 있습니다.

$$z_1 \otimes e_1 + z_2 \otimes e_2 + z_3 \otimes e_3.$$

여기서 텐서곱은  $\mathbb{R}$  위에서 이루어지므로,  $r \in \mathbb{R}$ 에 대해  $z \otimes re_i = (zr) \otimes e_i$ 가 성립합니다. 그러면  $V_{\mathbb{C}}$ 는  $i \in \{1, 2, 3\}$ 에 대한 기저  $1 \otimes e_i$ 를 가지는  $\mathbb{C}$  위의 3차원 벡터 공간으로 생각할 수 있습니다. 이런 방식으로, 텐서곱은 복소수 계수를 "덧붙인다"는 아이디어를 형식화할 수 있게 해줍니다.

$T: V \rightarrow W$ 가 사상이라면,  $T_{\mathbb{C}}: V_{\mathbb{C}} \rightarrow W_{\mathbb{C}}$ 는 단순히  $z \otimes v \mapsto z \otimes T(v)$ 인 사상입니다. 이는 때때로  $T_{\mathbb{C}} = \text{id} \otimes T$ 로 표기되는 것을 볼 수 있습니다. 이렇게 하면  $T_{\mathbb{C}}$ 에 정리들을 적용하여  $T$ 에 대한 해당 결과를 유도할 수 있습니다.

## §12.4 생각해 볼 만한 조금 더 어려운 문제

**문제 12A** (열 연산). 임의의 실수  $x_{ij}$  (여기서  $1 \leq i, j \leq n$ )에 대해 다음이 성립함을 보이십시오.

$$\det \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} & x_{n2} & \cdots & x_{nn} \end{bmatrix} = \det \begin{bmatrix} x_{11} + cx_{12} & x_{12} & \cdots & x_{1n} \\ x_{21} + cx_{22} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n1} + cx_{n2} & x_{n2} & \cdots & x_{nn} \end{bmatrix}.$$

**문제 12B** (행렬식은 고윳값들의 곱).  $V$ 를 대수적으로 닫힌 체  $k$  위의  $n$ 차원 벡터 공간이라 합시다.  $T: V \rightarrow V$ 를 고윳값  $\lambda_1, \lambda_2, \dots, \lambda_n$ 을 (대수적 중복도를 세어) 가지는 선형 사상이라 합시다.  $\det T = \lambda_1 \dots \lambda_n$ 임을 보이십시오.

**문제 12C** (지수 행렬).  $X$ 를 복소수 계수를 가지는  $n \times n$  행렬이라 합시다. 우리는 지수 사상을 다음과 같이 정의합니다.

$$\exp(X) = 1 + X + \frac{X^2}{2!} + \frac{X^3}{3!} + \cdots$$

(이것이 어떤  $n \times n$  행렬로 수렴한다는 것은 당연한 것으로 받아들이십시오.) 다음을 증명하십시오.

$$\det(\exp(X)) = e^{\text{Tr } X}.$$

**문제 12D** (문제 9B<sup>†</sup>의 확장).  $T: V \rightarrow V$ 를 유한 차원 벡터 공간들 사이의 사상이라 합시다.  $T$ 가 동형사상인 것과  $\det T \neq 0$ 인 것이 동치임을 증명하십시오.



**문제 12E** (스웨덴 2010에 기반함). 0이 아닌 무게를 가진 1000마리의 소 떼가 주어져 있습니다. 소 한 마리를 제거하여 남은 999마리의 소를 무게의 합이 같은 두 집합으로 분할할 수 없도록 할 수 있음을 증명하십시오.



**문제 12F** (퍼트넘 2015).  $S$ 를  $a, b, c, d$ 가 이 순서로 등차수열을 이루는 실수 행렬  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 의 집합이라고 정의합니다. 어떤 정수  $k > 1$ 에 대해  $M^k \in S$ 인 모든  $M \in S$ 를 구하십시오.



**문제 12G.**  $V$ 를  $k$  위의 유한 차원 벡터 공간이라 하고  $T: V \rightarrow V$ 라고 합시다. 다음을 보이십시오.

$$\det(a \cdot \text{id}_V - T) = \sum_{n=0}^{\dim V} a^{\dim V - n} \cdot (-1)^n \text{Tr} \left( \bigwedge^n (T) \right)$$

여기서 대각함은  $\bigwedge^n(T): \bigwedge^n(V) \rightarrow \bigwedge^n(V)$ 로 보고 취한 것입니다.



**문제 12H** (코시-비네 공식).  $n \geq s \geq 1$ 을 정수라 하고,  $A$ 와  $B$ 를 각각  $s \times n$  행렬과  $n \times s$  행렬이라고 하십시오. (따라서  $AB$ 는  $s \times s$  행렬입니다.)  $|S| = s$ 인 임의의 부분집합  $S \subseteq \{1, 2, \dots, n\}$ 에 대해,  $A_S$ 를 인덱스가  $S$ 에 속하는 행들로 이루어진  $A$ 의  $s \times s$  부분행렬이라 하고,  $B_S$ 를 인덱스가  $S$ 에 속하는 열들로 이루어진  $B$ 의  $s \times s$  부분행렬이라고 하십시오. 다음을 증명하십시오.

$$\det(AB) = \sum_{|S|=s} \det A_S \det B_S.$$

# 13 내적 공간

$\mathbb{R}^n$ 을 닮은 우리의 벡터 공간들은 종종 덧셈의 개념뿐만 아니라 직교성의 개념과 거리의 개념도 갖고 있음이 밝혀지곤 합니다. 이 모든 것은 벡터 공간에 이른바 **내적 형식**을 부여함으로써 얻어지며, 이는  $\mathbb{R}^n$ 에서 여러분이 이미 "점곱"으로 알고 있을 가능성이 높습니다. 실제로  $\mathbb{R}^n$ 에서 여러분은 다음을 이미 알고 있습니다

- $v \cdot w = 0$ 인 것과  $v$ 와  $w$ 가 수직인 것은 동치이며
- $|v|^2 = v \cdot v$ .

이 장의 목적은 이 구조를 완전히 일반적인 형태로 신속하게 정립하는 것입니다. 이 장의 주요 내용은 다음과 같습니다

- 고등학교에서 배우는 "점곱" 공식이 실제로 매우 자연스러운 것임을 보게 될 것입니다. 즉, 위에서 나열한 두 공리로부터 자연스럽게 도출됩니다.  $\sum a_i b_i$ 가 왜 그토록 좋은 성질을 갖는지 궁금했던 적이 있다면, 이제 그 이유를 알게 될 것입니다.
- 내적 형식을 이용해  $V$ 를 거리 공간으로 만드는 방법을 보이며, 이를 통해  $V$ 에 더 풍부한 기하학적 구조를 부여합니다.
- 몇 장 뒤에서는 이전에는 불가능했던 방식으로  $V \cong V^*$ 를 동일시할 것이며, 그 따름 정리로서 실수 성분을 갖는 대칭 행렬은 항상 실수 고윳값을 가진다는 훌륭한 결과를 이끌어낼 것입니다.

이 장 전체에서, 별도로 명시하지 않는 한 모든 벡터 공간은  $\mathbb{C}$  또는  $\mathbb{R}$  위에서 정의됩니다.  $\mathbb{C}$ 가 대수적으로 닫혀 있으므로(따라서 예를 들어 요르단 형식을 가질 수 있으므로) 우리는 일반적으로  $\mathbb{R}$  대신  $\mathbb{C}$  위에서 작업하는 쪽을 선호할 것입니다. 어차피 모든 실수 행렬은 복소수 성분을 갖는 행렬로 생각할 수 있습니다.

## §13.1 내적

이 절의 대표적인 예:  $\mathbb{R}^n$ 에서의 점곱.

### §13.1.i 실수의 경우: 쌍선형 형식

먼저 실수 공간에 대한 내적 형식을 정의해 보겠습니다. 일반적인 벡터 공간에 대해서는  $v \cdot w$ 라는 표기법보다  $\langle v, w \rangle$ 를 사용하는 것이 가장 일반적입니다.

**정의 13.1.1.**  $V$ 를 실수 벡터 공간이라 합시다. **실수 내적 형식**<sup>1</sup>은 다음과 같은 함수입니다

$$\langle \bullet, \bullet \rangle : V \times V \rightarrow \mathbb{R}$$

다음 성질들을 만족합니다

- 이 형식은 **대칭**입니다: 임의의  $v, w \in V$ 에 대해 다음이 성립합니다

$$\langle v, w \rangle = \langle w, v \rangle.$$

물론 곱셈이라면 당연히 기대할 만한 성질입니다.

<sup>1</sup>다른 이름으로는 "내적", "점곱", "양의 정부호 비퇴화 대칭 쌍선형 형식" ...등이 있습니다

- 이 형식은 **쌍선형**, 즉 **양쪽 인자에 대해 선형**입니다. 이는 임의로 고정된  $v$ 에 대해  $\langle -, v \rangle$ 와  $\langle v, - \rangle$ 가 선형 함수임을 의미합니다. 명시적으로 풀어 쓰면 다음을 의미합니다

$$\begin{aligned}\langle cx, v \rangle &= c \langle x, v \rangle \\ \langle x + y, v \rangle &= \langle x, v \rangle + \langle y, v \rangle.\end{aligned}$$

그리고  $v$ 가 왼쪽에 있는 경우에도 마찬가지입니다. 이는 종종 하나의 식  $\langle cx + y, z \rangle = c \langle x, z \rangle + \langle y, z \rangle$ 로 요약됩니다.

- 이 형식은 **양의 정부호**입니다. 즉  $\langle v, v \rangle \geq 0$ 은 음이 아닌 실수이며, 등호는  $v = 0_V$ 일 때만 성립합니다.

**연습문제 13.1.2.** 첫 번째 인자에 대한 선형성과 대칭성만으로 이미 두 번째 인자에 대한 선형성이 얻어짐을 보이십시오. 따라서 위의 정의를  $\langle -, v \rangle$ 가 선형이라는 조건만 요구하는 것으로 수정할 수 있습니다.

### 예제 13.1.3 ( $\mathbb{R}^n$ )

이미 알고 있듯이,  $\mathbb{R}^n$  위의 내적 형식은 다음과 같이 정의할 수 있습니다.  $e_1 = (1, 0, \dots, 0)$ ,  $e_2 = (0, 1, \dots, 0)$ , ...,  $e_n = (0, \dots, 0, 1)$ 을 통상적인 기저라고 합시다. 그러면 다음과 같이 정의합니다

$$\langle a_1 e_1 + \dots + a_n e_n, b_1 e_1 + \dots + b_n e_n \rangle := a_1 b_1 + \dots + a_n b_n.$$

이것이 쌍선형(양쪽 인자에 대해 대칭이고 선형)임을 확인하는 것은 쉽습니다. 이것이 양의 정부호임을 확인하려면,  $a_i = b_i$ 일 때 점곱이  $a_1^2 + \dots + a_n^2$ 이 되며, 이는 모든  $a_i$ 가 0일 때만 0이 됨에 주목하십시오.

## §13.1.ii 복소수의 경우: 세스퀴선형 형식

복소 내적 공간에 대한 정의도 이와 유사하지만 한 가지 차이가 있습니다: 대칭 대신 켤레 대칭, 즉  $\langle v, w \rangle = \overline{\langle w, v \rangle}$ 을 갖습니다. 따라서 첫 번째 인자에 대해서는 여전히 선형성을 갖지만, 두 번째 인자에 대해서는 실제로 다른 형태의 선형성을 갖게 됩니다. 명시적으로 쓰면 다음과 같습니다

**정의 13.1.4.**  $V$ 를 복소 벡터 공간이라 합시다. **복소 내적**은 다음 함수입니다

$$\langle \bullet, \bullet \rangle : V \times V \rightarrow \mathbb{C}$$

이는 다음 성질들을 만족합니다:

- 이 형식은 **켤레 대칭성**을 가지며, 이는 임의의  $v, w \in V$ 에 대해 다음이 성립함을 의미합니다

$$\langle v, w \rangle = \overline{\langle w, v \rangle}.$$

- 이 형식은 **반쌍선형**입니다(이 이름은 "1과 2분의 1 선형"을 의미합니다). 이는 다음을 의미합니다:

– 이 형식은 **첫 번째 인자에 대해 선형**이며, 따라서 다시 다음이 성립합니다

$$\begin{aligned}\langle x + y, v \rangle &= \langle x, v \rangle + \langle y, v \rangle \\ \langle cx, v \rangle &= c \langle x, v \rangle.\end{aligned}$$

이는 문헌에서 종종  $\langle cx + y, v \rangle = c \langle x, v \rangle + \langle y, v \rangle$ 라는 한 줄로 축약됩니다.

- 그러나 이제 이는 **두 번째 인자에 대해 반선형**입니다: 임의의 복소수  $c$ 와 벡터  $x, y$ 에 대해 다음이 성립합니다

$$\begin{aligned}\langle v, x+y \rangle &= \langle v, x \rangle + \langle v, y \rangle \\ \langle v, cx \rangle &= \bar{c} \langle v, x \rangle.\end{aligned}$$

새롭게 등장한 복소켈레  $\bar{c}$ 에 주목하십시오! 마찬가지로, 한 방정식만 쓰고자 한다면 이를 그저  $\langle v, cx+y \rangle = \bar{c} \langle v, x \rangle + \langle v, y \rangle$ 로 축약할 수 있습니다.

- 이 형식은 **양의 정부호**이며, 이는  $\langle v, v \rangle$ 가 음이 아닌 실수이고  $v = 0_V$ 일 때 정확히 영이 됨을 의미합니다.

**연습문제 13.1.5.** 반선형성이 켈레 대칭성과 첫 번째 인자에 대한 선형성으로부터 따라 나옴을 보이십시오.

### 예제 13.1.6 ( $\mathbb{C}^n$ )

$\mathbb{C}^n$ 에서의 내적은 다음과 같이 정의됩니다:  $e_1, e_2, \dots, e_n$ 을 표준 기저라 합시다. 복소수  $w_i, z_i$ 에 대해 다음과 같이 놓습니다

$$\langle w_1 e_1 + \dots + w_n e_n, z_1 e_1 + \dots + z_n e_n \rangle := w_1 \bar{z}_1 + \dots + w_n \bar{z}_n.$$

**질문 13.1.7.** 위의 것이 실제로 복소 내적 형식임을 확인하십시오.

## §13.1.iii 내적 공간

두 종류의 공간을 동시에 다루는 것이 유용할 것입니다:

**정의 13.1.8. 내적 공간**은 실 내적 형식을 갖춘 실 벡터 공간이거나, 복소 내적 형식을 갖춘 복소 벡터 공간입니다.

내적 공간 사이의 선형 사상은 기저의 벡터 공간 사이의 사상입니다(내적 형식과의 호환성은 요구하지 않습니다).

**비고 13.1.9 (왜 반쌍선형인가?)** — 위의 예는 단순한 대칭성이 아니라 켈레 대칭성을 만족시키고자 하는 한 가지 이유를 설명합니다. 만약 내적을  $\sum w_i z_i$ 로 정의하려 했다면, 양의 정부호 조건을 잃었을 것입니다. 왜냐하면  $\langle v, v \rangle = \sum z_i^2$ 가 실수가 되리라는 보장이 전혀 없기 때문입니다. 반면, 켈레 대칭성을 통해 우리는 실제로  $\langle v, v \rangle = \overline{\langle v, v \rangle}$ , 즉 모든  $v$ 에 대해  $\langle v, v \rangle \in \mathbb{R}$ 임을 강제합니다.

이 점을 좀 더 강하게 짚어봅시다. 복소 벡터 공간  $V$  위에 쌍선형 형식  $\langle -, - \rangle$ 를 두고자 시도했다고 합시다.  $e$ 를  $\langle e, e \rangle = 1$ 인 임의의 벡터(단위 벡터)라 합시다. 그러면 대신  $\langle ie, ie \rangle = -\langle e, e \rangle = -1$ 을 얻게 될 것입니다; 이는 길이가  $\sqrt{-1}$ 인 벡터인데, 이는 말이 되지 않습니다! 이것이 바로 복소 내적 공간을 다룰 때 우리의 형식이 쌍선형이 아니라 반쌍선형이어야 하는 이유입니다.

이제 내적을 갖추었으므로, 노름과 직교성에 대해 이야기할 수 있습니다.

## §13.2 노름

**이 절의 대표적인 예:**  $\mathbb{R}^n$ 은 벡터 노름과 함께 통상적인 유클리드 공간이 됩니다.

내적 형식은 우리의 벡터 공간에 거리라는 개념을 부여하며, 이를 노름이라 부릅니다.

**정의 13.2.1.**  $V$ 를 내적 공간이라 합시다.  $v \in V$ 의 **노름**은 다음과 같이 정의됩니다

$$\|v\| = \sqrt{\langle v, v \rangle}.$$

이 정의가 성립하는 이유는 우리가 형식을 양의 정부호라고 가정했으므로  $\langle v, v \rangle$ 가 음이 아닌 실수이기 때문입니다.

**예제 13.2.2** ( $\mathbb{R}^n$ 과  $\mathbb{C}^n$ 은 노름 벡터 공간입니다)

$V = \mathbb{R}^n$  또는  $V = \mathbb{C}^n$ 이고 표준 내적 노름을 사용하는 경우,  $v$ 의 노름은 우리에게 익숙한 절댓값에 대응합니다.

이제 우리의 목표는 다음을 증명하는 것입니다

**거리**  $d(v, w) = \|v - w\|$ 를 사용하면,  $V$ 는 거리 공간이 됩니다.

**질문 13.2.3.**  $d(v, w) = 0$ 인 것과  $v = w$ 인 것이 동치임을 확인하십시오.

그러므로 우리는 삼각부등식만 증명하면 됩니다. 이제 우리 모두가 알고 좋아하는 사실을 증명해 봅시다. 이는 나중에 디딤돌이 될 것입니다:

**보조정리 13.2.4** (코시-슈바르츠)

$V$ 를 내적 공간이라 합시다. 임의의  $v, w \in V$ 에 대해 다음이 성립합니다

$$|\langle v, w \rangle| \leq \|v\| \|w\|$$

여기서 등호는  $v$ 와  $w$ 가 선형종속인 경우에만 성립합니다.

증명.  $\langle v, w \rangle = 0$ 이면 이 정리는 자명합니다.  $\|v\| \|w\| = 0$ 인 경우도 자명한데, 이때는  $v$  또는  $w$  중 하나가 영벡터이기 때문입니다. 따라서 앞으로는 이 모든 값이 0이 아니라고 가정합니다(나중에 이 값들로 나누어야 하기 때문입니다).

증명의 핵심은 등호가 성립하는 경우를 생각해 보는 것입니다: 우리는 부등식  $\langle cv - w, cv - w \rangle \geq 0$ 을 사용할 것입니다.  $c$ 의 선택은 나중에 미루고, 다음을 계산합니다

$$\begin{aligned} 0 &\leq \langle cv - w, cv - w \rangle \\ &= \langle cv, cv \rangle - \langle cv, w \rangle - \langle w, cv \rangle + \langle w, w \rangle \\ &= |c|^2 \langle v, v \rangle - c \langle v, w \rangle - \bar{c} \langle w, v \rangle + \langle w, w \rangle \\ &= |c|^2 \|v\|^2 + \|w\|^2 - c \langle v, w \rangle - \bar{c} \overline{\langle v, w \rangle} \\ 2 \operatorname{Re} [c \langle v, w \rangle] &\leq |c|^2 \|v\|^2 + \|w\|^2 \end{aligned}$$

이 시점에서  $c$ 의 좋은 선택은

$$c = \frac{\|w\|}{\|v\|} \cdot \frac{|\langle v, w \rangle|}{\langle v, w \rangle}$$

그러면

$$c \langle v, w \rangle = \frac{\|w\|}{\|v\|} |\langle v, w \rangle| \in \mathbb{R}$$

$$|c| = \frac{\|w\|}{\|v\|}$$

따라서 부등식은 다음과 같이 됩니다

$$2 \frac{\|w\|}{\|v\|} |\langle v, w \rangle| \leq 2 \|w\|^2$$

$$|\langle v, w \rangle| \leq \|v\| \|w\|.$$

□

따라서:

### 정리 13.2.5 (삼각부등식)

우리는 항상 다음을 가집니다

$$\|v\| + \|w\| \geq \|v + w\|$$

여기서 등호는  $v$ 와  $w$ 가 선형종속이고 같은 방향을 가리키는 경우에만 성립합니다.

**연습문제 13.2.6.** 양변을 제곱하고 코시-슈바르츠 부등식을 적용하여 이를 증명하십시오.

이렇게 하여 우리의 벡터 공간은 이제 거리 공간이라는 위상 구조를 가지게 됩니다.

## §13.3 직교성

**이 절의 대표적인 예:** 여전히  $\mathbb{R}^n$ 입니다!

우리의 다음 목표는 "수직"이라는 기하학적 개념을 제시하는 것입니다. 정의는 충분히 쉽습니다:

**정의 13.3.1.** 내적 공간에서 두 개의 영이 아닌 벡터  $v$ 와  $w$ 는  $\langle v, w \rangle = 0$ 일 때 **직교**한다고 합니다.

$\mathbb{R}^n$ 에서의 기하학적 직관에서 예상할 수 있듯이, 이는 독립성을 함의합니다:

### 보조정리 13.3.2 (직교하는 벡터는 독립적입니다)

각  $i$ 에 대해  $\|v_i\| \neq 0$ 인, 쌍마다 직교하는 벡터들의 임의의 집합  $v_1, v_2, \dots, v_n$ 은 선형독립입니다.

증명. 다음과 같은 종속관계를 생각해 봅시다

$$a_1 v_1 + \dots + a_n v_n = 0$$

$a_i$ 가  $\mathbb{R}$  또는  $\mathbb{C}$ 에 속한다고 합시다. 그러면

$$0 = \left\langle v_1, \sum a_i v_i \right\rangle = \overline{a_1} \|v_1\|^2.$$

따라서  $\|v_1\| \neq 0$ 이라고 가정했으므로  $a_1 = 0$ 입니다. 마찬가지로  $a_2 = \dots = a_n = 0$ 입니다. □

이를 바탕으로, 이제 우리의 기저에 대해 더 강한 조건을 고려해 볼 수 있습니다.

**정의 13.3.3.** 유한 차원 내적 공간  $V$ 의 **정규직교** 기저란, 모든  $i$ 에 대해  $\|e_i\| = 1$ 이고  $i \neq j$ 인 임의의 경우에  $\langle e_i, e_j \rangle = 0$ 을 만족하는 기저  $e_1, \dots, e_n$ 을 말합니다.

**예제 13.3.4** ( $\mathbb{R}^n$ 과  $\mathbb{C}^n$ 은 표준 기저를 가집니다)

표준 내적을 갖춘  $\mathbb{R}^n$ 과  $\mathbb{C}^n$ 에서, 표준 기저  $e_1, \dots, e_n$  또한 정규직교입니다.

이는 일반성을 잃지 않습니다:

**정리 13.3.5** (그람-슈미트)

$V$ 를 유한 차원 내적 공간이라고 합시다. 그러면  $V$ 는 정규직교 기저를 가집니다.

증명 개요.  $V$ 의 임의의 기저  $e_1, \dots, e_n$ 으로부터 정규직교 기저를 명시적으로 구성할 수 있습니다.  $\text{proj}_u(v) = \frac{\langle v, u \rangle}{\langle u, u \rangle} u$ 로 정의합니다. 그런 다음 재귀적으로 다음과 같이 정의합니다

$$\begin{aligned} u_1 &= e_1 \\ u_2 &= e_2 - \text{proj}_{u_1}(e_2) \\ u_3 &= e_3 - \text{proj}_{u_1}(e_3) - \text{proj}_{u_2}(e_3) \\ &\vdots \\ u_n &= e_n - \text{proj}_{u_1}(e_n) - \dots - \text{proj}_{u_{n-1}}(e_n). \end{aligned}$$

$u_i$ 가 쌍마다 직교하며 영이 아님을 보일 수 있습니다. □

따라서 우리는 일반적으로 기저가 정규직교라고 가정할 수 있습니다.  
언급할 만한 점:

**예제 13.3.6** (점곱은 “유일한” 내적 형식입니다)

$V$ 를 유한 차원 내적 공간이라고 하고, 임의의 정규직교 기저  $e_1, \dots, e_n$ 을 생각합시다. 그러면 다음이 성립합니다

$$\langle a_1 e_1 + \dots + a_n e_n, b_1 e_1 + \dots + b_n e_n \rangle = \sum_{i,j=1}^n a_i \overline{b_j} \langle e_i, e_j \rangle = \sum_{i=1}^n a_i \overline{b_i}$$

이는  $\{e_i\}$ 가 정규직교라는 사실에서 비롯됩니다.

이제 여러분은 점곱 표현이 왜 그렇게 널리 쓰이는지 알게 되었습니다.

## §13.4 힐베르트 공간

대수학에서는 대개 무한을 경계하기 때문에, 여러 장 앞서 평범한 벡터 공간의 기저를 정의했을 때 우리는 유한 선형결합만을 허용했습니다. 그러나 내적 공간이 있다면 그것은 거리 공간이며, 우리는 때때로 실제로 수렴에 대해 이야기할 수 있습니다.

그 방법은 다음과 같습니다:

**정의 13.4.1.** **힐베르트 공간**이란, 대응하는 거리 공간이 완비인 내적 공간  $V$ 를 말합니다.

이 경우, 부분합의 수열을 살펴보고 그것을 수렴하게 함으로써 이제 무한 선형결합을 취하는 것이 종종 의미를 가지게 됩니다. 그 방법은 다음과 같습니다. 노름이 1이고 쌍마다 직교하는 무한 벡터 수열  $e_1, e_2, \dots$ 가 있다고 합시다.  $c_1, c_2, \dots$ 가 실수 또는 복소수의 수열이라고 합시다. 그러면 다음 수열을 생각합시다

$$\begin{aligned} v_1 &= c_1 e_1 \\ v_2 &= c_1 e_1 + c_2 e_2 \\ v_3 &= c_1 e_1 + c_2 e_2 + c_3 e_3 \\ &\vdots \end{aligned}$$

**명제 13.4.2 (힐베르트 공간에서의 수렴 판정 기준)**

위에서 정의한 수열  $(v_i)$ 는  $\sum |c_i|^2 < \infty$ 일 때, 그리고 오직 그때에만 수렴합니다.

증명. **장 26**를 읽었다면 이 내용이 더 잘 이해될 것이므로, 아직 그 장을 읽지 않았다면 이 증명은 건너뛰어도 좋습니다. 수열  $v_i$ 는 코시 수열일 때, 그리고 오직 그때에만 수렴하며, 이는  $i < j$ 일 때 다음을 의미합니다

$$\|v_j - v_i\|^2 = |c_{i+1}|^2 + \dots + |c_j|^2$$

$i$ 와  $j$ 가 커짐에 따라 0으로 수렴합니다. 이는 수열  $s_n = |c_1|^2 + \dots + |c_n|^2$ 이 코시 수열임과 동치입니다.

$\mathbb{R}$ 이 완비이므로,  $s_n$ 이 코시 수열인 것과 수렴하는 것은 동치입니다.  $s_n$ 이 음이 아닌 실수들로 이루어져 있으므로, 수렴은  $s_n$ 이 유계인 것과 동치이며, 이는 다시  $\sum |c_i|^2 < \infty$ 인 것과 동치입니다.  $\square$

따라서 힐베르트 공간을 다룰 때는 정의를 약간 바꿉니다:

**정의 13.4.3.** 힐베르트 공간  $V$ 에 대한 **정규직교 기저**란 다음을 만족하는 (무한할 수도 있는) 벡터열  $e_1, e_2, \dots$ 입니다.

- 모든  $i$ 에 대해  $\langle e_i, e_i \rangle = 1$ 이고,
- $i \neq j$ 일 때  $\langle e_i, e_j \rangle = 0$ , 즉 벡터들이 쌍마다 직교하며
- $V$ 의 모든 원소는 다음과 같은 무한 선형결합으로 유일하게 표현할 수 있습니다

$$\sum_i c_i e_i$$

여기서 앞서 설명한 대로  $\sum_i |c_i|^2 < \infty$ 입니다.

어쨌든 이것이 공식적인 정의입니다. ( $\dim V < \infty$ 이면 이 정의는 우리가 흔히 쓰는 정의와 일치함에 주목하십시오. 그 경우  $e_i$ 가 유한 개밖에 없기 때문입니다.) 하지만 우리의 목적을 위해서는 대체로 이를 신경 쓰지 않고 다음과 같이 생각해도 됩니다:

**힐베르트 공간이란 기저가 유한 선형결합뿐 아니라 무한 선형결합까지 필요로 하는 내적 공간입니다.**

$\sum |c_i|^2 < \infty$ 라는 기술적 조건은 바로 무한합이 의미를 갖도록 보장해 주는 조건입니다.

## §13.5 생각해 볼 만한 조금 더 어려운 문제

**문제 13A** (피타고라스 정리). 내적 공간에서  $\langle v, w \rangle = 0$ 이면  $\|v\|^2 + \|w\|^2 = \|v + w\|^2$ 임을 보이십시오.

**문제 13B\*** (유한 차원  $\implies$  힐베르트). 유한 차원 내적 공간은 힐베르트 공간임을 보이십시오.



**문제 13C** (대만 IMO 캠프). 어느 마을에  $n$ 명의 사람과  $k$ 개의 동아리가 있습니다. 각 동아리의 회원 수는 홀수이고, 임의의 두 동아리는 짝수 명의 공통 회원을 가집니다.  $k \leq n$ 임을 증명하십시오.

**문제 13D\*** (텐서의 내적 구조).  $V$ 와  $W$ 를  $k$  위의 유한 차원 내적 공간이라 합시다. 여기서  $k$ 는  $\mathbb{R}$ 이거나  $\mathbb{C}$ 입니다.

(a)  $V \otimes_k W$ 도 내적 공간으로 만드는 정준적인 방법을 찾으십시오.

(b)  $e_1, \dots, e_n$ 을  $V$ 의 정규직교 기저라 하고,  $f_1, \dots, f_m$ 을  $W$ 의 정규직교 기저라 합시다.  $V \otimes W$ 의 정규직교 기저는 무엇입니까?



**문제 13E** (Putnam 2014).  $n$ 을 양의 정수라고 합시다. 실수 성분을 갖는  $n \times n$  행렬  $M_1, \dots, M_k$ 과  $N_1, \dots, N_k$ 이 존재하여, 모든  $i$ 와  $j$ 에 대해 행렬 곱  $M_i N_j$ 의 대각선 어딘가에 0인 성분이 있는 것이  $i \neq j$ 와 동치가 되도록 하는 가장 큰  $k$ 는 무엇입니까?

**문제 13F** (수열 공간).  $\sum_i a_i^2 < \infty$ 를 만족하는 실수 무한수열  $a = (a_1, a_2, \dots)$ 들의 공간  $\ell^2$ 를 생각합시다. 이 공간에 다음과 같은 내적을 부여합니다

$$\langle a, b \rangle = \sum_i a_i b_i.$$

이것은 힐베르트 공간입니까? 그렇다면 힐베르트 기저를 하나 밝히십시오.

**문제 13G** (일반적인 노름 벡터 공간). 내적 공간을 일반화하면, **노름 벡터 공간**이란 다음 공리들을 만족하는 임의의 노름 함수  $\|\bullet\| : V \rightarrow \mathbb{R}$ 를 갖춘,  $\mathbb{R}$  또는  $\mathbb{C}$  위의 벡터 공간  $V$ 입니다:

- 모든  $v \in V$ 에 대해  $\|v\| \geq 0$ 이며, 등호는  $v$ 가 영벡터일 때에만 성립합니다.
- 스칼라  $\lambda$ 에 대해  $\|\lambda v\| = |\lambda| \cdot \|v\|$ 가 성립합니다.
- 모든  $v$ 와  $w$ 에 대해 삼각부등식  $\|v + w\| \leq \|v\| + \|w\|$ 가 성립합니다.

따라서 **정리 13.2.5**는, 임의의 내적 공간이 노름을  $\|v\| := \sqrt{\langle v, v \rangle}$ 로 택함으로써 노름 벡터 공간이 된다는 진술로 바꾸어 말할 수 있습니다.

$n \geq 2$ 에 대해  $\mathbb{R}^n$  위에 다음과 같이 노름을 정의할 수 있음을 증명하여, 그 역이 성립하지 않음을 보이십시오

$$\|(x_1, \dots, x_n)\| := \sum_{i=1}^n |x_i|$$

그리고 나아가 이 노름이 어떤 내적으로부터도 나오지 않음을 보이십시오.

**문제 13H** (쿠라토프스키 매장). **바나흐 공간**이란 대응하는 거리 공간이 완비인 노름 벡터 공간  $V$ 입니다. (따라서 힐베르트 공간은 바나흐 공간의 특수한 경우입니다.)

$(M, d)$ 를 임의의 거리 공간이라 하겠습니다. 바나흐 공간  $X$ 와 단사 함수  $f : M \hookrightarrow X$ 가 존재하여 임의의  $x$ 와  $y$ 에 대해  $d(x, y) = \|f(x) - f(y)\|$ 가 성립함을 증명하십시오.

# 14 보너스: 푸리에 해석

추상적인 내적 공간을 정의하기 위해 열심히 작업했으니, 이제 이 언어를 사용하여 푸리에 해석을 올바르게 설정하는 방법이라는 (선택적) 응용을 제시하고자 합니다.

재미 삼아, 이진 푸리에 해석을 사용하여 애로우의 불가능성 정리의 한 형태도 증명합니다.

이어지는 내용에서는  $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ 가 "원군"을 나타낸다고 하고, 이를 "법 1에 대한 실수"의 덧셈군으로 생각합니다.  $\mathbb{T}$ 를 복소 단위원으로 보내는 표준 사상  $e: \mathbb{T} \rightarrow \mathbb{C}$ 가 존재하며, 이는 다음과 같이 주어집니다

$$e(\theta) = \exp(2\pi i\theta).$$

## §14.1 개요

정의역  $Z$ 가 있고 함수  $f: Z \rightarrow \mathbb{C}$ 에 관심이 있다고 합시다. 자연스럽게, 이러한 함수들의 집합은 복소 벡터 공간을 이룹니다. 우리는 이러한 함수들의 집합에 양의 정부호 내적을 부여하고자 합니다.

푸리에 해석의 아이디어는 이 함수들의 집합에 대해 정규직교 기저를 선택하는 것으로, 이를  $(e_\xi)_\xi$ 라 하고 **지표(characters)**라고 부릅니다. 첨수  $\xi$ 는 **진동수(frequencies)**라고 부릅니다. 이 경우 기저가 있으므로, 모든 함수  $f: Z \rightarrow \mathbb{C}$ 는 다음과 같은 합이 됩니다

$$f(x) = \sum_{\xi} \hat{f}(\xi) e_{\xi}$$

여기서  $\hat{f}(\xi)$ 는 기저의 복소 계수이며, 이에 걸맞게  $\hat{f}$ 를 **푸리에 계수**라고 부릅니다. 변수  $x \in Z$ 는 **물리적** 변수라고 부릅니다. 이는 일반적으로 유용한데, 지표들이 사인파나 코사인파, 또는 기타 주기 함수와 같이 좋은 "대칭" 함수가 되도록 의도적으로 선택되었기 때문입니다. 이렇게 하여 우리는 임의로 복잡한 함수를 좋은 함수들의 합으로 분해합니다.

## §14.2 힐베르트 공간에 대한 상기

편의를 위해, 정규직교 기저에 관한 몇 가지 사실을 기록해 둡니다.

### 명제 14.2.1 (정규직교 기저에 관한 사실들)

$V$ 가 내적 형식  $\langle -, - \rangle$ 을 갖는 복소 힐베르트 공간이라 하고,  $x = \sum_{\xi} a_{\xi} e_{\xi}$ ,  $y = \sum_{\xi} b_{\xi} e_{\xi}$ 이며  $e_{\xi}$ 가 정규직교 기저라고 합시다. 그러면

$$\begin{aligned}\langle x, x \rangle &= \sum_{\xi} |a_{\xi}|^2 \\ a_{\xi} &= \langle x, e_{\xi} \rangle \\ \langle x, y \rangle &= \sum_{\xi} a_{\xi} \overline{b_{\xi}}.\end{aligned}$$

**연습문제 14.2.2.** 이 모두를 증명하십시오. (앞 절의 내용은 필요하지 않으며, 무서운  $\xi$ 들이 잔뜩 있는 표기법에 동기를 부여하기 위해서만 존재합니다.)

이어지는 내용에서, 대부분의 예시는 유한 차원 내적 공간(따라서 힐베르트 공간)에 관한 것이지만, "제곱 가측분 함수"의 예시는 실제로 무한 차원 예시가 될 것입니다. 다행히도, 앞서 언급했듯이 이는 걱정할 이유가 되지 않으며, 대체로 눈을 감고 무한대에 대해 신경 쓰지 않아도 됩니다.

## §14.3 혼한 예시들

### §14.3.i $\{\pm 1\}^n$ 위의 이진 푸리에 해석

어떤 양의 정수  $n$ 에 대해  $Z = \{\pm 1\}^n$ 이라 하면, 이진 값을 받는 함수  $f(x_1, \dots, x_n)$ 을 고려하는 셈입니다. 그러면 함수  $Z \rightarrow \mathbb{C}$ 들은  $2^n$ 차원 벡터 공간  $\mathbb{C}^Z$ 를 이루며, 여기에 다음과 같은 내적 형식을 부여합니다

$$\langle f, g \rangle = \frac{1}{2^n} \sum_{x \in Z} f(x) \overline{g(x)}.$$

특히,

$$\langle f, f \rangle = \frac{1}{2^n} \sum_{x \in Z} |f(x)|^2$$

는 제곱들의 평균이며, 이는 또한  $\langle -, - \rangle$ 이 양의 정부호임을 보여줍니다.

이 경우, **다중선형 다항식**들이  $\mathbb{C}^Z$ 의 기저를 이루는데, 이는 다음 다항식들입니다

$$\chi_S(x_1, \dots, x_n) = \prod_{s \in S} x_s.$$

**연습문제 14.3.1.** 이들이  $\langle -, - \rangle$  하에서 실제로 정규직교임을 보이십시오.  $2^n$ 개가 있으므로, 이는 이들이 기저를 이룬을 증명합니다.

따라서 우리의 진동수 집합은 실제로 부분집합  $S \subseteq \{1, \dots, n\}$ 들입니다. 따라서 우리는 다음과 같은 분해를 얻습니다

$$f = \sum_{S \subseteq \{1, \dots, n\}} \hat{f}(S) \chi_S.$$

#### 예제 14.3.2 (이진 푸리에 해석의 예시)

$n = 2$ 라 합시다. 그러면 이진 함수  $\{\pm 1\}^2 \rightarrow \mathbb{C}$ 는 다음 네 다항식으로 주어지는 기저를 갖습니다

$$1, \quad x_1, \quad x_2, \quad x_1 x_2.$$

예를 들어,  $(1, 1)$ 에서 1이고 그 외에서는 0인 함수  $f$ 를 생각해 봅시다. 그러면 다음과 같이 둘 수 있습니다

$$f(x_1, x_2) = \frac{x_1 + 1}{2} \cdot \frac{x_2 + 1}{2} = \frac{1}{4} (1 + x_1 + x_2 + x_1 x_2).$$

따라서 네 개의  $S$  각각에 대해 푸리에 계수는  $\hat{f}(S) = \frac{1}{4}$ 입니다.

이 개념은 특히 이진 함수  $f: \{\pm 1\}^n \rightarrow \{\pm 1\}$ 에 유용합니다; 이러한 함수(및 이들의 곱)에 대해서는 항상  $\langle f, f \rangle = 1$ 이 성립합니다.

진동수  $\emptyset$ 가 특별한 역할을 한다는 점은 주목할 만합니다:

**연습문제 14.3.3.** 다음을 보이십시오

$$\widehat{f}(\emptyset) = \frac{1}{|Z|} \sum_{x \in Z} f(x).$$

### §14.3.ii 유한군 $Z$ 위의 푸리에 해석

이번에는 유한 아벨 군  $Z$ 가 있고, 함수  $Z \rightarrow \mathbb{C}$ 를 고려한다고 합시다; 이는  $|Z|$ 차원 벡터 공간입니다. 내적은 이전과 동일합니다:

$$\langle f, g \rangle = \frac{1}{|Z|} \sum_{x \in Z} f(x) \overline{g(x)}.$$

진행하려면  $Z$ 의 두 원소를 곱할 수 있어야 합니다. 실제로는 어떤 사상을 선택하든 별로 중요하지 않기 때문에 이는 다소 성가신 일이므로, 빠르게 넘어가겠습니다; 나머지 단락의 대부분 또는 전체를 건너뛰어도 무방합니다.

**정의 14.3.4.** 우리는 대칭 비퇴화 쌍선형 형식을 선택합니다

$$\cdot : Z \times Z \rightarrow \mathbb{T}$$

다음 성질을 만족하는:

- $\xi \cdot (x_1 + x_2) = \xi \cdot x_1 + \xi \cdot x_2$ 이고  $(\xi_1 + \xi_2) \cdot x = \xi_1 \cdot x + \xi_2 \cdot x$ 입니다 (이것이 "쌍선형"이라는 단어의 의미입니다)
- $\cdot$ 는 대칭입니다,
- 임의의  $\xi \neq 0$ 에 대해,  $\xi \cdot x \neq 0$ 인  $x$ 가 존재합니다 (이것이 "비퇴화"라는 단어의 의미입니다).

#### 예제 14.3.5 ( $\mathbb{Z}/n\mathbb{Z}$ 위의 형식)

$Z = \mathbb{Z}/n\mathbb{Z}$ 이면  $\xi \cdot x = (\xi x)/n$ 이 위의 성질을 만족합니다.

일반적으로 유한 아벨 군은 순환군들의 합으로 분해된다는 사실이 알려져 있으며(절 18.1 참고), 이로써 그러한  $\cdot$ 를 찾기가 비교적 쉬워집니다; 하지만 앞서 말했듯이 선택은 중요하지 않으므로 넘어가겠습니다.

이제 재미있는 부분입니다: 지표를 정의하겠습니다.

#### 명제 14.3.6 ( $e_\xi$ 는 정규직교입니다)

각  $\xi \in Z$ 에 대해 지표를 다음과 같이 정의합니다

$$e_\xi(x) = e(\xi \cdot x).$$

$|Z|$ 개의 지표는 함수  $Z \rightarrow \mathbb{C}$ 의 공간에서 정규직교 기저를 이룹니다.

증명. 이 부분은 건너뛰기를 권장하지만, 다음과 같습니다:

$$\begin{aligned}\langle e_\xi, e_{\xi'} \rangle &= \frac{1}{|Z|} \sum_{x \in Z} e(\xi \cdot x) \overline{e(\xi' \cdot x)} \\ &= \frac{1}{|Z|} \sum_{x \in Z} e(\xi \cdot x) e(-\xi' \cdot x) \\ &= \frac{1}{|Z|} \sum_{x \in Z} e((\xi - \xi') \cdot x).\end{aligned}$$

□

이렇게 하면 진동수의 집합도  $Z$ 가 되지만,  $\xi \in Z$ 는 "물리적인"  $x \in Z$ 와는 매우 다른 역할을 합니다. 다음은 이해에 도움이 될 만한 예시입니다.

#### 예제 14.3.7 (단위원의 세제곱근 필터)

$Z = \mathbb{Z}/3\mathbb{Z}$ 이고, 내적 형식이  $\xi \cdot x = (\xi x)/3$ 로 주어진다고 합시다.  $\omega = \exp(\frac{2}{3}\pi i)$ 를 단위원의 원시 세제곱근이라 합시다. 다음을 주목하십시오

$$e_\xi(x) = \begin{cases} 1 & \xi = 0 \\ \omega^x & \xi = 1 \\ \omega^{2x} & \xi = 2. \end{cases}$$

그러면  $f(0) = a$ ,  $f(1) = b$ ,  $f(2) = c$ 인  $f: Z \rightarrow \mathbb{C}$ 가 주어질 때, 다음을 얻습니다

$$f(x) = \frac{a+b+c}{3} \cdot 1 + \frac{a+\omega^2 b + \omega c}{3} \cdot \omega^x + \frac{a+\omega b + \omega^2 c}{3} \cdot \omega^{2x}.$$

이렇게 해서 변환이 다음과 같음을 유도합니다

$$\begin{aligned}\hat{f}(0) &= \frac{a+b+c}{3} \\ \hat{f}(1) &= \frac{a+\omega^2 b + \omega c}{3} \\ \hat{f}(2) &= \frac{a+\omega b + \omega^2 c}{3}.\end{aligned}$$

**연습문제 14.3.8.** 이진 푸리에 해석에서의  $\hat{f}(\emptyset)$ 와 유사하게, 이제 다음이 성립함을 보이십시오

$$\hat{f}(0) = \frac{1}{|Z|} \sum_{x \in Z} f(x).$$

올림피아드 참가자라면 앞선 예시를 "단위원근 필터"로 알아볼 수도 있는데, 바로 그 점이 핵심입니다. 구체적으로, 다음을 계산하고자 한다고 합시다

$$\binom{1000}{0} + \binom{1000}{3} + \cdots + \binom{1000}{999}.$$

이 경우, 우리는 다음 함수를 고려할 수 있습니다

$$w: \mathbb{Z}/3 \rightarrow \mathbb{C}.$$

이때  $w(0) = 1$ 이지만  $w(1) = w(2) = 0$ 입니다. 표기의 남용으로, 우리는  $w$ 를 함수  $w: \mathbb{Z} \rightarrow \mathbb{Z}/3 \rightarrow \mathbb{C}$ 로도 생각할 것입니다. 그러면 문제의 합은

$$\begin{aligned} \sum_n \binom{1000}{n} w(n) &= \sum_n \binom{1000}{n} \sum_{k=0,1,2} \hat{w}(k) \omega^{kn} \\ &= \sum_{k=0,1,2} \hat{w}(k) \sum_n \binom{1000}{n} \omega^{kn} \\ &= \sum_{k=0,1,2} \hat{w}(k) (1 + \omega^k)^{1000}. \end{aligned}$$

우리의 상황에서는  $\hat{w}(0) = \hat{w}(1) = \hat{w}(2) = \frac{1}{3}$ 이며, 원하는 합을 계산한 것입니다. 더 일반적으로, 우리는 임의의 주기적 가중치  $w$ 를 취하고 푸리에 해석을 사용하여 합산 순서를 바꿀 수 있습니다.

### 예제 14.3.9 (이진 푸리에 해석)

$Z = \{\pm 1\}^n$ 이 점별 곱셈 아래 아벨 군으로 간주되어  $(\mathbb{Z}/2\mathbb{Z})^{\oplus n}$ 과 동형이라고 합시다. 우리는 다음과 같이 정의된 점곱을 선택한다고 가정합니다

$$\xi \cdot x := \frac{1}{2} \sum_i \frac{\xi_i - 1}{2} \cdot \frac{x_i - 1}{2}$$

여기서  $\xi = (\xi_1, \dots, \xi_n)$ 이고  $x = (x_1, \dots, x_n)$ 입니다.

우리는 이것이 우리가 제시한 첫 번째 예와 일치한다고 주장합니다. 실제로,  $S \subseteq \{1, \dots, n\}$ 이라 하고  $\xi \in \{\pm 1\}^n$ 을  $S$ 에 속한 위치에서는  $-1$ 이고  $S$ 에 속하지 않은 위치에서는  $+1$ 인 것으로 둡시다. 그러면 앞선 예의 지표  $\chi_S$ 는 새로운 표기법에서의 지표  $e_\xi$ 와 일치합니다. 특히,  $\hat{f}(S) = \hat{f}(\xi)$ 입니다.

따라서 유한 군  $Z$  위의 푸리에 해석은 이진 푸리에 해석을 포함합니다.

### §14.3.iii 함수 $L^2([-\pi, \pi])$ 에 대한 푸리에 급수

이것은 가장 유명한 것이며, 따라서 여러분이 들어본 적이 있을 것입니다.

**정의 14.3.10.** 공간  $L^2([-\pi, \pi])$ 는 적분  $\int_{[-\pi, \pi]} |f(x)|^2 dx$ 가 존재하고 유한한 모든 함수  $f: [-\pi, \pi] \rightarrow \mathbb{C}$ 로 이루어지며, "거의 모든 곳에서" 0인 함수는 0과 같다고 간주하는 관계에 대해 몫을 취한 것입니다.<sup>1</sup>

이것은 다음에 따라 내적 공간으로 만들어집니다

$$\langle f, g \rangle = \frac{1}{2\pi} \int_{[-\pi, \pi]} f(x) \overline{g(x)} dx.$$

(증명하지는 않겠지만) 이것이 (무한 차원) 힐베르트 공간임이 밝혀집니다!

이제, 푸리에 해석의 아름다움은 이 공간이 훌륭한 기저를 가진다는 것입니다:

<sup>1</sup>우리는 이것을 아직 정의하지 않을 것인데, 지금으로서는 우리에게 중요하지 않기 때문입니다. 하지만 측도론을 다루는 부분에서 이에 대해 더 자세히 설명할 것입니다.

이것이 관련이 있는 한 지점이 있습니다. 우리는 종종 함수  $f$ 가  $f(-\pi) = f(\pi)$ 를 만족하기를 요구하는데, 이렇게 하면  $f$ 가 주기 함수가 되어 이를  $f: \mathbb{T} \rightarrow \mathbb{C}$ 로 생각할 수 있습니다. 이는 한 점에서의 값만 바꾸는 것이므로 본질적인 차이를 만들지 않습니다.

**정리 14.3.11 (고전적 푸리에 기저)**

각 정수  $n$ 에 대해, 다음을 정의합니다

$$e_n(x) = \exp(inx).$$

그러면  $e_n$ 은 힐베르트 공간  $L^2([-\pi, \pi])$ 의 정규직교 기저를 이룹니다.

따라서 이번에는 진동수 집합  $\mathbb{Z}$ 가 무한하며, 우리는 다음을 연습니다

$$f(x) = \sum_n \hat{f}(n) \exp(inx) \quad \text{거의 모든 곳에서}$$

여기서 계수  $\hat{f}(n)$ 은  $\sum_n |\hat{f}(n)|^2 < \infty$ 을 만족합니다. 진동수 집합이  $\mathbb{Z}$ 로 색인되므로, 색인이  $n \in \mathbb{Z}$ 라는 사실을 반영하여 우리는 이를 **푸리에 급수**라고 부릅니다.

**연습문제 14.3.12.** 다시 한 번 보이십시오

$$\hat{f}(0) = \frac{1}{2\pi} \int_{[-\pi, \pi]} f(x) dx.$$

**§14.4 요약, 그리고 또 다른 예고편**

우리는 다음 표에서 푸리에 해석의 다양한 유형들을 요약합니다.

| 유형     | 물리 변수                         | 주파수 변수                             | 기저 함수                 |
|--------|-------------------------------|------------------------------------|-----------------------|
| 이진     | $\{\pm 1\}^n$                 | 부분집합 $S \subseteq \{1, \dots, n\}$ | $\prod_{s \in S} x_s$ |
| 유한군    | $Z$                           | $\xi \in Z$ , 의 선택.                | $e(\xi \cdot x)$      |
| 푸리에 급수 | $\mathbb{T}$ 또는 $[-\pi, \pi]$ | $n \in \mathbb{Z}$                 | $\exp(inx)$           |
| 이산     | $\mathbb{Z}/n\mathbb{Z}$      | $\xi \in \mathbb{Z}/n\mathbb{Z}$   | $e(\xi x/n)$          |

저는  $Z = \mathbb{Z}/n\mathbb{Z}$ 인 네 번째 행을 슬쩍 끼워 넣었는데, 이는 두 번째 행의 특수한 경우이므로 놀랄 필요는 없습니다.

앞으로의 내용을 암시하며, 저는 [장 39](#)이 어떻게 시작하는지 힌트를 드리고 싶습니다. 이들 각각은 실제로  $G \rightarrow \mathbb{C}$ 의 함수들이 어떤 "쌍대"  $\hat{G}$ 에 대한 함수  $\hat{G} \rightarrow \mathbb{C}$ 로 어떻게 표현될 수 있는지에 관한 진술입니다. 그런 의미에서, 우리는 위의 표를 다음과 같이 다시 쓸 수 있습니다:

| 이름     | 정의역 $G$                        | 쌍대 $\hat{G}$                     | 지표                    |
|--------|--------------------------------|----------------------------------|-----------------------|
| 이진     | $\{\pm 1\}^n$                  | $S \subseteq \{1, \dots, n\}$    | $\prod_{s \in S} x_s$ |
| 유한군    | $Z$                            | $\xi \in \hat{Z} \cong Z$        | $e(\xi \cdot x)$      |
| 푸리에 급수 | $\mathbb{T} \cong [-\pi, \pi]$ | $n \in \mathbb{Z}$               | $\exp(inx)$           |
| 이산     | $\mathbb{Z}/n\mathbb{Z}$       | $\xi \in \mathbb{Z}/n\mathbb{Z}$ | $e(\xi x/n)$          |

측도를 적분한다는 것이 무엇을 의미하는지 알게 되면, 일반적으로 우리는 많은 서로 다른 정의역  $G$ 에 대해 무언가를 말할 수 있음이 밝혀질 것입니다. 이것이 바로 이른바 폰트라긴 쌍대성이며, 이는 [장 39](#)에서 후속 보너스로 다루어집니다.

**§14.5 Parseval과 그 친구들**

여기서는 많은 유명한 이름들을 빠르게 배울 수 있는 재미있는 절입니다. 기본적으로 [명제 14.2.1](#)의 세 가지 결과 각각을 우리의 푸리에 해석 맥락(여기서는 힐베르트 공간의 정규 직교 기저를 가지고 있습니다)으로 옮겨서 유명한 결과를 얻을 수 있습니다.

**따름정리 14.5.1 (Parseval 정리)**

$Z$ 가 유한 아벨 군일 때,  $f: Z \rightarrow \mathbb{C}$ 라 합시다. 그러면

$$\sum_{\xi} |\hat{f}(\xi)|^2 = \frac{1}{|Z|} \sum_{x \in Z} |f(x)|^2.$$

마찬가지로,  $f: [-\pi, \pi] \rightarrow \mathbb{C}$ 가 제곱 적분 가능하다면 그 푸리에 급수는 다음을 만족합니다

$$\sum_n |\hat{f}(n)|^2 = \frac{1}{2\pi} \int_{[-\pi, \pi]} |f(x)|^2 dx.$$

증명.  $\langle f, f \rangle$ 는 계수들의 제곱합과 같음을 기억하십시오. □

**따름정리 14.5.2 (푸리에 반전 공식)**

$Z$ 가 유한 아벨 군일 때,  $f: Z \rightarrow \mathbb{C}$ 라 합시다. 그러면

$$\hat{f}(\xi) = \frac{1}{|Z|} \sum_{x \in Z} f(x) \overline{e_{\xi}(x)}.$$

마찬가지로,  $f: [-\pi, \pi] \rightarrow \mathbb{C}$ 가 제곱 적분 가능하다면 그 푸리에 급수는 다음과 같이 주어집니다

$$\hat{f}(n) = \frac{1}{2\pi} \int_{[-\pi, \pi]} f(x) \exp(-inx) dx.$$

증명. 정규직교 기저  $(e_{\xi})_{\xi}$ 에서  $f$ 에서의  $e_{\xi}$ 의 계수는  $\langle f, e_{\xi} \rangle$ 임을 기억하십시오. □

**질문 14.5.3.** 위에서  $\xi = 0$ 일 때는 어떻게 됩니까?

**따름정리 14.5.4 (Plancherel 정리)**

$Z$ 가 유한 아벨 군일 때,  $f: Z \rightarrow \mathbb{C}$ 라 합시다. 그러면

$$\langle f, g \rangle = \sum_{\xi \in Z} \hat{f}(\xi) \overline{\hat{g}(\xi)}.$$

마찬가지로,  $f: [-\pi, \pi] \rightarrow \mathbb{C}$ 가 제곱 적분 가능하다면

$$\langle f, g \rangle = \sum_n \hat{f}(n) \overline{\hat{g}(n)}.$$

**질문 14.5.5.** (이전처럼) 한 줄로 이것을 증명하십시오.

## §14.6 응용: 바젤 문제

$L^2([-\pi, \pi])$  위의 푸리에 해석에 관한 재미있는 응용 하나는, 약간의 미적분학을 기꺼이 사용하려고만 한다면 그렇지 않으면 계산하기 어려운 몇몇 합을 얻을 수 있다는 것입니다.

여기 고전적인 예시가 있습니다:

**정리 14.6.1 (바젤 문제)**

다음이 성립합니다

$$\sum_{n \geq 1} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

증명은 확실히 제곱 적분 가능한 항등 함수  $f(x) = x$ 를 고려하는 것입니다. 그러면 Parseval에 의해 다음을 얻습니다

$$\sum_{n \in \mathbb{Z}} |\hat{f}(n)|^2 = \langle f, f \rangle = \frac{1}{2\pi} \int_{[-\pi, \pi]} |f(x)|^2 dx.$$

미적분학 계산을 하면 다음을 얻습니다

$$\frac{1}{2\pi} \int_{[-\pi, \pi]} x^2 dx = \frac{\pi^2}{3}.$$

한편, 이제 모든 푸리에 계수를 계산해 보겠습니다. 우리는 이미 다음을 얻었습니다

$$\hat{f}(0) = \frac{1}{2\pi} \int_{[-\pi, \pi]} f(x) dx = \frac{1}{2\pi} \int_{[-\pi, \pi]} x dx = 0.$$

$n \neq 0$ 일 때, 정의에 의해(거창한 표현을 쓰고 싶다면 "푸리에 반전 공식"에 의해) 다음 공식을 얻습니다

$$\begin{aligned} \hat{f}(n) &= \langle f, \exp(inx) \rangle \\ &= \frac{1}{2\pi} \int_{[-\pi, \pi]} x \cdot \overline{\exp(inx)} dx \\ &= \frac{1}{2\pi} \int_{[-\pi, \pi]} x \exp(-inx) dx. \end{aligned}$$

부정적분은  $\frac{1}{n^2} \exp(-inx)(1 + inx)$ 와 같으며, 따라서 조금 더 계산하면 다음을 얻습니다

$$\hat{f}(n) = \frac{(-1)^n}{n} i.$$

그러므로

$$\sum_n |\hat{f}(n)|^2 = 2 \sum_{n \geq 1} \frac{1}{n^2}$$

이것이 결과를 함의합니다.

**§14.7 응용: Arrow의 불가능성 정리**

이진 푸리에 해석의 응용으로서, 이제 [Arrow의 정리](#)의 한 형태를 증명하겠습니다.

3명의 후보  $A, B, C$  중에서 투표하는  $n$ 명의 유권자를 고려합시다. 각 유권자는 다음과 같이 튜플  $v_i = (x_i, y_i, z_i) \in \{\pm 1\}^3$ 을 지정합니다:

- 사람  $i$ 가  $A$ 를  $B$ 보다 앞에 순위 매기면  $x_i = 1$ 이고, 그렇지 않으면  $x_i = -1$ 입니다.
- 사람  $i$ 가  $B$ 를  $C$ 보다 앞에 순위 매기면  $y_i = 1$ 이고, 그렇지 않으면  $y_i = -1$ 입니다.
- 사람  $i$ 가  $C$ 를  $A$ 보다 앞에 순위 매기면  $z_i = 1$ 이고, 그렇지 않으면  $z_i = -1$ 입니다.

암묵적으로 우리는  $v_i$ 에 대해  $3! = 6$ 가지 가능성만을 고려합니다: 사람들의 투표가 일관성이 있다고(즉, 선호가 추이적이라고) 가정함으로써  $x_i = y_i = z_i$  형태의 "역설적인" 투표를 금지합니다.

간결함을 위해  $x_\bullet = (x_1, \dots, x_n)$ 이라 하고,  $y_\bullet$ 와  $z_\bullet$ 도 비슷하게 정의합시다. 그러면 다음과 같은 투표 메커니즘을 고려할 수 있습니다

$$\begin{aligned} f: \{\pm 1\}^n &\rightarrow \{\pm 1\} \\ g: \{\pm 1\}^n &\rightarrow \{\pm 1\} \\ h: \{\pm 1\}^n &\rightarrow \{\pm 1\} \end{aligned}$$

다음을 만족시키도록

- $f(x_\bullet)$ 는  $A$ 와  $B$  사이의 전체 선호이고,
- $g(y_\bullet)$ 는  $B$ 와  $C$  사이의 전체 선호이며,
- $h(z_\bullet)$ 는  $C$ 와  $A$  사이의 전체 선호입니다.

전체 선호  $(f(x_\bullet), g(y_\bullet), h(z_\bullet))$  자체가 역설적인 상황은 피하고자 합니다.

$\mathbb{E}f$ 가 모든  $2^n$ 개의 입력에 걸친  $f$ 의 평균값을 나타낸다고 합시다.  $\mathbb{E}g$ 와  $\mathbb{E}h$ 도 비슷하게 정의합니다. 우리는  $\mathbb{E}f = \mathbb{E}g = \mathbb{E}h = 0$ 이라는 가정을 추가할 것인데, 이는 대칭성을 제공합니다(그리고 예컨대  $f, g, h$ 가 투표자의 입력을 무시하는 상수 함수일 가능성을 배제합니다). 이를 바탕으로 다음 결과를 증명하겠습니다:

#### 정리 14.7.1 (애로 불가능성 정리)

$(f, g, h)$ 가 항상 역설적인 결과를 피하며,  $\mathbb{E}f = \mathbb{E}g = \mathbb{E}h = 0$ 이라고 가정합시다. 그러면  $(f, g, h)$ 는 독재이거나 반독재입니다: 다음을 만족시키는 "독재자"  $k$ 가 존재합니다

$$f(x_\bullet) = \pm x_k, \quad g(y_\bullet) = \pm y_k, \quad h(z_\bullet) = \pm z_k$$

여기서 세 부호가 모두 일치합니다.

보통의 애로 정리와 달리, 우리는  $f(+1, \dots, +1) = +1$ 을 가정하지 않습니다 (따라서 반독재의 가능성이 있습니다).

증명. 투표자들이 각각  $3! = 6$ 가지 가능한 일관된 투표 중 하나를 무작위로 선택한다고 가정합시다. **문제 14B**에서 임의의 함수  $f, g, h$ 에 대해 역설적인 결과의 정확한 확률이 다음과 같이 정확히 주어짐이 보여집니다

$$\frac{1}{4} + \frac{1}{4} \sum_{S \subseteq \{1, \dots, n\}} \left(-\frac{1}{3}\right)^{|S|} \left(\hat{f}(S)\hat{g}(S) + \hat{g}(S)\hat{h}(S) + \hat{h}(S)\hat{f}(S)\right).$$

이 확률(역설적인 결과의 확률)이 0과 같다고 가정합시다. 그러면 다음을 유도합니다

$$1 = \sum_{S \subseteq \{1, \dots, n\}} -\left(-\frac{1}{3}\right)^{|S|} \left(\hat{f}(S)\hat{g}(S) + \hat{g}(S)\hat{h}(S) + \hat{h}(S)\hat{f}(S)\right).$$

하지만 이제 우리는 단순히 약한 부등식을 사용할 수 있습니다.  $\hat{f}(\emptyset) = \mathbb{E}f = 0$ 이고  $\hat{g}$ 와  $\hat{h}$ 에 대해서도 마찬가지로,  $|S| \geq 1$ 인 경우로 주의를 제한합니다. 그런 다음 (모든 실수에

대해 성립하는) 유명한 부등식  $|ab+bc+ca| \leq a^2+b^2+c^2$ 를 결합하여 다음을 이끌어냅니다

$$\begin{aligned}
 1 &= \sum_{S \subseteq \{1, \dots, n\}} -\left(-\frac{1}{3}\right)^{|S|} \left(\hat{f}(S)\hat{g}(S) + \hat{g}(S)\hat{h}(S) + \hat{h}(S)\hat{f}(S)\right) \\
 &\leq \sum_{S \subseteq \{1, \dots, n\}} \left(\frac{1}{3}\right)^{|S|} \left(\hat{f}(S)^2 + \hat{g}(S)^2 + \hat{h}(S)^2\right) \\
 &\leq \sum_{S \subseteq \{1, \dots, n\}} \left(\frac{1}{3}\right)^1 \left(\hat{f}(S)^2 + \hat{g}(S)^2 + \hat{h}(S)^2\right) \\
 &= \frac{1}{3}(1 + 1 + 1) = 1.
 \end{aligned}$$

마지막 단계는 파세발 정리에 의합니다. 따라서 모든 부등식은 등호로 성립해야 하며, 특히  $\hat{f}, \hat{g}, \hat{h}$ 는 단일 원소 집합에서만 지지되어야 합니다. 즉, 입력에 대해 선형입니다.  $f, g, h$ 가  $\pm 1$  값을 취하므로,  $f, g, h$  각각은 그 자체로 독재자 함수이거나 반독재자 함수입니다.  $(f, g, h)$ 가 항상 일관되므로, 이는 최종 결과를 함의합니다.  $\square$

## §14.8 생각해 볼 만한 조금 더 어려운 문제

문제 14A (미적분학 애호가를 위해). 다음을 증명하십시오

$$\sum_{n \geq 1} \frac{1}{n^4} = \frac{\pi^4}{90}.$$



문제 14B.  $f, g, h: \{\pm 1\}^n \rightarrow \{\pm 1\}$ 을 임의의 세 함수라 합시다. 각  $i$ 에 대해, 모두 같지는 않다는 제약 조건 하에  $(x_i, y_i, z_i) \in \{\pm 1\}^3$ 을 무작위로 선택합니다(따라서  $2^3 - 2 = 6$ 가지 가능성 중에서 선택합니다). 다음의 확률이

$$f(x_1, \dots, x_n) = g(y_1, \dots, y_n) = h(z_1, \dots, z_n)$$

다음 공식으로 주어짐을 증명하십시오

$$\frac{1}{4} + \frac{1}{4} \sum_{S \subseteq \{1, \dots, n\}} \left(-\frac{1}{3}\right)^{|S|} \left(\hat{f}(S)\hat{g}(S) + \hat{g}(S)\hat{h}(S) + \hat{h}(S)\hat{f}(S)\right)$$

# 15 쌍대, 수반, 그리고 전치

이 장은 행렬의 전치와 켈레 전치에 대한 기저 없는 해석을 다룹니다.  
포스터 따름정리: 실수 계수를 갖는 대칭행렬은 대각화 가능하며 실수 고유값을 가짐을 보일 것입니다.

## §15.1 사상의 쌍대

이 절의 대표적인 예: 아래의 예제입니다.

이제 행렬의 전치로 발전하게 될 개념을 정의해 보겠습니다.

**정의 15.1.1.**  $V$ 와  $W$ 를 벡터 공간이라 합시다.  $T: V \rightarrow W$ 가 선형 사상이라고 합시다. 그러면 실제로 다음과 같은 사상을 얻습니다

$$\begin{aligned} T^\vee: W^\vee &\rightarrow V^\vee \\ f &\mapsto f \circ T. \end{aligned}$$

이 사상을 **쌍대 사상**이라고 부릅니다.

### 예제 15.1.2 (쌍대 사상의 예)

$\mathbb{R}$  위에서 작업합니다. 기저  $e_1, e_2, e_3$ 를 갖는  $V$ 와 기저  $f_1, f_2$ 를 갖는  $W$ 를 생각해 봅시다. 다음과 같다고 합시다

$$\begin{aligned} T(e_1) &= f_1 + 2f_2 \\ T(e_2) &= 3f_1 + 4f_2 \\ T(e_3) &= 5f_1 + 6f_2. \end{aligned}$$

이제 쌍대 기저  $e_1^\vee, e_2^\vee, e_3^\vee$ 를 갖는  $V^\vee$ 와 쌍대 기저  $f_1^\vee, f_2^\vee$ 를 갖는  $W^\vee$ 를 생각해 봅시다.  $T^\vee(f_1^\vee) = f_1^\vee \circ T$ 를 계산해 봅시다. 이는 다음과 같이 주어집니다

$$\begin{aligned} f_1^\vee(T(ae_1 + be_2 + ce_3)) &= f_1^\vee((a + 3b + 5c)f_1 + (2a + 4b + 6c)f_2) \\ &= a + 3b + 5c. \end{aligned}$$

따라서 다음과 같이 쓸 수 있습니다

$$T^\vee(f_1^\vee) = e_1^\vee + 3e_2^\vee + 5e_3^\vee$$

마찬가지로,

$$T^\vee(f_2^\vee) = 2e_1^\vee + 4e_2^\vee + 6e_3^\vee.$$

이는  $T^\vee$ 를 완전히 결정합니다.

$T$ 와  $T^\vee$ 의 행렬을 우리의 기저에 대해 쓰면, 이제 다음을 알 수 있습니다.

$$T = \begin{bmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{bmatrix} \quad \text{그리고} \quad T^\vee = \begin{bmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{bmatrix}.$$

따라서 우리가 선택한 기저에서, 그 행렬들이 **전치**, 즉 대각선을 기준으로 서로의 거울상임을 알 수 있습니다.

물론 이는 일반적으로도 성립해야 합니다.

### 정리 15.1.3 ( $T^\vee$ 의 전치 해석)

$V$ 와  $W$ 를 유한 차원  $k$ -벡터 공간이라 하고,  $e_1, \dots, e_n$ 을  $V$ 의 임의의 기저,  $f_1, \dots, f_m$ 을  $W$ 의 임의의 기저라고 합시다. 그러면 임의의  $T: V \rightarrow W$ 에 대해, 다음 두 행렬은 서로 전치입니다:

- 기저  $(e_i), (f_j)$ 로 표현된  $T: V \rightarrow W$ 의 행렬입니다.
- 기저  $(f_j^\vee), (e_i^\vee)$ 로 표현된  $T^\vee: W^\vee \rightarrow V^\vee$ 의 행렬입니다.

증명. 행렬  $T$ 의  $(i, j)$ 번째 성분은  $T(e_j)$ 에서  $f_i$ 의 계수에 대응하며, 이는 다시  $f_i^\vee \circ T$ 에서  $e_j^\vee$ 의 계수에 대응합니다.  $\square$

이것의 좋은 점은  $T^\vee$ 의 정의가 기저와 무관하다는 것입니다. 즉, 임의의 선형 사상  $T$ 에서 시작하여 원하는 어떤 기저든 선택하더라도,  $T$ 와  $T^\vee$ 는 여전히 서로 전치가 된다는 뜻입니다.

## §15.2 (선택) 자연스러운 동형사상 $V \cong V^\vee$ 가 없을 때 무엇이 잘못될 수 있는지에 대한 교훈적인 이야기

이 절 이후로는  $V$ 와  $W$ 가 실제로 내적 공간이라고 가정하겠습니다. 이 선택적인 주의 사항은 그 가정이 없을 때 무엇이 잘못되는지 설명하기 위한 것입니다. 하지만 이 절은 상당히 헛갈리고 갈피를 잡기 어려우므로, 이 장의 나머지 부분을 마치고 끝부분의 문제 몇 개(예를 들어 **문제 15C<sup>†</sup>**)를 풀어본 후에 읽는 것도 좋습니다.

예를 들어 **정리 15.1.3**만 사용해도 다음을 증명할 수 있는데, 이는 전형적인 고등학교 선형대수 수업에서 가장 중요한 정리 중 하나입니다.

### 정리 15.2.1 (행 계수 = 열 계수)

어떤 체  $k$  위의  $m \times n$  행렬  $M$ 이 주어져 있습니다.  $M$ 의 열 계수는  $k^{\oplus m}$ 에서  $M$ 의  $n$ 개 열벡터가 생성하는 부분공간의 차원입니다.  $M$ 의 행 계수는  $k^{\oplus n}$ 에서  $M$ 의  $m$ 개 행벡터가 생성하는 부분공간의 차원입니다. 행 계수와 열 계수가 같음을 증명하십시오.

증명. **문제 15B**와 **문제 15C<sup>†</sup>**로 남겨둡니다. 한 가지 접근 방법은 **정리 9.7.6**와 **정리 15.1.3**를 결합하는 것입니다.  $\square$

하지만  $e_i \mapsto e_i^\vee$ 로 주어지는 비표준적 동형사상  $V \rightarrow V^\vee$ 를 지나치게 활용하려고 하면 무엇이 잘못될 수 있는지 살펴봅시다. 다음 "정리"를 생각해 봅시다.

**거짓 정리.** 어떤 체  $k$  위의  $m \times n$  행렬  $M$ 이 주어져 있습니다. 그러면  $M^\top M$ 과  $M$ 은 같은 계수를 갖습니다.

이제 이 결과에 대한 가짜 증명을 제시하겠습니다.

거짓 정리에 대한 잘못된 증명.  $V = k^{\oplus n}$ ,  $W = k^{\oplus m}$ 이라 하고,  $T: V \rightarrow W$ 를  $M$ 으로 부호화된 선형 사상이라 합시다. **정리 15.1.3**에 의해,  $T^\vee: W^\vee \rightarrow V^\vee$ 는  $M^\top$ 으로 부호화됩니다.

**정리 9.7.6**에 의해, ( $V$ 에 대한) 기저  $e_i$ 와 ( $W$ 에 대한) 기저  $f_j$ 로서 서로 다른 기저가 존재하여 다음을 만족합니다.

$$\begin{aligned} T(e_1) &= f_1, \dots, T(e_k) = f_k \\ T(e_{k+1}) &= \dots = T(e_n) = 0 \end{aligned}$$

여기서  $k = \text{rank } T$ 입니다. (계수와 기저체 모두에 문자  $k$ 를 사용해서 죄송합니다.) 이 새로운 기저는 어떤 행렬 부호화에도 사용하지 않고, 오직 계수를 계산하는 데에만 사용하겠습니다.

그러면  $T^\vee: W^\vee \rightarrow V^\vee$ 의 정의로부터 다음을 알 수 있습니다.

$$\begin{aligned} T^\vee(f_1^\vee) &= e_1^\vee, \dots, T^\vee(f_k^\vee) = e_k^\vee \\ T^\vee(f_{k+1}^\vee) &= \dots = T^\vee(f_m^\vee) = 0. \end{aligned}$$

이제 이것을 우리의 (비표준적인) 동형사상  $W \rightarrow W^\vee$ 와 결합하면,  $M^\top M$ 이 합성된 사상  $V \rightarrow V^\vee$ 에 대한 행렬이 됨을 다음과 같이 얻을 수 있습니다.

$$\begin{aligned} e_1 &\mapsto f_1 \mapsto f_1^\vee \mapsto e_1^\vee \\ e_2 &\mapsto f_2 \mapsto f_2^\vee \mapsto e_2^\vee \\ &\vdots \\ e_k &\mapsto f_k \mapsto f_k^\vee \mapsto e_k^\vee \\ e_{k+1} &\mapsto 0 \mapsto 0 \mapsto 0 \\ e_{k+2} &\mapsto 0 \mapsto 0 \mapsto 0 \\ &\vdots \\ e_n &\mapsto 0 \mapsto 0 \mapsto 0. \end{aligned}$$

이 합성된 사상 역시 계수  $k$ 를 가짐이 명백한데,  $e_1$ 부터  $e_k$ 까지의 출력값은 선형독립이고  $e_{k+1}$ 부터  $e_n$ 까지의 출력값은 모두 0이기 때문입니다. 따라서 원하는 대로  $M^\top M$  역시 계수  $k$ 를 갖습니다.  $\square$

괜찮아 보입니까? 하지만 **문제 15H†**에서 보게 되겠지만, 이 정리는  $k = \mathbb{R}$ 일 때는 실제로 참입니다. 하지만  $k = \mathbb{C}$ 일 때는 다음 연습문제가 보여주듯이 거짓입니다.

**연습문제 15.2.2.**  $M^\top M$ 이 영행렬이 되는, 복소수 성분을 갖는 영이 아닌  $2 \times 2$  행렬  $M$ 의 예를 들어 거짓 정리에 대한 반례를 찾으십시오.

그렇다면 이 가짜 증명의 오류는 어디에 있을까요? 위에서 주어진 사상

$$e_i \mapsto f_i \mapsto f_i^\vee \mapsto e_i^\vee$$

은  $T^\vee \circ T$ (이는 애초에 정의조차 되지 않습니다)가 아니라, 오히려  $T^\vee \circ \iota \circ T$ 이며, 여기서  $\iota: W \rightarrow W^\vee$ 는 우리가 아무것도 알지 못하는 "임의의" 동형사상입니다. 따라서 행렬로 부호화하면, 우리가 실제로 얻게 되는 행렬은  $M^\top N M$ 이며, 여기서  $N$ 은 우리가 전혀 통제할 수 없는 임의의 가역행렬입니다.

$k = \mathbb{R}$ 인 경우에는 다음과 같이 하면 이 증명을 고칠 수 있습니다.

- $\iota$ 를 다음 절에서 정의될 사상  $w \mapsto \langle -, w \rangle$ 로 선택하여,  $N$ 이 항등행렬로 부호화되도록 합니다. 그리고
- 추가로 **정리 9.7.6**에서  $f_i$ 가 정규직교이도록 요구하여(이는 가능합니다)  $\iota(f_i) = f_i^\vee$ 가 되도록 합니다.

하지만 이는 제 생각에는 상당히 지저분한 증명인데, 이 장이 끝날 무렵에는 **문제 15H†**에 대해 기저에 의존하지 않는 증명을 쓸 수 있는 도구를 갖추게 될 것이기 때문입니다.

### §15.3 쌍대 공간과의 동일시

하지만 이 장의 나머지 부분에서는 이제 내적을 논의에 끌어들이겠습니다.

앞서 저는 자연스러운 동형사상  $V \cong V^\vee$ 가 없다고 불평했습니다. 하지만 사실 내적 형식이 주어지면 실제로 이러한 동일시를 만들 수 있습니다: 즉 모든 선형 사상  $\xi: V \rightarrow k$ 를 벡터  $v \in V$ 와 자연스럽게 대응시킬 수 있습니다.

이를 어떻게 할 수 있는지 보기 위해, 우선  $V = \mathbb{R}^3$ 이고 정규직교 기저  $e_1, e_2, e_3$ 을 가진다고 합시다. 내적을 사용하여  $V \rightarrow \mathbb{R}$ 인 사상을 어떻게 나타낼 수 있을까요? 예를 들어  $\xi(e_1) = 3, \xi(e_2) = 4, \xi(e_3) = 5$ 로  $\xi \in V^\vee$ 를 취합시다. 사실 저는 다음과 같이 주장합니다:

$$\xi(v) = \langle v, 3e_1 + 4e_2 + 5e_3 \rangle$$

모든  $v$ 에 대하여.

**질문 15.3.1.** 이를 확인해 보십시오.

그리고 이는 실수의 경우 아름답게 작동합니다.

#### 정리 15.3.2 (실수 내적 형식에 대한 $V \cong V^\vee$ )

$V$ 를 유한 차원 실 내적 공간이라 하고  $V^\vee$ 를 그 쌍대 공간이라 하겠습니다. 그러면 사상  $V \rightarrow V^\vee$ 는 다음과 같이

$$v \mapsto \langle -, v \rangle \in V^\vee$$

실수 벡터 공간의 동형사상입니다.

증명. 이 사상이 단사이고 전사임을 보이면 충분합니다.

- 단사: 모든 벡터  $v \in V$ 에 대해  $\langle v, v_1 \rangle = \langle v, v_2 \rangle$ 라고 가정합시다. 이는 모든 벡터  $v \in V$ 에 대해  $\langle v, v_1 - v_2 \rangle = 0$ 임을 의미합니다. 이는 오직  $v_1 - v_2 = 0$ 일 때만 일어날 수 있습니다; 예를 들어  $v = v_1 - v_2$ 로 놓고 양의 정부호성을 사용하십시오.
- 전사: 정규직교 기저  $e_1, \dots, e_n$ 을 취하고,  $e_1^\vee, \dots, e_n^\vee$ 를  $V^\vee$  위의 쌍대 기저라 합시다. 그러면  $e_1$ 은  $e_1^\vee$ 로 대응되고, 나머지도 마찬가지입니다.  $\square$

사실 우리는 이미  $\dim V = \dim V^\vee$ 임을 알고 있으므로 위의 것 중 하나만 증명하면 되었습니다. 개인적인 취향으로는, 단사성의 증명이 더 우아하고 전사성의 증명이 더 깨우침을 준다고 생각하여 둘 다 포함시켰습니다. 따라서

**실수 내적 공간  $V$ 에 내적 형식이 주어지면,  $V$ 와  $V^\vee$ 는 표준적으로 동형입니다.**

안타깝게도  $V$ 가 복소수인 경우에는 일이 어긋나 버립니다. 그 결과는 다음과 같습니다:

#### 정리 15.3.3 (복소수 내적 형식에 대한 $V$ 와 $V^\vee$ 의 비교)

$V$ 를 유한 차원 복소 내적 공간이라 하고  $V^\vee$ 를 그 쌍대 공간이라 하겠습니다. 그러면 사상  $V \rightarrow V^\vee$ 는 다음과 같이

$$v \mapsto \langle -, v \rangle \in V^\vee$$

집합의 전단사입니다.

잠깐, 뭐라고요? 위의 증명은 이 사상이 단사이면서 전사임을 보여주는데, 왜 동형사상이 아닐까요? 그 답은 이것이 선형 사상이 아니라는 것입니다: 형식이 반쌍선형이기 때문에

예를 들어 다음과 같이

$$iv \mapsto \langle -, iv \rangle = -i \langle -, v \rangle$$

음의 부호가 도입됩니다! 사실 이는 앞서 정의한 의미에서 반선형 사상입니다.

열정적인 독자라면 대신 동형사상  $v \mapsto \langle v, - \rangle$ 를 정의하여 이를 고치려 할 수도 있습니다. 하지만 이 또한 실패하는데, 우변이  $V^\vee$ 의 원소조차 아니기 때문입니다: 이는 선형이 아니라 "반선형"입니다.

그래서 우리는 막다른 길에 이르렀습니다. 다행히도 앞으로는 "전단사" 결과만 필요하므로, 어쨌든 계속 진행할 수 있습니다. (이를 고치고 싶다면, **문제 15D**에서 그 방법을 제시합니다.)

## §15.4 딸림사상 (켈레 전치)

위에서 본 뒤바뀐 결과로, 켈레 전치가 실제로 내적 공간에 있어 더 나은 개념임을 보게 될 것입니다: 왜냐하면 이는 쌍대 공간을 전혀 언급하지 않고 오직 내적만을 사용하여 정의할 수 있기 때문입니다.

**정의 15.4.1.**  $V$ 와  $W$ 를 유한 차원 내적 공간이라 하고,  $T: V \rightarrow W$ 라 하겠습니다.  $T$ 의 **딸림사상**(또는 **켈레 전치**), 즉  $T^\dagger: W \rightarrow V$ 는 다음과 같이 정의됩니다: 모든 벡터  $w \in W$ 에 대해,  $T^\dagger(w) \in V$ 를 다음을 만족하는 유일한 벡터로 둡니다.

$$\langle v, T^\dagger(w) \rangle_V = \langle T(v), w \rangle_W$$

모든  $v \in V$ 에 대해.

이 정의에 대한 몇 가지 즉각적인 소견:

- 우리의  $T^\dagger$ 는 잘 정의됩니다. 왜냐하면  $v \mapsto \langle T(v), w \rangle_W$ 는  $V^\vee$  안의 어떤 함수이므로, 앞서의 전단사에 의해 어떤  $v \in V$ 에 대해 유일하게  $\langle -, v \rangle$  꼴이어야 하기 때문입니다.
- 이 사상  $T^\dagger$ 는 실제로 선형 사상입니다 (왜 그럴까요?).
- 이 정의의 장점은 어떤 기저에도, 심지어  $V^\vee$ 에도 의존하지 않는다는 것이며, 그래서 이것이 내적 공간에 대한 "올바른" 정의입니다.

### 예제 15.4.2 (수반 사상의 예)

$\mathbb{C}$  위에서 작업하여 켈레가 더 잘 보이도록 하겠습니다. 정규직교 기저  $e_1, e_2, e_3$ 을 갖는  $V$ 와 정규직교 기저  $f_1, f_2$ 를 갖는  $W$ 를 생각해봅시다. 다음과 같이 둡니다

$$\begin{aligned} T(e_1) &= if_1 + 2f_2 \\ T(e_2) &= 3f_1 + 4f_2 \\ T(e_3) &= 5f_1 + 6if_2. \end{aligned}$$

$T^\dagger(f_1)$ 을 계산해봅시다. 이는 다음을 만족하는 유일한 벡터  $x \in V$ 입니다

$$\langle v, x \rangle_V = \langle T(v), f_1 \rangle_W$$

임의의  $v \in V$ 에 대해.  $v = ae_1 + be_2 + ce_3$ 로 전개하면 위 등식은 다음이 됩니다

$$\begin{aligned} \langle ae_1 + be_2 + ce_3, x \rangle_V &= \langle T(ae_1 + be_2 + ce_3), f_1 \rangle_W \\ &= ia + 3b + 5c. \end{aligned}$$

하지만  $x$ 가 두 번째 인자에 있으므로, 이는 사실 우리가 다음을 취하고자 함을 의미합니다

$$T^\dagger(f_1) = -ie_1 + 3e_2 + 5e_3$$

세스퀴선형성이  $i$ 를 켈레화하도록 하기 위해서입니다.

이 패턴은 계속되지만, 진행하려면 기저가 정규직교여야 함을 독자에게 상기시켜 드립니다.

#### 정리 15.4.3 (수반 사상은 켈레 전치이다)

유한 차원 내적 공간  $V$ 의 정규직교 기저를 하나 고정합니다.  $T: V \rightarrow V$ 를 선형 사상이라 합니다. 이 기저에서  $T$ 를 행렬로 쓰면, (같은 기저에서의) 행렬  $T^\dagger$ 는  $T$ 의 행렬의 켈레 전치입니다. 즉,  $T^\dagger$ 의  $(i, j)$ 번째 성분은  $T$ 의  $(j, i)$ 번째 성분의 복소켈레입니다.

증명. 한 줄 버전:  $v$ 와  $w$ 를 기저 원소로 두면, 이는 바로 도출됩니다.

전체 증명: 다음과 같이 씁시다

$$T = \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix}$$

이 기저  $e_1, \dots, e_n$ 에서. 그러면  $w = e_i$ 이고  $v = e_j$ 로 두면 다음을 알 수 있습니다

$$\langle e_i, T^\dagger(e_j) \rangle = \langle T(e_i), e_j \rangle = a_{ji} \implies \langle T^\dagger(e_j), e_i \rangle = \overline{a_{ji}}$$

임의의  $i$ 에 대해, 이는 결과를 도출하기에 충분합니다. □

## §15.5 정규 사상의 고삐

이제 예고한 정리에 도달합니다.  $T: V \rightarrow V$ 인 상황으로 제한합니다. 아시다시피, 고유벡터로 이루어진 기저를 고를 수 있고 그 기저가 정규직교이기도 하다면 세상은 매우 아름다운 곳이 될 것입니다. 물론 이는 너무 많은 것을 바라는 것입니다. 정규직교 조건이 없어도, 조르당 표준형은 여전히 대각선 밖에 1을 가질 수 있음을 보았습니다.

하지만 우리의 과욕에 찬 꿈이 정확히 언제 참인지에 대한 완전한 특징 규명이 존재한다는 것이 밝혀집니다.

**정의 15.5.1.** 선형 사상  $T$  (유한 차원 내적 공간에서 자기 자신으로 가는)가  $TT^\dagger = T^\dagger T$ 를 만족하면 **정규**라고 합니다.

복소수  $T$ 가  $T = T^\dagger$ 를 만족하면 **자기수반**이거나 **에르미트**라고 합니다. 즉, 임의의 정규직교 기저에서 행렬로 나타냈을 때  $T$ 가 자기 자신의 켈레 전치라는 것입니다. 실수  $T$ 에 대해서는 "자기수반", "에르미트" 또는 **대칭**이라고 합니다.

#### 정리 15.5.2 (정규 $\iff$ 정규직교 기저로 대각화 가능)

$V$ 를 유한 차원 복소 내적 공간이라 합니다. 선형 사상  $T: V \rightarrow V$ 가 정규인 것은 고유벡터로 이루어진 정규직교 기저를 고를 수 있는 것과 동치입니다.

**연습문제 15.5.3.** 그러한 정규직교 기저가 존재하면  $T: V \rightarrow V$ 가 정규임을, 그 기저에서  $T$ 를 대각행렬로 씌으로써 보이십시오.

증명. 이는 길기 때문에 첫 독서에서는 생략해도 좋습니다.  $T$ 가 고유벡터로 이루어진 정규 직교 기저를 가지면 이 결과는 즉각적입니다.

이제  $T$ 가 정규(normal)라고 가정합니다. 먼저  $T$ 가 대각화 가능함을 증명합니다; 이것이 어려운 부분입니다.

**주장 15.5.4.**  $T$ 가 정규이면,  $r \geq 1$ 에 대해  $\ker T = \ker T^r = \ker T^\dagger$ 입니다. (여기서  $T^r$ 은  $T$ 를  $r$ 번 적용한 것입니다.)

주장의 증명.  $S = T^\dagger \circ T$ 라 하면, 이는 자기수반입니다. 먼저  $S$ 가 에르미트(Hermitian)이고  $\ker S = \ker T$ 임을 주목합니다. 에르미트임을 보이려면,  $\langle Sv, w \rangle = \langle Tv, Tw \rangle = \langle v, Sw \rangle$  임에 주목하십시오.  $v = w$ 로 두면 또한  $\ker S \subseteq \ker T$ 가 성립함을 알 수 있으며 (그리고 자명하게  $\ker T \subseteq \ker S$ 이므로 결과적으로 등식이 성립합니다).

먼저,  $\langle S^r(v), S^{r-2}(v) \rangle = \langle S^{r-1}(v), S^{r-1}(v) \rangle$ 이므로, 귀납법에 의해  $r \geq 1$ 에 대해  $\ker S = \ker S^r$ 임을 보일 수 있습니다. 이제  $T$ 가 정규이므로  $S^r = (T^\dagger)^r \circ T^r$ 이 성립하며, 따라서 다음 포함 관계를 얻습니다

$$\ker T \subseteq \ker T^r \subseteq \ker S^r = \ker S = \ker T$$

여기서 마지막 등식은 첫 번째 주장으로부터 따라옵니다. 따라서 실제로  $\ker T = \ker T^r$ 입니다.

마지막으로,  $\ker T^\dagger$ 와의 등식을 보이기 위해 우리는

$$\begin{aligned} \langle Tv, Tv \rangle &= \langle v, T^\dagger Tv \rangle \\ &= \langle v, TT^\dagger v \rangle \\ &= \langle T^\dagger v, T^\dagger v \rangle. \end{aligned}$$

■

이제 주어진  $T$ 와 임의의  $\lambda$ 를 고려합니다.

**질문 15.5.5.**  $(T - \lambda \text{id})^\dagger = T^\dagger - \bar{\lambda} \text{id}$ 임을 보이십시오. 따라서  $T$ 가 정규이면  $T - \lambda \text{id}$  또한 정규입니다.

특히,  $T$ 의 임의의 고윳값  $\lambda$ 에 대해,  $\ker(T - \lambda \text{id}) = \ker(T - \lambda \text{id})^r$ 임을 알 수 있습니다. 이는  $T$ 의 모든 조르당 블록(Jordan block)의 크기가 1임을, 즉  $T$ 가 실제로 대각화 가능함을 의미합니다. 마지막으로,  $T$ 와  $T^\dagger$ 의 고유벡터가 서로 일치하며, 고윳값은 서로 켤레 복소수임을 결론짓습니다.

그럼 이제  $T$ 를 대각화합시다. 서로 다른 고윳값을 갖는  $T$ 의 고유벡터  $v$ 와  $w$ 가 있다면 이들이 서로 직교함을 보이기만 하면 됩니다. (여러 번 나타나는 고윳값에 대해서는 그람-슈미트(Gram-Schmidt)를 사용할 수 있습니다.) 이를 보이기 위해,  $T(v) = \lambda v$ 이고  $T(w) = \mu w$ 라고 가정합시다 (따라서  $T^\dagger(w) = \bar{\mu} w$ 입니다). 그러면

$$\lambda \langle v, w \rangle = \langle \lambda v, w \rangle = \langle Tv, w \rangle = \langle v, T^\dagger(w) \rangle = \langle v, \bar{\mu} w \rangle = \bar{\mu} \langle v, w \rangle.$$

$\lambda \neq \bar{\mu}$ 이므로,  $\langle v, w \rangle = 0$ 임을 결론짓습니다. □

이는 다음을 쓸 수 있을 뿐만 아니라

$$T = \begin{bmatrix} \lambda_1 & \dots & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{bmatrix}$$

나아가 이 행렬과 연관된 기저가 마침 정규직교 벡터들이라는 것도 의미합니다.  
따름정리로서:

**정리 15.5.6 (에르미트 행렬은 실수 고윳값을 갖습니다)**

에르미트 행렬  $T$ 는 대각화 가능하며, 그 모든 고윳값은 실수입니다.

증명. 자명하게 에르미트  $\implies$  정규이므로, 고유벡터의 정규직교 기저로 표현합니다. 고윳값이 실수임을 보이려면,  $T = T^\dagger$ 가 모든  $i$ 에 대해  $\lambda_i = \overline{\lambda_i}$ 를 의미함에 주목하십시오.  $\square$

## §15.6 생각해 볼 만한 조금 더 어려운 문제



**문제 15A\*** (이중 쌍대).  $V$ 를 유한 차원 벡터 공간이라 합시다. 다음을 증명하십시오

$$\begin{aligned} V &\rightarrow (V^\vee)^\vee \\ v &\mapsto (\xi \mapsto \xi(v)) \end{aligned}$$

동형사상을 이룹니다. (이것이 중요한 이유는 이 동형사상이 정준적(*canonical*)이며, 특히 기저의 선택에 의존하지 않기 때문입니다. 그래서 이 결과는 더욱 인상적입니다.)

**문제 15B** (선형대수학의 기본정리).  $T: V \rightarrow W$ 를 유한 차원  $k$ -벡터 공간 사이의 사상이라 합시다. 다음을 증명하십시오

$$\dim \operatorname{im} T = \dim \operatorname{im} T^\vee = \dim V - \dim \ker T = \dim W - \dim \ker T^\vee.$$

**문제 15C<sup>†</sup>** (행 계수는 열 계수와 같다). 어떤 체  $k$  위의  $m \times n$  행렬  $M$ 이 주어져 있습니다.  $M$ 의 열 계수는  $k^{\oplus m}$ 에서  $n$ 개의 열벡터가 생성하는 부분공간의 차원입니다.  $M$ 의 행 계수는  $k^{\oplus n}$ 에서  $m$ 개의 행벡터가 생성하는 부분공간의 차원입니다. 행 계수와 열 계수가 같음을 증명하십시오.

**문제 15D** (복소 켈레 공간).  $V = (V, +, \cdot)$ 을 복소 벡터 공간이라 합시다. 곱셈만을 바꾸어 **복소 켈레 벡터 공간**을 정의하고, 이를  $\overline{V} = (V, +, *)$ 로 표기합니다:

$$c * v = \overline{c} \cdot v.$$

$V$  위의 임의의 반쌍선형 형식에 대해,  $V$ 가 유한 차원이면 다음이

$$\begin{aligned} \overline{V} &\rightarrow V^\vee \\ v &\mapsto \langle -, v \rangle \end{aligned}$$

복소 벡터 공간의 동형사상임을 보이십시오.

**문제 15E** ( $T^\dagger$ 와  $T^\vee$ ).  $V$ 와  $W$ 를 실수 내적 공간이라 하고  $T: V \rightarrow W$ 를 선형 사상이라 합시다. 다음 도식이 가환함을 보이십시오:

$$\begin{array}{ccc} W & \xrightarrow{T^\dagger} & V \\ \cong \downarrow & & \downarrow \cong \\ W^\vee & \xrightarrow{T^\vee} & V^\vee \end{array}$$

여기서 동형사상은  $v \mapsto \langle -, v \rangle$ 입니다. 따라서 실수 내적 공간에서는,  $T^\dagger$ 는 (정리 15.3.2에 의해) 쌍대가 제거된  $T^\vee$ 에 지나지 않습니다.

**문제 15F** (정규성에 대한 다항식 판정법).  $V$ 를 유한 차원 복소 내적 공간이라 하고  $T: V \rightarrow V$ 를 선형 사상이라 하십시오.  $T$ 가 정규 사상일 필요충분조건이 다음을 만족하는 다항식<sup>1</sup>  $p \in \mathbb{C}[t]$ 가 존재하는 것임을 보이십시오:

$$T^\dagger = p(T)$$



**문제 15G** (행렬의 크로네커 곱). **크로네커 곱**에 대한 다음 두 정의(전자는 수학자의 정의, 후자는 컴퓨터 과학자의 정의) 사이의 동치 관계를 찾으십시오:

- $A: V_1 \rightarrow W_1$ 과  $B: V_2 \rightarrow W_2$ 가  $\mathbb{R}$  위의 유한 차원 벡터 공간들의 선형 사상이라고 합시다. 그러면 단순 텐서에 대해  $v_1 \otimes v_2 \mapsto A(v_1) \otimes B(v_2)$ 로  $A \otimes B: V_1 \otimes V_2 \rightarrow W_1 \otimes W_2$ 를 정의합니다.
- $A$ 가  $m \times n$  행렬이고  $B$ 가  $p \times q$  행렬이라고 합시다. 그러면  $A \otimes B$ 는  $q \times n$  행렬  $X$ 를 받아  $p \times m$  행렬  $BXA^\top$ 를 반환하는 연산자입니다.

**문제 15H<sup>†</sup>**.  $M$ 을 복소수로 이루어진  $m \times n$  행렬이라 합시다.  $M^\dagger M$ 과  $M$ 의 계수가 같음을 보이십시오. (기저를 사용하지 않는 증명을 찾아보십시오.)

<sup>1</sup>여기서  $p(T)$ 는 케일리-해밀턴 정리에서와 같은 합성의 의미로 사용합니다.



V

군에 대하여 더 알아보기

## 제V부: 목차

---

|           |                                    |            |
|-----------|------------------------------------|------------|
| <b>16</b> | <b>군의 작용으로 AIME 문제를 압도적으로 풀어내기</b> | <b>213</b> |
| 16.1      | 군의 작용의 정의 . . . . .                | 213        |
| 16.2      | 안정자군과 궤도 . . . . .                 | 214        |
| 16.3      | 번사이드 보조정리 . . . . .                | 215        |
| 16.4      | 원소의 켈레화 . . . . .                  | 216        |
| 16.5      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .     | 217        |
| <b>17</b> | <b>모든 군을 찾으시오</b>                  | <b>219</b> |
| 17.1      | 실로우 정리 . . . . .                   | 219        |
| 17.2      | (선택) 실로우 정리 증명하기 . . . . .         | 220        |
| 17.3      | (선택) 단순군과 Jordan-Hölder . . . . .  | 222        |
| 17.4      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .     | 224        |
| <b>18</b> | <b>PID 구조 정리</b>                   | <b>225</b> |
| 18.1      | 유한 생성 아벨 군 . . . . .               | 225        |
| 18.2      | 환론의 몇 가지 선행 지식 . . . . .           | 226        |
| 18.3      | 구조 정리 . . . . .                    | 227        |
| 18.4      | 자유 $R$ -가군 사이의 사상으로서의 환원 . . . . . | 228        |
| 18.5      | 준소 형식의 유일성 . . . . .               | 229        |
| 18.6      | 스미스 표준형 . . . . .                  | 231        |
| 18.7      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .     | 234        |

---

# 16 군의 작용으로 AIME 문제를 압도적으로 풀어내기

1996년 AIME의 다음 문제를 생각해봅시다:

(AIME 1996)  $7 \times 7$  체커보드의 칸 중 두 개를 노란색으로 칠하고, 나머지는 초록색으로 칠합니다. 두 색칠 방식이 보드 평면 상의 회전으로 서로 얻어질 수 있다면 동치라고 합니다. 서로 동치가 아닌 색칠 방식은 몇 가지나 가능합니까?

여기서 무슨 일이 일어나고 있습니까?  $X$ 를 보드에 대해 가능한  $\binom{49}{2}$ 가지 색칠 방식들의 집합이라고 합시다. "회전"에 대한 자연스러운 해석은 무엇입니까? 답: 군  $\mathbb{Z}/4\mathbb{Z} = \langle r \mid r^4 = 1 \rangle$ 이 어떤 방식으로든 이 집합  $X$ 에 "작용"하여, 한 상태  $x \in X$ 를 또 다른 상태  $r \cdot x$ 로 보내는데, 이는 그저  $x$ 를  $90^\circ$  회전시킨 것입니다. 직관적으로 말하면, 두 배치가 이 "작용"에 의해 서로로부터 도달될 수 있다면 같다고 말하는 것입니다.

우리는 군의 작용이라는 개념을 이용해 이 모든 것을 엄밀하게 만들 수 있습니다.

## §16.1 군의 작용의 정의

이 절의 대표적인 예: AIME 문제.

**정의 16.1.1.**  $X$ 를 집합,  $G$ 를 군이라고 합시다. **군의 작용**이란 이항 연산  $\cdot: G \times X \rightarrow X$ 으로, 이는  $g \in G$ 가  $x \in X$ 를  $g \cdot x$ 로 보내도록 합니다. 이는 다음 공리를 만족합니다

- 임의의  $g_1, g_2 \in G$  및 모든  $x \in X$ 에 대해  $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ .
- 임의의  $x \in X$ 에 대해  $1_G \cdot x = x$ .

### 예제 16.1.2 (군의 작용의 예시)

$G = (G, \star)$ 를 군이라고 합시다.

- 군  $\mathbb{Z}/4\mathbb{Z}$ 는  $7 \times 7$  보드를 노란색 또는 초록색으로 칠하는 방식들의 집합에 작용할 수 있습니다.
- 군  $\mathbb{Z}/4\mathbb{Z} = \langle r \mid r^4 = 1 \rangle$ 은  $xy$ -평면  $\mathbb{R}^2$ 에 다음과 같이 작용합니다:  $r \cdot (x, y) = (y, -x)$ . 다시 말해, 이는  $90^\circ$  회전입니다.
- 이면군  $D_{2n}$ 은  $n$ 각형의 꼭짓점들을 칠하는 방식들의 집합에 작용합니다.
- 군  $S_n$ 은 치환  $\sigma$ 를 적용함으로써  $X = \{1, 2, \dots, n\}$ 에 작용합니다:  $\sigma \cdot x := \sigma(x)$ .
- 군  $G$ 는 자기 자신(즉  $X = G$ )에 좌측 곱셈으로 작용할 수 있습니다:  $g \cdot g' := g \star g'$ 로 둡니다.

**연습문제 16.1.3.** 군의 작용은  $G$ 에서  $S_X$ 로 가는 군 준동형사상으로도 동등하게 서술될 수 있음을 보이십시오. 여기서  $S_X$ 는  $X$  위의 치환들의 대칭군입니다.

## §16.2 안정자군과 궤도

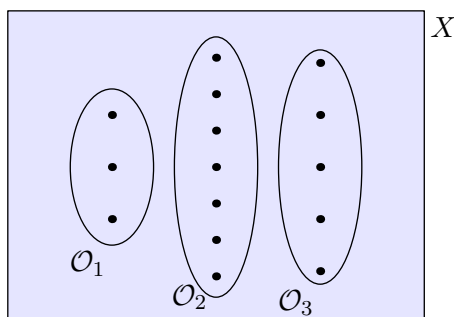
**이 절의 대표적인 예:** 다시 AIME 문제.

$X$  위의 군  $G$ 의 작용이 주어지면, 우리는  $X$  위에 다음과 같이 동치 관계  $\sim$ 을 정의할 수 있습니다: 어떤  $g \in G$ 에 대해  $x = g \cdot y$ 이면  $x \sim y$ 입니다. 예를 들어, AIME 문제에서  $\sim$ 은 "하나가 다른 하나로부터 회전에 의해 얻어질 수 있다"는 것을 의미합니다.

**질문 16.2.1.** 이것이 왜 동치 관계입니까?

그렇다면, AIME 문제는  $\sim$  아래에서의 동치류의 개수를 구하고자 하는 것입니다. 그러니 이 동치류들에 이름을 붙여봅시다: **궤도**. 우리는 보통 궤도를  $\mathcal{O}$ 로 표기합니다.

늘 그렇듯이, 궤도들은  $X$ 를 동치류들로 나눕니다.



아주 밀접하게 관련된 개념이 있는데, 다음과 같습니다:

**정의 16.2.2.** 점  $x \in X$ 의 **안정화군**(stabilizer)은  $\text{Stab}_G(x)$ 로 표기하며,  $x$ 를 고정하는  $g \in G$ 의 집합입니다; 다시 말해

$$\text{Stab}_G(x) := \{g \in G \mid g \cdot x = x\}.$$

### 예제 16.2.3

AIME 문제를 다시 생각해봅시다.  $X$ 는 가능한 상태들의 집합이고 (다시  $G = \mathbb{Z}/4\mathbb{Z}$ 입니다).  $x$ 를 마주 보는 두 모서리가 노란색으로 칠해진 배치라고 합시다. 분명히  $1_G$ 는  $x$ 를 고정하며,  $180^\circ$  회전  $r^2$ 도 마찬가지입니다. 하지만  $r$ 과  $r^3$ 은  $x$ 를 보존하지 않으므로,  $\text{Stab}_G(x) = \{1, r^2\} \cong \mathbb{Z}/2\mathbb{Z}$ 입니다.

**질문 16.2.4.**  $\text{Stab}_G(x)$ 는 왜  $G$ 의 부분군입니까?

안정화군이 군이라는 사실을 깨닫고 나면, 저는 개인적으로 “궤도의 크기에 관한 기본 정리”라고 부르는 결과에 이르게 됩니다.

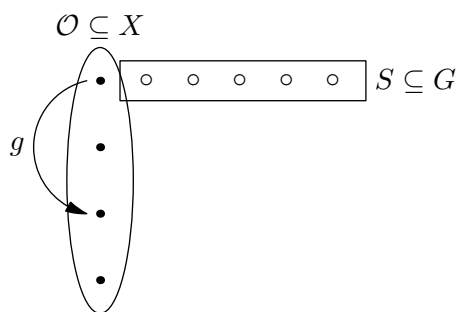
### 정리 16.2.5 (궤도-안정화군 정리)

$\mathcal{O}$ 를 궤도라 하고,  $x \in \mathcal{O}$ 를 하나 택합시다.  $S = \text{Stab}_G(x)$ 를  $G$ 의 부분군이라 합시다.  $\mathcal{O}$ 와 좌잉여류 사이에는 자연스러운 전단사가 존재합니다. 특히,

$$|\mathcal{O}| |S| = |G|.$$

특히, 각  $x \in \mathcal{O}$ 의 안정화 부분군은 크기가 같습니다.

증명. 핵심은 모든 잉여류  $gS$ 가  $\mathcal{O}$ 의 한 원소, 즉  $g \cdot x$ 를 지정한다는 것입니다.  $S$ 가 안정화 군이라는 사실은 어떤 대표원을 택하는지가 무관함을 함의합니다.



$|\mathcal{O}|$ 개의 잉여류가 각각 크기  $|S|$ 로  $G$ 를 분할하므로, 두 번째 결과를 얻습니다.  $\square$

### §16.3 번사이드 보조정리

이제 이 장의 핵심으로, 궤도의 개수를 세는 방법입니다.

#### 정리 16.3.1 (번사이드 보조정리)

$G$ 가 집합  $X$ 에 작용한다고 합시다. 이 작용의 궤도 개수는 다음과 같습니다

$$\frac{1}{|G|} \sum_{g \in G} |\text{FixPt } g|$$

여기서  $\text{FixPt } g$ 는  $g \cdot x = x$ 를 만족하는 점  $x \in X$ 의 집합입니다.

증명은 매우 올림피아드 취향의 풀이를 가지므로 보너스 문제로 미룹니다. 늘 그렇듯이, 이 보조정리는 실제로는 번사이드가 증명한 것이 아니며, 코시가 먼저 도달했기에 때로는 번사이드의 것이 아닌 보조정리라고 불리기도 합니다. 응용 예시:

#### 예제 16.3.2 (AIME 1996)

$7 \times 7$  체커판의 칸 중 두 칸을 노란색으로 칠하고, 나머지는 초록색으로 칠합니다. 두 색칠 방식은 판의 평면 상에서 회전을 적용하여 서로 얻을 수 있으면 동치라고 합니다. 서로 동치가 아닌 색칠 방식은 몇 가지입니까?

$G = \mathbb{Z}/4\mathbb{Z}$ 가 가능한 색칠 방식  $\binom{49}{2}$ 개로 이루어진 집합  $X$ 에 작용함을 알고 있습니다. 이제 각  $g \in \mathbb{Z}/4\mathbb{Z}$ 에 대해  $\text{FixPt } g$ 를 명시적으로 계산할 수 있습니다.

- $g = 1_G$ 이면 모든 색칠이 고정되므로, 그 개수는  $\binom{49}{2} = 1176$ 입니다.
- $g = r^2$ 이면  $g$ 에 의해 고정되는 색칠 방식은 정확히 24가지입니다: 이는 두 칸이 중심을 기준으로 서로 대칭일 때 발생하며, 이는  $180^\circ$  회전 하에서 보존됨을 의미합니다.
- $g = r$  또는  $g = r^3$ 이면, 고정되는 색칠 방식은 존재하지 않습니다.

$|G| = 4$ 이므로, 평균은

$$\frac{1176 + 24 + 0 + 0}{4} = 300.$$

**연습문제 16.3.3** (매스카운츠 챕터 타겟 라운드). 원형 회전판이 크기가 같은 일곱 개의 구역으로 나뉘어 있고, 각 구역은 빨간색 또는 파란색으로 칠해져 있습니다. 두 색칠은 하나를 회전시켜 다른 하나를 얻을 수 있으면 같은 것으로 간주합니다. 회전판을 칠하는 방법은 몇 가지입니까? (답: 20)

“실전적” 응용의 예시를 더 보려면 [Ma13b]를 참고하십시오.

## §16.4 원소의 켤레화

**이 절의 대표적인 예:**  $S_n$ 에서 켤레류는 “순환 유형”입니다.

특히 흔한 작용의 유형으로 이른바 **켤레화**가 있습니다. 우리는 다음과 같이  $G$ 가 자기 자신에 작용하도록 합니다:

$$g: h \mapsto ghg^{-1}.$$

이 정의가 다소 인위적이라고 생각하실 수도 있습니다. 원소  $ghg^{-1}$ 가 대체 무슨 의미가 있단 말입니까? 이 정의가 그리 부자연스럽지 않다는 것을 설득해 보겠습니다.

### 예제 16.4.1 ( $S_n$ 에서의 켤레화)

$G = S_5$ 라 하고,  $\pi \in S_5$ 를 하나 고정합시다. 여기서 질문은 다음과 같습니다:  $\pi\sigma\pi^{-1}$ 는  $\sigma$ 와 관련이 있습니까? 이를 설명하기 위해,  $\sigma \in S_5$ 인 완전히 임의의 치환 예시를 하나 적어 보겠습니다.

$$\begin{array}{ccc} \begin{array}{l} 1 \mapsto 3 \\ 2 \mapsto 1 \\ \text{만약 } \sigma = \begin{array}{l} 3 \mapsto 5 \\ 4 \mapsto 2 \\ 5 \mapsto 4 \end{array} \end{array} & \text{그렇다면} & \begin{array}{l} \pi(1) \mapsto \pi(3) \\ \pi(2) \mapsto \pi(1) \\ \pi\sigma\pi^{-1} = \begin{array}{l} \pi(3) \mapsto \pi(5) \\ \pi(4) \mapsto \pi(2) \\ \pi(5) \mapsto \pi(4) \end{array} \end{array} \end{array}$$

따라서 우리가 고정한  $\pi$ 는  $\sigma$ 의 구조를 사실상 전혀 바꾸지 않습니다: 그것은 단지 1, 2, 3, 4, 5 각 원소를  $\pi(1), \pi(2), \pi(3), \pi(4), \pi(5)$ 로 “이름만 바꿀” 뿐입니다.

하지만 잠깐, 이렇게 말씀하실 수도 있습니다. 그건 켤레화 아래에서 잘 작동하는 아주 특수한 유형의 군일 뿐이지 않느냐고 말입니다. 이것이 왜 더 일반적으로도 의미가 있는 것입니까? 제가 드릴 수 있는 말씀은 이것입니다: 케일리 정리를 기억하십시오! (이는 **문제 1F†**이었습니다.)

어쨌든, 이제 다음과 같이 정의할 수 있습니다:

**정의 16.4.2.** 군  $G$ 의 **켤레류**란 켤레화 작용 아래에서의  $G$ 의 궤도입니다.

예를 들어,  $S_n$ 의 켤레류가 무엇인지 살펴봅시다.

### 예제 16.4.3 ( $S_n$ 의 켤레류는 순환 유형에 대응됩니다)

직관적으로, 위의 논의는  $S_n$ 의 두 원소가 원소들에 어떤 이름이 붙어 있는지와 무관하게 같은 “모양”을 가지면 켤레 관계에 있어야 함을 말해줍니다. 이 “모양”이라는 개념을 엄밀하게 만드는 올바른 방법은 순환 표기법입니다. 예를 들어, 다음과 같은 치환을 생각해 봅시다

$$\sigma_1 = (1\ 3\ 5)(2\ 4)$$

순환 표기법에서 이는  $1 \mapsto 3 \mapsto 5 \mapsto 1$ 이고  $2 \mapsto 4 \mapsto 2$ 임을 의미합니다. 이것은 다음

치환과 켤레 관계에 있습니다

$$\sigma_2 = (1\ 2\ 3)(4\ 5)$$

또는 원소들을 다시 이름 붙이는 다른 어떤 방식이든 마찬가지입니다. 따라서 우리는  $\sigma$ 가 다음과 같은 켤레류를 갖는다고 생각할 수 있습니다.

$$(-\ -\ -)(-\ -).$$

더 일반적으로,  $S_n$ 의 두 원소가 켤레 관계에 있는 것은 순환 분해에서 같은 “모양”을 가질 때이고 오직 그때뿐임을 보일 수 있습니다.

**질문 16.4.4.**  $S_n$ 의 켤레류의 개수가  $n$ 의 분할의 개수와 같음을 보이십시오.

위 그림을 그린 김에, 다음도 정의해 보겠습니다.

**정의 16.4.5.**  $G$ 를 군이라 합시다.  $G$ 의 **중심**은  $Z(G)$ 로 표기하며, 모든  $g \in G$ 에 대해  $xg = gx$ 를 만족하는 원소  $x \in G$ 의 집합입니다. 더 간결하게는,

$$Z(G) := \{x \in G \mid gx = xg \ \forall g \in G\}.$$

이것이 실제로  $G$ 의 부분군임을 확인할 수 있습니다.

**질문 16.4.6.**  $Z(G)$ 는 왜  $G$ 의 정규 부분군일까요?

**질문 16.4.7.** 중심에 속한 원소들의 켤레류는 무엇일까요?

충분히 자주 쓰이므로 명시적으로 짚고 넘어가야 할 자명한 결과가 있습니다.

**따름정리 16.4.8 (아벨 군에서의 켤레 관계는 자명합니다)**

$G$ 가 아벨 군이면, 모든 켤레류의 크기는 1입니다.

## §16.5 생각해 볼 만한 조금 더 어려운 문제

**문제 16A** (PUMaC 2009 C8). Taotao는 주황색, 흰색, 검은색 중 하나인 구슬 일곱 개로 이루어진 팔찌를 사려고 합니다. (팔찌는 공간에서 회전하거나 뒤집을 수 있습니다.) 가능한 팔찌의 개수를 구하십시오.

**문제 16B.** 같은 켤레류에 속한 두 원소가 같은 위수를 가짐을 보이십시오.



**문제 16C.** 번사이드 보조정리(Burnside's lemma)를 증명하십시오.

**문제 16D\*** (“류 방정식”).  $G$ 를 유한군이라 하겠습니다. 각  $g \in G$ 에 대해 **중심화군**(centralizer)  $C_G(g) = \{x \in G \mid xg = gx\}$ 을 정의합니다. 다음을 보이십시오.

$$|G| = |Z(G)| + \sum_{s \in S} \frac{|G|}{|C_G(s)|}$$

여기서  $S \subseteq G$ 는 다음과 같이 정의됩니다:  $|C| > 1$ 인 각 켤레류  $C \subseteq G$ 에 대해,  $C$ 의 대표원을 하나 골라  $S$ 에 추가합니다.



**문제 16E<sup>†</sup>** (고전적).  $G$ 를 위수  $n \geq 2$ 인 유한군이라 가정하고,  $p$ 를  $n$ 을 나누는 가장 작은 소수라 합니다.  $H$ 를  $G$ 의 부분군이라 하고  $|G|/|H| = p$ 라 합니다.  $H$ 가  $G$ 에서 정규부분군임을 보이십시오.

# 17 모든 군을 찾으시오

다음 문제는 IMO에 출제되지 않기를 바랍니다.

$n$ 을 양의 정수라 하고  $S = \{1, \dots, n\}$ 이라 합시다. 다음을 만족하는 모든 함수  $f: S \times S \rightarrow S$ 를 찾으시오.

- (a) 모든  $x \in S$ 에 대해  $f(x, 1) = f(1, x) = x$ 입니다.
- (b) 모든  $x, y, z \in S$ 에 대해  $f(f(x, y), z) = f(x, f(y, z))$ 입니다.
- (c) 모든  $x \in S$ 에 대해  $f(x, y) = f(y, x) = 1$ 을 만족하는  $y \in S$ 가 존재합니다.

그럼에도 불구하고, 이 “문제”에 대해 우리가 이루어낸 진전은 놀랍습니다. 이 장에서는 우리가 이루어낸 몇 가지 성과에 대해 이야기해보겠습니다.

## §17.1 실로우 정리

여기서는 유한군에 대해 우리가 가진 가장 일반적인 결과 중 하나인 유명한 실로우 정리를 소개합니다.

### 정리 17.1.1 (실로우 정리)

$G$ 를 위수가  $p^n m$ 인 군이라 하고, 여기서  $\gcd(p, m) = 1$ 이며  $p$ 는 소수입니다. **실로우  $p$ -부분군**이란 위수가  $p^n$ 인 부분군입니다.  $n_p$ 를  $G$ 의 실로우  $p$ -부분군의 개수라 합시다. 그러면

- (a)  $n_p \equiv 1 \pmod{p}$ 입니다. 특히,  $n_p \neq 0$ 이며 실로우  $p$ -부분군이 존재합니다.
- (b)  $n_p$ 는  $m$ 을 나눕니다.
- (c) 임의의 두 실로우  $p$ -부분군은 켤레 부분군입니다(따라서 동형사상입니다).

실로우 정리는 군을 분류하는 데 있어 정말로 막대한 역할을 합니다. 특히,  $n_p \equiv 1 \pmod{p}$ 와  $n_p \mid m$ 이라는 조건은 종종  $n_p$ 의 값을 몇 개의 값으로 좁혀줍니다. 다음은 실로우 정리로부터 따라 나오는 몇 가지 결과입니다.

- 실로우  $p$ -부분군이 정규부분군인 것은  $n_p = 1$ 인 것과 동치입니다.
- $p < q$ 가 소수일 때, 위수가  $pq$ 인 임의의 군  $G$ 는 반드시  $n_q = 1$ 이어야 합니다. 왜냐하면  $n_q \equiv 1 \pmod{q}$ 이면서도  $n_q \mid p$ 이기 때문입니다. 따라서  $G$ 는 위수가  $q$ 인 정규부분군을 가집니다.
- 임의의 아벨 군은 모든 부분군이 정규부분군이므로, 임의의 아벨 군은 그 위수를 나누는 모든  $p$ 에 대해 정확히 하나의 실로우  $p$ -부분군을 가진다는 것이 따라 나옵니다.
- $p \neq q$ 이면, 실로우  $p$ -부분군과 실로우  $q$ -부분군의 교집합은  $\{1_G\}$ 뿐입니다. 이는 임의의 두 부분군의 교집합 또한 부분군이며, 라그랑주 정리에 의해 그 위수가  $p$ 의 거듭제곱과  $q$ 의 거듭제곱을 모두 나누어야 하기 때문입니다. 이는 그 부분군이 자명한 경우에만 가능합니다.

또 다른 “실용적” 응용의 예를 살펴보겠습니다.

### 명제 17.1.2 (소수의 삼중곱)

$|G| = pqr$ 가 서로 다른 소수들의 곱이라면,  $G$ 는 정규 실로우 부분군을 가져야 합니다.

증명. 일반성을 잃지 않고  $p < q < r$ 이라 합시다.  $n_p \equiv 1 \pmod{p}$ 이고  $n_p | qr$ 이며 순환적으로도 마찬가지임에 주목하고, 모순을 이끌어내기 위해  $n_p, n_q, n_r > 1$ 이라 가정합시다.

$n_r | pq$ 이므로,  $n_r \geq 1 + r > p, q$ 이기 때문에  $n_r$ 은  $p$ 도  $q$ 도 나누지 않으므로  $n_r = pq$ 입니다. 또한  $n_p \geq 1 + p$ 이고  $n_q \geq 1 + q$ 입니다. 따라서 우리는 적어도  $1 + p$ 개의 실로우  $p$ -부분군, 적어도  $1 + q$ 개의 실로우  $q$ -부분군, 그리고 적어도  $pq$ 개의 실로우  $r$ -부분군을 가져야 합니다. 하지만 이 군들은 상당히 배타적입니다.

**질문 17.1.3.**  $n_p + n_q + n_r$ 개의 실로우 부분군을 취하고, 이들 중 두 개, 예를 들어  $H_1$ 과  $H_2$ 를 생각해 봅시다.  $H_1 \cap H_2$ 가  $H_1$ 과  $H_2$  둘 다의 부분군임을 확인한 다음 라그랑주 정리를 사용하여  $|H_1 \cap H_2| = 1$ 임을 다음과 같이 보이십시오.

이제 원소가 너무 많다는 것을 주장합니다. 실제로 이 부분군들이 기여하는 항등원이 아닌 원소들을 세어보면 다음을 얻습니다.

$$n_p(p-1) + n_q(q-1) + n_r(r-1) \geq (1+p)(p-1) + (1+q)(q-1) + pq(r-1) > pqr$$

이는  $G$ 가 가진 것보다 더 많은 원소입니다! □

## §17.2 (선택) 실로우 정리 증명하기

실로우 정리의 증명은 다소 복잡하며, 실제로 여러 증명이 존재합니다. 저는 아래에서 그중 하나를 제시하겠습니다. 이 증명은 군 작용을 광범위하게 사용하므로, 먼저 몇 가지 사실을 상기하고자 합니다.  $G$ 가  $X$ 에 작용한다면,

- 작용의 궤도들은  $X$ 의 분할을 이룹니다.
- $\mathcal{O}$ 가 임의의 궤도라면, 궤도-안정자군 정리는 다음을 말합니다.

$$|\mathcal{O}| = |G| / |\text{Stab}_G(x)|$$

임의의  $x \in \mathcal{O}$ 에 대해.

- 특히, 위에서  $G$ 가  $p$ -군, 즉 어떤  $t$ 에 대해  $|G| = p^t$ 라고 합시다. 그러면  $|\mathcal{O}| = 1$ 이거나  $p$ 가  $|\mathcal{O}|$ 를 나눕니다.  $\mathcal{O} = \{x\}$ 인 경우, 정의에 의해  $x$ 는  $G$ 의 모든 원소의 **고정점**입니다. 즉 모든  $g$ 에 대해  $g \cdot x = x$ 입니다.

$x$ 가 고정점이라고 말할 때, 이는 군의 **모든** 원소에 의해 고정된다는 것, 즉 궤도의 크기가 정말로 1이라는 것을 의미함에 유의하십시오. 따라서 이는 정말로 강한 조건입니다.

### §17.2.i 정의

**이 절의 대표적인 예:**  $S_n$ 에서의 켄레.

저는 앞서 원소들의 켄레를 정의했지만, 이제 군에 대해서도 정의할 필요가 있습니다.

**정의 17.2.1.**  $G$ 를 군이라 하고,  $X$ 를  $G$ 의 부분군들의 집합이라고 합시다. 그러면 **결레화**는  $G$ 가  $X$ 에 작용하여 다음을 보내는 작용입니다.

$$H \mapsto gHg^{-1} = \{ghg^{-1} \mid h \in H\}.$$

$H$ 와  $K$ 가  $G$ 의 부분군이고 어떤  $g \in G$ 에 대해  $H = gKg^{-1}$ 라면 (다시 말해, 이 작용 아래 같은 궤도에 있다면), 우리는 이들을 **결레** 부분군이라고 부릅니다.

우리는 어쩌면 결레 원소들을 "그렇게 다르다"고 여기지 않기 때문에(예를 들어, 순열군에서), 다음은 놀랍지 않을 것입니다.

**질문 17.2.2.** 군  $G$ 의 임의의 부분군  $H$ 에 대해,  $h \mapsto ghg^{-1}$ 로 정의되는 사상  $H \rightarrow gHg^{-1}$ 가 실제로 동형사상임을 보이십시오. 이는 임의의 두 결레 부분군이 서로 동형사상임을 함의합니다.

**정의 17.2.3.**  $G$ 의 임의의 부분군  $H$ 에 대해  $H$ 의 **정규화군**은 다음과 같이 정의됩니다.

$$N_G(H) := \{g \in G \mid gHg^{-1} = H\}.$$

다시 말해, 이는 결레화 작용 아래에서  $H$ 의 안정자군입니다.

이제 증명을 제시할 준비가 되었습니다.

### §17.2.ii 1단계: 실로우 $p$ -부분군이 존재함을 증명하기

다음은 일종의 확률론적 방법과 비슷합니다. 크기  $p^n$ 인 모든 부분집합의 집합  $X$ 를 한꺼번에 고려함으로써, 우리는 다음과 같은 "심오한 수론적 사실"을 활용할 수 있습니다.

$$|X| = \binom{p^nm}{p^n} \not\equiv 0 \pmod{p}.$$

(사실 그렇게 심오하지는 않습니다. 뤼카의 정리를 사용하십시오.)

증명은 다음과 같습니다.

- $G$ 가  $g \cdot S := \{gs \mid s \in S\}$ 로  $X$ 에 작용하도록 합시다.
- 크기가  $p$ 로 나누어떨어지지 않는 궤도  $\mathcal{O}$ 를 잡습니다. (이는 우리의 심오한 정수론적 사실 덕분에 가능합니다.  $|X|$ 가  $\text{mod } p$ 로 0이 아니고 궤도들이  $X$ 를 분할하므로, 주장된 궤도가 존재해야 합니다.)
- $S \in \mathcal{O}$ ,  $H = \text{Stab}_G(S)$ 라고 합시다. 그러면 궤도-안정자군 정리에 의해  $p^n$ 이  $|H|$ 를 나눕니다.
- 두 번째 작용을 생각해봅시다:  $H$ 가  $h \cdot s := hs$ 로  $S$ 에 작용하도록 합시다 ( $H = \text{Stab}_G(S)$ 이므로  $hs \in S$ 임을 알고 있습니다).
- $\text{Stab}_H(s) = \{1_H\}$ 임을 관찰하십시오. 그러면 두 번째 작용의 모든 궤도는 크기가  $|H|$ 이어야 합니다. 따라서  $|H|$ 는  $|S| = p^n$ 을 나눕니다.
- 이는  $|H| = p^n$ 임을 의미하며, 이로써 증명이 끝납니다.

### §17.2.iii 2단계: 임의의 두 실로우 $p$ -부분군은 켈레입니다

$P$ 가 실로우  $p$ -부분군이고  $Q$ 가  $p$ -군일 때,  $Q \subseteq gPg^{-1}$ 임을 증명합니다.  $Q$  또한 실로우  $p$ -부분군이라면, 크기상의 이유로  $Q = gPg^{-1}$ 가 됨에 주목하십시오; 이는 임의의 두 실로우 부분군이 실제로 켈레임을 의미합니다.

$Q$ 가 왼쪽 곱셈으로  $P$ 의 왼쪽 잉여류들의 집합에 작용하도록 합시다. 다음을 주목하십시오

- $Q$ 는  $p$ -군이므로, 임의의 궤도는 크기가 1이 아닌 한  $p$ 로 나누어떨어집니다.
- 그러나 왼쪽 잉여류의 개수는  $m$ 이며, 이는  $p$ 로 나누어떨어지지 않습니다.

따라서 어떤 잉여류  $gP$ 는 모든  $q$ 에 대해 고정점이 되며, 이는 모든  $q$ 에 대해  $qgP = gP$ 임을 의미합니다. 이는 모든  $q \in Q$ 에 대해  $qg \in gP$ 임과 동치이므로, 원하는 대로  $Q \subseteq gPg^{-1}$ 입니다.

### §17.2.iv 3단계: $n_p \equiv 1 \pmod{p}$ 보이기

$S$ 가 모든 실로우  $p$ -부분군의 집합을 나타내도록 합시다. 첫 번째 단계에 의해, 어떤  $P \in S$ 가 존재합니다.

**질문 17.2.4.**  $|S|$ 가 왜  $n_p$ 와 같습니까? (다시 말해, 깨어 있습니까?)

이제 증명을 진행할 수 있습니다.  $P$ 가 켈레작용으로  $S$ 에 작용하도록 합시다. 그러면:

- $P$ 가  $p$ -군이므로, 이 작용의 궤도들은 크기가  $\{p^0, p^1, p^2, \dots\}$  안에 있습니다. 특히, 고정점의 개수는  $\text{mod } p$ 로  $n_p \pmod{p}$ 와 같습니다.
- 이제  $P$ 가 이 작용의 유일한 고정점임을 주장합니다.
- $Q$ 를 임의의 다른 고정점이라 합시다, 즉 임의의  $x \in P$ 에 대해  $xQx^{-1} = Q$ 입니다.
- 정규화군  $N_G(Q) = \{g \in G \mid gQg^{-1} = Q\}$ 를 정의합니다. 이는  $P$ 와  $Q$ 를 모두 포함합니다.
- 이제 놀라운 부분입니다:  $N_G(Q)$ 에 2단계를 적용합니다.  $P$ 와  $Q$ 가 이것의 실로우  $p$ -부분군이므로, 이들은 켈레여야 합니다.
- 따라서 원하는 대로  $P = Q$ 입니다.

### §17.2.v 4단계: $n_p$ 는 $m$ 을 나눕니다

$n_p \equiv 1 \pmod{p}$ 이므로,  $n_p$ 가  $|G|$ 를 나눴을 보이면 충분합니다.  $G$ 가 켈레작용으로 모든 실로우  $p$ -군의 집합에 작용하도록 합시다. 2단계에 의하면 이 작용은 오직 하나의 궤도만을 가지므로, 궤도-안정자군 정리에 의해  $n_p$ 가  $|G|$ 를 나눕니다.

## §17.3 (선택) 단순군과 Jordan-Hölder

**이 절의 대표적인 예:**  $\mathbb{Z}/12\mathbb{Z}$ 의 분해는  $1 \leq \mathbb{Z}/2\mathbb{Z} \leq \mathbb{Z}/4\mathbb{Z} \leq \mathbb{Z}/12\mathbb{Z}$ 입니다.

모든 정수가 소수의 곱으로 분해되는 것처럼, 모든 군도 “기본적인” 군의 곱으로 분해해 볼 수 있습니다. 몫군에 대한 아이디어로 무장하면, 올바른 개념은 다음과 같습니다.

**정의 17.3.1.** **단순군**이란 자기 자신과 자명군 외에는 정규 부분군을 갖지 않는 군입니다.

**질문 17.3.2.** 어떤  $n$ 에 대해  $\mathbb{Z}/n\mathbb{Z}$ 이 단순군입니까? (힌트:  $\mathbb{Z}/n\mathbb{Z}$ 이 아벨 군임을 기억하십시오.)

그다음 “군을 분해한다”는 것이 무엇을 의미하는지 정의해 볼 수 있습니다.

**정의 17.3.3.** 군  $G$ 의 **조성열**이란 다음을 만족하는 부분군  $H_0, H_1, \dots, H_n$ 의 수열입니다

$$\{1\} = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \dots \trianglelefteq H_n = G$$

최대 길이입니다(즉  $n$ 이 가능한 한 크지만, 모든  $H_i$ 는 물론 서로 다릅니다). **조성 인자**는  $H_1/H_0, H_2/H_1, \dots, H_n/H_{n-1}$  군들입니다.

“최대성” 조건이 조성인자가 모두 단순군임을 함의한다는 것을 보일 수 있습니다.

두 조성열이 (순열을 제외하고) 같은 조성 인자를 가지면 동치라고 합시다; 특히 이 경우 길이도 같습니다. 그러면 다음 정리가 실제로 참이라는 것이 밝혀집니다.

#### 정리 17.3.4 (Jordan-Hölder)

모든 유한군  $G$ 는 동치를 제외하면 유일한 조성열을 가집니다.

#### 예제 17.3.5 ( $n = 12$ 일 때의 산술의 기본 정리)

군  $\mathbb{Z}/12\mathbb{Z}$ 를 생각해 봅시다. 가능한 조성열이 다음과 같음을 확인하는 것은 어렵지 않습니다

$$\{1\} \trianglelefteq \mathbb{Z}/2\mathbb{Z} \trianglelefteq \mathbb{Z}/4\mathbb{Z} \trianglelefteq \mathbb{Z}/12\mathbb{Z} \text{ 인자가 } \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \text{ 인}$$

$$\{1\} \trianglelefteq \mathbb{Z}/2\mathbb{Z} \trianglelefteq \mathbb{Z}/6\mathbb{Z} \trianglelefteq \mathbb{Z}/12\mathbb{Z} \text{ 인자 } \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \text{ 를 가지며}$$

$$\{1\} \trianglelefteq \mathbb{Z}/3\mathbb{Z} \trianglelefteq \mathbb{Z}/6\mathbb{Z} \trianglelefteq \mathbb{Z}/12\mathbb{Z} \text{ 인자가 } \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \text{ 인.}$$

이는 인수분해  $12 = 2^2 \cdot 3$ 에 대응됩니다.

이는 모든 유한군이 어떤 의미에서 단순군의 “곱”이므로, 모든 유한 단순군을 분류하는 것이 큰 진전이 될 것임을 시사합니다. 유일한 문제는 구성 요소로부터 군을 만드는 방법이 여러 가지라는 것입니다.

놀랍게도, 우리는 실제로 단순군의 전체 목록을 가지고 있지만, 그 목록은 정말로 기이합니다. 모든 유한 단순군은 다음 범주 중 하나에 속합니다:

- 소수  $p$ 에 대한  $\mathbb{Z}/p\mathbb{Z}$ ,
- $n \geq 5$ 일 때,  $S_n$ 의 부분군 중 “짜” 순열로 이루어진 것,
- 리 타입의 단순군(설명하지 않겠습니다), 그리고
- 어떤 좋은 계열에도 속하지 않는 스물여섯 개의 “산발”군.

산발군 중 가장 큰 두 개는 귀여운 이름을 가지고 있습니다. **베이비 몬스터군**의 위수는

$$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47 \approx 4 \cdot 10^{33}$$

그리고 **몬스터군**(“**프렌들리 자이언트**”라고도 함)의 위수는

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \approx 8 \cdot 10^{53}.$$

이는 산발군 중 스무 개를 부분몫으로 포함하며(자기 자신 포함), 이 스무 개의 군을 “**행복한 가족**”이라고 부릅니다.

수학은 이상합니다.

**질문 17.3.6.** “위수 2의 유한 단순군”이라는 표현이 중복임을 보이십시오. 즉, 위수 2인 군은 항상 유한하면서 동시에 단순군입니다.

## §17.4 생각해 볼 만한 조금 더 어려운 문제

**문제 17A\*** (코시의 정리).  $G$ 를 군이라 하고  $p$ 를  $|G|$ 를 나누는 소수라 하십시오.  $G$ 가 위수  $p$ 인 원소를 가짐을 증명<sup>1</sup>하십시오.

**문제 17B.**  $G$ 를 유한 단순군이라 하십시오.  $|G| \neq 56$ 임을 보이십시오.



**문제 17C** (엔겔의 PSS?). 문자  $a$ 와  $b$ 로 이루어진 모든 단어의 집합을 생각해봅시다. 이러한 단어가 주어졌을 때, 주어진 단어의 어느 위치에나  $www$  형태의 단어(여기서  $w$ 는 하나의 단어)를 삽입하거나 그러한 수열을 단어에서 삭제함으로써 단어를 변형할 수 있습니다. 단어  $ab$ 를 단어  $ba$ 로 바꿀 수 있습니까?



**문제 17D.**  $p$ 를 소수라 하고  $G$ 가 위수가  $p$ 의 거듭제곱인 단순군이라고 합시다.  $G \cong \mathbb{Z}/p\mathbb{Z}$ 임을 보이십시오.



**문제 17E** (Athemath Community-Building Event #1, Fall 2022). 군 작용  $\cdot$ 은 군  $G$ 가 집합  $X$ 에 대해 하는 작용으로서, 다음과 같다고 합니다.

- **추이적**이라 함은, 모든  $x_1, x_2 \in X$ 에 대해 어떤  $g$ 가 존재하여  $g \cdot x_1 = x_2$ 가 성립하는 것을 말합니다;
- **충실**이라 함은,  $g \in G$  중에서  $g \cdot x = x$ 가 모든  $x \in X$ 에 대해 성립하는 유일한 원소가  $g = 1_G$ 인 경우를 말합니다. 다시 말해, 전체 집합  $X$ 에 자명하게 작용하는 유일한 원소는  $G$ 의 항등원입니다.

6개 원소로 이루어진 집합에 대한  $S_5$ 의 충실한 추이적 작용이 존재합니까?

<sup>1</sup>코시의 정리는 실로우 정리 없이도 증명할 수 있으며, 실제로 실로우 정리의 대안적 증명을 제공하는 데 종종 사용될 수 있습니다.

# 18 PID 구조 정리

이 장의 요지는 유한 생성 아벨 군에 대한 분류 정리를 다루는 것입니다. 이는 오래 걸리지 않으므로, 원하신다면 첫 번째 절만 읽고 넘어가셔도 됩니다.

하지만 이왕 여기까지 온 김에, 훨씬 더 일반적인 구조 정리의 특수한 경우로서 그 결과를 서술하겠습니다. 그 따름정리들은 다음을 포함합니다

- 모든 유한 차원 벡터 공간은  $k^{\oplus n}$ 입니다.
- 유한 생성 아벨 군에 대한 분류 정리,
- 앞서 나온 행렬의 조르당 분해,
- 행렬의 또 다른 표준형인 "프로베니우스 표준형",

## §18.1 유한 생성 아벨 군

**비고 18.1.1** — 이어지는 내용에서 아벨 군에 관해 이야기하겠지만, 사실 이러한 구조를 이해하는 도덕적으로 올바른 방법은 이를  $\mathbb{Z}$ -가군으로 보는 것입니다.

**정의 18.1.2.** 아벨 군  $G = (G, +)$ 가  $\mathbb{Z}$ -가군으로서 유한 생성이면 **유한 생성**이라고 합니다. (즉, 유한 개의 원소 모임  $b_1, \dots, b_m \in G$ 가 존재하여, 모든  $x \in G$ 가 어떤  $c_1, \dots, c_m \in \mathbb{Z}$ 에 대해  $c_1 b_1 + \dots + c_m b_m$ 의 형태로 쓰일 수 있음을 의미합니다.)

**예제 18.1.3** (유한 생성 아벨 군의 예시)

- (a)  $\mathbb{Z}$ 는 (1에 의해) 유한 생성됩니다.
- (b)  $\mathbb{Z}/n\mathbb{Z}$ 은 (1에 의해) 유한 생성됩니다.
- (c)  $\mathbb{Z}^{\oplus 2}$ 는 (두 원소  $(1, 0)$ 과  $(0, 1)$ 에 의해) 유한 생성됩니다.
- (d)  $\mathbb{Z}^{\oplus 3} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/2016\mathbb{Z}$ 은 다섯 개의 원소에 의해 유한 생성됩니다.
- (e)  $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ 는 두 개의 원소에 의해 유한 생성됩니다.

**연습문제 18.1.4.** 사실  $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ 는 하나의 원소에 의해 생성됩니다. 그것은 무엇일까요?

이 예시들이 그다지 다양하지 않다는 것을 눈치채셨을지도 모릅니다. 그 이유는 이것들이 실제로 유일한 예시들이기 때문입니다:

**정리 18.1.5 (유한 생성 아벨 군의 기본 정리)**

$G$ 를 유한 생성 아벨 군이라고 합시다. 그러면 다음을 만족하는 정수  $r$ 과 소수의 거듭제곱  $q_1, \dots, q_m$  (반드시 서로 다를 필요는 없음)이 존재합니다

$$G \cong \mathbb{Z}^{\oplus r} \oplus \mathbb{Z}/q_1\mathbb{Z} \oplus \mathbb{Z}/q_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/q_m\mathbb{Z}.$$

이 분해는  $\mathbb{Z}/q_i\mathbb{Z}$ 들의 순열을 제외하면 유일합니다.

**정의 18.1.6.** 유한 생성 아벨 군  $G$ 의 **계수**란 위의 정수  $r$ 을 말합니다.

이제 이 정리를 증명할 수도 있지만, 전체 구조 정리를 서술하고 증명하여 정공법으로 나아가는 것이 더 흥미롭습니다.

**§18.2 환론의 몇 가지 선행 지식**

**이 절의 대표적인 예:**  $R = \mathbb{Z}$ .

주요 정리를 서술하기 전에,  $\mathbb{Z}$ 와 매우 비슷하게 행동하는 UFD에 대한 몇 가지 용어를 정의해야 합니다:

$R = \mathbb{Z}$ 인 경우에 대한 직관은 기본적으로 그대로 이어집니다.

소 아이디얼을 다룰 필요조차 없으며, 대신 원소를 인수분해할 수 있습니다.

**정의 18.2.1.**  $R$ 이 UFD라면,  $(p)$ 가 소 아이디얼이고  $p \neq 0$ 일 때  $p \in R$ 을 **소원소**라고 합니다. UFD의 경우 이는 다음과 동치입니다:  $p = xy$ 이면  $x$  또는  $y$  중 하나는 단원입니다.

그러므로 예를 들어  $\mathbb{Z}$ 에서 소원소의 집합은  $\{\pm 2, \pm 3, \pm 5, \dots\}$ 입니다. 이제  $R$ 이 UFD이므로, 모든 원소  $r$ 은 소원소들의 곱으로 인수분해됩니다

$$r = up_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$$

**정의 18.2.2.** 어떤  $r' \in R$ 에 대해  $s = r'r$ 이면  $r$ 이  $s$ 를 **나눈다**고 합니다. 이는  $r \mid s$ 로 표기합니다.

**예제 18.2.3 ( $\mathbb{Z}$ 에서의 나눗셈)**

수 0은  $\mathbb{Z}$ 의 모든 원소로 나누어집니다. 그 외의 나눗셈은 예상한 대로입니다.

**질문 18.2.4.**  $r$ 에서 각 소원소의 지수가  $s$ 에서의 대응하는 지수보다 작거나 같을 때, 그리고 오직 그때만  $r \mid s$ 임을 보이십시오.

이제 관심 있는 경우는  $R$ 이 PID인, 훨씬 더 강한 경우입니다:

**명제 18.2.5 (PID는 뇌터 UFD입니다)**

$R$ 이 PID이면, 이는 뇌터 환이며 또한 UFD입니다.

**증명.**  $R$ 이 뇌터라는 사실은 자명합니다.  $R$ 이 UFD임을 보이기 위해서는  $\mathbb{Z}$ 에 대한 증명을 본질적으로 반복하며,  $(a, b)$ 가 주 아이디얼이라는 사실을 이용해  $\gcd(a, b)$ 를 추출합니다. □

이 경우, 원소에 대한 중국인의 나머지 정리를 가집니다.

**정리 18.2.6 (환에 대한 중국인의 나머지 정리)**

$m$ 과  $n$ 을 서로소인 원소, 즉  $(m) + (n) = (1)$ 이라고 하겠습니다. 그러면

$$R/(mn) \cong R/(m) \times R/(n).$$

여기서 환의 곱은 **예제 4.3.8**에서 정의한 대로입니다.

증명. 이는 일반적인 중국인의 나머지 정리의 증명과 같습니다. 먼저,  $(m, n) = (1)$ 이므로 어떤  $a$ 와  $b$ 에 대해  $am + bn = 1$ 입니다. 그러면 다음과 같은 사상을 가집니다

$$R/(m) \times R/(n) \rightarrow R/(mn) \quad \text{에 의해} \quad (r, s) \mapsto r \cdot bn + s \cdot am.$$

이 사상이 잘 정의되어 있고 환의 동형사상임을 확인할 수 있습니다. (근면한 독자는 직접 확인해 보시기 바랍니다.)  $\square$

마지막으로, 뇌터  $R$ -가군의 개념을 도입해야 합니다.

**정의 18.2.7.**  $R$ -가군  $M$ 은 다음 두 동치 조건 중 하나를 만족하면 **뇌터**라고 합니다:

- $M$ 의 부분가군은 오름 사슬 조건을 만족합니다: 즉  $M_1 \subsetneq M_2 \subsetneq \dots$ 와 같은 무한 수열의 가군은 존재하지 않습니다.
- $M$ 의 모든 부분가군은 ( $M$  자신을 포함하여) 유한하게 생성됩니다.

이는 뇌터 환의 개념을 일반화한 것입니다: 뇌터 환  $R$ 은  $R$ 이  $R$ -가군으로서 뇌터인 환입니다.

**질문 18.2.8.** 이 두 조건이 동치임을 확인하십시오. (환에 대한 증명을 그대로 따르십시오.)

## §18.3 구조 정리

우리의 구조 정리는 두 가지 형태를 취합니다:

**정리 18.3.1 (구조 정리, 불변량 형식)**

$R$ 을 PID라 하고  $M$ 을 임의의 유한 생성  $R$ -가군이라 합시다. 그러면

$$M \cong \bigoplus_{i=1}^m R/(s_i)$$

어떤  $s_i$ (0일 수도 있음)에 대해  $s_1 \mid s_2 \mid \dots \mid s_m$ 을 만족합니다.

**따름정리 18.3.2 (구조 정리, 준소 형식)**

$R$ 을 PID라 하고  $M$ 을 임의의 유한 생성  $R$ -가군이라 합시다. 그러면

$$M \cong R^{\oplus r} \oplus R/(q_1) \oplus R/(q_2) \oplus \dots \oplus R/(q_m)$$

여기서  $q_i = p_i^{e_i}$ 이며, 어떤 소원소  $p_i$ 와 정수  $e_i \geq 1$ 에 대해 성립합니다.

따름정리의 증명. ( $R$ 이 UFD이므로) 각  $s_i$ 를 소인수로 분해한 다음, 중국인의 나머지 정리를 사용합니다.  $\square$

**비고 18.3.3** — 두 정리 모두에서 그 분해는 합산항들의 순열을 제외하면 유일합니다.

## §18.4 자유 $R$ -가군 사이의 사상으로서의 환원

**정의 18.4.1.** 자유  $R$ -가군이란  $R^{\oplus n}$  꼴의 가군을 말합니다(더 일반적으로는, 무한 기저를 허용하기 위해 어떤 첨수 집합  $I$ 에 대한  $\bigoplus_I R$ ).

구조 정리의 증명은 두 가지 주요 단계로 진행됩니다. 먼저, 문제를 자유  $R$ -가군  $R^{\oplus d}$ 가 관여하는 선형대수 문제로 환원합니다. 이것이 끝나면, 그저 행렬을 다루기만 하면 되는데, 이는 다음 절에서 다룹니다.

$M$ 이  $d$ 개의 원소로 유한 생성된다고 합시다. 그러면 다음과 같은 전사  $R$ -가군 사상이 존재합니다

$$R^{\oplus d} \twoheadrightarrow M$$

$R^{\oplus d}$ 의 기저에 대한 상이  $M$ 의 생성원인 사상을 생각합니다.  $K$ 를 그 핵이라 합니다.

우리는  $K$  역시 유한 생성임을 주장합니다. 이를 위해 다음을 증명합니다

**보조정리 18.4.2** (뇌터 가군의 직합은 뇌터 가군이다)

$M$ 과  $N$ 을 두 뇌터  $R$ -가군이라 합시다. 그러면 직합  $M \oplus N$  역시 뇌터  $R$ -가군입니다.

증명.  $L \subseteq M \oplus N$ 이면  $L$ 이 유한 생성임을 보이는 것으로 충분합니다. 한 가지 추측은  $L = P \oplus Q$ 인데, 여기서  $P$ 와  $Q$ 는  $L$ 을  $M$ 과  $N$ 으로 사영한 것입니다. 안타깝게도 이는 거짓입니다( $M = N = \mathbb{Z}$ 이고  $L = \{(n, n) \mid n \in \mathbb{Z}\}$ 인 경우를 생각해 보십시오), 따라서 우리는 더 조심해야 합니다.

다음 부분가군들을 생각해 봅시다

$$A = \{x \in M \mid (x, 0) \in L\} \subseteq M$$

$$B = \{y \in N \mid \exists x \in M : (x, y) \in L\} \subseteq N.$$

( $A$ 와  $B$ 에 대한 비대칭성에 주목하십시오: 그렇지 않으면 증명이 성립하지 않습니다.) 그러면  $A$ 는  $a_1, \dots, a_k$ 에 의해 유한 생성되고,  $B$ 는  $b_1, \dots, b_\ell$ 에 의해 유한 생성됩니다.  $x_i = (a_i, 0)$ 이라 하고  $y_i = (*, b_i)$ 를  $L$ 의 원소라 합시다(여기서  $*$ 는 우리가 신경 쓰지 않는 임의의 것입니다). 그러면  $x_i$ 와  $y_i$ 가 함께  $L$ 을 생성합니다.  $\square$

**질문 18.4.3.**  $R$ 이 PID일 때  $R^{\oplus d}$ 가 뇌터 가군임을 이끌어 내십시오.

따라서  $K \subseteq R^{\oplus d}$ 는 주장한 대로 유한 생성입니다. 그러므로 우리는 또 다른 전사 사상  $R^{\oplus f} \twoheadrightarrow K$ 를 찾을 수 있습니다. 결과적으로, 우리는 다음과 같은 합성을 얻습니다

$$\begin{array}{ccccc} & & K & & \\ & \nearrow & \searrow & & \\ R^{\oplus f} & \xrightarrow{T} & R^{\oplus d} & \twoheadrightarrow & M \end{array}$$

$M$ 이 선형 사상  $T$ 의 여핵임을 관찰하십시오, 즉 다음이 성립합니다

$$M \cong R^{\oplus d} / \text{im}(T).$$

따라서 사상  $T$ 를 잘 이해하는 것으로 충분합니다.

## §18.5 준소 형식의 유일성

이 절에서 우리는,  $M \cong R^{\oplus r} \oplus R/(q_1) \oplus R/(q_2) \oplus \cdots \oplus R/(q_m)$ 이면 정수  $r$ 과 소수 거듭제곱  $q_i$ 가 순열을 제외하면 유일함을 증명할 것입니다.

먼저,  $M$ 이 자유가군인 경우를 고려합니다.

### 정리 18.5.1 (자유가군의 계수의 유일성)

가환 정역  $R$ 에 대해, 자유가군  $M$ 이 유한 기저를 가진다면, 다른 모든 기저도 같은 개수의 원소를 가집니다.

**정리 9.4.7**에서 증명 전략이 체의 경우로 넘어가는 것이라는 점을 한 번 언급한 바 있습니다. 실제로, 우리는  $R$ 의 분수체인 체  $F$ 로 넘어간 다음, 벡터 공간에 대한 차원 정리를 직접 적용할 것입니다.

**증명.** 이전과 마찬가지로, 이번에는 귀류법으로 증명합니다.  $v_1, \dots, v_n$ 이 계수  $n$ 인 자유가군  $M$ 의 기저이고,  $w_1, \dots, w_m$ 은  $m > n$ 을 만족하는  $M$ 의 임의의 원소들이라고 가정합니다.

$F$ 를  $R$ 의 분수체라 하고,  $R$ -가군  $M \cong R^n$ 을  $F$ -벡터 공간  $V \cong F^n$ 에 매장시킵니다.

그러면  $m > n$ 이므로  $V$ 의 원소로서  $w_1, \dots, w_m$ 은 선형종속이며, 이는 모두 0은 아닌 어떤 원소  $f_1, \dots, f_m \in F$ 가 존재하여  $f_1 w_1 + \cdots + f_m w_m = 0$ 이 성립함을 의미합니다.

분모를 제거함으로써, 모두 0은 아닌 환의 원소  $r_1, \dots, r_m \in R$ 을 얻을 수 있으며, 이는  $r_1 w_1 + \cdots + r_m w_m = 0$ 을 만족합니다. 이는  $w_1, \dots, w_m$ 이  $M$ 의 기저가 될 수 없음을 의미합니다.  $\square$

다음으로, 계수  $r$ 이 0인 경우를 증명합니다. 이 경우는 다른 전략이 필요하지만, 여전히 적절히 구성된 벡터 공간에 대해 차원 정리를 적용하는 것으로 귀결됩니다.

### 정리 18.5.2

$R$ 을 PID라 하고,  $p$ 를  $R$ 의 소원이라 하고, 양의 정수  $e_1, \dots, e_m$ 에 대해  $M \cong R/(p^{e_1}) \oplus R/(p^{e_2}) \oplus \cdots \oplus R/(p^{e_m})$ 이라 합시다. 그러면  $e_i$ 들은 순열까지 감안하면 유일합니다.

직관적으로, 다음 증명이 시도하는 것은 다음과 같습니다:

**$M$ 의 본질적인 성질로부터 지수  $e_i$ 를 계산할 수 있다면, 그 지수들은 유일할 수밖에 없습니다.**

간단한 경우를 생각해봅시다 —  $R = \mathbb{Z}$ 이고  $M = \mathbb{Z}/4\mathbb{Z}$ 인 경우를 생각해봅시다. 이 가군은 원소가 4개이지만,  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ 와 같지는 않습니다. 이 경우, 두 가군의 차이는  $M$ 에서 원소 1 (mod 4)에 2를 곱하면 0이 되지 않는 반면,  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ 의 모든 원소는 2를 곱하면 0이 된다는 사실로 확인할 수 있습니다.

표기의 편의를 위해,

**정의 18.5.3.**  $r \in R$ 과  $R$ -가군  $M$ 에 대해,  $rM = \{rm \mid m \in M\}$ 을 정의합니다. (이것이 여전히  $R$ -가군임을 확인하십시오.)

그러면, 위 문단이 말하는 바는  $|2M| = 2 \neq 1 = |2(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})|$ 이므로  $M \not\cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ 라는 것입니다. 다시 말해, 이 경우  $2M$ 의 원소 개수를 세는 것만으로 두 가군을 구별하기에 충분합니다.

$R = \mathbb{Z}$ 일 때  $M \cong R/(p^{e_1}) \oplus R/(p^{e_2}) \oplus \cdots \oplus R/(p^{e_m})$  형태의 가군에 대해서는, 이는 일반적으로 거의 통합니다 — 다만  $pM, p^2M, p^3M$  등의 원소 개수도 고려해야 합니다.

동등하게, 연속적인 몫  $M/pM, pM/p^2M, p^2M/p^3M$  등의 원소 개수를 고려할 수도 있습니다.

#### 예제 18.5.4

$R = \mathbb{Z}, p = 3, M = \mathbb{Z}/3^2\mathbb{Z} \oplus \mathbb{Z}/3^5\mathbb{Z}$ 라 합시다. 그러면:

- $|M/3M| = 9,$
- $|3M/3^2M| = 9,$
- $|3^2M/3^3M| = 3,$
- $|3^3M/3^4M| = 3,$
- $|3^4M/3^5M| = 3,$
- 모든 정수  $e \geq 5$ 에 대해  $|3^eM/3^{e+1}M| = 1$ 입니다.

이것이 어디로 향하는지 이미 알 수 있을 것입니다 — 몫의 크기가 감소할 때마다 소수의 거듭제곱  $p^{e_i}$  하나에 대응합니다.

그러나 몫이 무한할 때는 더 이상 이렇게 할 수 없습니다. 하지만 다음을 주목하십시오:

#### 보조정리 18.5.5

모든 정수  $e \geq 0$ 에 대해,  $p^eM/p^{e+1}M$ 은  $R/(p)$ -벡터 공간입니다.

따라서,  $p^eM/p^{e+1}M$ 의 원소 개수를 세는 대신,  $p^eM/p^{e+1}M$ 을  $R/(p)$ -벡터 공간으로서의 차원을 셉니다 — 정리 9.4.7에 의해, 이는 실제로 가군  $M$ 에 본질적인 성질입니다.

**정리 18.5.2**의 증명.  $M \cong R/(p^{e_1}) \oplus R/(p^{e_2}) \oplus \cdots \oplus R/(p^{e_m})$ 이므로, 다음이 성립함에 유의하십시오.

$$\pi(M) \cong \pi(R/(p^{e_1})) \oplus \pi(R/(p^{e_2})) \oplus \cdots \oplus \pi(R/(p^{e_m}))$$

여기서  $\pi(M) = p^eM/p^{e+1}M$ 이며,  $e \geq 0$ 은 임의의 정수입니다.

이는  $R/(p)$ -벡터 공간으로서 다음을 의미합니다.

$$\dim \pi(M) = \dim \pi(R/(p^{e_1})) + \dim \pi(R/(p^{e_2})) + \cdots + \dim \pi(R/(p^{e_m})).$$

각 항  $R/(p^{e_i})$ 에 대해, 다음이 성립함에 유의하십시오.

$$\dim p^e(R/(p^{e_i}))/p^{e+1}(R/(p^{e_i})) = \begin{cases} 1 & e < e_i \\ 0 & \text{그렇지 않으면.} \end{cases}$$

약간의 계산을 통해, 값  $e_i$ 가 실제로  $\dim p^eM/p^{e+1}M$ 에 의해 순열까지 고려하여 유일하게 결정됨을 알 수 있습니다.  $\square$

이는 분모의 소수들이 서로 다른 경우로도 쉽게 일반화될 수 있음에 유의하십시오. 왜냐하면  $R$ 의 서로 다른 소수  $p$ 와  $q$ 에 대해,  $p^e(R/(q))/p^{e+1}(R/(q))$ 는 0차원  $R/(p)$ -벡터 공간이기 때문입니다.

마지막으로, 일반적인 경우를 다룹니다.

### 정리 18.5.6

$M \cong R^{\oplus r} \oplus R/(q_1) \oplus R/(q_2) \oplus \cdots \oplus R/(q_m)$ 이면, 정수  $r$ 과 소수 거듭제곱  $q_i$ 들은 순열까지 고려하여 유일합니다.

증명. 위의 두 정리로부터,  $R^{\oplus r}$  부분과  $R/(q_1) \oplus R/(q_2) \oplus \cdots \oplus R/(q_m)$  부분이  $M$ 으로부터 유일하게 결정됨을 증명하면 충분합니다.

표기의 편의를 위해,  $r \neq 0$ 인  $r \in R$ 이 존재하여  $ra = 0$ 을 만족시킬 때 원소  $a \in M$ 을 **꼬임 원소**라고 부릅니다.

그러면,

- 원소  $a \in M$ 의  $R^{\oplus r}$  성분이 영이면,  $q_1 q_2 \cdots q_m \cdot a = 0$ 이므로  $a$ 는 꼬임 원소입니다.
- 원소  $a \in M$ 의  $R^{\oplus r}$  성분이 영이 아니면,  $a$ 는 꼬임 원소가 아닙니다.

다시 말해, 모든 꼬임 원소로 이루어진 부분가군은  $R^{\oplus r}$  성분이 영인 원소들의 부분가군과 일치하므로,  $R/(q_1) \oplus R/(q_2) \oplus \cdots \oplus R/(q_m)$ 과 동형입니다.

표기의 편의를 위해,  $\text{Tor}(M)$ 을  $M$ 의 모든 꼬임 원소로 이루어진 부분가군이라고 합시다. 그러면  $\text{Tor}(M) \cong R/(q_1) \oplus R/(q_2) \oplus \cdots \oplus R/(q_m)$ 이고  $M/\text{Tor}(M) \cong R^{\oplus r}$ 이며, 다시 말해  $R^{\oplus r}$  부분과  $R/(q_1) \oplus R/(q_2) \oplus \cdots \oplus R/(q_m)$  부분은  $M$ 으로부터 유일하게 결정되므로, 증명이 끝났습니다.  $\square$

## §18.6 스미스 표준형

이제 우리의 문제가 선형 사상  $T: R^{\oplus m} \rightarrow R^{\oplus n}$ 을 연구하는 것으로 환원되었다는 것이 아이디어이며, 이는 일반적인 행렬로 생각할 수 있습니다.

$$T = \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{bmatrix}$$

$R^{\oplus m}$ 의 기저  $e_1, \dots, e_m$ 과  $R^{\oplus n}$ 의 기저  $f_1, \dots, f_n$ 에 대해서입니다.

물론, 예상할 수 있듯이  $T$ 의 주어진 기저를 바꾸어  $T$ 가 더 나은 행렬 형태를 갖도록 하는 것이 가능할 것입니다. 우리는 이미 조르당 형식에서 이를 본 적이 있는데, 그때는 사상  $T: V \rightarrow V$ 가 있었고 기저를 바꾸어  $T$ 가 "거의 대각"이 되도록 했습니다. 이번에는 바꿀 수 있는 기저가 두 세트이므로, 대각 기저, 혹은 그보다 더 나은 것을 얻을 수 있기를 기대해 볼 수 있습니다.

진행하기 전에, 행렬을 어떻게 편집할 수 있을지 생각해 봅시다: 어떤 연산이 허용됩니까? 다음은 몇 가지 예입니다.

- 행과 열을 바꾸는 것으로, 이는 단순히 기저의 재정렬에 해당합니다.
- 한 열의 배수를 다른 열에 더하는 것입니다. 예를 들어, 첫 번째 열의 3배를 두 번째 열에 더하면, 이는 기저를 다음으로 바꾸는 것과 동치입니다.

$$(e_1, e_2, e_3, \dots, e_m) \mapsto (e_1, e_2 + 3e_1, e_3, \dots, e_m).$$

- 한 행의 배수를 다른 행에 더하는 것입니다. 첫 번째 행의 3배를 두 번째 행에 더하는 것이 기저를 다음으로 바꾸는 것과 동치임을 알 수 있습니다.

$$(f_1, f_2, f_3, \dots, f_n) \mapsto (f_1 - 3f_2, f_2, f_3, \dots, f_n).$$

더 일반적으로,

**$A$ 가 가역  $n \times n$  행렬이면  $T$ 를  $AT$ 로 바꿀 수 있습니다.**

이는 다음을 바꾸는 것에 대응됩니다

$$(f_1, \dots, f_n) \mapsto ((FA^{-1})_1, \dots, (FA^{-1})_n)$$

(“가역” 조건은 후자가 기저임을 보장할 뿐입니다). 여기서  $F$ 는 열이  $f_1, \dots, f_n$ 인  $n \times n$  행렬이고,  $(FA^{-1})_1$ 은  $FA^{-1}$ 의 첫 번째 열을 나타냅니다.

물론 마찬가지로  $B$ 가 가역  $m \times m$  행렬일 때  $T$ 를  $TB$ 로 바꿀 수 있습니다; 이는 다음에 대응됩니다

$$(e_1, \dots, e_m) \mapsto ((EB)_1, \dots, (EB)_m)$$

여기서  $E$ 는 열이  $e_1, \dots, e_m$ 인  $m \times m$  행렬입니다.

이 지식으로 무장하여, 이제 다음을 다룰 수 있습니다:

### 정리 18.6.1 (스미스 표준형)

$R$ 을 PID라 합시다.  $M = R^{\oplus m}$ 과  $N = R^{\oplus n}$ 을 자유  $R$ -가군이라 하고  $T: M \rightarrow N$ 을 선형 사상이라 합시다.  $k = \min\{m, n\}$ 으로 놓습니다.

그러면  $M$ 과  $N$ 에 대해 새로운 기저 쌍을 선택하여  $T$ 가 대각 성분  $s_1, s_2, \dots, s_k$ 만 가지며  $s_1 \mid s_2 \mid \dots \mid s_k$ 가 되도록 할 수 있습니다.

따라서  $m > n$ 이면, 행렬은 다음 형태를 취해야 합니다

$$\begin{bmatrix} s_1 & 0 & 0 & 0 & \dots & 0 \\ 0 & s_2 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \dots & \vdots \\ 0 & 0 & 0 & s_n & \dots & 0 \end{bmatrix}.$$

$m \leq n$ 일 때도 마찬가지입니다.

**질문 18.6.2.** 스미스 표준형이 구조 정리를 함의함을 보이십시오.

**비고 18.6.3** — 이것이 조르당 표준형의 일반화가 아님에 유의하십시오.

- 조르당 표준형에서는 사상  $T: V \rightarrow V$ 를 고려합니다; 정의역과 공역이 같으며, 공간  $V$ 에 대해 하나의 기저를 고려하고 있음에 유의하십시오.
- 스미스 표준형에서는 사상  $T: M \rightarrow N$ 이 서로 다른 가군 사이에 있으며, 두 개의 기저 집합(하나는  $M$ 에 대해, 하나는  $N$ 에 대해)을 선택합니다.

### 예제 18.6.4 (스미스 표준형의 예)

증명 아이디어의 느낌을 전달하기 위해,  $\mathbb{Z}$ -행렬을 사용한 구체적인 예를 함께 살펴봅시다

$$\begin{bmatrix} 18 & 38 & 48 \\ 14 & 30 & 32 \end{bmatrix}.$$

모든 성분의 GCD는 2이며, 이에 착안하여 **왼쪽 열에 대해 유클리드 호제법**을 수행합니다: 첫 번째 행에서 두 번째 행을 빼고, 그다음 두 번째 행에서 첫 번째 행의 세 배를 뺍니다:

$$\begin{bmatrix} 18 & 38 & 48 \\ 14 & 30 & 32 \end{bmatrix} \mapsto \begin{bmatrix} 4 & 8 & 16 \\ 14 & 30 & 32 \end{bmatrix} \mapsto \begin{bmatrix} 4 & 8 & 16 \\ 2 & 6 & -16 \end{bmatrix}.$$

이제 GCD인 2가 나타났으므로, 두 행을 바꾸어 이를 왼쪽 위로 옮긴 다음, 같은 행/열에 있는 모든 성분을 소거합니다; 2가 처음부터 GCD였으므로, 2를 완전히 고립시킬 수 있습니다:

$$\begin{bmatrix} 4 & 8 & 16 \\ 2 & 6 & -16 \end{bmatrix} \mapsto \begin{bmatrix} 2 & 6 & -16 \\ 4 & 8 & 16 \end{bmatrix} \mapsto \begin{bmatrix} 2 & 6 & -16 \\ 0 & -4 & 48 \end{bmatrix} \mapsto \begin{bmatrix} 2 & 0 & 0 \\ 0 & -4 & 48 \end{bmatrix}.$$

이로써 문제는  $1 \times 2$  행렬로 축소됩니다. 그러므로 그곳에도 유클리드 호제법을 다시 적용하기만 하면 됩니다:

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & -4 & 0 \end{bmatrix} \mapsto \begin{bmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \end{bmatrix}.$$

이제 남은 일은 이 증명을 임의의 PID에 대해 작동하도록 일반화하는 것뿐입니다. 이를 어떻게 할지는 직관적으로 명확합니다: PID 조건이 대체로 유클리드 호제법을 수행할 수 있게 해 줍니다.

스미스 표준형의 증명. 일반적인 행렬로 시작합니다

$$T = \begin{bmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nm} \end{bmatrix}$$

우리는 일련의 연산(주어진 기저를 점진적으로 바꾸는 것)을 통해 이 행렬을 스미스 표준형으로 재배열할 수 있음을 보이고자 합니다.

$\gcd(x, y)$ 를 주 아이디얼  $(x, y)$ 의 임의의 생성원으로 정의합니다.

**주장 18.6.5** (“유클리드 호제법”).  $a$ 와  $b$ 가 같은 행 또는 열의 성분이면, 기저를 바꾸어  $a$ 를  $\gcd(a, b)$ 로,  $b$ 를 다른 무언가로 바꿀 수 있습니다.

증명. 열(column)의 경우만 다룹니다. 가정에 의해 어떤  $x, y \in R$ 에 대해  $\gcd(a, b) = xa + yb$ 입니다. 이제 (UFD에 있으므로)  $(x, y) = (1)$ 이어야 합니다. 따라서  $xu + yv = 1$ 을 만족하는  $u$ 와  $v$ 가 존재합니다. 그러면

$$\begin{bmatrix} x & y \\ -v & u \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} \gcd(a, b) \\ \text{무언가} \end{bmatrix}$$

원하는 대로 첫 번째 행렬은 가역입니다 (이를 확인해 보십시오!). ■

$s_1 = (a_{ij})_{i,j}$ 를 모든 성분의 GCD라 합시다. 이제 이 알고리즘을 반복 적용하여  $s_1$ 이 좌상단에 나타나도록 만들 수 있습니다. 그런 다음 이를 이용해 첫 번째 행과 첫 번째 열의 모든 성분을 소거하여 다음과 같은 행렬에 이릅니다

$$\begin{bmatrix} s_1 & 0 & 0 & \cdots & 0 \\ 0 & a'_{22} & a'_{23} & \cdots & a'_{2n} \\ 0 & a'_{32} & a'_{33} & \cdots & a'_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a'_{m2} & a'_{m3} & \cdots & a'_{mn} \end{bmatrix}.$$

이제 이 우하단  $(m-1) \times (n-1)$  행렬에 대해 같은 절차를 반복하고, 이를 계속 진행합니다. 이로써 스미스 표준형(Smith normal form)을 얻습니다.  $\square$

스미스 표준형을 이용하면 원래 상황에서 다음이 성립합니다

$$M \cong R^{\oplus d} / \text{im } T$$

그리고  $T$ 에 정리를 적용하면 구조 정리의 증명이 완성됩니다.

## §18.7 생각해 볼 만한 조금 더 어려운 문제

이제 우리는 구조 정리를 적용할 수 있습니다!

**문제 18A<sup>†</sup>** (유한 차원 벡터 공간은 모두 동형이다). 체  $k$  위의 벡터 공간  $V$ 가 유한 생성 집합을 가진다고 합시다. 어떤  $n$ 에 대해  $V \cong k^{\oplus n}$ 임을 보이십시오.

**문제 18B<sup>†</sup>** (프로베니우스 표준형).  $T: V \rightarrow V$ 가 있고,  $V$ 는 임의의 체  $k$  (반드시 대수적으로 닫혀 있을 필요는 없음) 위의 유한 차원 벡터 공간이라 합시다.  $T$ 를 다음 형태의 블록들로 이루어진 블록 대각 행렬로 쓸 수 있음을 보이십시오

$$\begin{bmatrix} 0 & 0 & 0 & \dots & 0 & * \\ 1 & 0 & 0 & \dots & 0 & * \\ 0 & 1 & 0 & \dots & 0 & * \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & * \end{bmatrix}.$$

( $V$ 를 작용  $x \cdot v = T(v)$ 를 갖는  $k[x]$ -가군으로 간주하십시오.)

**문제 18C<sup>†</sup>** (조르당 표준형).  $T: V \rightarrow V$ 가 있고,  $V$ 는 대수적으로 닫힌 임의의 체  $k$  위의 유한 차원 벡터 공간이라 합시다.  $T$ 가 조르당 형태로 쓰일 수 있음을 증명하십시오.



**문제 18D.** 서로 동형이 아니지만 단사 준동형사상  $G \hookrightarrow H$ 와  $H \hookrightarrow G$ 가 존재하는 두 아벨 군  $G$ 와  $H$ 를 찾으십시오.



**문제 18E.**  $A \subseteq B \subseteq C$ 가 환이라고 합시다.  $C$ 가 유한 생성  $A$ -가군이라고 가정합니다. 그렇다면  $B$ 도 유한 생성  $A$ -가군이라는 결론이 따라 나오니까?

# VI

## 표현론

## 제VI부: 목차

---

|           |                             |            |
|-----------|-----------------------------|------------|
| <b>19</b> | <b>대수의 표현</b>               | <b>237</b> |
| 19.1      | 대수                          | 237        |
| 19.2      | 표현                          | 238        |
| 19.3      | 직합                          | 240        |
| 19.4      | 기약 표현과 분해불가능 표현             | 242        |
| 19.5      | 표현의 사상                      | 243        |
| 19.6      | $\text{Mat}_d(k)$ 의 표현들     | 245        |
| 19.7      | 생각해 볼 만한 조금 더 어려운 문제        | 246        |
| <b>20</b> | <b>반단순 대수</b>               | <b>249</b> |
| 20.1      | 슈어의 보조정리 (계속)               | 249        |
| 20.2      | 조밀성 정리                      | 251        |
| 20.3      | 반단순 대수                      | 253        |
| 20.4      | 마슈케 정리                      | 254        |
| 20.5      | 예시: $\mathbb{C}[S_3]$ 의 표현들 | 255        |
| 20.6      | 생각해 볼 만한 조금 더 어려운 문제        | 256        |
| <b>21</b> | <b>지표</b>                   | <b>257</b> |
| 21.1      | 정의                          | 257        |
| 21.2      | 교환자로 나눈 쌍대 공간               | 258        |
| 21.3      | 지표의 직교성                     | 259        |
| 21.4      | 지표표의 예                      | 261        |
| 21.5      | 생각해 볼 만한 조금 더 어려운 문제        | 262        |
| <b>22</b> | <b>몇 가지 응용</b>              | <b>265</b> |
| 22.1      | 프로베니우스 나눗셈성                 | 265        |
| 22.2      | 번사이드의 정리                    | 266        |
| 22.3      | 프로베니우스 행렬식                  | 267        |

---

# 19 대수의 표현

19세기에는 아직 “군”이라는 단어가 발명되지 않았으며, 모든 연구는  $GL(n)$  또는  $S_n$ 의 부분집합을 대상으로 이루어졌습니다. 훨씬 나중에서야 군의 추상적 정의, 즉 그 자체로 하나의 대상인 추상 집합  $G$ 가 주어졌습니다.

이러한 추상화는 여러 이유로 유용하지만, 구체적인 표현을 다루는 것 또한 종종 유용합니다. 이것이 표현론의 주제입니다. 선형대수학은 추상대수학보다 다루기 쉬우므로, 만약 군  $G$ 를 가져와  $GL(n)$  내의 행렬 집합으로 구체적으로 표현할 수 있다면, 이는 그것들을 연구하기 더 쉽게 만들어 줍니다. 이것이 바로 군의 표현론입니다: 어떻게 군을 가져와 그 원소들을 행렬로 표현할 수 있을까요?

## §19.1 대수

이 절의 대표적인 예:  $k[x_1, \dots, x_n]$ 과  $k[G]$ .

처음부터 군을 직접 다루기보다는, 이른바  $k$ -대수를 다루는 것이 더 편리할 것입니다. 이 설정은 군의 경우보다 더 자연스럽고 일반적이므로, 일단 대수의 이론을 충분히 잘 전개해 두면 군의 경우로 특수화하는 것은 상당히 수월할 것입니다.

구어적으로 말하면,

결합적  $k$ -대수란 그 내부에  $k$ 의 복사본을 지니는, 가환적이지 않을 수도 있는 환입니다. 따라서 이는  $k$ -벡터 공간입니다.

정의를 제시하기에 앞서 예시들을 먼저 보이겠습니다:

### 예제 19.1.1 ( $k$ -대수의 예시들)

$k$ 를 임의의 체라 하겠습니다. 다음은  $k$ -대수의 예시들입니다:

- (a) 체  $k$  그 자체.
- (b) 다항식환  $k[x_1, \dots, x_n]$ .
- (c)  $k$ 의 원소들을 성분으로 갖는  $n \times n$  행렬들의 집합으로, 이를  $\text{Mat}_n(k)$ 로 표기합니다. 여기서의 곱셈은 가환적이지 않음에 유의하십시오.
- (d) 선형 사상  $T: V \rightarrow V$ 들의 집합  $\text{Mat}(V)$ 로, 곱셈은 연산자의 합성으로 주어집니다. (여기서  $V$ 는  $k$  위의 어떤 벡터 공간입니다.) 이는 사실상 앞선 예시와 동일합니다.

**정의 19.1.2.**  $k$ 를 체라 하겠습니다.  $k$ -대수  $A$ 란 환 준동형사상  $k \hookrightarrow A$ 가 갖추어진, 가환적이지 않을 수도 있는 환으로서, 그 상이 바로 “ $k$ 의 복사본”입니다. (특히  $1_k \mapsto 1_A$ 입니다.)

따라서  $k$ 를  $A$ 의 부분집합으로 간주할 수 있으며, 이때 추가로 각  $\lambda \in k$ 와  $a \in A$ 에 대해  $\lambda \cdot a = a \cdot \lambda$ 일 것을 요구합니다.

곱셈 연산 또한 가환적이라면,  $A$ 를 **가환 대수**라고 합니다.

**정의 19.1.3.** 동치인 정의로,  $k$ -대수  $A$ 란 결합적이고 쌍선형인 곱셈 연산(항등원  $1_A$ 를 가짐)을 아울러 갖춘  $k$ -벡터 공간입니다. “ $k$ 의 복사본”은 각  $\lambda \in k$ 에 대해 원소  $\lambda 1_A$ 를 고려함으로써 얻어집니다 (즉, 벡터 공간 구조를 이용하여  $k$ 의 원소들로 항등원을 스칼라배함으로써 얻어집니다).

**표기의 남용 19.1.4.** 다른 저자들 중에는  $A$ 가 결합적이거나 항등원을 가질 것을 요구하지 않는 경우도 있는데, 그들에게는 우리가 방금 정의한 것이 “항등원 1을 갖는 결합 대수”에 해당합니다. 그러나 이는 우리의 목적에 있어 불필요하게 장황합니다.

### 예제 19.1.5 (군 대수)

**군 대수**  $k[G]$ 란 군  $G$ 의 원소들을 기저 원소로 갖는  $k$ -벡터 공간으로서, 두 기저 원소의 곱은 군의 곱셈으로 주어집니다. 예를 들어,  $G = \mathbb{Z}/2\mathbb{Z} = \{1_G, x\}$ 라 하겠습니다. 그러면

$$k[G] = \{a1_G + bx \mid a, b \in k\}$$

곱셈은 다음과 같이 주어집니다

$$(a1_G + bx)(c1_G + dx) = (ac + bd)1_G + (bc + ad)x.$$

### 질문 19.1.6. $k[G]$ 는 언제 가환적일까요?

$k[G]$ 라는 예시는 매우 중요한데, (곧 살펴보게 되겠지만) 대수  $k[G]$ 의 표현은 군  $G$  자체의 표현에 대응하기 때문입니다.

이 시점에서 다음을 언급할 가치가 있습니다:

**정의 19.1.7.**  $k$ -대수  $A, B$ 의 **준동형사상**은 곱셈을 보존하며(즉,  $T(xy) = T(x)T(y)$ )  $1_A$ 를  $1_B$ 로 보내는 선형 사상  $T: A \rightarrow B$ 입니다. 다시 말해,  $T$ 는 환으로서의 준동형사상이면서 동시에 벡터 공간으로서의 준동형사상입니다.

**예제 4.3.8**에서 나온 “곱환”도 다시 떠올려야 하겠지만, 대수의 경우에는 다른 이름과 표기법을 사용하겠습니다.

**정의 19.1.8.**  $k$ -대수  $A$ 와  $B$ 가 주어졌을 때, **직합**  $A \oplus B$ 는  $a + b$  꼴의 쌍으로 정의되며, 덧셈은 자명한 방식으로 이루어지지만 임의의  $a \in A$ 와  $b \in B$ 에 대해  $ab = 0$ 으로 선언합니다.

### 질문 19.1.9. $1_A + 1_B$ 가 $A \oplus B$ 의 곱셈 항등원임을 보이십시오.

동등하게, **정의 9.3.1**과 **예제 4.3.8**과 유사하게, 직합  $A \oplus B$ 를 순서쌍  $(a, b)$ 들의 집합으로 정의할 수도 있으며, 이때 곱셈은  $(a, b)(a', b') = (aa', bb')$ 로 정의됩니다. 이 표기법에서는  $(1_A, 1_B)$ 가  $A \oplus B$ 의 곱셈 항등원이 됩니다.

## §19.2 표현

**이 절의 대표적인 예:**  $k^{\oplus 3}$ 에 작용하는  $k[S_3]$ 가 제가 가장 좋아하는 예입니다.

**정의 19.2.1.**  $k$ -대수  $A$ 의 **표현**(**왼쪽  $A$ -가군**이라고도 함)이란 다음과 같습니다:

- (i)  $k$ -벡터 공간  $V$ , 그리고
- (ii)  $A$ 가  $V$ 에 작용하는 작용  $\cdot$ : 즉, 모든  $a \in A$ 에 대해  $v \in V$ 를 취하여 작용시켜  $a \cdot v$ 를 얻을 수 있습니다. 이는 다음과 같은 통상적인 공리들을 만족합니다:
  - $(a + b) \cdot v = a \cdot v + b \cdot v$ ,  $a \cdot (v + w) = a \cdot v + a \cdot w$ , 그리고  $(ab) \cdot v = a \cdot (b \cdot v)$ .
  - $\lambda \in k$ 에 대해  $\lambda \cdot v = \lambda v$ . 특히,  $1_A \cdot v = v$ 입니다.

**정의 19.2.2.**  $A$ 의 작용은  $k$ -대수 준동형사상  $\rho: A \rightarrow \text{Mat}(V)$ 가 존재한다는 말로 더 간결하게 서술할 수 있습니다. (즉  $a \cdot v = \rho(a)(v)$ .) 따라서  $A$ 의 **표현**을 다음과 같은 쌍으로도 정의할 수 있습니다

$$(V, \rho: A \rightarrow \text{Mat}(V)).$$

이는  $n$ 개의 원소를 가진 집합  $X$ 에 대한 군  $G$ 의 작용이 단지 군 준동형사상  $G \rightarrow S_n$ 에 지나지 않는 것과 완전히 유사합니다. 이러한 관점에서 볼 때, 우리가 실제로 하려는 것은 다음과 같습니다:

**$A$ 가 대수라면, 우리는  $A$ 의 원소들을 행렬로 표현하려는 것입니다.**

**표기의 남용 19.2.3.** 표현이란 벡터 공간  $V$ 와 작용  $\rho$  둘 다로 이루어진 쌍  $(V, \rho)$ 이지만, 우리는 종종 이를 그냥 " $V$ "로 줄여 부르겠습니다. 이는 아마 제가 저지를 최악의 남용 중 하나일 테지만, 다른 모든 사람들도 그렇게 하기에 저는 대중의 반발이 두렵습니다.

**표기의 남용 19.2.4.**  $\rho(a)(v)$  대신 그냥  $\rho(a)v$ 라고 쓰겠습니다.

### 예제 19.2.5 ( $\text{Mat}(V)$ 의 표현)

- (a)  $A = \text{Mat}_2(\mathbb{R})$ 라 합시다. 그러면 행렬  $a \in A$ 가 그저  $a \cdot v = \rho(a)(v) = a(v)$ 로 작용하는 표현  $(\mathbb{R}^{\oplus 2}, \rho)$ 가 존재합니다.
- (b) 더 일반적으로, 임의의 체  $k$  위의 벡터 공간  $V$ 가 주어졌을 때,  $a \cdot v = \rho(a)(v) = a(v)$  (여기서  $a \in \text{Mat}(V)$ )로 정의되는  $A = \text{Mat}(V)$ 의 자명한 표현이 존재합니다.  
행렬의 관점에서 보면:  $A = \text{Mat}(V)$ 라면,  $A$ 를 그저  $V$  위의 행렬로 표현할 수 있습니다.
- (c)  $A = \text{Mat}_2(\mathbb{R})$ 의 다른 표현들도 있습니다. 우스운 예시로는 다음과 같이 주어지는 표현  $(\mathbb{R}^{\oplus 4}, \rho)$ 가 있습니다

$$\rho: \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{bmatrix}.$$

더 추상적으로,  $\mathbb{R}^{\oplus 4}$ 를  $(\mathbb{R}^{\oplus 2}) \oplus (\mathbb{R}^{\oplus 2})$ 로 보면, 이는  $a \cdot (v_1, v_2) = (a \cdot v_1, a \cdot v_2)$ 입니다.

### 예제 19.2.6 (다항식 대수의 표현)

- (a)  $A = k$ 라고 합시다. 그러면  $k$ 의 표현은 그저 임의의  $k$ -벡터 공간  $V$ 입니다.
- (b)  $A = k[x]$ 라면,  $A$ 의 표현  $(V, \rho)$ 는 벡터 공간  $V$ 에 더해 선형 사상  $T \in \text{Mat}(V)$ 의 선택(즉  $T = \rho(x)$ )에 해당합니다.
- (c)  $A = k[x]/(x^2)$ 라면  $A$ 의 표현  $(V, \rho)$ 는 벡터 공간  $V$ 에 더해  $T^2 = 0$ 을 만족하는 선형 사상  $T \in \text{Mat}(V)$ 의 선택에 해당합니다.
- (d) 이러한 패턴으로 임의의 "함수 방정식"을 만들어낼 수 있습니다. 예를 들어  $A = k[x, y]/(x^2 - x + y, y^4)$ 라면  $V$ 로  $A$ 를 표현하는 것은  $S^2 = S - T$ 와  $T^4 = 0$ 을 만족하는 가환 연산자  $S, T \in \text{Mat}(V)$ 를 찾는 것에 해당합니다.

**예제 19.2.7 (군의 표현)**

(a)  $A = \mathbb{R}[S_3]$ 라고 합시다. 그러면

$$V = \mathbb{R}^{\oplus 3} = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}.$$

다음과 같이  $A$ 가  $V$ 에 작용하게 할 수 있습니다: 순열  $\pi \in S_3$ 이 주어지면,  $V$ 에서 대응하는 좌표를 치환합니다. 예를 들어

$$\text{만약 } \pi = (1\ 2) \text{ 그러면 } \pi \cdot (x, y, z) = (y, x, z).$$

이는 좌표를 치환함으로써 선형적으로 확장되어  $A$ 가  $V$ 에 작용하게 합니다.

행렬의 관점에서 보면, 우리가 하고 있는 것은  $S_3$ 의 순열들을  $k^{\oplus 3}$  위의 치환 행렬로 표현하는 것이며, 예를 들면

$$(1\ 2) \mapsto \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

(b) 더 일반적으로,  $A = k[G]$ 라고 합시다. 그러면  $A$ 의 표현  $(V, \rho)$ 는 군 준동형사상  $\psi: G \rightarrow \text{GL}(V)$ 에 해당합니다. (특히  $\rho(1_G) = \text{id}_V$ 입니다.) 이를  $G$ 의 **군 표현**이라 부릅니다.

**예제 19.2.8 (정칙 표현)**

임의의  $k$ -대수  $A$ 는 그 자신에 대한 표현  $(A, \rho)$ 이며,  $a \cdot b = \rho(a)(b) = ab$ 입니다(즉, 곱셈은  $A$ 에 의해 주어집니다). 이를 **정칙 표현**이라 부르며,  $\text{Reg}(A)$ 로 표기합니다.

**§19.3 직합**

**이 절의 대표적인 예:**  $\mathbb{R}[S_3]$ 를 사용한 예가 가장 좋아 보입니다.

**정의 19.3.1.**  $A$ 를  $k$ -대수라 하고,  $V = (V, \rho_V)$ 와  $W = (W, \rho_W)$ 를  $A$ 의 두 표현이라고 합시다. 그러면  $V \oplus W$ 는 표현이며, 그 작용  $\rho$ 는 다음과 같이 주어집니다

$$a \cdot (v, w) = (a \cdot v, a \cdot w).$$

이 표현을  $V$ 와  $W$ 의 **직합**이라 부릅니다.

**예제 19.3.2**

앞서 우리는  $\text{Mat}_2(\mathbb{R})$ 가  $\mathbb{R}^{\oplus 4}$ 에 다음과 같이 작용하게 했습니다

$$\rho: \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{bmatrix}.$$

이는 단지 두 개의 2차원 표현의 직합일 뿐입니다.

$\mathbb{R}^{\oplus 4}$ 의 벡터를  $\begin{pmatrix} e & f \\ g & h \end{pmatrix}$ 와 같이 “수평으로 쌓인”  $\mathbb{R}^{\oplus 2}$ 의 두 벡터로 볼 수도 있으므로,

작용은 다음과 같이 주어집니다

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix}.$$

**비고 19.3.3** — 이것이 아마 사람들이  $\rho_V$ 를 함께 표기하지 않고  $V$ 만을 표현으로 쓰는 경향이 있는 이유일 것인데,  $k$ -대수  $A$ 를  $\text{Mat}_d(k)$ 의 부분대수에 매장하는 것이 가능하기만 하다면,  $V$ 는 자명한  $k^{\oplus d}$  표현을 수평으로  $m$ 개 쌓은  $(k^{\oplus d})^{\oplus m}$ 의 부분표현으로 동형적으로 매장될 수 있기 때문입니다.

더 일반적으로, 표현  $(V, \rho_V)$ 와  $(W, \rho_W)$ 가 주어지면  $V \oplus W$ 의 표현  $\rho$ 는 다음과 같은 모습입니다

$$\rho(a) = \begin{bmatrix} \rho_V(a) & 0 \\ 0 & \rho_W(a) \end{bmatrix}.$$

**예제 19.3.4** ( $S_n$ 의 표현이 분해됨)

$A = \mathbb{R}[S_3]$ 이 다시 좌표의 치환을 통해 다음에 작용한다고 합시다

$$V = \mathbb{R}^{\oplus 3} = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}.$$

두 부분공간을 생각해봅시다.

$$W_1 = \{(t, t, t) \mid t \in \mathbb{R}\}$$

$$W_2 = \{(x, y, z) \mid x + y + z = 0\}.$$

$V = W_1 \oplus W_2$ 가 벡터 공간으로서 성립함에 유의하십시오. 그러나  $W_1$ 과  $W_2$  각각은 부분표현입니다 ( $A$ 의 작용이 각  $W_i$ 를 그대로 보존하기 때문입니다). 따라서  $V = W_1 \oplus W_2$ 는 표현으로서도 성립합니다.

직합은 대수를 다룰 때도 등장합니다.

**명제 19.3.5** ( $A \oplus B$ 의 표현은  $V_A \oplus V_B$ 입니다)

$A$ 와  $B$ 를  $k$ -대수라 합시다. 그러면  $A \oplus B$ 의 모든 표현은 다음 형태입니다

$$V_A \oplus V_B$$

여기서  $V_A$ 와  $V_B$ 는 각각  $A$ 와  $B$ 의 표현입니다.

**예제 19.3.6**

$A = B = \text{Mat}_2(\mathbb{R})$ 라고 합시다.  $k$ -대수  $A \oplus B$ 의 자명한 표현으로  $V_A$ 와  $V_B$  두 가지가 있으며, 이는 각각  $A$ 와  $B$ 의 작용에 대응합니다.

$V_A$ 와  $V_B$  각각은  $\mathbb{R}$ -벡터 공간으로서  $\mathbb{R}^{\oplus 2}$ 와 동형입니다.

이 명제가 말하는 바는,  $a \in A$ 와  $b \in B$ 에 대해  $(a + b) \cdot v = a \cdot v + 2b \cdot v$ 와 같은 방식으로  $A$ 와  $B$ 의 작용을 "섞어서"  $A \oplus B$ 의 어떤 표현  $V \cong \mathbb{R}^2$ 를 얻을 수는 없다는 것입니다.

증명의 개요.  $(V, \rho)$ 를  $A \oplus B$ 의 표현이라고 합시다. 임의의  $v \in V$ 에 대해  $\rho(1_A + 1_B)v = \rho(1_A)v + \rho(1_B)v$ 입니다. 그러면  $V_A = \{\rho(1_A)v \mid v \in V\}$ 와  $V_B = \{\rho(1_B)v \mid v \in V\}$ 로 놓을 수 있습니다. 이들은 서로소인데, 만약  $\rho(1_A)v = \rho(1_B)v'$ 이라면  $\rho(1_A)v = \rho(1_A 1_A)v = \rho(1_A 1_B)v' = 0_V$ 이 되며, 반대쪽도 마찬가지이기 때문입니다.  $\square$

위의 예시에서, 표현  $V_A \oplus V_B$ 를  $\mathbb{R}^4$ 로 본다면,  $A$ 의 원소가  $V_A \oplus V_B$ 의 원소에 작용할 때 벡터의  $V_B$ -성분을 0으로 만들게 됩니다.

그러므로 증명의 핵심 아이디어는 다음과 같습니다.

$A \oplus B$ 의  $A$  성분과  $B$  성분을 이용하여  $V$ 에 작용시킴으로써, 벡터 공간  $V$ 를 성분  $V_A$ 와  $V_B$ 로 사영하여 부분표현들을 분리해냅니다.

## §19.4 기약 표현과 분해불가능 표현

**이 절의 대표적인 예:**  $k[S_3]$ 는 두 공간의 합으로 분해됩니다.

표현론의 목표 중 하나는 대수  $A$ 의 가능한 모든 표현을 분류하는 것입니다. 이를 해낼 가능성을 가지려면, 다음과 같은 "사소한" 표현들은 버려두고자 합니다

$$\rho: \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{bmatrix}$$

대신 "기약" 표현에 주의를 집중하고자 합니다. 이것이 다음의 동기가 됩니다.

**정의 19.4.1.**  $V$ 를  $A$ 의 표현이라고 합시다. **부분표현**  $W \subseteq V$ 는 임의의  $a \in A$ 와  $w \in W$ 에 대해  $a \cdot w \in W$ 라는 성질을 가지는 부분공간  $W$ 입니다. 다시 말해, 이 부분공간은  $A$ 의 작용 아래 불변입니다.

따라서 예를 들어 표현  $W_1, W_2$ 에 대해  $V = W_1 \oplus W_2$ 이면  $W_1$ 과  $W_2$ 는  $V$ 의 부분표현입니다.

**정의 19.4.2.**  $V$ 가 진부분표현이면서 0이 아닌 부분표현을 가지지 않으면  $V$ 는 **기약**입니다.  $V = W_1 \oplus W_2$ 를 만족하는 진부분표현  $W_1, W_2$ 의 쌍이 존재하지 않으면,  $V$ 를 **분해불가능**이라고 합니다.

**정의 19.4.3.** 간결함을 위해, 대수/군의 **기약표현**이란 기약 표현을 뜻합니다. ( $A$ 가 유한 차원일 때, 모든 기약표현은 자동으로 차원이  $\dim A$  이하가 됩니다. 이 교재에서는  $\dim A$ 가 반드시 유한이지 않은 경우에도 무한 차원 기약표현은 전혀 다루지 않습니다.)

### 예제 19.4.4 ( $S_n$ 의 표현이 분해됨)

다시  $A = \mathbb{R}[S_3]$ 로 놓고, 다음에 좌표의 치환을 통해 작용한다고 합시다

$$V = \mathbb{R}^{\oplus 3} = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}.$$

다시 두 부분공간을 생각해봅시다

$$W_1 = \{(t, t, t) \mid t \in \mathbb{R}\}$$

$$W_2 = \{(x, y, z) \mid x + y + z = 0\}.$$

우리가 살펴보았듯이  $V = W_1 \oplus W_2$ 이고, 따라서  $V$ 는 기약이 아닙니다. 하지만 다음과 같이  $W_1$ 과  $W_2$ 가 기약(따라서 분해 불가능)임을 보일 수 있습니다.

- $W_1$ 에 대해서는  $W_1$ 이 일차원이므로 자명합니다.
- $W_2$ 에 대해서는,  $a+b+c=0$ 이고 모두 영이 아닌 임의의 벡터  $w=(a,b,c)$ 를 생각합니다. 그러면 일반성을 잃지 않고  $a \neq b$ 라고 가정할 수 있습니다(세 좌표가 모두 같지는 않으므로). 이 경우 (1 2)는  $w$ 를  $w'=(b,a,c)$ 로 보냅니다. 그러면  $w$ 와  $w'$ 는  $W_2$ 를 생성합니다.

따라서  $V$ 는 기약표현들로 완전히 분해됩니다.

안타깝게도  $W$ 가  $V$ 의 부분표현이라 하더라도,  $V=W \oplus W'$ 가 되는 보충 벡터 공간  $W'$ 를 반드시 찾을 수 있는 것은 아닙니다. 다시 말해,  $V$ 가 가약이면  $V$ 가 부분표현을 가짐은 알 수 있지만, 분해를 위해서는 두 개의 부분표현이 필요합니다. 다음은 표준적인 반례입니다.

**연습문제 19.4.5.**  $A = \mathbb{R}[x]$ 라 하고,  $V = \mathbb{R}^{\oplus 2}$ 를 다음 작용을 갖는 표현이라고 합시다.

$$\rho(x) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

유일한 부분표현이  $W = \{(t, 0) \mid t \in \mathbb{R}\}$ 임을 보이십시오. 따라서  $V$ 는 기약이 아니지만 분해 불가능합니다.

다음은 조금 더 낙관적인 예시이자, 여러분이 염두에 두어야 할 "전형적인 예시"입니다.

**연습문제 19.4.6.**  $A = \text{Mat}_d(k)$ 라 하고, 앞서 서술한  $A$ 의 자명한 표현  $k^{\oplus d}$ 를 생각합니다. 이것이 기약임을 보이십시오. (정의를 충분히 잘 이해하고 있다면 이는 자명합니다.)

## §19.5 표현의 사상

이제 표현들 사이의 사상을 정의하겠습니다.

**정의 19.5.1.**  $(V, \rho_V)$ 와  $(W, \rho_W)$ 를  $A$ 의 표현이라고 합시다. **교환 연산자**(intertwining operator), 또는 **사상**(morphism)은 다음을 만족하는 선형 사상  $T: V \rightarrow W$ 입니다.

$$T(a \cdot v) = a \cdot T(v)$$

임의의  $a \in A$ ,  $v \in V$ 에 대하여. (첫 번째  $\cdot$ 은  $\rho_V$ 의 작용이고, 두 번째  $\cdot$ 은  $\rho_W$ 의 작용임에 유의하십시오.)  $V$ 와  $W$ 를 "왼쪽  $A$ -가군"이라고 생각한다면 이는 정확히 예상하는 바입니다.  $T$ 가 가역이면 이는 표현의 **동형사상**(isomorphism)이며, 이때  $V \cong W$ 라고 말합니다.

**비고 19.5.2** (가환 도식을 좋아하는 사람들을 위해) — 조건  $T(a \cdot v) = a \cdot T(v)$ 는 다음을 나타낸다고 읽을 수 있습니다.

$$\begin{array}{ccc} V & \xrightarrow{\rho_1(a)} & V \\ T \downarrow & & \downarrow T \\ W & \xrightarrow{\rho_2(a)} & W \end{array}$$

임의의  $a \in A$ 에 대해 가환합니다.

**비고 19.5.3 (범주를 좋아하는 사람들을 위해)** — 표현이란 그저 아벨 단일 대상 범주  $\{*\}$ (따라서  $\text{Hom}(*, *) \cong A$ )로부터 아벨 범주  $\text{Vect}_k$ 로 가는 "쌍선형" 함자일 뿐입니다. 그러면 교환 연산자는 그저 자연 변환일 뿐입니다.

다음은 교환 연산자의 몇 가지 예시입니다.

**예제 19.5.4 (교환 연산자)**

- (a) 임의의  $\lambda \in k$ 에 대해, 스칼라 사상  $T(v) = \lambda v$ 는 교환 연산자입니다.
- (b)  $W \subseteq V$ 가 부분표현이면, 포함 사상  $W \hookrightarrow V$ 는 교환 연산자입니다.
- (c) 사영 사상  $V_1 \oplus V_2 \rightarrow V_1$ 은 교환 연산자입니다.
- (d)  $V = \mathbb{R}^2$ 라 하고,  $A = \mathbb{R}[x]$ 를  $(V, \rho)$ 로 표현하되 다음과 같이 합시다.

$$\rho(x) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

따라서  $\rho(x)$ 는 원점을 중심으로  $90^\circ$  회전입니다.  $T$ 를  $30^\circ$  회전이라고 합시다. 그러면  $T: V \rightarrow V$ 는 교환 연산자입니다(회전들은 교환됩니다).

**예제 19.5.5 (반례:  $\text{Mat}(V)$ 의 표현)**

$A = \text{Mat}_2(\mathbb{R}) \oplus \text{Mat}_2(\mathbb{R})$ 라 합시다. 그러면  $A$ 는 다음과 같은 형태의 행렬들로 이루어진  $\text{Mat}_4(\mathbb{R})$ 의 부분집합으로 볼 수 있습니다

$$\begin{bmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & e & f \\ 0 & 0 & g & h \end{bmatrix}.$$

$A$ 의 자명한 기약표현이 두 가지 있는데,  $(m, n, 0, 0)$  형태의  $\mathbb{R}^4$ 의 벡터들로 이루어진  $V_1$ 과  $(0, 0, p, q)$  형태의  $\mathbb{R}^4$ 의 벡터들로 이루어진  $V_2$ 로 주어집니다.

이 경우,  $V_1$ 과  $V_2$ 가  $\mathbb{R}$ -벡터 공간으로서는 동형사상이지만  $A$ 의 표현으로서는 동형사상이 아닙니다 – 따라서  $V_1$ 에서  $V_2$ 로 가는 얹힘 연산자는 반드시 항등적으로 영이어야 합니다.

**연습문제 19.5.6** (핵과 상은 부분표현입니다).  $T: V \rightarrow W$ 를 얹힘 연산자라 합시다.

- (a)  $\ker T \subseteq V$ 가  $V$ 의 부분표현임을 보이십시오.
- (b)  $\text{im } T \subseteq W$ 가  $W$ 의 부분표현임을 보이십시오.

앞의 연습문제로부터 유명한 슈어의 보조정리를 얻습니다.

**정리 19.5.7 (슈어의 보조정리)**

$V$ 와  $W$ 를  $k$ -대수  $A$ 의 표현이라 합시다.  $T: V \rightarrow W$ 를 영이 아닌 엷힘 연산자라 합시다. 그러면

(a)  $V$ 가 기약이면,  $T$ 는 단사입니다.

(b)  $W$ 가 기약이면,  $T$ 는 전사입니다.

특히  $V$ 와  $W$ 가 모두 기약이면  $T$ 는 동형사상입니다.

중요한 특수한 경우로,  $k$ 가 대수적으로 닫혀 있고 유한차원인 경우가 있는데, 이때는 엷힘 연산자  $T: V \rightarrow V$ 가 오직 상수배뿐입니다.

**정리 19.5.8 (대수적으로 닫힌 체에 대한 슈어의 보조정리)**

$k$ 를 대수적으로 닫힌 체라 합시다.  $V$ 를  $k$ -대수  $A$ 의 유한차원 기약표현이라 합시다. 그러면 임의의 엷힘 연산자  $T: V \rightarrow V$ 는 스칼라배입니다.

**연습문제 19.5.9.**  $T$ 가 고윳값  $\lambda$ 를 가진다는 사실을 이용하여 이를 슈어의 보조정리로부터 유도하십시오. ( $T - \lambda \cdot \text{id}_V$ 를 고려하고, 슈어의 보조정리를 이용해 이것이 영임을 유도하십시오.)

$k = \mathbb{R}$ 에 대해  $90^\circ$  회전이라는 반례를 이미 살펴본 바 있는데, 이는 모든 선형 사상이 고윳값을 가진다는 주장에 대해 제시했던 것과 같은 반례였습니다.

**§19.6  $\text{Mat}_d(k)$ 의 표현들**

이미 가능한 진전의 종류를 예로 보이기 위해, 다음을 증명합니다:

**정리 19.6.1 ( $\text{Mat}_d(k)$ 의 표현들)**

$k$ 를 임의의 체,  $d$ 를 양의 정수라 하고  $W = k^{\oplus d}$ 를  $A = \text{Mat}_d(k)$ 의 자명한 표현이라 합시다. 그러면  $\text{Mat}_d(k)$ 의 유한차원 표현은 (동형사상의 관점에서) 어떤 양의 정수  $n$ 에 대한  $W^{\oplus n}$ 뿐입니다. 특히, 이는  $n = 1$ 일 때에만 기약입니다.

구체성을 위해  $d = 2$ 인 경우만 스케치하겠는데, 동일한 증명이 다른 경우에도 그대로 적용되기 때문입니다. 이는 앞서 제시한  $\text{Mat}_2(\mathbb{R})$ 의 표현의 예들이 그것들뿐임을 보여줍니다.

이미 말했듯이 이는 본질적으로 함수 방정식입니다. 대수  $A = \text{Mat}_2(k)$ 는 네 개의 행렬로 주어지는 기저를 가지고 있습니다

$$E_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad E_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad E_3 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad E_4 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

$E_1 + E_2 = \text{id}_A$ ,  $E_1^2 = E_1$ ,  $E_2^2 = 0$ ,  $E_1 E_2 = 0$  등과 같은 관계식을 만족합니다. 이제  $V$ 를  $A$ 의 표현이라 하고, 각  $i$ 에 대해  $M_i = \rho(E_i)$ 라 합시다. 우리는 동일한 함수 방정식을 만족하는  $V$  위의 가능한 행렬  $M_i$ 들을 분류하고자 합니다. 이는 예를 들어 다음과 같기 때문입니다,

$$\text{id}_V = \rho(\text{id}_A) = \rho(E_1 + E_2) = M_1 + M_2.$$

같은 방식으로  $M_1 M_3 = M_3$ 입니다. 비슷한 방식으로 진행하면, 다음과 같은 곱셈표를 얻을 수 있습니다:

$$\begin{array}{c|cccc}
 \times & M_1 & M_2 & M_3 & M_4 \\
 \hline
 M_1 & M_1 & 0 & M_3 & 0 \\
 M_2 & 0 & M_2 & 0 & M_4 \\
 M_3 & 0 & M_3 & 0 & M_1 \\
 M_4 & M_4 & 0 & M_2 & 0
 \end{array}
 \quad \text{그리고} \quad M_1 + M_2 = \text{id}_V$$

각  $M_i$ 는 선형 사상  $V \rightarrow V$ 임에 유의하십시오. 우리가 아는 한, 이것은 수백 개의 성분을 가질 수도 있습니다. 그럼에도 불구하고, 기저  $E_i$ 의 곱셈표가 주어지면  $M_i$ 에 대응하는 표를 얻습니다.

요컨대, 문제는 다음과 같습니다.

**위의 곱셈표를 만족하는 모든 벡터 공간  $V$ 와 행렬의 사원조  $M_i$ 를 찾으십시오.**

$W_1 = M_1^{\text{img}}(V)$ 와  $W_2 = M_2^{\text{img}}(V)$ 를 각각  $M_1$ 과  $M_2$ 의 상이라고 합시다.

**주장 19.6.2.**  $V = W_1 \oplus W_2$ .

증명. 먼저, 임의의  $v \in V$ 에 대해 다음이 성립함에 유의하십시오

$$v = \rho(\text{id})(v) = (M_1 + M_2)v = M_1 v + M_2 v.$$

더욱이  $W_1 \cap W_2 = \{0\}$ 인데, 왜냐하면  $M_1 v_1 = M_2 v_2$ 라면  $M_1 v_1 = M_1(M_1 v_1) = M_1(M_2 v_2) = 0$ 이기 때문입니다.  $\square$

**주장 19.6.3.**  $W_1 \cong W_2$ .

증명. 다음 사상들이

$$W_1 \xrightarrow{\times M_4} W_2 \quad \text{그리고} \quad W_2 \xrightarrow{\times M_3} W_1$$

잘 정의되고 서로 역사상임을 확인하십시오.  $\square$

이제  $e_1, \dots, e_n$ 을  $W_1$ 의 기저 원소라고 합시다. 그러면  $M_4 e_1, \dots, M_4 e_n$ 은  $W_2$ 의 기저 원소입니다. 그런데 각  $\{e_j, M_4 e_j\}$ 는  $W = k^{\oplus 2}$ 와 동형인 부분표현의 기저를 이룹니다(그 동형사상은 무엇입니까?).

이는 결국  $A$ 의 모든 표현이  $W^{\oplus n}$  꼴임을 함의합니다. 특히, 그보다 작은 차원의 표현이 전혀 존재하지 않으므로  $W$ 는 기약입니다!

## §19.7 생각해 볼 만한 조금 더 어려운 문제

**문제 19A<sup>†</sup>.**  $A$ 의 1차원 표현  $V_1 = (V_1, \rho_1)$ 과  $V_2 = (V_2, \rho_2)$ 가 있다고 합시다.  $V_1 \cong V_2$ 인 것과 모든  $a \in A$ 에 대해  $\rho_1(a)$ 와  $\rho_2(a)$ 가 같은 상수에 의한 곱셈인 것이 동치임을 보이십시오.

**문제 19B<sup>†</sup>** (가환대수에 대한 슈어 보조정리).  $A$ 를 대수적으로 닫힌 체  $k$  위의 가환 대수라고 합시다.  $A$ 의 유한 차원 기약 표현은 모두 1차원임을 증명하십시오.

**문제 19C<sup>\*</sup>.**  $(V, \rho)$ 를  $A$ 의 표현이라고 합시다. 그러면  $\text{Mat}(V)$ 는 다음과 같이 주어진 작용을 갖는  $A$ 의 표현입니다

$$a \cdot T = \rho(a) \circ T$$

$T \in \text{Mat}(V)$ 에 대해

- (a)  $\rho: \text{Reg}(A) \rightarrow \text{Mat}(V)$ 가 교환 연산자임을 보이십시오.
- (b)  $V$ 가  $d$ 차원이면,  $A$ 의 표현으로서  $\text{Mat}(V) \cong V^{\oplus d}$ 임을 보이십시오.

**문제 19D\*.** 대수  $A$ 를 고정합시다. 모든 교환 연산자를 찾으십시오

$$T: \text{Reg}(A) \rightarrow \text{Reg}(A).$$



**문제 19E.**  $(V, \rho)$ 를 대수  $A$ 의 분해 불가능한(기약이 아닌) 표현이라고 합시다. 임의의 교환 연산자  $T: V \rightarrow V$ 는  $\rho$ 의 스칼라 곱이거나 동형사상임을 증명하십시오.

(체  $k$ 가 대수적으로 닫혀 있지 않을 수도 있으므로 정리 19.5.8는 적용되지 않음에 유의하십시오.)



# 20 반단순 대수

이어지는 내용에서는 체  $k$ 가 대수적으로 닫혀 있다고 가정합니다.

대수  $A$ 를 고정하고 그 표현을 연구하고자 한다고 합시다. 우리는 이미 "직합" 연산을 가지고 있습니다. 그러므로 소수에 특별히 주목하는 것과 마찬가지로, 기약 표현을 연구한 다음 이로부터  $A$ 의 모든 표현을 구성하고자 하는 동기가 생깁니다.

안타깝게도 우리는 (연습문제 19.4.5) 기약이 아니면서도 직합으로 분해될 수 없는(즉 비분해인) 표현이 존재함을 보았습니다. 이는 이상하고 나쁜 상황이므로, 더 다루기 좋은 성질을 가진 표현에 이름을 붙이고자 합니다. 표현이 이러한 나쁜 성질을 보이지 않을 때 그 표현을 **완전 기약**이라고 부릅니다.

더 나아가, 유한 차원 대수  $A$ 의 모든 유한 차원 표현이 완전 기약일 때  $A$ 를 **반단순**이라고 부릅니다. 따라서 반단순 대수  $A$ 의 유한 차원 표현을 연구할 때는, 기약 표현이 무엇인지만 알아내면 그것들을 조합하여  $A$ 의 모든 표현을 얻을 수 있습니다.

실제로 반단순 대수  $A$ 는 훨씬 더 좋은 성질을 가집니다. 이 장의 정점은  $A$ 가 반단순인 것과  $A \cong \bigoplus_i \text{Mat}(V_i)$ 인 것이 동치임을 증명하는 부분인데, 여기서  $V_i$ 는  $A$ 의 기약 표현들입니다(그렇습니다, 유한 개밖에 없습니다!).

결국 우리는 유한군  $G$ 의 군 대수  $k[G]$ 가 모두 반단순임을 (적어도  $k$ 의 표수가 0일 때) 보게 될 것이므로, 반단순 대수를 집중적으로 연구하는 것은 정당화됩니다.

**비고 20.0.1 (여담)** — 하지만 그 역은 성립하지 않습니다 —  $k$ 의 표수가 0이더라도, 모든 유한 차원 반단순  $k$ -대수가 어떤 군 대수와 동형인 것은 아닙니다.  $k$ -대수가 정확히 언제 군 대수와 동형인지를 분류하는 것은 어려운 문제로 밝혀져 있습니다. <https://mathoverflow.net/q/314502>를 참고하십시오.

## §20.1 슈어의 보조정리 (계속)

**이 절의 대표적인 예:**  $V$ 가 기약일 때,  $\text{Hom}_{\text{rep}}(V^{\oplus 2}, V^{\oplus 2}) \cong k^{\oplus 4}$ 입니다.

**정의 20.1.1.** 대수  $A$ 와 표현  $V, W$ 에 대해,  $\text{Hom}_{\text{rep}}(V, W)$ 를 이들 사이의 교환 연산자들의 집합이라고 하겠습니다. (이것 또한  $k$ -대수입니다.)

슈어의 보조정리에 의해 (다시 말하지만  $k$ 가 대수적으로 닫혀 있다는 것을 항상 가정하고 있으므로),  $V$ 와  $W$ 가 유한 차원 기약 표현이라면 다음이 성립함을 이미 알고 있습니다.

$$\text{Hom}_{\text{rep}}(V, W) \cong \begin{cases} k & V \cong W \text{인 경우} \\ 0 & V \not\cong W \text{인 경우.} \end{cases}$$

더 말할 것이 있을까요? 예를 들어, 이는 또한 다음을 알려줍니다.

$$\text{Hom}_{\text{rep}}(V, V^{\oplus 2}) = k^{\oplus 2}.$$

가능한 사상들은 어떤  $c_1, c_2 \in k$ 의 선택에 대해  $v \mapsto (c_1 v_1, c_2 v_2)$ 입니다.

더 일반적으로,  $V$ 가 유한 차원 기약 표현이라 하고  $\text{Hom}_{\text{rep}}(V^{\oplus m}, V^{\oplus n})$ 을 생각해 봅시다. 엄밀 연산자  $T: V^{\oplus m} \rightarrow V^{\oplus n}$ 은 다음 합성들의  $mn$ 가지 선택에 의해 완전히 결정됩니다.

$$V \hookrightarrow V^{\oplus m} \xrightarrow{T} V^{\oplus n} \twoheadrightarrow V$$

여기서 첫 번째 화살표는  $V^{\oplus m}$ 의  $i$ 번째 성분으로의 포함(단,  $1 \leq i \leq m$ )이고, 두 번째 화살표는  $V^{\oplus n}$ 의  $j$ 번째 성분으로의 사영(단,  $1 \leq j \leq n$ )입니다. 그러나 이 각각의 합성에 슈어의 보조정리를 적용하면, 이들이 상수여야 함을 알 수 있습니다.

따라서  $\text{Hom}_{\text{rep}}(V^{\oplus n}, V^{\oplus m})$ 은 상수들의  $m \times n$  "행렬"로 이루어지며, 그 사상은 다음과 같이 주어집니다.

$$\begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1(n-1)} & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2(n-1)} & c_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{m(n-1)} & c_{mn} \end{bmatrix} \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \in V^{\oplus m}$$

여기서  $c_{ij} \in k$ 이지만  $v_i \in V$ 입니다. 유형이 일치하지 않음에 주의하십시오! 이는 단순한  $k$ -선형 사상  $V^{\oplus n} \rightarrow V^{\oplus m}$ 이 아닙니다. 오히려 출력은 입력들의  $m$ 개의 선형결합입니다.

더 일반적으로, 다음이 성립합니다.

### 정리 20.1.2 (완전 기약 표현에 대한 슈어의 보조정리)

$V$ 와  $W$ 를 유한 차원 완전 기약 표현이라 하고, 정수  $n_i, m_i \geq 0$ 에 대해  $V = \bigoplus V_i^{\oplus n_i}$ ,  $W = \bigoplus V_i^{\oplus m_i}$ 라고 설정합니다. 여기서 각  $V_i$ 는 기약 표현입니다. 그러면 다음이 성립합니다.

$$\text{Hom}_{\text{rep}}(V, W) \cong \bigoplus_i \text{Mat}_{m_i \times n_i}(k)$$

이는 얹힘 연산자  $T: V \rightarrow W$ 가 각  $i$ 에 대해  $V_i^{\oplus n_i} \rightarrow V_i^{\oplus m_i}$ 인 사상을 주는  $m_i \times n_i$  상수 행렬에 해당함을 의미합니다.

### 따름정리 20.1.3 (완전 기약 표현의 부분표현)

$V = \bigoplus V_i^{\oplus n_i}$ 를 완전 기약이라고 합시다. 그러면  $V$ 의 임의의 부분표현  $W$ 는 각  $i$ 에 대해  $m_i \leq n_i$ 인  $\bigoplus V_i^{\oplus m_i}$ 와 동형이며, 포함  $W \hookrightarrow V$ 는 포함  $V_i^{\oplus m_i} \hookrightarrow V_i^{\oplus n_i}$ 의 직합으로 주어지는데, 이는  $n_i \times m_i$  행렬들입니다.

증명. 포함  $W \hookrightarrow V$ 에 슈어의 보조정리를 적용하십시오. □

**절 9.5**에서  $n$ 차원 벡터 공간에서  $m$ 차원 벡터 공간으로의 선형 사상은  $m \times n$  행렬로 쓸 수 있다는 것을 상기하십시오. 여기서도 상황은 비슷하지만, 행렬은 각 기약표현마다 독립적으로 만들어지며, 서로 동형이 아닌 기약표현들은 어떤 의미에서 "서로 대화하지 않습니다".

**비고 20.1.4** — 표현  $V^{\oplus n}$ 은 **예제 19.3.2**에서 했던 것처럼  $V$ 의  $n$ 개의 벡터를 "수평으로 쌓은 것"으로도 볼 수 있습니다:

$$\begin{pmatrix} \vdots & \vdots & \cdots & \vdots \\ v_1 & v_2 & \cdots & v_n \\ \vdots & \vdots & \cdots & \vdots \end{pmatrix} \in V^{\oplus n}.$$

그런 방식으로, 작용은 다음과 같이 주어집니다

$$\begin{pmatrix} \vdots & \vdots & \cdots & \vdots \\ v_1 & v_2 & \cdots & v_n \\ \vdots & \vdots & \cdots & \vdots \end{pmatrix} \begin{bmatrix} c_{11} & c_{21} & \cdots & c_{(m-1)1} & c_{m1} \\ c_{12} & c_{22} & \cdots & c_{(m-1)2} & c_{m2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ c_{1n} & c_{2n} & \cdots & c_{(m-1)n} & c_{mn} \end{bmatrix} \in V^{\oplus m}.$$

이런 방식이 타입 불일치가 발생하는 것을 더 명확히 볼 수 있게 해줄 수 있습니다. 그리고 이는 또한 **문제 19D\***의 뒤영킴 연산자가 왜 오른쪽 행렬 곱셈에 대응하는지에 대한 자연스러운 설명을 제공합니다.

## §20.2 조밀성 정리

우리는 앞선 결과를 활용하여 유한 차원 대수가 유한 개의 기약표현만을 가진다는 것을 증명할 것입니다.

### 정리 20.2.1 (야콥슨 조밀성 정리)

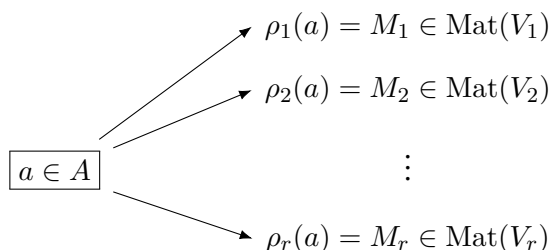
$(V_1, \rho_1), \dots, (V_r, \rho_r)$ 을  $A$ 의 서로 동형이 아닌 유한 차원 기약표현들이라 합시다. 그러면 다음과 같은 벡터 공간의 전사 사상이 존재합니다

$$\bigoplus_{i=1}^r \rho_i: A \rightarrow \bigoplus_{i=1}^r \text{Mat}(V_i).$$

이 정리를 생각하는 올바른 방법은 다음과 같습니다

**조밀성은  $A$ 의 유한 차원 기약표현들에 대한 "중국인의 나머지 정리"입니다.**

정수론에서 중국인의 나머지 정리는 서로 "무관한" 여러 합동식이 주어졌을 때, 이 모두를 동시에 만족하는 단 하나의  $N$ 을 찾을 수 있음을 알려준다는 것을 상기하십시오. 마찬가지로,  $A$ 의 서로 동형이 아닌 여러 유한 차원 기약표현이 주어졌을 때, 이는 우리가 원하는 임의의 작용 튜플  $(\rho_1(a), \dots, \rho_r(a))$ 을 유도하는 단 하나의  $a \in A$ 를 선택할 수 있다는 것을 의미합니다 — 이는 놀라운 결과인데,  $r = 1$ 인 경우조차 전혀 자명하지 않기 때문입니다!



이는 또한 다음과 같은 자명하지 않은 따름정리를 제공합니다:

### 따름정리 20.2.2 (표현의 개수의 유한성)

임의의 유한 차원 대수  $A$ 는 최대  $\dim A$ 개의 기약표현을 가집니다.

증명.  $V_i$ 가 그러한 기약표현들이라면  $A \twoheadrightarrow \bigoplus_i V_i^{\oplus \dim V_i}$ 이므로, 우리는 부등식  $\sum (\dim V_i)^2 \leq \dim A$ 를 얻습니다.  $\square$

조밀성 정리의 증명.  $V = V_1 \oplus \dots \oplus V_r$ 이라 하면,  $A$ 는  $\rho = \bigoplus_i \rho_i$ 에 의해  $V = (V, \rho)$ 에 작용합니다. 따라서 **문제 19C\***에 의해, 우리는 대신  $\rho$ 를 뒤영킴 연산자로 생각할 수 있습니다

$$\rho: \text{Reg}(A) \rightarrow \bigoplus_{i=1}^r \text{Mat}(V_i) \cong \bigoplus_{i=1}^r V_i^{\oplus d_i}.$$

우리는 이를 사용하는 것이 다루기 더 쉬우므로 이를 대신 사용할 것입니다.

먼저,  $r = 1$ 인 경우를 다룹니다.  $V = V_1$ 의 기저  $e_1, \dots, e_n$ 을 고정합니다. 모순을 이끌어내기 위해 이 사상이 전사가 아니라고 가정합니다. 그러면 ( $\rho$ 와 동형사상에 의한) 표현들의 사상  $\text{Reg}(A) \rightarrow V^{\oplus n}$ 이  $a \mapsto (a \cdot e_1, \dots, a \cdot e_n)$ 으로 존재합니다. 가정에 의해 이는 전사가 아닙니다: 그 상은  $V^{\oplus n}$ 의 진부분 부분표현입니다. 그 상이  $m < n$ 에 대해  $V^{\oplus m}$ 과 동형이라고 가정하면, 정리 20.1.2에 의해 다음을 만족하는 상수 행렬  $X$ 가 존재합니다

$$\begin{array}{ccc} \text{Reg}(A) & \longrightarrow & V^{\oplus n} \xleftarrow{X \cdot -} V^{\oplus m} \\ a & \longmapsto & (a \cdot e_1, \dots, a \cdot e_n) \\ 1_A & \longmapsto & (e_1, \dots, e_n) \longleftarrow (v_1, \dots, v_m) \end{array}$$

여기서 위쪽의 두 화살표는 같은 상을 가집니다; 따라서  $(e_1, \dots, e_n)$ 의 원상  $(v_1, \dots, v_m)$ 을 찾을 수 있습니다. 하지만  $m < n$ 이므로,  $X$ 를 열벡터  $(c_1, \dots, c_n)$ 에 적용했을 때 영이 되도록 모두 영은 아닌 상수  $c_1, \dots, c_n$ 을 찾을 수 있습니다:

$$\sum_{i=1}^n c_i e_i = \begin{bmatrix} c_1 & \dots & c_n \end{bmatrix} \begin{bmatrix} e_1 \\ \vdots \\ e_n \end{bmatrix} = \begin{bmatrix} c_1 & \dots & c_n \end{bmatrix} X \begin{bmatrix} v_1 \\ \vdots \\ v_m \end{bmatrix} = 0$$

이는  $e_i$ 가 선형 독립이라는 사실에 모순됩니다. 따라서  $r = 1$ 에 대해 정리를 결론짓습니다.

$r \geq 2$ 인 경우, 상  $\rho^{\text{img}}(A)$ 는 (따름정리 20.1.3에 의해) 반드시  $\bigoplus_i V_i^{\oplus d_i}$ 의 형태이며, 위에 서 본 바에 의해 각  $i$ 에 대해  $d_i = \dim V_i$ 입니다.  $\square$

### 예제 20.2.3 (조밀성 정리의 증명을 구체적인 예에 적용하기)

우리는 이 논증이 어떻게 작동하는지 더 잘 이해하기 위해 구체적인 예를 통해 논증을 실행해볼 수 있습니다 — 이를 위해서는  $V$ 가 기약표현이어야 하는데, 그렇지 않으면  $\text{Reg}(A)$ 의 상이  $V^{\oplus m}$ 과 동형이 아니게 되어, 우리는 논증을 끝까지 실행할 수 없게 됩니다.

$A = \text{Mat}_2(k)$ 이고, 자명한 작용을 갖는  $V \cong k^{\oplus 2}$ 라 합시다. 우리가 알고 있듯이, 이는 기약표현입니다.

조밀성 정리는  $\rho: A \rightarrow \text{Mat}(V)$ 가 전사임을 주장하는데, 이는 독립인 임의의  $e_1, e_2 \in V$ 와 임의의  $w_1, w_2 \in V$ 에 대해,  $a \cdot (e_1, e_2) = (w_1, w_2)$ 를 만족하는  $a \in A$ 를 찾을 수 있음을 의미합니다.

우리는 반례를 살펴보고 있으므로, 대신  $e_1 = (1, 0)$ ,  $e_2 = (2, 0)$ 을 선택합니다. 그러면 어떤  $w_1, w_2 \in V$ 에 대해서는,  $e_1$ 을  $w_1$ 으로,  $e_2$ 를  $w_2$ 로 보내는  $a$ 가 존재하지 않을 수 있습니다.

표현 사상  $\text{Reg}(A) \rightarrow V^{\oplus 2}$ 를  $a \mapsto (a \cdot e_1, a \cdot e_2)$ 로 생각해 봅시다; 그 상은  $\{(v, 2v) \mid v \in V\}$ 이며, 이는  $V^{\oplus 2}$ 의 부분표현으로서, 표현으로서  $V^{\oplus 1} \cong V$ 와 다음에 의해 동형입니다

$$v \mapsto (v, 2v) = v \begin{bmatrix} 1 & 2 \end{bmatrix}.$$

그러면  $v = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in V^{\oplus 1}$ 을 찾을 수 있고, 이에 대해

$$\begin{pmatrix} e_1 & e_2 \end{pmatrix} = v \begin{bmatrix} 1 & 2 \end{bmatrix}.$$

이제  $\begin{bmatrix} 1 & 2 \end{bmatrix}$ 라는 구체적인 수의 배열을 이용하면,  $e_1$ 과  $e_2$  사이의 선형 종속 관계를 쉽게 찾을 수 있습니다.

## §20.3 반단순 대수

**정의 20.3.1.** 유한 차원 대수  $A$ 가 **반단순**이라는 것은  $A$ 의 모든 유한 차원 표현이 완전 가약임을 의미합니다.

### 정리 20.3.2 (반단순 대수)

$A$ 를 유한 차원 대수라고 합시다. 그러면 다음이 동치입니다:

- (i) 어떤  $d_i$ 에 대해  $A \cong \bigoplus_i \text{Mat}_{d_i}(k)$ 입니다.
- (ii)  $A$ 는 반단순입니다.
- (iii)  $\text{Reg}(A)$ 는 완전 가약입니다.

증명. (i)  $\implies$  (ii)는 **명제 19.3.5**을 사용하여  $A$ 의 임의의 유한 차원 표현을  $\text{Mat}_{d_i}(k)$ 의 표현들의 직합으로 분해하고, 그다음 **정리 19.6.1**이 그러한 표현들이 모두 완전 가약임을 보임으로써 따라옵니다. (ii)  $\implies$  (iii)은 자명합니다.

(iii)  $\implies$  (i)를 보이기 위해, 다음의 영리한 트릭을 사용합니다. 다음을 생각해 봅시다

$$\text{Hom}_{\text{rep}}(\text{Reg}(A), \text{Reg}(A)).$$

한편으로, **문제 19D\***에 의해, 이는  $A^{\text{op}}$ ( $A$ 에 반대 곱셈을 준 것)와 동형인데, 왜냐하면  $\text{Reg}(A) \rightarrow \text{Reg}(A)$ 의 엄밀 연산자는 오직  $- \cdot a$  형태의 것들뿐이기 때문입니다. 다른 한편으로,  $\text{Reg}(A) = \bigoplus_i V_i^{\oplus n_i}$ 로 설정했다고 합시다. **정리 20.1.2**에 의해, 다음을 얻습니다

$$A^{\text{op}} \cong \text{Hom}_{\text{rep}}(\text{Reg}(A), \text{Reg}(A)) = \bigoplus_i \text{Mat}_{n_i \times n_i}(k).$$

그런데  $\text{Mat}_n(k)^{\text{op}} \cong \text{Mat}_n(k)$ 이므로(단순히 전치를 취함으로써), 원하는 결론을 얻습니다.  $\square$

**비고 20.3.3** — 위 증명의 트릭은 케일리 정리(**문제 1F†**)와 닮아 있는데, 대상이 자기 자신에 작용하게 하여 명시적인 표현을 얻는다는 점에서 그렇습니다.

**비고 20.3.4** — 이를 **따름정리 18.3.2**와 비교할 수 있습니다. 여기서,  $A$ 의 임의의 유한 차원 표현은 유한 차원 왼쪽  $A$ -가군이며, 위 정리로부터,  $A$ 가 반단순이면 그러한 임의의 가군은 기약표현  $V_i \cong k^{\oplus d_i}$ 들의 직합으로 분해될 수 있음을 알 수 있습니다.  $A$ 가 PID인 경우와 달리,  $k^{\oplus d_i}$ 는 환  $\text{Mat}_{d_i}(k)$ 의 몫과 동형이 아님에 유의하십시오.

실제로, 위 결과를 조밀성 정리(그리고 **따름정리 20.2.2**)와 결합하면, 다음을 얻습니다:

### 정리 20.3.5 (제공합 공식)

유한 차원 대수  $A$ 에 대해 다음이 성립합니다

$$\sum_i \dim(V_i)^2 \leq \dim A$$

여기서  $V_i$ 는  $A$ 의 기약표현들입니다; 등식은 정확히  $A$ 가 반단순일 때 성립하며, 이 경우

$$\text{Reg}(A) \cong \bigoplus_i \text{Mat}(V_i) \cong \bigoplus_i V_i^{\oplus \dim V_i}.$$

증명. 이 부등식은 이미 **따름정리 20.2.2**에서 언급되었습니다. 등식이 성립하는 것은 사상  $\rho: A \rightarrow \bigoplus_i \text{Mat}(V_i)$ 가 동형사상일 때이자 오직 그때뿐이며, 이는 모든  $V_i$ 가 존재함을 의미합니다.  $\square$

**비고 20.3.6 (여담)** — 임의의 유한 차원  $A$ 에 대해, 사상  $\rho: A \rightarrow \bigoplus_i \text{Mat}(V_i)$ 의 핵을  $\text{Rad}(A)$ 로 표기하며, 이는  $A$ 의 소위 **야콥슨 근기**입니다; 이는  $A$ 의 모든 기약 표현에서 영으로 작용하는 모든  $a \in A$ 의 집합입니다. 책에서 흔히 주어지는 "반단순"의 정의는 이 야콥슨 근기가 자명하다는 것입니다.

## §20.4 마슈케 정리

이제 군의 표현론이 가능한 한 좋다는 것을 증명하겠습니다.

### 정리 20.4.1 (마슈케 정리)

$G$ 를 유한군이라 하고,  $k$ 를 그 표수가  $|G|$ 를 나누지 않는 대수적으로 닫힌 체라고 합시다. 그러면  $k[G]$ 는 반단순입니다.

이는 군의 표현을 연구할 때 모든 표현이 완전 가약임을 말해줍니다.

증명.  $k[G]$ 의 임의의 유한 차원 표현  $(V, \rho)$ 을 생각해봅시다. 진부분표현  $W \subseteq V$ 가 주어졌을 때, 우리의 목표는

$$V = W \oplus W'.$$

를 만족하는 보충적인  $G$ -불변 부분공간  $W'$ 를 구성하는 것입니다. 이는 분해불가능  $\iff$  기약임을 보여줄 것이며, 이는  $k[G]$ 가 반단순임을 보이기에 충분합니다.

$\pi: V \rightarrow W$ 를  $V$ 에서  $W$ 로의 임의의 사영이라 하고, 이는  $\pi(v) = v \iff v \in W$ 를 의미합니다. 우리는 다음과 같은 평균화 사상  $P: V \rightarrow V$ 를 고려합니다

$$P = \frac{1}{|G|} \sum_{g \in G} \rho(g^{-1}) \circ \pi \circ \rho(g).$$

우리는 이 사상의 다음 성질들을 사용할 것입니다:

**연습문제 20.4.2.** 사상  $P$ 가 다음을 만족함을 보이십시오:

- 임의의  $w \in W$ 에 대해,  $P(w) = w$ 입니다.
- 임의의  $v \in V$ 에 대해,  $P(v) \in W$ 입니다.
- 사상  $P: V \rightarrow V$ 는 교환 연산자입니다.

따라서  $P$ 는 멱등원입니다(이는 그 상  $W$  위에서 항등사상입니다). 그러므로 **문제 9H\***에 의해  $V = \ker P \oplus \text{im } P$ 가 성립하는데,  $\ker P$ 와  $\text{im } P$  둘 다 원하는 대로 부분표현입니다.  $\square$

**비고 20.4.3** —  $k = \mathbb{C}$ 인 경우에는 더 짧은 증명이 있습니다.  $B: V \times V \rightarrow \mathbb{C}$ 가 임의의 쌍선형 형식이라고 합시다. 그러면 이를 "평균화"하여 새로운 쌍선형 형식을 얻을 수 있습니다

$$\langle v, w \rangle := \frac{1}{|G|} \sum_{g \in G} B(g \cdot v, g \cdot w).$$

평균화된 형식  $\langle -, - \rangle$ 는  $\langle g \cdot v, g \cdot w \rangle$ 라는 의미에서  $G$ -불변입니다. 그러면  $W \subseteq V$ 가 부분표현이면 그 직교 여공간  $W^\perp$ 도 부분표현임을 알 수 있습니다. 이로부터

터 결과가 따라옵니다.

## §20.5 예시: $\mathbb{C}[S_3]$ 의 표현들

우리는  $\mathbb{C}[S_3]$ 의 모든 기약표현을 계산합니다. 지금은 정확히 세 개의 그러한 표현이 존재한다는 것을 당연한 것으로 받아들이겠습니다(이는 다음 장의 첫 번째 정리에 의해 즉시 알 수 있을 것입니다: 실제로 우리는  $G$ 의 표현의 개수가  $G$ 의 켄레류의 개수와 정확히 같다는 것을 보게 될 것입니다).

이를 감안할 때,  $\mathbb{C}[S_3]$ 의 세 표현이 차원  $d_1, d_2, d_3$ 를 가진다면, 우리는 다음이 성립해야 합니다

$$d_1^2 + d_2^2 + d_3^2 = |G| = 6.$$

이로부터, 약간의 심오한 산술과 결합하여, 우리는  $d_1 = d_2 = 1$ 이고  $d_3 = 2$ 이거나 그 순열이어야 함을 추론합니다.

사실, 우리는 이 표현들을 명시적으로 기술할 수 있습니다. 먼저, 다음을 정의합니다:

**정의 20.5.1.**  $G$ 를 군이라 합시다. 군  $G$ 의 복소 **자명 군 표현**은 일차원 표현  $\mathbb{C}_{\text{triv}} = (\mathbb{C}, \rho)$ 로서, 모든  $g \in G$ 와  $v \in \mathbb{C}$ 에 대해  $g \cdot v = v$ 입니다(즉, 모든  $g \in G$ 에 대해  $\rho(g) = \text{id}$ 입니다).

**비고 20.5.2 (경고)** — 대수  $A$ 의 자명 표현은 우리에게 의미가 없습니다:  $a \cdot v = v$ 로 설정하고 싶을 수 있지만, 이는  $A$ 에서 선형이 아닙니다. (우리 정의에서 조건  $1_A \cdot v = v$ 를 삭제하여 이를 억지로 작동시키려 시도할 수는 있습니다; 그러면 단순히  $a \cdot v = 0$ 으로 설정할 수 있습니다. 하지만 그렇게 하더라도  $\mathbb{C}_{\text{triv}}$ 는  $k[G]$ 의 자명 표현이 되지 않을 것입니다.)

이를 확인하는 또 다른 방법은, 자명 표현이  $k$ -대수가 군 대수로 어떻게 쓰이는지에 의존한다는 것입니다:  $k[\mathbb{Z}/2\mathbb{Z}]$ 는  $g \mapsto -g$ 로 주어지는  $k$ -대수 자기동형사상을 가지는데, 여기서  $g$ 는 군  $\mathbb{Z}/2\mathbb{Z}$ 의 생성원입니다; 그러나 대응하는 자명 표현들은 서로 다릅니다.

그러면 표현들은 다음과 같습니다:

- 일차원  $\mathbb{C}_{\text{triv}}$ ; 각  $\sigma \in S_3$ 는 항등사상으로 작용합니다.
- $S_3 \rightarrow \mathbb{C}^\times$  사상이  $\sigma$ 를  $\sigma$ 의 부호로 보내는 자명하지 않은 일차원 표현  $\mathbb{C}_{\text{sign}}$ 이 있습니다. 따라서  $\mathbb{C}_{\text{sign}}$ 에서 모든  $\sigma \in S_3$ 는  $\pm 1$ 로 작용합니다. 물론,  $\mathbb{C}_{\text{triv}}$ 와  $\mathbb{C}_{\text{sign}}$ 은 동형이 아닙니다(일차원 표현들은 **문제 19A<sup>†</sup>**에서 보았듯이 모든  $a$ 에 대해 작용하는 상수가 일치하지 않는 한 결코 동형이 아니기 때문입니다).
- 마지막으로, 우리는 이미 이차원 표현을 살펴본 바 있으나, 이제 여기에 이름을 붙이도록 하겠습니다.  $\text{refl}_0$ 을 벡터 공간이  $\{(x, y, z) \mid x + y + z = 0\}$ 이고, 그 위에서의  $S_3$ 의 작용이 좌표의 순열인 표현으로 정의합니다.

**연습문제 20.5.3.**  $\text{refl}_0$ 이 기약임을 보이십시오. 예를 들어  $S_3$ 의 작용 아래 불변인 부분 공간이 없음을 직접 보임으로써 보일 수 있습니다.

따라서  $V$ 는 앞의 두 표현과도 동형이 아닙니다.

이는 이것들이  $S_3$ 의 모든 기약 표현임을 의미합니다.  $S_3$ 의  $k^{\oplus 3}$  위에서의 표현  $V$ 를 취하면,  $V = \text{refl}_0 \oplus \mathbb{C}_{\text{triv}}$ 를 얻는다는 점에 유의하십시오.

## §20.6 생각해 볼 만한 조금 더 어려운 문제

**문제 20A.**  $\mathbb{C}[\mathbb{Z}/n\mathbb{Z}]$ 의 모든 기약 표현을 구하십시오.

**문제 20B** (Maschke의 정리는  $|G|$ 가 유한할 것을 요구합니다). 덧셈에 대한 군  $\mathbb{R}$ 의  $\mathbb{C}^{\oplus 2}$  위에서의 표현을 준동형사상

$$\mathbb{R} \rightarrow \text{Mat}_2(\mathbb{C}) \quad \text{에 의해} \quad t \mapsto \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}.$$

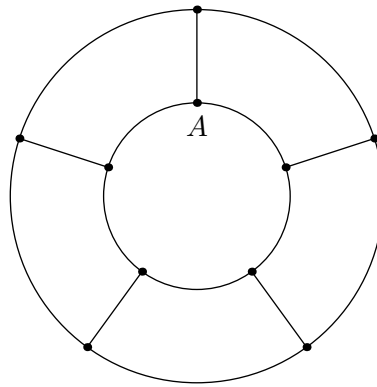
이 표현이 기약이 아니지만 분해 불가능함을 보이십시오.

**문제 20C.** 유한군의 모든 기약 표현이 유한 차원임을 증명하십시오.

**문제 20D.**  $D_{10}$ 의 모든 복소 기약 표현을 결정하십시오.



**문제 20E** (AIME 2018). 아래에 나타난 바퀴는 두 개의 원과 다섯 개의 바퀴살로 이루어져 있으며, 바퀴살이 원과 만나는 곳에 레이블이 붙어 있습니다. 벌레 한 마리가  $A$ 에서 출발하여 바퀴를 따라 걷습니다. 벌레는 15번의 걸음을 걷습니다. 각 걸음마다 벌레는 안쪽 원을 따라서는 반시계 방향으로만, 바깥쪽 원을 따라서는 시계 방향으로만 걷도록 인접한 레이블로 이동합니다. 모든 걸음을 마친 후 벌레가  $A$ 에 도달하는 경우의 수는 몇 가지입니까?



# 21 지표

지표는 기본적으로 최고의 개념입니다.  $A$ 의 모든 표현  $V$ 에 대해 우리는 이른바 지표라고 부르는  $\chi_V: A \rightarrow k$ 를 대응시킬 것입니다.  $A$ 의 유한 차원 기약표현들의 지표가 표현  $V$ 를 완전히 결정한다는 것이 밝혀질 것입니다. 따라서 유한 차원 기약표현은 단지  $\dim A$ 개의 숫자들의 집합으로 명시됩니다.

## §21.1 정의

**정의 21.1.1.**  $V = (V, \rho)$ 를  $A$ 의 유한 차원 표현이라 합시다.  $V$ 에 대응되는 **지표**  $\chi_V: A \rightarrow k$ 는  $\chi_V = \text{Tr} \circ \rho$ 로 정의됩니다. 즉

$$\chi_V(a) := \text{Tr}(\rho(a): V \rightarrow V).$$

$\text{Tr}$ 과  $\rho$ 가 가법적이므로, 이는  $k$ -선형 사상입니다(단 곱셈적이지는 않습니다). 또한 임의의 표현  $V$ 와  $W$ 에 대해  $\chi_{V \oplus W} = \chi_V + \chi_W$ 임에 유의하십시오.

물론 우리는 특히  $A = k[G]$ 인 경우에 관심이 있습니다. 평소와 같이, 전체 사상  $k[G] \rightarrow k$ 를 얻기 위해서는 각  $g \in G$ 에 대해  $\chi_V(g)$ 만 명시하면 됩니다. 따라서 우리는 종종  $\chi_V$ 를 함수  $G \rightarrow k$ 로 생각하며, 이를 군  $G$ 의 지표라고 부릅니다. 다음은  $G = S_3$ 인 경우입니다:

### 예제 21.1.2 ( $S_3$ 의 지표표)

앞서 다룬  $G = S_3$ 의 세 기약표현을 생각해 봅시다.  $\mathbb{C}_{\text{자명}}$ 에 대해서는 모든 대각합이 1이고,  $\mathbb{C}_{\text{부호}}$ 에 대해서는 부호에 따라 대각합이  $\pm 1$ 입니다(당연히, 일차원 사상  $k \rightarrow k$ 의 경우 대각합은 그 사상 자체와 "같습니다").  $\text{refl}_0$ 에 대해서는 예를 들어 기저  $(1, 0, -1)$ 과  $(0, 1, -1)$ 을 취하여 이 기저에서 직접 대각합을 계산합니다.

| $\chi_V(g)$                | id | (1 2) | (2 3) | (3 1) | (1 2 3) | (3 2 1) |
|----------------------------|----|-------|-------|-------|---------|---------|
| $\mathbb{C}_{\text{triv}}$ | 1  | 1     | 1     | 1     | 1       | 1       |
| $\mathbb{C}_{\text{sign}}$ | 1  | -1    | -1    | -1    | 1       | 1       |
| $\text{refl}_0$            | 2  | 0     | 0     | 0     | -1      | -1      |

위의 표는 군  $G$ 의 **지표표**라고 불립니다. 위 표는 이 장이 진행됨에 따라 우리가 증명할 몇 가지 신비로운 성질들을 지니고 있습니다.

- (I)  $\chi_V(g)$ 의 값은 오직  $g$ 의 켤레류에만 의존합니다.
- (II) 행의 개수는 켤레류의 개수와 같습니다.
- (III) 어느 행이든 그 제곱합은 다시 6이 됩니다!
- (IV) 임의의 두 행의 "내적"은 0입니다.

**표기의 남용 21.1.3.**  $\chi_V: G \rightarrow k$ 에 대해 "지표"라는 이름은 다소 오해의 소지가 있습니다. 위 예시에서 보듯이 이  $\chi_V$ 는 결코 곱셈적이지 않으며, 거의  $k^{\oplus |G|}$ 의 원소로 생각할 수 있습니다.

**질문 21.1.4.**  $\chi_V(1_A) = \dim V$ 임을 보이십시오. 따라서 지표표의 가장 왼쪽 열에서 표현들의 차원을 읽어낼 수 있습니다.

## §21.2 교환자로 나는 쌍대 공간

임의의 대수에 대해, 우리는 먼저  $\text{Tr}(TS) = \text{Tr}(ST)$ 이므로 임의의  $V$ 에 대해 다음이 성립함을 관찰합니다.

$$\chi_V(ab) = \chi_V(ba).$$

이는 앞서의 관찰 (I)을 설명합니다:

**질문 21.2.1.**  $g$ 와  $h$ 가 군  $G$ 의 같은 켤레류에 속하고  $V$ 가  $k[G]$ 의 표현일 때,  $\chi(g) = \chi(h)$ 임을 유도하십시오.

이제 대수  $A$ 가 주어졌을 때, **교환자**(commutator)  $[A, A]$ 를  $x, y \in A$ 에 대한  $xy - yx$ 로 생성되는  $k$ -벡터 부분공간으로 정의합니다. 따라서  $[A, A]$ 는 각  $\chi_V$ 의 핵에 포함됩니다.

**정의 21.2.2.** 공간  $A^{\text{ab}} := A/[A, A]$ 는  $A$ 의 **아벨화**라고 불립니다.  $A$ 의 각 지표는  $A^{\text{ab}} \rightarrow k$ 인 사상, 즉  $(A^{\text{ab}})^{\vee}$ 의 원소로 볼 수 있습니다.

### 예제 21.2.3 (아벨화의 예시)

- (a)  $A$ 가 가환이면,  $[A, A] = \{0\}$ 이고  $A^{\text{ab}} = A$ 입니다.
- (b)  $A = \text{Mat}_d(k)$ 이면,  $[A, A]$ 는 정확히 대각합이 0인  $d \times d$  행렬들로 이루어집니다. (증명: 간단한 연습문제입니다.) 그 결과,  $A^{\text{ab}}$ 는 일차원입니다.
- (c)  $A = k[G]$ 라고 합시다. 그러면  $A^{\text{ab}}$ 에서는 각  $g, h \in G$ 에 대해  $gh$ 와  $hg$ 를 동일시합니다. 이는  $ghg^{-1} = h$ 와 동치입니다. 다시 말해,  $A^{\text{ab}}$ 는  $G$ 의 켤레류들의  $k$ -선형결합으로 이루어진 공간과 동형입니다.

**비고 21.2.4 (경고)** — 군  $G$ 에 대하여,  $G$ 의 아벨화는  $G/[G, G]$ 로 정의되며, 여기서  $[G, G]$ 는 모든 교환자로 생성되는 부분군입니다.

$A = k[G]$ 일 때, 공간  $A^{\text{ab}}$ 는 군 대수  $k[G/[G, G]]$ 와 동형이 아닙니다! 이는 군  $G$ 의 아벨화에서는 모든  $g, h \in G$ 에 대해  $ghg^{-1}h^{-1} = 1$ 을 동일시하는데, 이는  $gh - hg$ 와 같지 않기 때문입니다.

사실 일반적인 경우에는,  $A^{\text{ab}}$ 는  $A$ 로부터  $k$ -대수의 구조를 물려받지도 못하며, 오직  $k$ -벡터 공간의 구조만 얻을 수 있습니다.

### 정리 21.2.5 (대수의 표현의 지표)

$A$ 를 대수적으로 닫힌 체 위의 대수라 합시다. 그러면

- (a) 서로 동형이 아닌 유한 차원 기약표현들의 지표는  $(A^{\text{ab}})^{\vee}$ 에서 선형 독립입니다.
- (b)  $A$ 가 유한 차원이고 반단순이면, 기약표현에 대응하는 지표들은  $(A^{\text{ab}})^{\vee}$ 의 기저를 이룹니다.

특히 (b)에서  $A$ 의 기약표현의 개수는  $\dim A^{\text{ab}}$ 와 같습니다.

증명. (a)는 조밀성 정리에 의해 거의 자명합니다. 선형 종속 관계가 있다고 가정하면, 모든  $a$ 에 대해 다음이 성립합니다

$$c_1 \chi_{V_1}(a) + c_2 \chi_{V_2}(a) + \cdots + c_r \chi_{V_r}(a) = 0$$

어떤 정수  $r$ 에 대하여.

**질문 21.2.6.** 조밀성 정리로부터  $c_1 = \cdots = c_r = 0$ 임을 유도하십시오.

(b)에 대해서는,  $r$ 개의 기약표현이 있다고 가정합시다. 우리는

$$A = \bigoplus_{i=1}^r \text{Mat}(V_i)$$

라고 가정할 수 있으며, 여기서  $V_1, \dots, V_r$ 은  $A$ 의 기약표현들입니다. 지표들이 선형 독립임을 이미 보였으므로,  $\dim(A/[A, A]) = r$ 임만 보이면 되는데, 이는 각  $\text{Mat}(V_i)$ 가 일차원 아벨화를 갖는다는 앞선 관찰로부터 따라옵니다.  $\square$

$G$ 는  $\dim k[G]^{\text{ab}}$ 개의 켈레류를 가지므로, 이로써 (II)의 증명이 완료됩니다.

## §21.3 지표의 직교성

이제  $\mathbb{C}$  위에서 표현된 유한군  $G$ 의 경우로 특수화합니다.

**정의 21.3.1.**  $\text{Classes}(G)$ 가  $G$ 의 켈레류의 집합을 나타낸다고 합시다.

$G$ 가  $r$ 개의 켈레류를 가지면,  $G$ 는  $r$ 개의 기약표현을 갖습니다. 각 (유한 차원) 표현  $V$ 는, 기약이든 아니든, 지표  $\chi_V$ 를 줍니다.

**표기의 남용 21.3.2.** 앞으로는  $\chi_V$ 를 함수  $G \rightarrow \mathbb{C}$ 로, 또는 함수  $\text{Classes}(G) \rightarrow \mathbb{C}$ 로 종종 간주할 것입니다. 예를 들어,  $\chi_V(g)$  ( $g \in G$ 에 대해)와  $\chi_V(C)$  (켈레류  $C$ 에 대해)를 둘 다 사용할 것인데, 후자는 단지 임의의 대표원  $g_C \in C$ 에 대한  $\chi_V(g_C)$ 를 의미합니다.

**정의 21.3.3.**  $\text{Func}_{\text{class}}(G)$ 가  $\mathbb{C}$  위의 벡터 공간으로 간주되는 함수  $\text{Classes}(G) \rightarrow \mathbb{C}$ 의 집합을 나타낸다고 합시다. 우리는 여기에 다음과 같은 내적 형식을 부여합니다

$$\langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} f_1(g) \overline{f_2(g)}.$$

이는 처음에  $S_3$ 의 지표표를 살펴보았을 때 언급했던 것과 같은 "내적"입니다. 이제 우리는 다음의 직교성 정리를 증명하고자 하는데, 이는 앞서 나온 (III)과 (IV)를 함의할 것입니다.

### 정리 21.3.4 (직교성)

$G$ 의 임의의 유한 차원 복소 표현  $V$ 와  $W$ 에 대해 다음이 성립합니다

$$\langle \chi_V, \chi_W \rangle = \dim \text{Hom}_{\text{rep}}(W, V).$$

특히,  $V$ 와  $W$ 가 기약표현이면 다음이 성립합니다

$$\langle \chi_V, \chi_W \rangle = \begin{cases} 1 & V \cong W \\ 0 & \text{그 외의 경우.} \end{cases}$$

### 따름정리 21.3.5 (기약표현은 정규직교 기저를 줍니다)

기약표현에 결부된 지표들은  $\text{Func}_{\text{class}}(G)$ 의 정규직교 기저를 이룹니다.

이 정리를 증명하기 위해서는 쌍대 표현과 텐서 표현을 정의해야 하는데, 이는 양  $\chi_V(g) \overline{\chi_W(g)}$ 을 다루는 자연스러운 방법을 제공합니다.

**정의 21.3.6.**  $V = (V, \rho)$ 를  $G$ 의 표현이라 합시다. 쌍대 표현  $V^\vee$ 은  $V^\vee$  위의 표현으로,  $G$ 의 작용은 다음과 같이 주어집니다: 각  $\xi \in V^\vee$ 에 대해,  $g$ 의 작용은 다음과 같이 명시된  $g \cdot \xi \in V^\vee$ 을 줍니다

$$v \xrightarrow{g \cdot \xi} \xi(\rho(g^{-1})(v)).$$

**정의 21.3.7.**  $V = (V, \rho_V)$ 와  $W = (W, \rho_W)$ 을  $G$ 의 군 표현이라 합시다.  $V$ 와  $W$ 의 텐서곱은  $V \otimes W$  위의 군 표현으로,  $G$ 의 작용은 순수 텐서에 대해 다음과 같이 주어집니다

$$g \cdot (v \otimes w) = (\rho_V(g)(v)) \otimes (\rho_W(g)(w))$$

이는 선형적으로 확장되어  $V \otimes W$  전체에 대한  $G$ 의 작용을 정의합니다.

**비고 21.3.8 —** 주의: 텐서에 대한 정의는 대수로 확장되지 않습니다.  $a \cdot (v \otimes w) = (a \cdot v) \otimes (a \cdot w)$ 가 성립하기를 바랄 수도 있지만, 이는  $a \in A$ 에 대해 선형적이지도 않습니다(예를 들어  $a = 2$ 를 취하면 어떻게 되겠습니까?).

### 정리 21.3.9 (지표의 대각합)

$V$ 와  $W$ 가  $G$ 의 유한 차원 표현이라면, 임의의  $g \in G$ 에 대해.

- (a)  $\chi_{V \oplus W}(g) = \chi_V(g) + \chi_W(g)$ .
- (b)  $\chi_{V \otimes W}(g) = \chi_V(g) \cdot \chi_W(g)$ .
- (c)  $\chi_{V^\vee}(g) = \overline{\chi_V(g)}$ .

증명. (a)와 (b)는 항등식  $\text{Tr}(S \oplus T) = \text{Tr}(S) + \text{Tr}(T)$ 와  $\text{Tr}(S \otimes T) = \text{Tr}(S) \text{Tr}(T)$ 로부터 따라 나옵니다. 하지만 (c)는 더 까다롭습니다. 라그랑주 정리에 의해  $(\rho(g))^{|G|} = \rho(g^{|G|}) = \rho(1_G) = \text{id}_V$ 이므로,  $\rho(g)$ 를 대각화할 수 있는데, 고윳값을  $\lambda_1, \dots, \lambda_n$ 이라 하면 이들은  $|G|$ 차 단위근이며, 고유벡터  $e_1, \dots, e_n$ 에 대응합니다. 그러면 기저  $e_1^\vee, \dots, e_n^\vee$ 에서  $V^\vee$  위의  $g$ 의 작용은 고윳값  $\lambda_1^{-1}, \lambda_2^{-1}, \dots, \lambda_n^{-1}$ 을 가짐을 알 수 있습니다. 따라서

$$\chi_V(g) = \sum_{i=1}^n \lambda_i \quad \text{그리고} \quad \chi_{V^\vee}(g) = \sum_{i=1}^n \lambda_i^{-1} = \sum_{i=1}^n \overline{\lambda_i}$$

여기서 마지막 단계는 항등식  $|z| = 1 \iff z^{-1} = \overline{z}$ 로부터 따라 나옵니다.  $\square$

**비고 21.3.10 (주의) —** 항등식 (b)와 (c)는  $\mathbb{C}[G]$ 로 선형적으로 확장되지 않습니다. 즉,  $\chi_V$ 를 사상  $\mathbb{C}[G] \rightarrow \mathbb{C}$ 로 생각할 때 예를 들어  $\chi_{V^\vee}(a) = \overline{\chi_V(a)}$ 가 성립하는 것은 사실이 아닙니다.

직교 관계의 증명. 핵심은 이제 곱들의 합을 다음을 통해 단 하나의 지표로 축소할 수 있다는 것입니다

$$\chi_V(g) \overline{\chi_W(g)} = \chi_{V \otimes W^\vee}(g).$$

따라서 문제의 합을 다음과 같이 다시 쓸 수 있습니다

$$\langle \chi_V, \chi_W \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_{V \otimes W^\vee}(g) = \chi_{V \otimes W^\vee} \left( \frac{1}{|G|} \sum_{g \in G} g \right).$$

$P: V \otimes W^\vee \rightarrow V \otimes W^\vee$ 을  $\frac{1}{|G|} \sum_{g \in G} g$ 의 작용이라 하면, 우리는  $\text{Tr } P$ 를 구하고자 합니다.

**연습문제 21.3.11.**  $P$ 가 멱등원임을 보이십시오. ( $P \circ P$ 를 직접 계산하십시오.)

따라서 (문제 9H\*에 의해)  $V \otimes W^\vee = \ker P \oplus \operatorname{im} P$ 이며,  $\operatorname{im} P$ 는  $G$  아래에서 고정된 원소들의 부분공간입니다. 이로부터 다음을 이끌어낼 수 있습니다

$$\operatorname{Tr} P = \dim \operatorname{im} P = \dim \{x \in V \otimes W^\vee \mid g \cdot x = x \ \forall g \in G\}.$$

이제 자연스러운 동형사상  $V \otimes W^\vee \rightarrow \operatorname{Hom}(W, V)$ 을 생각해 봅시다.

**연습문제 21.3.12.**  $g \in G$ 라 합시다. 이 동형사상 아래에서,  $T \in \operatorname{Hom}(W, V)$ 가  $g \cdot T = T$ 를 만족하는 것은 각  $w \in W$ 에 대해  $T(g \cdot w) = g \cdot T(w)$ 인 것과 동치임을 보이십시오. (이는 세 개 혹은 네 개의 정의를 풀어내기만 하면 됩니다.)

결과적으로,  $\chi_{V \otimes W^\vee}(P) = \operatorname{Tr} P = \dim \operatorname{Hom}_{\operatorname{rep}}(W, V)$ 이 원하는 대로 성립합니다.  $\square$

직교 관계는 유한 차원 표현  $V$ 가 기약인지를 확인하는 빠르고 기계적인 방법을 제공합니다. 즉, 각  $g \in G$ 에 대해 대각합  $\chi_V(g)$ 를 계산한 다음,  $\langle \chi_V, \chi_V \rangle = 1$ 인지를 확인하면 됩니다. 그래서 예를 들어, 우리가 찾았던  $S_3$ 의 세 표현이 기약표현임을 지표표로부터 직접 알 수 있었을 것입니다. 따라서 이제 우리는 기약표현의 완전한 집합을 가질 때마다 효율적으로 검증할 수 있습니다.

## §21.4 지표표의 예

**예제 21.4.1** (원소가 10개인 이면체군)

$D_{10} = \langle r, s \mid r^5 = s^2 = 1, rs = sr^{-1} \rangle$ 라 합시다.  $\omega = \exp(\frac{2\pi i}{5})$ 라 합시다.  $D_{10}$ 의 네 가지 표현을 씁니다:

- $\mathbb{C}_{\operatorname{triv}}$ 에서는,  $D_{10}$ 의 모든 원소가 항등원으로 작용합니다.
- $\mathbb{C}_{\operatorname{sign}}$ 에서  $r$ 은 항등원으로 작용하고  $s$ 는 부호 반전으로 작용합니다.
- $V_1$ 은 이차원이며  $r \mapsto \begin{bmatrix} \omega & 0 \\ 0 & \omega^4 \end{bmatrix}$ 와  $s \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ 로 주어집니다.
- $V_2$ 는 이차원이며  $r \mapsto \begin{bmatrix} \omega^2 & 0 \\ 0 & \omega^3 \end{bmatrix}$ 와  $s \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ 로 주어집니다.

이 네 표현이 기약이며 서로 동형이 아니라고 주장합니다. 이를 지표표를 작성하여 증명합니다:

| $D_{10}$                           | 1 | $r, r^4$              | $r^2, r^3$            | $sr^k$ |
|------------------------------------|---|-----------------------|-----------------------|--------|
| $\mathbb{C}_{\operatorname{triv}}$ | 1 | 1                     | 1                     | 1      |
| $\mathbb{C}_{\operatorname{sign}}$ | 1 | 1                     | 1                     | -1     |
| $V_1$                              | 2 | $\omega + \omega^4$   | $\omega^2 + \omega^3$ | 0      |
| $V_2$                              | 2 | $\omega^2 + \omega^3$ | $\omega + \omega^4$   | 0      |

그러면 직접 계산을 통해 직교 관계를 보일 수 있으므로, 실제로 정규직교기저를 갖습니다. 예를 들어  $\langle \mathbb{C}_{\operatorname{triv}}, \mathbb{C}_{\operatorname{sign}} \rangle = 1 + 2 \cdot 1 + 2 \cdot 1 + 5 \cdot (-1) = 0$ 입니다.

**예제 21.4.2** ( $S_4$ 의 지표표)

이제  $S_4$ 의 지표표를 계산할 만한 충분한 도구를 갖추었으며,  $S_4$ 는 다섯 개의 켤레류를 가집니다 (순환 유형 id, 2, 3, 4,  $2+2$ 에 대응). 먼저,  $S_4$ 는 두 개의 일차원 표현  $\mathbb{C}_{\text{triv}}$ 와  $\mathbb{C}_{\text{sign}}$ 을 가지며, 이것들이 전부임을 주목합니다 (준동형사상  $S_4 \rightarrow \mathbb{C}^\times$ 가 오직 두 개뿐이기 때문입니다). 따라서 지금까지 다음과 같은 표를 얻습니다

| $S_4$                      | 1 | (••) | (•••)    | (••••) | (••)(••) |
|----------------------------|---|------|----------|--------|----------|
| $\mathbb{C}_{\text{triv}}$ | 1 | 1    | 1        | 1      | 1        |
| $\mathbb{C}_{\text{sign}}$ | 1 | -1   | 1        | -1     | 1        |
| $\vdots$                   |   |      | $\vdots$ |        |          |

열들이  $1 + 6 + 8 + 6 + 3 = 24$ 개의 원소를 나타냄에 주목하십시오. 이제, 나머지 세 표현은 다음을 만족하는 차원  $d_1, d_2, d_3$ 을 가집니다

$$d_1^2 + d_2^2 + d_3^2 = 4! - 2 = 22$$

이는  $(d_1, d_2, d_3) = (2, 3, 3)$ 과 그 순열들만을 해로 가집니다. 이제  $\text{refl}_0$  표현을 취할 수 있습니다

$$\{(w, x, y, z) \mid w + x + y + z = 0\}$$

기저  $(1, 0, 0, -1), (0, 1, 0, -1), (0, 0, 1, -1)$ 을 가집니다. 이것이 기약임을 기하학적으로 확인할 수 있지만, 지표표 직접 계산함으로써 수치적으로도 확인할 수 있습니다 (지루한 작업입니다): 계산하면 3, 1, 0, -1, -1이 나오며, 이는 실제로 다음 노름을 줍니다

$$\langle \chi_{\text{refl}_0}, \chi_{\text{refl}_0} \rangle = \frac{1}{4!} \left( \underbrace{3^2}_{\text{id}} + \underbrace{6 \cdot (1)^2}_{(\bullet\bullet)} + \underbrace{8 \cdot (0)^2}_{(\bullet\bullet\bullet)} + \underbrace{6 \cdot (-1)^2}_{(\bullet\bullet\bullet\bullet)} + \underbrace{3 \cdot (-1)^2}_{(\bullet\bullet)(\bullet\bullet)} \right) = 1.$$

이것을 부호 표현과 텐서곱하여 또 다른 기약 표현을 얻을 수도 있음에 주목하십시오 ( $\mathbb{C}_{\text{sign}}$ 의 모든 대각합이  $\pm 1$ 이므로 노름이 변하지 않습니다). 마지막으로, 직교성을 이용해 마지막 행을 복원합니다 (더 나은 이름이 없어  $\mathbb{C}^2$ 라고 부릅니다); 따라서 완성된 표는 다음과 같습니다.

| $S_4$                                            | 1 | (••) | (•••) | (••••) | (••)(••) |
|--------------------------------------------------|---|------|-------|--------|----------|
| $\mathbb{C}_{\text{triv}}$                       | 1 | 1    | 1     | 1      | 1        |
| $\mathbb{C}_{\text{sign}}$                       | 1 | -1   | 1     | -1     | 1        |
| $\mathbb{C}^2$                                   | 2 | 0    | -1    | 0      | 2        |
| $\text{refl}_0$                                  | 3 | 1    | 0     | -1     | -1       |
| $\text{refl}_0 \otimes \mathbb{C}_{\text{sign}}$ | 3 | -1   | 0     | 1      | -1       |

**§21.5 생각해 볼 만한 조금 더 어려운 문제**

**문제 21A<sup>†</sup>** (지표표로부터 분해 읽어내기).  $W$ 를 유한군  $G$ 의 복소 표현이라 하십시오.  $V_1, \dots, V_r$ 을  $G$ 의 복소 기약 표현들이라 하고  $n_i = \langle \chi_W, \chi_{V_i} \rangle$ 로 두십시오. 각  $n_i$ 가 음이 아닌 정수이며 다음이 성립함을 증명하십시오

$$W = \bigoplus_{i=1}^r V_i^{\oplus n_i}.$$

**문제 21B.**  $G = S_4$ 의 복소 표현들을 생각하십시오. 표현  $\text{refl}_0 \otimes \text{refl}_0$ 은 9차원이므로 명백히 기약입니다. 이를 다섯 개의 기약 표현들로 분해하십시오.

**문제 21C** (일차원 기약 표현과의 텐서곱).  $V$ 와  $W$ 를  $G$ 의 기약 표현이라 하고,  $\dim W = 1$ 이라 하십시오.  $V \otimes W$ 가 기약임을 보이십시오.

**문제 21D** (사원수군). 사원수군  $Q_8$ 의 지표표를 계산하십시오.



**문제 21E\*** (제2 직교성 공식).  $g$ 와  $h$ 를 유한군  $G$ 의 원소라 하고,  $V_1, \dots, V_r$ 을  $G$ 의 기약 표현들이라 하십시오. 다음을 증명하십시오

$$\sum_{i=1}^r \chi_{V_i}(g) \overline{\chi_{V_i}(h)} = \begin{cases} |C_G(g)| & g \text{와 } h \text{가 켄레일 경우} \\ 0 & \text{그 외의 경우.} \end{cases}$$

여기서  $C_G(g) = \{x \in G : xg = gx\}$ 는  $g$ 의 중심화군입니다.



# 22 몇 가지 응용

이 모든 준비를 마쳤으니, 이제 그 자체로 흥미로운 몇 가지 좋은 결과를 전개해 보겠습니다.

## §22.1 프로베니우스 나눗셈성

### 정리 22.1.1 (프로베니우스 나눗셈성)

$V$ 가 유한군  $G$ 의 복소 기약표현이라 합시다. 그러면  $\dim V$ 는  $|G|$ 를 나눕니다.

이 증명에는 대수적 정수(대수적 수론 장에서 다룰 개념)가 필요합니다. 대수적 정수란 정수 계수를 갖는 모닉 다항식의 근이 되는 복소수를 말하며, 이러한 대수적 정수들은 덧셈과 곱셈에 대해 환  $\mathbb{Z}$ 를 이루고,  $\mathbb{Z} \cap \mathbb{Q} = \mathbb{Z}$ 임을 상기합니다.

먼저 다음을 증명합니다:

### 보조정리 22.1.2 ( $\mathbb{Z}[G]$ 의 원소는 정수적입니다)

$\alpha \in \mathbb{Z}[G]$ 라 합시다. 그러면 정수 계수를 갖는 모닉 다항식  $P$ 가 존재하여  $P(\alpha) = 0$ 이 성립합니다.

증명.  $A_k$ 를  $1, \alpha^1, \dots, \alpha^k$ 의  $\mathbb{Z}$ -생성 공간이라 합시다.  $\mathbb{Z}[G]$ 가 뇌터 환이므로, 포함 관계  $A_0 \subseteq A_1 \subseteq A_2 \subseteq \dots$ 가 모두 진부분일 수는 없으며, 따라서 어떤  $k$ 에 대해  $A_k = A_{k+1}$ 이 성립합니다. 이는  $\alpha^{k+1}$ 이  $\alpha$ 의 더 낮은 거듭제곱들로 표현될 수 있음을 의미합니다.  $\square$

프로베니우스 나눗셈성의 증명.  $C_1, \dots, C_m$ 이  $G$ 의 켈레류를 나타낸다고 합시다. 그러면

$$\frac{|G|}{\dim V};$$

를 생각해 봅시다. 우리는 이것이 대수적 정수임을 보일 것이며, 이로써 정리가 증명됩니다. 이를 다음과 같이 다시 쓸 수 있음을 관찰합니다

$$\frac{|G|}{\dim V} = \frac{|G| \langle \chi_V, \chi_V \rangle}{\dim V} = \sum_{g \in G} \frac{\chi_V(g) \overline{\chi_V(g)}}{\dim V}.$$

켈레류에 대한 합을 나누면, 따라서

$$\frac{|G|}{\dim V} = \sum_{i=1}^m \overline{\chi_V(C_i)} \cdot \frac{|C_i| \chi_V(C_i)}{\dim V}.$$

우리는 모든  $i$ 에 대해 다음이

$$\frac{|C_i| \chi_V(C_i)}{\dim V} = \frac{1}{\dim V} \text{Tr } T_i$$

대수적 정수임을 주장합니다, 여기서

$$T_i := \rho \left( \sum_{h \in C_i} h \right).$$

이를 확인하기 위해,  $T_i$ 가  $G$ 의 원소들과 가환임에 주목하면, 따라서  $T_i$ 는 뒤영킴 연산자  $T_i: V \rightarrow V$ 가 됩니다. 따라서 슈어의 보조정리에 의해  $T_i = \lambda_i \cdot \text{id}_V$ 이고  $\text{Tr } T_i = \lambda_i \dim V$ 입니다. **보조정리 22.1.2**에 의해  $\lambda_i \in \mathbb{Z}$ 이며, 원하는 결과를 얻습니다.

이제  $\overline{\chi_V(C_i)} \in \mathbb{Z}$  또한 성립하므로 (이는 단위근의 켤레들의 합이기 때문입니다) 증명이 끝났습니다. 따라서  $\frac{|G|}{\dim V}$ 는 대수적 정수들의 곱의 합이며, 그 자체로 대수적 정수입니다.  $\square$

## §22.2 번사이드의 정리

이제 군론적 결과를 증명합니다. 이 결과는 순수하게 군론적이기 때문에(마치 RSA가 정수론의 대표적 사례이듯) 표현론의 유명한 대표적 사례입니다.

군이 정규 부분군을 갖지 않으면 **단순**하다는 것을 상기합니다. 사실, 우리는 다음을 증명할 것입니다:

### 정리 22.2.1 (번사이드)

$G$ 가 위수  $p^a q^b$ 인 비아벨 군이라 합시다(여기서  $p, q$ 는 서로 다른 소수이고  $a, b \geq 0$ 입니다). 그러면  $G$ 는 단순하지 않습니다.

이어지는 내용에서  $p$ 와  $q$ 는 항상 소수를 나타냅니다.

### 보조정리 22.2.2 ( $\gcd(|C|, \dim V) = 1$ 에 관하여)

$V = (V, \rho)$ 가  $G$ 의 복소 기약표현이라 합시다.  $C$ 가  $\gcd(|C|, \dim V) = 1$ 을 만족하는  $G$ 의 켤레류라고 가정합니다. 그러면 임의의  $g \in C$ 에 대해, 다음 중 하나가 성립합니다

- $\rho(g)$ 가 스칼라에 의한 곱셈이거나, 또는
- $\chi_V(g) = \text{Tr } \rho(g) = 0$ .

증명.  $\varepsilon_i$ 가  $\rho(g)$ 의  $n$ 개 고윳값(단위근들)이라면, 프로베니우스 나눗셈성의 증명으로부터  $\frac{|C|}{n} \chi_V(g) \in \mathbb{Z}$ 임을 알 수 있으며, 따라서  $\gcd(|C|, n) = 1$ 로부터 다음을 얻습니다

$$\frac{1}{n} \chi_V(g) = \frac{1}{n} (\varepsilon_1 + \cdots + \varepsilon_n) \in \mathbb{Z}.$$

이는 대수적 수론의 한 사실, 즉 **문제 53C\***로부터 쉽게 따라 나옵니다:  $\varepsilon_1 = \cdots = \varepsilon_n$  (첫 번째 경우)이거나  $\varepsilon_1 + \cdots + \varepsilon_n = 0$  (두 번째 경우)입니다.  $\square$

### 보조정리 22.2.3 (단순군은 소수의 거듭제곱 크기의 켤레류를 갖지 않습니다)

$G$ 를 유한 단순군이라 합시다. 그러면  $G$ 는 크기가  $p^k$  ( $k > 0$ )인 켤레류를 가질 수 없습니다.

증명. 귀류법으로 증명합니다.  $C$ 가 그러한 켤레류라 가정하고, 임의의  $g \in C$ 를 고정합니다.  $g$ 와  $1_G$  ( $g \neq 1_G$ 이므로 켤레가 아닙니다)에 대해 두 번째 직교성 공식(**문제 21E\***)을 적용하면 다음을 얻습니다.

$$\sum_{i=1}^r \dim V_i \chi_{V_i}(g) = 0$$

여기서  $V_i$ 는 평소와 같이  $G$ 의 모든 기약 표현입니다.

**연습문제 22.2.4.**  $p \nmid \dim V$ 이고  $\chi_V(g) \neq 0$ 인 자명하지 않은 기약 표현  $V$ 가 존재함을 보이십시오. (그렇지 않다면  $-\frac{1}{p} \in \mathbb{Z}$ 가 됨을 귀류법으로 보이면서 진행하십시오.)

$V = (V, \rho)$ 를 앞서 언급한 기약 표현이라 합시다. 앞의 보조정리에 의해, 이제  $\rho(g)$ 가  $V$ 에서 스칼라로 작용함을 알 수 있습니다.

이제 다음 부분군을 생각해 봅시다.

$$H = \langle ab^{-1} \mid a, b \in C \rangle \subseteq G.$$

우리는 이것이  $G$ 의 자명하지 않은 정규 부분군임을 주장합니다.  $H$ 가 정규임을 확인하는 것은 쉬우며,  $|C| > 1$ 이므로  $H$ 가 자명하지 않음을 알 수 있습니다.  $V$ 로 표현되었을 때  $H$ 의 각 원소는  $V$ 에 자명하게 작용하므로,  $V$ 가 자명하지 않고 기약적이기 때문에  $H \neq G$ 입니다. 이는  $G$ 가 단순군이라는 가정에 모순됩니다.  $\square$

이 보조정리를 이용하면, 우리 군의  $|G|$ 개 원소를 켈레류로 분할함으로써 번사이드 정리가 따라 나옵니다. 귀류법을 위해  $G$ 가 단순군이라 가정합니다. 각 켈레류는 크기가 1이거나 (문제 16D\*에 의해 이러한 것이  $|Z(G)|$ 개 있습니다) 앞의 보조정리에 의해  $pq$ 로 나누어 떨어져야 하는데, 반면 그 합은  $|G| = p^a q^b$ 와 같습니다. 따라서  $|Z(G)| > 1$ 이어야 합니다. 그러나  $G$ 는 아벨 군이 아니므로  $Z(G) \neq G$ 이며, 따라서 중심  $Z(G)$ 는 자명하지 않은 정규 부분군이 되어,  $G$ 가 단순군이라는 가정에 모순됩니다.

## §22.3 프로베니우스 행렬식

표현론이라는 분야를 시작하게 만든 다음 문제로 마무리하겠습니다. 유한군  $G$ 가 주어지면,  $n$ 개의 변수  $\{x_g\}_{g \in G}$ 를 만들고,  $(g, h)$ 번째 성분이  $x_{gh^{-1}}$ 인  $n \times n$  행렬  $M_G$ 를 만듭니다.

**예제 22.3.1** (프로베니우스 행렬식들)

(a)  $G = \mathbb{Z}/2\mathbb{Z} = \langle T \mid T^2 = 1 \rangle$ 이라면 행렬은 다음과 같을 것입니다

$$M_G = \begin{bmatrix} x_{\text{id}} & x_T \\ x_T & x_{\text{id}} \end{bmatrix}.$$

그러면  $\det M_G = (x_{\text{id}} - x_T)(x_{\text{id}} + x_T)$ 입니다.

(b)  $G = S_3$ 이라면, 긴 계산을 통해  $\det M_G$ 의 기약 인수분해는 다음과 같이 주어집니다

$$\left( \sum_{\sigma \in S_3} x_\sigma \right) \left( \sum_{\sigma \in S_3} \text{sign}(\sigma) x_\sigma \right) \left( F(x_{\text{id}}, x_{(123)}, x_{(321)}) - F(x_{(12)}, x_{(23)}, x_{(31)}) \right)^2$$

여기서  $F(a, b, c) = a^2 + b^2 + c^2 - ab - bc - ca$ 이며, 뒤의 인수는 기약입니다.

**정리 22.3.2 (프로베니우스 행렬식)**

( $|G|$ 개의 변수로 이루어진) 다항식  $\det M_G$ 는 기약 다항식들의 곱으로 인수분해되며, 이때

- (i) 다항식의 개수는  $G$ 의 켤레류의 개수와 같으며,
- (ii) 각 다항식의 중복도는 그 차수와 같습니다.

”제곱의 합” 결과가 이와 어떻게 관련되는지 여러분은 이미 짐작할 수 있을지도 모릅니다! (실제로  $\deg \det M_G$ 를 살펴보십시오.)

전설에 따르면 데데킨트가 1896년에 이 현상을 처음 관찰했다고 합니다. 그는 이를 일반적으로 증명하는 방법을 알지 못했기에, 이를 편지에 담아 프로베니우스에게 보냈고, 프로베니우스는 이 문제를 풀기 위해 표현론을 창시했습니다.

지금까지 구축한 모든 도구를 이용하면, 이제 이 결과를 증명하는 것은 상당히 간단합니다.

증명.  $V = (V, \rho) = \text{Reg}(\mathbb{C}[G])$ 라 하고,  $V_1, \dots, V_r$ 을  $G$ 의 기약 표현들이라 합시다.  $\mathbb{C}[G]$ 의 통상적인 기저에서 행렬  $M_G$ 를 갖는 사상  $T: \mathbb{C}[G] \rightarrow \mathbb{C}[G]$ 를 생각해 봅시다. 즉

$$T: T(\{x_g\}_{g \in G}) = \sum_{g \in G} x_g \rho(g) \in \text{Mat}(V).$$

따라서 우리는  $\det T$ 를 살펴보고자 합니다.

하지만 이전과 같이  $V = \bigoplus_{i=1}^r V_i^{\oplus \dim V_i}$ 임을 알고 있으므로,  $T$ 를 그 부분공간들에 대해 분해하면 다음을 알 수 있습니다

$$\det T = \prod_{i=1}^r (\det(T|_{V_i}))^{\dim V_i}.$$

따라서 우리는 두 가지만 보이면 됩니다: 다항식  $\det T_{V_i}$ 가 기약이라는 것, 그리고 서로 다른  $i$ 에 대해 이들이 쌍마다 서로 다르다는 것입니다.

$V_i = (V_i, \rho)$ 라 하고,  $k = \dim V_i$ 라 둡시다.

- 기약성: 조밀성 정리에 의해, 임의의  $M \in \text{Mat}(V_i)$ 에 대해 복소수  $x_g \in G$ 의 특정한 선택이 존재하여 다음을 만족합니다

$$M = \sum_{g \in G} x_g \cdot \rho_i(g) = (T|_{V_i})(\{x_g\}).$$

$\rho_i(g)$ 를 복소수 계수를 갖는  $k \times k$  행렬로 봅시다. 따라서 다항식 항목을 갖는 행렬로 본 “일반적인”  $(T|_{V_i})(\{x_g\})$ 는 선형독립인 항목들을 가져야 합니다(그렇지 않으면 우리가 도달할 수 없는  $\text{Mat}(V_i)$ 의 어떤 행렬이 존재하게 됩니다).

그러면 이 주장은 (선형 변수 변환을 통해)  $m^2$ 개의 변수로 이루어진 다항식  $\det(y_{ij})_{1 \leq i, j \leq m}$ 이 항상 기약이라는 단순한 사실로부터 따라옵니다.

- 쌍마다 서로 다름:  $\det T|_{V_i}(\{x_g\})$ 로부터 지표  $\chi_{V_i}$ 를 읽어낼 수 있음을 보여, 이 주장을 증명하겠습니다. 실제로

**연습문제 22.3.3.**  $V_i$ 에 대해 임의의 기저를 택합시다.  $\dim V_i = k$ 이고  $1_G \neq g \in G$ 이면, 다음이 성립합니다

$$\chi_{V_i}(g) \text{의 계수입니다 } x_g x_{1_G}^{k-1}.$$

따라서 증명이 완료됩니다. □

# VII

양자 알고리즘

## 제VII부: 목차

---

|           |                                |            |
|-----------|--------------------------------|------------|
| <b>23</b> | <b>양자 상태와 측정</b>               | <b>271</b> |
| 23.1      | 브라-켓 표기법 . . . . .             | 271        |
| 23.2      | 상태 공간 . . . . .                | 272        |
| 23.3      | 관찰 . . . . .                   | 272        |
| 23.4      | 얽힘 . . . . .                   | 275        |
| 23.5      | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 278        |
| <br>      |                                |            |
| <b>24</b> | <b>양자 회로</b>                   | <b>279</b> |
| 24.1      | 고전 논리 게이트 . . . . .            | 279        |
| 24.2      | 가역 고전 논리 . . . . .             | 280        |
| 24.3      | 양자 논리 게이트 . . . . .            | 282        |
| 24.4      | 도이치-조사 알고리즘 . . . . .          | 284        |
| 24.5      | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 285        |
| <br>      |                                |            |
| <b>25</b> | <b>쇼어 알고리즘</b>                 | <b>287</b> |
| 25.1      | 고전적인 (역) 푸리에 변환 . . . . .      | 287        |
| 25.2      | 양자 푸리에 변환 . . . . .            | 288        |
| 25.3      | 쇼어 알고리즘 . . . . .              | 290        |

---

# 23 양자 상태와 측정

이 장에서는 선형대수를 사용하여 양자 상태를 설정하는 방법을 설명하겠습니다. 이를 통해 다음 장에서 양자 회로에 대해 이야기할 수 있게 되며, 이는 쇼어 알고리즘을 위한 무대를 마련할 것입니다.

저는 물리학을 아주 많이 다루지는 않을 것입니다 (사실은: 전혀 다루지 않을 것입니다). 즉, 물리적 실재가 무엇인지를 선형대수의 언어로만 서술하고, 왜 이것이 참인지에 대한 철학적 논의는 여러분 주변의 "양자역학의 철학" 강의(MIT에서는 "사회과학" 과목입니다!)에 맡기겠습니다.

## §23.1 브라-켓 표기법

물리학자들은 벡터에 대해 자신들만의 표기법을 가지고 있습니다: 앞서 저는  $v$ ,  $e_1$  등과 같은 표기를 사용했지만, 이 장에서는 악명 높은 **브라-켓(bra-ket)** 표기법을 보게 될 것입니다: 벡터는  $|\bullet\rangle$ 로 표기되며, 여기서  $\bullet$ 은 어떤 변수 이름입니다: 수학이나 파이썬에서와 달리, 이는 숫자, 기호, 유니코드 문자 등 무엇이든 포함할 수 있습니다. 이를 "켓(ket)"이라고 부릅니다. 모든 물리학자들에게 경의를 표하기 위해, 이 장에서도 이 표기법을 사용하겠습니다.

**표기의 남용 23.1.1** (이 부분에서는  $\dim H < \infty$ 입니다). 양자 계산에 관한 이 부분에서는 앞서 정의한 "힐베르트 공간"이라는 용어를 사용할 것이지만, 실제로는 우리가 다루는 모든 힐베르트 공간이 유한 차원일 것입니다.

$\dim H = n$ 이면, 그 정규직교 기저 원소들은 흔히 다음과 같이 표기됩니다

$$|0\rangle, |1\rangle, \dots, |n-1\rangle$$

( $e_i$  대신) 그리고  $H$ 의 일반적인 원소는 다음과 같이 표기됩니다

$$|\psi\rangle, |\phi\rangle, \dots$$

그리고 다양한 다른 그리스 문자들로 표기됩니다.

이제 임의의  $|\psi\rangle \in H$ 에 대해,  $H^\vee$  안에서 표준적인 쌍대 원소를 생각할 수 있는데 ( $H$ 가 내적 형식을 가지고 있으므로), 이를  $\langle\psi|$  ("브라")로 표기합니다. 예를 들어,  $\dim H = 2$ 이면 다음과 같이 쓸 수 있습니다

$$|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

정규직교 기저에서, 이 경우

$$\langle\psi| = [\bar{\alpha} \quad \bar{\beta}].$$

이 표기법으로 내적을 간결하게 쓸 수도 있습니다.  $|\phi\rangle = \begin{bmatrix} \gamma \\ \delta \end{bmatrix}$  일 때,  $\langle\psi|$ 와  $|\phi\rangle$ 의 내적은 다음과 같이 주어집니다.

$$\langle\psi|\phi\rangle = [\bar{\alpha} \quad \bar{\beta}] \begin{bmatrix} \gamma \\ \delta \end{bmatrix} = \bar{\alpha}\gamma + \bar{\beta}\delta.$$

따라서 좀 더 수학적인  $\langle|\psi\rangle, |\phi\rangle\rangle$  대신  $\langle\psi|\phi\rangle$ 라는 표기법을 사용하겠습니다. 특히  $|\psi\rangle$ 의 노름의 제곱은 그냥  $\langle\psi|\psi\rangle$ 입니다. 구체적으로  $\dim H = 2$ 일 때  $\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2$ 입니다.

## §23.2 상태 공간

이것이 이상하다고 생각하신다면, 상황은 더 심해집니다.

고전 계산에서 비트는 0 또는 1입니다. 더 일반적으로,  $n$ 개의 가능한 상태  $0, \dots, n-1$ 로 이루어진 고전적 공간을 생각할 수 있습니다. 따라서 고전적인 상황에서 가능한 상태들의 공간은 단순히  $n$ 개의 원소를 가진 이산 집합입니다.

양자 계산에서 **큐비트(qubit)**는 그 대신 0과 1의 임의의 복소 선형 결합입니다. 정확히 말하면, 다음과 같은 노름을 가진 복소 벡터 공간을 생각해봅시다

$$H = \mathbb{C}^2$$

그리고 정규직교 기저 원소들을  $|0\rangle$ 과  $|1\rangle$ 로 표기합니다. 그러면 큐비트는 영이 아닌 원소  $|\psi\rangle \in H$ 이며, 다음과 같은 형태로 쓸 수 있습니다

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

여기서  $\alpha$ 와  $\beta$ 는 둘 다 영이 아닙니다. 일반적으로  $|\psi\rangle$ 의 노름이 1이 되도록 정규화합니다:

$$\langle\psi|\psi\rangle = 1 \iff |\alpha|^2 + |\beta|^2 = 1.$$

특히,  $|0\rangle \in H$ 와  $|1\rangle \in H$ 로 "고전적인" 상황을 복원할 수 있지만, 이제는

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

과 같은 몇몇 "중간적인" 상태들도 존재합니다. 철학적으로 보면, 일어난 일은 다음과 같습니다:

$|0\rangle$ 과  $|1\rangle$ 이라는 상태만 허용하는 대신, 이들의 임의의 복소 선형 결합을 허용합니다.

더 일반적으로,  $\dim H = n$ 이면 가능한 상태들은 영이 아닌 원소들입니다

$$c_0|0\rangle + c_1|1\rangle + \dots + c_{n-1}|n-1\rangle$$

이는 보통  $|c_0|^2 + |c_1|^2 + \dots + |c_{n-1}|^2 = 1$ 이 되도록 정규화합니다.

## §23.3 관찰

**이 절의 대표적인 예:** id은 모든 고윳값이 같으므로 측정을 하지 않는 것에 대응하지만, 서로 다른 고윳값을 가진 연산자는 어떤 것이든 붕괴를 일으킵니다.

이것이 이상하다고 생각한다면, 더 이상한 것이 있습니다. 먼저 선형대수 복습입니다(**정의 15.5.1**):

**정의 23.3.1.**  $V$ 를 유한 차원 내적 공간이라 합시다. 사상  $T: V \rightarrow V$ 에 대해 다음 조건들은 동치입니다.

- 임의의  $x, y \in V$ 에 대해  $\langle Tx, y \rangle = \langle x, Ty \rangle$ 입니다.
- $T = T^\dagger$ .

이러한 조건을 만족하는 사상  $T$ 를 **에르미트**라고 부릅니다.

**질문 23.3.2.**  $T$ 가 정규임을 보이십시오.

따라서  $T$ 가 내적 형식에 대해 대각화 가능함을 알 수 있으므로, 적당한 기저에 대해 정규직교기저로 다음과 같이 쓸 수 있습니다

$$T = \begin{bmatrix} \lambda_0 & 0 & \dots & 0 \\ 0 & \lambda_1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_{n-1} \end{bmatrix}.$$

앞서 말했듯이, 이는 대단합니다: 고유벡터로 이루어진 기저를 가질 뿐만 아니라, 고유벡터들이 쌍마다 직교하므로  $V$ 의 정규직교기저를 이룹니다.

**질문 23.3.3.**  $T$ 의 모든 고윳값이 실수임을 보이십시오. ( $T = T^\dagger$ .)

다시 양자 계산으로 돌아갑시다.  $\dim H = 2$ 인  $H$ 에서 상태  $|\psi\rangle \in H$ 가 있다고 합시다; 아직 특정 기저를 구분하지 않았으므로 그저 0이 아닌 벡터를 가지고 있는 것입니다. 그러면 관측이 작동하는 방식은 (이는 물리학이므로 제 말을 믿을 수밖에 없습니다) 다음과 같습니다:

**에르미트 연산자  $T: H \rightarrow H$ 를 하나 고릅니다; 그러면  $T$ 에 대한 관측은  $T$ 의 고윳값을 반환합니다.**

정확히 말하면:

- 에르미트 연산자  $T: H \rightarrow H$ 를 하나 고르며, 이를 **관측가능량**이라 부릅니다.
- 그 고윳값  $\lambda_0, \dots, \lambda_{n-1}$ 과 이에 대응하는 고유벡터  $|0\rangle_T, \dots, |n-1\rangle_T$ 을 생각합니다. 암묵적으로  $|0\rangle_T, \dots, |n-1\rangle_T$ 이  $H$ 의 정규직교기저를 이룬다고 가정할 수 있습니다. (아래첨자  $T$ 는  $T$ 의 고유벡터를  $H$ 의 기저 원소와 구별하기 위한 것입니다.)
- $|\psi\rangle$ 를 정규직교기저로 다음과 같이 씁니다

$$c_0 |0\rangle_T + c_1 |1\rangle_T + \dots + c_{n-1} |n-1\rangle_T.$$

- 그러면  $\lambda_i$ 를 관측할 확률은

$$\frac{|c_i|^2}{|c_0|^2 + \dots + |c_{n-1}|^2}.$$

이를  **$T$ 를 따른 관측**을 한다고 부릅니다.

특히, 0이 아닌 임의의 상수  $c$ 에 대해  $|\psi\rangle$ 와  $c|\psi\rangle$ 는 구별할 수 없다는 점에 주목하십시오. 이것이 우리가  $|\psi\rangle$ 를 정규화하기를 선호하는 이유입니다. 하지만 가장 기이한 점은  $|\psi\rangle$ 에 일어나는 일입니다: 이를 측정함으로써 우리는 실제로 정보를 파괴합니다. 이러한 현상을 **양자 붕괴**라고 부릅니다.

- 간단히, 우리가  $|\psi\rangle$ 를  $T$ 로 관측하여 고윳값  $\lambda$ 를 얻었고,  $|i\rangle_T$ 가 이 고윳값을 갖는 유일한 고유벡터라고 합시다. 그러면 상태  $|\psi\rangle$ 는 상태  $c_i |i\rangle_T$ 로 붕괴합니다: 나머지 정보는 모두 파괴됩니다. (사실, 다시 상수배는 중요하지 않으므로  $|i\rangle_T$ 로 붕괴한다고 말해도 무방합니다.)

- 더 일반적으로,  $\lambda$ 를 관측했다면, 일반화된 고유공간  $H_\lambda$  (즉 같은 고윳값을 갖는 고유 벡터들의 생성 공간)를 생각합시다. 그러면 물리적 상태  $|\psi\rangle$  또한 변화합니다: 이제 고유공간  $H_\lambda$  위로 사영된 것입니다. 다시 말해, 관측 이후 상태는 다음으로 붕괴합니다

$$\sum_{\substack{0 \leq i \leq n-1 \\ \lambda_i = \lambda}} c_i |i\rangle_T.$$

다시 말해,

**측정을 수행하면, 서로 다른 고유공간에서 온 계수들은 파괴됩니다.**

왜 이런 일이 일어날까요? 저도 모릅니다... 물리학은 (따라서 현실도) 이상합니다. 하지만 어쨌든, 예시를 들어보겠습니다.

#### 예제 23.3.4 (상태 $|\psi\rangle$ 의 양자 측정)

$H = \mathbb{C}^{\oplus 2}$ 이고 정규직교 기저  $|0\rangle, |1\rangle$ 을 가진다고 합시다. 그리고 다음 상태를 고려합시다.

$$|\psi\rangle = \frac{i}{\sqrt{5}} |0\rangle + \frac{2}{\sqrt{5}} |1\rangle = \begin{bmatrix} i/\sqrt{5} \\ 2/\sqrt{5} \end{bmatrix} \in H.$$

(a)

$$T = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

라고 합시다. 이는 고유벡터  $|0\rangle = |0\rangle_T$ 와  $|1\rangle = |1\rangle_T$ 를 가지며, 고윳값은 각각  $+1$ 과  $-1$ 입니다. 따라서  $|\psi\rangle$ 를  $T$ 에 대해 측정하면  $1/5$ 의 확률로  $+1$ 을,  $4/5$ 의 확률로  $-1$ 을 얻습니다. 이 측정 이후, 원래 상태는  $+1$ 을 측정했다면  $|0\rangle$ 으로,  $-1$ 을 측정했다면  $|1\rangle$ 으로 붕괴합니다. 따라서 우리는 원래의 확률을 결코 알아낼 수 없습니다.

(b) 이제  $T = \text{id}$ 을 고려하고, 정규직교 고유벡터  $|0\rangle_T, |1\rangle_T$ 를 임의로 선택합시다. 그러면  $\psi = c_0 |0\rangle_T + c_1 |1\rangle_T$ 입니다.  $T$ 의 모든 고윳값이  $+1$ 이므로, 우리가 무엇을 하든 측정 결과는 항상  $+1$ 입니다. 하지만 붕괴 역시 일어나지 않는데, 계수 중 어느 것도 소멸되지 않기 때문입니다.

(c) 이제 다음을 생각해봅시다

$$T = \begin{bmatrix} 0 & 7 \\ 7 & 0 \end{bmatrix}.$$

정규화된 두 고유벡터는 다음과 같습니다

$$|0\rangle_T = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad |1\rangle_T = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

고윳값은 각각  $+7$ 과  $-7$ 입니다. 이 기저에서 우리는 다음을 얻습니다

$$|\psi\rangle = \frac{2+i}{\sqrt{10}} |0\rangle_T + \frac{-2+i}{\sqrt{10}} |1\rangle_T.$$

따라서 우리는 확률  $\frac{1}{2}$ 로  $+7$ 을 얻고 확률  $\frac{1}{2}$ 로  $-7$ 을 얻으며, 측정 후  $|\psi\rangle$ 는  $|0\rangle_T$ 와  $|1\rangle_T$  중 하나로 붕괴합니다.

**질문 23.3.5.**  $|\psi\rangle$ 를  $T$ 로 측정하여  $\lambda$ 를 얻었다고 합시다.  $T$ 로 다시 측정하면 무슨 일이 일어날까요?

$H = \mathbb{C}^{\oplus 2}$ 의 경우, 이른바 **파울리 행렬**을 이용하여 더 많은 종류의 예시를 만들어낼 수 있습니다. 이것은 다음 세 개의 에르미트 행렬입니다

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}.$$

이 행렬들이 중요한 이유는 다음과 같습니다

**질문 23.3.6.** 이 세 행렬과 항등 행렬이 함께 에르미트  $2 \times 2$  행렬 집합의 기저를 이룸을 보이십시오.

그러므로 파울리 행렬은 자연스러운 기저 선택입니다.<sup>1</sup>

이들의 정규화된 고유벡터는 다음과 같습니다

$$\begin{aligned} |\uparrow\rangle = |0\rangle &= \begin{bmatrix} 1 \\ 0 \end{bmatrix} & |\downarrow\rangle = |1\rangle &= \begin{bmatrix} 0 \\ 1 \end{bmatrix} \\ |\rightarrow\rangle &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} & |\leftarrow\rangle &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \\ |\otimes\rangle &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix} & |\odot\rangle &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -i \end{bmatrix} \end{aligned}$$

이를 각각 “ $z$ -업”, “ $z$ -다운”, “ $x$ -업”, “ $x$ -다운”, “ $y$ -업”, “ $y$ -다운”이라 부릅니다. (고윳값은 “업”의 경우  $+1$ 이고 “다운”의 경우  $-1$ 입니다.) 따라서 상태  $|\psi\rangle \in \mathbb{C}^{\oplus 2}$ 가 주어지면, 해당하는 파울리 행렬을 사용하여 이 세 기저 중 어느 것에 대해서든 측정을 할 수 있습니다.

이를 고려하면, 앞선 예시들은 (a)  $\sigma_z$ 를 따라 측정하는 것, (b)  $\text{id}$ 을 따라 측정하는 것, (c)  $7\sigma_x$ 를 따라 측정하는 것이었습니다.

만약 상태  $|\psi\rangle$ 가 주어지고, 그것이  $|\rightarrow\rangle$  또는  $|\leftarrow\rangle$  중 하나(또는 다른 어떤 직교 상태들 중 하나)라고 미리 알려져 있다면, 우리는 어느 정도 고전적인 상황에 놓여 있음을 주목하십시오. 구체적으로,  $\sigma_x$ 를 따라 측정을 하면,  $|\psi\rangle$ 가 어느 상태였는지를 (100%의 확실성으로) 알아낼 수 있으며, 상태는 어떠한 붕괴도 겪지 않습니다. 따라서 직교 상태들은 신뢰성 있게 구별 가능합니다.

## §23.4 얽힘

**이 절의 대표적인 예:** 단일항 상태: 유령 같은 원격 작용.

그것이 이상하다고 생각한다면, 음, 더 심해집니다.

큐비트는 단순히 독립적으로 작동하지 않습니다. 큐비트는 텐서곱을 통해 서로 소통할 수 있습니다. 구체적으로,

$$H = \mathbb{C}^{\oplus 2} \otimes \mathbb{C}^{\oplus 2}$$

에 **문제 13D\***에서 설명한 노름을 부여한 것을 생각해봅시다. 이것은 공간  $H_A$ 에 있는 큐비트  $A$ 와 다른 공간  $H_B$ 에 있는 두 번째 큐비트  $B$ 가 어떤 방식으로 상호작용하도록 허용된 것으로 생각해야 하며,  $H = H_A \otimes H_B$ 는 두 큐비트 모두의 가능한 상태들의 집합입니다. 따라서

$$|0\rangle_A \otimes |0\rangle_B, \quad |0\rangle_A \otimes |1\rangle_B, \quad |1\rangle_A \otimes |0\rangle_B, \quad |1\rangle_A \otimes |1\rangle_B$$

<sup>1</sup>음, 물리학적 이유로 자연스럽습니다.

이것은  $H$ 의 정규직교 기저입니다. 여기서  $|i\rangle_A$ 는 첫 번째  $\mathbb{C}^{\oplus 2}$ 의 기저이고  $|i\rangle_B$ 는 두 번째  $\mathbb{C}^{\oplus 2}$ 의 기저이므로, 이 벡터들은 다른 모든 텐서곱에서와 마찬가지로 “서로 무관한” 것으로 생각해야 합니다. 순수 텐서는 정확히 여러분이 원하는 바를 의미합니다: 예를 들어  $|0\rangle_A \otimes |1\rangle_B$ 는 “큐비트  $A$ 에 대해서는 0, 큐비트  $B$ 에 대해서는 1”을 의미합니다.

앞서와 마찬가지로,  $H$ 에서 상태를 측정하려면 에르미트 사상  $H \rightarrow H$ 가 필요합니다. 특히, 큐비트  $B$ 만  $M_B$ 를 따라 측정하고자 한다면, 다음 연산자를 사용할 수 있습니다

$$\text{id}_A \otimes M_B$$

이 연산자의 고윳값은  $M_B$ 의 고윳값과 일치하며,  $\lambda$ 에 대한 고유공간은  $H_A \otimes (H_B)_\lambda$ 가 되므로, 사영을 취할 때  $A$  큐비트는 영향을 받지 않습니다.

이것은  $H$ 의 순수 텐서에 대해 여러분이 바라는 대로 작동합니다:

#### 예제 23.4.1 (얽히지 않은 두 큐비트)

큐비트  $A$ 가 상태  $\frac{i}{\sqrt{5}}|0\rangle_A + \frac{2}{\sqrt{5}}|1\rangle_A$ 에 있고 큐비트  $B$ 가 상태  $\frac{1}{\sqrt{2}}|0\rangle_B + \frac{1}{\sqrt{2}}|1\rangle_B$ 에 있다고 합시다. 그러면 두 큐비트를 함께 나타내는 것은 다음의 순수 텐서입니다

$$|\psi\rangle = \left( \frac{i}{\sqrt{5}}|0\rangle_A + \frac{2}{\sqrt{5}}|1\rangle_A \right) \otimes \left( \frac{1}{\sqrt{2}}|0\rangle_B + \frac{1}{\sqrt{2}}|1\rangle_B \right).$$

$|\psi\rangle$ 를 다음을 따라 측정한다고 합시다.

$$M = \text{id}_A \otimes \sigma_z^B.$$

고유공간 분해는 다음과 같습니다.

- $|0\rangle_A \otimes |0\rangle_B$ 와  $|1\rangle_A \otimes |0\rangle_B$ 의 생성 공간에 대해서는 +1이고,
- $|0\rangle_A \otimes |1\rangle_B$ 와  $|1\rangle_A \otimes |1\rangle_B$ 의 생성 공간에 대해서는 -1입니다.

(첫 번째 고유공간에 대해  $|\rightarrow\rangle_A \otimes |0\rangle_B$ 와  $|\leftarrow\rangle_A \otimes |0\rangle_B$  같은 다른 기저를 사용할 수도 있었지만, 상관없습니다.)  $|\psi\rangle$ 를 네 원소로 이루어진 기저로 전개하면, 첫 번째 고유공간을 얻을 확률은 다음과 같음을 알 수 있습니다.

$$\left| \frac{i}{\sqrt{10}} \right|^2 + \left| \frac{2}{\sqrt{10}} \right|^2 = \frac{1}{2}.$$

그리고 두 번째 고유공간을 얻을 확률도 마찬가지로  $\frac{1}{2}$ 입니다. ( $A$ 에 대한 계수가 아무 역할도 하지 않는다는 점에 주목하십시오!) 측정 후에는 다른 고유공간의 계수를 소거하며, 따라서 (재정규화 후) 다음과 같이 붕괴된 상태를 얻습니다.

$$\left( \frac{i}{\sqrt{5}}|0\rangle_A + \frac{2}{\sqrt{5}}|1\rangle_A \right) \otimes |0\rangle_B \quad \text{또는} \quad \left( \frac{i}{\sqrt{5}}|0\rangle_A + \frac{2}{\sqrt{5}}|1\rangle_A \right) \otimes |1\rangle_B$$

이번에도 각각 50%의 확률로 그렇게 됩니다.

따라서 이 모델을 사용하면 두 큐비트를 어느 정도 독립적으로 다룰 수 있습니다: 측정을 수행할 때는 그저 다른 큐비트를 건드리지 않도록(즉 항등 연산자에 대응하도록) 하면 됩니다.

**연습문제 23.4.2.** 이 예시에서  $|\psi\rangle$ 에  $\text{id}_A \otimes \sigma_x^B$ 를 적용하면 전혀 붕괴가 일어나지 않음을 보이십시오. 이 측정의 결과는 무엇입니까?

⊗를 계속 쓰기가 번거로워지므로, 다음과 같이 표기하기로 합니다.

**표기의 남용 23.4.3.** 앞으로  $|0\rangle_A \otimes |0\rangle_B$ 는 그냥  $|00\rangle$ 으로 줄여 쓰며,  $|01\rangle$ ,  $|10\rangle$ ,  $|11\rangle$ 도 마찬가지로 표기합니다.

**예제 23.4.4 (일반적인 2-큐비트 상태의 동시 측정)**

$H = \mathbb{C}^{\oplus 2} \otimes \mathbb{C}^{\oplus 2}$  안의 정규화된 상태  $|\psi\rangle$ 를 다음과 같이 생각해 봅시다.

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle.$$

다음을 만족하는 대각 행렬  $T: H \rightarrow H$ 를 따라 측정을 수행할 수 있습니다.

$$T(|00\rangle) = 0|00\rangle, \quad T(|01\rangle) = 1|01\rangle, \quad T(|10\rangle) = 2|10\rangle, \quad T(|11\rangle) = 3|11\rangle.$$

따라서 고윳값 0, 1, 2, 3을 각각 확률  $|\alpha|^2$ ,  $|\beta|^2$ ,  $|\gamma|^2$ ,  $|\delta|^2$ 로 얻게 됩니다. 그러므로 원한다면 한 큐비트를 측정할 때와 같은 방식으로 두 큐비트에 대해 "동시" 측정을 수행할 수 있습니다.

그러나 어떤 상태는 매우 기묘하게 행동합니다.

**예제 23.4.5 (단일항 상태)**

다음 상태를 생각해 봅시다.

$$|\Psi_-\rangle = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$$

이는 **단일항 상태**라고 불립니다.  $|\Psi_-\rangle$ 가 단순 텐서가 아님을 알 수 있는데, 이는 곧 이 상태가 두 큐비트가 나란히 놓인 것에 지나지 않는 게 아님을 의미합니다:  $H_A$ 와  $H_B$ 의 큐비트들이 얽힘(entangled) 상태가 된 것입니다.

이제 큐비트  $A$ 만을 측정하면 어떻게 될까요? 이는 다음 측정을 수행하는 것에 대응합니다.

$$T = \sigma_z^A \otimes \text{id}_B.$$

$T$ 의 고유공간 분해는 다음과 같이 기술할 수 있습니다.

- $|00\rangle$ 과  $|01\rangle$ 의 생성 공간, 고윳값 +1.
- $|10\rangle$ 과  $|11\rangle$ 의 생성 공간, 고윳값 -1.

따라서 다음 두 가지 중 하나가 일어날 것입니다.

- 확률  $\frac{1}{2}$ 로 +1을 측정하며, 붕괴된 상태는  $|01\rangle$ 입니다.
- 확률  $\frac{1}{2}$ 로 -1을 측정하며, 붕괴된 상태는  $|10\rangle$ 입니다.

그런데 이제  $A$ 를 따른 측정이 비트  $B$ 의 상태가 무엇인지를 완전히 알려주었다는 것을 알 수 있습니다!

$A$ 에 대한 측정만을 살펴봄으로써  $B$ 를 알게 되는데, 이 역설은 유령 같은 원격 작용, 아인슈타인의 표현으로는 **spukhafte Fernwirkung**이라고 불립니다. 따라서,

**힐베르트 공간의 텐서곱에서, 순수 텐서가 아닌 상태들은 "얽힌" 상태에 해당합니다.**

이것이 실제로 의미하는 바는 큐비트들을 독립적으로 기술할 수 없다는 것이며, 시스템의 상태는 전체로서 주어져야 한다는 것입니다. 이것이 바로 얽힌 상태가 의미하는 바입니다: 큐비트들은 어떤 식으로든 서로 의존합니다.

## §23.5 생각해 볼 만한 조금 더 어려운 문제

**문제 23A.**  $|\Psi_-\rangle$ 를  $\sigma_x^A \otimes \text{id}_B$ 로 측정하여  $+1$  또는  $-1$ 을 얻습니다. 이 측정으로부터 큐비트  $B$ 의 상태를 결정하십시오.

**문제 23B** (그린버거-혼-자일링거 역설).  $(\mathbb{C}^{\oplus 2})^{\otimes 3}$ 에서 다음 상태를 고려하십시오

$$|\Psi\rangle_{\text{GHZ}} = \frac{1}{\sqrt{2}} (|0\rangle_A |0\rangle_B |0\rangle_C - |1\rangle_A |1\rangle_B |1\rangle_C).$$

다음 각각을 따른 측정값을 구하십시오

$$\sigma_y^A \otimes \sigma_y^B \otimes \sigma_x^C, \quad \sigma_y^A \otimes \sigma_x^B \otimes \sigma_y^C, \quad \sigma_x^A \otimes \sigma_y^B \otimes \sigma_y^C, \quad \sigma_x^A \otimes \sigma_x^B \otimes \sigma_x^C.$$

역설에 관해서는: 이 모든 측정값을 서로 곱하면 무슨 일이 일어나는지 살펴보십시오.

# 24 양자 회로

이제 큐비트에 대해 논의했으므로, 이를 회로에서 사용하는 방법에 대해 이야기할 수 있습니다. 핵심적인 변화 — 그리고 양자 회로가 고전 회로로는 할 수 없는 일을 할 수 있는 이유 — 는 우리가 0과 1의 선형 결합을 허용한다는 사실입니다.

## §24.1 고전 논리 게이트

고전 논리에서는 몇 개의 비트를 입력으로 받아 몇 개의 비트를 출력으로 내놓는 회로를 만듭니다. 이러한 회로는 개별 논리 게이트들로 구성됩니다. 예를 들어, **AND 게이트**는 다음과 같이 그림으로 나타낼 수 있습니다.



AND 게이트는 “진리표”를 사용해서도 나타낼 수 있습니다:

| A | B | A그리고B |
|---|---|-------|
| 0 | 0 | 0     |
| 0 | 1 | 0     |
| 1 | 0 | 0     |
| 1 | 1 | 1     |

마찬가지로, **OR 게이트**와 **NOT 게이트**가 있습니다:

| A | B | A또는B |
|---|---|------|
| 0 | 0 | 0    |
| 0 | 1 | 1    |
| 1 | 0 | 1    |
| 1 | 1 | 1    |

| A | 부정A |
|---|-----|
| 0 | 1   |
| 1 | 0   |

또한 비트를 복제하는, 이른바 **COPY 게이트**도 있습니다.



물론, 이러한 게이트들에 대해 배우게 되는 첫 번째 정리는 다음과 같습니다:

### 정리 24.1.1 (AND, OR, NOT, COPY는 보편적입니다)

AND, OR, NOT, COPY라는 네 개의 게이트 집합은, 임의의 불 함수  $f: \{0,1\}^n \rightarrow \{0,1\}$ 을 오직 이 게이트들만을 사용한 회로로 구현할 수 있다는 의미에서 보편적입니다.

증명. 다소 시시하긴 하지만: 본질적으로  $f^{\text{pre}}(1)$ 에 속하는 모든 입력 문자열에 대해 OR를 취하는 회로를 적어 내려가면 됩니다. 예를 들어,  $n = 3$ 이고  $f(011) = f(110) = 1$ 이며 나머지는 0인 함수  $f(abc)$ 를 시뮬레이션하고자 한다고 합시다. 그러면  $f$ 에 대응하는 불 표현식은 단순히 다음과 같습니다

$$f(abc) = [(a \text{가 아님}) \text{ 그리고 } b \text{ 그리고 } c] \text{ 또는 } [a \text{ 그리고 } b \text{ 그리고 } (c \text{가 아님})].$$

분명히, 다른 어떤  $f$ 에 대해서도 같은 방식을 적용할 수 있으며, 이 논리를 회로로 구현할 수 있습니다.  $\square$

**비고 24.1.2** —  $x$  그리고  $y = \text{부정}((x \text{가 아님}) \text{또는} (y \text{아님}))$ 이므로, 실제로 AND 게이트를 없앨 수 있다는 결론이 따릅니다.

## §24.2 가역 고전 논리

이 절의 대표적인 예: *CNOT* 게이트, *Toffoli* 게이트.

양자역학의 목적을 위해서는, 이것만으로는 충분하지 않습니다. 이 유비를 끝까지 이어 가려면, 사실 **가역**인 게이트가 필요합니다. 즉 이 게이트들이 입력 공간에서 출력 공간으로 가는 전단사여야 한다는 뜻입니다. 특히, 그러한 게이트는 입력 비트 수와 출력 비트 수가 같아야 합니다.

### 예제 24.2.1 (가역 게이트)

- (a) AND, OR, COPY 게이트는 차원상의 이유로 모두 가역이 아닙니다.
- (b) 그러나 NOT 게이트는 가역입니다: 이는  $\{0, 1\} \rightarrow \{0, 1\}$ 인 전단사입니다.

### 예제 24.2.2 (CNOT 게이트)

제어형-NOT 게이트, 즉 **CNOT** 게이트는 다음과 같은 진리표를 갖는 가역 2비트 게이트입니다.

| 입력  | 출력  |
|-----|-----|
| 0 0 | 0 0 |
| 1 0 | 1 1 |
| 0 1 | 0 1 |
| 1 1 | 1 0 |

다시 말해, 이 게이트는 첫 번째 비트는 그대로 둔 채 두 번째 비트에 첫 번째 비트를 XOR합니다. 이는 다음과 같이 나타낼 수 있습니다.

$$\begin{array}{c} x \text{ --- } \bullet \text{ --- } x \\ y \text{ --- } \oplus \text{ --- } x + y \pmod 2 \end{array}$$

첫 번째 점은 “제어(control)”라고 불리며,  $\oplus$ 는 “부정(negation)” 연산입니다: 첫 번째 비트가 두 번째 비트를 뒤집을지 말지를 제어합니다. 따라서 전형적인 적용 예는 다음과 같을 수 있습니다.

$$\begin{array}{c} 1 \text{ --- } \bullet \text{ --- } 1 \\ 0 \text{ --- } \oplus \text{ --- } 1 \end{array}$$

그러므로, 두 비트에 대한 자명하지 않은 가역 게이트는 NOT과 CNOT뿐입니다.

이제 우리의 가역 게이트에 대해 보편적이라는 개념을 다르게 정의할 필요가 있습니다.

**정의 24.2.3.** 가역 게이트들의 집합이 불 함수  $f(x_1 \dots x_n)$ 을 **시뮬레이션**할 수 있다는 것은, 다음을 받아들이는 회로를 구현할 수 있는 경우를 말합니다

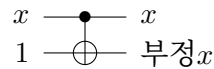
- 입력으로,  $x_1 \dots x_n$ 과 더불어 0 또는 1로 고정된 몇몇 비트를 사용하는데, 이를 **보조 비트**<sup>1</sup>라고 부릅니다.

<sup>1</sup>영어 단어 "ancilla"는 "하녀"를 의미합니다.

- 출력으로는, 입력 비트  $x_1, \dots, x_n$ 과 출력 비트  $f(x_1, \dots, x_n)$ , 그리고 경우에 따라 몇몇 추가 비트(이를 **쓰레기 비트**라고 부릅니다)가 있습니다.

어떤 임의의 불리언 함수든 시뮬레이션할 수 있다면 그 게이트(들)를 **보편적**이라고 합니다.

예를 들어, CNOT 게이트는 단 하나의 보조 비트 1을 사용하여 다음 회로에 따라 NOT 게이트를 시뮬레이션할 수 있습니다.



안타깝게도, 이는 보편적이지 않습니다.

#### 명제 24.2.4 (CNOT $\neq$ AND)

CNOT 게이트는 불리언 함수 " $x$ 그리고 $y$ "를 시뮬레이션할 수 없습니다.

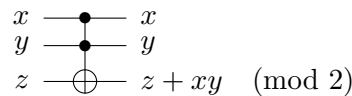
증명 스케치. CNOT 게이트만을 사용하여 시뮬레이션되는 어떤 함수든 다음 형태여야 함을 알 수 있습니다

$$a_1x_1 + a_2x_2 + \dots + a_nx_n \pmod{2}$$

왜냐하면 CNOT은 사상  $(x, y) \mapsto (x, x + y)$ 이기 때문입니다. 따라서 보조 비트를 사용하더라도, 고정된  $a, b, c$ 에 대해  $ax + by + c \pmod{2}$  형태의 함수만 만들 수 있습니다. AND 게이트는 이 형태가 아닙니다.  $\square$

그러므로, 최소한 3-큐비트 게이트가 필요합니다. 가장 흔히 사용되는 것은 다음과 같습니다:

**정의 24.2.5.** CCNOT 게이트라고도 불리는 3비트 **토폴리 게이트**는 다음과 같이 주어집니다



그래서 토폴리 게이트는 두 개의 제어 비트를 가지며, 두 제어 비트가 모두 1일 때에만 마지막 비트를 뒤집습니다.

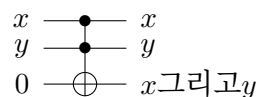
이 대체로 충분합니다.

#### 정리 24.2.6 (토폴리 게이트는 보편적입니다)

토폴리 게이트는 보편적입니다.

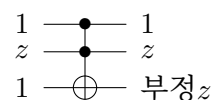
증명. 우리는 토폴리 게이트가 AND, NOT을 가역적으로 시뮬레이션할 수 있고, 따라서 OR도 시뮬레이션할 수 있음을 보일 것인데, 이는 보편성을 보이기에 충분함을 우리는 알고 있습니다. (가역성 덕분에 COPY는 필요하지 않습니다.)

AND 게이트에 대해서는, 다음 회로를 그립니다



하나의 보조 비트를 사용하며, 쓰레기 비트는 없습니다.

NOT 게이트에 대해서는, 두 개의 보조 비트 1과 하나의 쓰레기 비트를 사용합니다:



이로써 증명이 완료됩니다.  $\square$

따라서 이론적으로는 토폴리 게이트만을 사용하여 우리가 원하는 어떤 고전 회로든 만들 수 있습니다. 물론, 이는 가장 단순한 함수에 대해서조차 지수적으로 많은 게이트를 필요로 할 수 있습니다. 다행히도, 이는 전혀 문제가 되지 않는데, 왜냐하면 저는 수학 전공자이고,  $2^n$ 개의 게이트를 갖는 문제는 컴퓨터공학 전공자들에게 맡겨두는 것이 가장 좋은 문제이기 때문입니다.

### §24.3 양자 논리 게이트

양자역학에서는 기저 원소들의 선형결합을 가질 수 있기 때문에, 우리의 논리 게이트는 대신 선형 사상으로 구성될 것입니다. 더욱이, 양자 계산에서는 게이트가 항상 가역적인데, 이것이 바로 앞 절에서 우리가 시간을 들여 가역 게이트로 제한하더라도(예를 들어 토폴리 게이트를 사용하여) 여전히 어떤 함수든 시뮬레이션할 수 있음을 보인 이유입니다.

먼저, 몇 가지 선형대수 내용입니다:

**정의 24.3.1.**  $V$ 를 유한 차원 내적 공간이라 합시다. 그러면 사상  $U: V \rightarrow V$ 에 대해, 다음은 서로 동치입니다:

- $x, y \in V$ 에 대해  $\langle U(x), U(y) \rangle = \langle x, y \rangle$ 입니다.
- $U^\dagger$ 는  $U$ 의 역원입니다.
- $x \in V$ 에 대해  $\|x\| = \|U(x)\|$ 입니다.

사상  $U$ 가 이 동치인 조건들을 만족하면 **유니터리**라고 부릅니다.

그러면

**양자 논리 게이트는 유니터리 행렬입니다.**

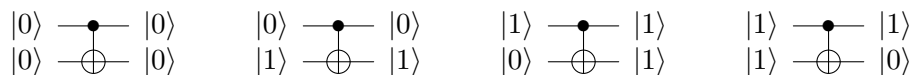
특히, 고전적인 상황과 달리 양자 게이트는 항상 가역적입니다(따라서 입력 비트와 출력 비트의 개수가 항상 같습니다).

예를 들어 CNOT 게이트를 생각해봅시다. 이것의 양자 유사체는 유니터리 사상  $U_{\text{CNOT}}: H \rightarrow H$ 여야 하며, 여기서  $H = \mathbb{C}^{\oplus 2} \otimes \mathbb{C}^{\oplus 2}$ 이고, 기저 원소들에 대해 다음과 같이 주어집니다.

$$U_{\text{CNOT}}(|00\rangle) = |00\rangle, \quad U_{\text{CNOT}}(|01\rangle) = |01\rangle$$

$$U_{\text{CNOT}}(|10\rangle) = |11\rangle, \quad U_{\text{CNOT}}(|11\rangle) = |10\rangle.$$

그림으로 나타내면 양자 CNOT 게이트는 다음과 같이 주어집니다.



그래서 어떻다는 말입니까? 양자역학의 요점 전체는 선형 큐비트가  $|0\rangle$ 과  $|1\rangle$ 의 선형결합 상태에 있는 것도 허용한다는 것이며, 이는 흥미로운 결과를 만들어냅니다. 예를 들어  $|\leftarrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ 을 취해 위쪽에 넣고 아래쪽에는  $|1\rangle$ 을 넣어 어떤 일이 일어나는지 살펴봅시다.

$$U_{\text{CNOT}}(|\leftarrow\rangle \otimes |1\rangle) = U_{\text{CNOT}}\left(\frac{1}{\sqrt{2}}(|01\rangle - |11\rangle)\right) = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |\Psi_-\rangle$$

이것은 완전히 얽힌 단일항 상태입니다! 그림:

$$\begin{array}{c} |\leftarrow\rangle \text{---} \bullet \text{---} |\Psi_{-}\rangle \\ |1\rangle \text{---} \oplus \text{---} \end{array}$$

따라서 혼합 상태를 양자 게이트에 입력하면, 원래 입력이 얽혀 있지 않더라도 출력은 종종 얽힌 상태가 됩니다.

### 예제 24.3.2 (양자 게이트의 더 많은 예시)

- (a) 이전에 접했던 모든 가역 고전 게이트는 CNOT과 같은 방식, 즉 기저 원소들에 대한 값을 지정함으로써 얻어지는 양자 유사체를 가집니다. 예를 들어 양자 토폴리 게이트가 있는데, 이는 예컨대 다음을 보냅니다.

$$\begin{array}{c} |1\rangle \text{---} \bullet \text{---} |1\rangle \\ |1\rangle \text{---} \bullet \text{---} |1\rangle \\ |0\rangle \text{---} \oplus \text{---} |1\rangle \end{array}$$

- (b) 한 큐비트에 대한 **아다마르 게이트**는 다음과 같이 주어지는 회전입니다.

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}.$$

따라서 이는  $|0\rangle$ 을  $|\rightarrow\rangle$ 으로,  $|1\rangle$ 을  $|\leftarrow\rangle$ 으로 보냅니다. 아다마르 게이트는 그 자신의 역원임에 유의하십시오. 이것은 "H" 상자로 표시됩니다.

$$|0\rangle \text{---} \boxed{H} \text{---} |\rightarrow\rangle$$

- (c) 더 일반적으로,  $U$ 가  $2 \times 2$  유니터리 행렬(즉, 사상  $\mathbb{C}^{\oplus 2} \rightarrow \mathbb{C}^{\oplus 2}$ )이라면, 이전 것과 유사한 **U-회전 게이트**가 있으며, 이는 입력에  $U$ 를 적용합니다.

$$|\psi\rangle \text{---} \boxed{U} \text{---} U|\psi\rangle$$

예를 들어 고전 NOT 게이트는  $U = \sigma_x$ 로 표현됩니다.

- (d) **제어형 U-회전 게이트**는 CNOT 게이트를 일반화합니다.  $U: \mathbb{C}^{\oplus 2} \rightarrow \mathbb{C}^{\oplus 2}$ 를 회전 게이트라 하고,  $H = \mathbb{C}^{\oplus 2} \otimes \mathbb{C}^{\oplus 2}$ 를 2-큐비트 공간이라 합시다. 그러면 제어형  $U$  게이트는 다음과 같은 회로도를 가집니다.

$$\begin{array}{cc} |0\rangle \text{---} \bullet \text{---} |0\rangle & |1\rangle \text{---} \bullet \text{---} |1\rangle \\ |\psi\rangle \text{---} \boxed{U} \text{---} |\psi\rangle & |\psi\rangle \text{---} \boxed{U} \text{---} U|\psi\rangle \end{array}$$

따라서 제어 비트가 1일 때  $U$ 가 적용되며, CNOT은  $U = \sigma_x$ 인 특수한 경우입니다. 이전과 마찬가지로, 제어가 혼합 상태이면 흥미로운 동작을 얻게 됩니다.

그리고 이제, 좀 더 직관에 반하는 양자적 동작을 살펴봅시다. CNOT을 다음과 같은 진리표를 가진 복사기로 사용하려 한다고 가정합니다.

| 입력  | 출력  |
|-----|-----|
| 0 0 | 0 0 |
| 1 0 | 1 1 |
| 0 1 | 0 1 |
| 1 1 | 1 0 |

이 게이트의 요점은 아래쪽에 쓰레기값 0을 넣어 "복사" 연산을 시뮬레이션하려는 데 있습니다. 실제로 다음을 확인할 수 있습니다.

$$\begin{array}{ccc} |0\rangle & \text{---} & |0\rangle \\ |0\rangle & \text{---} & |0\rangle \end{array} \quad U \quad \begin{array}{ccc} |1\rangle & \text{---} & |1\rangle \\ |0\rangle & \text{---} & |1\rangle \end{array}$$

따라서 우리는  $|0\rangle$ 과  $|1\rangle$ 을 복사할 수 있습니다. 하지만 이미 보았듯이  $|\leftarrow\rangle \otimes |0\rangle$ 을  $U$ 에 입력하면, 우리가 원했던  $|\leftarrow\rangle \otimes |\leftarrow\rangle$ 이 결코 아닌 얽힌 상태  $|\Psi\rangle$ 를 얻게 됩니다. 그리고 실제로 이른바 **복제 불가 정리**는 임의의  $|\psi\rangle$ 를 복제하는 것이 불가능함을 함의합니다. 우리가 할 수 있는 최선은 고전적인 경우처럼 특정한 직교 상태들을 복사하는 것뿐입니다. **문제 24B**도 참조하십시오.

## §24.4 도이치-조사 알고리즘

도이치-조사 알고리즘은 고전적으로 수행할 수 없는 자명하지 않은 양자 알고리즘의 첫 번째 예시로, 이는 훗날 그로버의 탐색 알고리즘과 쇼어의 소인수분해 알고리즘에 영감을 준 "개념 증명"입니다.

문제는 다음과 같습니다: 함수  $f: \{0,1\}^n \rightarrow \{0,1\}$ 가 주어졌고, 함수  $f$ 가 다음 중 하나임이 보장됩니다.

- 상수 함수이거나, 혹은
- 균형 함수, 즉 정확히 절반의 입력이 0으로, 절반의 입력이 1로 대응되는 함수입니다.

함수  $f$ 는 NOT 게이트의 제어인 가역 블랙박스  $U_f$ 의 형태로 주어지며, 따라서 다음과 같은 회로 도식으로 나타낼 수 있습니다.

$$\begin{array}{ccc} |x_1 x_2 \dots x_n\rangle & \xrightarrow{f} & |x_1 x_2 \dots x_n\rangle \\ |y\rangle & \text{---} & |y + f(x) \pmod 2\rangle \end{array} \quad U_f$$

즉,  $f(x_1, \dots, x_n) = 0$ 이면 게이트는 아무 일도 하지 않으며, 그렇지 않으면 게이트는 아래쪽의  $y$  비트를 뒤집습니다.  $n$ 이 붙은 슬래시는 입력의 위쪽이 실제로는 그려진 하나의 큐비트가 아니라  $n$ 개의 큐비트로 이루어져 있음을 나타내며, 따라서 블랙박스  $U_f$ 는  $n+1$ 개의 큐비트에 대한 사상입니다.

문제는 블랙박스  $U_f$ 에 대한 호출을 가능한 한 적게 사용하여  $f$ 가 균형인지 상수인지를 판별하는 것입니다.

**질문 24.4.1.** 고전적으로는, 최악의 경우 질문에 답하기 위해 함수  $f$ 에 대한 호출이 최대  $2^{n-1} + 1$ 번까지 필요할 수 있음을 보이십시오.

따라서 고전적인 도구만으로는  $f$ 가 균형인지 상수인지를 판별하는 데  $O(2^n)$ 번의 질의가 필요합니다. 하지만,

### 정리 24.4.2 (도이치-조사)

도이치-조사 문제는 블랙박스에 대한 단 한 번의 호출만으로 양자 회로에서 판별할 수 있습니다.

증명. 구체성을 위해  $n = 1$ 인 경우를 명시적으로 다루겠습니다; 일반적인 경우는 **문제 24C**에 포함되어 있습니다. 필요한 회로는 다음과 같음을 주장합니다.

$$\begin{array}{ccc} |0\rangle & \text{---} & H \\ |1\rangle & \text{---} & H \end{array} \quad U_f \quad \begin{array}{ccc} H & \text{---} & \text{---} \\ & & \end{array}$$

여기서  $H$ 들은 아다마르 게이트이며, 맨 오른쪽 선 끝의 계측기는 통상적인  $|0\rangle$ ,  $|1\rangle$  기저를 따라 측정을 수행함을 나타냅니다. 이는 오타가 아닙니다! 고전적으로는 위쪽 선이 단지 입력 정보를 반복하는 것에 불과하지만, 우리가 측정하고자 하는 것이 바로 이 위쪽임을 곧 보게 될 것입니다.

두 번의 아다마르 연산 이후 얻어지는 상태는 다음과 같음에 주목하십시오.

$$\begin{aligned} |01\rangle &\xrightarrow{H^{\otimes 2}} \left( \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right) \otimes \left( \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right) \\ &= \frac{1}{2}(|0\rangle \otimes (|0\rangle - |1\rangle) + |1\rangle \otimes (|0\rangle - |1\rangle)). \end{aligned}$$

따라서  $U_f$ 를 적용한 후, 우리는 다음을 얻습니다.

$$\frac{1}{2}(|0\rangle \otimes (|0 + f(0)\rangle - |1 + f(0)\rangle) + |1\rangle \otimes (|0 + f(1)\rangle - |1 + f(1)\rangle))$$

여기서 모듈로 2는 암묵적으로 생략되었습니다. 이제,  $|0\rangle - |1\rangle$ 에서  $|0 + f(x)\rangle - |1 + f(x)\rangle$ 로 넘어가는 것의 효과는 단지 상태를 그대로 유지하거나( $f(x) = 0$ 인 경우) 부호를 반전시키는( $f(x) = 1$ 인 경우) 것에 불과함을 관찰하십시오. 따라서 우리는 다음과 같이 단순화하고 인수분해할 수 있습니다.

$$\frac{1}{2}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle) \otimes (|0\rangle - |1\rangle).$$

따라서, 지금까지의 그림은 다음과 같습니다:

$$\begin{array}{c} |0\rangle \xrightarrow{H} \boxed{U_f} \xrightarrow{\frac{1}{\sqrt{2}}((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle)} \\ |1\rangle \xrightarrow{H} \boxed{U_f} \xrightarrow{\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)} \end{array}$$

특히, 결과 상태는 얽혀 있지 않으며, 우리는 단순히 마지막 큐비트를 버릴 수 있습니다(!). 이제 다음을 관찰하십시오:

- $f$ 가 상수이면, 가장 위쪽 상태는  $\pm|\rightarrow\rangle$ 입니다.
- $f$ 가 균형이면, 가장 위쪽 상태는  $\pm|\leftarrow\rangle$ 입니다.

따라서 단순히  $\sigma_x$ 를 따라 측정하는 것만으로 답을 얻을 수 있습니다. 이와 동등하게,  $H$  게이트를 한 번 더 적용하여( $H|\rightarrow\rangle = |0\rangle$ ,  $H|\leftarrow\rangle = |1\rangle$ 이 되도록) 통상적인  $|0\rangle$ ,  $|1\rangle$  기저에서  $\sigma_z$ 를 따라 측정할 수 있습니다. 따라서  $n = 1$ 인 경우 오라클에 대한 호출이 단 한 번만 필요합니다.  $\square$

## §24.5 생각해 볼 만한 조금 더 어려운 문제

**문제 24A** (프레드킨 게이트). **프레드킨 게이트**(제어 스왑, 즉 CSWAP 게이트라고도 불림)는 다음과 같은 진리표를 갖는 3비트 게이트입니다.

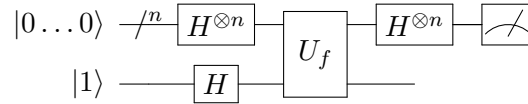
| 입력 |   |   | 출력 |   |   |
|----|---|---|----|---|---|
| 0  | 0 | 0 | 0  | 0 | 0 |
| 0  | 0 | 1 | 0  | 0 | 1 |
| 0  | 1 | 0 | 0  | 1 | 0 |
| 0  | 1 | 1 | 0  | 1 | 1 |
| 1  | 0 | 0 | 1  | 0 | 0 |
| 1  | 0 | 1 | 1  | 1 | 0 |
| 1  | 1 | 0 | 1  | 0 | 1 |
| 1  | 1 | 1 | 1  | 1 | 1 |

따라서 이 게이트는 첫 번째 비트가 1일 때마다 마지막 두 입력 비트를 교환합니다. 이 게이트 역시 가역적이며 보편적임을 보이십시오.

**문제 24B** (기본적인 복제 불가 정리). 두 큐비트 위의 유니터리 사상  $U$  중 임의의 큐비트  $|\psi\rangle$ 에 대해  $U(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$ 를 보내는 것이 존재하지 않음을 보이십시오. 즉, 다음의 회로 도식이 불가능함을 보이십시오.

$$\begin{array}{c} |\psi\rangle \\ |0\rangle \end{array} \xrightarrow{U} \begin{array}{c} |\psi\rangle \\ |\psi\rangle \end{array}$$

**문제 24C** (도이치-조사). 도이치-조사 알고리즘에서 설명한 블랙박스  $U_f$ 가 주어졌을 때, 다음 회로를 고려합니다.



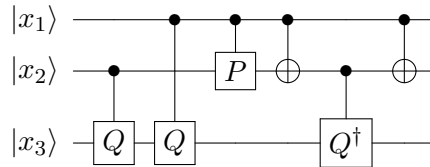
즉,  $|0\rangle$ 의  $n$ 개 사본을 취하여 이들 모두에 아다마르 회전을 적용하고,  $U_f$ 를 적용한 후,  $n$ 개의 입력 비트 모두에 아다마르를 역으로 적용하고(마지막 비트는 다시 버림), 그런 다음  $n$ 개의 비트 전부를  $|0\rangle/|1\rangle$  기저에서 측정합니다(예제 23.4.4에서와 같이).

$f$ 가 상수 함수이면  $|0\dots 0\rangle$ 을 측정할 확률이 1이고,  $f$ 가 균형 함수이면 0임을 보이십시오.

**문제 24D<sup>†</sup>** (Barenco et al, 1995; arXiv:quant-ph/9503016v1). 다음과 같다고 합시다

$$P = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \quad Q = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -i \\ -i & 1 \end{bmatrix}$$

양자 토폴리 게이트가 다음 회로를 통해 제어 회전만으로 구현될 수 있음을 확인하십시오



이는 발견 당시 연구자들에게 큰 놀라움을 주었는데, 고전적인 가역 논리는 3비트 게이트(예: 토폴리, 프레드킨)를 필요로 하기 때문입니다.

# 25 쇼어 알고리즘

이제 쇼어 알고리즘을 다룰 차례입니다:  $M = pq$ 를  $O((\log M)^2)$  시간에 인수분해하는 방법입니다.

이것이 아마도 미국 국가안보국(NSA) 같은 기관들이 양자 컴퓨팅에 수백만 달러를 쏟아 붓고 있는 이유일 것입니다.

## §25.1 고전적인 (역) 푸리에 변환

쇼어 알고리즘의 “핵심 수”는 이른바 양자 푸리에 변환입니다. 푸리에 변환은 데이터에서 주기성을 추출하는 데 사용되며, 그 양자적 대응물은 고전적인 것보다 훨씬 빠른 것으로 밝혀졌습니다.

먼저 정의를 던져 드리겠습니다.  $N$ 을 양의 정수라 하고,  $\omega_N = \exp\left(\frac{2\pi i}{N}\right)$ 이라 합시다.

**정의 25.1.1.** 복소수의 튜플이 주어졌을 때

$$(x_0, x_1, \dots, x_{N-1})$$

그 **이산 역 푸리에 변환**은 다음과 같이 정의되는 수열  $(y_0, y_1, \dots, y_{N-1})$ 입니다

$$y_k = \frac{1}{N} \sum_{j=0}^{N-1} \omega_N^{jk} x_j.$$

이는 다음 행렬을 적용하는 것과 동치입니다

$$\frac{1}{N} \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega_N & \omega_N^2 & \dots & \omega_N^{N-1} \\ 1 & \omega_N^2 & \omega_N^4 & \dots & \omega_N^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{N-1} & \omega_N^{2(N-1)} & \dots & \omega_N^{(N-1)^2} \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{bmatrix} = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{N-1} \end{bmatrix}.$$

이 연산이 중요한 이유는  $x_i$ 가 주기적인지 검출할 수 있게 해 주기 때문입니다. 더 일반적으로, 주기  $r$ 로 나타나는 1들의 수열이 주어지면, 진폭은  $\frac{N}{\gcd(N,r)}$ 로 나누어떨어지는 입력값에서 최고점을 이룹니다. 수학적으로는 다음이 성립합니다

$$x_k = \sum_{j=0}^{N-1} y_j \omega_N^{-jk}.$$

### 예제 25.1.2 (이산 역 푸리에 변환의 예)

$N = 6$ ,  $\omega = \omega_6 = \exp\left(\frac{2\pi i}{6}\right)$ 이고  $(x_0, x_1, x_2, x_3, x_4, x_5) = (0, 1, 0, 1, 0, 1)$ 이라 합시다

(따라서  $x_i$ 는 2를 법으로 주기적입니다). 그러면

$$\begin{aligned}y_0 &= \frac{1}{6} (\omega^0 + \omega^0 + \omega^0) = 1/2 \\y_1 &= \frac{1}{6} (\omega^1 + \omega^3 + \omega^5) = 0 \\y_2 &= \frac{1}{6} (\omega^2 + \omega^6 + \omega^{10}) = 0 \\y_3 &= \frac{1}{6} (\omega^3 + \omega^9 + \omega^{15}) = -1/2 \\y_4 &= \frac{1}{6} (\omega^4 + \omega^{12} + \omega^{20}) = 0 \\y_5 &= \frac{1}{6} (\omega^5 + \omega^{15} + \omega^{25}) = 0.\end{aligned}$$

따라서 역변환에서 “진폭”은 모두 3의 배수에 집중되며, 이는 원래 수열의 주기성이  $\frac{N}{3} = 2$ 임을 드러냅니다.

**비고 25.1.3** — 이 연산이 “역” 푸리에 변환이라 불리는 것은 제가 이해하기로는 대부분 역사적 우연입니다. 혼란스럽게도, 이에 대응하는 양자 연산은 (역이 아닌) 푸리에 변환입니다.

정의를 그대로 적용하면, 변환을 계산하는 데  $O(N^2)$  시간이 걸립니다. **고속 푸리에 변환**이라는 고전적 알고리즘(그 세부 사항은 다루지 않겠지만, 사실상 계산을 “재사용”합니다)을 사용하면 이를  $O(N \log N)$  시간으로 줄일 수 있음이 밝혀져 있습니다. 그러나 쇼어 알고리즘에는 이것으로도 충분하지 않으며,  $O((\log N)^2)$  정도가 필요합니다. 바로 여기서 양자 푸리에 변환이 등장합니다.

## §25.2 양자 푸리에 변환

푸리에 변환을 계산하려면  $N \times N$  행렬을  $N$ -벡터와 곱해야 하므로, 이는  $O(N^2)$ 번의 곱셈이 필요함에 유의하십시오. 그러나 이제 양자 컴퓨터를 사용하면  $N = 2^n$ 일 때  $n$ 개의 큐비트로 이루어진 시스템에서  $O((\log N)^2)$ 개의 양자 게이트만으로 이를 수행할 수 있음을 보이려 합니다.

먼저, 표기법을 좀 더 소개합니다:

**표기의 남용 25.2.1.** 이하에서  $|x\rangle$ 는 이진법으로  $x = x_n x_{n-1} \dots x_1$ 일 때  $|x_n\rangle \otimes |x_{n-1}\rangle \otimes \dots \otimes |x_1\rangle$ 을 가리킵니다. 예를 들어  $n = 3$ 이면  $|6\rangle$ 은 실제로  $|1\rangle \otimes |1\rangle \otimes |0\rangle$ 을 의미합니다. 마찬가지로,  $0.x_1 x_2 \dots x_n$ 을 이진법으로 표기합니다.

이제  $n$ -큐비트 공간이 정규직교 기저  $|0\rangle, |1\rangle, \dots, |N-1\rangle$ 을 가짐에 주목하십시오

**정의 25.2.2.**  $n$ -큐비트 상태를 생각해 봅시다

$$|\psi\rangle = \sum_{k=0}^{N-1} x_k |k\rangle.$$

**양자 푸리에 변환**은 다음과 같이 정의됩니다

$$U_{\text{QFT}}(|\psi\rangle) = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \left( \sum_{k=0}^{N-1} \omega_N^{jk} x_k \right) |j\rangle.$$

다시 말해, 기저  $|0\rangle, \dots, |N-1\rangle$ 을 사용하면  $U_{\text{QFT}}$ 는 다음 행렬로 주어집니다

$$U_{\text{QFT}} = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega_N & \omega_N^2 & \dots & \omega_N^{N-1} \\ 1 & \omega_N^2 & \omega_N^4 & \dots & \omega_N^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{N-1} & \omega_N^{2(N-1)} & \dots & \omega_N^{(N-1)^2} \end{bmatrix}$$

이는 앞서와 정확히 동일한 정의이지만,  $U_{\text{QFT}}$ 가 유니터리가 되도록  $\sqrt{N}$  인자가 추가되었습니다. 그러나 요령은, 양자적 설정에서는 이 행렬을 다시 쓸 수 있다는 점입니다:

### 명제 25.2.3 (텐서 표현)

$|x\rangle = |x_n x_{n-1} \dots x_1\rangle$ 이라 합시다. 그러면

$$\begin{aligned} U_{\text{QFT}}(|x_n x_{n-1} \dots x_1\rangle) &= \frac{1}{\sqrt{N}} (|0\rangle + \exp(2\pi i \cdot 0.x_1) |1\rangle) \\ &\quad \otimes (|0\rangle + \exp(2\pi i \cdot 0.x_2 x_1) |1\rangle) \\ &\quad \otimes \dots \\ &\quad \otimes (|0\rangle + \exp(2\pi i \cdot 0.x_n \dots x_1) |1\rangle) \end{aligned}$$

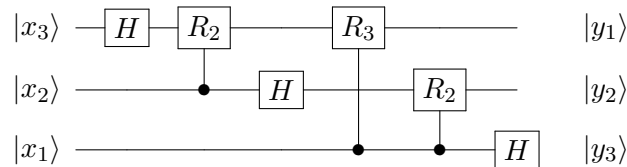
증명. 직접(그리고 상당히 성가신) 계산입니다. 요컨대, 모든 것을 전개하면 됩니다.  $\square$

따라서 혼합 상태를 사용함으로써, 양자 푸리에 변환은 고전적으로는 불가능한 이 “텐서 곱에 의한 곱셈” 기법을 사용할 수 있습니다.

이제 더 이상 미루지 말고, 회로를 살펴봅시다. 회전 행렬을 다음과 같이 정의합니다

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & \exp(2\pi i/2^k) \end{bmatrix}.$$

그러면  $n = 3$ 일 때 회로는 제어형  $R_k$ 들을 사용하여 다음과 같이 주어집니다:

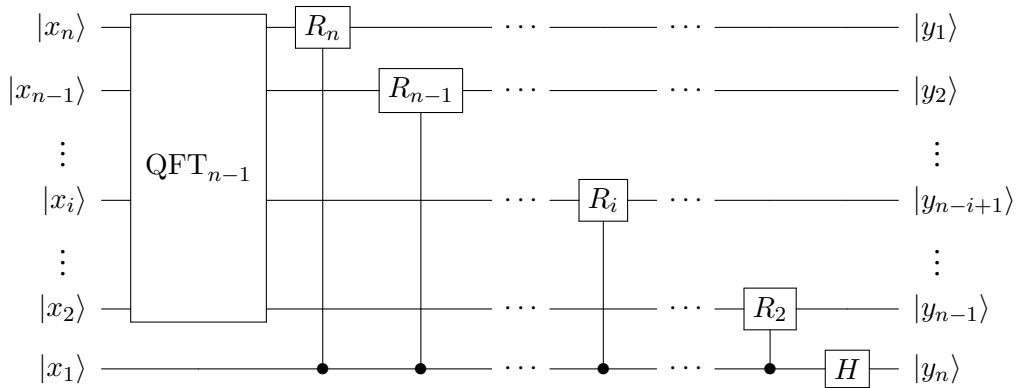


**연습문제 25.2.4.** 이 회로에서  $|x_3 x_2 x_1\rangle$ 의 상이 다음과 같음을 보이십시오

$$\left( |0\rangle + \exp(2\pi i \cdot 0.x_1) |1\rangle \right) \otimes \left( |0\rangle + \exp(2\pi i \cdot 0.x_2 x_1) |1\rangle \right) \otimes \left( |0\rangle + \exp(2\pi i \cdot 0.x_3 x_2 x_1) |1\rangle \right)$$

주장한 대로입니다.

일반적인  $n$ 에 대해서는, 이를 귀납적으로 다음과 같이 쓸 수 있습니다



**질문 25.2.5.**  $n = 3$ 일 때 표시된 두 회로가 동치임을 스스로 확인해 보십시오.

따라서 양자 푸리에 변환은  $O(n^2)$ 개의 게이트로 달성 가능하며, 이는 고전적인 고속 푸리에 변환이 달성하는  $O(N \log N)$ 번의 연산(여기서  $N = 2^n$ )보다 엄청나게 낮습니다.

### §25.3 쇼어 알고리즘

양자 푸리에 변환은 쇼어 알고리즘의 핵심 요소입니다. 이제 이를 갖추었으니, 소인수분해 문제를 풀 수 있습니다.

$p, q > 3$ 을 홀수 소수라 하고,  $p \neq q$ 라고 가정합시다. 주요 아이디어는 정수  $M = pq$ 를 소인수분해하는 문제를,  $x \pmod{M}$ 의 위수를 찾는 문제로 바꾸는 것입니다. 후자는 양자 푸리에 변환으로 풀 수 있는 “주기성” 문제입니다. 구체적으로,  $x \pmod{M}$ 이 다음을 만족하면 좋다고 합시다

- (i)  $\gcd(x, M) = 1$ ,
- (ii)  $x \pmod{M}$ 의 위수  $r$ 이 짝수이고, 그리고
- (iii)  $0 \equiv (x^{r/2} - 1)(x^{r/2} + 1) \pmod{M}$ 을 인수분해하면, 두 인수 중 어느 것도  $0 \pmod{M}$ 이 아닙니다. 따라서 그중 하나는  $p$ 로 나누어떨어지고, 다른 하나는  $q$ 로 나누어떨어집니다.

**연습문제 25.3.1** (경시 정수론 연습용).  $M = pq$ 일 때  $(\mathbb{Z}/M\mathbb{Z})^\times$ 의 잉여류 중 적어도 절반이 좋은 것임을 보이십시오.

그러므로 임의의  $x \in (\mathbb{Z}/M\mathbb{Z})^\times$ 의 위수를 찾을 수 있다면, 좋은  $x$ 를 뽑을 때까지 계속 뽑기만 하면 됩니다(이는 절반 이상의 확률로 일어납니다). 일단 그렇게 되면, 유클리드 호제법을 사용하여  $\gcd(x^{r/2} - 1, M)$ 을 계산함으로써  $M$ 의 소인수 중 하나를 뽑아낼 수 있으며, 이로써 문제는 해결됩니다.

이제 이를 어떻게 할까요? 아이디어는 그리 어렵지 않습니다. 먼저  $r$ 을 법으로 주기적인 수열을 생성합니다.

#### 예제 25.3.2 (77을 소인수분해하기: 주기 상태 생성하기)

$M = 77$ 을 소인수분해하려 하며, 무작위로  $x = 2$ 를 선택하고, 그 위수  $r$ 을 찾고자 한다고 합시다.  $n = 13$ 이고  $N = 2^{13}$ 이라 하고, 다음 상태를 초기화하는 것으로

시작합니다

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle.$$

이제 ( $x$ 에 의존하는) 회로  $U_x$ 를 만들어  $|k\rangle |0\rangle$ 을  $|k\rangle |x^k \bmod M\rangle$ 으로 보내도록 합니다. 이를  $|\psi\rangle \otimes |0\rangle$ 에 적용하면 다음이 얻어집니다

$$U(|\psi\rangle |0\rangle) = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} |k\rangle \otimes |x^k \bmod M\rangle.$$

이제 두 번째 큐비트를 측정하여  $|51\rangle$  상태를 얻었다고 합시다( $2^7 \equiv 51 \pmod{77}$ 임에 유의하십시오). 그러면 붕괴된 현재 상태는, 스케일링을 제외하면 다음과 같음을 알 수 있습니다

$$(|7\rangle + |7+r\rangle + |7+2r\rangle + \dots) \otimes |51\rangle.$$

사실 병목 지점은 회로  $U_x$ 입니다.  $x^k \pmod{M}$ 은 반복 제곱법을 사용하여 계산할 수 있지만, 그럼에도 전체 연산 중 가장 다루기 힘든 부분입니다.

일반적으로, 이 연산은 다음과 같습니다:

- 충분히 큰  $N = 2^n$ 을 선택합니다(예를 들어,  $N \geq M^2$ ).
- $|\psi\rangle = \sum_{k=0}^{2^n-1} |k\rangle$ 를 생성합니다.
- $|x^k \bmod M\rangle$ 을 계산하는 회로  $U_x$ 를 만듭니다.
- 이를 적용하여 상태  $\frac{1}{\sqrt{N}} \sum_{k=0}^{2^n-1} |k\rangle \otimes |x^k \bmod M\rangle$ 를 얻습니다.
- 두 번째 큐비트를 측정하여 첫 번째 큐비트가  $r$ 을 법으로 주기적인 무언가로 붕괴하도록 합니다.  $|\phi\rangle$ 가 왼쪽 큐비트를 나타낸다고 합시다.

이제 왼쪽 큐비트  $|\phi\rangle$ 에 양자 푸리에 변환을 적용한다고 합시다: 왼쪽 비트가  $r$ 을 법으로 주기적이므로, 우리는 이 변환이  $r$ 이 무엇인지 알려줄 것이라고 기대합니다. 안타깝게도 이는 그리 잘 맞아떨어지지 않는데,  $N$ 은 2의 거듭제곱이지만  $r$ 은 그렇지 않을 것으로 예상되기 때문입니다.

그럼에도 불구하고, 다음과 같은 상태를 고려합시다

$$|\phi\rangle = |k_0\rangle + |k_0+r\rangle + \dots$$

예를 들어 앞서  $x = 2$ 에서 51을 측정했을 때  $k_0 = 7$ 이었습니다. 양자 푸리에 변환을 적용하면, 변환된 이미지에서  $|j\rangle$ 의 계수가 다음과 같음을 알 수 있습니다

$$\omega_N^{k_0 j} \cdot \left( \omega_N^0 + \omega_N^{jr} + \omega_N^{2jr} + \omega_N^{3jr} + \dots \right)$$

이것이 단위근들의 합이므로,  $\omega_N^{jr} = 1$ 이 아닌 한 소멸 간섭이 일어남을 알 수 있습니다( $N$ 이 크기 때문입니다). 다시 말해, 근사적으로 다음이 성립합니다

$$U_{\text{QFT}}(|\phi\rangle) \approx \sum_{\substack{0 \leq j < N \\ jr/N \in \mathbb{Z}}} |j\rangle$$

늘 그렇듯이 스케일링을 제외하면 그렇습니다. 결론적으로 다음이 성립합니다

$U_{\text{QFT}}|\phi\rangle$ 를 측정하면,  $\frac{jr}{N}$ 이 어떤  $s \in \mathbb{Z}$ 에 가까운  $|j\rangle$ 를 얻습니다.

그리하여 충분한 운이 따른다면 연분수를 이용하여  $r$ 의 값을 추출할 수 있습니다.

**예제 25.3.3** ( $M = 77$ 의 인수분해 마무리)

앞서와 마찬가지로 우리는 두 번째 큐비트에 대해 관측을 하였고, 이에 따라 첫 번째 큐비트는 상태  $|\phi\rangle = |7\rangle + |7+r\rangle + \dots$ 로 붕괴합니다. 이제 측정을 하여  $j = 4642$ 를 얻는데, 이는 어떤 정수  $s$ 에 대해 다음이 성립함을 의미합니다

$$\frac{4642r}{2^{13}} \approx s.$$

이제  $\frac{4642}{2^{13}}$ 의 연분수를 분석합니다; 처음 몇 개의 근사분수는 다음과 같음을 알 수 있습니다

$$0, 1, \frac{1}{2}, \frac{4}{7}, \frac{13}{23}, \frac{17}{30}, \frac{1152}{2033}, \dots$$

따라서  $\frac{17}{30}$ 이 좋은 근사값이며, 이로부터  $s = 17$ 과  $r = 30$ 을 후보로 추론합니다. 그리고 실제로  $r = 30$ 이 원하는 위수임을 확인할 수 있습니다.

이는 항상 성립하지는 않습니다<sup>1</sup>(예를 들어, 운이 나빠  $j = 0$ , 즉  $s = 0$ 을 측정할 수도 있는데, 이는 우리에게 아무런 정보도 알려주지 않을 것입니다).

그러나

$$\gcd(s, r) = 1.$$

일 때마다 우리가 성공함을 보일 수 있습니다. 이는 최소  $\frac{1}{\log r}$ 의 확률로 일어나며,  $r < M$ 이므로 이는 충분히 많은 시행이 주어지면 결국 올바른 위수  $r$ 을 추출하게 됨을 의미합니다. 이것이 쇼어 알고리즘입니다.

<sup>1</sup>일반적인 잡음 문제는 말할 것도 없지만, 그것은 엔지니어들이 걱정할 몫입니다.

# VIII

미적분학 101

## 제VIII부: 목차

---

|           |                                                               |            |
|-----------|---------------------------------------------------------------|------------|
| <b>26</b> | <b>극한과 급수</b>                                                 | <b>295</b> |
| 26.1      | 완비성과 $\inf/\sup$ . . . . .                                    | 295        |
| 26.2      | $\mathbb{R}$ 의 두 가지 핵심 완비성 성질의 증명 . . . . .                   | 296        |
| 26.3      | 단조수열 . . . . .                                                | 298        |
| 26.4      | 무한급수 . . . . .                                                | 299        |
| 26.5      | 급수의 덧셈은 교환법칙이 성립하지 않습니다: 공포 이야기 . . . . .                     | 302        |
| 26.6      | 점에서의 함수의 극한 . . . . .                                         | 303        |
| 26.7      | 무한대에서의 함수의 극한 . . . . .                                       | 305        |
| 26.8      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                | 305        |
| <b>27</b> | <b>Bonus: A hint of p-adic numbers</b>                        | <b>307</b> |
| 27.1      | 동기 . . . . .                                                  | 307        |
| 27.2      | 대수적 관점 . . . . .                                              | 308        |
| 27.3      | 해석적 관점 . . . . .                                              | 312        |
| 27.4      | Mahler 계수 . . . . .                                           | 315        |
| 27.5      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                | 317        |
| <b>28</b> | <b>미분</b>                                                     | <b>319</b> |
| 28.1      | 정의 . . . . .                                                  | 319        |
| 28.2      | 계산하는 방법 . . . . .                                             | 320        |
| 28.3      | 극소 (및 극대) 최댓값 . . . . .                                       | 323        |
| 28.4      | 롤과 그 동료들 . . . . .                                            | 325        |
| 28.5      | 매끄러운 함수 . . . . .                                             | 328        |
| 28.6      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                | 328        |
| <b>29</b> | <b>멱급수와 테일러 급수</b>                                            | <b>331</b> |
| 29.1      | 동기 . . . . .                                                  | 331        |
| 29.2      | 멱급수 . . . . .                                                 | 332        |
| 29.3      | 멱급수의 미분 . . . . .                                             | 333        |
| 29.4      | 해석적 함수 . . . . .                                              | 334        |
| 29.5      | 오일러 상수와 지수화의 정의 . . . . .                                     | 335        |
| 29.6      | 이는 복소수에 대해서도 마찬가지로 성립하는데, 다만 복소해석학 또한 천국이라는 점만 다릅니다 . . . . . | 336        |
| 29.7      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                | 337        |
| <b>30</b> | <b>리만 적분</b>                                                  | <b>339</b> |
| 30.1      | 균등 연속 . . . . .                                               | 339        |
| 30.2      | 조밀 집합과 확장 . . . . .                                           | 340        |
| 30.3      | 리만 적분의 정의 . . . . .                                           | 341        |
| 30.4      | 메시(Mesh) . . . . .                                            | 342        |
| 30.5      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                | 344        |

---

# 26 극한과 급수

이제 거리 (및 위상) 공간의 이론을 충분히 전개하였으므로, 일변수 미적분학의 이론을 빠르게 다루는 세 개의 장으로 이루어진 시퀀스를 제시합니다.

사실 많은 작업이 이미 은밀히 이루어져 있습니다. 예를 들어,  $x_n$ 과  $y_n$ 이  $\lim_n x_n = x$ 와  $\lim_n y_n = y$ 를 만족하는 실수열이라면, 실제로  $\lim_n (x_n + y_n) = x + y$ 이거나  $\lim_n (x_n y_n) = xy$ 인데, 이는 **명제 2.5.5**에서 사칙연산이 연속임을 보였기 때문입니다. 또한 완비성이 결정적인 역할을 한다는 것도 보게 될 것입니다.

## §26.1 완비성과 inf/sup

**이 절의 대표적인 예:**  $\sup[0, 1] = \sup(0, 1) = 1$ .

$\mathbb{R}$ 은 거리 공간이므로, 연속성과 수렴에 대해 논할 수 있습니다.  $\mathbb{R}$ 에 관해서는 이후 대부분의 절이 작동하게 만드는 두 가지 중요한 사실이 있습니다.

첫 번째 사실은 이미 본 적이 있습니다.

### 정리 26.1.1 ( $\mathbb{R}$ 은 완비입니다)

거리 공간으로서  $\mathbb{R}$ 은 완비입니다: 수열이 수렴하는 것은 그것이 코시 수열인 것과 동치입니다.

두 번째 사실은 아직 본 적이 없는 것으로, 바로 inf와 sup의 존재입니다. 여러분의 직관은 다음과 같아야 합니다:

sup은 무한 집합에 맞게 약간 조정된 max입니다. (그리고 inf는 조정된 min입니다.)

왜 “조정”이 필요할까요?

### 예제 26.1.2 (왜 max로는 충분하지 않을까요?)

열린 구간  $S = (0, 1)$ 이 있다고 합시다. 원소들은 1에 얼마든지 가까워질 수 있으므로, “1이  $S$ 의 max이다”라고 생각하고 싶어지지만, 문제는  $1 \notin S$ 라는 것입니다. 일반적으로 무한 집합은 반드시 최댓값을 가지지는 않으며, 대신 경계에 대해 이야기해야 합니다.

그래서 우리는  $\sup S = 1$ 이 되도록  $\sup S$ 를 정의할 것입니다. 그 정의는 “1은  $S$ 의 모든 원소 이상인 수 중 가장 작은 수이다”라는 것입니다.

이를 풀어서 쓰면 다음과 같습니다:

**정의 26.1.3.**  $S$ 가 실수의 집합이라고 합시다:

- $S$ 에 대한 상계란 모든  $x \in S$ 에 대해  $x \leq M$ 을 만족하는 실수  $M$ 입니다. 그러한 것이 존재하면,  $S$ 가 **위로 유계**라고 말합니다;
- $S$ 에 대한 하계란 모든  $x \in S$ 에 대해  $m \leq x$ 를 만족하는 실수  $m$ 입니다. 그러한 것이 존재하면,  $S$ 가 **아래로 유계**라고 말합니다.

- 상계와 하계가 모두 존재하면,  $S$ 가 **유계**라고 말합니다.

#### 정리 26.1.4 ( $\mathbb{R}$ 은 inf와 sup을 가집니다)

$S$ 를 공집합이 아닌 실수의 집합이라고 합시다.

- $S$ 가 위로 유계이면 최소 상계를 가지며, 이를  $\sup S$ 로 표기하고  $S$ 의 **상한**이라고 부릅니다.
- $S$ 가 아래로 유계이면 최대 하계를 가지며, 이를  $\inf S$ 로 표기하고  $S$ 의 **하한**이라고 부릅니다.

**정의 26.1.5.** 편의상,  $S$ 가 위로 유계가 아니면  $\sup S = +\infty$ 로 씁니다. 마찬가지로,  $S$ 가 아래로 유계가 아니면  $\inf S = -\infty$ 로 씁니다.

#### 예제 26.1.6 (상한)

하한에 대한 예시는 기본적으로 동일하므로, 지금은 상한에 집중하겠습니다.

- 만약  $S = \{1, 2, 3, \dots\}$ 라면  $S$ 는 위로 유계가 아니므로,  $\sup S = +\infty$ 입니다.
- 만약  $S = \{\dots, -2, -1\}$ 가 음의 정수의 집합을 나타낸다면,  $\sup S = -1$ 입니다.
- $S = [0, 1]$ 을 닫힌 구간이라 합시다. 그러면  $\sup S = 1$ 입니다.
- $S = (0, 1)$ 을 열린 구간이라 합시다. 1 자체가  $S$ 의 원소가 아님에도 불구하고,  $\sup S = 1$ 입니다.
- $S = \mathbb{Q} \cap (0, 1)$ 이 0과 1 사이의 유리수 집합을 나타낸다고 합시다. 이 경우에도  $\sup S = 1$ 입니다.
- 만약  $S$ 가 유한한 공집합이 아닌 집합이라면,  $\sup S = \max S$ 입니다.

**정의 26.1.7** (수열로의 정의 이식).  $a_1, \dots$ 가 수열이라면, 우리는 종종 다음과 같이 씁니다

$$\sup_n a_n := \sup \{a_n \mid n \in \mathbb{N}\}$$

$$\inf_n a_n := \inf \{a_n \mid n \in \mathbb{N}\}$$

이는 해당 수열의 원소들로 이루어진 집합의 상한과 하한을 나타냅니다. 또한 수열에 대해서도 같은 방식으로 "위로/아래로 유계"라는 용어를 사용합니다.

#### 예제 26.1.8 (수열의 하한)

수열  $a_n = \frac{1}{n}$ 은 하한  $\inf a_n = 0$ 을 가집니다.

## §26.2 $\mathbb{R}$ 의 두 가지 핵심 완비성 성질의 증명

세심한 독자라면 우리가 아직 정리 26.1.4이나 정리 26.1.1 중 어느 것도 실제로 증명하지 않았음을 알아차렸을 것입니다. 여기서 그것을 증명하겠습니다.

먼저, 상한과 하한을 취할 수 있는 능력이  $\mathbb{R}$ 의 완비성을 증명하게 해준다는 것을 보이겠습니다.

**정리 26.1.4**이 **정리 26.1.1**을 함의함의 증명.  $a_1, a_2, \dots$ 를 코시 수열이라 합시다. 유한 개의 앞선 항들을 버림으로써, 모든  $i$ 와  $j$ 에 대해  $|a_i - a_j| \leq 100$ 이라고 가정해도 무방합니다. 특히, 이제 이 수열은 유계이며, 예를 들어  $[a_1 - 100, a_1 + 100]$  사이에 놓여 있습니다.

우리는 이 수열이 수렴함을 보이려고 하므로, 먼저 극한이 무엇인지 기술해야 합니다. 이를 위해서는 우리가 실제로  $\mathbb{R}$ 에 살고 있다는 사실을 사용해야 한다는 것을 알고 있습니다. (예를 들어  $\mathbb{Q}$ 에서는 1, 1.4, 1.41, 1.414, ...의 극한이 존재하지 않는다는 것을 우리는 알고 있습니다.)

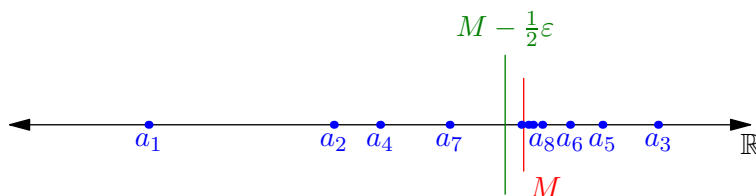
우리는 다음을 제안합니다: 다음과 같이 놓읍시다

$$S = \{x \in \mathbb{R} \mid a_n \geq x \text{ 무한히 많은 } n \text{에 대해}\}.$$

우리는 이 수열이  $M = \sup S$ 로 수렴한다고 주장합니다.

**연습문제 26.2.1.**  $a_1 - 100 \in S$ 임을 증명하여 ( $S$ 가 공집합이 아님을 보임) 이 상한이 의미가 있음을 보이는 동시에,  $S$ 의 모든 원소가  $a_1 + 100$  이하임을 보이십시오 ( $S$ 가 위로 유계임을 보임). 따라서 우리는 실제로 상한을 취하는 것이 허용됩니다.

이 집합  $S$ 는 다음과 같은 그림으로 생각할 수 있습니다. 실수선 위에 그려진, 우리가 수렴한다고 생각하는 코시 수열이 있으며, 이는 실수선 위의 순서가 매겨진 여러 점들의 무리로 시각화할 수 있습니다. 우리는 오직 유한 개의 점만이 칼의 왼쪽에 있도록 이 선을 칼로 자르고자 합니다. (예를 들어, 칼을 맨 왼쪽 끝에 놓으면 항상 성립합니다.) 집합  $S$ 는 우리가 칼을 놓을 수 있는 위치들을 나타내며,  $M$ 은 우리가 갈 수 있는 "가장 오른쪽" 지점입니다. 상한이 작동하는 방식 때문에  $M$  자체는 유효한 칼의 위치가 아닐 수도 있지만, 그보다 왼쪽에 있는 것은 확실히 유효합니다.



$\varepsilon > 0$ 이 주어졌다고 합시다. 우리는 결국 모든 항이  $M$ 으로부터  $\varepsilon$  이내에 들어옴을 보이려고 합니다. 수열이 코시 수열이므로,  $m \geq n \geq N$ 일 때 결국  $|a_m - a_n| < \frac{1}{2}\varepsilon$ 가 성립하는  $N$ 이 존재합니다.

이제  $n$ 을 고정하고  $m$ 을 변화시킨다고 합시다.  $M$ 의 정의에 의해,  $a_m \geq M - \frac{1}{2}\varepsilon$ 가 되도록 지표  $m$ 을 선택하는 것이 가능해야 합니다 ( $M - \frac{1}{2}\varepsilon$ 가 유효한 칼의 위치이므로 선택할 수 있는 항이 무한히 많고, 우리는  $m \geq n$ 만 필요합니다). 이 경우 우리는 다음을 얻습니다

$$|a_n - M| \leq |a_n - a_m| + |a_m - M| < \frac{1}{2}\varepsilon + \frac{1}{2}\varepsilon = \varepsilon$$

삼각부등식에 의해 성립합니다. 이것으로 증명이 완료됩니다.  $\square$

따라서 후자의 **정리 26.1.4**을 증명하는 것으로 충분합니다. 하지만 이를 위해서는 실수  $\mathbb{R}$ 에 대한 엄밀한 정의를 실제로 제시해야 하는데, 우리는 아직 이를 하지 않았습니다!

이를 쉽게 만드는 한 가지 접근법은 이른바 **데데킨트 절단**(Dedekind cut) 구성을 사용하는 것입니다. 유리수  $\mathbb{Q}$ 를 취한다고 합시다. 그러면 실수는 유리수 집합의 "절단"  $A \mid B$ 로 정의되는데, 이는 다음을 만족하는  $\mathbb{Q}$ 의 부분집합의 쌍입니다

- $\mathbb{Q} = A \sqcup B$ 는 서로소 합집합입니다;
- $A$ 와  $B$ 는 공집합이 아닙니다.
- 모든  $a \in A$ 와  $b \in B$ 에 대해  $a < b$ 가 성립하며,

- $A$ 는 최댓값을 갖지 않습니다 (즉,  $\sup A \notin A$ ).

이것 역시 여러분이 실수선이라고 생각하는 것을 어떤 실수에서 자른다고 상상하면 시각화할 수 있습니다. 부분집합  $\mathbb{Q} \subset \mathbb{R}$ 는 두 개의 반쪽  $A$ 와  $B$ 로 잘립니다. 만약 칼날이 정확히 유리수 지점에 떨어진다면, 관례상 그 수는 오른쪽 반쪽에 속하는 것으로 봅니다 (이것이  $\sup A \notin A$ 라는 마지막 조건을 설명해줍니다).

이 정의를 사용하면 **정리 26.1.4**은 쉽습니다: 실수 집합의 상한을 구하려면, 모든 왼쪽 반쪽들의 합집합을 취하면 됩니다. 어려운 부분은 이 다소 어색한 구성으로  $+$ ,  $-$ ,  $\times$ ,  $\div$  등을 어떻게 정의할지 알아내는 것입니다. 이 구성에 대해 자세히 더 읽어보고 싶다면, 제가 가장 좋아하는 참고 문헌은 [Pu02]이며, 여기서는 이 모든 것이 1장에서 신중하게 다루어집니다.

## §26.3 단조수열

여기 훌륭한 연습문제가 하나 있습니다.

**연습문제 26.3.1** (필수).  $a_1 \geq a_2 \geq \dots \geq 0$ 이면 다음 극한이

$$\lim_{n \rightarrow \infty} a_n$$

존재함을 증명하십시오. 힌트: 이전 절의 증명에 나온 아이디어가 도움이 됩니다;  $\mathbb{R}$ 의 완비성을 사용해 볼 수도 있습니다. 두 번째 힌트: 정말로 막힌다면, **명제 26.4.5** 이후까지 기다리십시오. 그 시점에서는 사실상 그 증명을 그대로 따라 쓸 수 있습니다.

여기서의 증명은 이동시킴으로써 쉽게 적용됩니다.

**정의 26.3.2.** 수열  $a_n$ 이  $a_1 \geq a_2 \geq \dots$  이거나  $a_1 \leq a_2 \leq \dots$  일 때 **단조**라고 합니다.

**정리 26.3.3** (단조 유계수열은 수렴한다)

$a_1, a_2, \dots$ 를 단조 유계수열이라 합시다. 그러면  $\lim_{n \rightarrow \infty} a_n$ 이 존재합니다.

**예제 26.3.4** (단조성의 사소한 예시)

다음과 같이 정의된 수열을 생각해봅시다

$$\begin{aligned} a_1 &= 1.2 \\ a_2 &= 1.24 \\ a_3 &= 1.248 \\ a_4 &= 1.24816 \\ a_5 &= 1.2481632 \\ &\vdots \end{aligned}$$

등등, 여기서 일반적으로 다음 2의 거듭제곱의 십진 표현을 이어 붙입니다. 이것은 어떤 실수로 수렴하겠지만, 물론 이 수는 상당히 부자연스러워서 좋은 설명 방법이 아마 없을 것입니다.

일반적으로, “무한소수”는 이제 절단된 유한소수들의 극한으로 정의될 수 있습니다.

**예제 26.3.5** ( $0.9999\cdots = 1$ )

특히, 여러분이 초등학교 시절에 논쟁했던 다음 개념을 이제 정확하게 만들 수 있습니다:

$$0.9999\cdots = 1.$$

우리는 순환소수를 단순히 수열  $0.9, 0.99, 0.999\cdots$ 의 극한으로 정의합니다. 그리고 이 수열의 극한이 1이라는 것은 명백합니다.

여러분 중 몇몇은 우리가 정말로  $0.9999 = 9 \cdot 10^{-1} + 9 \cdot 10^{-2} + \cdots$  — 즉 “부분합”의 극한 — 을 가져야 할 것 같아서 약간 놀랄 수도 있습니다. 걱정하지 마십시오, 곧 그것들을 정의할 것입니다.

여기 단조수열의 또 다른 훌륭한 활용이 있습니다.

**정의 26.3.6.**  $a_1, a_2, \dots$ 를 (반드시 단조일 필요는 없는) 아래로 유계인 수열이라 합시다. 우리는 다음과 같이 정의합니다

$$\limsup_{n \rightarrow \infty} a_n := \lim_{N \rightarrow \infty} \sup_{n \geq N} a_n = \lim_{N \rightarrow \infty} \sup \{a_N, a_{N+1}, \dots\}.$$

이것을  $(a_n)$ 의 **상극한**이라 부릅니다.  $a_n$ 이 위로 유계가 아니면  $\limsup_{n \rightarrow \infty} a_n$ 을  $+\infty$ 로 설정합니다.

$a_n$ 이 위로 유계이면, **하극한**  $\liminf_{n \rightarrow \infty} a_n$ 도 비슷하게 정의됩니다. 특히,  $a_n$ 이 아래로 유계가 아니면  $\liminf_{n \rightarrow \infty} a_n = -\infty$ 입니다.

**연습문제 26.3.7.** 상한들이 비증가하며 아래로 유계임을 확인하여, 이 정의들이 타당함을 보이십시오.

$\limsup_n a_n$ 은 “유한히 많은 항을 버리는 것을 허용한 상한”이라고 생각할 수 있습니다.

## §26.4 무한급수

**이 절의 대표적인 예:**  $\sum_{k=1}^{\infty} \frac{1}{k(k+1)} = \lim_{n \rightarrow \infty} \left(1 - \frac{1}{n+1}\right) = 1.$

우리는 실제로 무한급수를 다루는 것부터 시작할 것인데, 이전 장들에서 수열의 극한을 정의했으므로 이것이 실제로 다루기에 그다음으로 가까운 대상이기 때문입니다.<sup>1</sup>

이는 다음과 같은 서술을 엄밀하게 생각할 방법을 제공할 것입니다

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

그리고 “유리수를 더해서 어떻게 무리수를 얻을 수 있는가?”와 같은 질문에 답하는 데 도움이 될 것입니다.

<sup>1</sup>개념적으로 말하면, 이산적인 대상은 연속적인 대상보다 엄밀하게 다루기가 더 쉬우므로, 급수는 실제로 도함수보다 “더 쉽습니다”! 저는 대부분의 학교가 미적분학에서 급수를 마지막에 가르치는 이유가 대부분의 미적분학 강좌에 증명이 없기 때문이라고 짐작합니다.

**정의 26.4.1.** 실수의 수열  $a_1, \dots$ 을 생각합시다. 급수  $\sum_k a_k$ 가 극한  $L$ 로 **수렴한다**는 것은, "부분합"의 수열이

$$\begin{aligned}s_1 &= a_1 \\ s_2 &= a_1 + a_2 \\ s_3 &= a_1 + a_2 + a_3 \\ &\vdots \\ s_n &= a_1 + \dots + a_n\end{aligned}$$

극한  $L$ 로 수렴하면, 급수  $\sum_k a_k$ 는 극한  $L$ 로 **수렴한다**고 합니다. 그렇지 않으면 **발산한다**고 합니다.

**표기의 남용 26.4.2** (발산을  $+\infty$ 로 쓰기). 모든  $a_k$ 가 음이 아닌 경우, 급수가 발산함을 나타내기 위해  $\sum_k a_k = \infty$ 로 쓰는 것이 관례입니다.

수열의 정의를 사용함으로써, 그렇지 않았다면 온갖 문제를 일으켰을 "무한히 많은 수를 더하는" 문제를 훌륭하게 피했다는 것을 눈치채셨을 것입니다.

**"무한합"은 사실 부분합의 극한입니다. 무한한 덧셈은 전혀 관여하지 않습니다.**

그래서 예를 들어  $\sum_{n \geq 1} \frac{1}{n^2} = \frac{\pi^2}{6}$ 이 무리수여도 괜찮은 것입니다; 유리수의 수열이 무리수로 수렴할 수 있다는 것은 이미 여러 번 보았습니다. 이는 또한 중학생들의  $1 + 2 + 3 + \dots = -\frac{1}{12}$ 에 관한 짜증나는 게시물들을 기꺼이 무시할 수 있다는 뜻이기도 합니다; 부분합은  $+\infty$ 로 폭발하며, 그것으로 끝나고, 그 합에 값을 부여하고 싶다면 그것은 정의여야 마땅합니다.

#### 예제 26.4.3 (고전적인 망원급수)

이제 다음과 같은 고전적인 망원급수를

$$\sum_{k=1}^{\infty} \frac{1}{k(k+1)}$$

마무리를 손짓으로 얼버무리지 않는 방식으로 증명할 수 있습니다.  $k$ 번째 부분합이 다음과 같음을 주목하십시오

$$\begin{aligned}\sum_{k=1}^n \frac{1}{k(k+1)} &= \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \dots + \frac{1}{n(n+1)} \\ &= \left(\frac{1}{1} - \frac{1}{2}\right) + \dots + \left(\frac{1}{n} - \frac{1}{n+1}\right) \\ &= 1 - \frac{1}{n+1}.\end{aligned}$$

$n \rightarrow \infty$ 일 때 이 부분합의 극한은 1입니다.

#### 예제 26.4.4 (조화급수는 발산한다)

또한  $\sum_{k=1}^{\infty} \frac{1}{k} = \infty$ 라는 서술(즉, 발산한다는 것)의 의미도 명확히 할 수 있습니다.

$2^n$ 번째 부분합을 아래로부터 다음과 같이 유계로 만들 수 있습니다:

$$\begin{aligned}\sum_{k=1}^{2^n} \frac{1}{k} &= \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{2^n} \\ &\geq \frac{1}{1} + \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) \\ &\quad + \cdots + \underbrace{\left(\frac{1}{2^n} + \cdots + \frac{1}{2^n}\right)}_{2^{n-1} \text{ 항}} \\ &= 1 + \frac{1}{2} + \frac{1}{2} + \cdots + \frac{1}{2} = 1 + \frac{n-1}{2}.\end{aligned}$$

$s_{2^n} \geq 1 + \frac{1}{2}(n-1)$ 을 만족하는 수열은 결코 유한한 수로 수렴하지 않습니다!

음이 아닌 합에 대해서는, 수렴이 다음과 같은 의미에서 "유한한 합"을 갖는 것과 동일하다는 점도 언급해야겠습니다.

**명제 26.4.5** (음이 아닌 수의 부분합이 유계이면 수렴한다)

$\sum_k a_k$ 를 음이 아닌 실수의 급수라고 합시다. 그러면  $\sum_k a_k$ 가 어떤 극한으로 수렴하는 것은, 다음을 만족하는 상수  $M$ 이 존재하는 것과 동치입니다

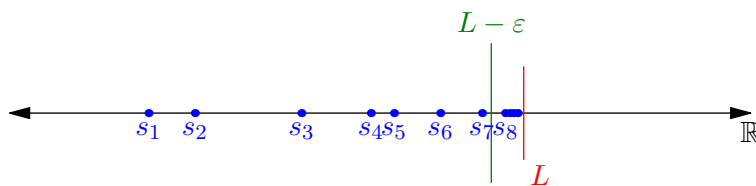
$$a_1 + \cdots + a_n < M$$

모든 양의 정수  $n$ 에 대하여.

증명. 이는 사실 **정리 26.3.3**가 모습을 바꾼 것에 불과하지만, 그때는 증명을 연습문제로 남겨두었으므로 이번에는 써 내려가겠습니다.

분명히 그러한  $M$ 이 존재하지 않는다면 수렴은 일어나지 않을 것인데, 이는 부분합의 수열  $s_n$ 이 유계가 아님을 의미하기 때문입니다.

반대로, 그러한  $M$ 이 존재한다면  $s_1 \leq s_2 \leq \cdots < M$ 을 얻습니다. 그러면 수열  $s_n$ 이  $L := \sup_n s_n < \infty$ 로 수렴한다고 주장할 수 있습니다. (완비성이 코시성을 함의한다는 증명을 읽으셨다면, 여기서의 그림도 거의 같지만 더 간단합니다.)



실제로 이는 임의의  $\varepsilon$ 에 대해 수열의 항 중  $L - \varepsilon$ 를 초과하는 항이 무한히 많다는 것을 의미합니다. 그러나 수열이 단조이므로, 일단  $s_n \geq L - \varepsilon$ 이면 모든  $n' \geq n$ 에 대해  $s_{n'} \geq L - \varepsilon$ 입니다. 이는 수렴을 함의합니다.  $\square$

**표기의 남용 26.4.6** ( $\sum < \infty$ 로 쓰기). 이러한 이유로,  $a_k$ 가 음이 아닌 실수일 때

$$\sum_k a_k < \infty$$

라고 쓰는 것이 관례인데, 이는 " $\sum_k a_k$ 가 유한한 극한으로 수렴한다"의 약칭입니다 (또는 어쩌면 " $\sum_k a_k$ 가 유계이다"의 약칭일 수도 있는데, 방금 이 두 가지가 동치임을 증명했기 때문입니다). 저희도 이 표기법을 사용하겠습니다.

## §26.5 급수의 덧셈은 교환법칙이 성립하지 않습니다: 공포 이야기

위 정의의 한 가지 불행한 성질은 그것이 실제로 원소들의 순서에 의존한다는 것입니다. 사실, 재배열이 괜찮은 경우를 명시적으로 설명하는 방법이 존재하는 것으로 밝혀집니다.

**정의 26.5.1.** 실수의 급수  $\sum_k a_k$ 가 **절대수렴한다**고 하는 것은 다음의 경우를 말합니다

$$\sum_k |a_k| < \infty$$

즉, 절댓값들의 급수가 어떤 극한으로 수렴한다는 것입니다. 급수가 수렴하지만 절대수렴하지는 않는 경우, 이를 **조건수렴한다**고 합니다.

### 명제 26.5.2 (절대수렴 $\implies$ 수렴)

실수의 급수  $\sum_k a_k$ 가 절대수렴하면, 이는 보통의 의미로도 수렴합니다.

**연습문제 26.5.3** (훌륭한 연습문제). 코시 판정법을 이용하여 이를 증명하십시오:  $\sum_k |a_k|$ 의 부분합이 코시 수열이면  $\sum_k a_k$ 의 부분합도 코시 수열임을 보이십시오.

그렇다면, 재배열은 아주 잘 작동합니다.

### 정리 26.5.4 (절대수렴에서는 항의 순열이 허용됨)

절대수렴하며 극한이  $L$ 인 급수  $\sum_k a_k$ 를 생각해봅시다. 그러면 항의 어떤 순열도 마찬가지로  $L$ 로 수렴합니다.

증명.  $\sum_k a_k$ 가  $L$ 로 수렴하고,  $b_n$ 이 그 재배열이라고 합시다.  $\varepsilon > 0$ 이라 합시다.  $b_n$ 의 부분합이 결국  $L$ 로부터  $\varepsilon$  이내에 들어옴을 보이겠습니다.

가정이 의미하는 바는,  $\varepsilon$ 에 대해 다음을 만족하는 충분히 큰  $N$ 이 존재한다는 것입니다

$$\left| \sum_{k=1}^N a_k - L \right| < \frac{1}{2}\varepsilon \quad \text{그리고} \quad \sum_{k=N+1}^n |a_k| < \frac{1}{2}\varepsilon$$

모든  $n \geq N$ 에 대해 (앞의 것은  $a_k$ 의 통상적인 수렴으로부터, 뒤의 것은  $a_k$ 가 절대수렴하여 그 부분합이 코시 수열이라는 사실로부터 나옵니다).

이제  $a_1, \dots, a_N$ 이 항  $\{b_1, \dots, b_M\}$  안에 포함될 만큼  $M$ 이 충분히 크다고 합시다. 그러면

$$b_1 + \dots + b_M = (a_1 + \dots + a_N) + \underbrace{a_{i_1} + a_{i_2} + \dots + a_{i_{M-N}}}_{\text{지표가 } > N \text{인 } M-N \text{개의 항}}$$

첫 번째 줄의 항들의 합은  $L$ 로부터  $\frac{1}{2}\varepsilon$  이내이고, 두 번째 줄의 항들의 합은 절댓값이 최대  $\frac{1}{2}\varepsilon$ 이므로, 전체  $b_1 + \dots + b_M$ 은  $L$ 로부터  $\frac{1}{2}\varepsilon + \frac{1}{2}\varepsilon = \varepsilon$  이내에 있습니다.  $\square$

특히, 항들이 음이 아닐 때는 상황이 아주 좋습니다:

**음이 아닌 급수는 원하는 대로 재배열될 수 있습니다.**

그리고 좋은 소식은, 실제로 실무에서는 대부분의 합이 음이 아닌 항으로 이루어진다는 것입니다.

그 역은 성립하지 않으며, 사실 상상할 수 있는 거의 최악의 역입니다.

**정리 26.5.5 (리만 재배열 정리: 조건수렴에서는 항의 순열이 무의미함)**

어떤 실수로 조건수렴하는 급수  $\sum_k a_k$ 를 생각해봅시다. 그러면 이 급수의 어떤 순열은 1337로 조건수렴합니다.  
(또는 어떤 상수로도 가능합니다. 발산하게 만들 수도 있습니다.)

따라서, 조건수렴하는 급수에 대해 순열은 최악의 상황이 될 수 있으므로, 시도조차 하지 않는 것이 좋습니다.

## §26.6 점에서의 함수의 극한

**이 절의 대표적인 예:**  $\lim_{x \rightarrow \infty} 1/x = 0$ .

저희는 실함수의 극한 개념도 정의해두는 것이 좋겠는데, (놀랍게도) 아직 실제로 정의하지 않았습니다. 이 정의는 앞서 연속성에서 본 것과 비슷한 형태를 띠 것입니다.

**정의 26.6.1.**  $f: \mathbb{R} \rightarrow \mathbb{R}$ 가 함수<sup>2</sup>이고  $p \in \mathbb{R}$ 이 정의역 내의 한 점이라고 합시다. 다음을 만족하는 실수  $L$ 이 존재한다고 가정합니다:

모든  $\varepsilon > 0$ 에 대해,  $|x - p| < \delta$ 이고  $x \neq p$ 이면  $|f(x) - L| < \varepsilon$ 가 성립하는  $\delta > 0$ 이 존재합니다.

그러면  $L$ 을  $x \rightarrow p$ 일 때  $f$ 의 **극한**이라고 하며, 다음과 같이 씁니다

$$\lim_{x \rightarrow p} f(x) = L.$$

여기서 중요한 점이 하나 있습니다: 이 정의에서 우리는  $x \neq p$ 를 일부러 요구합니다.

$\lim_{x \rightarrow p} f(x)$ 의 값은  $f(p)$ 에 의존하지 않으므로, 이에 따라 우리는 흔히  $f(p)$ 를 정의하는 수고조차 하지 않습니다.

**예제 26.6.2 (구멍이 있는 함수)**

함수  $f: \mathbb{R} \rightarrow \mathbb{R}$ 을 다음과 같이 정의합니다

$$f(x) = \begin{cases} 3x & \text{만약 } x \neq 0 \\ 2019 & \text{그렇지 않으면.} \end{cases}$$

그러면  $\lim_{x \rightarrow 0} f(x) = 0$ 입니다.  $f(0) = 2019$ 라는 값은 극한에 영향을 주지 않습니다. 당연히  $f(0)$ 은 극한과 일치하지 않는 어떤 인위적인 값으로 임의로 만들어졌기 때문에, 이 함수는  $x = 0$ 에서 불연속입니다.

**질문 26.6.3 (필수 문제).** 함수  $f$ 가  $p$ 에서 연속인 것은  $\lim_{x \rightarrow p} f(x)$ 가 존재하고  $f(p)$ 와 같은 것과 동치임을 보이십시오.

<sup>2</sup>또는  $f: (a, b) \rightarrow \mathbb{R}$ 이거나 그 변형이어도 됩니다. 우리는 그저  $f$ 가  $p$ 의 열린 근방에서 정의되어 있기만 하면 됩니다.

**예제 26.6.4 (덜 자명한 예: 유리수 조각별 함수)**

함수  $f: \mathbb{R} \rightarrow \mathbb{R}$ 을 다음과 같이 정의합니다:

$$f(x) = \begin{cases} 1 & \text{만약 } x = 0 \\ \frac{1}{q} & \text{만약 } x = \frac{p}{q} \text{ 여기서 } q > 0 \text{ 그리고 } \gcd(p, q) = 1 \\ 0 & \text{만약 } x \notin \mathbb{Q}. \end{cases}$$

예를 들어,  $f(\pi) = 0$ ,  $f(2/3) = \frac{1}{3}$ ,  $f(0.17) = \frac{1}{100}$ 입니다. 그러면

$$\lim_{x \rightarrow 0} f(x) = 0.$$

예를 들어,  $|x| < 1/100$ 이고  $x \neq 0$ 이면  $f(x)$ 는 ( $x$ 가 무리수인 경우) 0이거나, 그렇지 않으면 ( $x$ 가 유리수인 경우)  $\frac{1}{101}$ 입니다.  $f(0) = 1$ 이므로, 이 함수 역시  $x = 0$ 에서 불연속입니다. 그러나 정의를 바꾸어 대신  $f(0) = 0$ 으로 하면,  $f$ 는 0에서 연속이 됩니다.

**예제 26.6.5 (유명한 예)**

$f: \mathbb{R} \rightarrow \mathbb{R}$ 인  $f(x) = \frac{\sin x}{x}$ 를 생각합시다. 여기서  $f(0)$ 은 임의의 값으로 지정됩니다. 그러면

$$\lim_{x \rightarrow 0} f(x) = 1.$$

아직 삼각함수를 다루고 싶지 않으므로 여기서는 이를 증명하지 않겠습니다. 일반적으로 저는 삼각함수를 기본적으로 예시를 위해서만 사용할 뿐 어떤 이론을 위해서는 사용하지 않을 것이므로, 삼각함수의 대부분의 성질은 그저 인용만 될 것입니다.

**표기의 남용 26.6.6 (일반적인 표기법).** 이제부터 위 예시는 흔히 다음과 같이 줄여 씁니다

$$\lim_{x \rightarrow 0} \frac{\sin x}{x} = 1.$$

여기서 약간의 표기 남용이 있는 이유는, 원래 극한에는 함수  $f$ 를 넣어야 하는데, 대신 저는  $x = 0$ 을 제외한 모든 곳에서 정의되는 식을 적었기 때문입니다. 하지만 그  $f(0)$  값은 아무것도 바꾸지 않습니다. 따라서 위 표현은 다음을 의미합니다: " $f(x) = \frac{\sin x}{x}$ 로 기술되는 함수의 극한, 단  $f(0)$ 은 중요하지 않으므로 원하는 어떤 값이든 상관없다".

**비고 26.6.7 (거리 공간의 경우)** — 앞서 거리 공간 위의 함수  $f: M \rightarrow N$ 에 대해  $\lim_{x \rightarrow p} f(x)$ 라는 개념을 정의하지 않은 것이 의아할 수도 있습니다. 실제로 위와 같은 방식으로 정의할 수 있지만, 한 가지 미묘한 점이 있습니다: 만약 우리의 거리 공간  $M$ 이 이산적이어서  $p$  근처에 아무 점도 없다면 어떻게 될까요? (또는 더 간단히, 만약  $M$ 이 한 점짜리 공간이라면 어떻게 될까요?) 이 경우 우리는  $\lim_{x \rightarrow p} f(x)$ 를 아예 정의할 수 없습니다.

따라서  $f: M \rightarrow N$ 이고  $\lim_{x \rightarrow p} f(x)$ 를 정의하고자 한다면, 임의의  $\varepsilon > 0$ 에 대해  $p$ 로부터  $\varepsilon$  이내에 어떤 점이 있어야 한다는 조건이 필요합니다. 다시 말해,  $p$ 는 고립점이어서는 안 됩니다.

늘 그렇듯이, 산술 연산에는 아무런 놀라운 점이 없으며,  $\lim_{x \rightarrow p} (f(x) \pm g(x)) = \lim_{x \rightarrow p} f(x) \pm \lim_{x \rightarrow p} g(x)$ 가 성립하고, 이런 식으로 계속 성립합니다. 이 증명은 사실상 이전에 이미 해 보았으므로 다시 반복하지 않겠습니다.

## §26.7 무한대에서의 함수의 극한

성가시게도, 이 정의는 앞선 예시들과 전혀 다르게 느껴지지 않겠지만 실제로는 별도로 만들어야 합니다.

**정의 26.7.1.**  $f: \mathbb{R} \rightarrow \mathbb{R}$ 이라고 합시다. 다음을 만족하는 실수  $L$ 이 존재한다고 가정합니다:

모든  $\varepsilon > 0$ 에 대해,  $x > M$ 이면  $|f(x) - L| < \varepsilon$ 가 성립하는 상수  $M$ 이 존재합니다.

이때  $x$ 가  $\infty$ 에 접근할 때  $L$ 을  $f$ 의 **극한**이라 하고 다음과 같이 씁니다.

$$\lim_{x \rightarrow \infty} f(x) = L.$$

극한  $\lim_{x \rightarrow -\infty} f(x)$ 도  $x > M$ 을  $x < M$ 으로 바꾸어 마찬가지로 정의합니다.

다행히도  $\infty$ 는  $\mathbb{R}$ 의 원소가 아니므로, “임의로 설정된  $f(p)$ ”에서처럼  $f(\infty)$ 에 대해 같은 코예를 부릴 필요가 없습니다. 그래서 이러한 예시들은 더 쉽게 적을 수 있습니다.

### 예제 26.7.2 (무한대에서의 극한)

늘 그렇듯이:

$$\lim_{x \rightarrow \infty} \frac{1}{x} = 0.$$

증명까지 써 보겠습니다: 임의의  $\varepsilon > 0$ 에 대해,  $x > 1/\varepsilon$ 이면  $|\frac{1}{x} - 0| < \varepsilon$ 입니다.

산술 연산에는 놀라울 것이 없습니다:  $\lim_{x \rightarrow \infty} (f(x) \pm g(x)) = \lim_{x \rightarrow \infty} f(x) \pm \lim_{x \rightarrow \infty} g(x)$ 이며, 나머지도 마찬가지입니다. 이것을 언급하는 것이 이번이 대략 네 번째이므로, 더는 말하지 않겠습니다.

## §26.8 생각해 볼 만한 조금 더 어려운 문제

**문제 26A.** 다음 수열을 정의합니다

$$a_n = (-1)^n + \frac{n^3}{2^n}$$

모든 양의 정수  $n$ 에 대해. 극하한과 극상한을 계산하십시오.

**문제 26B.** 유계 수열  $a_n$  중 어떤 것들에서  $\liminf_n a_n = \limsup_n a_n$ 이 성립합니까?

**문제 26C<sup>†</sup>** (비교 판정법).  $\sum a_n$ 과  $\sum b_n$ 을 두 급수라 합시다.  $\sum b_n$ 이 절대수렴하고, 모든 정수  $n$ 에 대해  $|a_n| \leq |b_n|$ 이라 가정합니다.  $\sum_n a_n$ 이 절대수렴함을 증명하십시오.

**문제 26D** (등비급수).  $-1 < r < 1$ 을 실수라 합시다. 다음 급수가

$$1 + r + r^2 + r^3 + \dots$$

절대수렴함을 보이고 무엇으로 수렴하는지 구하십시오.

**문제 26E** (교대급수 판정법).  $a_0 \geq a_1 \geq a_2 \geq a_3 \geq \dots$ 를 음이 아닌 실수들로 이루어진 약하게 감소하는 수열이라 하고,  $\lim_{n \rightarrow \infty} a_n = 0$ 이라 가정합니다. 급수  $\sum_n (-1)^n a_n$ 이 수렴함을 보이십시오(절대수렴할 필요는 없습니다).



**문제 26F** ([Pu02, 제3장, 연습문제 55]).  $(a_n)_{n \geq 1}$ 과  $(b_n)_{n \geq 1}$ 을 실수들의 수열이라 합시다.  $a_1 \leq a_2 \leq \dots \leq 1000$ 이고 게다가  $\sum_n b_n$ 이 수렴한다고 가정합니다.  $\sum_n a_n b_n$ 이 수렴함을 증명하십시오. (가정과 결론 모두에서 절대수렴을 다루지 않음에 유의하십시오.)



**문제 26G** (Putnam 2016 B1).  $x_0 = 1$ 이고  $n \geq 0$ 에 대해 다음을 만족하는 수열  $x_0, x_1, x_2, \dots$ 가 있다고 합시다.

$$x_{n+1} = \log(e^{x_n} - x_n)$$

(통상적으로  $\log$ 는 자연로그입니다.) 무한급수  $x_0 + x_1 + \dots$ 가 수렴함을 증명하고 그 값을 구하십시오.

**문제 26H.** **예제 26.6.4**에서 다음과 같이 정의된 함수  $f: \mathbb{R} \rightarrow \mathbb{R}$ 를 다시 생각해 봅시다.

$$f(x) = \begin{cases} 1 & \text{만약 } x = 0 \\ \frac{1}{q} & \text{만약 } x = \frac{p}{q} \text{ 여기서 } q > 0 \text{ 그리고 } \gcd(p, q) = 1 \\ 0 & \text{만약 } x \notin \mathbb{Q}. \end{cases}$$

모든 실수  $c$ 에 대해,  $\lim_{x \rightarrow c} f(x)$ 가 존재한다면 이를 계산하십시오.  $f$ 는 어느 점에서 연속입니까?

# 27 Bonus: A hint of $p$ -adic numbers

이 보너스 장은 환과 체에 대해서도 읽은 분들을 위한 것으로, 대수학과 해석학이 만나는 지점에 있는 흥미로운 이야깃거리입니다.

이번 장에서는 절댓값  $|\cdot|$ 을  $p$ 진 절댓값으로 대체하여 이전 장의 내용 대부분을 다시 다루어 보겠습니다. 이를 통해  $p$ 진 정수  $\mathbb{Z}_p$ 와  $p$ 진수  $\mathbb{Q}_p$ 를 얻게 됩니다. 한 문장으로 설명하자면, 이들은 "법  $p^e$ 에 대한 완전한 정보를 담고 있는 정수/유리수"(오직 그 정보만을 담고 있는)입니다.

이어지는 모든 내용에서  $p$ 는 항상 소수를 나타낸다고 가정합니다. 처음 네 절에서는 기초가 되는 정의들을 다루며, USA TST 문제의 짧은 풀이로 마무리합니다. 그런 다음 연속함수  $f: \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ 에 관한 더욱 놀라운 결과들을 (대부분 증명 없이) 서술할 것입니다. 마지막으로  $p$ 진 해석학을 이용한 스킨-말러-레흐 정리의 유명한 증명으로 마무리합니다.

## §27.1 동기

$\mathbb{Z}_p$ 와  $\mathbb{Q}_p$ 가 실제로 무엇인지 알려드리기 전에, 이들이 어떤 역할을 할지 먼저 말씀드리겠습니다.

초등/올림피아드 정수론에서 우리는 이미 다음 두 가지 개념에 익숙합니다.

- 소수  $p$  또는 소수의 거듭제곱  $p^e$ 로 모듈로를 취하는 것, 그리고
- 지수  $\nu_p$ 를 살펴보는 것입니다.

첫 번째 항목을 좀 더 설명하겠습니다. 어떤 디오판토스 방정식이 있다고 합시다. 올림피아드 맥락에서는 방정식을  $p$ 로 모듈로 취해 다룰 수 있는 새로운 대상을 얻을 수 있습니다. 안타깝게도  $p$ 로 모듈로를 취하면 일부 정보를 잃게 됩니다. 축약사상  $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p$ 는 단사와는 거리가 멉니다.

더 세밀한 제어를 원한다면,  $p$  대신  $p^2$ 로 모듈로를 취하는 것을 고려할 수 있습니다. 이 역시 새로운 정보를 줄 수 있지만 (9를 법으로 한 세제곱수를 떠올려보십시오),  $\mathbb{Z}/p^2$ 는 체가 아니라는 단점이 있어,  $p$ 로 모듈로를 취했을 때 얻었던 좋은 대수적 성질들을 많이 잃게 됩니다.

$p$ 진수의 목표 중 하나는 앞서 설명한 이 두 가지 문제를 우회할 수 있다는 것입니다. 우리가 소개할  $p$ 진수는 다음과 같은 성질을 가질 것입니다.

1. 모든  $e$ 에 대해 " $p^e$ 로 모듈로를 한꺼번에" 취할 수 있습니다. 올림피아드 맥락에서는 특정 법을 선택한 다음 그 법을 취했을 때 어떤 일이 일어나는지 살펴보는 데 익숙합니다. 하지만  $p$ 진수를 사용하면 그러한 선택을 할 필요가 없습니다.  $p$ 진수의 방정식은  $p^e$ 로 모듈로를 취하기에 충분한 정보를 담고 있습니다.
2. 수  $\mathbb{Q}_p$ 는 체를 이룹니다. 이는 가능한 가장 좋은 대수적 구조로서,  $1/p$ 가 의미를 가집니다. 정역조차 아닌  $\mathbb{Z}/p^2$ 와 대조해 보십시오.
3.  $p$ 로 모듈로를 취하는 것만큼 정보를 잃지 않습니다. 전사사상  $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p$  대신, 단사사상  $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ 를 가집니다.
4. 그럼에도 불구하고, 몇몇 "무관한" 데이터를 "무시"하게 됩니다.  $p$ 로 모듈로를 취하는 것과 마찬가지로, 특정 종류의 대수적 정보에 집중하고자 하며, 이는 필연적으로

다른 것들을 놓치게 됨을 의미합니다.<sup>1</sup>

따라서  $p^e$  모듈로 정보에만 정말로 관심이 있지만 일반적인  $\mathbb{Z}/p^e$ 가 그다지 강력하지 못한 경우에 사용할 적절한 도구로  $p$ 진수를 생각할 수 있습니다.

좀 더 구체적으로, 이제 대표적인 예시를 하나 들겠습니다.

### 예제 27.1.1 (USA TST 2002/2)

소수  $p$ 에 대해, 다음 값이

$$f_p(x) = \sum_{k=1}^{p-1} \frac{1}{(px+k)^2} \pmod{p^3}$$

$x$ 에 의존하지 않음을 보이십시오.

여기 우리가 분명히  $p^e$  유형의 정보에만 관심이 있는 문제가 있습니다. 그럼에도  $p^3$ 을 법으로 필요한 조작을 수행하는 것은 만만치 않은 도전입니다 (직접 해보십시오!). 근본적인 문제는  $p^3$ 을 법으로 분모를 다룰 좋은 방법이 없다는 것입니다 (그 이유 중 하나는  $\mathbb{Z}/p^3$ 이 정역조차 아니기 때문입니다).

하지만  $p$ 진 해석학을 이용하면 이러한 한계를 극복하고 다음 항등식을 이용해 "간단한" 증명을 제시할 수 있습니다.

$$\left(1 + \frac{px}{k}\right)^{-2} = \sum_{n \geq 0} \binom{-2}{n} \left(\frac{px}{k}\right)^n.$$

이러한 항등식은 수렴 문제로 인해  $\mathbb{Q}$ 나  $\mathbb{R}$  위에서는 아무런 의미가 없지만,  $\mathbb{Q}_p$  위에서는 문제없이 작동하며, 우리에게 필요한 것은 그것뿐입니다.

## §27.2 대수적 관점

**이 절의 대표적인 예:**  $-1/2 = 1 + 3 + 3^2 + 3^3 + \dots \in \mathbb{Z}_3$ .

이제  $\mathbb{Z}_p$ 와  $\mathbb{Q}_p$ 를 구성하겠습니다. 앞서  $p$ 진 정수를 이용하면 "모든  $p^e$  나머지"를 한꺼번에 살펴볼 수 있다고 약속드렸습니다. 이 정의는 이를 공식화할 것입니다.

### §27.2.i $\mathbb{Z}_p$ 의 정의

**정의 27.2.1** ( $\mathbb{Z}_p$ 의 소개).  $p$ 진 정수는 다음과 같은 수열입니다

$$x = (x_1 \bmod p, x_2 \bmod p^2, x_3 \bmod p^3, \dots)$$

각 정수  $e$ 에 대해  $p^e$ 를 법으로 하는 나머지  $x_e$ 들이며,  $i < j$ 일 때 호환 관계  $x_i \equiv x_j \pmod{p^i}$ 를 만족합니다.

$p$ 진 정수들의 집합  $\mathbb{Z}_p$ 는 성분별 덧셈과 곱셈 아래 환을 이룹니다.

<sup>1</sup>비유를 들자면, 방정식  $a^2 + b^2 + c^2 + d^2 = -1$ 은 정수해를 갖지 않습니다. 그야, 제곱수는 음이 아니기 때문입니다. 하지만 이 방정식이 임의의 소수  $p$ 를 법으로 해를 갖는다는 것을 알게 될 것인데, 이는  $p$ 로 모듈로를 취하는 순간부터 수가 음이 아니라는 것을 더 이상 말할 수 없게 되기 때문입니다.  $p$ 진수로 작업할 때도 같은 일이 일어날 것입니다. 위 방정식은 모든 소수  $p$ 에 대해  $\mathbb{Z}_p$ 에서 해를 가집니다.

**예제 27.2.2 (몇 가지 3진 정수)**

$p = 3$ 이라 합시다. 모든 보통 정수  $n$ 은 각  $e$ 에 대해  $p^e$ 를 법으로 하는 (호환되는) 나머지 수열을 생성하므로, 각 보통 정수를  $p$ 진 정수로 볼 수 있습니다:

$$50 = (2 \bmod 3, 5 \bmod 9, 23 \bmod 27, 50 \bmod 81, 50 \bmod 243, \dots).$$

반면, 호환 관계를 만족함에도 불구하고 어떤 보통 정수에도 대응하지 않는 나머지 수열들이 존재합니다. 예를 들면

$$(1 \bmod 3, 4 \bmod 9, 13 \bmod 27, 40 \bmod 81, \dots)$$

이는  $x = 1 + p + p^2 + \dots$ 로 생각할 수 있습니다.

이런 방식으로 단사 사상을 얻습니다

$$\mathbb{Z} \hookrightarrow \mathbb{Z}_p \quad n \mapsto (n \bmod p, n \bmod p^2, n \bmod p^3, \dots)$$

이는 전사가 아닙니다. 따라서  $p$ 진 정수는 보통 정수보다 더 많습니다.

(전문가를 위한 비고: 범주론에 익숙하신 분들은 이 정의가 다음과 같이 간결하게 쓰일 수 있음을 알아차리실 수 있습니다)

$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^e \mathbb{Z}$$

여기서 역극한은  $e \geq 1$  범위에서 취해집니다.)

**연습문제 27.2.3.**  $\mathbb{Z}_p$ 가 정역임을 확인하십시오.

**§27.2.ii  $p$ 진 전개**

$p$ 진 정수를 생각하는 또 다른 방법으로 " $p$ 진법"을 사용하는 것이 있습니다. 앞선 예에서처럼, 모든 보통 정수는  $p$ 진법으로 쓸 수 있습니다. 예를 들면

$$50 = \overline{1212}_3 = 2 \cdot 3^0 + 1 \cdot 3^1 + 2 \cdot 3^2 + 1 \cdot 3^3.$$

더 일반적으로, 임의의  $x = (x_1, \dots) \in \mathbb{Z}_p$ 가 주어졌을 때,  $x_{k-1}$ 이 주어지면  $x_k$ 의 선택지가 정확히  $p$ 개 있다는 의미에서 " $p$ 진법" 전개를 적어볼 수 있습니다. 앞선 예를 계속하면 다음과 같이 쓸 수 있습니다

$$\begin{aligned} (1 \bmod 3, 4 \bmod 9, 13 \bmod 27, 40 \bmod 81, \dots) &= 1 + 3 + 3^2 + \dots \\ &= \overline{\dots 1111}_3 \end{aligned}$$

그리고 일반적으로 다음과 같이 쓸 수 있습니다

$$x = \sum_{k \geq 0} a_k p^k = \overline{\dots a_2 a_1 a_0}_p$$

여기서  $a_k \in \{0, \dots, p-1\}$ 이며, 각  $e$ 에 대해  $p^e$ 를 법으로 이 등식이 성립합니다. 이 전개가 왼쪽으로 무한하다는 점에 주목하십시오. 이는 여러분이 익숙한 것과 다릅니다.

(흥미롭게도, 음의 정수 또한 무한한  $p$ 진 전개를 가집니다:  $-4 = \overline{\dots 222212}_3$ 이며, 이는  $(2 \bmod 3, 5 \bmod 9, 23 \bmod 27, 77 \bmod 81, \dots)$ 에 대응됩니다.)

그러므로  $p$ 진 정수란 "어쩌면 무한할 수 있는  $p$ 진 전개"라는 설명을 자주 듣게 될 수 있습니다. 이는 맞는 말이지만, 이후로 우리는  $\mathbb{Z}_p$ 를 점점 더 "해석적인" 방식으로 생각하게 될 것이므로, 저는 이를 다음과 같이 생각하는 것을 선호합니다

$p$ 진 정수는 밑이  $p$ 인 테일러 급수입니다.

실제로, 생성함수  $K[[X]]$  (여기서  $K$ 는 체입니다)에 대한 여러분의 직관 대부분이  $\mathbb{Z}_p$ 로 옮겨갈 것입니다.

### §27.2.iii $\mathbb{Q}_p$ 의 구성

생성함수에 대한 직관이 옮겨가는 한 가지 방식은 다음과 같습니다:

**명제 27.2.4** ( $p$ 의 배수가 아닌 것은 모두 가역입니다)

$x \in \mathbb{Z}_p$ 인 수는  $x_1 \neq 0$ 일 때에만 가역입니다. 기호로 나타내면,

$$x \in \mathbb{Z}_p^\times \iff x \not\equiv 0 \pmod{p}.$$

$K[[X]]$ 에 대한 대응되는 명제와 이를 대조해 봅시다: 생성함수  $F \in K[[X]]$ 가 가역적인 것은  $F(0) \neq 0$ 일 때이고 오직 그때뿐입니다.

증명.  $x \equiv 0 \pmod{p}$ 이면  $x_1 = 0$ 이므로 명백히 가역적이지 않습니다. 그렇지 않으면 모든  $e$ 에 대해  $x_e \not\equiv 0 \pmod{p}$ 이므로,  $x_e y_e \equiv 1 \pmod{p^e}$ 을 만족하는  $p^e$ 법 역원  $y_e$ 를 취할 수 있습니다.  $y_e$  자체가 서로 호환되므로, 원소  $(y_1, y_2, \dots)$ 가 역원이 됩니다.  $\square$

**예제 27.2.5** ( $-\frac{1}{2} = \overline{\dots 1111}_3 \in \mathbb{Z}_3$ 입니다)

앞서 든 예시가 실제로는 다음과 같음을 주장합니다

$$\begin{aligned} -\frac{1}{2} &= (1 \bmod 3, 4 \bmod 9, 13 \bmod 27, 40 \bmod 81, \dots) = 1 + 3 + 3^2 + \dots \\ &= \overline{\dots 1111}_3. \end{aligned}$$

실제로, 이것에  $-2$ 를 곱하면 다음이 나옵니다

$$(-2 \bmod 3, -8 \bmod 9, -26 \bmod 27, -80 \bmod 81, \dots) = 1.$$

(이것을 “기하급수”  $1 + 3 + 3^2 + \dots = \frac{1}{1-3}$ 과 비교해 보십시오. 이는 나중에 실제로 형식화할 수 있게 되지만, 아직은 아닙니다.)

**비고 27.2.6** ( $p > 2$ 일 때  $\frac{1}{2}$ 는 정수입니다) — 앞선 명제는 (다른 것들 중에서도)  $\frac{1}{2} \in \mathbb{Z}_3$ 임을 함의합니다; 여기서 “정수”가 무엇인지에 대한 여러분의 직관은 다를 것입니다! 올림피아드적인 관점에서 우리는 이미  $\frac{1}{2} \pmod{3}$ 이 의미가 있음을 알고 있었으며, 이것이 바로 3진수에서  $\frac{1}{2}$ 를 “정수”라고 부르는 것이 옳은 이유입니다, 비록 이것이  $\mathbb{Z}$ 의 어떤 원소에도 대응하지 않지만 말입니다.

**연습문제 27.2.7** (중요하지는 않지만 까다로운 사실). 유리수는 정확히 결국 주기적인  $p$ 진 전개에 대응됩니다.

이 관찰을 바탕으로, 이제  $\mathbb{Q}_p$ 의 정의를 소개하겠습니다.

**정의 27.2.8** ( $\mathbb{Q}_p$  소개).  $\mathbb{Z}_p$ 가 정역이므로,  $\mathbb{Q}_p$ 를 그 분수체라고 하겠습니다. 이것이 바로  $p$ 진수입니다.

우리의 생성함수 유비를 계속 이어가면:

$$\mathbb{Z}_p \text{ 하는 것입니다 } \mathbb{Q}_p \text{ 와 같습니다 } K[[X]] \text{ 하는 것입니다 } K((X)).$$

이는 다음을 의미합니다

$\mathbb{Q}_p$ 는 밑을  $p$ 로 하는 로랑 급수로 생각할 수 있습니다.

그리고 특히 앞선 명제에 따라 다음을 유도할 수 있습니다:

**명제 27.2.9** ( $\mathbb{Q}_p$ 는 형식적 로랑 급수처럼 보입니다)

$\mathbb{Q}_p$ 의 모든 0이 아닌 원소는 유일하게 다음과 같은 꼴입니다

$$p^k u \quad \text{여기서 } k \in \mathbb{Z}, u \in \mathbb{Z}_p^\times.$$

따라서, 우리의  $p$ 진 유비를 계속 이어가면,  $\mathbb{Q}_p$ 의 원소들은 다음의 “로랑 급수”와 전단사 관계에 있습니다

$$\sum_{k \geq -n} a_k p^k = \overline{\dots a_2 a_1 a_0 \cdot a_{-1} a_{-2} \dots a_{-n} p}$$

여기서  $a_k \in \{0, \dots, p-1\}$ 입니다. 그러므로  $\mathbb{Q}_p$  원소의  $p$ 진 표현은 보통의 경우와 같은 것으로 생각할 수 있지만, (오른쪽이 아니라) 왼쪽으로 무한히 뻗어 나간다는 점이 다릅니다.

**비고 27.2.10 (경고)** — 체  $\mathbb{Q}_p$ 의 표수는  $p$ 가 아니라 0입니다.

**비고 27.2.11 (분수체에 관한 경고)** — 이 결과는 실제로는  $\mathbb{Q}_p$ 의 원소를  $(x, y \in \mathbb{Z}_p$ 에 대해)  $x/y$ 로 생각해서는 안 된다는 것을 함의합니다, 비록 이것이 공식적인 정의이고 (또한  $\mathbb{Q}_p$ 라는 이름에서 기대할 법한 것이기도) 하지만 말입니다. 필요한 분모는 오직  $p$ 의 거듭제곱뿐입니다.

형식적 로랑 급수 유비를 계속 밀고 나가면,  $K((X))$ 는 보통 생성함수의 몫으로 생각되지 않고 오히려 “일부 음의 지수를 갖는 형식적 급수”로 생각됩니다.  $\mathbb{Q}_p$ 에도 같은 직관을 적용해야 합니다.

**비고 27.2.12** — 이 시점에서  $1/p \in \mathbb{Q}_p$ 라는 사실에 대해 언급하고자 하며, 이를 앞서 제시했던 성질들의 희망 목록과 연결 짓고자 합니다. 초등 정수론에서는  $p$ 법으로 방정식을 취할 수 있지만, 그렇게 하면  $n \bmod p^2$ 을 알지 못하는 한  $n/p \bmod p$ 라는 양은 의미가 없습니다. 단순히  $p^2$ 법을 취하는 것으로는 이 문제를 해결할 수 없는데, 그러면  $n/p \bmod p^2$ 을 얻기 위해  $n \bmod p^3$ 이 필요하게 되고, 이는 무한히 계속됩니다. 이러한 문제는 우회할 수 있지만,  $\mathbb{Z}_p$ 와  $\mathbb{Q}_p$ 의 좋은 특징은 “모든  $e$ 에 대해 동시에”  $p^e$ 법 정보를 갖는다는 것입니다:  $x \in \mathbb{Q}_p$ 라는 정보는 모든  $p^e$ 법 정보를 동시에 담고 있습니다. 그러므로 아무런 부작용 없이  $p$ 로 나눌 수 있습니다.

## §27.3 해석적 관점

### §27.3.i 정의

지금까지 우리는 주로 대수적으로 사물을 생각해 왔지만, 앞으로는 해석학의 언어를 사용하기 시작하는 것이 도움이 될 것입니다. 보통 두 실수는 수직선 위에서 가까우면 “가깝다”고 여겨지지만,  $p$ -진적 목적을 위해서는 오직  $p^e$ 법 정보만이 중요합니다. 그러므로 우리는 대신  $\mathbb{Z}_p$ 나  $\mathbb{Q}_p$ 의 두 원소가  $p^e$ 의 큰 배수만큼 차이가 날 때 “가깝다”고 생각하겠습니다.

이를 위해 초등 정수론에서 친숙한  $\nu_p$ 를 빌려오겠습니다.

**정의 27.3.1** ( $p$ -진 값매김과 절댓값). 다음과 같은 두 가지 동치인 방법으로  $p$ -진 값매김  $\nu_p: \mathbb{Q}_p^\times \rightarrow \mathbb{Z}$ 을 정의합니다:

- $x = (x_1, x_2, \dots) \in \mathbb{Z}_p$ 에 대해,  $\nu_p(x)$ 를  $x_e \equiv 0 \pmod{p^e}$ 를 만족하는 가장 큰  $e$ 로 정의합니다 ( $x \in \mathbb{Z}_p^\times$ 인 경우에는  $e = 0$ ). 그런 다음  $\nu_p(xy) = \nu_p(x) + \nu_p(y)$ 에 의해  $\mathbb{Q}_p^\times$  전체로 확장합니다.
- 각  $x \in \mathbb{Q}_p^\times$ 는  $u \in \mathbb{Z}_p^\times$ ,  $k \in \mathbb{Z}$ 에 대해  $p^k u$ 의 꼴로 유일하게 쓸 수 있습니다. 이때  $\nu_p(x) = k$ 로 둡니다.

관례상  $\nu_p(0) = +\infty$ 로 둡니다. 마지막으로,  $p$ -진 절댓값  $|\cdot|_p$ 를 다음과 같이 정의합니다:

$$|x|_p = p^{-\nu_p(x)}.$$

특히  $|0|_p = 0$ 입니다.

이는 큰  $e$ 에 대해  $x$ 와  $y$ 가 법  $p^e$ 에서 같아 보이면 서로 가깝다는 약속을 충족시킵니다. 이 경우  $\nu_p(x - y)$ 가 크고, 그에 따라  $|x - y|_p$ 가 작아집니다.

### §27.3.ii 초거리 공간

이렇게 해서,  $\mathbb{Q}_p$ 와  $\mathbb{Z}_p$ 는  $|x - y|_p$ 로 주어지는 거리를 가진 거리 공간이 됩니다.

**연습문제 27.3.2.**  $f: \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ 가 연속이고 모든  $n \in \mathbb{Z}_{\geq 0}$ 에 대해  $f(n) = (-1)^n$ 이라고 합시다.  $p = 2$ 임을 증명하십시오.

사실, 이 공간들은  $\mathbb{R}$ 에서 익숙한 것보다 더 강한 형태의 삼각부등식을 만족합니다.

#### 명제 27.3.3 ( $|\cdot|_p$ 는 초거리입니다)

임의의  $x, y \in \mathbb{Z}_p$ 에 대해, 다음과 같은 **강한 삼각부등식**이 성립합니다

$$|x + y|_p \leq \max\{|x|_p, |y|_p\}.$$

$|x|_p \neq |y|_p$ 이면 (그러나 이 경우에만 그런 것은 아니고) 등호가 성립합니다.

하지만  $\mathbb{Q}_p$ 는 단순한 거리 공간 이상입니다: 그것은 고유한 덧셈과 곱셈을 가진 체입니다. 이는  $\mathbb{R}$ 이나  $\mathbb{C}$ 에서처럼 해석학을 할 수 있다는 것을 의미합니다: 기본적으로 “연속함수”, “수렴하는 급수” 등의 개념은 모두  $p$ -진 유사체를 가집니다. 특히, 무한합이 수렴한다는 것이 무엇을 의미하는지 정의할 수 있습니다:

**정의 27.3.4** (수렴 개념). 다음은 “현실 세계”의 개념에 대한  $p$ -진 유사체의 몇 가지 예시입니다.

- 수열  $s_1, \dots$  은  $\lim_{n \rightarrow \infty} |s_n - L|_p = 0$ 이면 극한  $L$ 로 수렴합니다.
- 무한급수  $\sum_k x_k$ 는 부분합의 수열  $s_1 = x_1, s_2 = x_1 + x_2, \dots$ 가 어떤 극한으로 수렴하면 수렴합니다.
- ... 기타 등등 ...

이 정의를 갖추면, 앞서 다룬 “ $p$ 진법” 논의는 이제 해석학적 의미에서 참이 됩니다:  $x = \dots \overline{a_2 a_1 a_0}_p \in \mathbb{Z}_p$ 이면

$$\sum_{k=0}^{\infty} a_k p^k \text{ 로 수렴합니다.}$$

실제로,  $x$ 와  $n$ 번째 부분합 사이의 차는  $p^n$ 으로 나누어떨어지므로,  $n \rightarrow \infty$ 일 때 부분합은  $x$ 에 접근합니다.

정의를 모두 동일하지만, 성립해야 할 성질에는 몇 가지 변화가 있습니다. 예를 들어,  $\mathbb{Q}_p$ 에서 부분합의 수렴은 더 간단합니다:

**명제 27.3.5** ( $|x_k|_p \rightarrow 0$ 과 급수의 수렴은 동치입니다)

$\mathbb{Q}_p$ 에서 급수  $\sum_{k=1}^{\infty} x_k$ 가 어떤 극한으로 수렴하는 것은  $\lim_{k \rightarrow \infty} |x_k|_p = 0$ 인 것과 동치입니다.

이는  $\mathbb{R}$ 에서  $\sum \frac{1}{n} = \infty$ 인 것과 대조됩니다. 이는 강한 삼각부등식의 결과로 생각할 수 있습니다.

증명. 충분히 큰  $p$ 의 거듭제곱을 곱함으로써,  $x_k \in \mathbb{Z}_p$ 라고 가정할 수 있습니다. (실제로 필요한 것은 아니지만, 표기를 더 깔끔하게 만들어 줍니다.)

$x_k \pmod{p}$ 가 결국 안정된다는 것을 관찰하십시오. 왜냐하면 충분히 큰  $n$ 에 대해  $|x_n|_p < 1 \iff \nu_p(x_n) \geq 1$ 이기 때문입니다. 따라서 큰  $N$ 에 대해  $\sum_{k=0}^N x_k \pmod{p}$ 의 최종적인 법  $p$  나머지를  $a_1$ 이라고 합시다. 같은 방식으로 법  $p^2$ 의 최종적인 나머지를  $a_2$ 라고 하고, 이런 식으로 계속합니다. 그러면 우리가 극한  $a = (a_1, a_2, \dots)$ 에 접근함을 확인할 수 있습니다.  $\square$

### §27.3.iii 등비급수에 관한 더 재미있는 이야기

이제 드디어 등비급수 공식의  $p$ 진 유사물을 서술해 보겠습니다.

**명제 27.3.6** (등비급수)

$|x|_p < 1$ 을 만족하는  $x \in \mathbb{Z}_p$ 가 있다고 합시다. 그러면

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \dots$$

증명. 부분합이  $1 + x + x^2 + \dots + x^n = \frac{1-x^{n+1}}{1-x}$ 를 만족하고,  $|x|_p < 1$ 이므로  $n \rightarrow \infty$ 일 때  $x^{n+1} \rightarrow 0$ 임에 주목하십시오.  $\square$

따라서  $1 + 3 + 3^2 + \dots = -\frac{1}{2}$ 는  $\mathbb{Z}_3$ 에서 실제로 올바른 수렴입니다. 다른 경우도 마찬가지입니다.

$\mathbb{Z}_p$ 가 밑을  $p$ 로 하는 생성함수라는 유비를 받아들인다면, 여러분이 익숙한 올림피아드의 모든 생성함수는  $p$ 진 유사물을 갖습니다. 예를 들어, 다음을 더 일반적으로 증명할 수 있습니다:

**정리 27.3.7 (일반화된 이항정리)**

$x \in \mathbb{Z}_p$ 이고  $|x|_p < 1$ 이면, 임의의  $r \in \mathbb{Q}$ 에 대해 다음과 같은 급수 수렴이 성립합니다

$$\sum_{n \geq 0} \binom{r}{n} x^n = (1+x)^r.$$

(( $(1+x)^r$ 을 정의하지는 않았지만, 여러분이 기대하는 성질을 갖습니다.)

**§27.3.iv 완비성**

$|\cdot|_p$ 의 정의는  $\mathbb{Q}$ 에 대해서도 마찬가지로 주어질 수 있었다는 점에 주목하십시오. 이를 도입하는 데  $\mathbb{Q}_p$ 가 필요하지는 않았습니(어쨌든 우리는 올림피아드에서 이미  $\nu_p$ 를 가지고 있습니다). 이제 제가 서술해야 할 크고 중요한 정리는 다음과 같습니다:

**정리 27.3.8 ( $\mathbb{Q}_p$ 는 완비이다)**

공간  $\mathbb{Q}_p$ 는  $|\cdot|_p$ 에 대한  $\mathbb{Q}$ 의 완비화입니다.

이것이 여러분이 더 자주 보게 될  $\mathbb{Q}_p$ 의 정의입니다. 그런 다음 (반대가 아니라)  $\mathbb{Q}_p$ 를 이용해  $\mathbb{Z}_p$ 를 다음에 따라 정의합니다

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

**§27.3.v 철학적 소견**

이 정의가 철학적으로 왜 좋은지 정당화해 보겠습니다. 여러분이 다음과 같은 문제를 받은 고대 그리스의 수학자라고 합시다:

**고대 그리스인을 위한 문제.** 다음 합의 값을

$$S = \frac{1}{1^2} + \frac{1}{2^2} + \cdots + \frac{1}{10000^2}$$

0.001 이내로 추정하십시오.

합  $S$ 는 전적으로 유리수로 이루어져 있으므로, 이 문제 서술은 고대 그리스에서도 합당한 문제일 것입니다. 하지만 좋은 추정값을 얻으려면 실수에 대해 아는 것이 정말로 도움이 된다는 사실이 밝혀집니다: 그러면 무한급수  $\sum_{n \geq 1} n^{-2} = \frac{1}{6}\pi^2$ 을 구성할 수 있고,  $\frac{1}{10001^2}$  이후의 항들에서 오는, 유계로 만들 수 있는 작은 오차항을 제외하면  $S \approx \frac{\pi^2}{6}$ 이라고 추론할 수 있기 때문입니다.

물론  $S = \pi^2/6$ 임을 증명할 수 있을 만큼 충분한 이론에 접근하려면 실수가 있어야 합니다.  $\mathbb{Q}$ 에서는 미적분학을 하는 것이 불가능합니다(수열 1, 1.4, 1.41, 1.414, ...는 "수렴하지 않는다"고 간주됩니다!)

이제 2002년으로 시간을 빨리 돌려서, 여러분이 다음과 같은 문제를 받았다고 합시다

**2002년 미국 TST 문제.** 다음 합을

$$f_p(x) = \sum_{k=1}^{p-1} \frac{1}{(px+k)^2}$$

$p^3$ 을 법으로 하여 이내로 추정하십시오.

$f_p(x)$ 가 유리수임에도 불구하고, 무한합을 가지고 해석을 할 수 있고 그런 다음 오차항을 유계로 만드는(즉  $p^3$ 을 법으로 취하는) 것은 여전히 도움이 됩니다. 하지만 공간  $\mathbb{Q}$  역시  $|\cdot|_p$ 에 대해 완비가 아니며, 따라서  $|\cdot|_p$ 에 대한  $\mathbb{Q}$ 의 완비화에서 작업하는 것이 타당합니다. 이것이 바로  $\mathbb{Q}_p$ 입니다.

어쨌든, 이제 드디어 **예제 27.1.1**을 풀어 봅시다.

### 예제 27.3.9 (2002년 미국 TST)

이제 다음을 계산하겠습니다

$$f_p(x) = \sum_{k=1}^{p-1} \frac{1}{(px+k)^2} \pmod{p^3}.$$

일반화된 이항 정리로 무장하면, 이는 간단해집니다.

$$\begin{aligned} f_p(x) &= \sum_{k=1}^{p-1} \frac{1}{(px+k)^2} = \sum_{k=1}^{p-1} \frac{1}{k^2} \left(1 + \frac{px}{k}\right)^{-2} \\ &= \sum_{k=1}^{p-1} \frac{1}{k^2} \sum_{n \geq 0} \binom{-2}{n} \left(\frac{px}{k}\right)^n \\ &= \sum_{n \geq 0} \binom{-2}{n} \sum_{k=1}^{p-1} \frac{1}{k^2} \left(\frac{x}{k}\right)^n p^n \\ &\equiv \sum_{k=1}^{p-1} \frac{1}{k^2} - 2x \left(\sum_{k=1}^{p-1} \frac{1}{k^3}\right) p + 3x^2 \left(\sum_{k=1}^{p-1} \frac{1}{k^4}\right) p^2 \pmod{p^3}. \end{aligned}$$

$p^2 \mid \sum_k k^{-3}$ 이고  $p \mid \sum_k k^{-4}$ 라는 기본적인 사실을 이용하면, 이는 문제를 해결합니다.

## §27.4 Mahler 계수

$p$ 진 해석학의 큰 놀라움 중 하나는 다음과 같습니다.

**우리는 기본적으로 모든 연속함수  $\mathbb{Z}_p \rightarrow \mathbb{Q}_p$ 를 서술할 수 있습니다.**

이들은 함수들의 기저로 주어지는데,

$$\binom{x}{n} := \frac{x(x-1)\dots(x-(n-1))}{n!}$$

다음과 같은 방식으로 주어집니다.

**정리 27.4.1** (Mahler; [Sc07, 정리 51.1, 연습문제 51.b] 참고)

$f: \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ 가 연속이라 하고, 다음을 정의합니다.

$$a_n = \sum_{k=0}^n \binom{n}{k} (-1)^{n-k} f(k). \quad (27.1)$$

그러면  $\lim_n a_n = 0$ 이며

$$f(x) = \sum_{n \geq 0} a_n \binom{x}{n}.$$

역으로,  $a_n$ 이 0으로 수렴하는 임의의 수열이라면,  $f(x) = \sum_{n \geq 0} a_n \binom{x}{n}$ 은 (27.1)를 만족하는 연속함수를 정의합니다.

$a_i$ 는  $f$ 의 Mahler 계수라고 불립니다.

**연습문제 27.4.2.** 앞서 우리는  $f: \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ 가 연속이고 모든  $n \in \mathbb{Z}_{\geq 0}$ 에 대해  $f(n) = (-1)^n$ 이면  $p = 2$ 임을 증명했습니다. Mahler 정리를 이용하여 이를 다시 증명하고, 이번에는 역으로  $p = 2$ 일 때 그러한  $f$ 가 유일하게 존재함을 보이십시오.

이것들은 고등학교 수학경시대회에서 다항식에 사용하는 것과 동일한 유한차분임을 알 수 있으며, 이 때문에 이들은 또한 "Mahler 차분"이라고도 불립니다.

$$\begin{aligned} a_0 &= f(0) \\ a_1 &= f(1) - f(0) \\ a_2 &= f(2) - 2f(1) + f(0) \\ a_3 &= f(3) - 3f(2) + 3f(1) - f(0). \end{aligned}$$

따라서  $a_n \rightarrow 0$ 이라는 것은,  $f(0), f(1), \dots$ 의 값들이 모든  $e \geq 0$ 에 대해 법  $p^e$ 로 다항식처럼 행동한다는 의미로 생각할 수 있습니다.

"해석적"이라는 개념 또한 Mahler적 해석을 가집니다. 먼저 정의부터 하겠습니다.

**정의 27.4.3.** 함수  $f: \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ 가 다음과 같은 거듭제곱급수 전개를 가지면 **해석적**이라고 말합니다

$$\sum_{n \geq 0} c_n x^n \quad c_n \in \mathbb{Q}_p \quad \text{에 대해 수렴하는 } x \in \mathbb{Z}_p.$$

**정리 27.4.4** ([Sc07, 정리 54.4])

함수  $f(x) = \sum_{n \geq 0} a_n \binom{x}{n}$ 이 해석적일 필요충분조건은 다음과 같습니다

$$\lim_{n \rightarrow \infty} \frac{a_n}{n!} = 0.$$

해석적 함수는 또한 다음과 같은 좋은 성질을 만족합니다.

**정리 27.4.5** (Strassmann의 정리)

$f: \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ 가 해석적이라 합시다. 그러면  $f$ 는 유한 개의 영점을 가집니다.

이러한 결과들의 응용을 하나 제시하기 위해, 다음 결과를 증명하겠습니다. 이는  $p$ 진수가 등장하기 전부터도 흥미로운 것이었습니다!

**정리 27.4.6 (Skolem-Mahler-Lech)**

$(x_i)_{i \geq 0}$ 가 정수 선형 점화식이라 합시다. 즉  $(x_i)_{i \geq 0}$ 는 다음을 만족하는 정수열입니다

$$x_n = c_1 x_{n-1} + c_2 x_{n-2} + \cdots + c_k x_{n-k} \quad n = 1, 2, \dots$$

어떤 정수  $c_1, \dots, c_k$ 의 선택에 대해 성립합니다. 그러면 지표 집합  $\{i \mid x_i = 0\}$ 은 결국 주기적입니다.

증명. 선형 점화식 이론에 따르면,  $x_i$ 를 내적으로 쓸 수 있게 하는 행렬  $A$ 가 존재합니다

$$x_i = \langle A^i u, v \rangle.$$

$p$ 를  $\det A$ 를 나누지 않는 소수라 합시다.  $T$ 를  $A^T \equiv \text{id} \pmod{p}$ 를 만족하는 정수라 합시다 ( $\text{id}$ 는 항등행렬을 나타냅니다).

$0 \leq r < T$ 을 임의로 고정합니다. 모든 항이

$$f(n) = x_{nT+r} \quad n = 0, 1, \dots$$

영이거나, 많아야 유한히 많은 항만 영이 아님을 증명하겠습니다. 이로써 증명이 마무리됩니다.

어떤 정수 행렬  $B$ 에 대해  $A^T = \text{id} + pB$ 라고 합시다. 다음을 얻습니다

$$\begin{aligned} f(n) &= \langle A^{nT+r} u, v \rangle = \langle (\text{id} + pB)^n A^r u, v \rangle \\ &= \sum_{k \geq 0} \binom{n}{k} \cdot p^k \langle B^k A^r u, v \rangle \\ &= \sum_{k \geq 0} a_k \binom{n}{k} \quad \text{여기서 } a_k = p^k \langle B^k A^r u, v \rangle \in p^k \mathbb{Z}. \end{aligned}$$

이렇게 하여  $f$ 를 말리 형식으로 나타냈습니다. 처음에는  $f: \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}$ 로 정의하지만, 말리의 정리에 의해 ( $\lim_n a_n = 0$ 이므로)  $f$ 가 함수  $f: \mathbb{Z}_p \rightarrow \mathbb{Q}_p$ 로 확장됨을 알 수 있습니다. 또한  $\lim_n \frac{a_n}{n!} = 0$ 임을 확인할 수 있으므로  $f$ 는 심지어 해석적입니다.

따라서 스트라스만의 정리에 의해,  $f$ 는 항등적으로 영이거나, 그렇지 않으면 원하는 대로 유한히 많은 영점을 가집니다.  $\square$

## §27.5 생각해 볼 만한 조금 더 어려운 문제

**문제 27A<sup>†</sup>** ( $\mathbb{Z}_p$ 는 콤팩트합니다).  $\mathbb{Q}_p$ 는 콤팩트하지 않지만  $\mathbb{Z}_p$ 는 콤팩트함을 보이십시오. (후자의 경우, 점렬 연속성을 이용할 것을 권합니다.)

**문제 27B<sup>†</sup>** (완전 비연결).  $\mathbb{Z}_p$ 와  $\mathbb{Q}_p$ 가 모두 완전 비연결임을 보이십시오: 즉 공집합과 한 원소 집합 외에는 연결 집합이 존재하지 않습니다.

**문제 27C** ([MathOverflow](#)에서 언급됨).  $p$ 를 소수라 합시다. 다음을 만족하는 유리수의 수열  $q_1, q_2, \dots$ 를 찾으십시오:

- 수열  $q_n$ 이 실수적 의미에서 0으로 수렴합니다;
- 수열  $q_n$ 이  $p$ 진법적 의미에서 2021로 수렴합니다.

**문제 27D** (USA TST 2011).  $p$ 를 소수라 합시다. 정수 수열  $\{z_n\}_{n=0}^{\infty}$ 이 다음 조건을 만족하면 이를  $p$ -pod라 부릅니다: 각  $e \geq 0$ 에 대해 어떤  $N \geq 0$ 이 존재하여,  $m \geq N$ 일 때마다  $p^e$ 가 다음 합을 나눕니다

$$\sum_{k=0}^m (-1)^k \binom{m}{k} z_k.$$

$\{x_n\}_{n=0}^{\infty}$ 과  $\{y_n\}_{n=0}^{\infty}$ 이 모두  $p$ -pod이면, 수열  $\{x_n y_n\}_{n=0}^{\infty}$ 도  $p$ -pod임을 증명하십시오.

# 28 미분

## §28.1 정의

이 절의 대표적인 예:  $x^3$ 의 도함수는  $3x^2$ 입니다.

여러분 대부분은 이것을 이전에 본 적이 있으리라 생각합니다만, 그럼에도:

**정의 28.1.1.**  $\mathbb{R}$ 의 열린 부분집합<sup>1</sup>  $U$ 를 잡고,  $f: U \rightarrow \mathbb{R}$ 를 함수라 합시다.  $p \in U$ 라 합시다. 극한<sup>2</sup>이 존재하면  $f$ 가  $p$ 에서 **미분가능하다**고 말합니다.

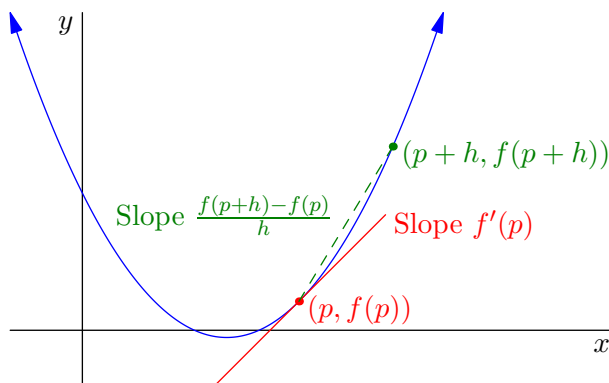
$$\lim_{h \rightarrow 0} \frac{f(p+h) - f(p)}{h}$$

이 존재할 때,  $f$ 가  $p$ 에서 **미분가능**하다고 말합니다. 존재하는 경우, 그 값을  $f'(p)$ 로 표기하고 이를  $p$ 에서의  $f$ 의 **도함수**라 부릅니다.

함수  $f$ 가 모든 점에서 미분가능하면  $f$ 는 미분가능하다고 합니다. 이 경우 도함수  $f': (a, b) \rightarrow \mathbb{R}$ 를 그 자체로 하나의 함수로 간주합니다.

**연습문제 28.1.2.**  $f$ 가  $p$ 에서 미분가능하면  $p$ 에서 연속이기도 함을 보이십시오.

다음은 그림입니다.  $f: \mathbb{R} \rightarrow \mathbb{R}$ 가 미분가능하다고(따라서 연속이라고) 합시다.  $f$ 의 그래프를 평소대로 그리고  $h$ 의 값들을 생각해 봅시다. 0이 아닌 임의의  $h$ 에 대해, 우리가 얻는 것은  $(p, f(p))$ 와  $(p+h, f(p+h))$ 를 잇는 할선의 기울기입니다. 그러나  $h$ 가 0에 가까워짐에 따라, 이 할선은 곡선의 그래프에 접하는 직선에 점점 가까워지기 시작합니다.  $f$ 가 포물선인 경우의 그림이 아래에 나와 있으며, 접선은 빨간색으로, 할선은 초록색 점선으로 표시되어 있습니다.



그러므로 여러분 머릿속에 있어야 할 그림은 다음과 같습니다.

$f'(p)$ 는  $(p, f(p))$ 에서의 접선의 기울기처럼 보입니다.

<sup>1</sup>우리는 거의 항상  $U = (a, b)$  또는  $U = \mathbb{R}$ 를 사용할 것이며, 정의를 이러한 경우들로 제한하더라도 크게 잃을 것은 없습니다.

<sup>2</sup>표기의 남용 26.6.6에서의 관례를 따르고 있음을 기억하십시오. 즉 우리가 의미하는 것은 “ $h = 0$ 에서의 값은 무엇이든 될 수 있는, 함수  $h \mapsto \frac{f(p+h)-f(p)}{h}$ 의 극한”입니다. 그리고 이것은 중요한데, 그 분수식이  $h = 0$ 에서는 정의되지 않기 때문입니다. 약속드린 대로, 우리는 이 점에 신경 쓰지 않습니다.

**비고 28.1.3** — 도함수는 열린 구간 위의 함수에 대해 정의된다는 점에 유의하십시오. 이는 중요합니다. 예를 들어  $f: [a, b] \rightarrow \mathbb{R}$ 인 경우, 각 내부점에서 도함수를 여전히 정의할 수 있지만,  $f'(a)$ 는 더 이상 의미가 없습니다.  $f$ 가  $a$ 의 어떤 열린 근방에서도 값이 주어지지 않기 때문입니다.

계산을 하나 해 보고 이 내용을 계속 진행합니다.

**예제 28.1.4** ( $x^3$ 의 도함수는  $3x^2$ )

$f: \mathbb{R} \rightarrow \mathbb{R}$ 를  $f(x) = x^3$ 로 정의합니다. 임의의 점  $p$ 와 0이 아닌  $h$ 에 대해 다음을 계산할 수 있습니다

$$\begin{aligned}\frac{f(p+h) - f(p)}{h} &= \frac{(p+h)^3 - p^3}{h} \\ &= \frac{3p^2h + 3ph^2 + h^3}{h} \\ &= 3p^2 + 3ph + h^2.\end{aligned}$$

따라서,

$$\lim_{h \rightarrow 0} \frac{f(p+h) - f(p)}{h} = \lim_{h \rightarrow 0} (3p^2 + 3ph + h^2) = 3p^2.$$

따라서  $f$ 의 각 점에서의 기울기는 공식  $3p^2$ 로 주어집니다. 이후 관례적으로  $f'(x) = 3x^2$ 를 함수  $f$  전체의 도함수로 씁니다.

**표기의 남용 28.1.5.** 이제부터 우리는 다소 느슨하게 이를  $(x^3)' = 3x^2$ 로 쓰겠습니다. 이는 "정의역이 어떠한 실숫값 함수  $x^3$ 은 그 정의역의 모든 점  $p$ 에서 도함수  $3p^2$ 를 가진다"는 훨씬 더 장황한 표현의 축약입니다.

일반적으로, 실숫값 미분가능 함수  $f: U \rightarrow \mathbb{R}$ 는 자연스럽게 모든 점  $p \in U$ 에서 도함수  $f'(p)$ 를 만들어내므로, 관례적으로  $p$ 는 아예 포기하고  $f'$  자체를  $U \rightarrow \mathbb{R}$ 인 함수로 취급합니다. 비록 이 실수가 "다른 해석"을 가지고 있음에도 말입니다:  $f'(p)$ 는 값(예: 시각  $t$ 에서의 여러분의 총 재산 가치)이 아니라 기울기(예: 여러분의 시간당 임금률)를 해석하려는 의도로 만들어진 것입니다.  $f$ 가 실생활에서 나온 함수라면 단위조차 맞지 않습니다!

이 관례는 너무나 깊이 뿌리내려 있어서, 그것을 뽑아내려 하면 그럴 가치보다 더 큰 혼란을 초래하지 않고서는 제거할 수 없습니다. 그러나 다변수 미적분학을 다루는 장들을 읽으면, 도함수를 단일 실수가 아니라 선형 사상으로 다시 정의해야 할 때 이것이 어떻게 우리를 곤란하게 하는지 보게 될 것입니다.

## §28.2 계산하는 방법

늘 그랬듯이, 그렇지 않습니까? 합의 법칙, 그런 것들 말입니다.

**정리 28.2.1 (여러분의 친숙한 고등학교 미적분학 법칙들)**

이하에서  $f$ 와  $g$ 는 미분가능한 함수이고,  $U, V$ 는  $\mathbb{R}$ 의 열린 부분집합입니다.

- (합의 법칙)  $f, g: U \rightarrow \mathbb{R}$ 이면  $(f + g)'(x) = f'(x) + g'(x)$ 입니다.
- (곱의 법칙)  $f, g: U \rightarrow \mathbb{R}$ 이면  $(f \cdot g)'(x) = f'(x)g(x) + f(x)g'(x)$ 입니다.
- (연쇄 법칙)  $f: U \rightarrow V$ 이고  $g: V \rightarrow \mathbb{R}$ 이면, 합성함수  $g \circ f: U \rightarrow \mathbb{R}$ 의 도함수는  $g'(f(x)) \cdot f'(x)$ 입니다.

증명. • 합의 법칙: 자명하므로, 관심이 있다면 직접 해보십시오.

- 곱의 법칙: 영이 아닌 모든  $h$ 와 점  $p \in U$ 에 대해 다음과 같이 쓸 수 있습니다

$$\frac{f(p+h)g(p+h) - f(p)g(p)}{h} = \frac{f(p+h) - f(p)}{h} \cdot g(p+h) + \frac{g(p+h) - g(p)}{h} \cdot f(p)$$

이것은  $h \rightarrow 0$ 일 때 원하는 식을 줍니다.

- 연쇄 법칙: 바로 여기서 표기의 남용 26.6.6이 실제로 문제가 됩니다.  $p \in U, q = f(p) \in V$ 라 하면

$$(g \circ f)'(p) = \lim_{h \rightarrow 0} \frac{g(f(p+h)) - g(q)}{h}.$$

우리는 극한의 식을 다음과 같이 쓰고 싶습니다

$$\frac{g(f(p+h)) - g(q)}{h} = \frac{g(f(p+h)) - g(q)}{f(p+h) - q} \cdot \frac{f(p+h) - f(p)}{h}.$$

문제는 분모  $f(p+h) - f(p)$ 가 영이 될 수도 있다는 것입니다. 그래서 대신 다음 식을 정의합니다

$$Q(y) = \begin{cases} \frac{g(y) - g(q)}{y - q} & \text{만약 } y \neq q \\ g'(q) & \text{만약 } y = q \end{cases}$$

이는  $g$ 가  $q$ 에서 미분가능했으므로 연속입니다. 그러면 다음 등식이 실제로 성립합니다

$$\frac{g(f(p+h)) - g(q)}{h} = Q(f(p+h)) \cdot \frac{f(p+h) - f(p)}{h}.$$

왜냐하면  $h \neq 0$ 이면서  $f(p+h) = q$ 인 경우, 어차피 양변이 모두 영이 되기 때문입니다.

그러면  $h \rightarrow 0$ 의 극한에서  $\lim_{h \rightarrow 0} \frac{f(p+h) - f(p)}{h} = f'(p)$ 이고, 연속성에 의해  $\lim_{h \rightarrow 0} Q(f(p+h)) = Q(q) = g'(q)$ 입니다. 이것이 원하던 결과입니다.  $\square$

**연습문제 28.2.2.** 함수  $f: \mathbb{R} \rightarrow \mathbb{R}$ 로 간주되는 다항식  $f(x) = x^3 + 10x^2 + 2019$ 의 도함수를 계산하십시오.

**비고 28.2.3** — 간단한 언어적 요점: 위의 정리들은 모두 각 개별 점에서 성립합니다. 예를 들어 합의 법칙은 실제로는  $f, g: U \rightarrow \mathbb{R}$ 가 점  $p$ 에서 미분가능하면  $f + g$ 도 미분가능하고 그 도함수가  $f'(p) + g'(p)$ 와 같다고 말해야 합니다. 따라서  $f$ 와  $g$ 가  $U$  전체에서 미분가능하다면, 물론  $(f + g)' = f' + g'$ 가 성립함이 따라옵니다. 그러므로 위의 각 법칙은 "점별" 형태를 가지며, 이로부터 " $U$  전체" 형태가 따라옵니다.

우리는 실제로 사용되는 것이 후자이므로 후자만 서술합니다. 하지만 드물게 함수가 구간  $U$  전체가 아니라  $U$ 의 특정 점들에서만 미분가능한 상황에서는, 여전히 아래의 것을 사용할 수 있습니다.

다음으로 잘 알려진 함수들의 몇 가지 도함수를 나열하겠지만, 이 함수들에 대한 엄밀한 정의를 제시하지 않으므로 여기서는 이를 증명하지 않습니다.

#### 명제 28.2.4 (몇 가지 잘 알려진 함수의 도함수)

- $\exp(x) = e^x$ 로 정의되는 지수함수  $\exp: \mathbb{R} \rightarrow \mathbb{R}$ 는 그 자신의 도함수입니다.
- 삼각함수  $\sin$ 과  $\cos$ 는  $\sin' = \cos$ ,  $\cos' = -\sin$ 을 만족합니다.

#### 예제 28.2.5 (전형적인 고등학교 미적분 문제)

이는 위의 것들을 이용해 얻은 임의의 인위적인 함수의 도함수를 기계적으로 계산할 수 있음을 의미하며, 이 때문에 이것이 미국 고등학교와 대학교에서 잡무의 훌륭한 원천이 됩니다. 예를 들어

$$f(x) = e^x + x \sin(x^2) \quad f: \mathbb{R} \rightarrow \mathbb{R}$$

이면, 다음과 같이  $f'$ 을 계산할 수 있습니다

$$\begin{aligned} f'(x) &= (e^x)' + (x \sin(x^2))' && \text{합 법칙} \\ &= e^x + (x \sin(x^2))' && \text{위 표} \\ &= e^x + (x)' \sin(x^2) + x(\sin(x^2))' && \text{곱셈 법칙} \\ &= e^x + \sin(x^2) + x(\sin(x^2))' && (x)' = 1 \\ &= e^x + \sin(x^2) + x \cdot 2x \cdot \cos(x^2) && \text{연쇄 법칙.} \end{aligned}$$

물론 이 함수  $f$ 는 전적으로 인위적이며 아무런 의미도 없는데, 이것이 바로 미적분학이 미국에서 널리 경멸받는 주제인 이유입니다. 그렇긴 하지만, 이러한 계산이 가능하다는 것은 인정할 만한 가치가 있습니다. 이를테면 우리에게는 "도함수는 실제로 계산 가능하다"라는 유사 정리가 있다고 할 수 있습니다.

$(e^x)' = e^x$ 를 당연하게 받아들이다면, 우리가 미분할 수 있는 함수들의 목록에 추가할 유용한 함수 두 개를 더 유도할 수 있습니다.

#### 따름정리 28.2.6 ( $\log$ 의 도함수는 $1/x$ 입니다)

함수  $\log: \mathbb{R}_{>0} \rightarrow \mathbb{R}$ 는 도함수  $(\log x)' = 1/x$ 를 가집니다.

증명.  $x = e^{\log x}$ 입니다. 양변을 미분하고, 다시 연쇄 법칙을 사용합니다<sup>3</sup>

$$1 = e^{\log x} \cdot (\log x)'.$$

따라서  $(\log x)' = \frac{1}{e^{\log x}} = 1/x$ 입니다. □

<sup>3</sup>사실 여기에는 작은 미묘한 점이 있습니다: 우리는  $\log$ 가 미분가능하다는 것을 당연하게 받아들이고 있습니다.

**따름정리 28.2.7 (거듭제곱 법칙)**

$r$ 을 실수라 합시다. 함수  $\mathbb{R}_{>0} \rightarrow \mathbb{R}$ ,  $x \mapsto x^r$ 의 도함수는  $(x^r)' = rx^{r-1}$ 입니다.

증명. 정수  $r$ 에 대해서는 이미 이를 알고 있었지만, 이제 임의의 양의 실수  $r$ 에 대해 이를 증명할 수 있습니다. 다음과 같이 씁니다

$$f(x) = x^r = e^{r \log x}$$

이는 함수  $f: \mathbb{R}_{>0} \rightarrow \mathbb{R}$ 로 간주됩니다. 연쇄 법칙(과  $(e^x)' = e^x$ 라는 사실)을 함께 사용하면 다음을 얻습니다

$$\begin{aligned} f'(x) &= e^{r \log x} \cdot (r \log x)' \\ &= e^{r \log x} \cdot \frac{r}{x} = x^r \cdot \frac{r}{x} = rx^{r-1}. \end{aligned}$$

$e^x$ 와  $\log x$ 에 대한 공식을 증명하지 않는 이유는, 현재로서는 둘 중 어느 것에 대해서도, 심지어  $x$ 가 유리수가 아닐 때의  $2^x$ 에 대해서조차도 엄밀한 정의를 갖고 있지 않기 때문입니다. 그러나 몇몇 사실들이 서로를 함의한다는 것을 아는 것은 좋은 일입니다.  $\square$

**§28.3 극소 (및 극대) 최댓값**

**이 절의 대표적인 예:** 포물선의 수평 접선은 일반적으로 좋은 그림입니다.

미적분학의 고전적인 용도 중 하나가 함수의 최솟값 또는 최댓값을 구하는 것이었다는 사실을 고등학교 때 기억하실 수도 있습니다. 여기서는 이를 수행하는 방법에 대한 엄밀한 설명을 제공하겠습니다.

**정의 28.3.1.**  $f: U \rightarrow \mathbb{R}$ 를 함수라고 합시다. **극댓값**은  $p$ 의 (열린) 근방  $V$ 가 ( $U$  안에 포함 되도록) 존재하여 모든  $x \in V$ 에 대해  $f(p) \geq f(x)$ 가 성립하는 점  $p \in U$ 입니다.

**극솟값**도 유사하게 정의됩니다.<sup>4</sup>

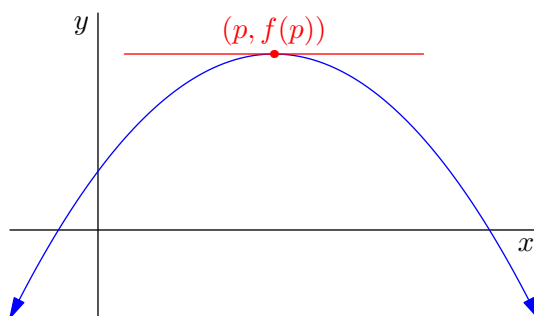
**정의 28.3.2.** 점  $p$ 가 이 둘 중 하나를 만족하면 **극값**이라 합니다.

도함수의 좋은 점은 모든 극값을 포착한다는 것입니다.

**정리 28.3.3 (정류점에 관한 페르마 정리)**

$f: U \rightarrow \mathbb{R}$ 가 미분 가능하고  $p \in U$ 가 극값이라 합시다. 그러면  $f'(p) = 0$ 입니다.

그림을 그려보면 이 결과는 놀랍지 않습니다.



<sup>4</sup>동등하게, 이는  $-f$ 의 극댓값입니다.

(또한 주의할 점: 역은 성립하지 않습니다. 예를 들어  $f(x) = x^{2019}$ 는  $f'(0) = 0$ 이지만  $x = 0$ 은  $f$ 의 극값이 아닙니다.)

증명. 모순을 위해  $f'(p) > 0$ 이라 가정합니다.  $\varepsilon < f'(p)$ 인 임의의  $\varepsilon > 0$ 을 선택합니다. 그러면 충분히 작은  $|h|$ 에 대해 다음이 성립해야 합니다

$$\frac{f(p+h) - f(p)}{h} > \varepsilon.$$

특히  $h > 0$ 일 때  $f(p+h) > f(p)$ 이고  $h < 0$ 일 때  $f(p+h) < f(p)$ 입니다. 따라서  $p$ 는 극값이 아닙니다.

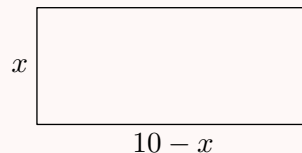
$f'(p) < 0$ 인 경우의 증명도 유사합니다. □

하지만 최적화를 위한 완전한 방법을 원한다면 이것만으로는 실제로 충분하지 않습니다. 문제는 우리가 구하고자 하는 것이 전역 극값이며, 이는 아예 존재하지 않을 수도 있다는 점입니다: 예를 들어  $f(x) = x$ (이는  $f'(x) = 1$ 을 가짐)는 명백히 극값이 전혀 없습니다. 이를 해결하는 핵심은 콤팩트성을 이용하는 것입니다: 정의역을 콤팩트 집합  $Z$ 로 바꾸면,  $f$ 가 어떤 전역 최댓값을 달성한다는 것을 알 수 있습니다. 집합  $Z$ 는 자연스럽게 어떤 내부  $S$ 를 가지며, 미적분학은  $S$  안의 모든 극값을 알려줄 것입니다. 그런 다음  $S$  바깥의 모든 경우를 직접 확인합니다.

확장된 예제 두 개를 살펴봅시다. 첫 번째 것은 간단하며 아마 이미 알고 계실 것이지만, 콤팩트성을 사용하여 철저하게 논증하는 방법과 "경계" 점들이 자연스럽게 나타나는 방식을 보여드리고 싶습니다.

#### 예제 28.3.4 (직사각형 넓이 최적화)

둘레가 20인 직사각형들을 고려하여 넓이가 가장 작거나 가장 큰 직사각형을 구하고자 한다고 합시다.



직사각형의 변을  $x$ 와  $10 - x$ 로 선택하면, 우리는 다음 함수를 최적화하려는 것입니다

$$f(x) = x(10 - x) = 10x - x^2 \quad f: [0, 10] \rightarrow \mathbb{R}.$$

콤팩트성에 의해 어떤 전역 최댓값과 어떤 전역 최솟값이 존재합니다.

$f$ 가  $(0, 10)$ 에서 미분 가능하므로, 임의의  $p \in (0, 10)$ 에 대해 전역 최댓값도 극댓값이 되며, 따라서 다음을 만족해야 함을 알 수 있습니다

$$0 = f'(p) = 10 - 2p \implies p = 5.$$

또한 점  $x = 0$ 과  $x = 10$ 은 정의역에는 속하지만 내부  $(0, 10)$ 에는 속하지 않습니다. 따라서 전역 극값은 (존재한다는 것에 더하여) 세 후보  $\{0, 5, 10\}$  중에 있어야 합니다. 마지막으로  $f(0) = 0$ ,  $f(5) = 25$ ,  $f(10) = 0$ 을 확인합니다. 따라서  $5 \times 5$  정사각형이 가장 큰 넓이를 가지며, 퇴화된 직사각형들이 가장 작은(0인) 넓이를 갖습니다.

다음은 초등적이지 않은 예시입니다.

**명제 28.3.5** ( $e^x \geq 1 + x$ )

모든 실수  $x$ 에 대해  $e^x \geq 1 + x$ 가 성립합니다.

증명. 미분 가능한 함수를 다음과 같이 정의합니다.

$$f(x) = e^x - (x + 1) \quad f: \mathbb{R} \rightarrow \mathbb{R}.$$

콤팩트 구간  $Z = [-1, 100]$ 을 생각해 봅시다.  $x \leq -1$ 이면 명백히  $f(x) > 0$ 입니다. 마찬가지로  $x \geq 100$ 이면 역시 명백히  $f(x) > 0$ 입니다. 따라서 우리는  $x \in Z$ 일 때  $f(x) \geq 0$ 임을 증명하기만 하면 됩니다.

실제로 어떤 전역 최솟값  $p$ 가 존재합니다. 이는 끝점  $-1$  또는  $100$ 일 수 있습니다. 그렇지 않고  $U = (-1, 100)$  안에 놓여 있다면, 다음을 만족해야 합니다.

$$0 = f'(p) = e^p - 1 \implies p = 0.$$

$f(-1) > 0$ ,  $f(100) > 0$ ,  $f(0) = 0$ 이므로,  $p = 0$ 이  $Z$ 의 전역 최솟값임을 결론지을 수 있습니다. 따라서 모든  $x \in Z$ 에 대해  $f(x) \geq 0$ 이고, 결국 모든  $x$ 에 대해 성립합니다.  $\square$

**비고 28.3.6** —  $\pm\infty$ 에서의 극한을 사용하고자 한다면, 위와 같은 증명을  $-1$ 이나  $100$  같은 끝점을 명시적으로 찾을 필요가 없는 방식으로 다시 쓸 수 있습니다. 여기서는 그렇게 하지 않겠지만, 생각해 볼 만한 좋은 소재입니다.

## §28.4 롤과 그 동료들

이 절의 대표적인 예: 경주로 원리, 어쩌면?

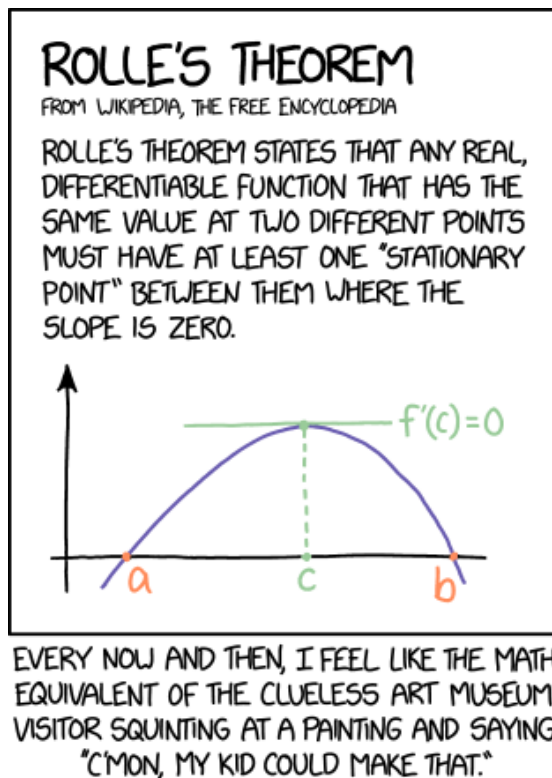
앞 절의 작업에서 얻은 한 가지 따름정리가 바로 롤의 정리입니다.

**정리 28.4.1** (롤의 정리)

$f: [a, b] \rightarrow \mathbb{R}$ 가 연속함수이고 열린 구간  $(a, b)$ 에서 미분 가능하며  $f(a) = f(b)$ 라고 합시다. 그러면  $f'(c) = 0$ 을 만족하는 점  $c \in (a, b)$ 가 존재합니다.

증명.  $f$ 가 상수함수가 아니라고 가정합니다 (그렇지 않다면 어떤  $c$ 든 성립합니다). 콤팩트성에 의해 전역 최댓값과 전역 최솟값이 모두 존재합니다.  $f(a) = f(b)$ 이므로, 전역 최댓값 또는 전역 최솟값 중 하나는 열린 구간  $(a, b)$  내부에 놓여야 하며, 그러면 정류점에 대한 페르마의 정리가 증명을 마무리해 줍니다.  $\square$

그림을 그리려고 했는데, xkcd #2042에 이미 그림이 있다는 것을 깨달았습니다.



이미지 출처 [Mu]

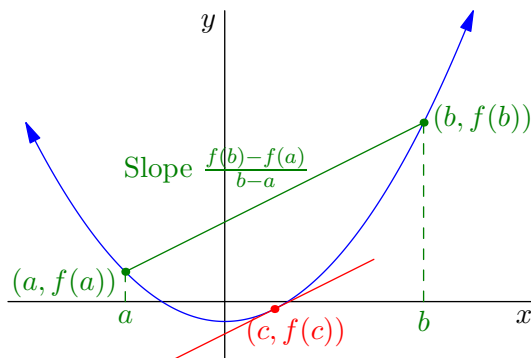
이 정리는 다음과 같이 확장할 수 있습니다.

#### 정리 28.4.2 (평균값 정리)

$f: [a, b] \rightarrow \mathbb{R}$ 가 연속함수이고 열린 구간  $(a, b)$ 에서 미분 가능하다고 합시다. 그러면 다음을 만족하는 점  $c \in (a, b)$ 가 존재합니다.

$$f'(c) = \frac{f(b) - f(a)}{b - a}.$$

그림으로 나타내면,  $c$ 에서의 접선이  $(a, f(a))$ 와  $(b, f(b))$ 를 잇는 할선과 같은 기울기를 갖는  $c$ 가 존재하며, 롤의 정리는 그 할선이 수평인 특수한 경우에 해당합니다.



평균값 정리의 증명.  $s = \frac{f(b)-f(a)}{b-a}$ 를 할선의 기울기라 하고, 다음과 같이 정의합시다.

$$g(x) = f(x) - sx$$

이는 직관적으로  $f$ 를 아래로 밀어내려 할선이 수평이 되도록 만드는 것입니다. 실제로 이제  $g(a) = g(b)$ 가 성립하므로,  $g$ 에 롤의 정리를 적용합니다.  $\square$

**비고 28.4.3 (운전면허 소지자를 위한 이야기)** — 이에 대한 좋은 실생활 해석을 하나 언급하고자 합니다. 자동차가 1차원 도로를 따라 이동하고 있습니다(여기서  $f(t)$ 는 시각  $t$ 에서의 위치를 나타냅니다). 여러분이 자동차로 5시간에 걸쳐 900킬로미터를 이동했다고 합시다(즉  $f(0) = 0$ ,  $f(5) = 900$ ). 그러면 그 순간의 속도가 정확히 시속 180킬로미터였던 시점이 어딘가에 존재하며, 따라서 경찰이 과속으로 여러분을 세우더라도 딱히 항의할 수 없습니다.

평균값 정리가 중요한 이유는 이것 없이는 사실상 불가능한 방식으로 **도함수 정보를 이용해 함수에 대한 정보를 얻을 수 있게** 해 주기 때문입니다. 다음은 이 점을 보여주는 간단한 응용 예시입니다.

**명제 28.4.4 (경주로 원리)**

$f, g: \mathbb{R} \rightarrow \mathbb{R}$ 를  $f(0) = g(0)$ 을 만족하는 두 미분 가능한 함수라고 합시다.

- (a) 모든  $x > 0$ 에 대해  $f'(x) \geq g'(x)$ 이면, 모든  $x > 0$ 에 대해  $f(x) \geq g(x)$ 입니다.
- (b) 모든  $x > 0$ 에 대해  $f'(x) > g'(x)$ 이면, 모든  $x > 0$ 에 대해  $f(x) > g(x)$ 입니다.

이 명제는 자명해 보일 수 있습니다. 이를 경주 트랙이라고 생각할 수 있는 데에는 이유가 있습니다: 만약  $f$ 와  $g$ 가 두 자동차(또는 말 등)의 위치를 나타내고 첫 번째 자동차가 항상 두 번째 자동차보다 빠르다면, 첫 번째 자동차는 결국 두 번째 자동차보다 앞서 있어야 합니다. 특수한 경우  $g = 0$ 일 때, 이는 만약  $f'(x) \geq 0$ 이라면, 즉 “ $f$ 가 증가한다”면, 음,  $x > 0$ 에 대해  $f(x) \geq f(0)$ 이라는 것을 말하는데, 이는 참이어야 마땅합니다. 그러나 이를 도함수의 정의로부터 증명하려 하면, 그것이 쉽지 않다는 것을 알게 될 것입니다! 그러나 이는 평균값 정리의 원형에 가깝습니다.

경주 트랙 원리의 증명. (a)를 증명합니다.  $h = f - g$ 라 하면,  $h(0) = 0$ 입니다. 모순을 가정하여 어떤  $p > 0$ 에 대해  $h(p) < 0$ 이라 합시다. 그러면  $(0, h(0))$ 과  $(p, h(p))$ 를 잇는 할선은 음의 기울기를 가지며; 다시 말해 평균값 정리에 의해 다음을 만족하는  $0 < c < p$ 가 존재합니다

$$f'(c) - g'(c) = h'(c) = \frac{h(p) - h(0)}{p} = \frac{h(p)}{p} < 0$$

따라서  $f'(c) < g'(c)$ 인데, 이는 모순입니다. (b) 부분도 마찬가지입니다. □

때로는 쉽게 분리할 수 없는 두 함수를 마주하게 될 것입니다; 이러한 경우에는 다음 형태가 더 유용할 수 있습니다.

**정리 28.4.5 (비율 평균값 정리)**

$f, g: [a, b] \rightarrow \mathbb{R}$ 가  $(a, b)$ 에서 미분가능한 두 연속함수라 합시다. 그러면 다음을 만족하는  $c \in (a, b)$ 가 존재합니다

$$f'(c)(g(b) - g(a)) = g'(c)(f(b) - f(a))$$

증명. 다음 함수에 롤의 정리를 사용하십시오

$$h(x) = [f(x) - f(a)][g(b) - g(a)] - [g(x) - g(a)][f(b) - f(a)]. \quad \square$$

이는 코시의 평균값 정리 또는 확장된 평균값 정리라고도 불립니다.

## §28.5 매끄러운 함수

**이 절의 대표적인 예:** 여러분에게 익숙한 모든 함수들입니다.

$f: U \rightarrow \mathbb{R}$ 가 미분가능하다고 합시다. 이로써 함수  $f': U \rightarrow \mathbb{R}$ 를 얻게 됩니다. 만약 처음 함수가 충분히 좋다면, 다시 도함수를 취할 수 있어 함수  $f'': U \rightarrow \mathbb{R}$ 를 얻게 되며, 이런 식으로 계속됩니다. 일반적으로, 도함수를  $n$ 번 취한 후, 그 결과 함수를  $f^{(n)}$ 으로 표기합니다. 관례상  $f^{(0)} = f$ 입니다.

**정의 28.5.1.** 함수  $f: U \rightarrow \mathbb{R}$ 가 무한히 미분가능하면 **매끄럽다**고 합니다; 즉 함수  $f^{(n)}$ 이 모든  $n$ 에 대해 존재한다는 것입니다.

**질문 28.5.2.** 절댓값 함수가 매끄럽지 않음을 보이십시오.

다항식,  $e^x$ ,  $\log$ ,  $\sin$ ,  $\cos$ 와 같이 우리가 마주치는 대부분의 함수는 매끄러우며, 그것들의 합성 또한 그러합니다. 다음은 다음 시간에 더 발전시킬 기이한 예입니다.

**예제 28.5.3** (모든 도함수가 영인 매끄러운 함수)

다음 함수를 고려해 보겠습니다

$$f(x) = \begin{cases} e^{-1/x} & x > 0 \\ 0 & x \leq 0. \end{cases}$$

이 함수는 매끄러우며  $f^{(n)}(0) = 0$ 임을 보일 수 있습니다. 따라서 이 함수는 상수 함수가 아님에도 불구하고 원점에서 모든 도함수가 영입니다!

## §28.6 생각해 볼 만한 조금 더 어려운 문제

**문제 28A** (몫의 법칙).  $f: (a, b) \rightarrow \mathbb{R}$ 와  $g: (a, b) \rightarrow \mathbb{R}_{>0}$ 를 미분가능한 함수라고 합시다.  $h = f/g$ 를 이들의 몫(마찬가지로  $(a, b) \rightarrow \mathbb{R}$ 인 함수)이라고 합시다.  $h$ 의 도함수가 다음과 같이 주어짐을 보이십시오

$$h'(x) = \frac{f'(x)g(x) - f(x)g'(x)}{g(x)^2}.$$

**문제 28B.** 실수  $x > 0$ 에 대해,  $x^x$ 는 얼마나 작을 수 있습니까?



**문제 28C** (RMM 2018). 실수 계수를 갖는 상수가 아닌 다항식  $P(x)$ 와  $Q(x)$ 가 다음을 만족하며 존재하는지 여부를 판정하십시오

$$P(x)^{10} + P(x)^9 = Q(x)^{21} + Q(x)^{20}.$$



**문제 28D.**  $P(x)$ 를 실수 계수를 갖는  $n$ 차 다항식이라 합시다. 방정식  $e^x = P(x)$ 가  $x$ 에 대해 많아야  $n + 1$ 개의 실근을 가짐을 증명하십시오.

**문제 28E** (옌센 부등식).  $f: (a, b) \rightarrow \mathbb{R}$ 가 모든  $x$ 에 대해  $f''(x) \geq 0$ 인 두 번 미분가능한 함수라 합시다(즉  $f$ 는 볼록합니다). 다음을 증명하십시오

$$f\left(\frac{x+y}{2}\right) \leq \frac{f(x) + f(y)}{2}$$

구간  $(a, b)$  안의 모든 실수  $x$ 와  $y$ 에 대하여.

**문제 28F** (로피탈 정리, 또는 최소한 한 가지 경우).  $f, g: \mathbb{R} \rightarrow \mathbb{R}$ 가 미분가능 함수이고  $p$ 가 실수라고 하십시오. 다음을 가정하십시오

$$\lim_{x \rightarrow p} f(x) = \lim_{x \rightarrow p} g(x) = 0.$$

다음을 증명하십시오

$$\lim_{x \rightarrow p} \frac{f(x)}{g(x)} = \lim_{x \rightarrow p} \frac{f'(x)}{g'(x)}$$

단, 우극한이 존재하는 경우에 한합니다.

**문제 28G.**  $f(x) = x^x$ 로 정의된 함수  $f: (0, \infty) \rightarrow \mathbb{R}$ 의 도함수를 계산하십시오.



# 29 멱급수와 테일러 급수

다항식은 매우 다루기 좋은 함수이며, 그런 이유로 광범위하게 연구됩니다. 예를 들어 해석적 관점에서 다항식은 매끄러우며, 그 도함수를 계산하기 쉽습니다.

이 장에서는 문자 그대로 "무한 다항식"  $\sum_n a_n x^n$ 인 멱급수를 공부하겠습니다. 급수와 미분에 대한 이해로 무장하여, 우리는 세 가지 훌륭한 사실을 보게 될 것입니다:

- 우리가 자연에서 보는 많은 함수들은 실제로 멱급수로 주어집니다. 그 가운데는  $e^x$ ,  $\log x$ ,  $\sin x$ 가 있습니다.
- 이들의 수렴 성질은 실제로 상당히 잘 다루어집니다: 계수들의 나열로부터, 이들이 어떤  $x$ 에 대해 수렴하는지 알아낼 수 있습니다.
- $\sum_n a_n x^n$ 의 도함수는 사실 그저  $\sum_n n a_n x^{n-1}$ 입니다.

## §29.1 동기

시작을 위해, 여러분이 알아볼 만한 하나의 무한 다항식으로 시작해봅시다: 임의로 고정된 수  $-1 < x < 1$ 에 대해 다음과 같은 급수 수렴이 성립합니다

$$\frac{1}{1-x} = 1 + x + x^2 + \dots$$

등비급수 공식에 의해서입니다.

이것을 **문제 26D**에서 이미 보지 않았다고 가정해봅시다. 그러면 대신 우리는 다음과 같은 매끄러운 함수  $f: (-1, 1) \rightarrow \mathbb{R}$ 를 갖습니다

$$f(x) = \frac{1}{1-x}.$$

원점 근처에서 이것이 "무한 다항식"과 같다고 가정하고 싶다고 합시다, 즉

$$(1-x)^{-1} = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + \dots$$

우리가 그 다항식을 미리 알지 못했다면, 어떻게 그것을 찾을 수 있을까요?

먼저 우선  $x=0$ 을 대입함으로써 우리는 당연히  $a_0=1$ 을 원한다는 것을 알 수 있습니다. 도함수가 있으므로, 사실 우리는 양변을 미분하여 다음을 얻을 수 있습니다

$$(1-x)^{-2} = a_1 + 2a_2 x + 3a_3 x^2 + 4a_4 x^3 + \dots$$

이제  $x=0$ 으로 놓으면,  $a_1=1$ 을 얻습니다. 실제로, 계속 미분을 취하며 무엇을 얻는지 살펴봅시다.

$$\begin{aligned} (1-x)^{-1} &= a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4 + a_5 x^5 + \dots \\ (1-x)^{-2} &= a_1 + 2a_2 x + 3a_3 x^2 + 4a_4 x^3 + 5a_5 x^4 + \dots \\ 2(1-x)^{-3} &= 2a_2 + 6a_3 x + 12a_4 x^2 + 20a_5 x^3 + \dots \\ 6(1-x)^{-4} &= 6a_3 + 24a_4 x + 60a_5 x^2 + \dots \\ 24(1-x)^{-5} &= 24a_4 + 120a_5 x + \dots \\ &\vdots \end{aligned}$$

$x=0$ 으로 놓으면  $1 = a_0 = a_1 = a_2 = \dots$ 를 발견하는데, 이는 우리가 기대하는 바입니다; 등비급수  $\frac{1}{1-x} = 1 + x + x^2 + \dots$ 입니다. 그리하여 실제로 미분을 취하는 것만으로 올바른 주장을 얻기에 충분했습니다!

## §29.2 멱급수

**이 절의 대표적인 예:**  $\frac{1}{1-z} = 1 + z + z^2 + \dots$ 이며, 이는  $(-1, 1)$ 에서 수렴합니다.

물론 이것은 엄밀하지 않은데, 우변이 무엇인지 기술하지 않았을 뿐만 아니라, 그것이 항별로 미분될 수 있음을 보이지도 않았기 때문입니다. 그러므로 이제 주인공을 정의하겠습니다.

**정의 29.2.1.** 멱급수는 다음과 같은 형태의 합입니다

$$\sum_{n=0}^{\infty} a_n z^n = a_0 + a_1 z + a_2 z^2 + \dots$$

여기서  $a_0, a_1, \dots$  는 실수이고,  $z$ 는 변수입니다.

**표기의 남용 29.2.2** ( $0^0 = 1$ ). 매우 주의 깊게 살펴본다면,  $z = 0$ 이고  $n = 0$ 일 때  $0^0$  항이 나타남을 알아챌 수 있습니다. 이 장에서는 그러한 항들이 모두 1과 같다는 관례를 따릅니다.

이제, 만약 특정한 실수  $h$ 를 대입한다면, 실수들의 급수  $\sum_{n=0}^{\infty} a_n h^n$ 을 얻습니다. 그래서 우리는 이 급수가 언제 수렴하는지 물을 수 있습니다. 이에 대해 정확한 답이 존재함이 밝혀 집니다.

**정의 29.2.3.** 멱급수  $\sum_{n=0}^{\infty} a_n z^n$ 이 주어졌을 때, **수렴 반지름**  $R$ 은 다음 공식으로 정의됩니다

$$\frac{1}{R} = \limsup_{n \rightarrow \infty} |a_n|^{1/n}$$

우변이  $\infty$ 이면  $R = 0$ 으로, 우변이 0이면  $R = \infty$ 로 정한다는 관례를 따릅니다.

### 정리 29.2.4 (코시-아다마르 정리)

$\sum_{n=0}^{\infty} a_n z^n$ 을 수렴 반지름이  $R$ 인 멱급수라 합시다.  $h$ 를 실수라 하고, 다음과 같은 무한급수를 생각합시다

$$\sum_{n=0}^{\infty} a_n h^n$$

실수들의 급수를 생각합시다. 그러면 다음이 성립합니다:

- $|h| < R$ 이면 급수는 절대수렴합니다.
- $|h| > R$ 이면 급수는 발산합니다.

증명. 이는 실제로 어렵지는 않지만 필수적이지는 않으므로 포함하지 않습니다. □

**비고 29.2.5** —  $|h| = R$ 인 경우에는 어느 쪽으로도 갈 수 있습니다.

### 예제 29.2.6 ( $\sum z^n$ 의 반지름은 1입니다)

기하급수  $\sum_{n=0}^{\infty} z^n = 1 + z + z^2 + \dots$ 를 생각합시다. 모든  $n$ 에 대해  $a_n = 1$ 이므로  $R = 1$ 을 얻는데, 이는 우리가 예상한 바입니다.

따라서  $\sum_{n=0}^{\infty} a_n z^n$ 이 수렴 반지름  $R > 0$ 이 아닌 멱급수라면, 이는 또한 다음과 같은 함수로 생각할 수 있습니다

$$(-R, R) \rightarrow \mathbb{R} \quad \text{에 의해} \quad h \mapsto \sum_{n=0}^{\infty} a_n h^n.$$

이는 홀름합니다. 또한  $R = \infty$ 이면 이는 함수  $\mathbb{R} \rightarrow \mathbb{R}$ 를 얻는다는 것을 뜻함을 유의하십시오.

**표기의 남용 29.2.7** (멱급수 대 함수). 다시 한 번 대상들의 "타입"과 관련하여 미묘한 점이 있습니다. 다항식과의 유비가 도움이 될 수 있습니다.

다항식  $P(x) = x^3 + 7x + 9$ 를 생각합시다. 임의의 실수  $h$ 에 대해  $P(h)$ 에 대입하여 실수를 얻는 것이 가능합니다. 그러나 다항식 그 자체에서는 기호  $x$ 가 변수여야 하는데 — 때로는 여기에 실수를 대입하겠지만, 그것은 다항식이 정의된 이후에나 일어나는 일입니다.

그럼에도 불구하고 "다항식  $P(x) = x^3 + 7x + 9$ "(계수들로 생각할 수 있음)와 "실숫값 함수  $x \mapsto x^3 + 7x + 9$ "는 종종 서로 바꿔 쓰입니다. 멱급수에서도 비슷한 일이 일어나려 합니다: 멱급수는 처음에는 계수들의 수열로 여겨졌지만, 코시-아다마르 정리 덕분에 이를 함수로도 생각할 수 있게 되었고, 따라서 우리는 둘 사이의 구별을 흐리게 됩니다.

## §29.3 멱급수의 미분

**이 절의 대표적인 예:** 앞서  $1 + x + x^2 + x^3 + \dots$ 의 도함수가  $1 + 2x + 3x^2 + \dots$ 임을 보았습니다.

약속드린 대로, 미분은 여러분이 원하는 대로 정확히 작동합니다.

### 정리 29.3.1 (미분은 항별로 작동합니다)

$\sum_{n \geq 0} a_n z^n$ 을 수렴 반지름  $R > 0$ 인 멱급수라 하고, 그에 대응하는 함수를 다음과 같이 생각합시다

$$f: (-R, R) \rightarrow \mathbb{R} \quad \text{에 의해} \quad f(x) = \sum_{n \geq 0} a_n x^n.$$

그러면  $f$ 의 모든 도함수가 존재하며, 다음과 같은 멱급수로 주어집니다

$$\begin{aligned} f'(x) &= \sum_{n \geq 1} n a_n x^{n-1} \\ f''(x) &= \sum_{n \geq 2} n(n-1) a_n x^{n-2} \\ &\vdots \end{aligned}$$

이 멱급수들 또한 임의의  $x \in (-R, R)$ 에 대해 수렴합니다. 특히  $f$ 는 매끄럽습니다.

증명. 이 역시 생략합니다. 이를 증명하는 올바른 방법은 "고르게 수렴한다"는 개념을 정의하고, 이것 또한 결론으로 갖도록 코시-아다마르 정리를 강화하는 것입니다.  $\square$

### 따름정리 29.3.2 (멱급수 계수에 대한 서술)

$\sum_{n \geq 0} a_n z^n$ 을 수렴 반지름  $R > 0$ 인 멱급수라 하고, 위와 같이 그에 대응하는 함수  $f(x)$ 를 생각합시다. 그러면

$$a_n = \frac{f^{(n)}(0)}{n!}.$$

증명.  $n$ 번째 도함수를 취하고  $x = 0$ 을 대입하십시오.  $\square$

## §29.4 해석적 함수

**이 절의 대표적인 예:** 조각별로  $e^{-1/x}$  또는 0으로 정의되는 함수는 해석적이지 않지만 매끄럽습니다.

멱급수에 관한 이 모든 좋은 결과들을 바탕으로, 이제 이 과정을 반대 방향으로 수행할 방법이 생겼습니다:  $f: U \rightarrow \mathbb{R}$ 가 함수라고 합시다. 이를 멱급수로 표현할 수 있습니까?

이것이 성립하는 함수들을 해석적이라고 부릅니다.

**정의 29.4.1.** 함수  $f: U \rightarrow \mathbb{R}$ 가 점  $p \in U$ 에서 **해석적**이라 함은,  $p$ 의 ( $U$  내부의) 어떤 열린 근방  $V$ 와 다음을 만족하는 멱급수  $\sum_n a_n z^n$ 이 존재하는 경우입니다.

$$f(x) = \sum_{n \geq 0} a_n (x - p)^n$$

임의의  $x \in V$ 에 대해 성립합니다. 늘 그렇듯이, 함수 전체가 각 점에서 해석적이면 그 함수는 해석적입니다.

**질문 29.4.2.**  $f$ 가 해석적이면 매끄러움을 보이십시오.

게다가,  $f$ 가 해석적이면 위의 따름정리에 의해 그 계수들이 실제로 정확히 다음과 같이 기술됩니다.

$$f(x) = \sum_{n \geq 0} \frac{f^{(n)}(p)}{n!} (x - p)^n.$$

$f$ 가 매끄럽지만 해석적이지 않더라도, 적어도 멱급수는 써 내려갈 수 있습니다. 이것에 이름을 붙여 봅시다.

**정의 29.4.3.** 매끄러운  $f$ 에 대해, 멱급수  $\sum_{n \geq 0} \frac{f^{(n)}(p)}{n!} z^n$ 을  $p$ 에서의  $f$ 의 **테일러 급수**라고 부릅니다.

**예제 29.4.4 (해석적 함수의 예시)**

(a) 다항식,  $\sin$ ,  $\cos$ ,  $e^x$ ,  $\log$ 는 모두 해석적인 것으로 밝혀집니다.

(b) 앞서 다음과 같이 정의된 매끄러운 함수는

$$f(x) = \begin{cases} \exp(-1/x) & x > 0 \\ 0 & x \leq 0 \end{cases}$$

해석적이지 않습니다. 실제로, 모순을 이끌어내기 위해 그렇다고 가정해봅시다. 모든 도함수가 0이므로, 그 테일러 급수는  $0 + 0x + 0x^2 + \dots$ 가 될 것입니다. 이 테일러 급수는 수렴하지만, 올바른 값으로 수렴하지는 않습니다 — 임의의  $\varepsilon > 0$ 에 대해  $f(\varepsilon) > 0$ 이므로, 모순입니다.

예시 (b)는 함수  $f: \mathbb{R} \rightarrow \mathbb{R}$ 가 있을 때,  $f$ 가 매끄럽다는 것과  $p$ 에서의 완전한 테일러 급수를 안다고 하더라도,  $f$ 의 다른 값들을 복원하거나  $f$ 가  $p$ 를 포함하는 어떤 구간에서 해석적이라고 추론하는 것이 여전히 불가능함을 보여줍니다.

하지만 적어도 다음은 참입니다.

**명제 29.4.5** (한 점에서의 해석성은 구간에서의 해석성을 함의함)

$f: \mathbb{R} \rightarrow \mathbb{R}$ 가 매끄럽고,  $p \in \mathbb{R}$ 가 정의역 내의 한 점이라고 합시다. 다음을 가정합니다.

- $p$ 에서의  $f$ 의 테일러 급수가 수렴 반지름  $R > 0$ 을 가진다. 그리고
- 그 테일러 급수는 수렴 반경 내의 모든 입력  $x \in (p - R, p + R)$ 에 대해 실제로 값  $f(x)$ 로 수렴합니다.

그러면  $f$ 는  $(p - R, p + R)$ 에서 해석적입니다.

이 결과가 자명하지 않은 이유는, 사전에 우리는  $f$ 가  $p$ 에서 해석적이라는 것만 알고 있기 때문입니다. 이 결과는 이를 확장하여  $R > 0$ 이면 수렴 반지름 전체에서 해석적임을 보여줍니다. 잠시 후 실제로 멱급수로 정의되는  $\exp$ 에 대해 이를 사용할 것입니다.

미분가능 함수의 경우와 마찬가지로:

**명제 29.4.6** (해석적 함수에 대한 통상적인 모든 폐포 성질)

해석적 함수들의 합, 곱, 합성, 0이 아닌 나눗셈은 해석적입니다.

이것의 요점은, 자연에서 나타나는 대부분의 통상적인 함수들, 심지어  $f(x) = e^x + x \sin(x^2)$  같은 인위적인 함수들조차도 해석적이며, 따라서 국소적으로 테일러 급수로 기술될 수 있다는 것입니다.

## §29.5 오일러 상수와 지수화의 정의

이제 우리가 가진 도구들을 사용하여 실제로  $e^x$ 의 정의를 줄 수 있습니다.

**정의 29.5.1.** 다음과 같이 무한한 수렴 반지름을 가지는 멱급수를 사용하여 사상  $\exp: \mathbb{R} \rightarrow \mathbb{R}$ 를 정의합니다.

$$\exp(x) = \sum_{n \geq 0} \frac{x^n}{n!}.$$

그러면 오일러 상수를  $e = \exp(1)$ 로 정의합니다.

**질문 29.5.2.** 이 정의 아래에서  $\exp' = \exp$ 임을 보이십시오. 또한 **명제 29.4.5**로부터  $\exp$ 가 해석적임을 결론지으십시오.

그러면 다음과 같이 정리됩니다:

**명제 29.5.3** ( $\exp$ 는 곱셈적이다)

이 정의 아래에서,

$$\exp(x + y) = \exp(x) \exp(y).$$

증명의 아이디어. 여기서 합의 순서를 바꾸는 것과 관련된 다소 미묘한 부분이 있는데, 이는

다루지 않습니다. 그 점을 제외하면:

$$\begin{aligned}
 \exp(x) \exp(y) &= \sum_{n \geq 0} \frac{x^n}{n!} \sum_{m \geq 0} \frac{y^m}{m!} = \sum_{n \geq 0} \sum_{m \geq 0} \frac{x^n y^m}{n! m!} \\
 &= \sum_{k \geq 0} \sum_{\substack{m+n=k \\ m, n \geq 0}} \frac{x^n y^m}{n! m!} = \sum_{k \geq 0} \sum_{\substack{m+n=k \\ m, n \geq 0}} \binom{k}{n} \frac{x^n y^m}{k!} \\
 &= \sum_{k \geq 0} \frac{(x+y)^k}{k!} = \exp(x+y). \quad \square
 \end{aligned}$$

#### 따름정리 29.5.4 (exp는 양수이다)

- (a) 임의의 실수  $x$ 에 대해  $\exp(x) > 0$ 입니다.
- (b) 함수  $\exp$ 는 강한 의미로 증가합니다.

증명. 먼저

$$\exp(x) = \exp(x/2)^2 \geq 0$$

이므로  $\exp$ 가 음이 아님을 알 수 있습니다. 또한  $1 = \exp(0) = \exp(x) \exp(-x)$ 로부터 임의의  $x$ 에 대해  $\exp(x) \neq 0$ 임이 따라오며, 이로써 (a)가 증명됩니다.

(b)는  $\exp'$ 가 항상 양수라는 사실(경주로 원리)에서 바로 따라옵니다.  $\square$

그다음으로 로그 함수가 나옵니다.

**정의 29.5.5.**  $\exp$ 의 역함수로서  $\log: \mathbb{R}_{>0} \rightarrow \mathbb{R}$ 을 정의할 수 있습니다.

그 도함수가  $1/x$ 이므로 매끄러우며, 이후 그 계수들을 계산하여 해석적임을 보일 수 있습니다.

이것이 실제로 모든  $a > 0$ 과  $r > 0$ 에 대해  $a^r$ 을 엄밀하게 정의하는 방법을 제공한다는 점에 유의하십시오. 즉,

$$a^r := \exp(r \log a).$$

## §29.6 이는 복소수에 대해서도 마찬가지로 성립하는데, 다만 복소해석학 또한 천국이라는 점만 다릅니다

이제 위에서 언급했던 모든 정리가  $\mathbb{C}$  위에서 작업하더라도 본질적으로 수정 없이 그대로 성립한다는 점을 언급합니다.

- 거듭제곱 급수는  $a_n \in \mathbb{R}$  대신  $a_n \in \mathbb{C}$ 인  $\sum_n a_n z^n$ 으로 정의됩니다.
- 수렴 반경  $R$ 의 정의는 변하지 않습니다! 급수는  $|z| < R$ 이면 수렴합니다.
- 미분도 여전히 훌륭하게 작동합니다. (도함수의 정의는 변하지 않습니다.)
- 해석성도  $U \subseteq \mathbb{C}$ 가 열린집합일 때 함수  $f: U \rightarrow \mathbb{C}$ 에 대해 여전히 훌륭하게 작동합니다.

특히 이제 복소 지수함수까지 정의할 수 있으며, 멱급수가 여전히  $R = \infty$ 를 가지므로 함수

$$\exp: \mathbb{C} \rightarrow \mathbb{C}$$

가 주어집니다. 더 일반적으로  $a > 0$ 이고  $z \in \mathbb{C}$ 이면 여전히

$$a^z := \exp(z \log a).$$

로 정의할 수 있습니다. (다만  $\log a$ 가 정의되도록 밑  $a$ 는 여전히 양의 실수여야 합니다. 따라서 이  $i^i$  문제는 여전히 남아 있습니다.)

그러나 실수의 경우에서 했던 것처럼 복소함수에 대해 미적분학을 연구하려 하면, 대부분의 결과가 그대로 성립하는 것 외에도 커다란 놀라움을 마주하게 됩니다:

만약  $f: \mathbb{C} \rightarrow \mathbb{C}$ 가 미분가능하다면, 이는 해석적입니다.

그리고 이것은 복소 해석 함수에 대해 성립하는, 거의 믿기 어려운 결과들의 시작에 불과합니다. 하지만 이 부분은 실해석학에 관한 것이므로, 이에 대해서는 나중에 살펴보아야 할 것입니다!

## §29.7 생각해 볼 만한 조금 더 어려운 문제

**문제 29A.**  $\log(1-x)$ 의 테일러 급수를 구하십시오.

**문제 29B<sup>†</sup>** (오일러 공식). 임의의 실수  $\theta$ 에 대해

$$\exp(i\theta) = \cos \theta + i \sin \theta$$

임을 보이십시오.

**문제 29C<sup>†</sup>** (테일러 정리, 라그랑주 형식).  $f: [a, b] \rightarrow \mathbb{R}$ 가 연속이고  $(a, b)$ 에서  $n+1$ 번 미분가능하다고 합시다. 다음을 정의합니다.

$$P_n = \sum_{k=0}^n \frac{f^{(k)}(a)}{k!} \cdot (b-a)^k.$$

다음을 만족하는  $\xi \in (a, b)$ 가 존재함을 증명하십시오.

$$f^{(n+1)}(\xi) = (n+1)! \cdot \frac{f(b) - P_n}{(b-a)^{n+1}}.$$

이는 평균값 정리를 일반화한 것입니다 ( $P_0 = f(a)$ 인 특수한 경우  $n=0$ 이 평균값 정리에 해당합니다).



**문제 29D** (Putnam 2018 A5).  $f: \mathbb{R} \rightarrow \mathbb{R}$ 가 매끄럽고,  $f(0) = 0$ ,  $f(1) = 1$ 이며 모든 실수  $x$ 에 대해  $f(x) \geq 0$ 이라고 가정하십시오. 어떤 양의 정수  $n$ 과 실수  $x$ 에 대해  $f^{(n)}(x) < 0$ 임을 증명하십시오.



**문제 29E.**  $f: \mathbb{R} \rightarrow \mathbb{R}$ 가 매끄럽다고 하십시오. 모든 점  $p$ 에 대해  $p$ 에서의  $f$ 의 테일러 급수가 양의 수렴 반경을 가진다고 가정하십시오. 적어도 한 점에서  $f$ 가 해석적임을 증명하십시오.



# 30 리만 적분

“불연속함수를 리만 적분하려는 것은 다소 시대에 뒤떨어진 일입니다.”

— Dennis Gaitsgory, [Ga15]

우리는 계속해서 리만 적분을 정의하겠지만, 이것으로 많은 것을 하지는 않을 것입니다. 그 이유는 르베그 적분이 기본적으로 더 낫기 때문이며, 따라서 리만 적분을 정의하고 미적분학의 기본 정리를 확인한 뒤(정확히는 이를 이 장 끝의 문제로 남겨두고), 이후로는 항상 르베그 적분을 사용할 것입니다.

## §30.1 균등 연속

**이 절의 대표적인 예:**  $f(x) = x^2$ 은  $\mathbb{R}$  위에서 균등 연속이 아니지만, 콤팩트 집합 위의 함수는 항상 균등 연속입니다.

**정의 30.1.1.** 두 거리 공간 사이의 연속 사상  $f: M \rightarrow N$ 이 있다고 합시다. 모든  $\varepsilon > 0$ 에 대해 어떤  $\delta > 0$ 이 존재하여 다음이 성립할 때  $f$ 가 **균등 연속**이라고 말합니다.

$$d_M(p, q) < \delta \implies d_N(f(p), f(q)) < \varepsilon.$$

차이점은  $\varepsilon > 0$ 이 주어졌을 때, 입력  $p$ 와  $q$ 의 모든 선택에 대해 작동하는  $\delta > 0$ 을 지정해야 한다는 점입니다. 반면 보통은  $\delta$ 가  $p$ 와  $q$ 에 의존하는 것이 허용됩니다. (또한 이 정의는 일반적인 위상 공간으로 옮길 수 없습니다.)

### 예제 30.1.2 (균등 연속성의 실패)

- (a)  $x \mapsto x^2$ 로 정의된 함수  $f: \mathbb{R} \rightarrow \mathbb{R}$ 는 균등 연속이 아닙니다. 예를 들어  $\varepsilon = 0.1$ 을 취해 봅시다.  $|x - y| < \delta$ 이면  $|x^2 - y^2| < 0.1$ 이 되도록 하는  $\delta$ 는 존재하지 않는데,  $x$ 와  $y$ 가 커질수록 함수  $f$ 가 작은 변화에 점점 더 민감해지기 때문입니다.
- (b)  $x \mapsto x^{-1}$ 로 정의된 함수  $(0, 1) \rightarrow \mathbb{R}$ 는 균등 연속이 아닙니다.
- (c)  $x \mapsto \sqrt{x}$ 로 정의된 함수  $\mathbb{R}_{>0} \rightarrow \mathbb{R}$ 는 (도함수가 유계가 아님에도 불구하고!) 실제로 균등 연속인 것으로 밝혀집니다. 실제로 다음 주장이

$$|x - y| < \varepsilon^2 \implies |\sqrt{x} - \sqrt{y}| < \varepsilon$$

임의의  $x, y, \varepsilon > 0$ 에 대해 성립함을 확인할 수 있습니다.

좋은 소식은 콤팩트한 경우에는 모든 것이 잘 성립한다는 것입니다.

### 정리 30.1.3 (콤팩트 공간에서는 균등 연속성이 공짜로 얻어짐)

$M$ 을 콤팩트 거리 공간이라 합시다. 그러면 임의의 연속 사상  $f: M \rightarrow N$ 은 균등 연속이기도 합니다.

증명. 모순을 위해 어떤 나쁜  $\varepsilon > 0$ 이 존재한다고 가정합시다. 그러면  $\delta = 1/n$ 을 취하면, 각 정수  $n$ 에 대해 서로  $1/n$  이내에 있지만  $f$ 에 의해  $\varepsilon$ 보다 멀리 떨어진 곳으로 사상되는 점  $p_n$ 과

$q_n$ 이 존재함을 알 수 있습니다. 기호로 쓰면,  $d_M(p_n, q_n) \leq 1/n$ 이지만  $d_N(f(p_n), f(q_n)) > \varepsilon$ 입니다.

$M$ 의 콤팩트성에 의해, 어떤  $x \in M$ 으로 수렴하는 수렴 부분수열  $p_{i_1}, p_{i_2}, \dots$ 을 찾을 수 있습니다.  $q_{i_n}$ 이  $p_{i_n}$ 과  $1/i_n$  이내에 있으므로, 이 역시 같은 점  $x \in M$ 으로 수렴해야 마땅합니다. 그러면 수열  $f(p_{i_n})$ 과  $f(q_{i_n})$ 은 둘 다  $f(x) \in N$ 으로 수렴해야 하지만, 이는 이들이 항상  $\varepsilon$ 보다 멀리 떨어져 있으므로 불가능합니다.  $\square$

이는 예를 들어 연속 함수  $[0, 1] \rightarrow \mathbb{R}$ 로 간주된  $x^2$ 이 자동으로 균등 연속임을 의미합니다. 이야, 콤팩트성이란 정말 대단하지 않습니까?

## §30.2 조밀 집합과 확장

**이 절의 대표적인 예:**  $\mathbb{Q} \rightarrow N$ 인 함수가 균등 연속이고  $N$ 이 완비이면, 이 함수는  $\mathbb{R} \rightarrow N$ 으로 확장됩니다. 아래의 반례도 참고하십시오.

**정의 30.2.1.** 위상 공간  $X$ 의 부분집합(또는 부분공간)  $S$ 가 있다고 합시다.  $X$ 의 모든 열린 집합이  $S$ 의 점을 포함할 때  $S$ 가 **조밀**하다고 말합니다.

### 예제 30.2.2 (조밀 집합)

- (a)  $\mathbb{Q}$ 는  $\mathbb{R}$ 에서 조밀합니다.
- (b) 일반적으로, 임의의 거리 공간  $M$ 은 그 완비화  $\overline{M}$ 에서 조밀합니다.

조밀 집합은 함수를 완성하는 데 유용합니다. 아이디어는, 어떤 거리 공간  $N$ 에 대해 연속 함수  $f: \mathbb{Q} \rightarrow N$ 이 있다면, 이를 함수  $\tilde{f}: \mathbb{R} \rightarrow N$ 으로 확장하는 방법이 많아야 하나 있어야 한다는 것입니다. 왜냐하면 우리는 각 유리수를 실수로 근사할 수 있기 때문입니다. 만약  $f(1), f(1.4), f(1.41), \dots$ 를 안다면,  $\tilde{f}(\sqrt{2})$ 는 이 수열의 극한이어야 마땅합니다. 따라서 이는 확실히 유일합니다.

그러나 이것이 잘못될 수 있는 두 가지 경우가 있습니다:

### 예제 30.2.3 (확장의 부존재)

- (a)  $N$ 이 완비가 아닐 수도 있으며, 그러면 극한이  $N$  안에 존재조차 하지 않을 수 있습니다. 예를 들어  $N = \mathbb{Q}$ 라면, 항등함수  $f: \mathbb{Q} \rightarrow \mathbb{Q}$ 조차도 함수  $\tilde{f}: \mathbb{R} \rightarrow \mathbb{Q}$ 으로 확장할 방법이 확실히 없습니다.
- (b)  $N$ 이 완비라 하더라도,  $f$ 가 폭발하는 문제가 생길 수 있습니다. 예를 들어  $N = \mathbb{R}$ 이라 하고 다음과 같이 정의합니다

$$f(x) = \frac{1}{x - \sqrt{2}} \quad f: \mathbb{Q} \rightarrow \mathbb{R}.$$

$\sqrt{2} \notin \mathbb{Q}$  근방에서  $f$ 가 폭발하기 때문에 이 경우에도 확장할 방법이 없으며, 이는  $\tilde{f}(\sqrt{2})$ 가 정의되지 않게 만들 것입니다.

그러나 이를 고치는 방법은  $f$ 가 균등연속일 것을 요구하는 것이며, 그 경우에는 유일한 확장을 얻게 됩니다.

**정리 30.2.4 (균등 연속 함수의 확장)**

$M$ 을 거리 공간,  $N$ 을 완비 거리 공간,  $S$ 를  $M$ 의 조밀 부분공간이라 하겠습니다.  $\psi: S \rightarrow N$ 가 균등 연속 함수라고 가정하겠습니다. 그러면 유일한 연속 함수  $\tilde{\psi}: M \rightarrow N$ 가 존재하여 다음 도식이

$$\begin{array}{ccc} M & \xrightarrow{\tilde{\psi}} & N \\ \uparrow & \nearrow \psi & \\ S & & \end{array}$$

가환합니다.

증명 개요. 논의에서 언급했듯이, 각  $x \in M$ 은  $S$  안의 수열  $x_1, x_2, \dots$ 로 근사할 수 있으며  $x_i \rightarrow x$ 입니다. 이제 두 가지 주요 가정인 완비성과 균등연속성이 사용됩니다.

**연습문제 30.2.5.** 균등연속성을 이용해  $\psi(x_1), \psi(x_2), \dots$ 이 코시 수열임을 보이고, 그다음  $N$ 의 완비성에 호소하여 이 수열이  $N$ 에서 수렴함을 증명합니다.

따라서 우리는  $\tilde{\psi}(x)$ 를 그 수열의 극한으로 정의합니다. 이는 수열의 선택에 의존하지 않으며, 수열적 연속성을 이용하여  $\tilde{\psi}$ 가 연속임을 보일 수 있습니다.  $\square$

### §30.3 리만 적분의 정의

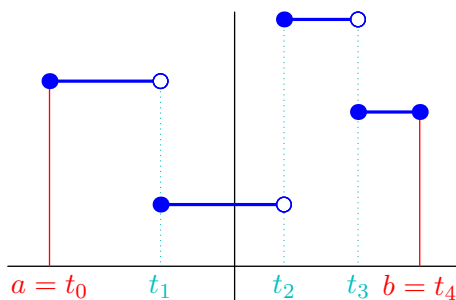
확장을 이용하면 리만 적분을 정의할 수 있습니다. 몇 가지 표기법을 도입해야 하니 잠시 참아 주십시오.

**정의 30.3.1.**  $[a, b]$ 를 닫힌구간이라 합시다.

- $C^0([a, b])$ 를  $[a, b] \rightarrow \mathbb{R}$  위의 연속함수들의 집합이라 합시다.
- $R([a, b])$ 를  $[a, b] \rightarrow \mathbb{R}$  위의 **계단 함수**들의 집합이라 합시다. 이 함수들은 구간  $[t_0, t_1), [t_1, t_2), [t_2, t_3), \dots, [t_{n-2}, t_{n-1})$ , 그리고  $[t_{n-1}, t_n]$ 에서 상수이며, 여기서  $a = t_0 < t_1 < t_2 < \dots < t_n = b$ 입니다.
- $M([a, b]) = C^0([a, b]) \cup R([a, b])$ 라 합시다.

주의:  $C^0([a, b])$ 만이 통상적인 표기법이며, 나머지 두 가지는 임의로 만든 것입니다.

전형적인 계단 함수의 예는 아래 그림을 참조하십시오. (각  $t_i$ 에 대해 자연스럽게 원하는 값이 두 개 있음에도 공식적으로 단 하나의 값을 지정해야 한다는 점이 성가시며, 그래서 왼쪽 끝점을 닫힌 것으로 두는 관례를 사용합니다.)



**정의 30.3.2.**  $M([a, b])$  위에 다음과 같이 정의하여 거리를 부여할 수 있습니다

$$d(f, g) = \sup_{x \in [a, b]} |f(x) - g(x)|.$$

그런데 계단 함수에 대해서는 자연스러운 적분 개념이 있습니다: 자명한 사각형들을 그제 합산하면 됩니다! 공식적으로는 다음 식입니다

$$f(a)(t_1 - a) + f(t_1)(t_2 - t_1) + f(t_2)(t_3 - t_2) + \cdots + f(t_n)(b - t_n).$$

이 함수를 다음과 같이 표기합니다

$$\Sigma: R([a, b]) \rightarrow \mathbb{R}.$$

### 정리 30.3.3 (리만 적분)

다음과 같은 유일한 연속 사상이 존재합니다

$$\int_a^b: M([a, b]) \rightarrow \mathbb{R}$$

다음 도식이

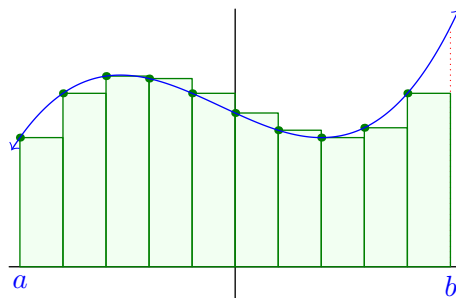
$$\begin{array}{ccc} M([a, b]) & \xrightarrow{\int_a^b} & \mathbb{R} \\ \uparrow & \nearrow \Sigma & \\ R([a, b]) & & \end{array}$$

가환하도록 합니다.

증명. 확장 정리를 적용하고자 하므로, 몇 가지만 확인하면 됩니다:

- $R([a, b])$ 가  $M([a, b])$ 의 조밀 부분집합임을 주장합니다. 다시 말해, 임의의 연속함수  $f: [a, b] \rightarrow \mathbb{R}$ 와  $\varepsilon > 0$ 에 대해,  $f$ 를  $\varepsilon$  이내로 근사하는 직사각형 함수가 존재하기를 원합니다.

이는 균등연속성에 의해 성립합니다.  $|x - y| < \delta$ 일 때마다  $|f(x) - f(y)| < \varepsilon$ 가 되도록 하는  $\delta > 0$ 가 존재함을 알고 있습니다. 따라서 폭이  $\delta$ 보다 작은 직사각형들로 이루어지고, 각 직사각형의 왼쪽 위 모서리가  $f$ 의 그래프 위에 놓이는 직사각형 함수를 선택하기만 하면 충분합니다.



- “직사각형을 더하는” 사상  $\Sigma: R([a, b]) \rightarrow \mathbb{R}$ 는 균등연속입니다. 사실 이는 꽤 자명합니다: 두 직사각형 함수  $f$ 와  $g$ 가  $d(f, g) < \varepsilon$ 를 만족하면,  $d(\Sigma f, \Sigma g) < \varepsilon(b - a)$ 입니다.
- $\mathbb{R}$ 는 완비입니다. □

## §30.4 메시(Mesh)

위의 정의는 취향에 따라 환상적이거나, 지나치게 복잡하거나, 우스꽝스럽거나, 끔찍하게 보일 수 있습니다. 하지만 이를 풀어보면 실제로는 여러분이 익숙한 그림과 다르지 않습니다.

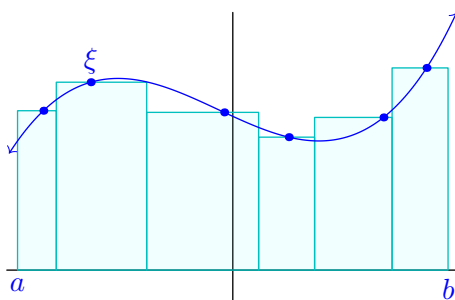
우리가 한 일은 모든 연속함수  $f: [a, b] \rightarrow \mathbb{R}$ 를 취하여 이것이 직사각형 함수로 근사될 수 있음을 보인 것입니다(이를 조밀 포함으로 표현했습니다). 그런 다음 직사각형들의 넓이를 더했습니다. 그럼에도 불구하고, 다른 곳에서 흔히 보던 것에 더 가까운 정의를 하나 제시하겠습니다.

**정의 30.4.1.**  $[a, b]$ 의 표시된 분할(tagged partition)  $P$ 는  $[a, b]$ 를  $n$ 개의 구간으로 나누는 분할과,  $i$ 번째 구간에 있는 점  $\xi_i$ 로 구성되며, 다음과 같이 표기합니다

$$a = t_0 < t_1 < t_2 < \cdots < t_n = b \quad \text{그리고} \quad \xi_i \in [t_{i-1}, t_i] \quad \forall 1 \leq i \leq n.$$

$P$ 의 메시(mesh)는 가장 긴 구간의 폭, 즉  $\max_i(t_i - t_{i-1})$ 입니다.

물론 이 정의의 핵심은 직사각형들을 더한다는 것이지만,  $\xi_i$ 는 표본점(sample point)입니다.



#### 정리 30.4.2 (리만 적분)

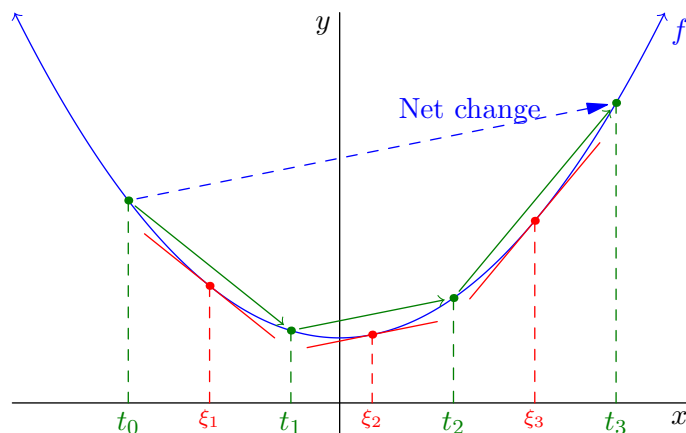
$f: [a, b] \rightarrow \mathbb{R}$ 가 연속함수라고 합시다. 그러면

$$\int_a^b f(x) dx = \lim_{\substack{P \text{ 표시된 분할} \\ \text{mesh } P \rightarrow 0}} \left( \sum_{i=1}^n f(\xi_i)(t_i - t_{i-1}) \right).$$

여기서 극한이란 메시가 0에 접근하는 분할들의 임의의 수열을 취할 수 있음을 의미합니다.

증명. 우변은 폭이 점점 좁아지는 직사각형들을 가진 직사각형 함수  $g_1, g_2, \dots$ 의 넓이에 대응합니다. 정리 30.3.3의 증명에서와 같이, 이 직사각형들의 메시가 0에 접근함에 따라, 균등연속성에 의해  $d(f, g_n) \rightarrow 0$  또한 성립합니다. 따라서 정리 30.3.3의 도식에서의 연속성에 의해, 필요한 대로  $\lim_n \Sigma(g_n) = \int(f)$ 를 얻습니다.  $\square$

평균값 정리와 결합하면, 이는 연속 도함수를 갖는 함수  $f$ 에 대한 미적분학의 기본정리의 짧은 증명을 제공하는 데 사용될 수 있습니다. 그 아이디어는, 임의의 분할  $a \leq t_0 < t_1 < t_2 < \cdots < t_n \leq b$ 의 선택에 대해, 평균값 정리를 사용하여 각 구간에서 할선의 기울기와 일치하도록  $\xi_i$ 를 고를 수 있어야 한다는 것입니다: 그 시점에서 넓이들의 합은  $f$ 의 전체 변화량과 같아집니다. 우리는 이 상황을 세 개의 점으로 예시하며, 독자에게 그 세부 사항을 문제 30B\*로 채워 넣기를 권합니다.



한 가지 짚고 넘어갈 점은, 제가 리만 적분을 연속함수에 대해서만 정의했지만, 이것이 존재하는 다른 함수들도 있어야 한다는 것입니다(예를 들어 “구간별 연속함수” 또는 “거의 모든 곳에서 연속인” 함수 등을 포함합니다). 관련 정의는 다음과 같습니다:

**정의 30.4.3.**  $f: [a, b] \rightarrow \mathbb{R}$ 가 반드시 연속일 필요는 없는 함수이지만, 다음 극한이

$$\lim_{\substack{P \text{ 표시된 분할} \\ \text{mesh } P \rightarrow 0}} \left( \sum_{i=1}^n f(\xi_i)(t_i - t_{i-1}) \right).$$

어쨌든 존재한다면,  $f$ 가  $[a, b]$ 에서 **리만 적분 가능**하다고 말하고 그 값을 그 극한  $\int_a^b f(x) dx$ 로 정의합니다.

모든 리만 적분 가능한 함수는 르베그 적분 가능하며, 르베그 적분이 더 낫다는 것을 보게 될 것이므로, 이 정의를 실제로는 그다지 사용하지 않을 것입니다.

#### 예제 30.4.4 (여러분의 AP 미적분학이 돌아옵니다)

**문제 30B\***가 우리가 실제로 리만 적분을 계산할 수 있음을 함의한다는 점을 언급해야겠지만, 여러분 대부분은 이미 고등학교 미적분학에서 이를 알고 있을 것입니다. 예를 들어, 구간  $(1, 4)$ 에서 함수  $F(x) = \frac{1}{3}x^3$ 의 도함수는  $F'(x) = x^2$ 입니다.  $f(x) = x^2$ 가 연속함수  $f: [1, 4] \rightarrow \mathbb{R}$ 이므로, 다음을 연습합니다

$$\int_1^4 x^2 dx = F(4) - F(1) = \frac{64}{3} - \frac{1}{3} = 21.$$

$F(x) = \frac{1}{3}x^3 + 2019$ 를 선택할 수도 있었음에 유의하십시오; 함수  $F$ 는 평행이동을 제외하면 유일하며, 이 상수는 뺄셈을 할 때 상쇄됩니다. 이것이 고등학교에서 (실제로) 표기법을 남용하여  $\int x^2 dx = \frac{1}{3}x^3 + C$ 라고 쓰는 것이 흔한 이유입니다.

### §30.5 생각해 볼 만한 조금 더 어려운 문제

**문제 30A.**  $f: (a, b) \rightarrow \mathbb{R}$ 가 미분가능하고  $f'$ 가 유계라고 가정합니다.  $f$ 가 균등연속임을 보이십시오.

**문제 30B\*** (미적분학의 기본정리).  $f: [a, b] \rightarrow \mathbb{R}$ 가 연속이고  $(a, b)$ 에서 미분가능하며, 도함수  $f'$ 가 연속함수  $f': [a, b] \rightarrow \mathbb{R}$ 로 확장된다고 하십시오. 다음을 증명하십시오.

$$\int_a^b f'(x) dx = f(b) - f(a).$$

**문제 30C\*** (이상적분). 각 양의 실수  $r > 0$ 에 대해, 다음 극한값을 구하십시오.<sup>1</sup>

$$\lim_{\varepsilon \rightarrow 0^+} \int_{\varepsilon}^1 \frac{1}{x^r} dx$$

또는 극한이 존재하지 않음을 보이십시오.

이는 직관적으로 "이상" 적분  $\int_0^1 x^{-r} dx$ 로 생각할 수 있습니다. 우리가 콤팩트하지 않은  $(0, 1]$  위에서의 적분을 정의하지 않았으며(또한 정의할 수도 없으므로) 이는 원래 정의에서는 의미가 없지만, 임의의  $\varepsilon > 0$ 에 대해  $[\varepsilon, 1]$  위에서의 적분은 여전히 고려할 수 있습니다.

**문제 30D.** 다음을 보이십시오.

$$\lim_{n \rightarrow \infty} \left( \frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{2n} \right) = \log 2.$$

<sup>1</sup>표기  $\varepsilon \rightarrow 0^+$ 에 익숙하지 않다면,  $\varepsilon$ 를  $M > 0$ 에 대한  $1/M$ 로 바꾸고 대신  $M \rightarrow \infty$ 로 놓으셔도 됩니다.



# IX

복소해석학

## 제IX부: 목차

---

|           |                               |            |
|-----------|-------------------------------|------------|
| <b>31</b> | <b>정칙 함수</b>                  | <b>349</b> |
| 31.1      | 세상에서 가장 훌륭한 함수들               | 349        |
| 31.2      | 복소 미분                         | 351        |
| 31.3      | 경로 적분                         | 352        |
| 31.4      | 코시-구르사 정리                     | 354        |
| 31.5      | 코시의 적분 정리                     | 355        |
| 31.6      | 정칙 함수는 해석적입니다                 | 357        |
| 31.7      | 선택: 정칙 함수가 해석적임을 증명하기         | 359        |
| 31.8      | 생각해 볼 만한 조금 더 어려운 문제          | 362        |
| <b>32</b> | <b>유리형 함수</b>                 | <b>365</b> |
| 32.1      | 세상에서 두 번째로 멋진 함수들             | 365        |
| 32.2      | 유리형 함수                        | 365        |
| 32.3      | 회전수와 유수 정리                    | 369        |
| 32.4      | 편각 원리                         | 371        |
| 32.5      | 여담: 기하학적으로 바라본 편각 원리          | 372        |
| 32.6      | 철학: 정칙 함수는 왜 그렇게 좋은 성질을 가지는가? | 373        |
| 32.7      | 생각해 볼 만한 조금 더 어려운 문제          | 374        |
| <b>33</b> | <b>정칙 제곱근과 로그</b>             | <b>375</b> |
| 33.1      | 동기 부여: 복소수의 제곱근               | 375        |
| 33.2      | 정칙 함수의 제곱근                    | 377        |
| 33.3      | 피복 사영                         | 378        |
| 33.4      | 복소 로그                         | 378        |
| 33.5      | 몇 가지 특수한 경우                   | 379        |
| 33.6      | 생각해 볼 만한 조금 더 어려운 문제          | 380        |
| <b>34</b> | <b>보너스: 위상수학적 아벨-루피니 정리</b>   | <b>381</b> |
| 34.1      | 진행 계획                         | 381        |
| 34.2      | 단계 1: 가장 단순한 경우               | 381        |
| 34.3      | 단계 2: 중첩된 근호                  | 382        |
| 34.4      | 3단계: 정규 근                     | 383        |
| 34.5      | 요약                            | 384        |
| 34.6      | 생각해 볼 만한 조금 더 어려운 문제          | 384        |

---

# 31 정칙 함수

이 장 전체에서  $U$ 는 복소평면의 열린집합을 나타내고,  $\Omega$ 는 단순 연결이기도 한 열린집합을 나타냅니다. 이 장의 주요 참고 문헌은 [Ya12; Ba10]였습니다.

## §31.1 세상에서 가장 훌륭한 함수들

고등학교에서 여러분은 실숫값 함수를 미분하고 적분하는 방법을 배웠습니다. 복소해석학을 다루는 이 장에서는 이를 복소숫값 함수의 미분과 적분으로 확장하겠습니다.

별거 아니라고 생각하실 수도 있습니다. 미적분학은 이미 충분히 지루했으니까요. 복소 미적분학에 왜 신경을 써야 할까요?

실해석학과 복소해석학을 비교하는 것이 아마도 이를 동기부여하는 가장 쉬운 방법일 것입니다. 실해석학에서는 입력값이 실수선  $\mathbb{R}$  안에 존재합니다. 이 실수선은 그다지 까다롭지 않아서, 매우 좋지 않은 성질을 가진 함수들을 많이 만들어낼 수 있습니다. 다음은 그 예시입니다.

### 예제 31.1.1 (선택 사항: 나쁜 실함수들)

이 부분은 요점을 보여주기 위한 것일 뿐이므로 매우 빠르게 훑어보셔도 됩니다.

(a) **악마의 계단**(또는 칸토어 함수)은 “거의 모든 곳에서” 도함수가 0인 연속함수  $H: [0, 1] \rightarrow [0, 1]$ 이지만,  $H(0) = 0$ 이고  $H(1) = 1$ 입니다.

(b) **바이어슈트라스  $\beta$  함수**

$$x \mapsto \sum_{n=0}^{\infty} \left(\frac{1}{2}\right)^n \cos(2015^n \pi x)$$

는 모든 곳에서 연속이지만 어느 곳에서도 미분 가능하지 않습니다.

(c) 다음 함수는

$$x \mapsto \begin{cases} x^{100} & x \geq 0 \\ -x^{100} & x < 0 \end{cases}$$

처음 99개의 도함수는 존재하지만 100번째 도함수는 존재하지 않습니다.

(d) 어떤 함수가 모든 도함수를 가진다면(이런 함수를 **매끄러운**(smooth) 함수라고 부릅니다), 그 함수는 테일러 급수를 가집니다. 하지만 실함수의 경우 그 테일러 급수는 여전히 틀릴 수 있습니다. 다음 함수는

$$x \mapsto \begin{cases} e^{-1/x} & x > 0 \\ 0 & x \leq 0 \end{cases}$$

모든 점에서 도함수를 가집니다. 하지만  $x = 0$ 에서 테일러 급수를 전개하면  $0 + 0x + 0x^2 + \dots$ 를 얻는데, 이는 어떤  $x > 0$ (심지어  $x = 0.0001$ )에 대해서도 틀립니다.

병리적인 경우는 잠시 제쳐 두겠습니다. 실수 매끄러운 함수의 값을 구간  $[-1, 1]$  위에서

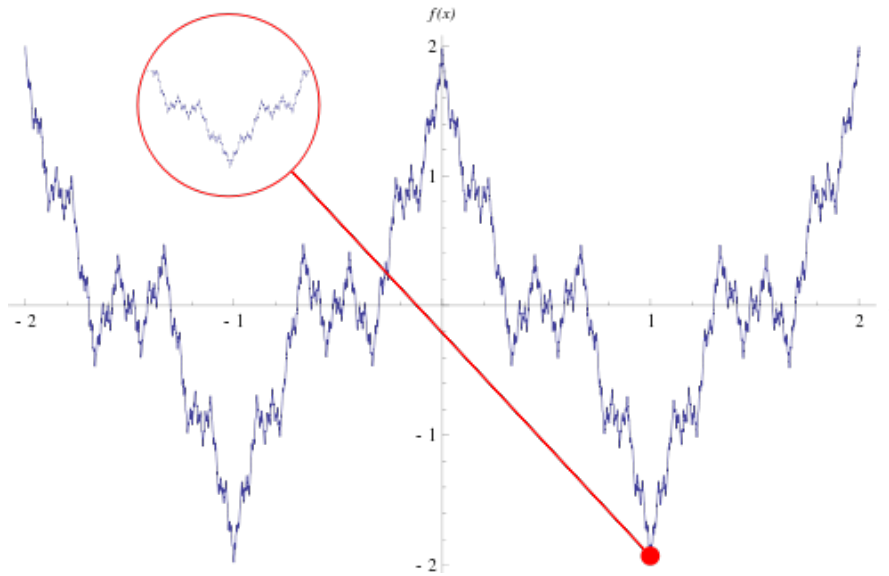


그림 31.1: 바이어슈트라스 함수(이미지 출처 [Ee]).

알려준다고 해도, 그것만으로는 함수 전체에 대해 아무것도 알 수 없습니다. 매끄러운 함수들을 어떻게든 "이어 붙이는" 것이 가능하기 때문에, 그 함수는 말 그대로 무엇이든 될 수 있습니다.

그렇다면 복소함수는 어떨까요? 이를  $\mathbb{R}^2 \rightarrow \mathbb{R}^2$ 의 함수로 본다면, 이제 선분이 아닌 것들을 따라서도 적분할 수 있다는 흥미로운 성질을 갖게 됩니다. 즉, 평면 위의 곡선을 가로지르는 적분을 쓸 수 있습니다. 하지만  $\mathbb{C}$ 에는 그 이상의 것이 있습니다: 그것은 체(field)이므로, 두 복소수를 곱하고 나눌 수 있습니다.

그래서 우리는 관심을 정칙 함수(holomorphic function)라고 불리는 미분가능한 함수들로 제한합니다.  $\mathbb{C}$  위의 곱셈이 모든 차이를 만들어낸다는 것이 밝혀집니다. 이어지는 내용의 핵심 주제는, 정칙 함수가 정말, 정말 좋은 성질을 가진다는 것과, 함수에 대한 아주 적은 양의 정보만 알아도 함수의 모든 값을 결정할 수 있다는 것입니다.

이 장의 두 가지 주요 하이라이트는 다음과 같으며, 다른 모든 결과는 거의 여기서 나오는 따름정리입니다:

- 폐곡선을 따른 등고선 적분(contour integral)은 항상 0입니다.
- 정칙 함수는 본질적으로 그 테일러 급수로 주어집니다. 특히, 한 번 미분가능하다는 것은 무한히 미분가능하다는 것을 함의합니다. 따라서 정칙 함수는 다항식과 상당히 비슷하게 행동합니다.

이로부터 나오는 몇 가지 따름정리는 다음과 같습니다:

- 단위원 경계 위에서 정칙 함수의 값을 아는 것만으로 그 내부에서의 값을 알 수 있다는 것이 밝혀질 것입니다.
- $1, \frac{1}{2}, \frac{1}{3}, \dots$ 에서의 함수 값을 아는 것만으로도 함수 전체를 결정하기에 충분합니다!
- 유계인 정칙 함수  $\mathbb{C} \rightarrow \mathbb{C}$ 는 반드시 상수여야 합니다.
- 그리고 더 많은 것들이...

[Pu02]에서 다음과 같이 말합니다: “복소해석학은 선한 쌍둥이이고 실해석학은 악한 쌍둥이이다: 아름다운 공식과 우아한 정리들이 복소 영역에서는 저절로 피어나는 것처럼 보이는 반면, 실수 영역에서는 고생과 병리 현상이 지배한다”.

## §31.2 복소 미분

**이 절의 대표적인 예:** 다항식은 정칙이지만,  $\bar{z}$ 는 그렇지 않습니다.

$f: U \rightarrow \mathbb{C}$ 를 복소 함수라 합시다. 그러면 어떤  $z_0 \in U$ 에 대해,  $z_0$ 에서의 **도함수**를 다음과 같이 정의합니다

$$\lim_{h \rightarrow 0} \frac{f(z_0 + h) - f(z_0)}{h}.$$

이 극한이 존재하지 않을 수도 있음에 유의하십시오. 극한이 존재할 때  $f$ 가  $z_0$ 에서 **미분가능**하다고 말합니다.

“복소” 극한  $h \rightarrow 0$ 이란 무엇을 의미할까요? 예상하시는 그대로입니다: 모든  $\varepsilon > 0$ 에 대해 다음을 만족하는  $\delta > 0$ 이 존재해야 합니다

$$0 < |h| < \delta \implies \left| \frac{f(z_0 + h) - f(z_0)}{h} - L \right| < \varepsilon.$$

위상수학을 좋아하신다면, 이를 복소평면에서의 열린 근방의 관점에서 생각해 보시길 권합니다. (이것이 바로  $U$ 가 열려 있어야 하는 이유입니다: 그래야 그 안에서  $\delta$ -근방을 취할 수 있기 때문입니다.)

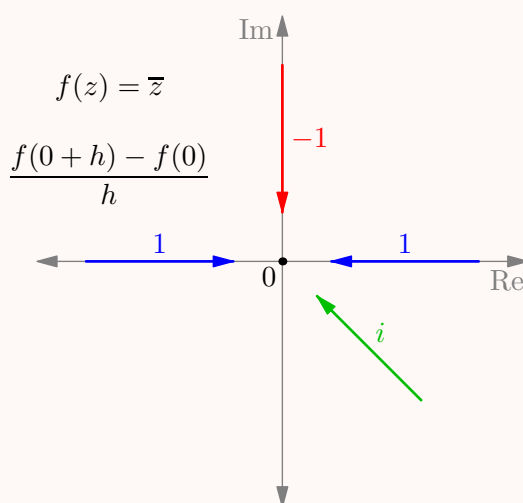
그러나 복소 도함수를 갖는다는 것은 실함수가 도함수를 갖는 것보다 실제로 훨씬 더 강한 조건임에 유의하십시오. 실수선에서는  $h$ 가 오직 아래와 위에서만 0에 접근할 수 있으며, 극한이 존재하려면 “좌극한”이 “우극한”과 같아야 합니다. 하지만 복소수는 평면을 이룹니다:  $h$ 는 여러 방향에서 0에 접근할 수 있으며, 우리는 그 모든 극한이 같아야 함을 필요로 합니다.

### 예제 31.2.1 (중요: 켈레는 정칙이 아닙니다)

$f(z) = \bar{z}$ 를 복소 켈레,  $f: \mathbb{C} \rightarrow \mathbb{C}$ 라 합시다. 이 함수는 단순한 성질에도 불구하고 정칙이 아닙니다! 실제로,  $z = 0$ 에서 우리는 다음을 얻습니다,

$$\frac{f(h) - f(0)}{h} = \frac{\bar{h}}{h}.$$

이는  $h \rightarrow 0$ 일 때 극한을 갖지 않는데, 왜냐하면 “어느 방향”에서 0에 접근하느냐에 따라 서로 다른 값을 갖기 때문입니다.



함수  $f: U \rightarrow \mathbb{C}$ 가 그 정의역의 모든 점에서 복소 미분 가능하다면 이를 **정칙**(holomorphic)이라고 부릅니다. 정의역이  $U = \mathbb{C}$ 인 정칙 함수의 특수한 경우에는 이 함수를 **전해석적**

라고 부릅니다.<sup>1</sup>

### 예제 31.2.2 (정칙 함수의 예시)

아래 모든 예시에서 함수의 도함수는 실수 유사물에서와 동일합니다(예를 들어  $e^z$ 의 도함수는  $e^z$ 입니다).

- (a) 임의의 다항식  $z \mapsto z^n + c_{n-1}z^{n-1} + \dots + c_0$ 은 정칙입니다.
- (b) 복소 지수 함수  $\exp: x + yi \mapsto e^x(\cos y + i \sin y)$ 는 정칙임을 보일 수 있습니다.
- (c)  $\sin$ 과  $\cos$ 는  $\cos z = \frac{e^{iz} + e^{-iz}}{2}$ 와  $\sin z = \frac{e^{iz} - e^{-iz}}{2i}$ 로 복소평면에 확장했을 때 정칙입니다.
- (d) 평소와 같이 합, 곱, 연쇄 법칙 등이 적용되며, 따라서 **정칙 함수들의 합, 곱, 영이 아닌 몫, 합성 역시 정칙입니다.**

이 결과들을 증명해 보셔도 좋지만, 저는 굳이 그렇게 하지 않겠습니다.

## §31.3 경로 적분

**이 절의 대표적인 예:** 단위원을 도는  $\oint_{\gamma} z^m dz$ .

실수선에서는 함수를 선분  $[a, b]$ 에 걸쳐 적분하는 방법을 알고 있었습니다: 본질적으로 그 선분을 "따라가며" 보이는  $f$ 의 값들을 더해 어떤 넓이를 얻는 것이었습니다. 실수선과 달리 복소평면에서는 임의의 경로에 걸쳐 적분할 수 있는 힘을 가집니다: 예를 들어, 단위원을 도는 적분을 계산할 수도 있습니다. 경로 적분은 이를 형식화할 수 있게 해줍니다.

먼저,  $f: \mathbb{R} \rightarrow \mathbb{C}$ 이고  $u, v \in \mathbb{R}$ 에 대해  $f(t) = u(t) + iv(t)$ 라면, 단순히 실수부와 허수부를 더함으로써 적분  $\int_a^b$ 를 정의할 수 있습니다:

$$\int_a^b f(t) dt = \left( \int_a^b u(t) dt \right) + i \left( \int_a^b v(t) dt \right).$$

이제  $\alpha: [a, b] \rightarrow \mathbb{C}$ 를 복소 미분 가능<sup>2</sup> 함수로 여겨지는 경로라고 합시다. 이러한 경로를 **경로**(contour)라고 부르며, 그 **경로 적분**을 다음과 같이 정의합니다

$$\oint_{\alpha} f(z) dz = \int_a^b f(\alpha(t)) \cdot \alpha'(t) dt.$$

이것은 거의  $u$ -치환으로 생각할 수 있습니다(여기서  $\alpha'$ 가 나오는 것입니다). 특히, 이 적분은  $\alpha$ 가 어떻게 "매개변수화"되는지에 의존하지 않는다는 것이 밝혀집니다:

$$[0, 2\pi] \rightarrow \mathbb{C}: t \mapsto e^{it}$$

로 주어지는 원과,

$$[0, 1] \rightarrow \mathbb{C}: t \mapsto e^{2\pi it}$$

로 주어지는 또 다른 원과,

$$[0, 1] \rightarrow \mathbb{C}: t \mapsto e^{2\pi it^5}$$

<sup>1</sup>미안합니다, "holomorphic"이라는 단어가 훨씬 더 멋지게 들린다는 것을 알고 있습니다. 바로 그 이유 하나만으로 좀 더 일반적으로 다루어 보겠습니다.

<sup>2</sup>여기서 이는 완전히 정확하지는 않습니다: 경로  $\alpha$ 가 연속이고 대부분 미분 가능하기를 원하지만, 유한 개의 점에서 "날카로운 굽음"을 가지는 것은 허용합니다; 다시 말해,  $n$ 개의 매끄러운 조각들의 결합인 경로들을 고려할 수 있습니다. 하지만 이를 위해서는  $\alpha$ 가 "유계 길이"를 가진다는 조건도 필요합니다.

로 주어지는 또 다른 원은 모두 같은 경로 적분을 줍니다. 왜냐하면 이들이 나타내는 경로들이 “단위원을 한 바퀴 돈다”는 동일한 기하학적 묘사를 가지기 때문입니다.

이어지는 내용에서 저는 일반적인 경로에는  $\alpha$ 를, 고리인 특수한 경우에는  $\gamma$ 를 사용하려고 합니다.

경로 적분의 예를 하나 살펴보겠습니다.

### 정리 31.3.1

$\gamma: [0, 2\pi] \rightarrow \mathbb{C}$ 를 다음으로 명시되는 단위원이라 하겠습니다

$$t \mapsto e^{it}.$$

그러면 임의의 정수  $m$ 에 대해 다음이 성립합니다

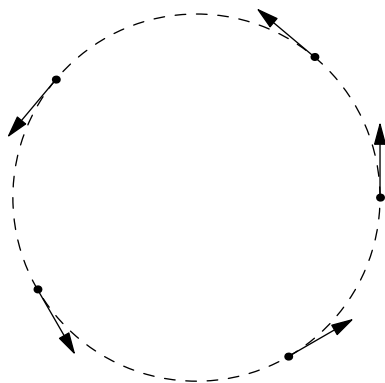
$$\oint_{\gamma} z^m dz = \begin{cases} 2\pi i & m = -1 \\ 0 & \text{그렇지 않으면} \end{cases}$$

증명.  $e^{it}$ 의 도함수는  $ie^{it}$ 입니다. 따라서 정의에 의해 답은 다음의 값입니다

$$\begin{aligned} \int_0^{2\pi} (e^{it})^m \cdot (ie^{it}) dt &= \int_0^{2\pi} i(e^{it})^{1+m} dt \\ &= i \int_0^{2\pi} \cos[(1+m)t] + i \sin[(1+m)t] dt \\ &= - \int_0^{2\pi} \sin[(1+m)t] dt + i \int_0^{2\pi} \cos[(1+m)t] dt. \end{aligned}$$

이제 이것은 초보적인 미적분학 문제입니다.  $m = -1$ 일 때 이것이  $2\pi i$ 와 같고, 그렇지 않으면 적분이 소멸함을 알 수 있습니다.  $\square$

$m = 0$ 인 경우에 이것이 직관적으로 왜 참이어야 하는지 설명해 보겠습니다. 이 경우  $\oint_{\gamma} 1 dz$ 를 가집니다. 따라서 적분이 단위원을 따라 걸어갈 때, 그것은 모든 점에서의 모든 접벡터(그것이 걸어가는 방향입니다)에 1을 곱한 것을 “합산”합니다. 그리고 원의 아름다운 대칭성을 감안하면, 모든 것이 상쇄된다는 것은 놀라운 일이 아닐 것입니다. 이 정리는  $m \neq -1$ 에 대해  $z^m$ 을 곱하더라도 같은 상쇄가 일어난다고 말합니다.



**정의 31.3.2.**  $\alpha: [0, 1] \rightarrow \mathbb{C}$ 가 주어지면, 우리는  $\bar{\alpha}$ 로 “역방향” 경로  $\bar{\alpha}(t) = \alpha(1 - t)$ 를 표기합니다.

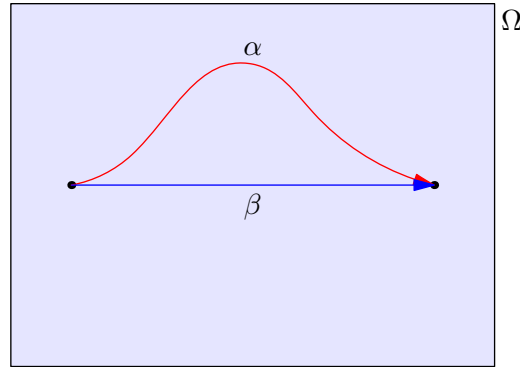
**질문 31.3.3.**  $\oint_{\alpha} f dz$ 와  $\oint_{\bar{\alpha}} f dz$  사이의 관계는 무엇입니까? 증명하십시오.

이것은 다소 지루하게 보일 수 있습니다. 정말로 멋진 일들이 곧 시작될 것이라고 약속드립니다.

### §31.4 코시-구르사 정리

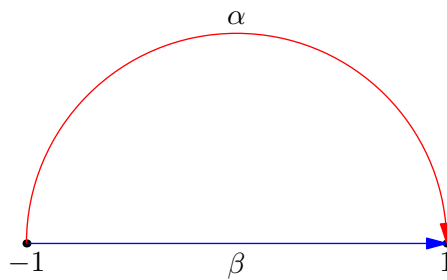
**이 절의 대표적인 예:**  $m \geq 0$ 일 때  $\oint_{\gamma} z^m dz = 0$ 입니다. 하지만  $m < 0$ 이면 코시 정리가 적용되지 않습니다.

$\Omega \subseteq \mathbb{C}$ 가 단순 연결(simply connected)이라 하고(예를 들어,  $\Omega = \mathbb{C}$ ), 시작점과 끝점이 같은 두 경로  $\alpha, \beta$ 를 생각해봅시다.



$\oint_{\alpha} f(z) dz$ 와  $\oint_{\beta} f(z) dz$  사이에는 어떤 관계가 있을까요? 공간  $\Omega$ 가 단순 연결이라는 점을 고려하면 둘 사이에 어떤 관계가 있으리라 기대할 수 있을 것입니다. 하지만 아마도 많은 관계가 있으리라고는 기대하지 않을 것입니다.

구체적인 예로,  $\Psi: \mathbb{C} \rightarrow \mathbb{C}$ 를  $z \mapsto z - \operatorname{Re}[z]$ 인 함수라 하겠습니다(예를 들어,  $\Psi(2015 + 3i) = 3i$ ).  $-1$ 에서  $1$ 로 가는 두 경로를 생각해봅시다. 즉  $\beta$ 는 실수축을 따라 걷고,  $\alpha$ 는 위쪽 반원을 따릅니다.



당연히  $\oint_{\beta} \Psi(z) dz = 0$ 입니다. 하지만  $\oint_{\alpha} \Psi(z) dz$ 가 얼마와 같아야 하는지는 하늘만이 알 것입니다. 게으름 피우지 않고 지금 한번 계산해 볼 수 있습니다. 원한다면 직접 계산해 보셔도 좋습니다 (조금 번거롭지만 어렵지는 않습니다). 저 자신이 실수하지 않았다면, 그 값은

$$\oint_{\alpha} \Psi(z) dz = - \oint_{\bar{\alpha}} \Psi(z) dz = - \int_0^{\pi} (i \sin(t)) \cdot ie^{it} dt = \frac{1}{2}\pi i$$

이는 특히 0이 아닙니다.

하지만 어쨌든  $\Psi$ 는 그다지 자연스러운 함수가 아닙니다. 입력값의 실수부를 무례하게 잘라내 버리기 때문에  $\mathbb{C}$ 의 좋은 곱셈적 구조를 전혀 존중하지 않습니다. 더 정확히 말하면,

**질문 31.4.1.**  $\Psi(z) = z - \operatorname{Re}[z]$ 가 정칙이 아님을 보이십시오. (힌트:  $\bar{z}$ 는 정칙이 아닙니다.)

이제 기적이 하나 있습니다: 정칙 함수의 경우, 두 적분은 항상 같습니다. 동등하게 말하면 ( $\alpha$  다음에  $\beta$ 를 잇는다고 생각하면), 고리의 등고선 적분은 항상 0입니다. 이것이 바로 저명한 코시-구르사 정리입니다 (코시 적분 정리라고도 불리지만, 나중에 “코시 적분 공식”이 따로 나오므로 그 얘기는 접어두겠습니다).

#### 정리 31.4.2 (코시-구르사 정리)

$\gamma$ 를 고리라 하고,  $f: \Omega \rightarrow \mathbb{C}$ 를 정칙 함수라 하되  $\Omega$ 는  $\mathbb{C}$ 에서 열려 있고 단순 연결이라고 합시다. 그러면

$$\oint_{\gamma} f(z) dz = 0.$$

**비고 31.4.3 (타당성 점검)** — 앞서  $\oint_{\gamma} z^{-1} dz = 2\pi i$ 임을 본 것을 생각하면 이는 놀라워 보일 수 있습니다. 미묘한 점은  $z^{-1}$ 이  $z = 0$ 에서조차 정의되지 않는다는 것입니다. 반면,  $\mathbb{C} \setminus \{0\} \rightarrow \mathbb{C}$ 인 함수  $z \mapsto \frac{1}{z}$ 는 정칙입니다! 이제 문제는  $\Omega = \mathbb{C} \setminus \{0\}$ 이 단순 연결이 아니라는 점입니다. 따라서 이 정리는, 비록 가까스로이지만, 우리의 타당성 점검을 통과합니다.

코시 정리의 전형적인 증명은 추가로  $f$ 의 편도함수가 연속이라고 가정한 뒤 이른바 그린 정리를 적용합니다. 하지만 위에서 서술한,  $f$ 가 정칙이라는 것만을 가정하는 완전히 일반적인 정리를 성공적으로 증명한 사람은 바로 구르사였습니다.

어쨌든 이 정리는  $m \geq 0$ 일 때  $\oint_{\gamma} z^m dz = 0$ 임을 함의합니다. 앞서 우리가 애써 한 작업이 이렇게 정리되는군요. 하지만 지금까지 우리는 원에서만 놀아봤습니다. 이 정리는 고리인 임의의 경로에 대해 성립합니다. 그러면 우리는 또 무엇을 할 수 있을까요?

## §31.5 코시의 적분 정리

이제 우리는 코시-구르사의 놀라운 응용, 즉 하나의 “표현 정리”를 제시합니다: 본질적으로 이는 원판 내부에서  $f$ 의 값이 경계에서의 값만으로 결정된다는 것을 말합니다! 실제로 우리는 정확한 공식까지 적어낼 것입니다. [Yal12]가 말하듯, “어떤 종류의 함수가 일종의 표현 정리를 만족할 때마다, 더 많은 심오한 정리들이 뒤따를 가능성이 높습니다.” 이제 커튼을 걷어봅시다:

#### 정리 31.5.1 (코시의 적분 공식)

$\gamma: [0, 2\pi] \rightarrow \mathbb{C}$ 를  $t \mapsto Re^{it}$ 로 주어지는, 평면 위에서 원판  $D$ 를 경계로 갖는 원이라고 합시다.  $f: U \rightarrow \mathbb{C}$ 가 정칙이고  $U$ 가 이 원과 그 내부를 포함한다고 합시다. 그러면  $D$ 의 내부에 있는 임의의 점  $a$ 에 대해 다음이 성립합니다.

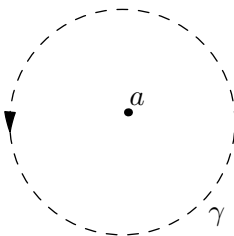
$$f(a) = \frac{1}{2\pi i} \oint_{\gamma} \frac{f(z)}{z - a} dz.$$

우리는  $U$ 가 단순 연결일 것을 요구하지 않는다는 점에 유의하십시오. 하지만 그 이유는 꽤 시시합니다: 우리는 어차피 열린 원판인  $D$ 에 대해서만  $f$ 를 적분할 것이고, 따라서 그 원판은 어쨌든 단순 연결이기 때문입니다.

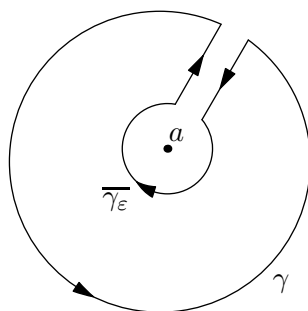
앞서  $\oint_{\gamma} z^{-1} dz$ 의 형태로 보았던  $2\pi i$ 의 등장은 우연이 아닙니다. 실제로 그것이 바로 우리가 이 결과를 증명하는 데 사용할 핵심 결과입니다.

**비고 31.5.2** — 다음 장에서 유리형 함수를 도입하면서, **비고 32.3.5**에서 이 공식을 직관적으로 유도하는 방법을 보게 될 것입니다.

증명. 여러 증명이 있지만, 저는 코시 정리의 힘을 정말로 잘 이끌어내는 증명을 보여드리고자 합니다. 여기 우리가 가진 그림이 있습니다: 원  $\gamma$  내부에 점  $a$ 가 놓여 있고, 우리는 값  $f(a)$ 를 손에 넣고 싶어합니다.



우리는 하나의 트릭을 쓸 것입니다: 바깥쪽 원  $\gamma$ 와, 그 안쪽에  $a$ 를 중심으로 하고 반지름이  $\epsilon$ 이며 시계 방향으로 도는 원  $\bar{\gamma}_\epsilon$ (따라서  $\gamma_\epsilon$ 는 반시계 방향으로 돕니다)를 갖는 **열쇠구멍 경로**  $\Gamma_{\delta,\epsilon}$ 를 구성하는 것입니다. 통로의 "폭"은  $\delta$ 입니다. 그림을 보십시오:



따라서  $\Gamma_{\delta,\epsilon}$ 는 네 개의 매끄러운 곡선으로 이루어집니다.

**질문 31.5.3.** 전체  $\Gamma_{\delta,\epsilon}$ 를 포함하지만 점  $a$ 는 포함하지 않는 단순 연결 열린집합  $\Omega$ 를 그려봅시다.

함수  $\frac{f(z)}{z-a}$ 는  $\Omega$  전체에서 정칙 함수가 됩니다. 따라서 코시의 정리가 적용되며, 다음을 알려줍니다.

$$0 = \oint_{\Gamma_{\delta,\epsilon}} \frac{f(z)}{z-a} dz.$$

$\delta \rightarrow 0$ 로 보내면, 열쇠구멍의 두 벽은 서로 상쇄됩니다(왜냐하면  $f$ 는 연속이고, 두 벽이 반대 방향으로 진행하기 때문입니다). 그러므로  $\delta \rightarrow 0$ 일 때 극한을 취하면,  $\gamma$ 와  $\gamma_\epsilon$ 만 남게 되고, (다시 방향을 고려하면) 다음을 얻습니다.

$$\oint_{\gamma} \frac{f(z)}{z-a} dz = - \oint_{\bar{\gamma}_\epsilon} \frac{f(z)}{z-a} dz = \oint_{\gamma_\epsilon} \frac{f(z)}{z-a} dz.$$

따라서  $\gamma$ 를  $a$ 를 중심으로 하는 훨씬 더 작은 원  $\gamma_\epsilon$ 로 대체하는 데 성공했으며, 나머지는 대수적 계산입니다.

마지막 양을 계산하기 위해 다음과 같이 씁니다.

$$\begin{aligned} \oint_{\gamma_\epsilon} \frac{f(z)}{z-a} dz &= \oint_{\gamma_\epsilon} \frac{f(z) - f(a)}{z-a} dz + f(a) \cdot \oint_{\gamma_\epsilon} \frac{1}{z-a} dz \\ &= \oint_{\gamma_\epsilon} \frac{f(z) - f(a)}{z-a} dz + 2\pi i f(a). \end{aligned}$$

여기서 정리 31.3.1을 사용했습니다. 따라서 우리가 해야 할 일은 다음을 보이는 것뿐입니다.

$$\oint_{\gamma_\varepsilon} \frac{f(z) - f(a)}{z - a} dz = 0.$$

이를 위해 기본적으로 가장 약한 형태의 경계, 이른바  $ML$  보조정리를 증명 없이 인용하여 사용할 수 있습니다. 이는 "함수를 어디서나 그 최댓값으로 경계 짓는다"는 것을 말합니다.

#### 보조정리 31.5.4 ( $ML$ 추정 보조정리)

$f$ 를 정칙 함수,  $\alpha$ 를 경로라고 합시다.  $M = \max_{z \text{ 위에서 } \alpha} |f(z)|$ 라 하고,  $L$ 을  $\alpha$ 의 길이라고 합시다. 그러면 다음이 성립합니다.

$$\left| \int_{\alpha} f(z) dz \right| \leq ML.$$

(길이의 정의, 즉  $\alpha: [a, b] \rightarrow \mathbb{C}$ 일 때  $L = \int_a^b |\alpha'(t)| dt$ 를 안다면 이는 증명하기 어렵지 않습니다.)

어쨌든,  $\varepsilon \rightarrow 0$ 일 때  $\frac{f(z)-f(a)}{z-a}$ 라는 양은  $f'(a)$ 에 가까워지므로, 충분히 작은  $\varepsilon$ 에 대해(즉  $z$ 가  $a$ 에 가까울 때) 어떤 상계  $M$ 이 존재합니다. 그런데  $\gamma_\varepsilon$ 의 길이는 둘레  $2\pi\varepsilon$ 입니다. 따라서  $ML$  보조정리에 의하면

$$\left| \oint_{\gamma_\varepsilon} \frac{f(z) - f(a)}{z - a} \right| \leq 2\pi\varepsilon \cdot M \rightarrow 0$$

원하는 대로입니다. □

## §31.6 정칙 함수는 해석적입니다

**이 절의 대표적인 예:** 형식적 급수  $\sum_k c_k x^k$ 를 상상해 보십시오!

이전 문제의 설정에서, 우리는 원  $\gamma: [0, 2\pi] \rightarrow \mathbb{C}$ 와 원판  $D$ 를 포함하는 정칙 함수  $f: U \rightarrow \mathbb{C}$ 를 가지고 있습니다. 다음과 같이 쓸 수 있습니다

$$\begin{aligned} f(a) &= \frac{1}{2\pi i} \oint_{\gamma} \frac{f(z)}{z - a} dz \\ &= \frac{1}{2\pi i} \oint_{\gamma} \frac{f(z)/z}{1 - \frac{a}{z}} dz \\ &= \frac{1}{2\pi i} \oint_{\gamma} f(z)/z \cdot \sum_{k \geq 0} \left(\frac{a}{z}\right)^k dz \end{aligned}$$

(이른바 바이어슈트라스  $M$ -판정법을 사용하여) 합산 순서를 바꿀 수 있음을 증명할 수 있습니다:

$$\begin{aligned} f(a) &= \frac{1}{2\pi i} \sum_{k \geq 0} \oint_{\gamma} \frac{f(z)}{z} \cdot \left(\frac{a}{z}\right)^k dz \\ &= \frac{1}{2\pi i} \sum_{k \geq 0} \oint_{\gamma} a^k \cdot \frac{f(z)}{z^{k+1}} dz \\ &= \sum_{k \geq 0} \left( \frac{1}{2\pi i} \oint_{\gamma} \frac{f(z)}{z^{k+1}} dz \right) a^k. \end{aligned}$$

$c_k = \frac{1}{2\pi i} \oint_{\gamma} \frac{f(z)}{z^{k+1}} dz$ 라고 하고, 이것이  $a$ 와 무관함을 유의하면, 이것은

$$f(a) = \sum_{k \geq 0} c_k a^k$$

그리고 이것이 바로 그 기적입니다: 정칙 함수는 **테일러 급수**로 주어진다는 것입니다! 이는 복소해석학에서 가장 중요한 결과 중 하나입니다. 더욱이, 도함수를  $k$ 번 취할 수 있다고 믿을 의향이 있다면, 다음을 얻습니다

$$c_k = \frac{f^{(k)}(0)}{k!}$$

그리고 이는  $f^{(k)}(0) = k! \cdot c_k$ 를 우리에게 줍니다.

당연히 이 작업은 (원점을 중심으로 하는 원뿐만 아니라) 임의의 원에 대해서도 할 수 있습니다. 그러면 임의의 중심  $p$ 에 대해 아래에서 전체 결과를 서술하겠습니다.

### 정리 31.6.1 (코시의 미분 공식)

$f: U \rightarrow \mathbb{C}$ 가 정칙 함수이고,  $D$ 는 원  $\gamma$ 로 둘러싸인, 점  $p$ 를 중심으로 하는 원판이라고 합시다.  $D$ 가  $U$  안에 포함되어 있다고 가정합니다. 그러면  $f$ 는  $D$  전체에서 테일러 급수로 주어집니다

$$f(z) = c_0 + c_1(z-p) + c_2(z-p)^2 + \dots$$

여기서

$$c_k = \frac{f^{(k)}(p)}{k!} = \frac{1}{2\pi i} \oint_{\gamma} \frac{f(w)}{(w-p)^{k+1}} dw$$

특히,

$$f^{(k)}(p) = k!c_k = \frac{k!}{2\pi i} \oint_{\gamma} \frac{f(w)}{(w-p)^{k+1}} dw.$$

가장 중요하게는,

**임의의 원판 위에서, 정칙 함수는 정확히 테일러 급수로 주어집니다.**

이는 이 장의 시작 부분에서 서술했던 결과, 즉 함수가 한 번 복소 미분 가능하다는 것은 무한히 미분 가능할 뿐만 아니라 실제로 그 테일러 급수와 같다는 것을 의미한다는 결과를 확립합니다.

**비고 31.6.2** — 이것을 가정할 의향이 있다면, 코시-구르사 정리가 왜 성립해야 하는지 알 수 있습니다: 다음을 가정하면

$$f(z) = c_0 + c_1 z + c_2 z^2 + \dots$$

그러면,  $\gamma$ 를 단위원이라 할 때,

$$\begin{aligned} \oint_{\gamma} f(z) dz &= \oint_{\gamma} c_0 + c_1 z + c_2 z^2 + \dots dz \\ &= \left( \oint_{\gamma} c_0 dz \right) + \left( \oint_{\gamma} c_1 z dz \right) + \left( \oint_{\gamma} c_2 z^2 dz \right) + \dots \end{aligned}$$

각  $\oint_{\gamma} z^m dz = 0$ 임을 이미 증명했으므로, 그 합 역시 0이어야 합니다.

물론 이 논증은 완전히 엄밀하지는 않은데, 적분과 무한합을 정당화 없이 교환하고 있기 때문입니다.

**비고 31.6.3** —  $\frac{f(w)}{(w-p)^{k+1}}$  항이 어디서 나오는지 **비고 32.3.5**에서 확인할 수 있습니다. 이는 매우 직관적이어서, 설령 잊어버리더라도 스스로 유도해 낼 수 있습니다!

이 결과의 작은 미묘한 점을 하나 강조해야 할 것 같습니다.  $p$ 를 중심으로 하는 테일러 급수는,  $p$ 를 중심으로 하며 정의역  $U$  안에 완전히 포함되는 원판에서만 유효합니다.  $U = \mathbb{C}$ 인 경우에는 원하는 어떤 점이든 포함할 만큼 원판을 크게 만들 수 있으므로 문제가 되지 않습니다. 하지만 예컨대  $U$ 가 정사각형인 경우에는 좀 더 미묘한데, 정사각형을 벗어나지 않으면서 어떤 점을 중심으로 한 원판으로 정사각형 전체를 덮을 수는 없기 때문입니다. 그러나  $U$ 가 열린집합이므로, 적어도 테일러 급수가 성립하는 열린 근방을 어떻게든 찾을 수는 있습니다 – 이는 실수의 경우와는 극명하게 대조됩니다. 실제로 문제들에서 보게 되겠지만, 테일러 급수의 존재는 놀라울 만큼 강력합니다.

## §31.7 선택: 정칙 함수가 해석적임을 증명하기

위의 코시 미분 공식에서  $\frac{f(w)}{(w-p)^{k+1}}$  항이 어디에서 비롯되는지 이해하려면 다음 장을 먼저 읽는 것을 권장합니다.

증명의 각 단계는 다소 길기는 해도 상당히 직관적입니다. 개요는 다음과 같습니다.

- 함수  $f$ 가 해석적이라고 가정합니다. (그렇습니다, 이것은 순환 논증이 아닙니다!)
- 코시 미분 공식을 사용하여 멱급수를 적어 봅니다.<sup>3</sup>

$$c_0 + c_1 z + c_2 z^2 + \cdots$$

- 코시-구르사 정리를 이용해 이 멱급수가  $f$ 와 일치함을 증명합니다.
- “ $f$ 가 해석적이다”라는 진술은 문자 그대로 “모든  $k \geq 0$ 에 대해,  $f^{(k)}$ 가 미분 가능하다”는 것을 의미함에 유의하십시오. 따라서  $f^{(k)}$ 에 대한 멱급수를 적고, 그것이 미분 가능함을 보입니다. (이는 실수의 경우에 대해 **명제 29.4.5**에서 이미 수행한 바 있습니다.)

### §31.7.i 코시-구르사 정리의 증명

$f$ 가 정칙, 즉 미분 가능하다고 가정합니다. 우리는  $\oint_{\gamma} f dz = 0$ 임을 증명하고자 합니다.

이 문제를 어떻게 공략할 수 있을까요? 결론을 살펴보면,  $\oint_{\gamma} f dz \neq 0$ 인 어떤 함수를 들여다보고 싶어질 수 있습니다.

우리는 이전 장에서 이미 예시를 얻었습니다:  $f(z) = \frac{1}{z}$ 입니다.

**질문 31.7.1.** 가정 중 어느 부분이 성립하지 않습니까?

어쨌든, 문제는  $f$ 가 0에서 특이점을 가지기 때문이라는 것을 알 수 있습니다 (아직 특이점이 무엇인지 formal하게 정의하지는 않았지만 말입니다). 그래서 우리는 대우 명제를 증명하고자 합니다:

<sup>3</sup> $0 \in U$ 라고 가정합니다.

**정리 31.7.2**

$\oint_{\gamma} f dz \neq 0$ 이라고 가정합니다. 그러면  $\gamma$  내부 어딘가에서  $f$ 에 이상한 일이 일어납니다.

(하지만 임의의 루프에 대해서는 조금 더 어려워집니다. “ $\gamma$  내부”란 무엇을 의미합니까?) 이렇게 표현하면, 그다지 어렵지 않습니다. 계속 읽기 전에  $f(z) = \frac{1}{z}$ 를 조금 살펴보고 증명이 어떻게 이어지는지 스스로 알아내 보고 싶을 수도 있습니다.

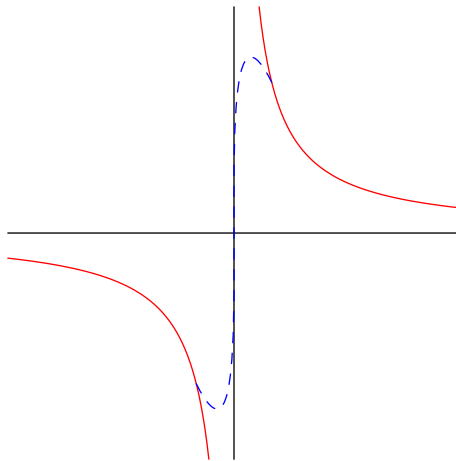
간단히 하기 위해, 저는  $\gamma$ 가 직사각형인 경우에 대해 명제를 증명하고, 예를 들어  $\gamma$ 가 원인 경우는 독자에게 남겨두겠습니다. 완전히 일반적인  $\gamma$ 의 경우는 나중에 다루겠습니다.

이미 알아차렸을 수도 있듯이,  $f(z) = \frac{1}{z-w}$ 에 대해서는 “이분 탐색”을 통해 특이점  $w$ 의 위치를 찾아볼 수 있습니다:  $\oint_{\gamma} f dz$ 를 계산해서, 그것이  $2\pi i$ 라면  $w$ 가  $\gamma$  내부에 있다는 것을 알 수 있습니다. 우리는 바로 그것을 할 것입니다.

무엇을 탐색해야 할까요? 살펴봅시다:

**연습문제 31.7.3.**  $\oint_{\gamma} f dz \neq 0$ 이라고 가정하겠습니다.  $\frac{1}{z}$ 에서  $z = 0$ 인 점처럼,  $f$ 가 무한대로 발산하는 점이 반드시 존재해야 합니까?

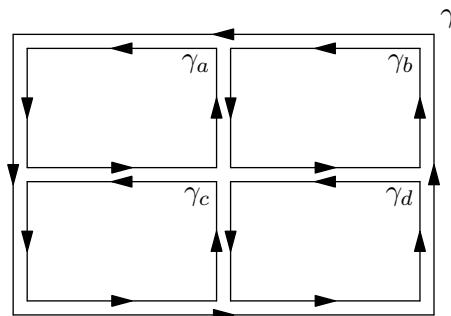
답: 아쉽게도 그렇지 않습니다. 위의 함수  $f$ 를 가져와서 특이점을 “매끄럽게 만들” 수 있습니다.



(실수부만 나타냈습니다. 허수부는 상상하시면 됩니다.)

그렇다면 우리가 기대할 수 있는 최선은,  $f$ 가 정칙(복소 미분 가능)이 아닌 점을 찾는 것입니다.

다음과 같이 4개의 경로  $\gamma_a, \gamma_b, \gamma_c, \gamma_d$ 를 구성하십시오. 여백은 오직 설명을 위한 것이며, 실제로는 변들이 서로 정확히 겹칩니다.



안쪽 변들이 모두 상쇄되므로

$$\oint_{\gamma} f dz = \oint_{\gamma_a} f dz + \oint_{\gamma_b} f dz + \oint_{\gamma_c} f dz + \oint_{\gamma_d} f dz.$$

이는 어떤  $i \in \{a, b, c, d\}$ 에 대해  $\oint_{\gamma_i} f dz \neq 0$ 임을 의미합니다. (아이디어: 특이점의 위치를 더 정확하게 찾았으며, 이제 그것이  $\gamma_i$  안에 있다는 것을 알게 되었습니다. 물론 특이점이 여러 개일 가능성도 있습니다.)

또한 어떤  $i$ 에 대해  $|\oint_{\gamma_i} f dz| \geq \frac{1}{4} \cdot |\oint_{\gamma} f dz|$ 가 성립합니다. 단순히  $\neq 0$ 이라고 말하는 대신 크기를 세심하게 추적해야 하는 이유는 나중에 분명해질 것입니다.

그렇게 계속하면 감소하는 사각형 수열  $\{\gamma_j\}$ 를 얻게 됩니다. 변의 길이가 매번 절반이 되므로, 사각형들은 하나의 점  $p$ 로 수렴합니다.

사각형의 둘레는 어떻게 감소할까요? 아마도 다음과 같을 것입니다.

| $j$ | $\gamma_j$ 의 둘레 | $ \oint_{\gamma_j} f dz $ |
|-----|-----------------|---------------------------|
| 0   | 1               | 1                         |
| 1   | $\frac{1}{2}$   | $\geq \frac{1}{4}$        |
| 2   | $\frac{1}{4}$   | $\geq \frac{1}{16}$       |
| 3   | $\frac{1}{8}$   | $\geq \frac{1}{64}$       |

$|\oint_{\gamma_j} f dz|$ 는 둘레에 비해 상당히 빠르게 감소합니다 — 예상대로,  $f$ 가  $p$ 에서 발산하기를 기대할 수는 없지만, 이는  $f$ 가 정칙이 아님을 보이기에 충분합니다.

모순을 가정하기 위해, 그렇지 않다고 가정하겠습니다. 그러면 정의에 의해

$$\lim_{h \rightarrow 0} \frac{f(p+h) - f(p)}{h} = f'(p)$$

여기서  $p$ 는 위에서 정의한 대로 사각형  $\{\gamma_j\}$ 가 수렴하는 점이며,  $f'(p) \in \mathbb{C}$ 는 도함수입니다. 다시 말해, 0에 충분히 가까운  $h \in \mathbb{C}$ 에 대해,

$$f(p+h) = f(p) + f'(p) \cdot h + \varepsilon(h) \cdot h \text{에 대해 } \varepsilon(h) \in o(1).$$

이것이 왜 문제가 될까요?  $f(p)$ 와  $f'(p) \cdot h$ 는 둘 다 다항식이므로,

$$\oint_{\gamma_j} f(p) + f'(p) \cdot (z-p) dz = 0,$$

이는 다음을 의미합니다

$$\oint_{\gamma_j} f(z) dz = \oint_{\gamma_j} \varepsilon(h) \cdot (z-p) dz.$$

좌변은  $4^{-j}$ 로 감소한다는 것을 알고 있지만, 우변의 적분은 길이가  $2^{-j}$ 로 감소하는 곡선 위에서의 적분입니다.

**연습문제 31.7.4.** 증명을 마무리하십시오. ( $ML$  추정 보조정리를 사용하십시오.)

마지막으로, 내부가 존재하지 않을 수도 있는<sup>4</sup> 임의의 곡선에 대해서는 어떻게 해야 할까요?

우리는 사각형의 변을 따라  $f$ 를 적분함으로써 원시함수  $F: \Omega \rightarrow \mathbb{C}$ 를 구성하고,  $F' = f$ 임을 증명하여, "미적분학의 기본정리"를 얻습니다. 즉,

$$\oint_{\alpha} f(z) dz = F(\alpha(b)) - F(\alpha(a))$$

여기서  $\alpha: [a, b] \rightarrow \mathbb{C}$ 는 어떤 경로입니다.  $\alpha = \gamma$ 인 경우를 생각하면, 고리  $\gamma$ 의 시작점과 끝점이 같으므로 당연히 적분 값은 0이 될 것입니다.

<sup>4</sup>공간 채움 곡선이 그 예입니다.

### §31.7.ii 나머지 부분

다음 단계로, 우리는 거듭제곱 급수가  $f$ 와 일치함을 보여야 합니다. 즉,

$$f(z) = \frac{1}{2\pi i} \oint_{\gamma} \frac{f(t)}{t} dt + \frac{1}{2\pi i} \oint_{\gamma} \frac{f(t)}{t^2} dt \cdot z + \frac{1}{2\pi i} \oint_{\gamma} \frac{f(t)}{t^3} dt \cdot z^2 + \dots$$

여기서는  $\gamma$ 가 단위원이고, 거듭제곱 급수의 중심이 0이며,  $t$ 가 단위원판 내부에 있다고 가정합니다.

**연습문제 31.7.5.** 증명하십시오. (이 상황에서 무한합과 적분의 순서를 바꿀 수 있다는 사실<sup>a</sup>, 등비급수의 합을 구하는 방법, 그리고 코시 적분 공식만 알면 됩니다)

<sup>a</sup>극한과 적분의 순서를 바꿀 수 없는 끔찍한 사례들에 대해서는 [예제 38.1.4](#)를 참고하십시오.

**비고 31.7.6** — 잠깐, 코시-구르사 정리는 어디에서 쓰였을까요? 잊으셨다면, 이는 코시 적분 공식의 증명에서 사용됩니다.

$f$ 가 거듭제곱 급수임을 증명한 후에는, [명제 29.4.5](#)(복소 정칙 함수의 경우에 맞게 적절히 변형하여) 사용하면 결과가 따라옵니다.

## §31.8 생각해 볼 만한 조금 더 어려운 문제

이것들은 올림피아드 문제는 아니지만, 특히 훌륭하다고 생각합니다! 다음 복소해석학 장에서 더 멋진 응용을 보게 될 것입니다.

처음 몇 개의 결과가 가장 중요합니다.



**문제 31A\*** (리우빌 정리).  $f: \mathbb{C} \rightarrow \mathbb{C}$ 를 정함수라 하겠습니다. 모든 복소수  $z$ 에 대해  $|f(z)| < 1000$ 이라 가정하겠습니다.  $f$ 가 상수 함수임을 증명하십시오.

**문제 31B\*** (영점은 고립되어 있습니다). 복소평면의 열린집합  $U$  안의 **고립 집합**이란,  $S$  안의 각 점 주위에  $S$ 의 다른 어떤 점과도 교차하지 않는 열린 근방을 그릴 수 있는 점들의 집합  $S$ 를 말합니다.

영이 아닌 정칙 함수  $f: U \rightarrow \mathbb{C}$ 의 영점 집합은,  $f$ 가 항등적으로 영이 되는  $U$ 의 공집합이 아닌 열린 부분집합이 존재하지 않는 한, 고립 집합임을 보이십시오.



**문제 31C\*** (항등 정리).  $f, g: U \rightarrow \mathbb{C}$ 가 정칙이고,  $U$ 가 연결되어 있다고 가정합니다.  $f$ 와  $g$ 가 어떤 열린 근방에서 일치하면  $f = g$ 임을 증명하십시오.

**문제 31D<sup>†</sup>** (최댓값은 경계에서 발생합니다).  $f: U \rightarrow \mathbb{C}$ 가 정칙이고,  $Y \subseteq U$ 가 콤팩트이며,  $\partial Y$ 가  $Y$ 의 경계<sup>5</sup>라고 합시다. 다음을 보이십시오.

$$\max_{z \in Y} |f(z)| = \max_{z \in \partial Y} |f(z)|.$$

다시 말해,  $|f|$ 의 최댓값은 경계에서 발생합니다. (그러한 최댓값은 콤팩트성에 의해 존재합니다.)

**문제 31E** (Harvard 자격시험).  $f: \mathbb{C} \rightarrow \mathbb{C}$ 가 상수가 아닌 정함수(entire function)라고 합시다.  $f^{\text{img}}(\mathbb{C})$ 가  $\mathbb{C}$ 에서 조밀함을 증명하십시오. (사실 훨씬 더 강한 결과가 성립합니다: 소피카르 정리(Little Picard's theorem)는 상수가 아닌 정함수의 상이 많아야 한 점을 제외한 모든 점을 포함한다고 말합니다.)

<sup>5</sup>경계  $\partial Y$ 는  $p$ 의 어떤 열린 근방도  $Y$ 에 포함되지 않는 점  $p$ 들의 집합입니다.  $Y$ 가 콤팩트이면 이 역시 콤팩트 집합입니다.

**문제 31F** (제거 가능한 특이점 정리).  $U$ 가 열린집합이고,  $p \in U$ 이며,  $f: U \setminus \{p\} \rightarrow \mathbb{C}$ 가 정칙이라 하겠습니다.  $f$ 가 유계라고 가정하십시오.  $\lim_{z \rightarrow p} f(z)$ 가 존재하며, 확장된  $f: U \rightarrow \mathbb{C}$ 가  $p$ 에서 정칙임을 보이십시오.



# 32 유리형 함수

## §32.1 세상에서 두 번째로 멋진 함수들

정칙 함수가 다항식과 같다면, 유리형 함수는 유리 함수와 같습니다. 기본적으로, 유리형 함수는  $\frac{A(z)}{B(z)}$  형태의 함수이며, 여기서  $A, B: U \rightarrow \mathbb{C}$ 는 정칙이고  $B$ 는 영이 아닙니다. 유리형 함수의 가장 중요한 예시는  $\frac{1}{z}$ 입니다.

우리는 유리형 함수가 "거의 정칙인" 함수처럼 작동함을 볼 것입니다. 구체적으로, 유리형 함수  $A/B$ 는  $B$ 의 영점(극이라 불림)을 제외한 모든 점에서 정칙일 것입니다. 항등 정리에 의해,  $B$ 의 영점은 그리 많을 수 없습니다! 따라서 유리형 함수는 "거의 정칙"인 것으로 생각할 수 있습니다(원점을 제외한 모든 곳에서 정칙인  $\frac{1}{z}$ 처럼 말입니다). 우리는 다음을 보았습니다

$$\frac{1}{2\pi i} \oint_{\gamma} \frac{1}{z} dz = 1$$

단위원인  $\gamma(t) = e^{it}$ 에 대해서 말입니다. 우리는 경로에 대한 결과를 이러한 상황으로 확장할 것입니다.

알고 보니, 정칙인 경우처럼 단순히  $\oint_{\gamma} f(z) dz = 0$ 을 얻는 대신, 경로 적분은 실제로 고리  $\gamma$  내부의 극의 개수를 세는 데 사용될 것입니다. 터무니없다는 것, 저도 압니다.

## §32.2 유리형 함수

**이 절의 대표적인 예:**  $\frac{1}{z}$ ,  $z = 0$ 에서 위수 1의 극과 유수 1을 가짐.

$U$ 를 다시  $\mathbb{C}$ 의 열린 부분집합이라고 하겠습니다.

**정의 32.2.1.** 함수  $f: U \rightarrow \mathbb{C}$ 가 **유리형**이라는 것은, 정칙 함수  $A, B: U \rightarrow \mathbb{C}$ 가 존재하여  $B$ 가 어떤 열린 근방에서도 항등적으로 영이 아니고,  $B(z) \neq 0$ 일 때마다  $f(z) = A(z)/B(z)$ 가 성립함을 의미합니다.

이 함수  $f$ 가 어떻게 작동하는지 살펴보겠습니다.  $z \in U$ 가  $B(z) \neq 0$ 을 만족하면, 어떤 작은 열린 근방에서 함수  $B$ 는 전혀 영이 아니며, 따라서  $A/B$ 는 실제로 정칙입니다. 따라서  $f$ 는  $z$ 에서 정칙입니다. (구체적인 예시:  $\frac{1}{z}$ 는 0을 포함하지 않는 모든 원판에서 정칙입니다.)

반면,  $p \in U$ 가  $B(p) = 0$ 을 만족한다고 합시다. 일반성을 잃지 않고, 표기를 간단히 하기 위해  $p = 0$ 이라 하겠습니다.  $p = 0$ 에서의 테일러 급수를 이용하면 다음과 같이 놓을 수 있습니다

$$B(z) = c_k z^k + c_{k+1} z^{k+1} + \dots$$

$c_k \neq 0$ 인 경우입니다( $B$ 가 항등적으로 영이 아니므로 어떤 계수는 확실히 0이 아닙니다!). 그러면 다음과 같이 쓸 수 있습니다.

$$\frac{1}{B(z)} = \frac{1}{z^k} \cdot \frac{1}{c_k + c_{k+1}z + \dots}.$$

하지만 오른쪽의 분수는 이 열린 근방에서 정칙 함수입니다! 그러므로 일어난 일이라고는 여분의  $z^{-k}$ 이 붙어 다니게 된 것뿐입니다.

이것은 유리형 함수를 바라보는 동등한 방법을 제공해 줍니다.

**정의 32.2.2.** 평소와 같이  $f: U \rightarrow \mathbb{C}$ 라 하겠습니다. **유리형** 함수란 고립점들의 집합  $S$ 를 제외하고  $U$  위에서 정칙인 함수를 말합니다(즉 함수  $U \setminus S \rightarrow \mathbb{C}$ 로서 정칙임을 의미합니다).

$f$ 의 **극점**이라 불리는 각  $p \in S$ 에 대해, 함수  $f$ 는 추가로 **로랑 급수**를 가져야 하며, 이는 다음을 의미합니다.

$$f(z) = \frac{c_{-m}}{(z-p)^m} + \frac{c_{-m+1}}{(z-p)^{m-1}} + \cdots + \frac{c_{-1}}{z-p} + c_0 + c_1(z-p) + \cdots$$

$z = p$ 를 제외하고  $p$ 의 어떤 열린 근방에 속하는 모든  $z$ 에 대해서입니다. 여기서  $m$ 은 양의 정수이며,  $c_{-m} \neq 0$ 입니다.

끝부분이 반드시 종결되어야 함에 유의하십시오. "고립된 집합"이라는 것은,  $S$ 에 속한 각 극점 주위에 열린 근방을 그릴 수 있되, 어떤 두 열린 근방도 서로 교차하지 않도록 할 수 있다는 뜻입니다.

### 예제 32.2.3 (유리형 함수의 예)

함수

$$\frac{z+1}{\sin z}.$$

를 생각해 보겠습니다. 이 함수는  $\sin z$ 의 영점을 제외한 모든 곳에서 정칙이므로 유리형입니다. 이러한 각 점에서 로랑 급수를 놓을 수 있습니다. 예를 들어  $z = 0$ 에서는 다음과 같습니다.

$$\begin{aligned} \frac{z+1}{\sin z} &= (z+1) \cdot \frac{1}{z - \frac{z^3}{3!} + \frac{z^5}{5!} - \cdots} \\ &= \frac{1}{z} \cdot \frac{z+1}{1 - \left( \frac{z^2}{3!} - \frac{z^4}{5!} + \frac{z^6}{7!} - \cdots \right)} \\ &= \frac{1}{z} \cdot (z+1) \sum_{k \geq 0} \left( \frac{z^2}{3!} - \frac{z^4}{5!} + \frac{z^6}{7!} - \cdots \right)^k. \end{aligned}$$

이 끔찍한 합을 전개해 보면 (여기서 직접 하지는 않겠습니다),  $\frac{1}{z}$  곱하기 완전히 정상적인 테일러 급수, 즉 로랑 급수를 얻게 됩니다.

**표기의 남용 32.2.4.** 우리는 종종 " $z \mapsto \frac{1}{z}$ 에 의한 함수  $f: \mathbb{C} \rightarrow \mathbb{C}$ 를 생각해 보자"와 같은 표현을 사용하곤 합니다. 물론 이것은 완전히 정확한 것은 아니데,  $f$ 가  $z = 0$ 에서 값을 갖지 않기 때문입니다. 만약 완전히 엄밀하게 하고자 한다면 그냥  $f(0) = 2015$  정도로 정해 놓고 넘어가면 되겠지만, 실질적으로는 그냥 " $z = 0$ 에서 정의되지 않음"이라고 생각하도록 하겠습니다.

그렇다면 왜 그냥  $g: \mathbb{C} \setminus \{0\} \rightarrow \mathbb{C}$ 라고 쓰지 않을까요? 이렇게 해야 하는 이유는,  $z = 0$ 에서 값이 배정되어 있지 않더라도  $f$ 가  $\mathbb{C}$  위에서 정칙이 "되고자" 한다는 것을 여전히 기억해 두는 것이 중요하기 때문입니다. 함수  $\mathbb{C} \setminus \{0\} \rightarrow \mathbb{C}$ 로서 함수  $\frac{1}{z}$ 는 실제로 정칙입니다.

**비고 32.2.5** — 저는 임의의 함수  $A(z)/B(z)$ 가 극점을 통한 이러한 특성화를 가짐을 보였습니다만, 중요한 결과는 그 역 또한 성립한다는 것입니다: 만약 어떤 고립된 집합  $S$ 에 대해  $f: U \setminus S \rightarrow \mathbb{C}$ 가 정칙이고, 나아가  $f$ 가  $S$ 의 각 점에서 로랑 급수를 갖는다면,  $f$ 는 정칙 함수들의 유리 몫으로 쓸 수 있습니다. 여기서 이를 증명하지는 않겠지만, 알아 두면 좋습니다.

**정의 32.2.6.** 유리형 함수  $f$ 의 극점  $p$ 를 생각하고, 로랑 급수는 다음과 같다고 하겠습니다.

$$f(z) = \frac{c_{-m}}{(z-p)^m} + \frac{c_{-m+1}}{(z-p)^{m-1}} + \cdots + \frac{c_{-1}}{z-p} + c_0 + c_1(z-p) + \cdots$$

정수  $m$ 을 극의 **위수**(order)라고 부릅니다. 위수가 1인 극을 **단순극**(simple pole)이라고 부릅니다.

또한 계수  $c_{-1}$ 에도 이름을 붙이는데, 이를  $p$ 에서의  $f$ 의 **유수**(residue)라고 하며  $\text{Res}(f; p)$ 로 씁니다.

극의 위수는 그 극이 얼마나 "나쁜지"를 말해줍니다. 극의 위수는 **영점의 중복도**와 "반대" 개념입니다. 만약  $f$ 가 영점 근처에 극을 가진다면,  $z = 0$  근처에서의 로랑 급수는 다음과 같은 모양일 수 있습니다

$$f(z) = \frac{1}{z^5} + \frac{8}{z^3} - \frac{2}{z^2} + \frac{4}{z} + 9 - 3z + 8z^2 + \dots$$

따라서  $f$ 는 위수 5의 극을 가집니다. 유사하게,  $g$ 가  $z = 0$ 에서 영점을 가진다면, 다음과 같은 모습일 수 있습니다

$$g(z) = 3z^3 + 2z^4 + 9z^5 + \dots$$

따라서  $g$ 는 중복도 3의 영점을 가집니다. 이러한 위수들은 가법적입니다:  $f(z)g(z)$ 는 여전히 위수  $5 - 3 = 2$ 의 극을 가지지만,  $f(z)g(z)^2$ 는 이제 완전히 메워졌으며, 사실 이제 **단순영점**(simple zero)을 가집니다 (즉, 차수 1의 영점입니다).

**연습문제 32.2.7.** 위에서 설명한 대로 위수가 가법적임을 스스로 확인해 보십시오. (테일러/로랑 급수를 곱하고 있다는 것을 이해하면 이는 자명합니다.)

비유적으로, 극은 "음의 영점"으로 생각할 수 있습니다.

이제 더 많은 예를 들 수 있습니다.

### 예제 32.2.8 (유리형 함수의 예)

- (a) 임의의 정칙 함수는 극을 전혀 가지지 않는 유리형 함수입니다. 당연한 얘기입니다, 그렇습니다.
- (b)  $z \neq 0$ 에 대해  $z \mapsto 100z^{-1}$ 로 정의되고 영점에서는 정의되지 않는 함수  $\mathbb{C} \rightarrow \mathbb{C}$ 는 유리형 함수입니다. 이 함수의 유일한 극은 영점에 있으며, 위수는 1이고 유수는 100입니다.
- (c) 함수  $z \mapsto z^{-3} + z^2 + z^9$ 로 정의되는  $\mathbb{C} \rightarrow \mathbb{C}$  역시 유리형 함수입니다. 이 함수의 유일한 극은 영점에 있으며, 위수는 3이고 유수는 0입니다.
- (d)  $z \mapsto \frac{e^z}{z^2}$ 로 정의된 함수  $\mathbb{C} \rightarrow \mathbb{C}$ 는 유리형 함수이며,  $z = 0$ 에서의 로랑 급수는 다음과 같이 주어집니다.

$$\frac{e^z}{z^2} = \frac{1}{z^2} + \frac{1}{z} + \frac{1}{2} + \frac{z}{6} + \frac{z^2}{24} + \frac{z^3}{120} + \dots$$

따라서 극점  $z = 0$ 은 위수 2이고 유수는 1입니다.

### 예제 32.2.9 (유리 유리형 함수)

다음과 같이 주어진 함수  $\mathbb{C} \rightarrow \mathbb{C}$ 를 생각해 봅시다.

$$\begin{aligned} z \mapsto \frac{z^4 + 1}{z^2 - 1} &= z^2 + 1 + \frac{2}{(z-1)(z+1)} \\ &= z^2 + 1 + \frac{1}{z-1} \cdot \frac{1}{1 + \frac{z-1}{2}} \\ &= \frac{1}{z-1} + \frac{3}{2} + \frac{9}{4}(z-1) + \frac{7}{8}(z-1)^2 - \dots \end{aligned}$$

이 함수는  $z = 1$ 에서 위수 1의 극점을 가지며 유수는 1입니다. (또한  $z = -1$ 에서도 위수 1의 극점을 가지는데, 유수를 직접 계산해 보시기 바랍니다.)

### 예제 32.2.10 (극점이 무한히 많은 함수)

$$z \mapsto \frac{1}{\sin(z)}$$

로 정의된 함수  $\mathbb{C} \rightarrow \mathbb{C}$ 는 극점이 무한히 많은데, 바로  $z = \pi k$  ( $k$ 는 정수)로 주어지는 수들입니다. 우선  $z = 0$ 에서의 로랑 급수만 계산해 봅시다.

$$\begin{aligned} \frac{1}{\sin(z)} &= \frac{1}{\frac{z}{1!} - \frac{z^3}{3!} + \frac{z^5}{5!} - \dots} \\ &= \frac{1}{z} \cdot \frac{1}{1 - \left(\frac{z^2}{3!} - \frac{z^4}{5!} + \dots\right)} \\ &= \frac{1}{z} \sum_{k \geq 0} \left( \frac{z^2}{3!} - \frac{z^4}{5!} + \dots \right)^k. \end{aligned}$$

이는 로랑 급수이지만, 계수가 무엇인지는 전혀 알 수 없습니다. 그래도 유수는 알 수 있는데, 이 거대한 급수의 상수항이 1이므로 유수는 1입니다. 또한 이 극점의 위수는 1입니다.

### 예제 32.2.11 (유리형 함수가 아닌 함수)

다음 함수를 생각해 봅시다.

$$z \mapsto \frac{1}{\sin(1/z)}.$$

이 함수는 다음 위에서 정칙 함수입니다.

$$U = \mathbb{C} \setminus \{0\} \setminus S$$

여기서  $S = \{\frac{1}{\pi k} \mid k \in \mathbb{Z} \setminus \{0\}\}$ 로 정의합니다.  $z \mapsto \frac{1}{\sin(z)}$ 와 마찬가지로, 집합  $S$ 의 각 점은 위수 1의 극점을 가집니다.

그러나  $z = 0$ 에서는 이 함수의 로랑 급수가 존재하지 않습니다 — 만약 존재한다면  $z = 0$  주위에 함수가 정의되는 근방이 있어야 하는데, 그런 집합은 존재하지 않습니다. 그러나  $f$ 는  $\mathbb{C} \setminus \{0\}$  위에서는 유리형 함수입니다 — 집합  $S$ 는 고립되어 있지만,  $S \cup \{0\}$ 은 고립되어 있지 않기 때문입니다.

로랑 급수는 존재한다면 (짐작하셨을 수도 있듯이) 유일하며, 정칙 함수에 대한 우리의 결과에 의해 실제로는  $p$ 를 중심으로 하는 임의의 원판(점  $p$ 는 제외)에서 성립합니다.  $\frac{c_{-1}}{z-p} + \cdots + \frac{c_{-m}}{(z-p)^m}$  부분은 **주부**라고 하며, 급수의 나머지  $c_0 + c_1(z-p) + \cdots$ 는 **정칙부**라고 합니다.

### §32.3 회전수와 유수 정리

반시계 방향 원  $\gamma$ 와 그 내부의 점  $p$ 에 대해 우리가 다음을 얻었음을 기억하십시오

$$\oint_{\gamma} (z-p)^m dz = \begin{cases} 0 & m \neq -1 \\ 2\pi i & m = -1 \end{cases}$$

여기서  $m$ 은 정수입니다. 이 결과를 확장하면 실제로 임의의 루프  $\gamma$ 에 대해  $m \neq -1$ 일 때  $\oint_{\gamma} (z-p)^m dz = 0$ 임을 보일 수 있습니다. 그래서 우리는  $m = -1$ 에서의 영이 아닌 값에 특별한 이름을 붙입니다.

**정의 32.3.1.** 점  $p \in \mathbb{C}$ 와 이 점을 지나지 않는 루프  $\gamma$ 에 대해, 다음과 같이 **회전수**를 정의하며  $I(\gamma, p)$ 로 표기합니다

$$I(\gamma, p) = \frac{1}{2\pi i} \oint_{\gamma} \frac{1}{z-p} dz$$

예를 들어 앞선 결과에 의해  $\gamma$ 가 원이라면 다음을 얻을 수 있습니다

$$I(\text{원}, p) = \begin{cases} 1 & \text{원 내부의 } p \\ 0 & \text{원 바깥의 } p. \end{cases}$$

기본군에 대한 장을 읽으셨다면, 이는 단지  $\mathbb{C} \setminus \{p\}$ 에 결부된 기본군에 지나지 않습니다. 특히 회전수는 항상 정수입니다. (본질적으로 이는 복소 로그를 사용하여 함수의 편각이 어떻게 변하는지를 추적합니다. 세부 사항은 더 복잡하므로 여기서는 생략합니다.) 가장 간단한 경우에는 회전수가 0 또는 1입니다.

**정의 32.3.2.**  $\gamma$  내부의 모든 점  $p$ 에 대해  $I(\gamma, p) = 1$ 이면 루프  $\gamma$ 가 **정칙**이라고 합니다(예를 들어  $\gamma$ 가 반시계 방향 원인 경우).

이 모든 요소를 갖추면 코시-구르사 정리의 놀라운 일반화를 얻습니다

#### 정리 32.3.3 (코시의 유수 정리)

$\Omega$ 가 단순 연결일 때  $f: \Omega \rightarrow \mathbb{C}$ 가 유리형이라고 합시다. 그러면 극점을 지나지 않는 임의의 루프  $\gamma$ 에 대해 다음이 성립합니다

$$\frac{1}{2\pi i} \oint_{\gamma} f(z) dz = \sum_{\text{극점 } p} I(\gamma, p) \text{Res}(f; p).$$

특히  $\gamma$ 가 정칙이면 경로 적분은 다음과 같은 형태로 모든 유수의 합이 됩니다

$$\frac{1}{2\pi i} \oint_{\gamma} f(z) dz = \sum_{\substack{\text{극점 } p \\ \gamma \text{ 내부에서}}} \text{Res}(f; p).$$

**질문 32.3.4.**  $\gamma$ 가 반시계 방향 원일 때  $\oint_{\gamma} cz^{-1} dz$ 를 적분하면 이 결과가 여러분이 기대하는 바와 일치하는지 확인하십시오.

여기서부터의 증명은 그다지 인상적이지 않습니다 – “작업”은 이미 회전수에 대한 우리의 진술에서 끝났습니다.

증명. 0이 아닌 회전수를 갖는 극점들을  $p_1, \dots, p_k$ 라 합시다 (다른 극점들은 합에 영향을 주지 않습니다).<sup>1</sup> 그러면  $f$ 를 다음과 같은 형태로 쓸 수 있습니다

$$f(z) = g(z) + \sum_{i=1}^k P_i \left( \frac{1}{z - p_i} \right)$$

여기서  $P_i \left( \frac{1}{z - p_i} \right)$ 는 극점  $p_i$ 의 주요부입니다. (예를 들어,  $f(z) = \frac{z^3 - z + 1}{z(z+1)}$ 이라면  $f(z) = (z-1) + \frac{1}{z} - \frac{1}{1+z}$ 로 쓸 수 있습니다.)

이렇게 하는 이유는 함수  $g$ 가 정칙이 되기 때문입니다 (모든 “나쁜” 부분을 제거했습니다), 따라서

$$\oint_{\gamma} g(z) dz = 0$$

코시-구르사예 의해.

반면,  $P_i(x) = c_1x + c_2x^2 + \dots + c_dx^d$ 이라면

$$\begin{aligned} \oint_{\gamma} P_i \left( \frac{1}{z - p_i} \right) dz &= \oint_{\gamma} c_1 \cdot \left( \frac{1}{z - p_i} \right) dz + \oint_{\gamma} c_2 \cdot \left( \frac{1}{z - p_i} \right)^2 dz + \dots \\ &= c_1 \cdot \mathbf{I}(\gamma, p_i) + 0 + 0 + \dots \\ &= \mathbf{I}(\gamma, p_i) \operatorname{Res}(f; p_i). \end{aligned}$$

이는 결론을 줍니다. □

**비고 32.3.5** (코시 적분 공식 뒤에 있는 직관) — 정리 31.5.1의 설정에서,  $f$ 가 원판  $D$ 에서 유리형이라면, 점  $a$ 에서  $f$ 의 로랑 급수를 계산할 수 있음에 주목하십시오:

$$f(z) = \frac{c_{-m}}{(z-a)^m} + \frac{c_{-m+1}}{(z-a)^{m-1}} + \dots + \frac{c_{-1}}{z-a} + c_0 + c_1(z-a) + \dots$$

유수 정리에 의해,  $f(z)$ 를  $D$ 의 경계를 따라 적분하면 로랑 급수의  $c_{-1}$  계수가 나옵니다:

$$\frac{1}{2\pi i} \oint_{\gamma} f(z) dz = \operatorname{Res}(f; a) = c_{-1}.$$

물론 이는 쓸모가 없습니다 —  $f$ 는  $a$ 에서 정칙이므로  $c_{-1} = 0$ 입니다. 우리는 대신  $c_0 = f(a)$ 를 계산하고자 합니다.

그럼에도 불구하고, 그 요령은 함수  $f$ 를 조작할 수 있다는 것에 있으며, 이를 통해 계산하고자 하는 계수를  $(z-a)^{-1}$ 에 대응하는 계수로 옮길 수 있습니다. 어떻게 그렇게 할까요? 물론  $z-a$ 로 나누면 됩니다!

그러므로,  $\frac{f(z)}{z-a}$ 는 원판  $D$ 에서 유리형이며,  $a$  주위에서의 로랑 급수 전개는 다음과

<sup>1</sup>이러한 극점이 유한 개임을 보이려면: 우리의 모든 경로  $\gamma: [a, b] \rightarrow \mathbb{C}$ 가 실제로는 유계라는 사실을 상기하십시오. 따라서  $\gamma$  전체를 포함하는 어떤 큰 닫힌 원판  $D$ 가 존재합니다. 따라서  $D$  바깥의 극점들은 회전수가 0입니다. 이제 원판  $D$  안에 무한히 많은 극점이 있을 수는 없는데,  $D$ 는 콤팩트이고 극점들의 집합은 닫혀 있으면서 고립된 집합이기 때문입니다!

같습니다

$$\frac{f(z)}{z-a} = \frac{c_{-m}}{(z-a)^{m+1}} + \frac{c_{-m+1}}{(z-a)^m} + \cdots + \frac{c_{-1}}{(z-a)^2} + \frac{c_0}{z-a} + c_1 + c_2(z-a) + \cdots$$

$\frac{f(z)}{z-a}$ 는  $a$ 를 제외하고  $D$  안에 다른 극점이 없으므로, 유수 정리는 즉시 적분  $\frac{1}{2\pi i} \oint_{\gamma} \frac{f(z)}{z-a} dz$ 가  $\text{Res}(\frac{f(z)}{z-a}; a)$ 와 같음을 알려주며, 이는 위의 로랑 급수를 보면  $c_0$ 와 같습니다.

### §32.4 편각 원리

까다로운 응용 하나는 다음과 같습니다. 다항식  $P(x) = (x-a_1)^{e_1}(x-a_2)^{e_2} \cdots (x-a_n)^{e_n}$ 이 주어졌을 때, 다음이 성립함을 알고 있을 수도 있습니다

$$\frac{P'(x)}{P(x)} = \frac{e_1}{x-a_1} + \frac{e_2}{x-a_2} + \cdots + \frac{e_n}{x-a_n}.$$

양  $P'/P$ 는 **로그 도함수**라 불리는데, 이는  $\log P$ 의 도함수이기 때문입니다. 이 요령은  $P$ 의 영점을  $P'/P$ 의 차수 1짜리 극점으로 변환할 수 있게 해줍니다; 게다가 이 극점들의 유수는 근들의 중복도입니다.

유사한 방식으로, 임의의 유리형 함수  $f$ 에 대해서도 비슷한 결과를 얻을 수 있습니다.

#### 명제 32.4.1 (로그 도함수)

$f: U \rightarrow \mathbb{C}$ 를 유리형 함수라 합시다. 그러면 로그 도함수  $f'/f$ 는  $U$ 에서  $\mathbb{C}$ 로 가는 함수로서 유리형입니다; 그 극점들은 오직 다음과 같습니다:

- (i)  $f$ 의 각 영점에서, 그 유수가 중복도인 극점, 그리고
- (ii)  $f$ 의 각 극점에서, 그 유수가 극점 차수의 음수인 극점.

다시 말해, 극점을 거의 음의 중복도를 갖는 영점으로 생각할 수 있습니다. 이러한 정신은 아래에서 예시됩니다.

증명. 로랑 급수를 쓰면 매우 쉽습니다.  $a$ 를  $f$ 의 영점/극점이라 하고, 일반성을 잃지 않고 편의상  $a=0$ 으로 둡시다. 0에서의 로랑 급수를 취하면

$$f(z) = c_k z^k + c_{k+1} z^{k+1} + \cdots$$

가 되는데, 여기서 0이 극점이면  $k < 0$ 이고 0이 영점이면  $k > 0$ 입니다. 도함수를 취하면

$$f'(z) = k c_k z^{k-1} + (k+1) c_{k+1} z^k + \cdots$$

이제  $f'/f$ 를 살펴보면; 약간의 계산을 통해 이는 다음과 같아집니다

$$\frac{f'(z)}{f(z)} = \frac{1}{z} \frac{k c_k + (k+1) c_{k+1} z + \cdots}{c_k + c_{k+1} z + \cdots}.$$

따라서  $z=0$ 에서 유수가  $k$ 인 단순 극점을 얻습니다. □

이 기법을 이용하면 이른바 편각 원리를 사용하여 정칙 폐곡선 내부의 영점과 극점의 개수를 결정할 수 있습니다.<sup>2</sup>

### 정리 32.4.2 (편각 원리)

$\gamma$ 를 정칙 곡선이라 합시다.  $f: U \rightarrow \mathbb{C}$ 가  $\gamma$  내부와  $\gamma$  위에서 유리형이고,  $f$ 의 영점과 극점 중 어느 것도  $\gamma$  위에 놓여 있지 않다고 가정합니다. 그러면

$$\frac{1}{2\pi i} \oint_{\gamma} \frac{f'}{f} dz = \frac{1}{2\pi i} \oint_{f \circ \gamma} \frac{1}{z} dz = Z - P$$

여기서  $Z$ 는  $\gamma$  내부의 영점 개수(중복도를 포함하여 셈)이고  $P$ 는  $\gamma$  내부의 극점 개수(역시 중복도를 포함하여 셈)입니다.

증명. 코시의 유수 정리를 앞선 명제와 함께 적용하면 바로 얻어집니다. 실제로는 회전수를 통해 임의의 곡선  $\gamma$ 로 일반화할 수 있습니다: 적분값은

$$\frac{1}{2\pi i} \oint_{\gamma} \frac{f'}{f} dz = \sum_{\text{영점 } z} \mathbf{I}(\gamma, z) - \sum_{\text{극점 } p} \mathbf{I}(\gamma, p)$$

여기서 합은 중복도를 포함하여 계산됩니다. □

따라서 편각 원리를 이용하면 원하는 임의의 영역 내부의 영점과 극점의 개수를 셀 수 있습니다.

컴퓨터는 이를 이용하여, 값은 계산할 수 있지만 전체적인 거동은 이해하기 어려운 함수에 대한 정보를 얻을 수 있습니다. 정칙 함수  $f$ 가 있고 그 영점이 어디에 있는지 알고 싶다고 합시다. 그러면 그저 다양한 원  $\gamma$ 를 골라 시작하면 됩니다. 기계적인 반올림 오차가 있더라도, 적분값은 참인 정수값에 충분히 가까워서 임의로 주어진 원 안에 영점이 몇 개 있는지 결정할 수 있습니다. 리만 가설(리만 제타 함수의 영점에 관한 가설)에 대한 수치적 증거도 이러한 방식으로 얻을 수 있습니다.

## §32.5 여담: 기하학적으로 바라본 편각 원리

편각 원리를 이해하는 또 다른, 더 기하학적인 방법이 있습니다.

함수  $f$ 가 0을 포함하는 연결된 열린집합  $U$  위에서 정칙이며, 0에서 영점이나 극점을 가질 수도 있다고 가정합니다.  $\gamma: [0, 2\pi] \rightarrow U$ 를  $U$ 에 포함된 곡선으로서, 0이 이 곡선의 상에 속하지 않는 것으로 둡시다.

$a = \gamma(0)$ 을  $\gamma$ 의 시작점으로,  $b = \gamma(2\pi)$ 를  $\gamma$ 의 끝점으로 둡시다.

$z \mapsto \log z$ 가 실제 함수가 아니라는 것은 모두 알고 있습니다 — 0에서의 특이점을 무시하더라도, 이는 분지 절단을 가지고 있습니다 (이는 [장 33](#)에서 형식적으로 다룰 것입니다).

그럼에도 불구하고, 눈을 감고 기호들을 이리저리 옮겨보면 다음을 얻습니다:

$$\begin{aligned} \frac{1}{2\pi i} \oint_{\gamma} \frac{f'(z)}{f(z)} dz &= \frac{1}{2\pi i} \oint_{\gamma} \frac{d}{dz} \log f(z) dz \\ &= \frac{1}{2\pi i} \oint_{\gamma} d(\log f(z)) \\ &= \frac{1}{2\pi i} \cdot (\log f(b) - \log f(a)). \end{aligned}$$

<sup>2</sup>복소수  $z$ 의 편각이 실수축과  $z$ 를 나타내는 벡터가 이루는 각도이기 때문에 이렇게 불리는 것이지, 어떤 논증(argument)을 사용해야 하기 때문은 아닙니다.  $z \in \mathbb{C}$ 를  $\mathbb{R}^2$ 의 한 점으로 해석하면,  $z$ 의 편각은 [예제 44.7.4](#)에서 정의한  $\theta(z)$ 와 같습니다.

놀랍게도, 모든 것이 아주 깔끔하게 소거되는 것처럼 보입니다! 이는 우연이 아닙니다.

이제,  $\gamma$ 가 원이라면  $a = b$ 이므로, 위 공식은 겉보기에 적분값이 0이라고 말하는 것처럼 보입니다? 다행히도, 그렇지 않습니다 —  $\log$ 은 사실 함수가 아니기 때문입니다.

그렇다면, 위 공식은 어떤 의미를 가질까요? 그렇습니다! 엄밀하게 증명하지는 않겠지만, 요점은 다음과 같습니다:

점  $p$ 가  $a$ 에서  $b$ 까지 매끄럽게 이동하고,  $\log f(p)$ 가 그 값을 따라간다고 하면,  $\log f(b) - \log f(a)$ 는  $\log f(p)$  값의 변화량을 나타냅니다.

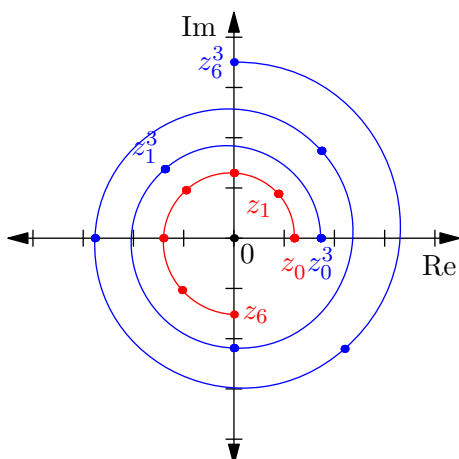
**절 66.2**의 표기법에서, 쥐는  $\gamma$ 를 따라  $a$ 에서  $b$ 까지 이동하고, 첫 번째 로봇은  $f \circ \gamma$ 를 따라  $f(a)$ 에서  $f(b)$ 까지 이동하며, 두 번째 로봇은  $\log f(a)$ 에서  $\log f(b)$ 까지 이동합니다.

잠시 쥐에 대해서는 잊는다면, 다음을 주목하십시오:

$\frac{1}{2\pi i} \oint_{\gamma} \frac{f'(z)}{f(z)} dz$ 의 값은 첫 번째 로봇이 원점을 감는 횟수와 같습니다.

즉,  $I(f \circ \gamma, 0)$ 입니다. (이는  $\oint d \log z = \oint \frac{1}{z} dz$ 가 감김수와 같다는 것을 증명하기 위해 우리가 해온 모든 작업 덕분에 본질적으로 자명하게 알 수 있습니다.)

마지막으로,  $z^3$ 과 같은 간단한 예시들을 살펴보면:



회전수와 영점의 중복도 사이의 관계를 바로 확인할 수 있습니다:

$z$ 가 원점 주위를 원을 그리며 한 번 돈다면,  $z^n$ 은 원점 주위를 원을 그리며  $n$ 번 돕니다.

$z^{-n}$ 도 크게 다르지 않습니다 — 이 역시 원점 주위를 원을 그리며  $n$ 번 돌지만, 방향만 반대입니다.

이 모든 조각을 짜맞추면 편각 원리를 얻습니다 — 로그 도함수를 이용하여 근의 중복도와 극점의 위수를 셀 수 있습니다.

### §32.6 철학: 정칙 함수는 왜 그렇게 좋은 성질을 가지는가?

정칙 함수와 유리형 함수를 다루며 누렸던 모든 즐거움은 복소 미분가능성이 매우 강한 조건이라는 사실로 귀결됩니다. 언뜻 보기에는  $\mathbb{R}^2$ 처럼만 보이는  $\mathbb{C}$ 가 실은 체(field)라는 것은 작은 기적입니다. 게다가  $\mathbb{R}^2$ 는 자명하지 않은 폐곡선을 그릴 수 있다는 좋은 성질을 가지고 있으며(실함수에 대해서도  $\int_a^a f dx = 0$ 이라는 사실은 성립하지만, 이는 그다지 흥미롭지 않습니다!), 이 때문에 이론이 훨씬 더 흥미로워집니다.

시우<sup>3</sup>의 또 다른 직관 하나를 들자면: 사원수 위에서 (좌측) 미분가능한 함수를 얻으려 하면, 결국 선형 함수만 남는다는 것을 발견하게 됩니다.

### §32.7 생각해 볼 만한 조금 더 어려운 문제

**문제 32A** (대수학의 기본 정리).  $f$ 가 차수  $n$ 인 영이 아닌 다항식이면  $n$ 개의 근을 가짐을 증명하십시오.

**문제 32B<sup>†</sup>** (루셰 정리).  $f, g: U \rightarrow \mathbb{C}$ 가 정칙 함수이고,  $U$ 가 단위원판을 포함한다고 하십시오. 단위원 위의 모든  $z$ 에 대해  $|f(z)| > |g(z)|$ 라고 가정하십시오.  $f$ 와  $f + g$ 가 단위원 내부에 엄격하게 놓인 영점의 개수(중복도를 포함하여)가 같음을 증명하십시오.



**문제 32C** (썰기 윤곽).  $n \geq 3$ 인 각 홀수 정수에 대해, 다음 이상적분의 값을 구하십시오

$$\int_0^\infty \frac{1}{1+x^n} dx.$$



**문제 32D** (또 다른 경로). 다음 적분이

$$\int_{-\infty}^\infty \frac{\cos x}{x^2 + 1} dx$$

수렴함을 증명하고 그 값을 구하십시오.



**문제 32E<sup>\*</sup>**.  $f: U \rightarrow \mathbb{C}$ 를 상수가 아닌 정칙 함수라 하십시오.

(a) (열린 사상 정리)  $f^{\text{img}}(U)$ 가  $\mathbb{C}$ 에서 열린집합임을 증명하십시오.<sup>4</sup>

(b) (최대 절댓값 원리)  $|f|$ 가  $U$  위에서 최댓값을 가질 수 없음을 보이십시오. 즉, 임의의  $z \in U$ 에 대해  $|f(z)| < |f(z')|$ 를 만족하는  $z' \in U$ 가 존재함을 보이십시오.

<sup>3</sup>하버드 대학교 교수.

<sup>4</sup>따라서 임의의 열린집합  $V \subseteq U$ 의 상도  $\mathbb{C}$ 에서 열린집합입니다( $f$ 를  $V$ 로 제한한 것에 대해 증명을 반복함으로써).

# 33 정칙 제곱근과 로그

이 장에서는 정칙 제곱근과 로그의 의미를 명확히 하겠습니다. 주요 결과는 정리 33.3.2, 정리 33.4.2, 따름정리 33.5.1, 정리 33.5.2입니다. 원하신다면 이 네 가지 결과만 읽고 그것들이 어떻게 도출되었는지에 대한 논의는 건너뛰셔도 됩니다.

$f: U \rightarrow \mathbb{C}$ 를 정칙 함수라 하겠습니다.  $f$ 의 정칙  $n$ 제곱근이란 모든  $z \in U$ 에 대해  $f(z) = g(z)^n$ 을 만족하는 함수  $g: U \rightarrow \mathbb{C}$ 를 말합니다.  $f$ 의 로그란 모든  $z \in U$ 에 대해  $f(z) = e^{g(z)}$ 를 만족하는 함수  $g: U \rightarrow \mathbb{C}$ 를 말합니다. 우리가 알아내고자 하는 주요 질문은 다음과 같습니다: 이러한 것들은 언제 존재할까요? 특히  $f = \text{id}$ 인 경우는 어떨까요?

## §33.1 동기 부여: 복소수의 제곱근

먼저, 임의의 복소수  $z$ 에 대해  $\sqrt{z}$ 를 정의할 수 있을까요?

처음 마주치는 명백한 문제는, 임의의  $z$ 에 대해  $w^2 = z$ 를 만족하는 수  $w$ 가 두 개 존재한다는 것입니다. 어떻게 하나를 선택할 수 있을까요? 일반적인 제곱근 함수의 경우, 우리는 "양수"라는 개념을 가지고 있었으므로 단순히 양의 근을 취했습니다.

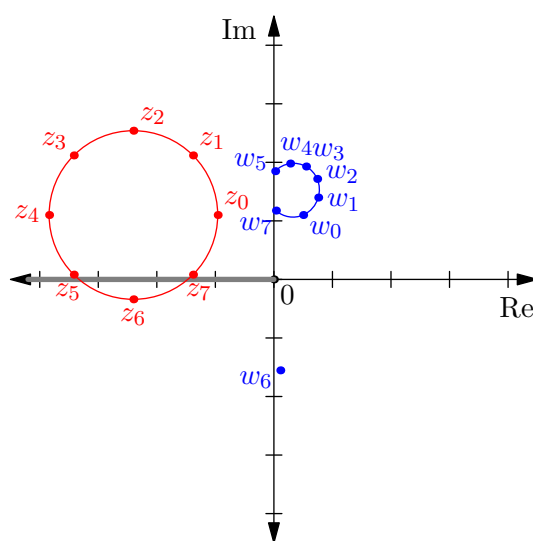
이를 좀 더 발전시켜 보겠습니다:  $z = r(\cos \theta + i \sin \theta)$ 가 주어졌을 때(여기서  $r \geq 0$ ), 우리는 근을 다음과 같이 취해야 합니다

$$w = \sqrt{r}(\cos \alpha + i \sin \alpha).$$

이때  $2\alpha \equiv \theta \pmod{2\pi}$ 를 만족합니다;  $\alpha \pmod{2\pi}$ 에 대해서는  $\pi$ 만큼 차이 나는 두 가지 선택지가 있습니다.

복소수의 경우,  $\alpha$ 를 선택하는 명백한 방법이 없습니다. 그럼에도 불구하고 우리는 임의의 구분을 시도해 볼 수도 있을 것입니다: 단순히  $-\frac{1}{2}\pi < \alpha \leq \frac{1}{2}\pi$ 인  $\alpha$ 를 선택하면 어떻게 되는지 살펴보겠습니다.

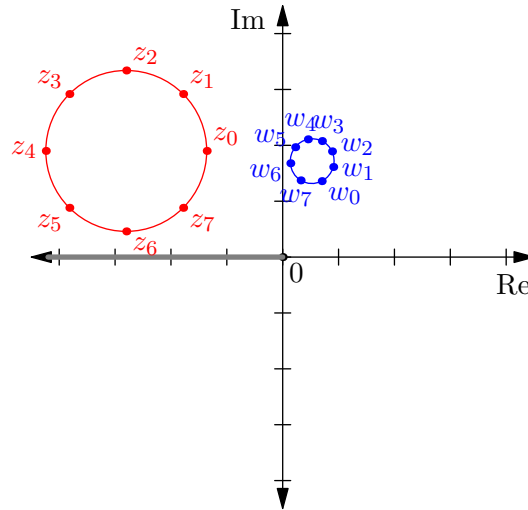
아래 그림에는 이 "위쪽-절반" 제곱근에 따른 몇몇 점들(빨간색)과 그 상(파란색)이 나타나 있습니다.  $\alpha$ 에 대한 조건은 파란색 점들이 오른쪽-절반 평면에 놓이도록 강제한다는 것을 의미합니다.



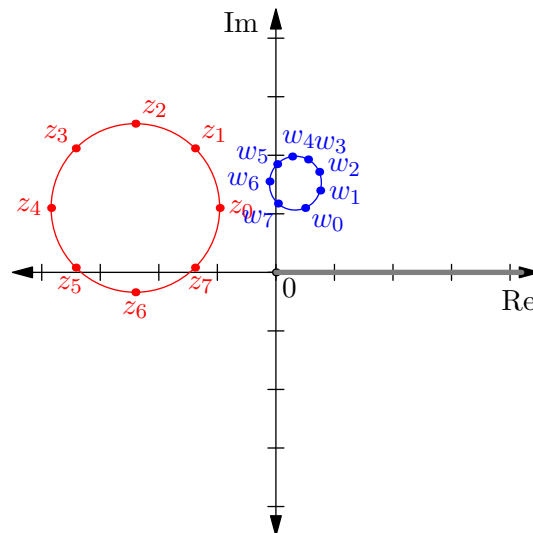
여기서 각  $i$ 에 대해  $w_i^2 = z_i$ 이며, 우리는  $w_i$ 가 복소평면의 오른쪽 절반에 놓이도록 제약을 가하고 있습니다. 명백한 문제가 있음을 알 수 있습니다: 점  $w_5$ 와  $w_7$  근처에서 큰 불연속이

발생합니다! 근처의 점  $w_6$ 은 매우 멀리 떨어진 곳으로 매핑되었습니다. 이러한 불연속은 음의 실수축 위의 점들이 "경계"에 있기 때문에 발생합니다. 예를 들어,  $-4$ 가 주어지면 이를  $2i$ 로 보내지만, 우리는 경계에 도달한 것입니다: 구간  $-\frac{1}{2}\pi < \alpha \leq \frac{1}{2}\pi$ 에서 우리는 바로 오른쪽 끝에 있는 것입니다.

우리가 건드리면 안 되는 이 음의 실수축이 바로 나중에 분지 절단이라 부르게 될 것이지만, 지금은 이를 **죽음의 광선**이라고 부르겠습니다. 이는 빨간 점들에게 보내는 경고입니다: 이 선을 넘으면 죽게 됩니다! 하지만 빨간 원을 약간만 위로 옮기면(음의 실수축을 벗어나도록) 이 문제는 완전히 피할 수 있으며, 우리는 "좋은" 제곱근처럼 보이는 것을 얻게 됩니다.



사실 죽음의 광선은 상당히 임의적입니다: 이는 우리가  $-\frac{1}{2}\pi < \alpha \leq \frac{1}{2}\pi$ 를 택했을 때 발생한 "경계 문제"의 집합입니다. 대신 구간  $0 \leq \alpha < \pi$ 를 고집했다고 합시다; 그러면 죽음의 광선은 대신 양의 실수축이 될 것입니다. 앞서 있던 원은 이제 아무 문제 없이 작동합니다.



우리가 보는 것은, 특정  $\alpha$ -구간을 선택하면 서로 다른 경계 사례 집합으로 이어지고, 따라서 서로 다른 죽음의 광선이 생긴다는 것입니다. 이 광선들이 공통으로 가지는 유일한 점은 그 시작점인 영입니다. 다시 말해, 빨간 원과  $\alpha$ 의 제한이 주어졌을 때, 죽음의 광선이 그것을 비껴가는 한 저는 멋진 "제곱근을 취한" 파란 원을 만들 수 있습니다.

그렇다면 도대체 무슨 일이 벌어지고 있는 것일까요?

## §33.2 정칙 함수의 제공근

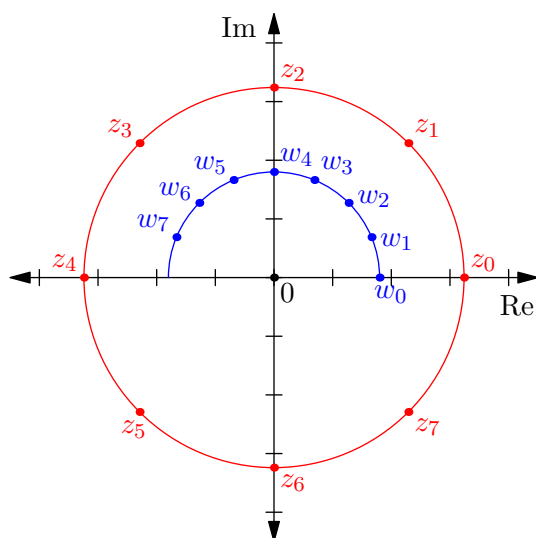
무슨 일이 일어나고 있는지 그림을 얻기 위해, 좀 더 일반적인 문제를 고려해보고자 합니다:  $f: U \rightarrow \mathbb{C}$ 가 정칙이라고 합시다. 그러면 우리는

$$f(z) = g(z)^2.$$

를 만족하는 정칙 함수  $g: U \rightarrow \mathbb{C}$ 가 존재하는지 판단하고자 합니다. 앞서  $f = \text{id}$ 로 논의한 바에 따르면  $U = \mathbb{C}$ 에 대해서는 이를 달성할 수 없다는 것을 알 수 있습니다; 문제를 일으키는 “반직선”이 존재하기 때문입니다. 그러나  $g$ 가 존재하는 함수  $f: \mathbb{C} \rightarrow \mathbb{C}$ 도 분명히 존재합니다. 가장 간단한 예로,  $f(z) = z^2$ 은 분명 제공근을 가져야 합니다!

이제 제공근을 얻기설기 짜맞출 수 있는지 살펴봅시다. 앞서 우리가 했던 것은 각 점에서 두 선택지 중 하나를 강제하는 규칙을 명시하려는 시도였습니다. 이는 불필요하게 엄격합니다. 아마 다음과 같이 할 수도 있을 것입니다:  $z_0 \in U$ 의 한 점에서 시작하여,  $f(z_0)$ 의 제공근  $w_0$ 을 선택한 다음, 거기서부터 다른 점들의 제공근을 “짜맞추어” 나가는 것입니다. 짜맞춘다는 것이 무슨 뜻일까요? 자,  $z_1$ 이  $z_0$ 에 매우 가까운 점이고, 우리가  $f(z_1)$ 의 제공근  $w_1$ 을 선택하고자 한다고 합시다. 두 가지 선택지가 있지만, 우리는 또한  $w_0$ 이  $w_1$ 에 가까울 것이라고 기대할 수 있습니다. 우리가 매우 운이 나쁘지 않은 한, 이것이  $w_1$ 의 어느 선택을 골라야 하는지 알려줄 것입니다. (어리석은 구체적 예: 만약 제가  $-17$ 의 제공근으로  $-4.12i$ 를 택했고, 그런 다음 여러분에게 이 제공근을  $-16$ 까지 계속하라고 요청한다면,  $\pm 4i$  중 어느 부호를 골라야 할까요?)

위의 스킴에는 운이 나쁠 수 있는 두 가지 경우가 있습니다: 첫째,  $w_0 = 0$ 이면 우리는 가망이 없습니다. 하지만 이를 피하더라도, 복소평면에서 완전히 한 바퀴를 돌면 시작한 곳과 다른 곳에 도달할 수도 있다는 점을 걱정해야 합니다. 구체적으로, 다시  $f = \text{id}$ 인 다음 상황을 고려해 봅시다:



우리는 점  $z_0$ 에서 시작했으며, 그것의 제공근 중 하나를  $w_0$ 으로 삼았습니다. 그런 다음 원점 주위로 완전한 빨간 원을 한 바퀴 감았는데, 결국 그 끝에서 파란 호가 시작했던 곳과 다른 곳에 있음을 발견했습니다!

앞서의 구간 구성 또한 통하지 않습니다:  $\alpha$ 의 구간을 어떻게 선택하더라도, 어떤 죽음의 광선이든 우리의 빨간 원에 부딪히기 마련입니다. 문제는 어쩐지 우리가 매우 특별한 점 0을 둘러쌌다는 사실에 있습니다.

그럼에도 불구하고,  $f(z) = z^2$ 을 취하면 우리의 “되는 대로 만들어가는” 절차에서 아무런 문제도 생기지 않는다는 것을 알고 있습니다. 그렇다면 도대체 무슨 일이 벌어지고 있는 것일까요?

### §33.3 피복 사영

지금쯤이면, 만약 여러분이 대수적 위상수학을 다룬 부분을 읽었다면, 이 모든 것이 상당히 익숙하게 느껴질 것입니다. “짜맞추는” 절차는 정확히 올림(lifting)의 개념을 설명합니다.

더 정확히 말하면, 다음과 같은 피복 사영이 존재함을 상기하십시오

$$(-)^2: \mathbb{C} \setminus \{0\} \rightarrow \mathbb{C} \setminus \{0\}.$$

$V = \{z \in U \mid f(z) \neq 0\}$ 라고 하겠습니다.  $z \in U \setminus V$ 에 대해서는 이미 제곱근  $g(z) = \sqrt{f(z)} = \sqrt{0} = 0$ 을 얻었습니다. 따라서 남은 과제는  $g: V \rightarrow \mathbb{C}$ 를 완성하는 것입니다. 그러면 본질적으로 우리가 하려는 것은 다음 도식에서 올림  $g$ 를 구성하는 것입니다

$$\begin{array}{ccc} & E = \mathbb{C} \setminus \{0\} & \\ g \nearrow & \downarrow p = \bullet^2 & \\ V & \xrightarrow{f} & B = \mathbb{C} \setminus \{0\}. \end{array}$$

우리의 사상  $p$ 는 “두 번 감기”로 설명될 수 있습니다. 이제 정리 66.2.6에 따르면 이러한 올림이 존재할 필요충분조건은 다음과 같습니다

$$f_*^{\text{img}}(\pi_1(V)) \subseteq p_*^{\text{img}}(\pi_1(E))$$

$p$ 에 의한  $\pi_1(E)$ 의 상의 부분집합인 것입니다.  $B$ 와  $E$ 가 모두 punctured plane이므로, 이들을  $S^1$ 과 동일시할 수 있습니다.

**질문 33.3.1.**  $\pi_1(B) = \mathbb{Z}$ 로 동일시하면  $p$ 에 의한 상이 정확히  $2\mathbb{Z}$ 임을 보이십시오.

이는  $V$  안의 임의의 고리  $\gamma$ 에 대해  $f \circ \gamma$ 가  $0 \in B$  둘레로 짝수 감김수를 가져야 함을 의미합니다. 이는 다음과 같습니다

$$\frac{1}{2\pi i} \oint_{\gamma} \frac{f'}{f} dz \in 2\mathbb{Z}$$

$f$ 가 극을 갖지 않기 때문입니다.

2를  $n$ 으로 바꾸어 논의를 그대로 이어가면 첫 번째 주요 결과를 얻습니다.

#### 정리 33.3.2 (정칙 $n$ 제곱근의 존재)

$f: U \rightarrow \mathbb{C}$ 를 정칙 함수라고 하겠습니다. 그러면  $f$ 가 정칙  $n$ 제곱근을 가질 필요충분 조건은 다음과 같습니다

$$\frac{1}{2\pi i} \oint_{\gamma} \frac{f'}{f} dz \in n\mathbb{Z}$$

$U$  안의 모든 등고선  $\gamma$ 에 대해 성립하는 것입니다.

### §33.4 복소 로그

복소 로그의 다가성은 다음 사실에서 비롯됩니다

$$\exp(z + 2\pi i) = \exp(z).$$

따라서  $e^w = z$ 이면, 임의의 복소수  $w + 2\pi i k$  또한 해가 됩니다.

이는 이전과 같은 방식으로 다룰 수 있으며, 다음 도식을 들어올리는 것에 해당합니다.

$$\begin{array}{ccc}
 & E = \mathbb{C} & \\
 g \nearrow & \downarrow p=\exp & \\
 U & \xrightarrow{f} & B = \mathbb{C} \setminus \{0\}
 \end{array}$$

다음과 같은 이유로 더 이상 별도의  $V$ 를 다룰 필요가 없습니다:

**질문 33.4.1.**  $f$ 가 영점을 하나라도 가지면  $g$ 가 존재할 수 없음을 보이십시오.

사실,  $\mathbb{C}$ 가 단순연결이므로 사상  $\exp: \mathbb{C} \rightarrow \mathbb{C} \setminus \{0\}$ 은 보편 피복입니다. 따라서  $p^{\text{img}}(\pi_1(\mathbb{C}))$ 는 자명합니다. 그러므로  $f$ 는 영점이 없을 뿐만 아니라,  $0 \in B$ 에 대한 감김수 또한 전혀 가질 수 없습니다. 다시 말해:

#### 정리 33.4.2 (로그의 존재성)

$f: U \rightarrow \mathbb{C}$ 를 정칙 함수라 하십시오. 그러면  $f$ 가 로그를 가질 필요충분조건은 다음과 같습니다

$$\frac{1}{2\pi i} \oint_{\gamma} \frac{f'}{f} dz = 0$$

$U$  안의 모든 폐곡선  $\gamma$ 에 대해.

### §33.5 몇 가지 특수한 경우

가장 흔한 특수한 경우는

#### 따름정리 33.5.1 (단순 연결 정의역에서의 영이 아닌 함수들)

$f: \Omega \rightarrow \mathbb{C}$ 가 연속함수이고,  $\Omega$ 는 단순 연결이라고 합시다. 모든  $z \in \Omega$ 에 대해  $f(z) \neq 0$ 이면,  $f$ 는 로그와 정칙  $n$ 제곱근을 모두 가집니다.

마지막으로, 맨 처음의  $f = \text{id}$ 에 대한 질문으로 돌아가 봅시다.

$$\sqrt{\cdot}: U \rightarrow \mathbb{C}$$

가 잘 정의되도록 하는 가장 좋은 정의역  $U$ 는 무엇일까요? 분명히  $U = \mathbb{C}$ 는 성립할 수 없지만, 거의 그만큼 잘 해낼 수 있습니다.  $f = \text{id}$ 의 유일한 영점은 원점에 있다는 점에 주목하십시오. 따라서 로그가 존재하도록 만들고자 한다면, 원점을 둘러싸는 고리를 만드는 것이 불가능하도록 복소평면에 절개를 넣기만 하면 됩니다. 흔히 선택하는 방법은 실수축의 음의 절반, 즉 우리의 첫 번째 죽음의 광선을 제거하는 것입니다. 이를 **가지 절단**(branch cut)이라 부르고,  $0 \in \mathbb{C}$ (둘러쌀 수 없는 점)를 **가지점**(branch point)이라 부릅니다. 이로부터 다음을 얻습니다.

#### 정리 33.5.2 (가지 절단 함수)

다음은 만족하는 정칙 함수들이 존재합니다

$$\log: \mathbb{C} \setminus (-\infty, 0] \rightarrow \mathbb{C}$$

$$\sqrt[n]{\cdot}: \mathbb{C} \setminus (-\infty, 0] \rightarrow \mathbb{C}$$

명백한 성질들을 만족시키는

이러한 함수의 선택은 여러 가지가 가능합니다( $n$ 제곱근에 대해서는  $n$ 가지,  $\log$ 에 대해서는 무한히 많은 선택). 이러한 함수의 선택을 **가지**(branch)라고 부릅니다. 이것이 바로 로그의 "가지"라는 말이 의미하는 바입니다.

**주가지**(principal branch)는 "표준적인" 가지로서,  $\sqrt{\cdot}: \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$ 를 정의할 때 임의로 양의 가지를 선택하는 방식과 유사합니다.  $\log$ 에 대해서는,  $e^w = z$ 이고  $w$ 의 허수부가  $(-\pi, \pi]$ 에 속하는  $w$ 를 취합니다( $2\pi i$ 의 정수배만큼 이동할 수 있기 때문입니다). 저자들은 종종 이러한 선택을 강조하기 위해  $\text{Log } z$ 라고 씁니다.

### §33.6 생각해 볼 만한 조금 더 어려운 문제

**문제 33A.** 정칙 함수  $f: U \rightarrow \mathbb{C}$ 가 정칙 로그를 갖는 것은 모든 정수  $n$ 에 대해 정칙  $n$ 제곱근을 갖는 것과 동치임을 보이십시오.

**문제 33B.**  $U$ 가 닫힌구간  $[0, 1]$ 을 제외한 복소평면 전체일 때,  $z \mapsto z(z-1)$ 로 정의된 함수  $f: U \rightarrow \mathbb{C}$ 가 정칙 제곱근을 가짐을 보이십시오.

# 34 보너스: 위상수학적 아벨-루피니 정리

우리는 이미 대수학의 기본 정리를 증명했습니다. 이제 정칙  $n$ 제곱근에 대한 앞선 직관을 바탕으로, 오차 다항식의 근에 대한 일반적인 공식이 존재하지 않음을 보일 수 있습니다.

## §34.1 진행 계획

먼저, 여기서 “공식”이 의미하는 바는 무엇일까요?

**정의 34.1.1.** 오차 공식이란 차수 5 다항식  $P$ 의 계수  $(a_0, \dots, a_5)$ 를 입력으로 받아, 연산  $+$ ,  $-$ ,  $\times$ ,  $\div$ ,  $\sqrt[n]{\phantom{x}}$ 를 유한 번 사용하여  $P$ 의 다섯 근  $(z_1, \dots, z_5)$ 로 대응시키는 공식일 것입니다.

이제, 제안된 오차 공식  $F$ 는 근이 같으면 같은 계수를 받으므로 같은 출력을 냅니다. 이는 얼핏 보기엔 문제가 없어 보이지만, 두 근을 연속적으로 맞바꾸는 경우 더 많은 문제가 생길 수 있습니다.  $F$ 는 이러한 순열 아래에서 근들의 어떤 순서를 만들어내고 보존해야 합니다.

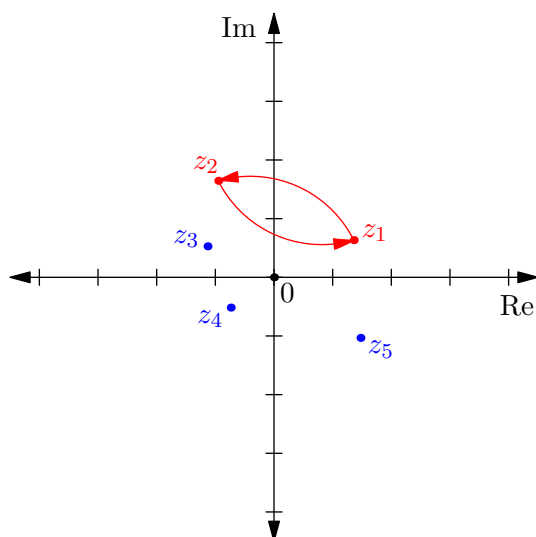
**질문 34.1.2.** 임의의  $F$ 가 근들을 매끄러운 경로를 따라 움직일 때 실제로 어느 근이 어느 근인지 추적해야만 함을 스스로 확인해 보십시오.

**비고 34.1.3 — 브링 근호**와 같은 더 복잡한 함수를 끌어들이면 이는 성립하지 않습니다. 하지만 이는 딱히 “공정한 경기”로 여겨지지 않았습니다.

## §34.2 단계 1: 가장 단순한 경우

동기 부여를 위해 먼저  $\sqrt[n]{\phantom{x}}$  연산자를 무시해 봅시다. 어떤 유리함수  $R$ 이 항상 오차 다항식  $P(z) = (z - z_1)(z - z_2)(z - z_3)(z - z_4)(z - z_5)$ 의 근 하나를 찾아낸다고 말했다고 가정해 봅시다. 단순화를 위해, 모든 근이 서로 다르다고 합시다.

처음에  $R$ 이  $z_1$ 을 출력한다고 가정해 봅시다. 다른 근들을 지나지 않는 두 개의 서로 교차하지 않는 경로를 따라 근  $z_1$ 과  $z_2$ 를 매끄럽게 맞바꿀 때 무슨 일이 일어나는지 살펴봅시다.



$R$ 이 연속이므로, 같은 근을 추적하고 있어야 합니다. 하지만  $z_1$ 과  $z_2$ 를 맞바꾸는 것을 마치면,  $P$ 의 계수는 처음과 동일해집니다. 그런데 이는  $R$ 이 속아서 출력하는 근을 바꾸었다는 것을 의미하며, 모순입니다!

여기서 더 큰 그림은,  $S_5$ 에서 근들의 순서를 바꾸면서도  $R$ 을 고정시키는 연산을 찾을 수 있었다는 점입니다.

### §34.3 단계 2: 중첩된 근호

$\sqrt[n]{\phantom{x}}$ 를 다시 그림에 추가하면, 이 아이디어는 그대로는 더 이상 통하지 않습니다.

#### 예제 34.3.1 (이차 공식)

경시대회 수학을 해본 적이 있다면, 다항식  $P(z) = az^2 + bz + c = (z - z_1)(z - z_2)$ 에 대해 다음의 두 분지가

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$z_1$ 과  $z_2$ 를 준다는 것을 알고 있을 것입니다.

그렇다면 왜 여기서  $z_1$ 과  $z_2$ 를 맞바꾸는 것이 모순을 낳지 않을까요? 그것은 모든 계수가 결국 시작 위치로 돌아오는 반면,  $\sqrt{b^2 - 4ac}$ 가 이동하는 방식의 들어올림은 그렇지 않을 수 있기 때문입니다.

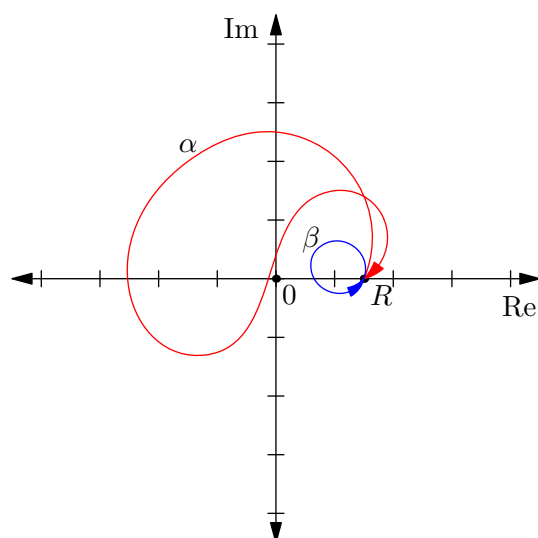
**연습문제 34.3.2.** 다항식  $z^2 - 1$ 을 생각해 봅시다. 그런 다음 근들을 매끄럽게 맞바꾸어  $(z - e^{it})(z + e^{it})$ 라는 중간 다항식들을 얻습니다. 이차 공식으로 주어지는 두 근 역시 위치가 맞바뀔을 확인해 보십시오.

이제 유리함수의  $n$ 제곱근  $\sqrt[n]{R}$ 이라는 다음으로 단순한 경우를 생각해 보고, 근들의 자명하지 않은 순열로 이를 고정시켜 봅시다.

근  $z_1$ 과  $z_2$ 를 맞바꾸면  $R$ 은 그대로 유지되지만, 원점을 도는  $R$ 의 경로  $\alpha$ 는 위상에서  $2\pi a$ 만큼의 변화를 누적했을 수 있습니다.  $z_1$ 과  $z_2$ 를 같은 방식으로 다시 맞바꾼다면, 위상의 변화는 원래대로 되돌리겠지만, 결국 아무것도 하지 않은 것과 같아질 것입니다.

하지만 위상의 변화는 아벨적인 반면, 순열은 그렇지 않습니다. 근  $z_2$ 와  $z_3$ 을 맞바꾸는 또 다른 연산을 생각해 봅시다. 두 연산의 교환자를 취하면, 모든 위상은 그대로 유지되지만 결국 순열  $(12)(23)(12)^{-1}(23)^{-1}$ 을 얻게 됩니다.

두 번째 연산의 경로를  $\beta$ 로 표시한다면, 이는  $\alpha\beta\alpha^{-1}\beta^{-1}$ 에 대응됩니다.



**연습문제 34.3.3.** 이 순열 연산이 자명하지 않음을 보이십시오.

이제 우리는 더 나은 도구를 가지고 있습니다: 유리 함수의  $n$ 제곱근을 고정하는  $S_5$ 의 순열들과,  $+$ ,  $-$ ,  $\times$ ,  $\div$  하에서의 이들의 합성을 가지고 있습니다.

이제 중첩된 근호는 어떻게 다루어야 합니까?

#### 예제 34.3.4 (삼차 공식)

삼차 공식에는 까다로운 항이 포함되어 있습니다.

$$\sqrt[3]{\frac{2b^3 - 9abc + 27a^2d + \sqrt{(2b^3 - 9abc + 27a^2d)^2 - 4(b^2 - 3ac)^3}}{2}}.$$

여기서 우리는 여러 개의 근을 취했습니다.

**정의 34.3.5.** 중첩된 근호의 차수를, 근호가 다른 근호 안에서 발견될 수 있는 최대 횟수로 정의합니다.

이제 예를 들어  $\sqrt[3]{\sqrt{ab+c} - \sqrt{d}}$ 와 같은, 차수가 2인 중첩된 근호를 생각해 봅시다. 우리는 세제곱근의 내부를 고정하는 자명하지 않은 교환자  $\sigma$ 와  $\rho$ 를 가지고 있음을 알고 있지만, 이번에도 위상은 각 연산 개별적으로는 보존되지 않을 수 있습니다. 다시 한번, 우리는 이 교환자들의 교환자, 예를 들어 같은 논리에 의해 위상 문제를 해결하는  $\sigma\rho\sigma^{-1}\rho^{-1}$ 를 고려할 수 있습니다.

차수가 3인 근호 등을 해결하기 위해 교환자들의 교환자들의 교환자를 고려하지 못할 이유는 없습니다. 따라서 우리가 항상 자명하지 않은 교환자를 계속 얻을 수 있다는 것만 남습니다.

## §34.4 3단계: 정규 군

우리는 이를 군론 문제로 환원했습니다. 교환자들의 사슬이 주어졌을 때

$$S_5 = G \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \dots$$

여기서 각 군은 이전 군의 교환자 부분군이며, 우리는  $G^{(n)}$ 이 결코 자명해지지 않음을 보이고자 합니다. 이 사슬을 **유도열**이라고 부릅니다.

**연습문제 34.4.1.** 군  $G$ 의 교환자 부분군  $[G, G]$ 에 대해  $[G, G] \leq G$ 가 성립하며,  $G/[G, G]$ 가 아벨 군임을 보이십시오.

**정의 34.4.2.** 군  $G$ 는 그 유도열이 결국 자명해지면 **가해군**이라고 합니다.

따라서 남은 것은  $S_5$ 가 가해군이 아님을 보이는 것입니다. 이는 이 장의 위상수학적 아이디어와는 관련이 없는 계산이므로, **문제 34A**로 미루겠습니다.

## §34.5 요약

이것이 실제로 타당한 증명이기는 하지만, 여기에는 몇 가지 장단점이 있습니다. 단점으로는,  $z^5 - z - 1$ 과 같은 다항식이 중첩된  $n$ 제곱근을 사용하여 표현할 수 없는 근을 가진다는 것을 우리가 보이지 않았다는 점입니다. 우리는 단지 모든 5차 다항식에 대한 공식이 존재하지 않는다는 것만을 보였을 뿐입니다.

장점으로는, 이 논증을 통해  $\exp$ ,  $\sin$ ,  $\cos$ 와 같은 함수들을 더 추가하더라도 그러한 공식이 존재하지 않음을 쉽게 보일 수 있다는 점입니다. 또한 이 정리를  $A_5$ 가 가해군이 아니라는 사실과 비교할 때 사람들이 무엇을 의미하는지를 대략적으로 이해할 수 있게 해줍니다.

## §34.6 생각해 볼 만한 조금 더 어려운 문제



**문제 34A.**  $A_5$ 가 가해군이 아님을 보이십시오.

X

측도론

## 제X부: 목차

---

|           |                                  |            |
|-----------|----------------------------------|------------|
| <b>35</b> | <b>측도 공간</b>                     | <b>387</b> |
| 35.1      | 문자 연상                            | 387        |
| 35.2      | 확률 변수를 통해 측도 공간의 동기 부여하기         | 387        |
| 35.3      | 측도 공간을 기하학적으로 동기 부여하기            | 388        |
| 35.4      | $\sigma$ -대수와 가측 공간              | 388        |
| 35.5      | 측도 공간                            | 389        |
| 35.6      | 바나흐-타르스키의 힌트                     | 391        |
| 35.7      | 가측 함수                            | 391        |
| 35.8      | “거의”라는 단어에 대하여                   | 392        |
| 35.9      | 생각해 볼 만한 조금 더 어려운 문제             | 393        |
| <b>36</b> | <b>보렐 측도와 르베그 측도 구성하기</b>        | <b>395</b> |
| 36.1      | 사전측도                             | 395        |
| 36.2      | 외측도                              | 396        |
| 36.3      | 외측도에 대한 Carathéodory 확장          | 398        |
| 36.4      | 르베그 측도 정의하기                      | 399        |
| 36.5      | 네 번째 행: 준측도에 대한 Carathéodory 정리  | 401        |
| 36.6      | 지금부터, 우리는 보렐 측도를 가정합니다           | 403        |
| 36.7      | 생각해 볼 만한 조금 더 어려운 문제             | 403        |
| <b>37</b> | <b>르베그 적분</b>                    | <b>405</b> |
| 37.1      | 정의                               | 405        |
| 37.2      | 동치인 정의                           | 408        |
| 37.3      | 리만 적분과의 관계 (또는: 실제로 르베그 적분 계산하기) | 409        |
| 37.4      | 생각해 볼 만한 조금 더 어려운 문제             | 410        |
| <b>38</b> | <b>르베그 적분과 순서 교환하기</b>           | <b>411</b> |
| 38.1      | 극한 교환의 동기                        | 411        |
| 38.2      | 개요                               | 412        |
| 38.3      | 파투 보조정리                          | 413        |
| 38.4      | 그 외 모든 것                         | 413        |
| 38.5      | 푸비니와 토넬리                         | 417        |
| 38.6      | 생각해 볼 만한 조금 더 어려운 문제             | 417        |
| <b>39</b> | <b>보너스: 폰트랴긴 쌍대성에 대한 힌트</b>      | <b>419</b> |
| 39.1      | LCA 군                            | 419        |
| 39.2      | 폰트랴긴 쌍대                          | 420        |
| 39.3      | 콤팩트한 경우의 정규직교 기저                 | 421        |
| 39.4      | 비콤팩트한 경우의 푸리에 변환                 | 422        |
| 39.5      | 요약                               | 422        |
| 39.6      | 생각해 볼 만한 조금 더 어려운 문제             | 423        |

---

# 35 측도 공간

다음으로 우리가 나아갈 방향에 대한 개요를 소개합니다. 앞으로 몇 개의 장에 걸친 우리의 목표는 큰 수의 법칙과 중심극한정리를 서술(그리고 경우에 따라서는 증명)하기 위한 장치를 발전시키는 것입니다. 이러한 목적을 위해서는 미적분학 101에서 다룬 얼마 안 되는 작업으로는 심각하게 부족할 것입니다:  $\mathbb{R}$ (또는  $\mathbb{R}^n$ )에서의 적분만으로는 도저히 해낼 수 없을 것입니다.

이 장에서는 "크기라는 개념을 갖춘 공간"으로 생각할 수 있는 "측도 공간"의 이론을 발전시킬 것입니다. 그러면 이른바 르베그 적분(어떤 의미에서는 리만 적분보다 거의 엄격하게 더 낫다고 할 수 있습니다)을 이용해 이러한 공간 위에서 적분할 수 있게 됩니다.

## §35.1 문자 연상

앞으로 등장할 객체의 "종류"가 매우 많으므로, 다음 몇 개의 장에 걸쳐 우리가 사용할 문자 연상을 소개합니다. 이렇게 하면 어떤 문자가 사용되었는지만 보고도 각 객체의 "종류"를 더 쉽게 알 수 있습니다.

- 측도 공간은  $\Omega$ 로 표기하고, 그 원소는  $\omega$ 로 표기합니다.
- 대수와  $\sigma$ -대수는 필기체  $\mathcal{A}, \mathcal{B}, \dots$ 로 표기합니다. 그 안에 속한 집합은 초반부 대문자 로마자  $A, B, C, D, E, \dots$ 로 표기합니다.
- 측도(즉, 집합을 실수에 대응시키는 함수)는 보통  $\mu$  또는  $\rho$ 로 표기합니다.
- 확률 변수(세계를 실수로 보내는 함수)는 보통 후반부 대문자 로마자  $X, Y, Z, \dots$ 로 표기합니다.
- $\mathbb{R} \rightarrow \mathbb{R}$  함수는 로마자로 표기하며, pdf에는  $f, g$  같은 문자를, cdf에는  $F, G$  같은 문자를 사용합니다.
- 실수는 소문자 로마자  $x, y, z$  같은 문자로 표기합니다.

## §35.2 확률 변수를 통해 측도 공간의 동기 부여하기

우리가 왜 측도 공간을 구성하고 싶어 하는지 동기를 부여하기 위해, (실제) **확률 변수**에 대해 이야기해 보고자 합니다. 이는 다음과 같은 것으로 생각할 수 있습니다.

- 동전 던지기의 결과,
- 토요일 보스턴의 최고 기온,
- 다음 주말 여러분의 18.725 데이트에 비가 올 가능성.

왜 이것을 제대로 발전시키려면 긴 이론이 필요할까요? 단순한 동전 던지기라면 직관적으로 그저 "앞면 50%, 뒷면 50%"라고 생각하고 끝낼 것입니다. 기온의 경우는 이산적이지 않고 연속적이기 때문에 상황이 조금 더 까다롭지만, 여러분이 신경 쓰는 것이 오직 그 하나의 기온뿐이라면 미적분학만으로도 이를 다루기에 충분해 보입니다.

하지만 변수들이 서로 "이야기를 나누기" 시작하면 상황은 더 미묘해집니다: 최고 기온은 비가 올지에 대해 약간의 정보를 알려줍니다. 예를 들어 기온이 매우 높으면 맑을 가능성이 상당히 높기 때문입니다. 갑자기 우리는 조건부 확률에 대해 이야기하고 싶어지지만, 이는

완전히 골치 아픈 문제입니다 — 이러한 것들 사이의 관계는 매우 빠르게 매우 복잡해질 수 있습니다.

이를 위한 형식 체계를 얻는 큰 아이디어는 다음과 같습니다:

**우리의 측도 공간  $\Omega$ 는 세계 전체의 공간으로 생각될 것이며, 각  $\omega \in \Omega$ 는 하나의 세계를 나타냅니다. 확률 변수는 세계에서  $\mathbb{R}$ 로 가는 함수입니다.**

이런 방식으로, "세계"의 공간이 모든 지저분한 상호의존성을 처리해 줍니다.

그러면 우리는 세계의 집합에 "측도"를 부여할 수 있습니다: 예를 들어, 공정한 동전이 라는 것은, 여러분이 오직 그 한 번의 동전 던지기에만 관심이 있다면, 그 동전이 앞면을 보인 세계의 "비율"이  $\frac{1}{2}$ 여야 한다는 것을 의미합니다. 이는 어떤 면에서는 여러분이 고등학교에서 배운 것과는 거꾸로입니다: 공식적으로는, 확률에서 시작하는 것이 아니라 세계의 공간에서 시작합니다.

$2^\Omega$ 개의 부분집합 모두에 대해 잘 정의된 측도를 부여할 방법이 없다는 것이 곧 명백해질 것입니다. 다행히도 실제로는 그렇게 할 필요가 없으며,  $\sigma$ -대수라는 개념이 "우리가 그럴 저러 해나가기에 충분한 측정 가능한 집합"이라는 아이디어를 포착해 낼 것입니다.

**비고 35.2.1 (무작위 시드)** — 프로그래밍을 해 보셨다면 또 다른 비유로 이해하실 수 있습니다: 각  $\omega \in \Omega$ 는 무작위 시드이며, 모든 것이 거기서부터 결정됩니다.

### §35.3 측도 공간을 기하학적으로 동기 부여하기

자, 우리에게는 가능한 점들의 집합  $\Omega$ 가 있고 (이는 앞선 논의의 맥락에서 세계들의 집합으로 생각할 수 있습니다),  $\Omega$  안의 점들의 부분집합에 측도(부피라고 생각하십시오)를 부여하고자 합니다. 이제 우리가 마주칠 몇 가지 장애물들을 설명하여, 측도 공간이 어떻게 정의되는지에 대한 동기를 부여하고자 합니다 (앞 절에서는 우리가 왜 그런 것을 원하는지에 대해서만 동기를 부여했습니다).

이를 순진하게(naïvely) 시도하면, 기본적으로 곧바로 집합론적인 문제에 부딪히게 됩니다. 이런 일이 왜 일어날 수 있는지 생각해 볼 좋은 예시는  $\Omega = \mathbb{R}^2$ 이고 측도가 넓이에 대응하는 경우입니다. 고등학교에서처럼 삼각형의 넓이를 정의할 수 있고, 그다음 다각형으로 근사하는 방식으로 원의 넓이도 정의해 볼 수 있습니다. 하지만 예를 들어 부분집합  $\mathbb{Q}^2$ 에는 어떤 넓이를 부여해야 할까요? (" $0$ "이 실제로 통하는 답이라는 것이 밝혀집니다.) 또는, 단위 원판은 무한히 많은 점들로 이루어져 있는데, 각 점은 측도가  $0$ 이어야 마땅하지만 그렇다면 그것들의 합집합은 왜 측도  $\pi$ 를 갖는 것일까요? 등등.

이에 대해서는 나중에 더 이야기하겠지만, 여러분은 이미 **바나흐-타르스키 역설**에 대해 들어보았을 수도 있습니다. 이 역설은 본질적으로  $\mathbb{R}^3$ 의 모든 낱알의 부분집합에 측도를 부여하면서도 기본적인 상식 검사를 만족시킬 수 있는 좋은 방법이 없다는 것을 보여줍니다. 유클리드 공간의 가능한 부분집합이 그저 너무나 많습니다.

하지만 좋은 소식은, 이러한 집합들 대부분은 우리가 결코 신경 쓰지 않을 것들이며, 특정한 "충분히 좋은 집합들"에 대해서만 측도를 정의하면 충분하다는 것입니다. 우리가 사용할 형용사는 가측이며, 이것이 실용적인 목적에 있어서 훨씬, 훨씬 더 충분히 좋다는 것이 밝혀질 것입니다.

우리는 일반적으로 가측 집합에 대해  $A, B, \dots$ 를 사용하고, 가측 집합 전체의 모임을 필기체  $\mathcal{A}$ 로 표기하겠습니다.

### §35.4 $\sigma$ -대수와 가측 공간

여기 기계어 코드가 있습니다.

**정의 35.4.1.** **가측 공간**은 점들의 공간  $\Omega$ 와,  $\Omega$ 의 부분집합들의  $\sigma$ -대수  $\mathcal{A}$  ( $\Omega$ 의 "가측 집합들")로 이루어집니다. 집합  $\mathcal{A}$ 는 다음 공리들을 만족해야 합니다:

- $\mathcal{A}$ 는  $\emptyset$ 과  $\Omega$ 를 포함합니다.
- $\mathcal{A}$ 는 여집합과 가산 합집합/교집합에 대해 닫혀 있어야 합니다. (명명법에 대한 힌트:  $\sigma$ 는 보통 일종의 "가산 유한" 조건을 나타냅니다.)

(불만: 이 용어는 나중에 "측도 공간"과 혼동될 수 있기 때문에 발음상 헷갈립니다. 이렇게 생각하는 방법이 있습니다: "가측(measurable) 가능한" 공간은  $\sigma$ -대수를 가지고 있어서 그 위에 측도를 두려고 시도할 수는 있지만, 아직 두지는 않았다"는 것입니다.)

이 정의는 몇몇 특정한 경우에는 실제로 우리가 생각하는 방식이지만, 대부분의 경우 우리는 실제로  $\mathcal{A}$ 를 다른 방식으로 구체화할 것입니다:

**정의 35.4.2.**  $\Omega$ 를 집합이라 하고,  $\Omega$ 의 부분집합들의 어떤 모임  $\mathcal{F}$ 를 생각해 봅시다. 그러면  $\mathcal{F}$ 에 의해 생성된  $\sigma$ -대수는  $\mathcal{F}$ 를 포함하는 가장 작은  $\sigma$ -대수  $\mathcal{A}$ 입니다.

수학에서 흔히 그렇듯, "생성된다"라는 말을 보면 이는 정의가 스스로 "알아서 처리하도록" 내버려 둔다는 뜻입니다. 그러니 만약  $\Omega = \mathbb{R}$ 이고, 제가  $\mathcal{A}$ 가 모든 열린집합을 포함하기를 원한다고 합시다. 그러면 정의에 의해 모든 여집합도 포함해야 하므로, 모든 닫힌 집합도 포함하게 됩니다. 그다음에는 모든 반열린 구간도 포함해야 하며, 그러고 나서는.... 최종적으로  $\mathcal{A}$ 의 모양이 정확히 어떻게 되는지 따져보려 하기보다는(이는 기본적으로 불가능한 것으로 밝혀집니다), 그냥 포기하고 " $\mathcal{A}$ 는 열린집합에서 시작해 합집합/여집합 연산을 반복적으로 적용하여 얻을 수 있는 모든 집합이다"라고 말합니다. 혹은 더 노골적으로: "열린집합에서 시작해서 세차게 혼든다."<sup>1</sup>

예시 없이 너무 길게 이야기했습니다.

### 예제 35.4.3 (가측 공간의 예시들)

처음 두 예시는 실제로  $\mathcal{A}$ 가 무엇인지 말해줍니다. 세 번째 예시(가장 중요함)는 생성을 사용할 것입니다.

- $\Omega$ 가 임의의 집합이라면, 멱집합  $\mathcal{A} = 2^\Omega$ 는 명백히  $\sigma$ -대수입니다. 이는  $\Omega$ 가 가산일 때 사용될 것이지만,  $\Omega$ 가 거대하다면 그다지 도움이 되지 않을 것입니다.
- $\Omega$ 가 비가산 집합이라면, 우리는  $\mathcal{A}$ 를  $\Omega$ 의 부분집합 중 가산이거나 그 여집합이 가산인 것들 전부로 선언할 수 있습니다. (이것이 정의를 만족함을 확인해 보아야 합니다.) 이는 매우 "성진" 대수입니다.
- $\Omega$ 가 위상 공간이라면, **보렐  $\sigma$ -대수**는  $\Omega$ 의 모든 열린집합에 의해 생성된  $\sigma$ -대수로 정의됩니다. 이를  $\mathcal{B}(\Omega)$ 로 표기하고, 그 공간을 **보렐 공간**이라 부릅니다. 앞서 경고했듯이, 그것이 어떻게 생겼는지 기술하는 것은 기본적으로 불가능하며, 대신 "우리는 열린집합을 측정할 수 있다"라고 말하는 것으로 생각해야 합니다.

**질문 35.4.4.** 임의의 위상 공간  $\Omega$ 에 대해 닫힌집합들이  $\mathcal{B}(\Omega)$ 에 속함을 보이십시오.  $[0, 1]$  또한  $\mathcal{B}(\mathbb{R})$ 에 속함을 보이십시오.

## §35.5 측도 공간

**정의 35.5.1.** 그런 다음 가측 공간  $(\Omega, \mathcal{A})$ 에는 **측도**라 불리는 함수  $\mu: \mathcal{A} \rightarrow [0, +\infty]$ 가 갖추어지는데, 이는 다음 공리들을 만족해야 합니다:

<sup>1</sup>나중에 절 36.4에서 언급하겠지만, 초한 귀납법을 이용한 명시적인 구성이 가능합니다. 그 구성은 예를 들어  $|\mathcal{B}(\mathbb{R})| = |\mathbb{R}|$ 을 증명하는 데에도 유용합니다.

- $\mu(\emptyset) = 0$
- **가산 가법성:**  $A_1, A_2, \dots$ 가  $\mathcal{A}$ 의 서로소인 집합들이라면,

$$\mu\left(\bigsqcup_n A_n\right) = \sum_n \mu(A_n).$$

삼중항  $(\Omega, \mathcal{A}, \mu)$ 을 **측도 공간**이라고 합니다.  $\mu(\Omega) = 1$ 이면 이를 **확률 공간**이라고 합니다.

**연습문제 35.5.2** (더 약한 동치 정의). 저는 사람들이 실제로  $\mathcal{A}$ 와  $\mu$ 를 어떻게 생각하는지를 포착하는 공리를 제시하기로 했는데, 이는 약간의 중복이 있음을 의미합니다: 예를 들어, 여집합과 합집합에 대해 닫혀 있다는 것만으로도 드모르간의 법칙에 의해 교집합을 얻기에 충분합니다. 다음은 더 최소한의 정의로서, 어떤 것이 이 조건들을 만족함을 증명하려 할 때 해야 할 작업량을 줄이는 데 유용합니다:

- $\mathcal{A}$ 에 대한 공리는 (i)  $\emptyset \in \mathcal{A}$ 이고 (ii)  $\mathcal{A}$ 가 여집합과 가산 합집합에 대해 닫혀 있다는 조건으로 약화될 수 있습니다.
- $\mu$ 에 대한 공리는 (i)  $\mu(\emptyset) = 0$ , (ii)  $\mu(A \sqcup B) = \mu(A) + \mu(B)$ , (iii)  $\mu(A_1) < \infty$ 인  $A_1 \supseteq A_2 \supseteq \dots$ 에 대해  $\mu(\bigcap_n A_n) = \lim_n \mu(A_n)$ 이라는 조건으로 약화될 수 있습니다.

**비고 35.5.3** — 이 정의들에 대한 몇 가지 즉각적인 언급을 살펴보겠습니다.

- 만약  $A \subseteq B$ 가 가측이면,  $\mu(B) = \mu(A) + \mu(B - A)$ 이므로  $\mu(A) \leq \mu(B)$ 입니다.
- 특히, 확률 공간에서는 모든 측도가  $[0, 1]$  안에 있습니다. 반면에, 일반적인 측도 공간에서는  $+\infty$ 도 측도의 가능한 값으로 허용할 것입니다 (그래서  $\mu$ 의 공역으로  $[0, +\infty]$ 를 선택한 것입니다).
- 적어도 가산 합집합/가산 가법성은 허용하고 싶은데, 유한 합집합만으로는 진전을 이루기가 너무 어렵기 때문입니다: 가산 무한히 많은 삼각형의 극한을 이야기할 수 없다면 원의 넓이를 추정하기가 너무 어렵습니다.

반면 비가산 합집합과 비가산 가법성은 허용하고 싶지 않는데, 비가산 합은 거의 항상 잘 성립하지 않기 때문입니다. 특히, 다음과 같은 좋은 초등적 연습문제가 있습니다:

**연습문제 35.5.4** (까다로움).  $S$ 를 양의 실수들로 이루어진 비가산 집합이라고 합시다. 어떤 유한 부분집합  $T \subseteq S$ 가 존재하여 그 합이  $10^{2019}$ 보다 큼을 보이십시오. 구어체로 말하면, "비가산개의 양의 실수는 유한한 합을 가질 수 없다"는 것입니다.

그러므로 무한합은 가산합까지만 허용할 것입니다. 이것이 애초에 우리가  $\sigma$ -대수를 고려했던 이유입니다.

### 예제 35.5.5 (측도)

이제 앞선 예시들의 각 공간에서의 측도를 논의하겠습니다.

- $\mathcal{A} = 2^\Omega$ 이면 (또는 사실 어떤  $\mathcal{A}$ 이든) 각  $A \in \mathcal{A}$ 에 대해  $\mu(A) = |A|$ 로 선언할 수 있습니다 ( $|A| = \infty$ 인 경우도 포함하여). 이를 **셈측도**라고 하며, 단순히 원소의 개수를 세는 것입니다.

이는  $\Omega$ 가 가산 무한일 때 유용하며,  $\Omega$ 가 유한(이면서 공집합이 아닐) 때 최적입니다. 후자의 경우, 우리는 종종  $\mu(A) = \frac{|A|}{|\Omega|}$ 로 정규화하여  $\Omega$ 가 확률 공간이 되도록 합니다.

(b)  $\Omega$ 가 비가산이고  $\mathcal{A}$ 를 가산 집합들과 그 여집합들로 잡았다고 합시다. 그러면

$$\mu(A) = \begin{cases} 0 & A \text{는 가산입니다} \\ 1 & \Omega \setminus A \text{는 가산입니다} \end{cases}$$

이는 측도입니다. (이를 확인하십시오.)

(c) 방 안의 코끼리:  $\mathcal{B}(\Omega)$  위에 측도를 정의하는 것은  $\Omega = \mathbb{R}$ 인 경우조차도 어려우며, 이는 다음 장에서 다룹니다. 그러니 잠시 숨을 참고 기다려야 합니다. 지금으로서,  $\mathcal{B}(\Omega)$  위에 측도를 정의하겠다는 저의 의도를 밝힘으로써, 적어도 모든 열린집합이 부피를 갖기를 바란다는 것만 알면 됩니다.

## §35.6 바나흐-타르스키의 힌트

이제 저는  $\mathcal{B}(\Omega)$ 가 필요한 타협임을, 그리고  $\Omega = \mathbb{R}^n$ 과 같은 일반적인 위상 공간에서는  $2^\Omega$ 에 측도를 부여할 가망이 없음을 여러분에게 납득시켜 보겠습니다. (문헌에서는 이 예시를 비탈리 집합이라고 부릅니다.)

**예제 35.6.1** ( $\mathcal{A} = 2^\Omega$ 가 적합하지 않은 이유에 대한 기하학적 예시)

$\Omega$ 를  $\mathbb{R}^2$  안의 단위원이라 하고  $\mathcal{A} = 2^\Omega$ 라 합시다. 우리는  $\mu(\Omega) = 1$ 인  $\Omega$  위의 임의의 측도  $\mu$ 가 바람직하지 않은 성질을 가짐을 보이겠습니다.

$\sim$ 을 다음과 같이 정의되는  $\Omega$  위의 동치 관계라고 합시다: 두 점이 원점을 중심으로  $\pi$ 의 유리수 배만큼 회전한 차이만 있다면 동치라고 합니다. 각 동치류에서 대표원을 하나씩 뽑아,  $X$ 를 그 대표원들의 집합이라고 합시다. 그러면

$$\Omega = \bigsqcup_{\substack{q \in \mathbb{Q} \\ 0 \leq q < 2}} (Xq\pi \text{ 라디안만큼 회전된}).$$

우리는  $X$ 를 회전시키기만 했으므로, 각 회전은 동일한 측도  $m$ 을 가져야 합니다. 그런데  $\mu(\Omega) = 1$ 이고, 이 측도에 부여할 수 있는 값은 존재하지 않습니다:  $m = 0$ 이면  $\mu(\Omega) = 0$ 이 되고,  $m > 0$ 이면  $\mu(\Omega) = \infty$ 가 됩니다.

**비고 35.6.2 (선택)** — 전문가라면 대표원을 뽑는 것(즉 집합  $X$ 를 만드는 것)이 엄밀히는 선택공리를 필요로 함을 알아차릴 것입니다. 그렇기 때문에 사람들이 바나흐-타르스키 문제를 이야기할 때, 선택공리도 거의 항상 함께 언급됩니다.

다음 장에서  $\mathcal{B}(\mathbb{R}^n)$ 에 대한 실제 구성을 보게 될 것이니 계속 지켜봐 주십시오.

## §35.7 가측 함수

**이 절의 대표적인 예:**  $S \subseteq \Omega$ 에 대해,  $1_S: \Omega \rightarrow \mathbb{R}$ 가 가측 함수인 것은  $S$ 가 가측 집합인 것과 동치입니다.

예전에 위상 공간을 다룰 때는 연속 함수를 고려했습니다. 여기서의 유사 개념은 다음과 같습니다:

**정의 35.7.1.**  $(X, \mathcal{A})$ 와  $(Y, \mathcal{B})$ 를 가측 공간(또는 측도 공간)이라 합시다. 함수  $f: X \rightarrow Y$ 가 **가측**이라는 것은, 임의의 가측 집합  $S \subseteq Y$  (즉  $S \in \mathcal{B}$ )에 대해  $f^{\text{pre}}(S)$ 가 가측 (즉  $f^{\text{pre}}(S) \in \mathcal{A}$ )임을 의미합니다.

대부분의 경우  $Y$ 는 실제로 보렐  $\sigma$ -대수를 가진 위상 공간(예:  $Y = \mathbb{R}$ )이며, 이 경우 “가측 집합  $S$ ”를 “열린집합  $S$ ”로 바꿀 수 있습니다. 이 책의 나머지 부분에서는 이를 기본 가정으로 삼아도 좋습니다.

연속 함수의 정의와의 명백한 대칭성 외에도, **절 37.2**에서 보게 되듯이, 이 정의는 음이 아닌 함수  $f: \Omega \rightarrow \mathbb{R}_{\geq 0}$ 에 대해  $\int_{\Omega} f \, d\mu$ 가 존재하는 것이  $f$ 가 가측인 것과 동치가 되도록 만듭니다.

**비고 35.7.2** — 다음 예시가 보여주듯이, 가측 함수가 반드시 연속일 필요는 없다는 점에 유의하십시오. 반면, 실제로 접하게 되는 대부분의 함수는 연속일 것이므로, 그런 경우에는 문제가 없습니다.

**예제 35.7.3** (가측 집합의 비가측 원상을 갖는 연속 함수)

$f: [0, 1] \rightarrow [0, 1]$ 을 데블스 스테어케이스(또는 칸토어 함수)라 합시다. 이 함수는 연속이며,  $C \subseteq [0, 1]$ 을 칸토어 집합이라 하면  $|C| = 0$ 이지만  $f^{\text{img}}(C) = [0, 1]$ 이고 측도는 1이라는 성질을 갖습니다.

$g: [0, 1] \rightarrow [0, 2]$ 를  $g(x) = f(x) + x$ 로 정의합시다. 그러면,

- 칸토어 집합  $C$ 에서 제거되는 각 열린 구간  $(a, b)$ 에 대해,  $|g^{\text{img}}((a, b))| = |(a, b)|$ 입니다.
- $g^{\text{img}}(C)$ 는 측도 1을 갖습니다.

$g$ 가 전단사임에 유의하고,  $h: [0, 2] \rightarrow [0, 1]$ ,  $h = g^{-1}$ 라 합시다. 그러면  $h$ 는 연속이지만, 다음이 성립합니다:

- $h^{\text{pre}}(C) = g^{\text{img}}(C)$ 는 측도 1을 가지므로, 비가측 부분집합을 갖습니다,
- $C$ 는 측도 0을 가지므로,  $C$ 의 모든 부분집합은 (르베그) 가측입니다,
- 따라서, 어떤 가측 부분집합  $D \subseteq C$ 에 대해  $h^{\text{pre}}(D)$ 는 비가측입니다.

**명제 35.7.4** (연속이면 보렐 가측)

$X$ 와  $Y$ 가 위상 공간이고, 두 공간 모두에 보렐 측도를 택했다고 합시다. 위상 공간의 사상으로서 연속인 함수  $f: X \rightarrow Y$ 는 가측이기도 합니다.

증명. 열린집합의 원상이 열린집합이며, 따라서 보렐 가측이라는 사실로부터 따라옵니다.  $\square$

## §35.8 “거의”라는 단어에 대하여

이후 장들에서 “거의 모든 곳에서”와 “거의 확실히”라는 표현이 등장하기 시작할 것이므로, 지금 시간을 내어 이에 관해 이야기하는 것이 신중해 보입니다.

**정의 35.8.1.** 성질  $P$ 가 **거의 모든 곳에서** 또는 **거의 확실히** 성립한다는 것은, 다음 집합이

$$\{\omega \in \Omega \mid \omega \text{에 대해 } P \text{가 성립하지 않습니다}\}$$

측도 0을 가짐을 의미합니다.

예를 들어, 측도 공간  $\Omega$  위에서 정의된 어떤 함수  $f$ 와  $g$ 에 대해 “ $f = g$  거의 모든 곳에서”라고 말한다면, 이는 측도 0인 집합을 제외한 모든  $\omega \in \Omega$ 에 대해  $f(\omega) = g(\omega)$ 임을 의미합니다.

자, 이것이 정의입니다. 이제 여러분의 직관을 갱신해야 할 핵심은 다음과 같습니다.

**측도론에서는 기본적으로 거의 모든 곳에서라는 개념까지만 신경 씁니다.**

몇 가지 예시는 다음과 같습니다:

- $f = g$ 가 거의 모든 곳에서 성립한다면, 측도론은 기본적으로 이 함수들을 구별하지 못합니다. 예를 들어, 거의 모든 곳에서 일치하는 두 함수에 대해  $\int_{\Omega} f d\omega = \int_{\Omega} g d\omega$ 가 성립합니다.
- 또 다른 예로, “어떤 조건을 만족하는 함수  $f$ 가 유일하게 존재한다”는 것을 증명한다면, 그 유일성은 보통 측도 0인 집합의 차이까지만 성립하게 됩니다.

이것은 군의 동형사상과 다소 비슷하다고 생각할 수 있는데, 두 군이 동형일 때 “본질적으로 같다”고 간주하는 것과 같습니다. 다만 이쪽은 익숙해지는 데 시간이 좀 걸릴 수 있습니다.<sup>2</sup>

### §35.9 생각해 볼 만한 조금 더 어려운 문제

**문제 35A<sup>†</sup>.**  $(\Omega, \mathcal{A}, \mu)$ 를 확률 공간이라 합시다. 측도가 1인 가산 개의 집합들의 교집합 역시 측도가 1임을 보이십시오.



**문제 35B** (가산  $\sigma$ -대수에 관하여). 집합  $\Omega$  위의  $\sigma$ -대수를  $\mathcal{A}$ 라고 합시다.  $\mathcal{A}$ 가 가산 기수를 가진다고 가정합니다.  $|\mathcal{A}|$ 가 유한하고 2의 거듭제곱과 같음을 증명하십시오.

<sup>2</sup>실제로 일부 사람들은 측도 공간 위의 함수를, 측도 0인 집합 바깥에서의 일치 관계로 나눈 사상들의 동치류로 정의하기도 합니다.



# 36 보렐 측도와 르베그 측도 구성하기

보렐 공간  $\mathcal{B}(\mathbb{R}^n)$  위의 측도를 단번에 정의하는 것은 매우 어렵습니다. 먼저 더 약한 개념을 정의하면 더 쉽습니다. 우리가 정의할 이러한 약한 개념은 두 가지입니다:

- **준측도(pre-measure)**: 측도의 공리를 만족시키지만, 측도보다 더 적은 집합들에 대해 정의됩니다: 이들은 완전한 형태의 “ $\sigma$ -대수”가 아니라 “대수” 위에서 정의될 것입니다.
- **외측도(outer measure)**:  $2^\Omega$  위에서 정의되지만 더 약한 공리를 만족시킵니다.

준측도는 외측도를 낳고, 외측도는 측도를 낳는다는 것이 밝혀질 것입니다.

## §36.1 사전측도

**이 절의 대표적인 예:**  $\Omega = \mathbb{R}^2$ 라고 합시다. 그러면 직사각형들로 생성된  $\mathcal{A}_0$ 을 취하고,  $\mu_0$ 은 일반적인 넓이로 둡니다.

사전측도를 정의하는 방법은  $\sigma$ -대수를 대수로 약화시키는 것입니다.

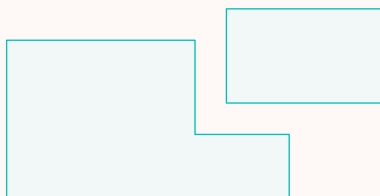
**정의 36.1.1.**  $\Omega$ 를 집합이라고 합시다. **대수**의 개념을 정의하는데, 이는 모든 곳에서 “가산”을 유한으로 바꾼 것을 제외하면  $\sigma$ -대수와 동일합니다.

즉:  $\Omega$  위의 대수  $\mathcal{A}_0$ 란  $2^\Omega$ 의 공집합이 아닌 부분집합으로서, 여집합과 유한 합집합에 대해 닫혀 있는 것입니다. 부분집합  $\mathcal{F} \subseteq 2^\Omega$ 를 포함하는 가장 작은 대수를  **$\mathcal{F}$ 에 의해 생성된 대수**라고 합니다.

실제로 우리는 대수에 대해 기본적으로 항상 생성 방법을 사용할 것입니다.

### 예제 36.1.2

$\Omega = \mathbb{R}^n$ 일 때,  $[a_1, b_1] \times \cdots \times [a_n, b_n]$ 에 의해 생성된 대수를  $\mathcal{L}_0$ 이라 할 수 있습니다. 전형적인 원소는 다음과 같이 생겼을 것입니다:



놀랄 것도 없이, 여기에는 유한개의 직사각형과 그 여집합만 관련되어 있으므로, 이 경우에는 실제로 넓이를 모호함 없이 부여할 수 있으며, 곧 그렇게 할 것입니다.

**정의 36.1.3.** 대수  $\mathcal{A}_0$  위의 **준측도**  $\mu_0$ 란 다음 공리를 만족시키는 함수  $\mu_0: \mathcal{A}_0 \rightarrow [0, +\infty]$ 입니다

- $\mu_0(\emptyset) = 0$ 이고,
- **가산 가법성:**  $A_1, A_2, \dots$ 가  $\mathcal{A}_0$  안의 서로소인 집합들이고 게다가 서로소 합집합  $\bigsqcup A_i$ 가  $\mathcal{A}_0$ 에 포함된다면(이는 대수의 공리에 의해 보장되지 않습니다!), 다음이 성립합니다

$$\mu_0\left(\bigsqcup_n A_n\right) = \sum_n \mu_0(A_n).$$

**예제 36.1.4** ( $\mathbb{R}^n$  위의 준측도)

$\Omega = \mathbb{R}^2$ 이라 합시다. 그러면  $\mathcal{L}_0$ 을 직사각형  $[a_1, a_2] \times [b_1, b_2]$ 에 의해 생성된 대수라 합시다. 이제 다음과 같이 둡니다

$$\mu_0([a_1, a_2] \times [b_1, b_2]) = (a_2 - a_1)(b_2 - b_1)$$

직사각형의 넓이입니다.  $\mathcal{L}_0$ 의 원소들은 단순히 직사각형들과 그 여집합들의 유한 합집합이므로(앞서 그린 그림 참조), 이를 여러분이 예상하는 대로 작동하는 준측도  $\lambda_0$ 으로 확장하는 것은 어렵지 않습니다 — 다만 우리는 이를 실제로 하지는 않을 것입니다.

우리가 개념적으로 중요한 것으로 밝혀질 어떤 것을 카펫 밑으로 쓸어 넣고 있으므로, 나서서 이를 파란 상자로 표시하겠습니다.

**명제 36.1.5** (우리가 증명하지 않을 기하학적 타당성 점검)

$\Omega = \mathbb{R}^n$ 이고  $\mathcal{L}_0$ 이 직육면체에 의해 생성된 대수일 때,  $\mathcal{L}_0$  위에 준측도  $\lambda_0$ 을 정의할 수 있습니다.

이 지점부터는, 측도  $\mathcal{B}(\mathbb{R}^n)$ 을 정의하는 데 있어 기본적으로 거의 어떠한 기하학도<sup>1</sup> 사용하지 않을 것이며, 오직 집합론만을 사용하여 측도를 확장할 것입니다. 따라서 **명제 36.1.5**은 우리의 “초기 정의”가 타당함을 확인하는 유일한 보조입니다.

다른 방식으로 논점을 말하자면, **미친 과학자**<sup>2</sup>가 모든 직사각형이 넓이 1을 갖는 넓이 개념을 정의하려 시도했다고 합시다. 직관적으로 이는 불가능해야 합니다: 모든 직사각형은 두 개의 반쪽으로 나눌 수 있고 우리는  $1 + 1 \neq 1$ 이어야 하기 때문입니다. 그러나 그들을 막을 유일한 것은 그들이 대수  $\mathcal{L}_0$  위의 준측도를 확장할 수 없다는 점입니다. 만약 그들이 어떻게든 그 장벽을 넘어서 준측도를 얻었다면, 이 절의 나머지 부분에서는 그들이 이 성질을 갖는 완전한 진정한 측도를 얻는 것을 막을 것이 아무것도 없습니다. 따라서 르베그 측도를 구성함에 있어, 기하학적 작업의 대부분은 (생략된) **명제 36.1.5**의 증명 안에 담겨 있습니다.

**§36.2 외측도**

**이 절의 대표적인 예:** 계속해서  $\Omega = \mathbb{R}^2$ 로 둡니다; 이어질 그림을 참조하십시오.

측도를 약화시키는 또 다른 방법은 가산 가법성을 완화하는 것이며, 이는 다음을 낳습니다:

**정의 36.2.1.** 집합  $\Omega$  위의 **외측도**(outer measure)  $\mu^*$ 란 다음 공리들을 만족하는 함수  $\mu^*: 2^\Omega \rightarrow [0, +\infty]$ 입니다:

- $\mu^*(\emptyset) = 0$ ;
- $E \subseteq F$ 이고  $E, F \in 2^\Omega$ 이면  $\mu^*(E) \leq \mu^*(F)$ 입니다;
- $\Omega$ 의 임의의 부분집합  $E_1, E_2, \dots$ 에 대해 다음이 성립합니다

$$\mu^*\left(\bigcup_n E_n\right) \leq \sum_n \mu^*(E_n).$$

<sup>1</sup>작은 거짓말입니다. 엄밀히 말하면, **연습문제 36.5.1**에서와 같이  $\mathbb{R}^n$ 의 열린집합이 가산 개의 직사각형으로 덮일 수 있다는 사실을 하나 더 사용할 것입니다. 다만 이 단계는 어떠한 넓이 배정도 포함하지 않습니다.

<sup>2</sup>“매드 사이언티스트”는 과대평가되었으니까요.

(저는 "외측도"라는 단어를 그다지 좋아하지 않는데, 이는 다소 잘못된 명칭이라고 생각하기 때문입니다: 이것 역시 측도가 아니므로 차라리 "가짜 측도"라고 부르고 싶습니다.)

"외측도"라는 이름의 이유는, 거의 항상 집합을 "바깥에서" 근사함으로써 외측도를 얻기 때문입니다. 공식적으로 이 결과는 흔히 다음과 같이 서술됩니다(문제 36A<sup>†</sup>로서).

집합  $\Omega$ 에 대해,  $\mathcal{E}$ 를  $2^\Omega$ 의 임의의 부분집합이라 하고,  $\rho: \mathcal{E} \rightarrow [0, +\infty]$ 를 임의의 함수라 합시다. 그러면

$$\mu^*(E) = \inf \left\{ \sum_{n=1}^{\infty} \rho(E_n) \mid E_n \in \mathcal{E}, E \subseteq \bigcup_{n=1}^{\infty} E_n \right\}$$

는 외측도입니다.

하지만 저는 위 정리를 실제로 사용하기에는 기본적으로 항상 옳지 않다고 생각하는데, 이는 지나치게 일반적이기 때문입니다. 제가 미친 과학자 예시로 경고했듯이, 우리는 정말로  $\rho$ 에 대해 어떤 종류의 정상성(sanity) 조건을 원합니다: 그렇지 않으면, 위 결과를 그대로 적용할 경우  $\mu^*$ 가 어떤 식으로든  $\rho$ 와 호환된다는 보장이 없습니다.

그래서 저는 결과로 얻어지는  $\mu^*$ 가  $\mu_0$ 와 호환된다는 어떤 종류의 보장을 실제로 갖는 전측도(pre-measure)  $\mu_0$ 에 이 정리를 적용하는 것이 정말 더 낫다고 생각합니다. 실제로는, 이것이 항상 우리가 외측도를 구성하고자 하는 방식이 될 것입니다.

### 정리 36.2.2 (전측도로부터 외측도 구성하기)

$\mu_0$ 를 집합  $\Omega$  위의 대수(algebra)  $\mathcal{A}_0$  위의 전측도라 합시다.

(a) 다음과 같이 정의되는 사상  $\mu^*: 2^\Omega \rightarrow [0, +\infty]$ 는

$$\mu^*(E) = \inf \left\{ \sum_{n=1}^{\infty} \mu_0(A_n) \mid A_n \in \mathcal{A}_0, E \subseteq \bigcup_{n=1}^{\infty} A_n \right\}$$

외측도입니다.

(b) 게다가, 이 측도는  $\mathcal{A}_0$ 의 집합들 위에서  $\mu_0$ 와 일치합니다.

직관적으로, 일어나고 있는 일은  $\mu^*(A)$ 가  $\mathcal{A}_0$ 의 원소들의 가산 합집합에 의한  $A$ 의 덮개들의 하한이라는 것입니다. (b) 부분은 제가 약속했던 호환성 조건의 전반부이며; 나머지는 절반은 나중에 **명제 36.3.2**로 등장합니다.

**정리 36.2.2**의 증명. 이미 언급했듯이, (a) 부분은 **문제 36A<sup>†</sup>**의 특수한 경우입니다(그리고 이렇게 일반적인 형태로 증명하는 것이 실제로 더 쉬운데, 불필요한 성질들에 정신이 팔리지 않기 때문입니다).

이제 (b)를 확인해 봅시다, 즉  $A \in \mathcal{A}_0$ 에 대해  $\mu^*(A) = \mu_0(A)$ 임을 확인합니다. 한쪽 부등식은 빠릅니다:

**질문 36.2.3.**  $\mu^*(A) \leq \mu_0(A)$ 임을 보이십시오.

역방향을 위해,  $A \subseteq \bigcup_n A_n$ 이라고 가정합시다. 그러면 다음 집합들을 정의합니다

$$\begin{aligned} B_1 &= A \cap A_1 \\ B_2 &= (A \cap A_2) \setminus B_1 \\ B_3 &= (A \cap A_3) \setminus (B_1 \cup B_2) \\ &\vdots \end{aligned}$$

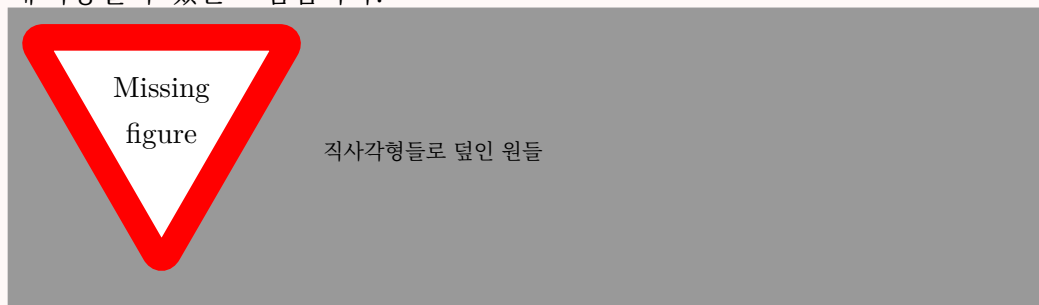
등등입니다. 그러면  $B_n$ 들은  $\mathcal{A}_0$ 의 서로소인 원소들이며  $B_n \subset A_n$ 을 만족하고, 정의를 조작하여  $\bigcup_n B_n = A$ 가 되도록 하였습니다. 따라서 전측도의 정의에 의해,

$$\mu_0(A) = \sum_n \mu_0(B_n) \leq \sum_n \mu_0(A_n)$$

원하는 대로입니다. □

#### 예제 36.2.4

$\Omega = \mathbb{R}^2$ 이고  $\lambda_0$ 을 앞서 나온 전측도라 합시다. 그러면  $\lambda^*(A)$ 는 직관적으로 집합  $A$ 를 직사각형들로 덮는 덮개들의 하한입니다. 다음은  $A$ 가 단위 원판인 상황을 상상하는데 사용할 수 있는 그림입니다.



### §36.3 외측도에 대한 Carathéodory 확장

이제 임의의 외측도를 취하여 이를 제대로 된 측도로 바꾸겠습니다. 이를 위해서는 먼저 측도를 정의할  $\sigma$ -대수를 지정해야 합니다.

**정의 36.3.1.**  $\mu^*$ 를 외측도라고 합시다. 집합  $A$ 가  $\mu^*$ 에 대해 Carathéodory 가측이다, 또는 줄여서  $\mu^*$ -가측이라고 하는 것은 다음 조건이 성립하는 경우를 말합니다: 임의의 집합  $E \in 2^\Omega$ 에 대하여,

$$\mu^*(E) = \mu^*(E \cap A) + \mu^*(E \setminus A).$$

이 정의의 동기를 설명하기는 어렵지만, 결국 옳은 정의임이 밝혀집니다. 동기를 설명하는 한 가지 방법은 다음과 같습니다:  $\mathbb{R}^n$ 에서는 이것이 합리적인 기하학적 조건(명제 36.4.3에서 서술할 것입니다)과 동치임이 밝혀지지만, 그 기하학적 정의는  $\mathbb{R}^n$  자체에 대한 정보를 필요로 하므로, 이것이 일반적인 측도 공간에 대한 "올바른" 일반화입니다.

우리의 목표가  $\mathcal{A}_0$ 를 확장하는 것이었으므로, 이 정의가 우리가 처음 시작했던 집합들을 측정할 수 있게 해주는지 반드시 확인해야 합니다!

#### 명제 36.3.2 (Carathéodory 가측성은 초기 $\mathcal{A}_0$ 와 호환됩니다)

$\mu^*$ 가 정리 36.2.2에서처럼 대수  $\mathcal{A}_0$  위의 전측도  $\mu_0$ 로부터 얻어졌다고 합시다. 그러면  $\mathcal{A}_0$ 의 모든 집합은  $\mu^*$ -가측입니다.

이는 초기  $\mu_0$ 가 적어도 전측도 공리를 만족하도록 하면 얻어지는 호환성 조건의 후반부입니다. (전반부는 정리 36.2.2의 (b)였습니다.)

**증명.**  $A \in \mathcal{A}_0$ 이고  $E \in 2^\Omega$ 라고 합시다; 우리는  $\mu^*(E) = \mu^*(E \cap A) + \mu^*(E \setminus A)$ 를 증명하고자 합니다. 외측도의 정의는 이미  $\mu^*(E) \leq \mu^*(E \cap A) + \mu^*(E \setminus A)$ 를 요구하므로, 역부등식만 증명하면 충분합니다.

하한의 정의에 의해, 임의의  $\varepsilon > 0$ 에 대해,  $\mu^*(E) + \varepsilon \geq \sum_n \mu_0(A_n)$ 을 만족하는 덮개  $E \subset \bigcup_n A_n$ 가 존재합니다. 그러나

$$\sum_n \mu_0(A_n) = \sum_n (\mu_0(A_n \cap A) + \mu_0(A_n \setminus A)) \geq \mu^*(E \cap A) + \mu^*(E \setminus A)$$

이며, 첫 번째 등식은  $\mathcal{A}_0$  위의 전측도 정의에 의한 것이고, 두 번째는 단지  $\mu^*$ 의 정의에 의한 것입니다(예를 들어  $A_n \cap A$ 가 확실히  $E \cap A$ 를 덮으므로). 따라서  $\mu^*(E) + \varepsilon \geq \mu^*(E \cap A) + \mu^*(E \setminus A)$ 입니다. 이 부등식이 임의의  $\varepsilon > 0$ 에 대해 성립하므로, 증명이 끝났습니다.  $\square$

케이크 위에 추가로 장식을 올리자면, 여기 우리가 구성한 측도가 우연히 만족하게 될 또 하나의 좋은 조건이 있습니다.

**정의 36.3.3.** 측도 공간  $(\Omega, \mathcal{A}, \mu)$ 의 **영집합**이란  $\mu(A) = 0$ 을 만족하는 집합  $A \in \mathcal{A}$ 입니다. 측도 공간  $(\Omega, \mathcal{A}, \mu)$ 는  $A$ 가 영집합일 때마다  $A$ 의 모든 부분집합 역시  $\mathcal{A}$ 에 속하는(따라서 영집합이 되는) 경우 **완비**라고 합니다.

이는 명백한 이유로 가지고 있으면 좋은 성질입니다. 시각적으로 보면, 제가 무게 0을 이미 부여한 면지 한 무더기를 가지고 있고, 그중 일부를 붙어서 날려버린다면, 남은 면지에도 여전히 부여된 무게 — 0 — 이 있어야 합니다. 확장 정리는 이러한 성질을 갖는  $\sigma$ -대수를 우리에게 제공할 것입니다.

#### 정리 36.3.4 (외측도에 대한 Carathéodory 확장 정리)

$\mu^*$ 가 외측도이고,  $\mathcal{A}^{\text{cm}}$ 가  $\mu^*$ 에 대해  $\mu^*$ -가측인 집합들의 모임이라면,  $\mathcal{A}^{\text{cm}}$ 는  $\Omega$  위의  $\sigma$ -대수이며,  $\mu^*$ 를  $\mathcal{A}^{\text{cm}}$ 로 제한한  $\mu^{\text{cm}}$ 는 완비 측도 공간을 이룹니다.

(발음 관련 첨언: 위첨자 <sup>cm</sup>는 "Carathéodory 가측(measurable)" 또는 "완비(complete)"를 나타낸다고 생각할 수 있습니다. 둘 다 이 표기가 무엇을 나타내는지 기억하는 데 도움이 됩니다. 이 표기법은 표준은 아니지만, 말장난이 너무 좋아서 참을 수 없었습니다.)

따라서 정리 36.2.2와 정리 36.3.4를 합성하면, 대수  $\mathcal{A}_0$  위의 모든 전측도  $\mu_0$ 는 완비 측도  $\mu^{\text{cm}}$ 를 갖는  $\sigma$ -대수  $\mathcal{A}^{\text{cm}}$ 를 자연스럽게 만들어내며, 우리의 두 호환성 결과(즉 정리 36.2.2의 (b)와 명제 36.3.2)는  $\mathcal{A}^{\text{cm}} \supset \mathcal{A}_0$ 이고  $\mu^{\text{cm}}$ 가  $\mu_0$ 와 일치함을 의미합니다.

다음은 이 과정을 보여주는 표로서, 표의 각 행을 따라 내려가는 것이 제한 과정에 대응합니다.

|                           |                   | 순서 구성 | 참고사항                                                                                                     |
|---------------------------|-------------------|-------|----------------------------------------------------------------------------------------------------------|
| $2^\Omega$                | $\mu^*$           | 2단계   | $\mu^*$ 는 $\mu_0$ 로부터 얻어진 외측도입니다                                                                         |
| $\mathcal{A}^{\text{cm}}$ | $\mu^{\text{cm}}$ | 3단계   | $\mathcal{A}^{\text{cm}}$ 는 $\mu^*$ -가측 집합들로 정의되며, $(\mathcal{A}^{\text{cm}}, \mu^{\text{cm}})$ 는 완비입니다. |
| $\mathcal{A}_0$           | $\mu_0$           | 1단계   | $\mu_0$ 는 준측도입니다                                                                                         |

## §36.4 르베그 측도 정의하기

이로써 마침내  $\mathbb{R}^n$  위의 르베그 측도를 정의할 수 있습니다. 이제 모든 것을 한 번에 종합해 보겠습니다.

**정의 36.4.1.** 다음 절차에 따라  $\mathbb{R}^n$  위의 측도를 만듭니다.

- 직육면체들이 생성하는 대수  $\mathcal{L}_0$ 에서 시작하여, 이  $\mathcal{L}_0$  위에 전측도  $\lambda_0$ 를 정의합니다 (이는 예시에서 대충 넘어갔던 부분입니다).

- 정리 36.2.2에 의해, 이는  $2^{\mathbb{R}^n}$  위의 **르베그 외측도**  $\lambda^*$ 를 주며, 이는 모든 직육면체에 대해 호환됩니다.
- Carathéodory에 의해(정리 36.3.4), 이는  $\lambda^*$ -가측 집합들의  $\sigma$ -대수  $\mathcal{L}(\mathbb{R}^n)$  위의 완비 측도  $\lambda$ 로 제한되며(약속한 대로 모든 직사각형 상자를 포함합니다).<sup>3</sup>

그 결과로 얻어지는 완비 측도는  $\lambda$ 로 표기하며, **르베그 측도**라고 부릅니다.

우리가 얻은 대수  $\mathcal{L}(\mathbb{R}^n)$ 는 **르베그  $\sigma$ -대수**라고 부를 것이며, 이에 속하는 집합들은 **르베그 가측**이라고 합니다.

다음은 특수한 경우  $\Omega = \mathbb{R}^n$ 에 대해 값을 채워 넣은, 앞서 본 것과 동일한 표이며, 이는 우리에게 르베그 대수를 제공합니다.

|                             |             | 순서 구성 | 주해                       |
|-----------------------------|-------------|-------|--------------------------|
| $2^{\mathbb{R}^n}$          | $\lambda^*$ | 2단계   | $\lambda^*$ 는 르베그 외측도입니다 |
| $\mathcal{L}(\mathbb{R}^n)$ | $\lambda$   | 3단계   | 르베그 $\sigma$ -대수(완비)     |
| $\mathcal{L}_0$             | $\lambda_0$ | 1단계   | 직사각형에 대한 사전측도 정의         |

물론 여기까지 온 이상, 실제로 어떤 측도를 계산하고자 한다면 측도를 실제로 어떻게 구성했는지는 대체로 기꺼이 잊어버리고 그 성질들만 사용하면 됩니다. 어려운 부분은 측도를 일관되게 부여하는 방법이 존재한다는 것을 보이는 것이었습니다. 그 측도의 값이 존재한다는 것을 전제로 실제로 그 값을 알아내는 것은 대체로 훨씬 쉽습니다. 여기 하나의 예가 있습니다.

#### 예제 36.4.2 (칸토어 집합은 측도 0입니다)

표준적인 **중간 삼분의 일 칸토어 집합**은 다음과 같이 얻어지는  $[0, 1]$ 의 부분집합입니다: 먼저 열린구간  $(1/3, 2/3)$ 을 제거합니다. 그러면 두 구간  $[0, 1/3]$ 과  $[2/3, 1]$ 이 남으며, 이 둘에서 다시 각각의 가운데 삼분의 일을 제거합니다. 즉  $(1/9, 2/9)$ 과  $(7/9, 8/9)$ 을 제거합니다. 이 과정을 무한히 반복하고 그 결과를  $C$ 라고 합니다. 아래에 그림이 나와 있습니다.



[1207]에서 가져온 이미지입니다

$C$ 가 비가산이라는 것은 고전적인 사실입니다(이는 숫자 1을 배제한 삼진 전개들로 이루어져 있습니다). 하지만 이는 가측이며(닫힌집합들의 교집합이기 때문입니다!), 우리는 이것이 측도 0을 가진다고 주장합니다. 실제로  $n$ 번째 단계에서 그 결과는  $(2/3)^n$ 의 측도가 남아 있습니다. 따라서 모든  $n$ 에 대해  $\mu(C) \leq (2/3)^n$ 이므로  $\mu(C) = 0$ 이 강제됩니다.

훌륭하지만, 방 안의 코끼리가 하나 있습니다: 르베그  $\sigma$ -대수와 보렐  $\sigma$ -대수는 어떻게 관련되어 있을까요? 이 질문에 간단히 답하기 위해, 저는 두 가지 결과를 서술하겠습니다(다만 다른 답은 다음 절에서 주어집니다). 첫 번째는 기이한 Carathéodory 가측 가정에 대한 기하학적 해석입니다.

<sup>3</sup>앞선 정리들과의 일관성을 위해서라면, 강조를 위해  $\mathcal{L}^{\text{cm}}$ 와  $\lambda^{\text{cm}}$ 로 표기하는 편을 선호했을 것입니다. 하지만 아무도 그렇게 하지 않는 것 같으므로, 저도 그렇게 하지 않았습니다.

**명제 36.4.3** (르베그 가측성에 대한 기하학적 해석)

집합  $A \subseteq \mathbb{R}^n$ 가 르베그 가측일 필요충분조건은 모든  $\varepsilon > 0$ 에 대해 다음을 만족하는 열린집합  $U \supset A$ 가 존재하는 것입니다

$$\lambda^*(U \setminus A) < \varepsilon$$

여기서  $\lambda^*$ 는 르베그 외측도입니다.

이것이 르베그의 원래 "가측"의 정식화였다고 말하고 싶지만, 확실하지는 않습니다. 어쨌든 우리는 이를 사용할 필요는 없지만, 우리의 르베그 가측 정의가 소박한 기하학적 해석을 갖는다는 것을 보는 것은 좋습니다.

**질문 36.4.4.** 모든 열린집합이 르베그 가측임을 유도하십시오. 르베그  $\sigma$ -대수가 보렐  $\sigma$ -대수를 포함함을 결론지으십시오. (다른 증명이 뒤에서 주어집니다.)

그러나 이 포함관계는 진부분집합 관계입니다: 보렐 가측 집합보다 르베그 가측 집합이 더 많습니다. 실제로 (여기서는 다루지 않겠지만) 초한 귀납법을 사용하여  $|\mathcal{B}(\mathbb{R})| = |\mathbb{R}|$ 임을 증명할 수 있습니다.<sup>4</sup> 이를 이용하면 다음을 얻습니다:

**연습문제 36.4.5.** 보렐  $\sigma$ -대수가 완비가 아님을 보이십시오. (힌트: 칸토어 집합을 고려하십시오. 비가측 집합의 예를 직접 적어낼 수는 없겠지만, 기수 논증을 사용할 수 있습니다.) 따라서 르베그  $\sigma$ -대수는 보렐  $\sigma$ -대수를 진부분집합으로서 포함합니다.

그럼에도 불구하고, 완비성이라는 개념을 이용하여 르베그  $\sigma$ -대수를 기술하는 훌륭한 방법이 있습니다.

**정의 36.4.6.**  $(\Omega, \mathcal{A}, \mu)$ 를 측도 공간이라고 합시다. **완비화**  $(\Omega, \overline{\mathcal{A}}, \overline{\mu})$ 는 다음과 같이 정의됩니다: 우리는 다음과 같이 둡니다

$$\overline{\mathcal{A}} = \{A \cup N \mid A \in \mathcal{A}, N \text{ 영집합의 부분집합}\}.$$

그리고  $\overline{\mu}(A \cup N) = \mu(A)$ 라고 둡니다. 이것이 잘 정의되어 있음을 확인할 수 있으며, 실제로  $\overline{\mu}$ 는  $\mu$ 를  $\mathcal{A}$ 에서  $\overline{\mathcal{A}}$ 로 확장한 유일한 확장입니다.

이것은 실제보다 더 복잡해 보입니다. 직관적으로, 우리가 하고 있는 일은 영집합의 임의의 부분집합 역시 측도 영을 갖는 것으로 간주하도록  $\overline{\mu}$ 에게 알려줌으로써 측도를 "완비화"하는 것입니다.

그러면, 구원의 손길은:

**정리 36.4.7** (르베그는 보렐의 완비화입니다)

$\mathbb{R}^n$ 에 대해, 르베그 측도는 보렐 측도의 완비화입니다.

증명. 이는 사실 다음 절의 결과, 즉 **연습문제 36.5.1**과 준측도에 대한 Carathéodory 정리의 (c) 부분(**정리 36.5.5**)으로부터 따라 나옵니다.  $\square$

## §36.5 네 번째 행: 준측도에 대한 Carathéodory 정리

**이 절의 대표적인 예:** 르베그 측도에 대한 네 번째 행은  $\mathcal{B}(\mathbb{R}^n)$ 입니다.

<sup>4</sup>개략적인 설명은 <https://math.stackexchange.com/a/70891>을 참고하십시오.

많은 경우,  $\mathcal{A}^{\text{cm}}$ 는 실제로 우리의 원래 목표보다 더 크며, 대신 우리는  $\mathcal{A}_0$  위의  $\mu_0$ 를  $\mathcal{A}$  위의  $\mu$ 로 확장하기만 하면 됩니다. 여기서  $\mathcal{A}$ 는  $\mathcal{A}_0$ 에 의해 생성된  $\sigma$ -대수입니다. 실제로, 우리의 원래 목표는  $\mathcal{B}(\mathbb{R}^n)$ 를 얻는 것이었으며, 사실상:

**연습문제 36.5.1.**  $\mathcal{B}(\mathbb{R}^n)$ 가 앞서 정의한  $\mathcal{L}_0$ 에 의해 생성된  $\sigma$ -대수임을 보이십시오.

다행히도, 이 제한은 하기가 자명합니다.

**질문 36.5.2.**  $\mathcal{A}^{\text{cm}} \supset \mathcal{A}$ 임을 보이십시오. 따라서 우리는  $\mu^{\text{cm}}$ 를 그냥  $\mathcal{A}$ 로 제한하면 됩니다.

우리는 잠시 후 이것을 우리 표의 네 번째 행으로 추가할 것입니다.

하지만 이것이 최종 목표라면, 종종 하나 더 좋은 성질이 성립하기 때문에 다소 다른 카라테오도리(Carathéodory) 정리를 서술할 수 있습니다:

**정의 36.5.3.**  $\Omega$  위의 준측도 또는 측도  $\mu$ 는,  $\Omega$ 가 각  $n$ 에 대해  $\mu(A_n) < \infty$ 를 만족하는 가산 합집합  $\Omega = \bigcup_n A_n$ 으로 쓰일 수 있을 때  **$\sigma$ -유한**이라고 합니다.

**질문 36.5.4.** 우리가 가지고 있던 준측도  $\lambda_0$ 뿐만 아니라 보렐 측도  $\mathcal{B}(\mathbb{R}^n)$ 도 둘 다  $\sigma$ -유한임을 보이십시오.

사실, 우리에게는  $\sigma$ -유한이 기본적으로 항상 성립할 것이므로, 여러분은 대체로 이를 그냥 당연한 것으로 받아들이셔도 됩니다.

#### 정리 36.5.5 (예측도에 대한 카라테오도리(Carathéodory) 확장 정리)

$\mu_0$ 를  $\Omega$ 의 대수  $\mathcal{A}_0$  위의 준측도라 하고,  $\mathcal{A}$ 를  $\mathcal{A}_0$ 에 의해 생성된  $\sigma$ -대수라 합시다.  $\mathcal{A}^{\text{cm}}$ ,  $\mu^{\text{cm}}$ 를 정리 36.3.4에서와 같다고 합시다. 그러면:

- (a)  $\mathcal{A}$ 로 제한된  $\mu^{\text{cm}}$ 는  $\mu_0$ 를 확장하는 측도  $\mu$ 를 줍니다.
- (b)  $\mu_0$ 가  $\sigma$ -유한이었다면,  $\mu$ 는  $\mu_0$ 의  $\mathcal{A}$ 로의 유일한 확장입니다.
- (c)  $\mu_0$ 가  $\sigma$ -유한이었다면,  $\mu^{\text{cm}}$ 는  $\mu$ 의 완비화이며, 따라서  $\mu_0$ 의  $\mathcal{A}^{\text{cm}}$ 로의 유일한 확장입니다.

다음은  $\mu_0$ 가 실제로  $\sigma$ -유한이었을 경우의 설명이 달린, 갱신된 표입니다.

|                           |                   | 순서 구성 | 주해                                                                                                                               |
|---------------------------|-------------------|-------|----------------------------------------------------------------------------------------------------------------------------------|
| $2^\Omega$                | $\mu^*$           | 2단계   | $\mu^*$ 는 $\mu_0$ 로부터 얻어진 외측도입니다                                                                                                 |
| $\mathcal{A}^{\text{cm}}$ | $\mu^{\text{cm}}$ | 3단계   | $(\mathcal{A}^{\text{cm}}, \mu^{\text{cm}})$ 는 $(\mathcal{A}, \mu)$ 의 완비화입니다, $\mathcal{A}^{\text{cm}}$ 는 $\mu^*$ -가측 집합들로 정의됩니다 |
| $\mathcal{A}$             | $\mu$             | 4단계   | $\mathcal{A}$ 는 $\mathcal{A}_0$ 에 의해 생성된 $\sigma$ -대수로 정의됩니다                                                                     |
| $\mathcal{A}_0$           | $\mu_0$           | 1단계   | $\mu_0$ 는 전측도입니다                                                                                                                 |

그리고 다음은 보렐과 르베그가 포함된,  $\Omega = \mathbb{R}^n$ 에 대한 표입니다.

|                             |             | 순서 구성 | 주해                                        |
|-----------------------------|-------------|-------|-------------------------------------------|
| $2^{\mathbb{R}^n}$          | $\lambda^*$ | 2단계   | $\lambda^*$ 는 르베그 외측도입니다                  |
| $\mathcal{L}(\mathbb{R}^n)$ | $\lambda$   | 3단계   | 르베그 $\sigma$ -대수, 보렐 $\sigma$ -대수의 완비화    |
| $\mathcal{B}(\mathbb{R}^n)$ | $\mu$       | 4단계   | 보렐 $\sigma$ -대수, $\mathcal{L}_0$ 에 의해 생성됨 |
| $\mathcal{L}_0$             | $\lambda_0$ | 1단계   | 직사각형에 대한 사전 측도 정의                         |

표의 한 행을 내려가는 것은 제한에 대응하며,  $\mu_0 \rightarrow \mu \rightarrow \mu^{\text{cm}}$ 의 각 단계는  $\mu_0$ 가  $\sigma$ -유한일 때 유일한 확장입니다.

**정리 36.5.5**의 증명. (a)에 대해: 이는 단지 **정리 36.2.2**와 **정리 36.3.4**를 결합한 것으로,  $\mathcal{A}^{\text{cm}} \supset \mathcal{A}_0$ 이며 따라서  $\mathcal{A}^{\text{cm}} \supset \mathcal{A}$ 라는 관찰과 결합됩니다. (b)와 (c) 부분은 더 기술적이므로 생략합니다.  $\square$

## §36.6 지금부터, 우리는 보렐 측도를 가정합니다

그 이유를 설명하십시오

## §36.7 생각해 볼 만한 조금 더 어려운 문제

**문제 36A<sup>†</sup>** (임의의  $\rho$ 로부터 외측도 구성하기). 집합  $\Omega$ 에 대해,  $\mathcal{E}$ 를  $2^\Omega$ 의 임의의 부분집합이라 하고  $\rho: \mathcal{E} \rightarrow [0, +\infty]$ 를 임의의 함수라 합시다. 다음을 증명하십시오

$$\mu^*(E) = \inf \left\{ \sum_{n=1}^{\infty} \rho(E_n) \mid E_n \in \mathcal{E}, E \subseteq \bigcup_{n=1}^{\infty} E_n \right\}$$

은 외측도입니다.

**문제 36B** (미친 과학자).  $\Omega = \mathbb{R}^2$ 라 하고,  $\mathcal{E}$ 를 (퇴화하지 않은) 직사각형의 집합이라 합시다. 모든 직사각형  $E \in \mathcal{E}$ 에 대해  $\rho(E) = 1$ 이라 합시다. 저의 조언을 무시하고, 그 미친 과학자는 **문제 36A<sup>†</sup>**에서와 같이  $\rho$ 를 사용하여 외측도  $\mu^*$ 를 구성합니다.

(a)  $\mathbb{R}^2$ 의 각 부분집합  $S$ 에 대해  $\mu^*(S)$ 를 구하십시오.

(b) 어떤 집합들이  $\mu^*$ -가측입니까?

어떤 직사각형도  $\mu^*$ -가측이 아니라는 것을 알게 될 것이며, 이는 놀랍지 않게도 그 과학자를 좌절시킵니다.



**문제 36C.** 함수  $f: \mathbb{R} \rightarrow \mathbb{R}$ 가 연속이라고 합시다.  $f$ 는  $\mathbb{R}$  위의 르베그 측도에 대해 반드시 가측이어야 합니까?



# 37 르베그 적분

임의의 측도 공간  $(\Omega, \mathcal{A}, \mu)$  위에서, 함수  $f: \Omega \rightarrow [0, \infty]$ 에 대해 적분을 정의할 수 있습니다

$$\int_{\Omega} f \, d\mu.$$

이 적분은 (설령  $f$ 가 유한하더라도)  $+\infty$ 일 수 있습니다. 구성의 세부 사항은 나중에 우리에게 중요하지 않으므로, 관련된 정의들만 서술하고 모든 증명은 생략하며, 실제로 필요한 성질들만 서술하겠습니다. 따라서 이 장은 상당히 짧을 것입니다.

## §37.1 정의

구성은 네 단계로 이루어집니다.

**정의 37.1.1.**  $A$ 가  $\Omega$ 의 가측 집합이면, **지시함수**  $\mathbf{1}_A: \Omega \rightarrow \mathbb{R}$ 는 다음과 같이 정의됩니다

$$\mathbf{1}_A(\omega) = \begin{cases} 1 & \omega \in A \\ 0 & \omega \notin A. \end{cases}$$

**단계 1 (지시함수)** — 지시함수에 대해서는 다음을 요구합니다

$$\int_{\Omega} \mathbf{1}_A \, d\mu := \mu(A)$$

(무한대일 수 있습니다.)

이제 이를 지시함수들의 합인 음이 아닌 함수들로 선형적으로 확장합니다: 이러한 함수들을 **단순함수**라고 부릅니다.

**단계 2 (단순함수)** —  $A_1, \dots, A_n$ 을 유한 개의 가측 집합들의 모임이라 합시다.  $c_1, \dots, c_n$ 을 음이 아닌 실수 또는  $+\infty$ 라 합시다. 그러면 다음과 같이 정의합니다

$$\int_{\Omega} \left( \sum_{i=1}^n c_i \mathbf{1}_{A_i} \right) d\mu := \sum_{i=1}^n c_i \mu(A_i).$$

$c_i = \infty$ 이고  $\mu(A_i) = 0$ 이면,  $c_i \mu(A_i) = 0$ 으로 취급합니다.

이렇게 얻은 합이 단순 함수를  $\sum c_i \mathbf{1}_{A_i}$ 로 나타내는 표현에 의존하지 않음을 확인할 수 있습니다. 특히, 이는 이전 단계와 호환됩니다.

편리하게도, 이것만으로 이미  $f: \Omega \rightarrow [0, +\infty]$ 에 대한 적분을 정의하기에 충분합니다.  $[0, +\infty]$ 는 우리가 통상적으로 사용하는 열린 구간들의 기저에 각 실수  $a$ 에 대한 새로운 열린 집합  $(a, +\infty]$ 를 추가한 위상 공간으로 생각할 수 있음에 유의하십시오. 따라서 여기에 보렐  $\sigma$ -대수를 부여할 수 있습니다.<sup>1</sup>

<sup>1</sup>여기에 측도를 정의해 볼 수도 있겠지만, 그렇게 하지는 않을 것입니다: 우리에게는 이것이 가측 공간이라는 사실만으로 충분합니다.

**단계 3 (음이 아닌 함수)** — 각 가측 함수  $f: \Omega \rightarrow [0, +\infty]$ 에 대해, 다음과 같이 둡니다

$$\int_{\Omega} f \, d\mu := \sup_{0 \leq s \leq f} \left( \int_{\Omega} s \, d\mu \right)$$

여기서 상한은  $0 \leq s \leq f$ 를 만족하는 모든 단순  $s$ 에 대해 취합니다. 이전과 마찬가지로, 이 적분은  $+\infty$ 일 수 있습니다.

즉,

**우리는 적분을 계산하는 방법을 알고 있는 단순함수들로 아래쪽에서 근사함으로써 적분  $\int_{\Omega} f \, d\mu$ 를 정의합니다.**

이것이 이전 정의들과 부합함을 확인할 수 있습니다. 이 시점에서, 중요한 용어를 하나 도입하겠습니다.

**정의 37.1.2.** 가측 (음이 아닌) 함수  $f: \Omega \rightarrow [0, +\infty]$ 가  $\int_{\Omega} f \, d\mu < \infty$ 를 만족하면, 이를 **절대적분가능** 또는 그냥 **적분가능**하다고 합니다.

주의: 저는 "적분가능"이라는 용어가 정말로 혼란스럽다고 생각합니다. 실제로,  $\Omega$ 에서  $[0, +\infty]$ 로 가는 모든 가측 함수에는 르베그 적분을 부여할 수 있으며, 다만 이 적분이  $+\infty$ 일 수 있을 뿐입니다. 따라서 이 정의는 이름이 시사하는 것보다 훨씬 더 엄격합니다. 상수함수조차도 적분가능하지 않을 수 있습니다:

**예제 37.1.3** (사실은 "유한적분가능"이라고 불러야 합니다)

상수함수 1은  $\mathbb{R}$  위에서 적분가능하지 않습니다, 왜냐하면  $\int_{\mathbb{R}} 1 \, d\mu = \mu(\mathbb{R}) = +\infty$ 이기 때문입니다.

이러한 이유로, 저는 대체로 "절대적분가능"이라는 용어를 선호할 것입니다. (만약 제 마음대로 할 수 있다면, "유한적분가능"이라고 부를 것이며, 개인적으로는 보통 그렇게 부릅니다.)

**비고 37.1.4** (적분을 위쪽에서 근사하지 않는 이유는 무엇인가?) —  $|\Omega| < \infty$ 인 측도 공간 위의 유계 함수에 대해서는, 다음과 같이 동등하게 정의할 수 있습니다

$$\int_{\Omega} f \, d\mu := \inf_{0 \leq f \leq s} \left( \int_{\Omega} s \, d\mu \right)$$

여기서 하한은  $f \leq s$ 를 만족하는 모든 단순  $s$ 에 대해 취합니다. 그러나 함수가 유계가 아니거나  $|\Omega| = \infty$ 인 경우, 상황은 그렇게 간단하지 않습니다:

- $\Omega = (1, \infty)$  위에서 정의된 함수  $f(x) = x^{-2}$ 는 절대 적분 가능하지만,  $f \leq s$ 인 모든 단순 함수  $s$ 에 대해  $\int_{\Omega} s \, d\mu = \infty$ 입니다.
- $\Omega = (0, 1)$  위에서 정의된 함수  $f(x) = x^{-0.5}$ 는 절대 적분 가능하지만,  $f \leq s$ 이고  $s$ 가 거의 모든 곳에서 유한한 단순 함수  $s$ 는 존재하지 않습니다.

마지막으로, 이를 통해 일반적인 함수를 적분할 수 있습니다.

**정의 37.1.5.** 일반적으로, 가측 함수  $f: \Omega \rightarrow [-\infty, \infty]$ 는  $|f|$ 가 그러할 때 **절대 적분 가능**하다 또는 단순히 **적분 가능**하다고 합니다.

첫 번째 단어를 사용할 것이므로 이는 기억하기 쉽습니다: "절대 적분 가능"은 절댓값을 취할 것을 요구합니다.

**단계 4 (절대 적분 가능 함수)** —  $f: \Omega \rightarrow [-\infty, \infty]$ 가 절대 적분 가능하다면, 다음과 같이 정의합니다

$$f^+(x) = \max\{f(x), 0\}$$

$$f^-(x) = \min\{f(x), 0\}$$

그리고 다음과 같이 둡니다

$$\int_{\Omega} f \, d\mu = \int_{\Omega} |f^+| \, d\mu - \int_{\Omega} |f^-| \, d\mu$$

이는 특히 유한합니다.

그렇긴 하지만, 여기서 이를 "유한 적분 가능"이라고 부르는 것도 마찬가지로 기억하기 쉬울 것입니다:

**연습문제 37.1.6.**  $\int_{\Omega} |f| \, d\mu < \infty$ 인 것과  $\int_{\Omega} |f^+| \, d\mu < \infty$ 이고  $\int_{\Omega} |f^-| \, d\mu < \infty$ 인 것이 동치임을 보이십시오.

여러분은 이미 우리가 음이 아닌 함수를 정말 좋아한다는 것을 눈치채기 시작했을지도 모릅니다: 측도 이론을 사용하면 그러한 함수를 적분하는 것이 가능하고, 심지어  $+\infty$ 를 아무 데나 집어넣어도 괜찮습니다. 하지만 양수도 될 수 있고 음수도 될 수 있는 함수를 다루기 시작하면, 유한성 제약을 추가해야 합니다 — 실제로 우리가 본질적으로 하고 있는 일은 함수를 양의 부분과 음의 부분으로 나누어, 둘 다 유한할 것을 요구한 다음 적분하는 것입니다.

이 절을 마무리하기 위해, 완결성을 위해 여러분이 아마 참이라고 짐작했을 몇 가지 결과를 서술합니다.  $\Omega = (\Omega, \mathcal{A}, \mu)$ 를 고정하고,  $f$ 와  $g$ 를 가측인 실숫값 함수라 합시다.

- (거의 모든 곳에서의 보존)  $f(x) = g(x)$ 가 거의 모든 곳에서 성립하면,  $f$ 가 절대 적분 가능한 것과  $g$ 가 절대 적분 가능한 것은 동치이며, 그럴 경우 둘의 르베그 적분값은 일치합니다.
- (가법성)  $f$ 와  $g$ 가 절대 적분 가능하다면

$$\int_{\Omega} f + g \, d\mu = \int_{\Omega} f \, d\mu + \int_{\Omega} g \, d\mu.$$

$f$ 와  $g$ 가 음이 아니라면 "절대 적분 가능" 가정은 제외할 수 있습니다.

- (스칼라배)  $f$ 가 절대 적분 가능하고  $c \in \mathbb{R}$ 이면  $cf$ 는 절대 적분 가능하며

$$\int_{\Omega} cf \, d\mu = c \int_{\Omega} f \, d\mu.$$

$f$ 가 음이 아니고  $c > 0$ 이라면 "절대 적분 가능" 가정은 제외할 수 있습니다.

- (단조성)  $f$ 와  $g$ 가 절대 적분 가능하고  $f \leq g$ 이면

$$\int_{\Omega} f \, d\mu \leq \int_{\Omega} g \, d\mu.$$

$f$ 와  $g$ 가 음이 아니라면 "절대 적분 가능" 가정은 제외할 수 있습니다.

단조/지배 수렴 정리와 같이 더 유명한 결과들도 참이지만, 확률론의 맥락에서는 실제로 쓸 일이 없을 것이므로 여기서는 서술하지 않겠습니다. (이 결과들은 나중에 보너스 장에서 등장합니다.)

## §37.2 동치인 정의

르베그 적분은 다음과 같이도 정의할 수 있는데 — 이는 우리가 그 단계들에서 내린 다양한 정의상의 선택에 대해 더 직관적일 것입니다.

이 정의에서,

**적분  $\int_{\Omega} f \, d\mu$ 는 단지  $f$ 의 그래프 아래 영역의 부피일 뿐입니다.**

정의해 봅시다:

**단계 1 (그래프 아래 영역)** — 음이 아닌 함수  $f: \Omega \rightarrow \mathbb{R}$ 에 대해, **함수 아래 영역**  $f, R(f)$ 를  $\{(x, y) \in \Omega \times \mathbb{R}, 0 \leq y \leq f(x)\}$ 로 정의합니다.

**비고 37.2.1** — 왜 처음에는 음이 아닌 함수에 대해서만 이를 정의하는지는 분명할 것입니다 — 일반적인 함수  $f$ 에 대해서는, 영역을 합리적으로 정의할 수 있는 유일한 방법이 다음과 같은 것뿐이기 때문입니다:

$$R^+(f) = \{(x, y) \in \Omega \times \mathbb{R}, f(x) \geq 0, 0 \leq y \leq f(x)\},$$

$$R^-(f) = \{(x, y) \in \Omega \times \mathbb{R}, f(x) \leq 0, 0 \geq y \geq f(x)\}.$$

그럼에도 불구하고,  $R^+(f)$ 는 단순히 함수  $f^+(x) = \max\{f(x), 0\}$  아래의 영역이며,  $R^-(f)$ 는 함수  $f^-(x) = \min\{f(x), 0\}$  아래 영역과 같은 측도를 가짐에 주목하십시오. 따라서 음이 아닌 함수에 대해  $\int_{\Omega} f \, d\mu$ 를 먼저 정의하는 것이 실제로 정의를 더 단순하게 만듭니다.

**단계 2 ( $\Omega \times \mathbb{R}$ 를 측도 공간으로 만들기)** —  $\Omega \times \mathbb{R}$  위에 다음과 같은 자명한 방식으로 준측도를 정의합니다:  $X \subseteq \Omega$ 와  $Y \subseteq \mathbb{R}$ 가 각각 가측 부분집합이라면,  $|X \times Y| = |X| \times |Y|$ 로 지정합니다.

이 준측도는, 앞 장에서 했던 것처럼, 측도로 확장될 수 있습니다.

**단계 3 (음이 아닌 함수)** — 함수  $f: \Omega \rightarrow [0, +\infty]$  각각에 대해, 다음과 같다고 합시다

$$\int_{\Omega} f \, d\mu := |R(f)|.$$

이 적분은  $R(f)$ 가 가측일 때마다 잘 정의됩니다.

**절 35.7**에서 약속했듯이, 가측 함수의 정의는 다음을 만족합니다:

**음이 아닌 함수  $f$ 가 가측인 것과  $f$ 의 그래프 아래 영역을 "측정"할 수 있는 것은 동치입니다.**

마지막 단계는 앞 절에서와 정확히 동일합니다.

**단계 4 (절대 적분가능한 함수)** —  $f: \Omega \rightarrow [-\infty, \infty]$ 가 절대 적분가능하다면, 다음과 같이 정의합니다

$$\int_{\Omega} f \, d\mu = \int_{\Omega} |f^+| \, d\mu - \int_{\Omega} |f^-| \, d\mu.$$

### §37.3 리만 적분과의 관계 (또는: 실제로 르베그 적분 계산하기)

닫힌 구간의 경우, 이는 실제로 아무런 수정 없이 그대로 작동합니다.

#### 정리 37.3.1 (르베그 적분은 리만 적분을 일반화한다)

$f: [a, b] \rightarrow \mathbb{R}$ 를 리만 적분가능한 함수라고 합시다 (여기서  $[a, b]$ 에는 보렐 측도가 주어져 있습니다). 그러면  $f$ 는 또한 르베그 적분가능하며 두 적분값은 일치합니다:

$$\int_a^b f(x) \, dx = \int_{[a, b]} f \, d\mu.$$

리만 적분가능한 함수는 반드시 유계여야 함에 주목하십시오. 이는 **문제 37B<sup>†</sup>**와 같은 방식으로 함수  $f: [0, 1] \rightarrow \mathbb{R}$ 를 다음과 같이 구성하려 한다면

$$f(x) = \begin{cases} \frac{\sin(1/x)}{x} & x > 0 \\ 0 & x = 0 \end{cases}$$

함수  $f$ 는 사실 리만 적분가능하지 않게 됨을 의미합니다! 물론 부정 리만 적분  $\lim_{\varepsilon \rightarrow 0^+} \int_{\varepsilon}^1 f(x) \, dx$  자체는 존재합니다.

따라서 실제로는 (더 편리한) 르베그 적분으로 모든 이론을 전개하지만, 실제로  $\int_{[1, 4]} x^2 \, d\mu$ 를 계산해야 할 때는 그저 미적분학의 기본정리를 이용한 평소의 방식으로 되돌아갑니다.

#### 예제 37.3.2 ( $[1, 4]$ 에 걸쳐 $x^2$ 적분하기)

예전 예제를 다시 살펴봅시다:

$$\int_{[1, 4]} x^2 \, d\mu = \int_1^4 x^2 \, dx = \frac{1}{3} \cdot 4^3 - \frac{1}{3} \cdot 1^3 = 21.$$

함수가 음이 아니라면, 이는 부정 적분에 대해서도 성립합니다. 이 명제를 적는 것은 다소 번거롭지만, 여기 적어 보겠습니다.

#### 정리 37.3.3 (부정 적분은 좋은 르베그 적분이다)

$(a, b) \subseteq \mathbb{R}$  위에서 정의된 음이 아닌 연속함수  $f \geq 0$ 이 있다고 합시다. 이때  $a = -\infty$ 이거나  $b = \infty$ 인 경우도 허용합니다. 그러면

$$\int_{(a, b)} f \, d\mu = \lim_{\substack{a' \rightarrow a^+ \\ b' \rightarrow b^-}} \int_{a'}^{b'} f(x) \, dx$$

여기서  $f$ 가 절대 적분가능하지 않다면 양변이 모두  $+\infty$ 가 되는 것을 허용합니다.

우변은  $[a', b'] \subsetneq (a, b)$ 가  $f$ 가 연속인 콤팩트 구간이므로 의미가 있습니다. 이는 음이 아닌 함수의 부정 리만 적분이 해당하는 열린 구간 위의 르베그 적분으로 간주될 수 있음을 의미합니다.

그래도 예제를 하나 살펴보는 편이 아마 더 나을 것입니다.

#### 예제 37.3.4 ((0, 1)에서 $1/\sqrt{x}$ 적분하기)

예를 들어, 여러분은 다음과 같은 이상 적분에 익숙할 수 있습니다

$$\int_0^1 \frac{1}{\sqrt{x}} dx := \lim_{\varepsilon \rightarrow 0^+} \int_{\varepsilon}^1 \frac{1}{\sqrt{x}} dx = \lim_{\varepsilon \rightarrow 0^+} (2\sqrt{1} - 2\sqrt{\varepsilon}) = 2.$$

(이는 앞서 **문제 30C\***로 등장했음에 유의하십시오.) 리만 적분 상황에서는  $\varepsilon \rightarrow 0^+$ 일 때의 극한이 필요했는데, 그렇지 않으면  $\frac{1}{\sqrt{x}}$ 는 함수  $[0, 1] \rightarrow \mathbb{R}$ 로 정의되지 않기 때문입니다. 그러나 이는 측정 가능한 음이 아닌 함수  $(0, 1) \rightarrow [0, +\infty]$ 이며, 따라서

$$\int_{(0,1)} \frac{1}{\sqrt{x}} d\mu = 2.$$

$f$ 가 음이 아닌 함수가 아니라면, 상황은 완전히 달라집니다. 실제로 **문제 37B†**가 그 유명한 반례입니다.

### §37.4 생각해 볼 만한 조금 더 어려운 문제

**문제 37A\*** (유리수의 지시함수). 유리수에 대한 지시함수  $\mathbf{1}_{\mathbb{Q}}: \mathbb{R} \rightarrow \{0, 1\} \subseteq \mathbb{R}$ 을 생각해 봅시다.

(a)  $\mathbf{1}_{\mathbb{Q}}$ 가 리만 적분 가능하지 않음을 증명하십시오.

(b)  $\int_{\mathbb{R}} \mathbf{1}_{\mathbb{Q}}$ 가 존재함을 보이고 그 값을 구하십시오 — 여러분이 예상하는 바로 그 값입니다!

**문제 37B†** (부호가 바뀌는 이상 리만 적분).  $f: (1, \infty) \rightarrow \mathbb{R}$ 를  $f(x) = \frac{\sin(x)}{x}$ 로 정의합시다.  $f$ 가 절대 적분 가능하지 않지만, 이상 리만 적분

$$\int_1^{\infty} f(x) dx := \lim_{b \rightarrow \infty} \int_1^b f(x) dx$$

그럼에도 불구하고 존재합니다.

# 38 르베그 적분과 순서 교환하기

## §38.1 극한 교환의 동기

이 절의 대표적인 예:  $1_{\mathbb{Q}}$ 는 좋습니다!

리만 적분의 문제점 중 하나는 함수의 수렴에 대해 나쁘게 동작한다는 것이며, 르베그 적분은 이를 해결합니다. 따라서 이는 르베그 적분이 리만 적분보다 더 나은 성질을 갖는 이유에 대한 대표적인 예시로 자주 제시됩니다.

우리는 기술적으로 이를 이미 본 적이 있습니다: 지시함수  $1_{\mathbb{Q}}$ 를 생각해 봅시다. 이는 **문제 37A\***에 의해 리만 적분 가능하지 않습니다. 하지만 우리는 이것의  $[0, 1]$  위에서의 르베그 적분을 다음과 같이 쉽게 계산할 수 있습니다,

$$\int_{[0,1]} 1_{\mathbb{Q}} d\mu = \mu([0, 1] \cap \mathbb{Q}) = 0$$

이는 가산집합이기 때문입니다.

이는 리만 적분에 대한 존재성의 실패로 생각될 수 있습니다.

**예제 38.1.1** ( $1_{\mathbb{Q}}$ 는 유한 지지 함수들의 극한입니다)

우리는 함수의 수열  $g_1, g_2, \dots$  을 다음과 같이 정의할 수 있습니다

$$g_n(x) = \begin{cases} 1 & (n!)x \text{ 정수입니다} \\ 0 & \text{그렇지 않으면.} \end{cases}$$

그러면 각  $g_n$ 은 조각별로 연속이며 따라서  $[0, 1]$  위에서 리만 적분 가능합니다(적분값은 0), 하지만  $\lim_{n \rightarrow \infty} g_n = 1_{\mathbb{Q}}$ 는 그렇지 않습니다.

여기서 극한은 다음과 같은 의미로 정의됩니다:

**정의 38.1.2.**  $f$ 와  $f_1, f_2, \dots : \Omega \rightarrow \mathbb{R}$ 를 함수들의 수열이라 합시다. 각  $\omega \in \Omega$ 에 대해 다음 수열이

$$f_1(\omega), f_2(\omega), f_3(\omega), \dots$$

$f(\omega)$ 로 수렴한다고 가정합시다. 그러면 우리는  $f_1, f_2, \dots$  이 극한  $f$ 로 **점별 수렴**한다고 말하며, 이를  $\lim_{n \rightarrow \infty} f_n = f$ 로 씁니다.

우리는  $\liminf_{n \rightarrow \infty} f_n$ 과  $\limsup_{n \rightarrow \infty} f_n$ 을 비슷하게 정의할 수 있습니다.

”르베그 적분이 더 나은 성질을 갖는다”는 것은 다음을 의미합니다:

**명제 38.1.3**

만약  $f_1, f_2, \dots : \Omega \rightarrow \mathbb{R}$ 가 가측 함수들이라면,  $\liminf_{n \rightarrow \infty} f_n$ 과  $\limsup_{n \rightarrow \infty} f_n$ 은 가측입니다.

$f_n$ 이 모두 음이 아닐 때, 이는  $\int_{\Omega} \liminf_{n \rightarrow \infty} f_n d\mu$ 와  $\int_{\Omega} \limsup_{n \rightarrow \infty} f_n d\mu$ 가 존재함을 의미합니다. (만약 이들이 음수가 될 수 있다면, 그 동작은 그렇게 좋지 않습니다. **문제 37B†**가 그 예시를 제공합니다.)

안타깝게도, 적분이 존재하더라도 우리는 점별 극한과 르베그 적분을 항상 교환할 수 있는 것은 아닙니다.

왜 그렇게 하고 싶을까요? 예를 들어, 다음과 같은 문제에 직면했다고 합시다:

$\lim_{k \rightarrow \infty} \int_1^\infty \frac{1}{k} e^{-x^2} dx$ 를 계산하십시오.

적분  $\int e^{-x^2} dx$ 는 초등적인 방법으로 계산 불가능하지만, 우리는 그 극한이 단순히 0이라고 말하고 싶어집니다(왜 아니겠습니까?)

안타깝게도, 점별 수렴은 실제로 상당히 약한 수렴 개념입니다.

#### 예제 38.1.4

이 모든 예시들에서, 우리는 결과를 바꾸지 않고서는 극한과 적분을 교환할 수 없습니다.

- 수열  $f_k(x) = \frac{\sin(x)}{x} \cdot \mathbf{1}_{(1,k)}$ 는  $k \rightarrow \infty$ 일 때  $f(x) = \frac{\sin(x)}{x} \cdot \mathbf{1}_{(1,\infty)}$ 로 점별 수렴하며, 극한  $\lim_{k \rightarrow \infty} \int f_k(x) dx$ 는 존재하지만,  $f$ 는 적분 가능하지 않습니다.
- 마찬가지로,  $f_k(x) = \frac{\sin(1/x)}{x} \cdot \mathbf{1}_{(1/k,\infty)}$ 는  $k \rightarrow \infty$ 일 때  $f(x) = \frac{\sin(1/x)}{x} \cdot \mathbf{1}_{(0,\infty)}$ 로 점별 수렴하며, 극한  $\lim_{k \rightarrow \infty} \int f_k(x) dx$ 는 존재하고 유한하지만,  $f$ 는 적분 가능하지 않습니다.
- 수열  $f_k(x) = \frac{1}{k} \cdot \mathbf{1}_{(0,k)}$ 는  $k \rightarrow \infty$ 일 때  $f(x) = 0$ 으로 점별 수렴하며, 모든  $k$ 에 대해  $\int f_k(x) dx = 1$ 이지만  $\int f(x) dx = 0$ 입니다.  
이 경우 수렴이 실제로 균등수렴이라는 점에 주목하십시오!
- 분모에  $k$ 가 있을 필요조차 없습니다 — 수열  $f_k(x) = \mathbf{1}_{(k,\infty)}$  역시  $f(x) = 0$ 으로 점별 수렴하지만, 이번에는 모든  $k$ 에 대해  $\int f_k(x) dx = \infty$ 입니다!
- 수열  $f_k(x) = k \cdot \mathbf{1}_{(0,1/k)}$ 는  $k \rightarrow \infty$ 일 때  $f(x) = 0$ 으로 점별 수렴합니다. 하지만 위와 비슷하게, 모든  $k$ 에 대해  $\int f_k(x) dx = 1$ 이지만  $\int f(x) dx = 0$ 입니다.

마지막 예시는 마녀의 모자(Witch's hat)로 알려진 예시와 거동이 비슷합니다.<sup>a</sup>

<sup>a</sup><https://www.geogebra.org/m/dv7ctmed>에 애니메이션이 있습니다.

이런 이유로, 아래에서 서술하는 수렴 정리들은 가능한 모든 이상 현상을 분류하고, “일반적인” 경우에는 극한과 적분을 교환하는 것이 그대로 성립함을 보이려는 시도입니다.

앞서 언급했듯이, 이러한 경우에는 르베그 적분이 대체로 존재하기 때문에 리만 적분 대신 르베그 적분을 사용하기로 선택합니다.

## §38.2 개요

점별 극한과 르베그 적분을 교환하기 위한 세 가지 대표적인 결과는 다음과 같습니다:

- 파투 보조정리: 음이 아닌 임의의 가측 함수에 대해 성립하는 가장 일반적인 형태의 명제입니다.
- 단조수렴: “증가하는 극한”은 그대로 성립합니다.
- 지배수렴(실제로는 파투-르베그): 너무 크지 않은(절대적으로 적분 가능한 어떤 함수로 유계인) 극한은 그대로 성립합니다.

### §38.3 파투 보조정리

위의 모든 예시에서 다음을 확인할 수 있습니다:

- 극한과 적분의 교환이 실패하는 것은 수열 내 함수들이 “이리저리 흔들릴” 여지가 너무 많기 때문이며,
- 이런 이유로, 적분  $\int f_k(x)dx$ 는 모두 극한의 적분  $\int f(x)dx$ 보다 큼니다.

물론, 모든 함수  $f_k(x)$ 의 부호를 바꾸면  $\lim_{k \rightarrow \infty} \int f_k(x)dx < \int f(x)dx$ 를 얻을 수 있습니다. 하지만 밝혀진 바에 따르면, 음이 아닌 함수에 대해서는 이런 종류의 거동만이 유일하게 가능한 거동입니다. 다시 말해,

**음이 아닌 함수에 대해, 적분의 극한이 극한의 적분과 같지 않다면, 전자가 항상 더 큼니다.**

#### 보조정리 38.3.1 (파투 보조정리, 예비 버전)

$f_1, f_2, \dots : \Omega \rightarrow [0, +\infty]$ 를  $f$ 로 점별 수렴하는 음이 아닌 가측 함수들의 수열이라 합시다. 그러면  $f$ 는 음이 아니고, 가측이며,

$$\int_{\Omega} f \, d\mu \leq \lim_{n \rightarrow \infty} \left( \int_{\Omega} f_n \, d\mu \right).$$

여기서는 양변 모두  $+\infty$ 가 될 수 있도록 허용합니다.

밝혀진 바에 따르면, 이 보조정리는 다음과 같이 상당히 일반화될 수 있습니다. 두 명제를 비교해 보면, 두  $\lim$  연산자가  $\liminf$ 로 바뀐 것을 확인할 수 있습니다 — 수열이 실제로 수렴할 때는  $\liminf$ 와  $\lim$ 이 같아집니다.

#### 보조정리 38.3.2 (파투 보조정리)

$f_1, f_2, \dots : \Omega \rightarrow [0, +\infty]$ 를 음이 아닌 가측 함수들의 수열이라 합시다. 그러면  $\liminf_{n \rightarrow \infty} f_n : \Omega \rightarrow [0, +\infty]$ 는 가측이며,

$$\int_{\Omega} \left( \liminf_{n \rightarrow \infty} f_n \right) d\mu \leq \liminf_{n \rightarrow \infty} \left( \int_{\Omega} f_n \, d\mu \right).$$

여기서는 양변 모두  $+\infty$ 가 될 수 있도록 허용합니다.

$f_n$ 에 대해 음이 아니라는 것 외에는 어떠한 추가 가정도 없다는 점에 주목하십시오. 이는 어떤 일반적인 결과를 증명하려 할 때 이 보조정리를 놀라울 만큼 다재다능하게 만듭니다.

### §38.4 그 외 모든 것

큰 놀라움은 모든 “유명한” 정리들이 파투 보조정리로부터 얼마나 빠르게 따라 나오는가입니다. 다음은 이른바 “단조 수렴 정리”입니다.

**따름정리 38.4.1 (단조 수렴 정리)**

$f$ 와  $f_1, f_2, \dots : \Omega \rightarrow [0, +\infty]$ 를  $\lim_n f_n = f$ 이고 각  $n$ 에 대해  $f_n(\omega) \leq f(\omega)$ 인 음이 아닌 가측함수들의 열이라 합시다. 그러면  $f$ 는 가측이고

$$\lim_{n \rightarrow \infty} \left( \int_{\Omega} f_n d\mu \right) = \int_{\Omega} f d\mu.$$

여기서는 양변 중 어느 쪽이든  $+\infty$ 가 되는 것을 허용합니다.

증명. 다음이 성립합니다

$$\begin{aligned} \int_{\Omega} f d\mu &= \int_{\Omega} \left( \liminf_{n \rightarrow \infty} f_n \right) d\mu \\ &\leq \liminf_{n \rightarrow \infty} \int_{\Omega} f_n d\mu \\ &\leq \limsup_{n \rightarrow \infty} \int_{\Omega} f_n d\mu \\ &\leq \int_{\Omega} f d\mu \end{aligned}$$

여기서 첫 번째  $\leq$ 는 파투 보조정리에 의한 것이고, 세 번째는 모든  $n$ 에 대해  $\int_{\Omega} f_n \leq \int_{\Omega} f$ 라는 사실에 의한 것입니다. 이는 모든 부등식이 등식이 됨을 의미하며, 이로써 증명이 끝납니다.  $\square$

증명이 얼마나 짧은지 알 수 있습니다 —  $\limsup_{n \rightarrow \infty} \int_{\Omega} f_n d\mu \leq \int_{\Omega} f d\mu$ 를 증명하는 것이 쉬운 절반이고, 어려운 절반은 파투 보조정리가 자동으로 처리해 줍니다.

**비고 38.4.2 (단조 수렴 정리는 단조성을 요구하지 않습니다!)** — 문헌에서는 모든  $n$ 에 대해 단순히  $f_n(\omega) \leq f(\omega)$ 라는 가정보다는  $f_1(\omega) \leq f_2(\omega) \leq \dots \leq f(\omega)$ 라는 가정을 훨씬 더 흔히 볼 수 있는데, 이것이 이 정리가 그 이름을 얻게 된 이유입니다. 그러나 우리가 보였듯이 이 가정은 불필요합니다! 이는 “알려지지 않은 채로 남아 있는 매우 중요한 정리를 알고 계십니까?”라는 제목의 질문에 대한 답변인 <https://mathoverflow.net/a/296540/70654>에서 지적된 바 있습니다.

**예제 38.4.3 (단조 수렴이  $1_{\mathbb{Q}}$ 를 준다)**

이는 이미 **예제 38.1.1**를 함의합니다.  $g_n$ 을 그 예제에서 설명한 대로  $\frac{1}{n!}\mathbb{Z}$ 에 대한 지시 함수라 하면,  $g_n \leq 1_{\mathbb{Q}}$ 이고 각 개별  $x$ 에 대해  $\lim_{n \rightarrow \infty} g_n(x) = 1_{\mathbb{Q}}(x)$ 입니다. 따라서 각  $n$ 에 대해  $\int_{[0,1]} g_n d\mu = 0$ 이므로, 이는 우리가 이미 알고 있던  $\int_{[0,1]} 1_{\mathbb{Q}} = 0$ 을 줍니다.

그러나 가장 유명한 결과는 다음과 같습니다.

**따름정리 38.4.4 (파투-르베그 정리)**

$f_1, f_2, \dots: \Omega \rightarrow \mathbb{R}$ 를 가측함수들의 열이라 합시다.  $g: \Omega \rightarrow \mathbb{R}$ 가 모든  $\omega \in \Omega$ 에 대해  $|f_n(\omega)| \leq g(\omega)$ 를 만족하는 절대 적분 가능한 함수라고 가정합시다. 그러면 다음 부등식이

$$\begin{aligned} \int_{\Omega} \left( \liminf_{n \rightarrow \infty} f_n \right) d\mu &\leq \liminf_{n \rightarrow \infty} \left( \int_{\Omega} f_n d\mu \right) \\ &\leq \limsup_{n \rightarrow \infty} \left( \int_{\Omega} f_n d\mu \right) \leq \int_{\Omega} \left( \limsup_{n \rightarrow \infty} f_n \right) d\mu. \end{aligned}$$

증명. 세 개의 부등식이 있습니다:

- 첫 번째 부등식은 음이 아닌  $g + f_n$ 에 대해 파투 보조정리를 적용한 것에서 따라 나옵니다.
- 두 번째 부등식은 그저  $\liminf \leq \limsup$ 일 뿐입니다. (이 덕분에 정리의 진술을 외우기 쉽습니다!)
- 세 번째 부등식은 음이 아닌  $g - f_n$ 에 대해 파투 보조정리를 적용한 것에서 따라 나옵니다.  $\square$

**연습문제 38.4.5.** 이 증명에서  $g$ 가 절대 적분 가능하다는 사실은 어디에 쓰였습니까?

**따름정리 38.4.6 (지배 수렴 정리)**

$f_1, f_2, \dots: \Omega \rightarrow \mathbb{R}$ 를  $f = \lim_{n \rightarrow \infty} f_n$ 이 존재하는 가측함수들의 열이라 합시다.  $g: \Omega \rightarrow \mathbb{R}$ 가 모든  $\omega \in \Omega$ 에 대해  $|f_n(\omega)| \leq |g(\omega)|$ 를 만족하는 절대 적분 가능한 함수라고 가정합시다. 그러면

$$\int_{\Omega} f d\mu = \lim_{n \rightarrow \infty} \left( \int_{\Omega} f_n d\mu \right).$$

다시 말해,

**함수  $f_k$ 가 “흔들릴” 수 있는 “공간”이 유한하기만 하다면, 어떤 이상 현상도 일어날 수 없습니다.**

증명.  $f(\omega) = \lim_{n \rightarrow \infty} f_n(\omega)$ 이면,  $f(\omega) = \liminf_{n \rightarrow \infty} f_n(\omega) = \limsup_{n \rightarrow \infty} f_n(\omega)$ 입니다. 따라서 파투-르베그 정리의 모든 부등식은, 가장 왼쪽 변과 가장 오른쪽 변이 서로 같으므로 등식이 됩니다.  $\square$

이는 **예제 38.1.1**을 검증하는 또 다른 방법을 줍니다. 일반적으로, 지배 수렴 정리는 학부 시험에서 즐겨 쓰이는 상투적인 소재인데, 이는 그에 관한 문제를 만들기가 쉽기 때문입니다. 다음은 그것들이 어떤 모습인지 보여주는 한 가지 예시입니다.

**예제 38.4.7 (흔히 보는 르베그 지배 수렴 예제)**

다음을 계산하고자 한다고 합시다

$$\lim_{n \rightarrow \infty} \left( \int_{(0,1)} \frac{n \sin(n^{-1}x)}{\sqrt{x}} \right) dx$$

그러면 안쪽 항이 절대 적분 가능한 함수  $x^{-1/2}$ 로 유계라는 것을 관찰하는 것에서 시작합니다. 따라서 그것은 다음과 같습니다

$$\begin{aligned} \int_{(0,1)} \lim_{n \rightarrow \infty} \left( \frac{n \sin(n^{-1}x)}{\sqrt{x}} \right) dx &= \int_{(0,1)} \frac{x}{\sqrt{x}} dx \\ &= \int_{(0,1)} \sqrt{x} dx = \frac{2}{3}. \end{aligned}$$

이상 현상의 동작에 대해 다른 사실도 말할 수 있습니다 — 즉,  $|\Omega| < \infty$ 일 때, 이상 현상은 오직 측도가 작은 집합에서만 발생합니다.

#### 정리 38.4.8 (Egorov 정리)

$f_1, f_2, \dots: \Omega \rightarrow \mathbb{R}$ 을  $|\Omega| < \infty$ 인 측도 공간  $\Omega$  위의 가측함수열이라 하고,  $f = \lim_{n \rightarrow \infty} f_n$ 이 존재하며 거의 모든 곳에서 유한하다고 합시다. 그러면 임의의  $\varepsilon > 0$ 에 대해, 나머지가 작은 측도를 갖도록 하는 부분집합  $U \subseteq \Omega$ 를 찾을 수 있습니다:

$$|\Omega \setminus U| < \varepsilon,$$

그리고 수렴은  $U$  위에서 균등하게 일어납니다: 수열

$$f_1|_U, f_2|_U, \dots$$

$f|_U$ 로 균등하게 수렴합니다.

이는 다음 정리 때문입니다.

#### 정리 38.4.9 (균등수렴 정리)

$f_1, f_2, \dots: \Omega \rightarrow \mathbb{R}$ 을  $|\Omega| < \infty$ 인 측도 공간  $\Omega$  위의 적분 가능한 함수열이라 하고,  $\lim_{n \rightarrow \infty} f_n = f$ 이며 이 수렴이 균등하다고 합시다. 그러면  $f$ 는 적분 가능하고,

$$\lim_{n \rightarrow \infty} \left( \int_{\Omega} f_n d\mu \right) = \int_{\Omega} f d\mu.$$

다시 말해,

$\int f d\mu \neq \lim \int f_k d\mu$ 라는 사실은 오직  $\int_{\Omega \setminus U} f d\mu \neq \lim \int_{\Omega \setminus U} f d\mu$ 에 의해서만 발생합니다.

**예제 38.4.10** (측도가 작은 집합을 제거하면 적분과 극한을 서로 바꿀 수 있습니다)

예제 38.1.4에서 몇 가지 예시를 가져와, 여기서 측도가 작은 집합을 제거하면 어떤

일이 일어나는지 살펴봅시다.

- 수열  $f_k(x) = k \cdot \mathbf{1}_{(0,1/k)}$ 을 생각해 봅시다. 임의의  $\varepsilon > 0$ 에 대해,  $f_k$ 의 정의역에서 구간  $(0, \varepsilon)$ 를 제거하면,  $k \rightarrow \infty$ 일 때  $f_k$ 가  $f$ 로 균등하게 수렴하며,  $\lim_{k \rightarrow \infty} \int f_k(x) dx = \int f(x) dx = 0$ 이 성립함을 알 수 있습니다.
- 마찬가지로, 수열  $f_k(x) = \frac{\sin(1/x)}{x} \cdot \mathbf{1}_{(1/k, 1)}$ 은  $f(x) = \frac{\sin(1/x)}{x} \cdot \mathbf{1}_{(0, 1)}$ 으로 점별 수렴하며, 구간  $(0, \varepsilon)$ 를 제거하면 모든 것이 문제없이 성립합니다.

**비고 38.4.11** — 측도가 작은 집합만 제거하면 된다고 해서, 그 집합이 작은 구간 안에 밀집되어 있다는 뜻은 아닙니다. 독자는  $f$ 로 점별 수렴하지만, 수렴을 균등하게 만들기 위해서는  $[0, 1]$ 의 조밀한 부분집합을 제거해야 하는 수열  $f_k: [0, 1] \rightarrow \mathbb{R}^+$ 을 구성해 보기 바랍니다. (힌트: 어디에서나 불연속이고 어디에서나 음이 아닌 임의의 함수  $f$ 를 취하고,  $f_k = \min(k, f)$ 로 놓으십시오.)

## §38.5 푸비니와 토넬리

작성 예정

## §38.6 생각해 볼 만한 조금 더 어려운 문제

문제



# 39 보너스: 폰트랴긴 쌍대성에 대한 힌트

이 짧은 장에서는 우리의 푸리에 해석(보너스 장 [장 14](#))을 훨씬 더 넓은 부류의 군  $G$ 로 일반화하는 방법에 대한 서술을 제시하겠습니다.

## §39.1 LCA 군

이 절의 대표적인 예:  $\mathbb{T}$ ,  $\mathbb{R}$ .

앞서 우리는  $\mathbb{R}$ 을 다루었는데, 이것이 좋은 이유는 위상 공간일 뿐만 아니라 덧셈에 대해 아벨 군이기도 하기 때문입니다. 이처럼 군이면서 동시에 공간이기도 한 이러한 종류의 대상에는 이름이 있습니다.

**정의 39.1.1. 위상군**  $G$ 란 하우스도르프<sup>1</sup> 위상 공간이면서 동시에 군 연산  $(G, \cdot)$ 을 갖추고 있어서, 다음 두 사상이

$$\begin{aligned} G \times G &\rightarrow G & \text{에 의해 } (x, y) &\mapsto xy \\ G &\rightarrow G & \text{에 의해 } x &\mapsto x^{-1} \end{aligned}$$

연속인 것을 말합니다.

우리의 푸리에 해석을 위해서는 몇 가지 추가 조건이 필요합니다.

**정의 39.1.2. 국소 콤팩트 아벨(LCA) 군**  $G$ 란 군 연산이 아벨적이며, 나아가 위상이 국소 콤팩트한 것을 말합니다:  $G$ 의 모든 점  $p$ 에 대해,  $K \ni p$ 이고  $K$ 가  $p$ 의 어떤 열린 근방을 포함하는 콤팩트 부분집합  $K$ 가  $G$  안에 존재합니다.

우리가 앞서 다룬 예들은 모두 이 범주에 속합니다:

### 예제 39.1.3 (국소 콤팩트 아벨 군의 예)

- 이산 위상을 갖는 임의의 유한군  $Z$ 는 LCA입니다.
- 원군  $\mathbb{T}$ 는 LCA이며 사실 콤팩트하기도 합니다.
- 실수  $\mathbb{R}$ 은 콤팩트하지 않은 LCA 군의 한 예입니다.

이러한 조건들은 공간  $G$  위에 측도를 정의하기에 충분한 것으로 밝혀집니다. 관련된 정리는 다음과 같으며, 여기서는 그저 인용만 하겠습니다:

<sup>1</sup>일부 저자는 하우스도르프 조건을 생략합니다.

**정리 39.1.4 (하르 측도)**

$G$ 를 국소 콤팩트 아벨 군이라 합시다. 우리는 이를 보렐  $\sigma$ -대수  $\mathcal{B}(G)$ 를 사용하여 가측 공간으로 간주합니다. 다음 성질들을 만족하는, **하르 측도**라 불리는 측도  $\mu: \mathcal{B}(G) \rightarrow [0, \infty]$ 가 존재합니다:

- 모든  $g \in G$ 와 가측 집합  $S$ 에 대해  $\mu(gS) = \mu(S)$ 입니다. 이는  $\mu$ 가  $G$ 에 의한 평행이동에 대해 "평행이동 불변"임을 의미합니다.
- 임의의 콤팩트 집합  $K$ 에 대해  $\mu(K)$ 는 유한합니다.
- $S$ 가 가측이면,  $\mu(S) = \inf \{ \mu(U) \mid U \supseteq S \text{ 열린} \}$ 입니다.
- $U$ 가 열린집합이면,  $\mu(U) = \sup \{ \mu(K) \mid K \subseteq U \text{ 콤팩트} \}$ 입니다.

나아가, 이는 양의 상수배까지를 제외하면 유일합니다.

**비고 39.1.5** —  $G$ 가 콤팩트하면  $\mu(G)$ 는 유한(하며 양수)임에 유의하십시오. 이러한 이유로 LCA 군  $G$  위의 하르 측도는 보통  $\mu(G) = 1$ 이 되도록 정규화됩니다.

이 장에서는 처음 두 성질만을 사용할 것이며, 나머지 두 성질은 완결성을 위해 언급될 뿐입니다. 사실 이는  $\mathbb{R}^n$ 이 LCA 군이므로, 우리가  $\mathcal{B}(\mathbb{R}^n)$  위에 측도를 구성했던 장을 실제로 일반화한 것임에 유의하십시오!

그러므로 요약하면: LCA 군이 있으면, 그 위에 측도  $\mu$ 가 있습니다.

**§39.2 폰트라긴 쌍대**

이제 핵심적인 정의는 다음과 같습니다:

**정의 39.2.1.**  $G$ 를 LCA 군이라 합시다. 그러면 이것의 **폰트라긴 쌍대**는 다음과 같은 아벨 군입니다

$$\widehat{G} := \{ \text{연속 군 준동형사상 } \xi: G \rightarrow \mathbb{T} \}.$$

사상  $\xi$ 들은 **지표**라고 불립니다. 이것 자체도 LCA 군으로 만들 수 있습니다.<sup>2</sup>

**예제 39.2.2 (폰트라긴 쌍대의 예시)**

- $\widehat{\mathbb{Z}} \cong \mathbb{T}$ 인데, 군 준동형사상  $\mathbb{Z} \rightarrow \mathbb{T}$ 는 1의 상에 의해 결정되기 때문입니다.
- $\widehat{\mathbb{T}} \cong \mathbb{Z}$ 입니다. 지표들은  $n \in \mathbb{Z}$ 에 대해  $\theta \mapsto n\theta$ 로 주어집니다.
- $\widehat{\mathbb{R}} \cong \mathbb{R}$ 입니다. 이는 영이 아닌 연속 준동형사상  $\mathbb{R} \rightarrow S^1$ 이  $1 \in S^1$  위의 올에 의해 결정되기 때문입니다. (대수적 위상수학자라면 여기서 피복 사영을 볼 수도 있을 것입니다.)
- $\widehat{\mathbb{Z}/n\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z}$ 인데, 지표  $\xi$ 는 상  $\xi(1) \in \mathbb{T}$ 에 의해 결정됩니다.
- $\widehat{G \times H} \cong \widehat{G} \times \widehat{H}$ .

<sup>2</sup>만약 위상을 꼭 알아야 한다면, 그것은 **콤팩트-열린 위상**입니다: 임의의 콤팩트 집합  $K \subseteq G$ 와 열린집합  $U \subseteq \mathbb{T}$ 에 대해,  $\xi^{\text{img}}(K) \subseteq U$ 를 만족하는 모든  $\xi$ 의 집합을 열린집합으로 선언하고, 그러한 모든 집합을 포함하는 가장 작은 위상을 취합니다. 우리는 이것을 전혀 사용하지 않을 것입니다.

**연습문제 39.2.3** (절 18.1를 읽은 분들을 위한  $\widehat{\widehat{Z}} \cong Z$ ).  $Z$ 가 유한 아벨 군이라면, 앞선 예시의 결과를 이용하여  $\widehat{\widehat{Z}} \cong Z$ 임을 보이십시오. 이제 쌍선형 형식  $\cdot : Z \times Z \rightarrow \mathbb{T}$ 가 정확히 동형사상  $Z \rightarrow \widehat{\widehat{Z}}$ 의 한 선택임을 알아볼 수 있을 것입니다. 이는 "표준적"이지 않습니다.

쌍대라는 이름에 걸맞게, 벡터 공간  $V$ 에 대한  $(V^\vee)^\vee \cong V$ 와 유사하게, 다음이 성립합니다:

**정리 39.2.4 (폰트랴긴 쌍대성 정리)**

임의의 LCA 군  $G$ 에 대해, 다음과 같은 동형사상이 존재합니다

$$G \cong \widehat{\widehat{G}} \quad \text{에 의해} \quad x \mapsto (\xi \mapsto \xi(x)).$$

콤팩트한 경우가 특히 훌륭합니다.

**명제 39.2.5** ( $G$ 가 콤팩트  $\iff \widehat{G}$ 가 이산)

$G$ 를 LCA 군이라 합시다. 그러면  $G$ 가 콤팩트인 것과  $\widehat{G}$ 가 이산인 것은 동치입니다.

증명. 문제 39B. □

### §39.3 콤팩트한 경우의 정규직교 기저

$G$ 를 콤팩트 LCA 군이라 하고, 그것의 하르 측도를 가지고 다룹시다. 이제  $L^2(G)$ 를  $\mathbb{C}$ 로 가는 제곱 적분 가능한 함수들의 공간으로 둘 수 있습니다, 즉

$$L^2(G) = \left\{ f: G \rightarrow \mathbb{C} \quad \text{이도록} \quad \int_G |f|^2 < \infty \right\}.$$

따라서 우리는 이것에 다음과 같은 내적 형식을 부여할 수 있습니다

$$\langle f, g \rangle = \int_G f \cdot \bar{g}.$$

그러한 경우, 우리는 이전에 원했던 모든 결과를 얻습니다:

**정리 39.3.1** ( $\widehat{G}$ 의 지표들이 정규직교 기저를 이룬다)

$G$ 가 LCA이면서 콤팩트하다고 가정합시다 (따라서  $\widehat{G}$ 는 이산입니다). 그러면 지표들은

$$(e_\xi)_{\xi \in \widehat{G}} \quad \text{에 의해} \quad e_\xi(x) = e(\xi(x)) = \exp(2\pi i \xi(x))$$

$L^2(G)$ 의 정규직교 기저를 이룹니다. 따라서 각  $f \in L^2(G)$ 에 대해 다음이 성립합니다

$$f = \sum_{\xi \in \widehat{G}} \widehat{f}(\xi) e_\xi$$

여기서

$$\widehat{f}(\xi) = \langle f, e_\xi \rangle = \int_G f(x) \exp(-2\pi i \xi(x)) d\mu.$$

합  $\sum_{\xi \in \widehat{G}}$ 은  $\widehat{G}$ 가 이산이기 때문에 뜻이 통합니다. 특히,

- 유한 군  $Z$ 에 대해  $G = Z$ 로 두면 "유한 군 위의 푸리에 변환"을 얻습니다.
- 특수한 경우인  $G = \mathbb{Z}/n\mathbb{Z}$ 는 자신만의 위키피디아 페이지를 가지고 있습니다: 바로 "이산 푸리에 변환"입니다.
- $G = \mathbb{T}$ 로 두면 앞서 나온 "푸리에 급수"가 됩니다.

### §39.4 비콤팩트한 경우의 푸리에 변환

$G$ 가 LCA이지만 콤팩트하지 않다면, 정리 39.3.1는 거짓이 됩니다. 반면,  $\widehat{G}$ 를 정의하는 것은 여전히 가능합니다. 이제 어쨌든 푸리에 계수를 써보려 시도할 수 있습니다:  $\xi \in \widehat{G}$ 이고  $f: G \rightarrow \mathbb{C}$ 일 때

$$\widehat{f}(\xi) = \int_G f \cdot \overline{e_\xi} d\mu$$

로 둡니다. 이 경우 결과는 덜 흥미롭지만, 여전히 예를 들어 다음이 성립합니다:

#### 정리 39.4.1 (비콤팩트한 경우의 푸리에 역변환 공식)

$\mu$ 를  $G$  위의 하르 측도라 합시다. 그러면  $\widehat{G}$  위에 유일한 하르 측도  $\nu$ (쌍대 측도라 불림)가 존재하여,  $f \in L^1(G)$ 이고  $\widehat{f} \in L^1(\widehat{G})$ 일 때마다 다음이 성립합니다:

$$f(x) = \int_{\widehat{G}} \widehat{f}(\xi) \xi(x) d\nu$$

(거의 모든  $x \in G$ 에 대해,  $\mu$ 에 관하여).  $f$ 가 연속이면, 이는 모든  $x$ 에 대해 성립합니다.

따라서 이전만큼 완전한 내적의 좋은 성질은 가지고 있지 않지만, 여전히 몇몇 경우에는 적어도  $f$ 를 이전과 비슷한 방식으로 적분으로 쓸 수 있습니다.

특히, 몇몇 특별한  $G$ 에 대해서는 특별한 이름이 붙어 있습니다:

- $G = \mathbb{R}$ 이면,  $\widehat{G} = \mathbb{R}$ 이 되어 "(연속) 푸리에 변환"이 됩니다.
- $G = \mathbb{Z}$ 이면,  $\widehat{G} = \mathbb{T}$ 가 되어 "이산 시간 푸리에 변환"이 됩니다.

### §39.5 요약

앞선 절들에서 다룬 다양한 형태의 푸리에 해석을 다음 표에 요약합니다. 첫 번째 부분에서는  $G$ 가 콤팩트이고, 두 번째 부분에서는  $G$ 가 콤팩트가 아닙니다.

| 이름            | 정의역 $G$                        | 쌍대 $\widehat{G}$                       | 지표                    |
|---------------|--------------------------------|----------------------------------------|-----------------------|
| 이진 푸리에 해석     | $\{\pm 1\}^n$                  | $S \subseteq \{1, \dots, n\}$          | $\prod_{s \in S} x_s$ |
| 유한군 위의 푸리에 변환 | $Z$                            | $\xi \in \widehat{Z} \cong Z$          | $e(i\xi \cdot x)$     |
| 이산 푸리에 변환     | $\mathbb{Z}/n\mathbb{Z}$       | $\xi \in \mathbb{Z}/n\mathbb{Z}$       | $e(\xi x/n)$          |
| 푸리에 급수        | $\mathbb{T} \cong [-\pi, \pi]$ | $n \in \mathbb{Z}$                     | $\exp(inx)$           |
| 연속 푸리에 변환     | $\mathbb{R}$                   | $\xi \in \mathbb{R}$                   | $e(\xi x)$            |
| 이산 시간 푸리에 변환  | $\mathbb{Z}$                   | $\xi \in \mathbb{T} \cong [-\pi, \pi]$ | $\exp(i\xi n)$        |

다양한 이름들이 형편없다는 것을 눈치채셨을 것입니다. 이것이 제가 고등학생 시절 혼란스러워했던 이유 중 하나입니다: 위에 나온 모든 종류의 푸리에 급수는 각각 자신만의 위키백과 문서를 가지고 있습니다. 저에게 결정권이 있었다면, 우리는 그냥 " $G$ -푸리에 변환"이라는 용어를 사용했을 것이고, 그것이 모두의 삶을 훨씬 편하게 만들었을 것입니다.

### §39.6 생각해 볼 만한 조금 더 어려운 문제

문제 39A.  $G$ 가 콤팩트여서  $\hat{G}$ 가 이산이라면, 쌍대 측도  $\nu$ 를 설명하십시오.

문제 39B. LCA 군  $G$ 가 콤팩트인 것과  $\hat{G}$ 가 이산인 것이 동치임을 보이십시오. (이를 위해서는 콤팩트-열림 위상이 필요할 것입니다.)



# XI

확률 (작성 예정)

## 제XI부: 목차

---

|           |                                     |            |
|-----------|-------------------------------------|------------|
| <b>40</b> | <b>확률 변수 (작성 예정)</b>                | <b>427</b> |
| 40.1      | 확률 변수 . . . . .                     | 427        |
| 40.2      | 분포 함수 . . . . .                     | 428        |
| 40.3      | 확률 변수의 예 . . . . .                  | 428        |
| 40.4      | 특성 함수 . . . . .                     | 428        |
| 40.5      | 독립 확률 변수 . . . . .                  | 428        |
| 40.6      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .      | 428        |
| <b>41</b> | <b>큰 수의 법칙 (작성 예정)</b>              | <b>429</b> |
| 41.1      | 수렴의 개념들 . . . . .                   | 429        |
| 41.2      | 약한 큰 수의 법칙 . . . . .                | 430        |
| 41.3      | 강한 큰 수의 법칙 . . . . .                | 430        |
| 41.4      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .      | 435        |
| <b>42</b> | <b>정지된 마팅게일 (작성 예정)</b>             | <b>437</b> |
| 42.1      | 거의 확실하게 돈을 버는 방법 . . . . .          | 437        |
| 42.2      | 부분 $\sigma$ -대수와 여과 . . . . .       | 437        |
| 42.3      | 조건부 기댓값 . . . . .                   | 439        |
| 42.4      | 슈퍼마팅게일 . . . . .                    | 442        |
| 42.5      | 선택적 정지(Optional stopping) . . . . . | 444        |
| 42.6      | 최적 정지의 재미있는 응용 (작성 예정) . . . . .    | 446        |
| 42.7      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .      | 449        |

---

# 40 확률 변수 (작성 예정)

챕터 작성

르베그 측도와 그 위의 적분을 제대로 전개했으므로, 이제 확률 변수를 전개할 수 있습니다.

## §40.1 확률 변수

이러한 준비 과정을 모두 마쳤으므로, 확률 변수는 정말 빠르게 정의할 수 있습니다.

**정의 40.1.1.** 확률 공간  $\Omega = (\Omega, \mathcal{A}, \mu)$  위의 (실)확률 변수  $X$ 는 가측 함수  $X: \Omega \rightarrow \mathbb{R}$ 이며, 여기서  $\mathbb{R}$ 에는 보렐  $\sigma$ -대수가 주어져 있습니다.

특히 확률 변수의 덧셈 등은 단순히 더하기만 하면 되므로 모두 성립합니다. 또한 앞 장의 내용에 따라  $X$ 를  $\Omega$  위에서 적분할 수 있습니다.

**정의 40.1.2** (확률 변수의 기본 성질). 확률 변수  $X$ 가 주어졌을 때,  $X$ 의 기댓값은 다음 르베그 적분으로 정의됩니다

$$\mathbb{E}[X] = \int_{\Omega} X(\omega) d\mu.$$

헛갈리게도, 문자  $\mu$ 가 종종 기댓값을 나타내는 데 사용됩니다.

$X$ 의  $k$ 번째 모멘트는 각 양의 정수  $k \geq 1$ 에 대해  $\mathbb{E}[X^k]$ 로 정의됩니다.  $X$ 의 분산은 그러면 다음과 같이 정의됩니다

$$\text{Var}(X) = \mathbb{E}[(X - \mathbb{E}[X])^2].$$

**질문 40.1.3.**  $1_A$ 가 확률 변수임을 보이고(보렐 가측임을 확인하기만 하면 됩니다), 그 기댓값이  $\mu(A)$ 임을 보이십시오.

여러분이 이미 알고 있을 법한 기댓값의 중요한 성질은 다음과 같습니다:

### 정리 40.1.4 (기댓값의 선형성)

$X$ 와  $Y$ 가  $\Omega$  위의 확률 변수라면 다음이 성립합니다

$$\mathbb{E}[X + Y] = \mathbb{E}[X] + \mathbb{E}[Y].$$

증명.  $\mathbb{E}[X + Y] = \int_{\Omega} X(\omega) + Y(\omega) d\mu = \int_{\Omega} X(\omega) d\mu + \int_{\Omega} Y(\omega) d\mu = \mathbb{E}[X] + \mathbb{E}[Y]$ .  $\square$

여기서  $X$ 와  $Y$ 가 굳이 “독립”일 필요는 없다는 점에 유의하십시오. 독립이라는 개념은 곧 정의할 것입니다.

## §40.2 분포 함수

## §40.3 확률 변수의 예

## §40.4 특성 함수

## §40.5 독립 확률 변수

## §40.6 생각해 볼 만한 조금 더 어려운 문제

**문제 40A** (등분포).  $X_1, X_2, \dots$ 를  $[0, 1]$  위의 독립 동일 분포 균등 확률 변수라 합시다. 거의 확실하게  $X_i$ 들이 등분포한다는 것, 즉 다음이

$$\lim_{N \rightarrow \infty} \frac{\#\{1 \leq i \leq N \mid a \leq X_i(\omega) \leq b\}}{N} = b - a \quad \forall 0 \leq a < b \leq 1$$

거의 모든  $\omega$ 의 선택에 대해 성립함을 보이십시오.

**문제 40B** (중선과 독립인 삼각형의 변 길이).  $X_1, Y_1, X_2, Y_2, X_3, Y_3$ 을 여섯 개의 독립인 표준 가우스 확률변수라 합시다. 데카르트 평면에서 삼각형  $ABC$ 를  $A = (X_1, Y_1)$ ,  $B = (X_2, Y_2)$ ,  $C = (X_3, Y_3)$ 으로 정의합니다. 변  $BC$ 의 길이가  $A$ -중선의 길이와 독립임을 증명하십시오.

# 41 큰 수의 법칙 (작성 예정)

장 작성

## §41.1 수렴의 개념들

### §41.1.i 거의 확실한 수렴

**정의 41.1.1.** 확률 공간  $\Omega$  위의 확률 변수  $X, X_n$ 이 있다고 합시다. 다음이 성립하면  $X_n$ 이  $X$ 에 **거의 확실히 수렴한다**고 말합니다.

$$\mu\left(\omega \in \Omega : \lim_n X_n(\omega) = X(\omega)\right) = 1.$$

이는 매우 강한 수렴의 개념입니다: 이는 거의 모든 세계에서  $X_n$ 의 값이  $X$ 로 수렴한다는 것을 의미합니다. 사실, 비예시를 드는 것이 오히려 더 나을 것 같습니다.

#### 예제 41.1.2 (거의 확실한 수렴의 비예시)

불멸의 스켈레톤 궁수가 사격을 연습하고 있으며,  $n$ 번째 사격에서 확률  $1 - \frac{1}{n}$ 로 명중시킨다고 상상해 봅시다 (궁수가 시간이 지날수록 향상되므로 이 확률은 1에 수렴합니다).  $X_n \in \{0, 1, \dots, 10\}$ 을  $n$ 번째 사격의 점수라고 합시다. 스켈레톤이 점차 완벽에 가까워지고 있지만, 궁수가 유한 번만 빗맞히는 세계는 거의 존재하지 않습니다: 즉

$$\mu\left(\omega \in \Omega : \lim_n X_n(\omega) = 10\right) = 0.$$

### §41.1.ii 확률 수렴

따라서 많은 목적을 위해서는 더 약한 수렴 개념이 필요합니다.

**정의 41.1.3.** 확률 공간  $\Omega$  위의 확률 변수  $X, X_n$ 이 있다고 합시다. 모든  $\varepsilon > 0$ 과  $\delta > 0$ 에 대해 다음이 성립하면  $X_n$ 이  $X$ 에 **확률 수렴한다**고 말합니다.

$$\mu(\omega \in \Omega : |X_n(\omega) - X(\omega)| < \varepsilon) \geq 1 - \delta$$

충분히 큰  $n$ 에 대해 ( $\varepsilon$ 와  $\delta$ 에 따라 결정됨).

이런 의미에서 우리의 스켈레톤 궁수는 실제로 성공합니다: 임의의  $\delta > 0$ 에 대해,  $n > \delta^{-1}$ 이면 스켈레톤 궁수는  $1 - \delta$  비율의 세계에서 명중시킵니다. 일반적으로, 이는 임의의  $\delta > 0$ 에 대해  $n$ 번째 단계에서  $\varepsilon$ -이상 사건이 일어날 확률이 결국  $\delta$  아래로 떨어진다는 것을 의미한다고 생각할 수 있습니다.

**비고 41.1.4** — 정의에서  $\delta$ 를 감추기 위해, 이는 때때로 다음과 같이 대신 쓰이기도 합니다: 모든  $\varepsilon$ 에 대해

$$\lim_{n \rightarrow \infty} \mu(\omega \in \Omega : |X_n(\omega) - X(\omega)| < \varepsilon) = 1.$$

큰 차이는 없다고 생각하지만, 저는 개인적으로 이 비대칭성이 마음에 들지 않습니다.

### §41.1.iii 법칙 수렴

## §41.2 약한 큰 수의 법칙

이름에서 알 수 있듯이, 이는 강한 큰 수의 법칙의 직접적인 따름정리입니다. 그럼에도 불구하고, 이 법칙의 증명은 더 간단하며, 일부 응용에서는 약한 법칙만으로도 충분합니다.

작성

### §41.2.i 응용: 바이어슈트라스 근사

## §41.3 강한 큰 수의 법칙

### §41.3.i 동기: 편향된 랜덤 워크

다음과 같이 정의된 랜덤 워크를 생각해 봅시다:

- $X_0 = 1$ 이라고 합시다.
- 각  $i \geq 1$ 에 대해,  $X_i$ 를 확률  $p = 0.6$ 으로  $X_{i-1} - 1$ , 확률  $1 - p = 0.4$ 로  $X_{i-1} + 1$ 이 되도록 정의합니다.

그러면 다음과 같이 물을 수 있습니다: 어떤  $X_i$ 가 0이 될 때까지의 단계 수의 기댓값은 얼마입니까?

소박한 시도는 다음과 같을 것입니다.

$f(i)$ 를  $X_0 = i$ 에서 시작하여 0에 도달하기까지의 단계 수의 기댓값이라고 합시다.

그러면:

- $f(0) = 0$ ,
- $f(1) = 1 + 0.6f(0) + 0.4f(2)$ ,
- $f(2) = 1 + 0.6f(1) + 0.4f(3)$ ,
- $\vdots$

항이 무한히 많기 때문에 이 방법으로는 진전이 없습니다. 더 나은 시도는 다음과 같습니다:

답을  $x$ 라고 합시다.  $X_0 = 2$ 에서 시작한다면,  $i$ 를  $X_i = 1$ 이 되는 첫 시점,  $j$ 를  $i$  이후  $X_j = 0$ 이 되는 첫 시점이라고 합시다. 그러면

$$\mathbb{E}[i] = \mathbb{E}[j - i] = x.$$

따라서,

$$x = 1 + 0.6 \cdot 0 + 0.4 \cdot (2x)$$

이 방정식을 풀면  $x = 5$ 를 얻습니다.

이 방법은 올바른 결과를 줍니다 — 하지만 아래로 갈 확률이  $p = 0.4$ 일 때 같은 방법을 적용하면  $x = -5$ 가 나오는데, 이는 명백히 말이 되지 않습니다.

무엇이 잘못되었을까요? 문제는  $p = 0.4$ 일 때 수열이 결코 0에 도달하지 못할 확률<sup>1</sup>이 0이 아니라는 데 있으며, 따라서 기댓값이 정의되지 않고 증명에서  $\infty$ 에서  $\infty$ 를 빼고 있다는 것입니다.

이 경우, 강대수의 법칙은 거의 모든 세계에서 수열  $X_i$ 가 결국 0에 도달한다는 것을 보임으로써 이 허점을 메우는 데 도움을 줄 수 있습니다.

<sup>1</sup>미리보기: 다음 장에서 마팅게일 이론을 이용하면, 수열이 결코 0에 도달하지 못할 확률이 정확히  $1 - \frac{0.4}{0.6}$ 임을 증명할 수 있습니다.

## §41.3.ii 진술

**정리 41.3.1 (강대수의 법칙)**

$X_1, X_2, \dots$  를 평균이 0인 독립 항등 분포 확률 변수라고 합시다. 부분 평균을 다음과 같이 정의합니다

$$M_n = \frac{X_1 + \dots + X_n}{n}.$$

그러면, 거의 모든 세계에서,  $M_n \rightarrow 0$ 입니다.

다시 말해,  $M_n$ 은 거의 확실하게 0으로 수렴합니다.

평균이 0이라는 조건은 단지 증명을 간단히 하기 위한 것으로, 평균이 존재하기만 하면 확률 변수에서 평균을 빼서 정리를 적용할 수 있습니다.

**예제 41.3.2 (가설  $\mathbb{E}[X_i] = 0$ 은 중요합니다)**

$M_n \rightarrow 0$ 이 성립하지 않는 예를 살펴봅시다 — 이는 상트페테르부르크 역설의 약간 변형된 버전입니다.

각  $X_i$ 의 분포를 다음과 같다고 합시다:

$$X_i = \begin{cases} 1 & \text{확률로 } \frac{1}{4} \\ -1 & \text{확률로 } \frac{1}{4} \\ 2 & \text{확률로 } \frac{1}{8} \\ -2 & \text{확률로 } \frac{1}{8} \\ 4 & \text{확률로 } \frac{1}{16} \\ -4 & \text{확률로 } \frac{1}{16} \\ \vdots & \end{cases}$$

형식적으로,  $X_i$ 는 확률  $2^{-k-2}$ 로  $\{2^k, -2^k\}$ 의 각 값을 취합니다.

이 경우, 평균  $\mathbb{E}[X_i] = \int_{\Omega} X_i(\omega)$ 는 실제로 정의되지 않습니다. 게다가, 분포가 아무리 대칭적으로 보이더라도, 거의 어떤 세계에서든  $M_n$ 은 0으로 수렴하지 않습니다.

직관적으로, 그 이유를 알 수 있습니다:

- 처음 16개 값 중 평균적으로  $|X_i| = 4$ 인  $X_i$ 가 하나 있으며, 이는  $M_{16}$ 을  $\frac{1}{4}$ 만큼 왜곡시킵니다.
- 처음 32개 값 중 평균적으로  $|X_i| = 8$ 인  $X_i$ 가 하나 있으며, 이는  $M_{32}$ 을  $\frac{1}{4}$ 만큼 왜곡시킵니다.
- 이하 마찬가지입니다.

다시 말해, 우리의 해골 공수와 마찬가지로,  $M_n$ 이  $\frac{1}{4}$ 보다 크게 왜곡된 경우가 유한 번만 발생하는 세계는 거의 존재하지 않습니다.

## §41.3.iii 유한 분산의 경우에 대한 증명

실제로 우리가 마주치는 대부분의 분포는 유한 분산을 가지므로, 반례를 하나 드는 편이 나을 것입니다.

**예제 41.3.3 (평균은 유한하지만 분산은 무한한 분포)**

위의 상트페테르부르크 역설 예시에서의  $X_i$ 에 대해  $Y_i = \text{sgn}(X_i)\sqrt{|X_i|}$ 로 두면 충분합니다. 계산해 보면  $\mathbb{E}[Y_i] = 0$ 이지만  $\mathbb{E}[Y_i^2] = \infty$ 임을 알 수 있습니다.

먼저  $\mathbb{E}[X_i^2]$ 이 유한한 경우에 대한 증명을 제시하겠습니다.

먼저, 얼핏 무관해 보이는 다음과 같은 급수를 정의합니다.

$$T_n = X_1 + \frac{X_2}{2} + \frac{X_3}{3} + \cdots + \frac{X_n}{n}.$$

이 단계는 동기를 설명하기가 다소 어렵습니다. 긍정적인 측면으로는, 다음을 보이기가 쉽다는 점입니다.

**주장 41.3.4.** 거의 모든 세계에서 수열  $T_n$ 은 수렴합니다.

이는 다음 급수가

$$X_1 + \frac{X_2}{2} + \frac{X_3}{3} + \cdots$$

수렴한다는 것과 같은 말입니다.

핵심 아이디어는 합산 항들의 총 분산이 유한함을 보이는 것입니다. 실제로:

$$\begin{aligned} \text{Var}[X_1] + \text{Var}\left[\frac{X_2}{2}\right] + \text{Var}\left[\frac{X_3}{3}\right] + \cdots &= \text{Var}[X_1] + \frac{1}{4}\text{Var}[X_2] + \frac{1}{9}\text{Var}[X_3] + \cdots \\ &= \text{Var}[X_1] \cdot \left(1 + \frac{1}{4} + \frac{1}{9} + \cdots\right) \end{aligned}$$

이는 유한합니다.

왜 총 분산이 유한하면 거의 확실한 수렴이 성립할까요? 직관적으로, 다음을 상기해 봅시다.

**정리 41.3.5 (체비쇼프 부등식)**

$X$ 를 평균이 0이고 분산이  $\sigma^2$ 인 확률 변수라고 합시다. 그러면

$$\Pr[|X| \geq k\sigma] \leq \frac{1}{k^2}.$$

또는 동등하게,  $\sigma$ 의 정의에 암묵적으로 포함된  $\sqrt{\cdot}$ 를 피하기 위해 다음과 같은 형태로 쓸 수도 있습니다.

$$\Pr[|X| \geq a] \leq \frac{1}{a^2} \text{Var}[X].$$

그러면 예를 들어  $T_{1000}$ 과  $T_{2000}$ 을 살펴보면:

$$\text{Var}[T_{2000} - T_{1000}] = \sum_{i=1001}^{2000} \frac{\text{Var}[X_i]}{i^2}$$

$\sum_{i=1}^{\infty} \frac{\text{Var}[X_i]}{i^2}$ 이 유한하므로,  $\sum_{i=1001}^{2000} \frac{\text{Var}[X_i]}{i^2}$ 은 매우 작을 것으로 예상되며, 이는  $T_{2000}$ 이  $T_{1000}$ 에서 거의 벗어나지 않아야 함을 의미합니다.

그러나 수렴을 보이려면 더 강력한 것이 필요합니다.

**정리 41.3.6 (콜모고로프 부등식)**

$X_1, \dots, X_n$ 을 평균이 0인 독립 확률 변수라 합시다. 각  $1 \leq i \leq n$ 에 대해  $S_i = X_1 + \dots + X_i$ 라고 정의합니다. 그러면

$$\Pr[|S_i| \geq a \text{ 임의의 } i \text{에 대해 } 1 \leq i \leq n] \leq \frac{1}{a^2} \text{Var}[S_n].$$

이 정리가 왜 더 강력한지 알 수 있습니다 — 체비셰프 부등식으로는 다음만 보일 수 있습니다

$$\Pr[|S_n| \geq a] \leq \frac{1}{a^2} \text{Var}[S_n].$$

따라서 같은 우변으로,  $|S_1| \geq a \vee |S_2| \geq a \vee \dots$ 의 확률도 공짜로 한계 지을 수 있습니다!

증명.  $A_i$ 를  $i$ 가  $|S_i| \geq a$ 를 만족하는 가장 작은 값이 되는 사건이라고 정의합니다. 그러면 위 좌변은 다음과 같습니다

$$\Pr[|S_i| \geq a \text{ 임의의 } i \text{에 대해 } 1 \leq i \leq n] = \Pr[A_1] + \Pr[A_2] + \dots + \Pr[A_n].$$

직관적으로, 만약 사건  $|S_i| \geq a$ 들이 독립이었다면, 우리가 할 수 있는 최선은 체비셰프 부등식을 사용하여 개별 확률 값들을 한계 짓는 것입니다

$$\Pr[|S_i| \geq a] \leq \frac{1}{a^2} \text{Var}[S_i]$$

하지만 이들은 전혀 독립이 아닙니다 — 사실, 이들은 양의 상관관계를 가지고 있습니다! 예를 들어, 다음이 성립합니다

$$\mathbb{E}[S_n \mid S_1 = a] = a$$

왜냐하면  $\mathbb{E}[X_2 + \dots + X_n] = 0$ 이기 때문입니다. 따라서 각  $X_i$ 가 대칭 분포를 따른다면,  $\Pr[S_n \geq a \mid S_1 = a] \geq \frac{1}{2}$ 이며, 이는  $a$ 가 클 때  $\frac{1}{a^2} \text{Var}[S_n]$ 보다 훨씬 큼니다.

여기 형식적인 증명이 있습니다. 각  $1 \leq i \leq n$ 에 대해, 다음이 성립합니다

$$\mathbb{E}[S_i^2 \mid A_i] \geq a^2$$

이는 다음과 동치입니다

$$\Pr[A_i] \leq \frac{1}{a^2} \mathbb{E}[S_i^2 \cdot \mathbf{1}_{A_i}]$$

그리고

$$\begin{aligned} \mathbb{E}[S_n^2 \cdot \mathbf{1}_{A_i}] &= \mathbb{E}[(S_i + (S_n - S_i))^2 \cdot \mathbf{1}_{A_i}] \\ &= \mathbb{E}[S_i^2 \cdot \mathbf{1}_{A_i}] + \mathbb{E}[S_i \cdot \mathbf{1}_{A_i}(S_n - S_i)] + \mathbb{E}[(S_n - S_i)^2 \cdot \mathbf{1}_{A_i}] \end{aligned}$$

가운데 항  $\mathbb{E}[S_i \cdot \mathbf{1}_{A_i}(S_n - S_i)]$ 은 0인데, 이는  $S_i \cdot \mathbf{1}_{A_i}$ 와  $S_n - S_i = X_{i+1} + \dots + X_n$ 이 독립이고  $\mathbb{E}[X_{i+1} + \dots + X_n] = 0$ 이기 때문이며, 마지막 항은  $\geq 0$ 입니다.

부등식들을 결합하면, 다음을 얻습니다

$$a^2 \Pr[A_i] \leq \mathbb{E}[S_n^2 \cdot \mathbf{1}_{A_i}].$$

모든  $i$ 에 대해 합하면 최종 결과를 얻습니다. □

일반화하면:

### 따름정리 41.3.7

$X_1, \dots$ 을 평균이 0인 독립 확률 변수라 합시다.  $S_i$ 를 위와 같이 정의합니다. 그러면

$$\Pr[|S_i| \geq a \text{ 임의의 } i \text{ 에 대해 } 1 \leq i] \leq \frac{1}{a^2} \sum_{1 \leq i} \text{Var}[X_i].$$

증명. 사건

$$|S_i| \geq a \text{ 임의의 } i \text{ 에 대해 } 1 \leq i \leq n$$

은 다음 사건의 부분집합입니다

$$|S_i| \geq a \text{ 임의의 } i \text{ 에 대해 } 1 \leq i \leq n+1$$

따라서 다음을 얻습니다

$$\Pr[|S_i| \geq a \text{ 임의의 } i \text{ 에 대해 } 1 \leq i] = \lim_{n \rightarrow \infty} \Pr[|S_i| \geq a \text{ 임의의 } i \text{ 에 대해 } 1 \leq i \leq n].$$

각  $\Pr[|S_i| \geq a \text{ 임의의 } i \text{ 에 대해 } 1 \leq i \leq n]$ 에 콜모고로프 부등식을 적용하면, 결과를 얻습니다.  $\square$

이제, 아이디어는 이를 수열의 꼬리에 적용하는 것입니다

$$X_1, \frac{X_2}{2}, \frac{X_3}{3}, \dots$$

따름정리에 의해, 모든  $\varepsilon > 0$ 에 대해, 거의 모든 세계에서, 임의의  $i \geq n_\varepsilon$ 에 대해  $|T_i - T_{n_\varepsilon}| < \frac{\varepsilon}{2}$ 가 되는  $n_\varepsilon$ 가 존재함을 알 수 있습니다. 삼각 부등식에 의해, 임의의  $i, j \geq n_\varepsilon$ 에 대해  $|T_i - T_j| < \varepsilon$ 가 됩니다.

코시 수렴 판정법에 의해, 이는 수열  $T_n$ 이 거의 모든 세계에서 수렴함을 의미합니다.

마지막으로, 원래 목표와의 관계는 다음과 같습니다

**주장 41.3.8** (원래 급수와의 관계).  $T_n$ 이 수렴하는 모든 세계에서,  $M_n$ 은 0으로 수렴합니다.

증명. 약간의 대수적 조작일 뿐입니다.  $M_n$ 을  $T_n$ 에 대해 표현해 보겠습니다.

다음을 얻습니다

$$X_n = n \cdot (T_n - T_{n-1})$$

따라서

$$\begin{aligned} M_n &= \frac{(T_1 - T_0) + 2(T_2 - T_1) + \dots + n(T_n - T_{n-1})}{n} \\ &= \frac{nT_n - (T_0 + T_1 + \dots + T_{n-1})}{n} \\ &= T_n - \frac{T_0 + T_1 + \dots + T_{n-1}}{n}. \end{aligned}$$

이제 이것은 쉽습니다:  $T_n$ 이 수렴한다고 할 때,  $\frac{T_0 + T_1 + \dots + T_{n-1}}{n}$ 도 같은 값으로 수렴해야 하므로(Cesàro 평균), 필요한 대로  $M_n \rightarrow 0$ 이 됩니다.  $\square$

**연습문제 41.3.9.** 역은 성립하지 않습니다:  $M_n \rightarrow 0$ 이라 해도,  $T_n$ 이 반드시 수렴하는 것은 아닙니다. 반례를 찾으십시오. ( $T_n$ 을  $M_n$ 에 대해 표현하고, 어떤 일이 일어나는지 살펴봅시다)

시오.)

**§41.3.iv 일반적인 증명**다음과 같이  
씁니다

기본 아이디어는 각  $X_i$ 의 값을 절단하여 각각이 유한한 분산을 갖도록 하는 것입니다.

**§41.4 생각해 볼 만한 조금 더 어려운 문제**

**문제 41A** (한정사 지옥). 확률 수렴의 정의에서  $\delta > 0$  대신  $\delta = 0$ 을 허용했다고 가정합니다. 수정된 정의가 거의 확실한 수렴과 동치임을 보이십시오.

**문제 41B** (거의 확실한 수렴은 위상화할 수 없음).  $\Omega = [0, 1]$  위의 모든 확률 변수의 공간을 생각합니다. 다음 명제를 참으로 만드는 거리를 이 공간에 부여하는 것이 불가능함을 증명하십시오:

확률 변수  $X_1, X_2, \dots$ 의 수열이  $X$ 로 거의 확실하게 수렴하는 것은  $X_i$ 가 그 거리에서  $X$ 로 수렴하는 것과 동치입니다.



# 42 정지된 마팅게일 (작성 예정)

## §42.1 거의 확실하게 돈을 버는 방법

이제 측도론에 대해 새로 얻은 지식을 카지노로 가져가 봅시다.

여기 가장 고전적인 예시가 있습니다: 카지노에서 공정한 동전 던지기에 원하는 만큼 베팅할 수 있는 게임을 하게 해주는데, 승률이 나쁩니다: 동전이 앞면이면  $\$n$ 을 따지만, 뒷면이면  $\$2n$ 을 잃습니다. 여기서  $n$ 의 값은 우리가 선택합니다. 제정신인 사람이라면 아무도 하고 싶어하지 않을 것 같은 게임처럼 보입니다.

그런데, 시간과 돈이 무제한이라면, 실제로 거의 확실하게 이익을 낼 수 있습니다.

### 예제 42.1.1 (18세기 프랑스보다도 더 탐욕스러워지기)

위 게임에서, 우리는  $\$1$ 을 베팅하며 시작합니다.

- 이기면,  $\$1$ 을 벌고 떠납니다.
- 지면, 대신  $\$10$ 을 베팅하고,
  - 이기면,  $\$10 - \$2 = \$8$ 을 벌고 떠나며,
  - 지면 대신  $\$100$ 을 베팅하고,
    - \* 이기면,  $\$1000 - \$20 - \$2 = \$978$ 을 벌고 떠나며,
    - \* 지면 대신  $\$1000$ 을 베팅하고, 이런 식으로 계속됩니다...

동전은 언젠가 거의 확실하게 앞면이 나올 것이므로, 그 일이 일어날 때마다 돈을 벌니다. 사실, 동전이 앞면을 보일 때까지 걸리는 기대 시간은 단 2번의 던지기입니다! 무엇이 잘못될 수 있을까요?

이 장에서는 “유한한 시간”이나 “유한한 돈”과 같은 정상적인 조건 하에서는, 실제로 이런 방식으로 돈을 벌 수 없다는 것을 보일 것입니다 — 바로 선택적 정지 정리입니다. 이는 조건부 확률을 정의할 구실을 마련해 주며, 그 다음 마팅게일(공정한 카지노를 일반화한 것)에 대해 이야기하게 될 것입니다.

라스베이거스에서 돈을 뽑아내려는 시도가 가망 없는 일임을 깨닫고 나면, 우리는 도박을 그만두고 수학 문제 풀이로 돌아가서, 도박과는 전혀 관계없어 보이는 문제들이 적절한 마팅게일을 고려함으로써 풀릴 수 있는 몇 가지 까다로운 놀라움들을 보여줄 것입니다.

이후 모든 내용에서,  $\Omega = (\Omega, \mathcal{A}, \mu)$ 는 확률 공간입니다.

## §42.2 부분 $\sigma$ -대수와 여과

**이 절의 대표적인 예:** 확률 변수로 생성된  $\sigma$ -대수, 그리고 동전 던지기 여과

우리는  $\Omega$ 를,  $\Omega$  위에서 적분을 할 수 있게 해주는  $\sigma$ -대수  $\mathcal{A}$ 를 갖춘 세계들의 공간으로 생각했습니다. 그러나 슬픈 삶의 진실은, 어느 주어진 시점에서든 세계에 대해 부분적인 정보만을 알 수 있다는 것입니다. 예를 들어, 이 글을 쓰는 시점에서, 우리는 세계가 2012년에 끝나지 않았다는 것을 알고 있지만 ([https://en.wikipedia.org/wiki/2012\\_phenomenon](https://en.wikipedia.org/wiki/2012_phenomenon) 참조), 앞으로 인류의 운명은 다소 불확실한 채로 남아 있습니다.

이를 측도론적으로 써 봅시다: 다음을 고려할 수 있습니다

$$\Omega = A \sqcup B$$

$$A = \{\omega \mid 2012\text{년에 세상이 끝나는 경우}\}$$

$$B = \{\omega \mid 2012\text{년에 세상이 끝나지 않는 경우}\}.$$

$A$ 와  $B$ 가 가측 집합, 즉  $A, B \in \mathcal{A}$ 라고 가정하겠습니다. 이는  $\mu(A)$ 와  $\mu(B)$ 의 값이 어떠해야 하는지에 대해("세상이 2012년에 끝날 사전 확률") 재미있게 논쟁할 수 있다는 뜻이지만, 이제 다른 엉뚱한 예시로 넘어갑시다.

이제 나중에 조건부 확률을 정의할 때 필요할 새로운 개념을 소개하겠습니다.

**정의 42.2.1.**  $\Omega = (\Omega, \mathcal{A}, \mu)$ 를 확률 공간이라 합시다.  $\Omega$  위의 **부분  $\sigma$ -대수**  $\mathcal{F}$ 는 말 그대로의 의미입니다: 집합  $\Omega$  위의  $\sigma$ -대수  $\mathcal{F}$ 로서, 각  $A \in \mathcal{F}$ 가 가측이도록 하는 것입니다(즉,  $\mathcal{F} \subseteq \mathcal{A}$ ).

그 동기는,  $\mathcal{F}$ 가 어떤 정보에 대해 질문을 던질 수 있게 해주는 집합들의  $\sigma$ -대수라는 것입니다. 예를 들어, 위에서 든 2012년 예시에서, 우리는  $\mathcal{F} = \{\emptyset, A, B, \Omega\}$ 로 둘 수 있는데, 이는 2012년만을 생각하고 있을 때 우리가 관심을 갖는 집합들입니다.

여기 좀 더 진지한 예시들이 있습니다.

**예제 42.2.2 (부분  $\sigma$ -대수의 예시)**

- (a)  $X: \Omega \rightarrow \{0, 1, 2\}$ 를 세 값 중 하나를 취하는 확률 변수라고 합시다. 만약 우리가  $X$ 에 관심이 있다면 다음과 같이 정의할 수 있습니다

$$A = \{\omega \mid X(\omega) = 1\}$$

$$B = \{\omega \mid X(\omega) = 2\}$$

$$C = \{\omega \mid X(\omega) = 3\}$$

그러면 다음과 같이 쓸 수 있습니다

$$\mathcal{F} = \{\emptyset, A, B, C, A \cup B, B \cup C, C \cup A, \Omega\}.$$

이것은 예컨대 " $X \neq 3$ 일 확률은 얼마인가"와 같이  $X$ 에 대한 질문을 할 수 있게 해주는  $\mathcal{F}$  위의 부분  $\sigma$ -대수입니다.

- (b) 이제  $Y: \Omega \rightarrow [0, 1]$ 가 또 다른 확률 변수라고 합시다. 만약 우리가  $Y$ 에 관심이 있다면, 우리의 궁금증을 담아내는  $\mathcal{F}$ 는 다음과 같습니다

$$\mathcal{F} = \{Y^{\text{pre}}(B) \mid B \subseteq [0, 1] \text{가측입니다}\}.$$

여기서 어떤 경향을 눈치챌 수도 있는데, 이제 이를 형식화합니다.

**정의 42.2.3.**  $X: \Omega \rightarrow \mathbb{R}$ 를 확률 변수라고 합시다.  $X$ 에 의해 생성된 **부분  $\sigma$ -대수**는 다음과 같이 정의됩니다

$$\sigma(X) := \{X^{\text{pre}}(B) \mid B \subseteq \mathbb{R} \text{가측입니다}\}.$$

만약  $X_1, \dots$ 가 확률 변수들의 (유한 또는 무한) 수열이라면, 이들에 의해 생성된 부분  $\sigma$ -대수는 각  $i$ 에 대해  $\sigma(X_i)$ 를 포함하는 가장 작은  $\sigma$ -대수입니다.

마지막으로, 이런 것들을 많이 모아볼 수 있습니다 — 시간에 대해 이야기하고 있으므로, 우리는 나이가 들수록 더 많은 것을 알게 되고, 이는 형식화될 수 있습니다.

**정의 42.2.4.**  $\Omega = (\Omega, \mathcal{A}, \mu)$  위의 **여과**는 중첩된 수열<sup>1</sup>

$$\mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \mathcal{F}_2 \subseteq \dots$$

$\Omega$  위의 부분  $\sigma$ -대수들의

**예제 42.2.5 (여과)**

무한히 긴 수업 시간에 지루해서 시간을 보내려고 공정한 동전을 던지기 시작했다고 합시다. (이에 따라  $\Omega = \{H, T\}^\infty$ 가 앞면  $H$ 와 뒷면  $T$ 의 무한 수열들로 이루어진다고 할 수 있습니다.)  $\mathcal{F}_n$ 이 처음  $n$ 번의 동전 던지기 값에 의해 생성된 부분  $\sigma$ -대수를 나타낸다고 합시다. 그러면:

- $\mathcal{F}_0 = \{\emptyset, \Omega\}$ ,
- $\mathcal{F}_1 = \{\emptyset, \text{첫 번째 던지기가 } H, \text{첫 번째 던지기가 } T, \Omega\}$ ,
- $\mathcal{F}_2 = \{\emptyset, \text{첫 두 번의 던지기가 } HH, \text{두 번째 던지기가 } T, \Omega, \text{첫 번째 던지기와 두 번째 던지기가 다른,}$
- 이런 식으로 계속되며,  $\mathcal{F}_n$ 은 오직 처음  $n$ 번의 동전 던지기에 의해서만 "결정되는" 가측 집합들입니다.

**연습문제 42.2.6.** 앞의 예시에서, 각 정수  $n$ 에 대해 크기  $|\mathcal{F}_n|$ 를 계산하십시오.

더 중요한 것은,

**$X$ 가  $\mathcal{F}$ 에 주어진 정보에 의해서만 결정된다면  $X$ 는  $\mathcal{F}$ -가측입니다.**

**예제 42.2.7**

위의 예시에서,  $X_3$ 을 세 번째 동전 던지기의 값이라고 합시다. 그러면:

- $X_3$ 은  $\mathcal{F}_2$ -가측이 아닙니다. (즉,  $X_3$ 은 처음 2번의 동전 던지기 정보만으로는 알 수 없습니다.)
- 하지만 이것은  $\mathcal{F}_3$ -가측입니다.

**연습문제 42.2.8.** 이를 확인하십시오! (함수는 열린집합을 가측 집합으로 끌어올릴 때 가측이라는 것을 상기하십시오. 따라서 예를 들어  $X_3^{\text{pre}}(\{H\}) \notin \mathcal{F}_2$ 임을 보여야 합니다.)

따라서, 우리는 세상에 대한 부분적인 정보를 형식화할 수 있을 뿐만 아니라, 무언가가 그 부분적인 정보에만 의존한다는 것이 무엇을 의미하는지도 형식화할 수 있습니다.

## §42.3 조건부 기댓값

**이 절의 대표적인 예:**  $[0, 1]$  위에 분포된  $X$ 와  $Y$ 에 대한  $\mathbb{E}(X \mid X + Y)$ 입니다.

마팅게일을 정의하기 위해서는 조건부 확률의 정의가 필요하지만, 이는 놀랍게도 까다로운 것으로 밝혀집니다. 그 이유를 살펴보기 위해 다음의 간단한 예시를 고려해 봅시다.

<sup>1</sup>편의를 위해  $\mathbb{Z}_{\geq 0}$ 로 색인된 여과로 한정하지만, 사실 어떤 색인 집합이든 상관없습니다.

**예제 42.3.1** (고등학교 수준의 방법이 여기서 충분하지 않은 이유)

$[0, 1]$  위에 균등하게 분포된 두 개의 독립적인 확률 변수  $X, Y$ 가 있다고 합시다 (그러므로  $\Omega = [0, 1]^2$ 로 두어도 무방합니다). 다음과 같은 질문을 던져 볼 수 있습니다:

“ $X + Y = 0.6$ 이라는 조건 하에서  $X$ 의 기댓값은 무엇인가?”

직관적으로, 답이 0.3이 되어야 함을 알고 있습니다. 하지만 정의를 적어 보려고 하면 곧 문제에 부딪히게 됩니다. 이상적으로는 다음과 같은 형태로 말하고 싶습니다

$$\mathbb{E}[X \text{ 주어진 } X + Y = 0.6] = \frac{\int_S X}{\int_S 1} \text{ 여기서 } S = \{\omega \in \Omega \mid X(\omega) + Y(\omega) = 0.6\}.$$

문제는  $S$ 가 측도가 0인 집합이라는 것으로, 이로 인해 곧 0에 부딪히게 되며, 이는 이러한 형태의 정의가 통하지 않는다는 것을 의미합니다.

측도론에서 이를 다루는 전형적인 방법은 우리가 정의한 부분- $\sigma$ -대수의 개념을 이용하는 것입니다.

하지만 먼저,  $\mathbb{E}(X \mid X + Y)$ 가 무엇을 의미하는지 설명해야 합니다 — 왜 사건이 아니라 다른 확률 변수에 대해 조건을 거는 것일까요?

확률 변수에 대해 조건을 거는 것의 동기를 설명하기 위해 다음의 상황을 고려해 봅시다. 내일의 날씨가 오늘의 날씨와 무작위적인 변동에 의존한다고 합시다. 그러면 다음과 같은 진술을 할 수 있습니다:

$$\begin{aligned} \Pr(\text{내일 비가 올} \mid \text{오늘 비가 올}) &= 0.6, \\ \Pr(\text{내일 비가 올} \mid \text{오늘 비가 오지 않음}) &= 0.3. \end{aligned}$$

이는 표준적인 조건부 확률입니다:  $\Pr(A \mid B) = \frac{\Pr(A \cap B)}{\Pr(B)}$ .

“오늘의 날씨” 자체가 확률 변수임에 유의하십시오.

$Z$ 를 오늘 밤 일기예보가 예측한 확률이라고 하고, 이것이 위와 같이 작동한다고 합시다. 그러면  $Z$ 는 다음과 같이 정의되는 확률 실숫값 변수입니다:

$$\begin{aligned} Z: \Omega &\rightarrow \mathbb{R} \\ Z(\omega) &= \Pr(\text{내일 비가 올} \mid \text{오늘의 날씨} = \text{오늘의 날씨}(\omega)) \end{aligned}$$

다음과 같이 적는 것만이 타당할 것입니다

$$Z = \Pr(\text{내일 비가 올} \mid \text{오늘의 날씨}).$$

우리는 확률 변수에 대해 조건을 걸고 있으며,  $\Pr(\dots \mid \dots)$  자체가  $\mathbb{R}$  안의 단일 값이 아니라 확률 변수인데, 이는 전혀 문제가 없습니다.

마찬가지로,  $\Omega$ 가 유한하고 그 모든 부분집합이 가측이라면, 확률 실숫값 변수  $X$ 와  $Y$ 에 대해 확률 실숫값 변수  $Z = \mathbb{E}(X \mid Y)$ 를 다음과 같이 정의하는 것이 합리적일 것입니다

$$\begin{aligned} Z: \Omega &\rightarrow \mathbb{R} \\ Z(\omega) &= \mathbb{E}[X \mid Y = Y(\omega)]. \end{aligned}$$

**예제 42.3.2**

$X$ 와  $Y$ 를 두 주사위를 굴린 결과라고 합시다. 그러면:

- $\mathbb{E}[X \mid X + Y = 3] = 1.5$ 이며, 이는 쉽게 계산할 수 있습니다.

- $\mathbb{E}(X \mid X+Y)$ 는 확률 변수로서,  $X+Y = 3$ 이든 아니든 모든 세계에서 값 1.5를 취할 것입니다.
- 더 일반적으로, 실제로 다음이 성립합니다

$$\mathbb{E}(X \mid X+Y) = \frac{X+Y}{2}.$$

확률 변수  $\mathbb{E}(X \mid X+Y)$ 가 오직  $X+Y$ 의 값에만 의존한다는 것에 주목하십시오 — 정의에 의해서 그러합니다.

물론, 앞서 설명했듯이, 이러한 소박한 시도는 연속적인 경우에 대해서는 어디서나 0으로 나누기를 야기합니다 — 그래서, 부분- $\sigma$ -대수가 등장하게 됩니다.

### 명제 42.3.3 (조건부 기댓값의 정의)

$X: \Omega \rightarrow \mathbb{R}$ 를 확률 공간  $\Omega$  위의 절대 적분가능한 확률 변수 (즉  $\mathbb{E}[|X|] < \infty$ 를 의미합니다)라 하고,  $\mathcal{F}$ 를 그 위의 부분- $\sigma$ -대수라 합시다.

그러면 다음 두 성질을 만족하는 함수  $\eta: \Omega \rightarrow \mathbb{R}$ 가 존재합니다:

- $\eta$ 는  $\mathcal{F}$ -가측입니다 (즉, 함수  $(\Omega, \mathcal{F}, \mu) \rightarrow \mathbb{R}$ 로서 가측입니다); 그리고
- 임의의 집합  $A \in \mathcal{F}$ 에 대해  $\mathbb{E}[\eta \cdot \mathbf{1}_A] = \mathbb{E}[X \cdot \mathbf{1}_A]$ 가 성립합니다.

더욱이, 이 확률 변수는 거의 확실히(almost surely) 유일합니다.

증명. 생략하지만, 관련된 전문 용어로 “라돈-니코딤 도함수(Radon-Nikodym derivative)”가 사용됩니다.  $\square$

**정의 42.3.4.**  $\eta$ 를 앞의 명제에서와 같이 놓읍시다.

- 우리는  $\eta$ 를  $\mathbb{E}(X \mid \mathcal{F})$ 로 표기하고, 이를  $\mathcal{F}$ 에 대한  $X$ 의 **조건부 기댓값(conditional expectation)**이라 부릅니다.
- $Y$ 가 확률 변수라면,  $\mathbb{E}(X \mid Y)$ 는  $\mathbb{E}(X \mid \sigma(Y))$ 를 나타내며, 즉  $Y$ 에 의해 생성된  $\sigma$ -대수에 대한  $X$ 의 조건부 기댓값을 의미합니다.

### 예제 42.3.5

예상할 수 있듯이,  $\eta = \frac{X+Y}{2}$ 는 위의  $\mathbb{E}(X \mid X+Y)$ 의 조건을 만족합니다.

이 모든 것을 하는 동기를 부여하는 방법은 다음과 같습니다. 우리는 다음과 같은 것을 말할 수 있기를 원합니다:

$$\mathbb{E}[X \mid X+Y = 0.6] = \lim_{\varepsilon \rightarrow 0} \mathbb{E}[X \mid 0.6 - \varepsilon < X+Y < 0.6 + \varepsilon]$$

안타깝게도,  $\mathcal{F}$ 가 단 하나의 확률 실수 변수에 의해 생성되지 않을 수도 있는 일반적인 경우에는 이러한 설정이 작동하지 않습니다. 위의 정의가 우리에게 어떻게 도움이 되는지 살펴봅시다.

- $A = \{\omega \in \Omega \mid 0.6 - \varepsilon < X(\omega) + Y(\omega) < 0.6 + \varepsilon\}$ 라 하면, 이 집합은 확실히  $X+Y$ 에 의해 생성된 부분- $\sigma$ -대수에 속합니다 (왜냐하면 이는  $(X+Y)^{\text{pre}}((0.6 - \varepsilon, 0.6 + \varepsilon))$ 이기 때문입니다).

- $\eta$ 가  $\mathcal{F}$ -가측이라는 것은  $\eta$ 가  $\mathcal{F} = \sigma(X + Y)$ 에 있는 정보에만, 즉  $X + Y$ 에만 의존한다는 것을 의미함을 상기하십시오. 이는 이치에 맞습니다.
- 우변을 살펴봅시다:

$$\mathbb{E}[X \mid 0.6 - \varepsilon < X + Y < 0.6 + \varepsilon] = \mathbb{E}[X \cdot \mathbf{1}_A].$$

전체 기댓값의 법칙(law of total expectation)은  $\mathbb{E}[\mathbb{E}(X \mid Y)] = \mathbb{E}[X]$ 라고 말합니다. 따라서 직관적으로, 위의 두 번째 성질은 단순히 이 법칙이 모든 집합  $A \in \mathcal{F}$ 에 대해 성립할 것을 요구합니다.

우리의 경우, 다음과 같습니다:

$$\mathbb{E}[\eta \mid 0.6 - \varepsilon < X + Y < 0.6 + \varepsilon] = \mathbb{E}[X \mid 0.6 - \varepsilon < X + Y < 0.6 + \varepsilon].$$

좀 더 자세한 설명:

**비고 42.3.6 (이 표기법은 형편없습니다)** —  $\mathbb{E}(X \mid \mathcal{F})$ 라는 표기법은 인정하건대 혼란스러운데, 이는 실제로  $\mathbb{E}[X]$ 와 같은 단순한 실수가 아니라 함수 전체  $\Omega \rightarrow \mathbb{R}$ 이기 때문입니다 — 그러나 보시다시피, 나름의 장점이 있습니다. 이러한 이유로 저는 조건부 기댓값에 대해서는 대괄호가 아니라 소괄호를 사용하는 것을 잊지 않도록 조심하려 합니다; 모두가 이렇게 하는 것은 아닙니다.

**표기의 남용 42.3.7.** 또한,  $Y = \mathbb{E}(X \mid \mathcal{F})$ 라고 쓸 때, 여기에는 어느 정도의 표기법 남용이 발생하고 있는데, 이는  $\mathbb{E}(X \mid \mathcal{F})$ 가 어느 정도 합리적인 유일성까지만(즉, 측도 0인 변화까지는 허용하여) 정의되기 때문입니다. 따라서 이는 실제로는 “ $Y$ 가 **명제 42.3.3**의 가정을 만족한다”는 것을 의미하지만, 이는 너무 세밀해서 아무도 신경 쓰지 않습니다.

예를 들어, 위의 예시에서 만약  $\eta$ 를 다음과 같이 바꾸면

$$\eta(\omega) = \begin{cases} 0 & \text{만약 } X(\omega) + Y(\omega) = 0.6 \\ \frac{X(\omega) + Y(\omega)}{2} & \text{그렇지 않으면} \end{cases}$$

그러면  $\mathbb{E}[\eta \cdot \mathbf{1}_A] = \mathbb{E}[X \cdot \mathbf{1}_A]$ 는 모든 집합  $A$ 에 대해 여전히 성립하지만, 이제 이는  $\mathbb{E}[X \mid X + Y = 0.6] = 0$ 이라고 말하는 것처럼 보이지 않습니까?

그럼에도 불구하고, 우리는 측도 0인 집합을 희생해야 한다는 데 동의해야 하는데, 그렇지 않으면 다음과 같은 경우

$$T(\omega) = \begin{cases} 1 & \text{만약 } Y(\omega) > 0.5 \text{ 또는 } (Y(\omega) = 0.5 \text{ 그리고 } X(\omega) \in \mathbb{Q}) \\ 0 & \text{그렇지 않으면} \end{cases}$$

그러면 이는 확실히 가측이지만(즉, 확률 변수이지만),  $\mathbb{E}[T \mid Y = 0.4] = 0$ 이고  $\mathbb{E}[T \mid Y = 0.6] = 1$ 인데,  $\mathbb{E}[T \mid Y = 0.5]$ 는 무엇입니까? (여러분은 이것이 0이어야 한다고 주장할 수도 있지만,  $\mathbb{Q}$ 가 더욱 비가측적인 어떤 것으로 바뀐다면 어떻게 되겠습니까? 게다가, 확률이 0인 집합에서만  $T$ 를 수정했을 뿐인데 조건부 기댓값이 왜 바뀌어야 합니까?)

성질

## §42.4 슈퍼마팅게일

**이 절의 대표적인 예:** 하우스 확률을 가정할 때, 카지노를 방문하는 것은 슈퍼마팅게일입니다.

**정의 42.4.1.**  $X_0, X_1, \dots$  를 확률 공간  $\Omega$  위의 확률 변수의 수열이라 하고,  $\mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \dots$  를 여과라 합시다.

그러면 다음 조건들이 성립할 때  $(X_n)_{n \geq 0}$  는  $(\mathcal{F}_n)_{n \geq 0}$  에 대한 **슈퍼마팅게일**입니다:

- $X_n$  은 모든  $n$ 에 대해 절대 적분 가능합니다;
- $X_n$  은  $\mathcal{F}_n$  에 대해 가측입니다; 그리고
- 각  $n = 1, 2, \dots$  에 대해 부등식

$$\mathbb{E}(X_n \mid \mathcal{F}_{n-1}) \leq X_{n-1}$$

은 모든  $\omega \in \Omega$  에 대해 성립합니다.

**서브마팅게일**에서는 부등식  $\leq$  가  $\geq$  로 대체되며, **마팅게일**에서는  $=$  로 대체됩니다.

이 용어의 어원은 무엇인가요?

**표기의 남용 42.4.2** (어차피 그 여과라는 것을 쓰는 사람은 아무도 없습니다). 우리는 항상  $\mathcal{F}_n$  을 이전 변수들  $X_0, X_1, \dots, X_{n-1}$  로 생성되는  $\sigma$ -대수로 취할 것이며, 이에 대해 따로 언급하지 않겠습니다. 그럼에도 이어지는 모든 결과는 어떤 여과에 대한 슈퍼마팅게일이라는 더 일반적인 상황에서도 성립합니다.

우리는 모든 정리를 슈퍼마팅게일에 대해 증명할 것입니다; 서브마팅게일에 대한 유사한 버전은 모든 곳에서  $\leq$  를  $\geq$  로 대체하여 얻을 수 있고 ( $X_n$  이 마팅게일인 것과  $-X_n$  이 슈퍼마팅게일인 것이 동치이므로), 마팅게일에 대해서는 모든 곳에서  $\leq$  를  $=$  로 대체하여 얻을 수 있습니다 ( $X_n$  이 마팅게일인 것과 그것이 슈퍼마팅게일이면서 동시에 서브마팅게일인 것이 동치이므로).

예시를 들어봅시다.

#### 예제 42.4.3 (슈퍼마팅게일)

- (a) **랜덤 워크:** 개미 한 마리가 수직선 위의 위치 0 에서 출발합니다. 매 분마다 이 개미는 공정한 동전을 던져 왼쪽으로 한 칸 건너거나 오른쪽으로 한 칸 걸습니다.  $X_t$  가  $t$ 번째 시각의 위치라면,  $X_t$  는 마팅게일인데, 그 이유는

$$\mathbb{E}(X_t \mid X_0, \dots, X_{t-1}) = \frac{(X_{t-1} + 1) + (X_{t-1} - 1)}{2} = X_{t-1}.$$

- (b) **카지노 게임:** 이 장의 도입부에서 설명한 전략을 사용하는 도박꾼을 생각해 봅시다. 도박꾼이 거는 모든 배팅의 기댓값이 0 이므로, 이는 마팅게일입니다.
- (c) **독립 변수의 곱:**  $X_1, X_2, \dots$  를 (반드시 동일하게 분포하지는 않는) 평균이 1인 독립인 적분 가능 확률 변수들이라 합시다. 그러면 다음과 같이 정의되는 수열  $Y_1, Y_2, \dots$  는

$$Y_n := X_1 X_2 \cdots X_n$$

$$\mathbb{E}(Y_n \mid Y_1, \dots, Y_{n-1}) = \mathbb{E}[X_n] \cdot Y_{n-1} = Y_{n-1} \text{ 이므로 마팅게일입니다.}$$

- (d) **반복 블랙잭:** 어떤 사람이 카지노에 가서 무한히 많은 블랙잭 게임을 한다고 합시다.  $X_t$  가 시각  $t$ 에서의 그의 재산이라면,  $X_t$  는 슈퍼마팅게일입니다. 이는 각 게임의 기댓값이 음수이기 때문입니다 (하우스 엣지).

**예제 42.4.4 (경박한/도발적인 예시 — 실생활은 슈퍼마팅게일이다)**

$X_t$  를 당신 인생의  $t$ 번째 날의 행복도라 합시다. 인생에는 오르막과 내리막이 있으므로, 모든  $t$ 에 대해  $X_t \leq X_{t-1}$  인 것은 아닙니다. 예를 들어, 어느 날 복권에 당첨될 수도 있습니다.

그러나 어느 특정한 날이든 여러 가지 일이 잘못될 수 있으며 (예: 좀비 대재앙), 머피의 법칙에 따르면 이것이 일이 잘 풀리는 것보다 더 가능성이 높습니다. 또한 나이가 들수록 책임은 점점 늘어나고 건강은 점차 나빠지기 시작합니다. 따라서 다음과 같은 것이

$$\mathbb{E}(X_t \mid X_0, \dots, X_{t-1}) \leq X_{t-1}$$

미래에 대한 합리적인 설명으로 보입니다 — 기댓값 상으로는, 각 연속하는 날이 이전 날보다 조금씩 더 나쁩니다. (특히 죽음이 닥쳤을 때  $X_t = -\infty$  로 설정한다면, 죽을 확률이 양수인 한 위에 제시된 부등식은 자명하게 참입니다.)

계속하기 전에, 증명 없이 유용한 결과 하나를 제시하겠습니다: 마르팅게일이 유계이면, 그것은 거의 확실하게 수렴합니다.

**정리 42.4.5 (둑의 마르팅게일 수렴 정리)**

$X_0, \dots$  를 확률 공간  $\Omega$  위의 상마르팅게일(supermartingale)이라 하고 다음을 만족한다고 합시다

$$\sup_{n \in \mathbb{Z}_{\geq 0}} \mathbb{E}[|X_n|] < \infty.$$

그러면, 다음을 만족하는 확률변수  $X_\infty: \Omega \rightarrow \mathbb{R}$  가 존재합니다

$$X_n \xrightarrow{\text{a.s.}} X_\infty.$$

**§42.5 선택적 정지(Optional stopping)**

이 절의 대표적인 예: 라스베이거스.

첫 번째 절에서 우리는 거의 확실하게 돈을 버는 방법을 설명했습니다. 도박꾼이 가진 핵심적인 이점은 원할 때 언제든지 그만둘 수 있는 능력이었습니다(이는 판돈의 크기를 조절할 수 있는 능력과 동치입니다; 영원히 \$0을 거는 것은 그만두는 것과 같습니다). 정지 시간(stopping time)이라는 개념을 formalize해봅시다.

아이디어는 다음을 만족하는 함수  $\tau: \Omega \rightarrow \{0, 1, 2, \dots\} \cup \{\infty\}$  를 정의하고자 하는 것입니다

- $\tau(\omega)$  는 그 이후에 마르팅게일을 정지시키는 인덱스를 지정합니다. 시각  $n$  이후 정지할지에 대한 결정은 그 시점에 이용 가능한 정보만을 사용하여 이루어져야 함에 유의하십시오 — 즉, 필터레이션의  $\mathcal{F}_n$  에 대해서만 이루어져야 합니다.
- $X_{\tau \wedge n}$  은 정지된 마르팅게일의 시각  $n$  에서의 값을 나타내는 확률변수이며, 만약  $n$  이 정지 시간 이후라면, 우리는 그것을 단지 우리가 떠난 이후의 현재 값으로 취합니다. 예를 들어, 시각 3 에서 정지한 세계  $\omega$  에서는,  $X_{\tau \wedge 0}(\omega) = X_0(\omega)$ ,  $X_{\tau \wedge 1}(\omega) = X_1(\omega)$ ,  $X_{\tau \wedge 2}(\omega) = X_2(\omega)$ ,  $X_{\tau \wedge 3}(\omega) = X_3(\omega)$  이지만, 그 이후에는

$$X_3(\omega) = X_{\tau \wedge 4}(\omega) = X_{\tau \wedge 5}(\omega) = X_{\tau \wedge 6}(\omega) = \dots$$

우리가 정지했으므로 — 값이 더 이상 변하지 않습니다.

- $X_\tau$  는 정지 이후의 최종 값을 나타냅니다(또는 만약 결코 정지하지 않는다면 극한  $X_\infty$  를 나타냅니다).

여기 컴파일된 기계어 코드가 있습니다.

**정의 42.5.1.**  $\mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \dots$  를 확률 공간  $\Omega$  위의 필터레이션이라 합시다.

- **정지 시간(stopping time)**이란 다음과 같은 함수입니다

$$\tau: \Omega \rightarrow \{0, 1, 2, \dots\} \cup \{\infty\}$$

각 정수  $n$  에 대해, 다음 집합이

$$\{\omega \in \Omega \mid \tau(\omega) = n\}$$

$\mathcal{F}_n$ -가측(즉,  $\mathcal{F}_n$  에 속함)이라는 성질을 갖습니다.

- 각  $n \geq 0$  에 대해, 우리는  $X_{\tau \wedge n}: \Omega \rightarrow \mathbb{R}$  를 다음과 같이 정의합니다

$$X_{\tau \wedge n}(\omega) = X_{\min\{\tau(\omega), n\}}(\omega)$$

- 마지막으로, 우리는 최종 결과를 다음과 같이 나타내겠습니다

$$X_\tau(\omega) = \begin{cases} X_{\tau(\omega)}(\omega) & \tau(\omega) \neq \infty \\ \lim_{n \rightarrow \infty} X_n(\omega) & \tau(\omega) = \infty \text{ 그리고 } \lim_{n \rightarrow \infty} X_n(\omega) \text{ 존재함} \\ \text{정의되지 않음} & \text{그렇지 않으면.} \end{cases}$$

우리는 "정의되지 않은" 경우가 오직 측도 0인 집합에 대해서만 발생하기를 요구합니다(예를 들어, **정리 42.4.5** 가 적용되는 경우입니다). 그렇지 않으면 우리는  $X_\tau$  가 정의되도록 허용하지 않습니다.

**명제 42.5.2** (정지된 상마르팅게일은 여전히 상마르팅게일이다)

$X_0, X_1, \dots$  를 상마르팅게일이라 합시다. 그러면 다음 수열은

$$X_{\tau \wedge 0}, X_{\tau \wedge 1}, \dots$$

그 자체로 상마르팅게일입니다.

**증명.** 우리는 거의 어디서나 다음 부등식들을 갖습니다

$$\begin{aligned} \mathbb{E}(X_{\tau \wedge n} \mid \mathcal{F}_{n-1}) &= \mathbb{E}(X_{n-1} + \mathbf{1}_{\tau(\omega)=n-1}(X_n - X_{n-1}) \mid \mathcal{F}_{n-1}) \\ &= \mathbb{E}(X_{n-1} \mid \mathcal{F}_{n-1}) + \mathbb{E}(\mathbf{1}_{\tau(\omega)=n-1} \cdot (X_n - X_{n-1}) \mid \mathcal{F}_{n-1}) \\ &= X_{n-1} + \mathbf{1}_{\tau(\omega)=n-1} \cdot \mathbb{E}(X_n - X_{n-1} \mid \mathcal{F}_{n-1}) \leq X_{n-1} \end{aligned}$$

$\Omega \rightarrow \mathbb{R}$ 로 가는 함수로서.

□

**정리 42.5.3 (Doob의 최적 정지 정리)**

$X_0, X_1, \dots$  을 확률 공간  $\Omega$  위에서, 필터레이션  $\mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \dots$ 에 대한 초마팅계일이라고 합시다.  $\tau$ 를 이 필터레이션에 대한 정지 시간이라고 합시다. 어떤 상수  $C$ 에 대해 다음 가정 중 어느 것이든 성립한다고 가정합니다:

- (a) **유한 시간:** 거의 모든  $\omega$ 에 대해  $\tau(\omega) \leq C$ 입니다.
- (b) **유한 자금:** 각  $n \geq 1$ 에 대해, 거의 모든  $\omega$ 에 대해  $|X_{\tau \wedge n}(\omega)| \leq C$ 입니다.
- (c) **유한 베팅:**  $\mathbb{E}[\tau] < \infty$ 이며, 각  $n \geq 1$ 에 대해 조건부 기댓값

$$\mathbb{E}(|X_n - X_{n-1}| \mid \mathcal{F}_n)$$

은  $\tau(\omega) \geq n$ 을 만족하는 거의 모든  $\omega \in \Omega$ 에 대해 최대  $C$ 의 값을 취합니다. 그러면  $X_\tau$ 는 거의 모든 곳에서 잘 정의되며, 더 중요하게는 다음이 성립합니다.

$$\mathbb{E}[X_\tau] \leq \mathbb{E}[X_0].$$

마지막 식은 장난스럽게 "유일한 승리 수는 플레이하지 않는 것이다"라고 표현할 수 있습니다.

오늘 밤 나중  
에 하기

증명.

□

**연습문제 42.5.4.** 첫 절에서 설명한 전략을 가지고 라스베이거스에 가는 것은 정말 나쁜 생각이라는 것을 결론지으십시오. 무엇이 잘못되는 것입니까?

이것이 우리가 도박을 그만두게 만드는 데는 유용하지만, 무언가를 계산할 수 있게 해주지는 않습니다 — 우리는  $\mathbb{E}[X_\tau]$ 에 대해 그것이  $\leq \mathbb{E}[X_0]$ 라는 것 외에는 아무것도 알지 못합니다. 그러나:

**따름정리 42.5.5**

위와 동일한 가정 하에서:

- 만약  $X_0, X_1, \dots$  가 준마팅계일이면,  $\mathbb{E}[X_\tau] \geq \mathbb{E}[X_0]$ 입니다.
- 만약 이것이 마팅계일이면,  $\mathbb{E}[X_\tau] = \mathbb{E}[X_0]$ 입니다.

증명. 만약  $X_0, X_1, \dots$  가 준마팅계일이면,  $Y_i = -X_i$ 로 정의된  $Y_0, Y_1, \dots$  는 초마팅계일이며, 가정은 여전히 만족됩니다. 정리를  $Y_\tau$ 에 적용하면 결과를 얻습니다.

만약  $X_0, X_1, \dots$  가 마팅계일이면, 이것은 초마팅계일이면서 동시에 준마팅계일이므로, 결과는 즉시 따라옵니다. □

이로써 마침내 우리는 무언가를 계산할 수 있게 됩니다 — 만약  $\mathbb{E}[X_0]$ 를 계산할 수 있고 그 결과를 어떤 마팅계일에 대한  $\mathbb{E}[X_\tau]$ 로 쓸 수 있다면, 우리는 문제를 풀 수 있습니다!

**§42.6 최적 정지의 재미있는 응용 (작성 예정)**

이제 우리는 지금까지 개발한 결과들의 위력을 보여주는 세 가지 문제를 제시합니다.

### §42.6.i 투표 문제

Alice와 Bob이 선거에서 경쟁하고 있다고 합시다. Alice는 총  $a$ 표를, Bob은 총  $b$ 표를 받았으며,  $a > b$ 입니다. 표가 무작위 순서로 선택된다면, Alice가 선거 내내 Bob보다 엄격하게 앞서 있을 확률은 얼마인지 물을 수 있습니다.



#### 명제 42.6.1 (투표 문제)

이것은 확률  $\frac{a-b}{a+b}$ 로 발생합니다.

우리는 이것을 마팅게일로 모델링해 보아야 합니다. 이를 수행하는 자연스러운 방법은 [예제 42.4.3](#)에서와 같은 무작위 보행입니다:

$$X_0 = 0$$

$$X_i = X_{i-1} + \begin{cases} 1 & \text{확률로 } \frac{1}{2} \\ -1 & \text{그렇지 않으면.} \end{cases}$$

여기서 각 1은 앨리스가 표를 얻는 것을 나타내고, 각 -1은 밥이 표를 얻는 것을 나타냅니다. 그러면 우리는 다음을 계산해야 합니다

$$\Pr[X_i > 0 \text{ 모든 것에 대하여 } 1 \leq i \leq a+b \mid X_{a+b} = a-b].$$

이것이 자연스럽기는 하지만, 확률이  $X_{a+b} = a-b$ 에 조건화되어 있다는 사실 때문에 선택적 정지 정리를 적용할 수 없습니다.

대신 다음과 같은 방법이 통합니다: 모든 표에서 시작하여, 무작위 순서로 그것들을 제거합니다.

$$(A_0, B_0) = (a, b),$$

$$(A_i, B_i) = \begin{cases} (A_{i-1} - 1, B_{i-1}) & \text{확률로 } \frac{A_{i-1}}{A_{i-1} + B_{i-1}} \\ (A_{i-1}, B_{i-1} - 1) & \text{그렇지 않으면} \end{cases} \quad \text{에 대하여 } 1 \leq i \leq a+b.$$

물론 여기서  $A_i$ 는 앨리스에게 남은 표의 수를 나타내고,  $B_i$ 는 밥에게 남은 표의 수를 나타냅니다.

이제 우리는 다음을 계산하기만 하면 됩니다

$$\Pr[A_i > B_i \text{ 모든 것에 대하여 } 0 \leq i \leq a+b-1].$$

더 이상 조건부 기댓값이 없습니다!

다음으로 우리는 마팅게일을 구성해야 합니다. 위와 비슷하게  $X_i = A_i - B_i$ 로 정의해 볼 수도 있지만, 그것은 마팅게일이 되지 않습니다.

여기 요령이 있습니다: 우리는  $X_i$ 를 수정하여 마팅게일로 만듭니다. (확률 변수의 수열을 수정하여 마팅게일을 만드는 더 많은 예시는 [문제 42A](#)에서 찾을 수 있습니다.)

**예제 42.6.2**

$a = 2$ 이고  $b = 1$ 이라고 합시다. 그러면:

$$(A_0, B_0) = (2, 1),$$

$$(A_1, B_1) = \begin{cases} (1, 1) & \text{확률로 } \frac{2}{3} \\ (2, 0) & \text{그렇지 않으면.} \end{cases}$$

그러므로  $\mathbb{E}[A_0 - B_0] = 1$ 인 반면  $\mathbb{E}[A_1 - B_1] = \frac{2}{3} \cdot 0 + \frac{1}{3} \cdot 2 = \frac{2}{3}$ 이므로, 만약 우리가  $X_i$ 를 위와 같이 정의한다면 물론 마팅계일이 되지 않을 것입니다.

하지만 그것을 수정하여 마팅계일을 만드는 방법을 찾는 것은 어렵지 않습니다. 예를 들면:

- 만약 우리가  $X_1 = A_1 - B_1 + \frac{1}{3}$ 로 정의한다면,  $\mathbb{E}[X_1] = 1$ 이 되므로 문제없습니다.
- 마찬가지로, 우리는  $X_1 = \frac{3}{2} \cdot (A_1 - B_1)$ 로도 정의할 수 있습니다.
- 또는  $X_1 = \frac{9}{4} \cdot (A_1 - B_1)^2$ 로도 정의할 수 있습니다.
- ... 기타 등등...

우리는 모든  $i$ 와 모든  $(x_0, x_1, \dots, x_{i-1})$ 에 대해  $\mathbb{E}[X_i \mid X_0 = x_0, X_1 = x_1, \dots, X_{i-1} = x_{i-1}] = x_{i-1}$ 이 되도록 만들어야 합니다. (계속 읽기 전에 어떤 수정이 통할지 스스로 알아내 보십시오.)

알고 보니, 다음과 같은 방법이 통합니다:

$$X_i = \frac{A_i - B_i}{a + b - i} \text{에 대하여 } 0 \leq i \leq a + b - 1.$$

우리는 이것을  $i \geq a + b$ 까지 확장할 수 없지만, 그것으로 충분합니다. (걱정된다면,  $i \geq a + b$ 에 대해 그냥  $X_i = X_{a+b-1}$ 로 정의하십시오.)

**연습문제 42.6.3.** 이것이 작동하는지 확인해 보십시오. (이 수학적 계산은 [문제 42A](#)의 폴야의 항아리(Pólya's urn) 문제와 매우 유사합니다.)

정지 시간에 대해서는, 그것을 정의하는 자연스러운 방법이 하나뿐입니다: 모든  $0 \leq i \leq a + b - 1$ 에 대해  $X_i > 0$ 이어서 앨리스가 밥보다 계속 앞서 있다면  $\tau$ 는  $a + b - 1$ 이고, 그렇지 않다면  $\tau$ 는  $X_i = 0$ 이 되는 가장 작은  $i$ 입니다.

그러면 선택적 정지 정리는 다음을 말해 줍니다:

$$\mathbb{E}[X_\tau] = \mathbb{E}[X_0].$$

$\mathbb{E}[X_0]$ 는 계산하기 쉬운데, 그것은  $\frac{A_0 - B_0}{a + b} = \frac{a - b}{a + b}$ 입니다.  $\mathbb{E}[X_\tau]$ 는 무엇일까요?

- 만약 앨리스가 밥보다 계속 앞서 있다면,  $X_\tau = X_{a+b-1} = 1$ 입니다.
- 그렇지 않으면  $X_\tau = 0$ 입니다.

따라서  $\mathbb{E}[X_\tau]$ 는 정확히 우리가 계산해야 하는 확률이므로, 증명이 완료됩니다.

**비고 42.6.4 (이것은 약간 반칙입니다)** — 다음과 같이 동등하게 쓸 수 있음에 유의하십시오

$$X_i = \frac{A_i - B_i}{A_i + B_i}.$$

이것이 정확히 답의 형태입니다.

즉, 답의 형태를 이미 알고 있다면 마팅게일 이론이 그것을 확인하는 데 도움이 될 수 있습니다. 하지만 모른다면...

### §42.6.ii ABRACADABRA

작성 예정입니다.

<https://www.jeremykun.com/2014/03/03/martingales-and-the-optional-stopping-theorem/>

### §42.6.iii USA TST 2018

작성 예정입니다.

<https://aops.com/community/p9513099>

## §42.7 생각해 볼 만한 조금 더 어려운 문제

**문제 42A** (마팅게일의 예시). 마팅게일의 몇 가지 예시를 더 제시하겠습니다.

- (a) (**단순 확률보행**)  $X_1, X_2, \dots$  를 확률  $1/2$ 로  $+1$ 이 되고 확률  $1/2$ 로  $-1$ 이 되는 독립동일 분포 확률변수라 하십시오. 다음이

$$Y_n = (X_1 + \dots + X_n)^2 - n$$

마팅게일임을 증명하십시오.

- (b) (**드무아브르 마팅게일**)  $p, q > 0$ 이고  $p + q = 1$ 인 실수  $p$ 와  $q$ 를 고정하십시오.  $X_1, X_2, \dots$  을 확률  $p$ 로  $+1$ 과 같고, 확률  $q$ 로  $-1$ 과 같은 독립 항등 분포 확률 변수라고 합시다. 다음이

$$Y_n = (qp^{-1})^{X_1 + X_2 + \dots + X_n}$$

마팅게일임을 보이십시오.

- (c) (**폴리아의 항아리**) 항아리에 처음에 빨간 구슬 하나와 파란 구슬 하나가 들어 있습니다. 매분마다 항아리에서 구슬 하나를 무작위로 꺼내고, 같은 색깔의 구슬 두 개를 항아리에 더 넣습니다. 따라서  $n$ 분 후에는 항아리에  $n + 2$ 개의 구슬이 있게 됩니다.

$r_n$ 을 빨간 구슬의 비율이라 하십시오.  $r_n$ 이 마팅게일임을 보이십시오.

**문제 42B.** 카드 덱에는 52장의 카드가 있으며, 그중 26장은 빨간색이고 26장은 검은색입니다. 카드는 한 장씩 뽑혀 공개됩니다. 어느 시점에서든 덱에 카드가 최소 한 장 남아 있으면 딜러를 멈출 수 있으며, 덱의 다음 카드가 빨간색인 경우에만(그리고 그 경우에 한해) 승리합니다. 모든 카드가 다 뽑히면 패배합니다. 가능한 모든 전략 중에서, 승리할 최대 확률을 구하십시오.

**문제 42C** (발드의 항등식).  $\mu$ 를 실수라 하십시오.  $X_1, X_2, \dots$  를 확률 공간  $\Omega$  위에서 정의된, 평균이  $\mu$ 인 독립 확률변수라 하십시오. 마지막으로  $\tau: \Omega \rightarrow \{1, 2, \dots\}$ 를  $\mathbb{E}[\tau] < \infty$ 이고 사건  $\tau = n$ 이 오직  $X_1, \dots, X_n$ 에만 의존하는 멈춤 시각이라 하십시오.

다음을 증명하십시오

$$\mathbb{E}[X_1 + X_2 + \dots + X_\tau] = \mu \mathbb{E}[\tau].$$

**문제 42D** (편향 없는 취객의 보행). 개미가 수직선 위의 0에서 출발하여, 확률  $1/2$ 로 왼쪽 또는 오른쪽으로 한 칸씩 이동합니다. 개미는  $-17$  또는  $+8$ 에 도달하면 멈춥니다.

(a)  $-17$ 보다 먼저  $+8$ 에 도달할 확률을 구하십시오.

(b) 두 끝점 중 하나에 도달하는 데 걸리는 시간의 기댓값을 구하십시오.

**문제 42E** (편향된 취객의 걸음).  $0 < p < 1$ 을 실수라 하십시오. 개미가 수직선 위 0에서 출발하여, 확률  $p$ 로 좌우로 한 칸씩 걸읍니다. 개미는  $-17$  또는  $+8$  중 하나에 도달하면 멈춥니다. 개미가  $+8$ 에 먼저 도달할 확률을 구하십시오.

**문제 42F**. 칠판에 숫자 1이 적혀 있습니다. 매 분마다, 칠판에 숫자  $a$ 가 적혀 있으면 그것을 지우고 구간  $[0, 2.01a]$ 에서 균등하게 무작위로 선택한 실수로 대체합니다. 그 결과로 얻어지는 수열이 0에 접근할 확률은 얼마입니까?

# XII

미분기하학

## 제XII부: 목차

---

|           |                                                               |            |
|-----------|---------------------------------------------------------------|------------|
| <b>43</b> | <b>올바르게 하는 다변수 미적분학</b>                                       | <b>453</b> |
| 43.1      | 전미분 . . . . .                                                 | 453        |
| 43.2      | 사영 원리 . . . . .                                               | 455        |
| 43.3      | 전미분과 편미분 . . . . .                                            | 456        |
| 43.4      | (선택) 고계 도함수에 관한 소고 . . . . .                                  | 458        |
| 43.5      | 미분 형식을 향하여 . . . . .                                          | 459        |
| 43.6      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                | 459        |
| <br>      |                                                               |            |
| <b>44</b> | <b>미분 형식</b>                                                  | <b>461</b> |
| 44.1      | 미분 형식의 그림 . . . . .                                           | 461        |
| 44.2      | 외미분의 그림 . . . . .                                             | 463        |
| 44.3      | 미분 형식 . . . . .                                               | 464        |
| 44.4      | 외미분 . . . . .                                                 | 466        |
| 44.5      | 여담: $\bigwedge^k(V^\vee)$ 대 $(\bigwedge^k(V))^\vee$ . . . . . | 467        |
| 44.6      | 결가지 언급: 호의 길이 $ds$ 는 1-형식이 아닙니다 . . . . .                     | 470        |
| 44.7      | 단형 형식과 완전 형식 . . . . .                                        | 471        |
| 44.8      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                | 472        |
| <br>      |                                                               |            |
| <b>45</b> | <b>미분 형식 적분하기</b>                                             | <b>473</b> |
| 45.1      | 동기: 선적분 . . . . .                                             | 473        |
| 45.2      | 당겨오기 . . . . .                                                | 474        |
| 45.3      | 세포 . . . . .                                                  | 475        |
| 45.4      | 경계 . . . . .                                                  | 477        |
| 45.5      | 스토크스 정리 . . . . .                                             | 479        |
| 45.6      | 다시 현실로: 벡터 미적분학에서 배운 내용과의 비교 . . . . .                        | 479        |
| 45.7      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                | 483        |
| <br>      |                                                               |            |
| <b>46</b> | <b>다양체에 대한 약간의 이야기</b>                                        | <b>485</b> |
| 46.1      | 위상 다양체 . . . . .                                              | 485        |
| 46.2      | 매끄러운 다양체 . . . . .                                            | 486        |
| 46.3      | 정칙값 정리 . . . . .                                              | 487        |
| 46.4      | 다양체 위의 미분 형식 . . . . .                                        | 488        |
| 46.5      | 방향 . . . . .                                                  | 488        |
| 46.6      | 다양체에 대한 스토크스 정리 . . . . .                                     | 489        |
| 46.7      | (선택) 접공간과 여접공간 . . . . .                                      | 490        |
| 46.8      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                                | 492        |

---

# 43 올바르게 하는 다변수 미적분학

전에도 불평한 적이 있듯이, 선형대수학은 행렬을 과도하게 사용하여 선형 사상의 구조를 흐리게 함으로써 잘못된 방식으로 다루어지고 있습니다. 다변수 미적분학에서도 비슷한 문제가 발생하므로, 여기서 바로잡고자 합니다.

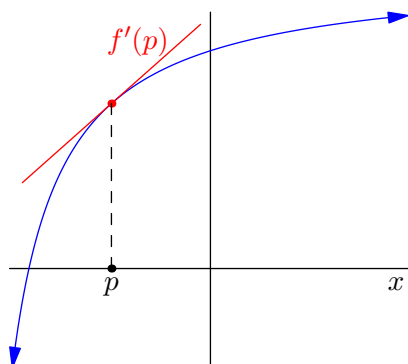
이 장에서는 도덕적으로 올바른 선형대수학을 사용하여 진행하므로, 선형 사상, 특히 앞으로 반복해서 사용할 쌍대 공간  $V^\vee$ 에 익숙해지는 것이 필수적입니다.

이 장에서 모든 벡터 공간은 노름을 가지며  $\mathbb{R}$  위에서 유한 차원입니다. 따라서 특히 모든 벡터 공간은 (노름으로 주어지는 거리를 갖는) 거리 공간이기도 하며, 우리는 평소처럼 열린집합에 대해 이야기할 수 있습니다.

## §43.1 전미분

**이 절의 대표적인 예:**  $f(x, y) = x^2 + y^2$ 이면,  $(Df)_{(x,y)} = 2xe_1^\vee + 2ye_2^\vee$ 입니다.

먼저  $f: [a, b] \rightarrow \mathbb{R}$ 라고 합시다. 고등학교 미적분학에서 모든 점  $p \in \mathbb{R}$ 에 대해, (만약 존재한다면) 점  $p$ 에서의 미분을  $f'(p)$ 로 정의했으며, 이를 "접선"의 기울기로 해석했던 것을 기억하실 것입니다.



그것도 좋지만, 저는 그 점에서 미분을 해석하는 "더 나은" 방법은 선형 사상으로, 즉 함수로 보는 것이라고 주장합니다. 만약  $f'(p) = 1.5$ 라면, 이 미분은 제가  $p$ 에서  $\epsilon$ 만큼 떨어진 곳으로 이동할 때  $f$ 가 대략  $1.5\epsilon$ 만큼 변할 것으로 예상해야 한다는 것을 말해줍니다. 다시 말해,

$p$ 에서  $f$ 의 미분은  $p$  근처에서  $f$ 를 선형 함수로 근사합니다.

더 일반적으로는 어떨까요?  $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ 와 같은 함수가 있다고 합시다. 예를 들어

$$f(x, y) = x^2 + y^2$$

구체성을 위해서든 뭐든 말입니다. 점  $p \in \mathbb{R}^2$ 에 대해,  $p$ 에서  $f$ 의 "미분"은 그 점  $p$ 에서  $f$ 를 근사하는 선형 사상을 나타내야 합니다. 즉, 저는 다음을 만족하는 선형 사상  $T: \mathbb{R}^2 \rightarrow \mathbb{R}$ 를 원합니다.

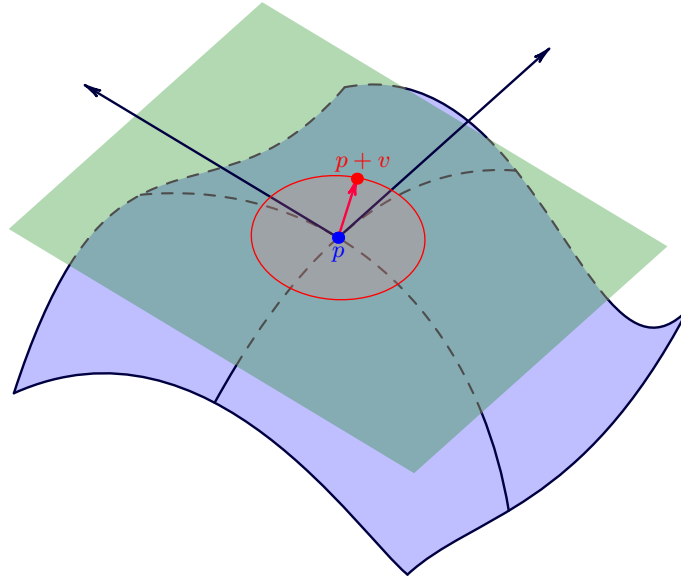
$$f(p + v) \approx f(p) + T(v)$$

작은 변위  $v \in \mathbb{R}^2$ 에 대해서 말입니다.

더욱 일반적으로,  $U \subseteq V$ 가 (평소처럼  $\|\bullet\|_V$  거리에서) 열려 있고  $f: U \rightarrow W$ 일 때,  $p \in U$ 에서의 미분은 다음을 만족해야 합니다.

$$f(p+v) \approx f(p) + T(v) \in W.$$

( $U$ 가 열린집합이어야 하는 이유는, 충분히 작은  $v$ 에 대해  $p+v \in U$ 도 성립하도록 하기 위함입니다.) 사실 이것은 고등학교에서  $f'(p)$ 를 다룰 때 우리가 하던 것과 정확히 같습니다.



이미지는 [gk]에서 파생됨

유일한 차이는, 불행한 우연으로 인해, 선형 사상  $\mathbb{R} \rightarrow \mathbb{R}$ 는 단지 그 기울기만으로 표현될 수 있다는 것입니다. 그리고 모든 것을 숫자로 만들어 AP 시험을 볼 수 있게 하려는 끝없는 추구 속에서, 우리는 애초에 무엇을 하려고 했는지 즉시 잊어버리고 그저  $f$ 의 미분을 함수가 아니라 숫자로 정의해 버렸습니다.

**미적분학의 근본적인 발상은 함수를 선형 함수로 국소적으로 근사하는 것입니다. 미분은 정확히 이것을 합니다.**

[Pu02]에 인용된 Jean Dieudonné는 다음과 같이 이어갑니다:

미적분학의 고전적인 교육에서, 이 발상은 1차원 벡터 공간에서 선형 형식과 숫자 사이에 일대일 대응이 존재한다는 우연한 사실로 인해 즉시 흐려지며, 그 결과 한 점에서의 미분은 선형 형식이 아니라 숫자로 정의됩니다. 어떤 대가를 치르더라도 수치적 해석이라는 표어에 대한 이 노예적 복종은 훨씬 더 심각해집니다...

그러니 이것을 제대로 해봅시다. 우리가 해야 할 유일한 일은 " $\approx$ "가 무엇을 의미하는지 말하는 것이며, 이를 위해 벡터 공간의 노름을 사용합니다.

**정의 43.1.1.**  $U \subseteq V$ 가 열려 있다고 합시다.  $f: U \rightarrow W$ 를 연속 함수라 하고,  $p \in U$ 라 합시다. 다음을 만족하는 선형 사상  $T: V \rightarrow W$ 가 존재한다고 가정합시다.

$$\lim_{\|v\|_V \rightarrow 0} \frac{\|f(p+v) - f(p) - T(v)\|_W}{\|v\|_V} = 0.$$

그러면  $T$ 는  $p$ 에서  $f$ 의 **전미분**입니다. 이를  $(Df)_p$ 로 표기하며,  $f$ 는  $p$ 에서 **미분 가능**하다고 말합니다.

$(Df)_p$ 가 모든 점에서 존재하면,  $f$ 는 **미분 가능**하다고 말합니다.

**질문 43.1.2.**  $V = W = \mathbb{R}$ 인 경우, 이것이 단변수 정의와 동치임을 확인해 보십시오. ( $V$ 에서  $W$ 로 가는 선형 사상은 무엇입니까?)

**예제 43.1.3** ( $f(x, y) = x^2 + y^2$ 의 전미분)

$V = \mathbb{R}^2$ 가 표준 기저  $\mathbf{e}_1, \mathbf{e}_2$ 를 가지고  $W = \mathbb{R}$ 이라 하고,  $f(x\mathbf{e}_1 + y\mathbf{e}_2) = x^2 + y^2$ 이라 합시다.  $p = a\mathbf{e}_1 + b\mathbf{e}_2$ 라 합시다. 그러면 다음을 주장합니다:

$$(Df)_p: \mathbb{R}^2 \rightarrow \mathbb{R} \quad \text{에 의해} \quad v \mapsto 2a \cdot \mathbf{e}_1^\vee(v) + 2b \cdot \mathbf{e}_2^\vee(v).$$

여기서  $\mathbf{e}_1^\vee$ 와  $\mathbf{e}_2^\vee$ 라는 표기가 성립하는 이유는, 정의상  $(Df)_p \in V^\vee$ 이기 때문입니다: 이들은  $V$ 에서  $\mathbb{R}$ 로 가는 함수입니다!

극한의 정의로 이를 직접 확인해 봅시다.  $v = xe_1 + ye_2$ 로 두고,  $V$  위의 노름은  $\|(x, y)\|_V = \sqrt{x^2 + y^2}$ 이고  $W$  위의 노름은 그저 절댓값  $\|c\|_W = |c|$ 임에 유의하십시오. 그러면 다음을 계산합니다

$$\begin{aligned} \frac{\|f(p+v) - f(p) - T(v)\|_W}{\|v\|_V} &= \frac{|(a+x)^2 + (b+y)^2 - (a^2 + b^2) - (2ax + 2by)|}{\sqrt{x^2 + y^2}} \\ &= \frac{x^2 + y^2}{\sqrt{x^2 + y^2}} = \sqrt{x^2 + y^2} \\ &\rightarrow 0 \end{aligned}$$

$\|v\| \rightarrow 0$ 일 때, 따라서  $p = a\mathbf{e}_1 + b\mathbf{e}_2$ 에 대해 실제로  $(Df)_p = 2a \cdot \mathbf{e}_1^\vee + 2b \cdot \mathbf{e}_2^\vee$ 입니다.

**비고 43.1.4** — 늘 그렇듯이, 미분가능성은 연속성을 함의합니다.

**비고 43.1.5** —  $U \subseteq V$ 이긴 하지만,  $U$ 와  $V$ 의 벡터를 서로 다른 종류의 대상으로 생각하는 것이 도움이 될 수 있습니다(특히  $0_V \notin U$ 일 수 있음에 유의하십시오).  $U$ 의 벡터는 우리 공간의 "입력"인 반면,  $V$ 에서 오는 벡터는 "작은 변위"입니다. 이러한 이유로, 저는 가능한 한  $p \in U$ 와  $v \in V$ 를 의도적으로 구분하여 사용하고자 합니다.

## §43.2 사영 원리

여러분은 일변수 미적분학을, 일변수 함수  $\mathbb{R} \rightarrow \mathbb{R}$ 에 대해 미분과 적분을 수행하는 주제로서 배웠을 것입니다. 그렇다면 "다변수 미적분학"은 함수  $\mathbb{R}^n \rightarrow \mathbb{R}^m$ 에 관한 미적분학이어야 합니다. 여기서 두 가지 확장이 일어나고 있음을 알아차렸을 수도 있습니다:

- 정의역이  $\mathbb{R}$ 에서  $\mathbb{R}^n$ 으로 확장되었습니다.
- 공역이  $\mathbb{R}$ 에서  $\mathbb{R}^m$ 으로 확장되었습니다.

이 절의 요점은, 첫 번째 확장에 비해 두 번째 확장은 매우 쉽고, 사실상 새로운 것을 전혀 필요로 하지 않는다는 것입니다. 흥미로운 일들은 모두 정의역을 확장했기 때문에 일어나는 것이지, 공역을 확장했기 때문이 아닙니다. 그 이유는 다음과 같습니다:

**정리 43.2.1 (사영 원리)**

$U$ 를 벡터 공간  $V$ 의 열린 부분집합이라 합시다.  $W$ 를 기저  $w_1, \dots, w_m$ 을 갖는  $m$ 차원 실벡터 공간이라 합시다. 그러면 연속함수  $f: U \rightarrow W$ 와,  $i$ 번째 기저 원소로의 사영에 의한 연속함수  $m$ -튜플  $f_1, f_2, \dots, f_m: U \rightarrow \mathbb{R}$  사이에는 전단사가 존재합니다. 즉

$$f(v) = f_1(v)w_1 + \dots + f_m(v)w_m.$$

증명. 자명합니다. □

”연속”을 ”미분가능”, ”매끄러움”, ”임의”, 또는 그 밖의 대부분의 합리적인 단어로 바꾸어도 이 정리는 여전히 성립합니다. 번역하면:

**함수  $f: U \rightarrow \mathbb{R}^m$ 을 생각하려면, 각 좌표를 따로따로 생각하는 것으로 충분합니다.**

이러한 이유로, 우리는 대부분 함수  $f: U \rightarrow \mathbb{R}$ 에 관심을 갖게 될 것입니다. 이것이 바로 쌍대 공간  $V^\vee$ 가 그토록 중요한 이유입니다.

**§43.3 전미분과 편미분**

**이 절의 대표적인 예:**  $f(x, y) = x^2 + y^2$ 이면,  $(Df): (x, y) \mapsto 2x \cdot \mathbf{e}_1^\vee + 2y \cdot \mathbf{e}_2^\vee$ 이고,  $\frac{\partial f}{\partial x} = 2x$ ,  $\frac{\partial f}{\partial y} = 2y$ 입니다.

$U \subseteq V$ 가 열린집합이고  $V$ 가 기저  $\mathbf{e}_1, \dots, \mathbf{e}_n$ 을 갖는다고 합시다.  $f: U \rightarrow \mathbb{R}$ 가 모든 점에서 미분가능한 함수, 즉 모든  $p$ 에 대해  $(Df)_p \in V^\vee$ 가 존재하는 함수라고 합시다. 이 경우,  $Df$ 를 그 자체로 하나의 함수로 볼 수 있습니다:

$$\begin{aligned} Df: U &\rightarrow V^\vee \\ p &\mapsto (Df)_p. \end{aligned}$$

이는 조금 이상해 보입니다:  $U$ 의 모든 점에  $V^\vee$ 의 함수를 대응시키는 것이기 때문입니다. 우리가 다루는 정보의 양을 반영하여,  $Df$ 를  $f$ 의 **전미분**이라고 부릅니다.  $(Df)_p$ 는  $p$ 에서의 전미분이라고 부릅니다.

이제 사영 원리를  $Df$ 에 적용해 봅시다.  $V$ 의 기저  $\mathbf{e}_1, \dots, \mathbf{e}_n$ 을 택했으므로, 이에 대응하는 쌍대 기저  $\mathbf{e}_1^\vee, \mathbf{e}_2^\vee, \dots, \mathbf{e}_n^\vee$ 가 존재합니다. 사영 원리에 따르면  $Df$ 는 단지  $n$ 개의 함수로 생각할 수 있으므로, 다음과 같이 쓸 수 있습니다

$$Df = \psi_1 \mathbf{e}_1^\vee + \dots + \psi_n \mathbf{e}_n^\vee.$$

사실, 우리는  $\psi_i$ 가 무엇인지도 구체적으로 서술할 수 있습니다.

**정의 43.3.1.**  $f: U \rightarrow \mathbb{R}$ 의  $i^{\text{th}}$  **편미분**은 다음과 같이 표기됩니다

$$\frac{\partial f}{\partial \mathbf{e}_i}: U \rightarrow \mathbb{R}$$

다음과 같이 정의됩니다

$$\frac{\partial f}{\partial \mathbf{e}_i}(p) := \lim_{t \rightarrow 0} \frac{f(p + t\mathbf{e}_i) - f(p)}{t}.$$

이것을 “ $\mathbf{e}_i$  방향의  $f$ ”이라고 생각할 수 있습니다.

**질문 43.3.2.**  $Df$ 가 존재하면

$$(Df)_p(\mathbf{e}_i) = \frac{\partial f}{\partial \mathbf{e}_i}(p).$$

임을 확인하십시오.

**비고 43.3.3** — 물론  $\mathbf{e}_i$ 뿐만 아니라 임의의  $v$ 에 대해서도  $\frac{\partial f}{\partial v}$ 의 정의를 적을 수 있습니다.

위의 논의로부터 다음을 유도할 수 있습니다

$$Df = \frac{\partial f}{\partial \mathbf{e}_1} \cdot \mathbf{e}_1^\vee + \cdots + \frac{\partial f}{\partial \mathbf{e}_n} \cdot \mathbf{e}_n^\vee.$$

따라서  $V$ 의 기저가 주어지면,  $Df$ 를 단지  $n$ 개의 편미분으로 생각할 수 있습니다.

**비고 43.3.4** — 각  $\frac{\partial f}{\partial \mathbf{e}_i}$ 가  $U$ 에서 실수로 가는 함수임을 기억하십시오. 즉,

$$(Df)_p = \underbrace{\frac{\partial f}{\partial \mathbf{e}_1}(p)}_{\in \mathbb{R}} \cdot \mathbf{e}_1^\vee + \cdots + \underbrace{\frac{\partial f}{\partial \mathbf{e}_n}(p)}_{\in \mathbb{R}} \cdot \mathbf{e}_n^\vee \in V^\vee.$$

**예제 43.3.5** ( $f(x, y) = x^2 + y^2$ 의 편미분)

$f: \mathbb{R}^2 \rightarrow \mathbb{R}$ 을  $(x, y) \mapsto x^2 + y^2$ 로 정의합시다. 그러면 우리의 새로운 언어로는,

$$Df: (x, y) \mapsto 2x \cdot \mathbf{e}_1^\vee + 2y \cdot \mathbf{e}_2^\vee.$$

따라서 편미분은 다음과 같습니다

$$\frac{\partial f}{\partial x}: (x, y) \mapsto 2x \in \mathbb{R} \quad \text{그리고} \quad \frac{\partial f}{\partial y}: (x, y) \mapsto 2y \in \mathbb{R}$$

이렇게 말했지만, 전미분 자체를 어떻게 구하는지에 대해서는 별로 이야기하지 않았습다. 예를 들어, 제가 여러분에게

$$f(x, y) = x \sin y + x^2 y^4$$

를 알려준다면, 앞서 언급한 그 끔찍한 극한 정의를 거치지 않고  $Df$ 를 계산하고 싶은 것입니다.

다행히도, 여러분은 이미 편미분을 계산하는 방법을 알고 있는데, 왜냐하면 인생의 어느 시점엔가 AP 미적분학을 수강해야 했기 때문입니다. 대부분의 적당한 함수에 대해서는 이것만으로 충분하다는 것이 밝혀집니다.

**정리 43.3.6** (연속인 편미분은 미분가능성을 함의합니다)

$U \subseteq V$ 를 열린집합이라 하고 임의의 기저  $\mathbf{e}_1, \dots, \mathbf{e}_n$ 을 택합시다.  $f: U \rightarrow \mathbb{R}$ 이라 하고 각  $i$ 에 대해  $\frac{\partial f}{\partial \mathbf{e}_i}$ 가 정의되며 나아가 연속이라고 가정합시다. 그러면  $f$ 는 미분가능하고  $Df$ 는 다음과 같이 주어집니다

$$Df = \sum_{i=1}^n \frac{\partial f}{\partial \mathbf{e}_i} \cdot \mathbf{e}_i^\vee.$$

증명. 세부 사항을 다 적지는 않겠지만...  $v = t_1 e_1 + \dots + t_n e_n$ 이 주어졌을 때, 아이디어는 그저  $p$ 에서  $p + t_1 e_1$ 로,  $p + t_1 e_1 + t_2 e_2$ 로, ...,  $p + t_1 e_1 + t_2 e_2 + \dots + t_n e_n = p + v$ 까지 걸어가면서 도중에 편미분들을 모으는 것입니다. 계산을 좀 해 보십시오.  $\square$

**비고 43.3.7** — 연속 조건은 생략할 수 없습니다. 다음 함수

$$f(x, y) = \begin{cases} \frac{xy}{x^2+y^2} & (x, y) \neq (0, 0) \\ 0 & (x, y) = (0, 0). \end{cases}$$

는 고전적인 반례입니다 – 두 편미분이 모두 존재함에도 불구하고, 영점에서 전미분  $Df$ 는 존재하지 않습니다.

**예제 43.3.8** (실제로 전미분 계산하기)

$f(x, y) = x \sin y + x^2 y^4$ 라 합시다. 그러면

$$\begin{aligned} \frac{\partial f}{\partial x}(x, y) &= \sin y + y^4 \cdot 2x \\ \frac{\partial f}{\partial y}(x, y) &= x \cos y + x^2 \cdot 4y^3. \end{aligned}$$

따라서 정리 43.3.6가 적용되어,  $Df = \frac{\partial f}{\partial x} \mathbf{e}_1^\vee + \frac{\partial f}{\partial y} \mathbf{e}_2^\vee$ 이며, 이는 굳이 다 적지 않습니다.

$f(x, y) = x^2 + y^2$ 의 예도 마찬가지입니다. 그렇다고는 해도, 도대체 누가  $x \sin y + x^2 y^4$  따위에 신경을 쓰겠습니까?

**§43.4 (선택) 고계 도함수에 관한 소고**

$U \subseteq V$ 를 열린집합이라 하고,  $f: U \rightarrow W$ 를 취하여  $Df: U \rightarrow \text{Hom}(V, W)$ 가 되도록 합시다.

사실,  $\text{Hom}(V, W)$  역시 그 자체로 하나의 노름 벡터 공간으로 생각할 수 있습니다: 다음과 같이 설정함으로써 그 위에 작용소 노름을 정의할 수 있다는 것이 밝혀집니다

$$\|T\| := \sup \left\{ \frac{\|T(v)\|_W}{\|v\|_V} \mid v \neq 0_V \right\}.$$

따라서  $\text{Hom}(V, W)$  역시 노름 벡터 공간으로 생각할 수 있습니다. 그러므로 다음과 같이 쓰는 것이 합리적입니다

$$D(Df): U \rightarrow \text{Hom}(V, \text{Hom}(V, W))$$

이를  $D^2f$ 로 축약합니다. 모든 의심을 버리고 계속 나아가면,

$$D^3f: U \rightarrow \text{Hom}(V, \text{Hom}(V, \text{Hom}(V, W))).$$

죄송합니다. 위안이 되는 점은, 적어도  $\text{Hom}(V, W) \cong V^\vee \otimes W$ 가 자연스러운 방식으로 성립한다는 것을 알고 있으므로, 이를 최소한 다음과 같이 압축할 수 있다는 것입니다

$$D^k f: V \rightarrow (V^\vee)^{\otimes k} \otimes W$$

여러 개의 Hom을 나열해 쓰는 대신 말입니다.

**비고 43.4.1** —  $k = 2$ 이고  $W = \mathbb{R}$ 이면,  $D^2f(v) \in (V^\vee)^{\otimes 2}$ 이므로, 이는  $n \times n$  행렬로 나타낼 수 있으며, 이는 어떤 이유에서인지 **헤세 행렬**이라고 불립니다.

이계도함수의 가장 중요한 성질은 다음과 같습니다

**정리 43.4.2** ( $D^2f$ 의 대칭성)

$U \subseteq V$ 가 열린집합이고  $f: U \rightarrow W$ 라 합시다. 어떤  $p \in U$ 에서  $(D^2f)_p$ 가 존재하면, 이는 대칭입니다. 즉

$$(D^2f)_p(v_1, v_2) = (D^2f)_p(v_2, v_1).$$

저는 이계도함수를 생각하면 머리가 어지러워지므로, 이를 증명 없이 그저 인용만 하겠습니다(예를 들어 [Pu02, §5, theorem 16] 참고). 이 정리의 중요한 따름정리는 다음과 같습니다:

**따름정리 43.4.3** (클레로 정리: 혼합 편미분의 대칭성)

$U \subseteq V$ 가 열린집합이고  $f: U \rightarrow \mathbb{R}$ 가 두 번 미분가능하다고 합시다. 그러면 해당 양들이 정의되는 임의의 점  $p$ 에 대해,

$$\frac{\partial}{\partial \mathbf{e}_i} \frac{\partial}{\partial \mathbf{e}_j} f(p) = \frac{\partial}{\partial \mathbf{e}_j} \frac{\partial}{\partial \mathbf{e}_i} f(p).$$

## §43.5 미분 형식을 향하여

이로써 도함수가 실제로 무엇인지에 대한 설명을 마칩니다. 이 장에서 전달하고자 하는 핵심 아이디어는  $Df$ 를  $U \rightarrow V^\vee$ 로 가는 사상으로 생각해야 한다는 것입니다.

다음으로 자연스럽게 할 일은 적분에 대해 이야기하는 것입니다. 이를 제대로 하는 방법은 이른바 미분 형식을 통하는 것입니다. 그러면 그 지긋지긋한  $dx$ 와  $dy$ 들이 실제로 무엇을 의미하는지 마침내 알게 될 것입니다. (장식으로 거기 있었던 게 아닙니다!)

## §43.6 생각해 볼 만한 조금 더 어려운 문제

**문제 43A\*** (연쇄 법칙).  $U_1 \xrightarrow{f} U_2 \xrightarrow{g} U_3$ 가 노름 벡터 공간  $V_i$ 의 열린집합들 사이의 미분 가능한 사상이고,  $h = g \circ f$ 라 하십시오. 연쇄 법칙을 증명하십시오: 임의의 점  $p \in U_1$ 에 대해 다음이 성립합니다

$$(Dh)_p = (Dg)_{f(p)} \circ (Df)_p.$$

**문제 43B.**  $U \subseteq V$ 가 열린집합이고,  $f: U \rightarrow \mathbb{R}$ 가  $k$ 번 미분 가능하다고 하십시오.  $(D^k f)_p$ 가 그  $k$ 개의 인자에 대해 대칭임을 보이십시오. 즉 임의의  $v_1, \dots, v_k \in V$ 와  $\{1, \dots, k\}$  위의 임의의 순열  $\sigma$ 에 대해 다음이 성립합니다

$$(D^k f)_p(v_1, \dots, v_k) = (D^k f)_p(v_{\sigma(1)}, \dots, v_{\sigma(k)}).$$

# 44 미분 형식

이 장에서는 모든 벡터 공간이 유한 차원 실수 내적 공간입니다. 먼저 (엄밀하지 않게) 이 장에서 정의할 모든 것을 그림으로 그려보는 것으로 시작합니다. 그런 다음 그것을 적절한 대수적 맥락에서 다시 처음부터 진행합니다.

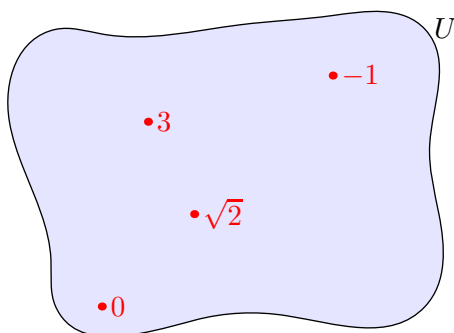
## §44.1 미분 형식의 그림

미분 형식을 정의하기 전에, 먼저 몇 가지 그림을 그려봅시다. 명심해야 할 핵심은 다음과 같습니다

“미분 형식의 정의는: 적분할 수 있는 어떤 것이다.”  
— 조 해리스(Joe Harris)

모든 함수가 **매끄럽다**고, 즉 무한히 미분 가능하다고 가정하겠습니다.

$U \subseteq V$ 를 벡터 공간  $V$ 의 열린집합이라 합시다. 함수  $f: U \rightarrow \mathbb{R}$ 가 있다고, 즉  $U$ 의 모든 점에 값을 하나씩 대응시킨다고 합시다.



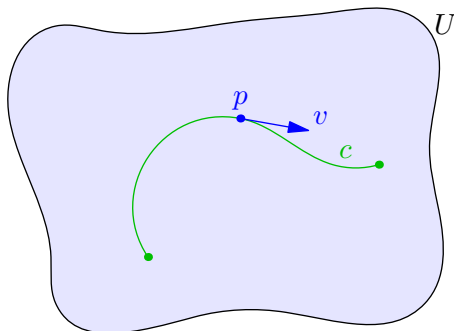
**정의 44.1.1.**  $U$  위의 **0-형식**  $f$ 는 그저 매끄러운 함수  $f: U \rightarrow \mathbb{R}$ 입니다.

따라서  $U$  안의 점들로 이루어진 유한 집합  $S$ 를 지정하면, 그 점들의 값을 단순히 더함으로써  $S$ 에 대해 “적분”할 수 있습니다:

$$0 + \sqrt{2} + 3 + (-1) = 2 + \sqrt{2}.$$

그러므로 0-형식  $f$ 는 0차원 “세포”에 대해 적분할 수 있게 해줍니다.

하지만 이는 상당히 지루한데, 우리가 알다시피 우리는 단일 점이 아니라 곡선 같은 것에 대해 적분하고 싶어하기 때문입니다. 그래서 유비적으로, 1차원 세포, 즉 곡선에 대해 적분할 수 있게 해주는 1-형식을 원합니다. 이를 위해서는 어떤 정보가 필요할까요? 이 질문에 답하기 위해, 함수  $c: [0, 1] \rightarrow U$ 로 생각할 수 있는 곡선  $c$ 의 그림을 그려봅시다.



$U$ 의 모든 점에 숫자 하나를 지정하는 것만으로(즉 0-형식  $f$ 만으로) 충분하고, 그런 다음 곡선을 따라  $f$ 의 모든 값을 어떻게든 “더하기만” 하면 될 것이라고 생각할 수도 있습니다. 잠시 후 이 발상을 사용하겠지만, 사실 우리는 더 일반적인 것을 할 수 있습니다. 매끄러운 곡선을 따라 걸을 때, 모든 점  $p$ 에서 우리에게 추가 정보, 즉 접벡터  $v$ 도 있다는 점에 주목하십시오. 그래서 우리는 1-형식  $\alpha$ 를 다음과 같이 정의할 수 있습니다. 0-형식은 그저 점 하나를 받아 실수 하나를 내놓았지만, 1-형식은 점 그리고 그 점에서의 접벡터를 함께 받아, 실수 하나를 내놓습니다. 그래서 1-형식  $\alpha$ 는 쌍  $(p, v)$ (여기서  $v$ 는  $p$ 에서의 접벡터입니다)에서  $\mathbb{R}$ 로 가는 매끄러운 함수입니다. 따라서

$$\alpha: U \times V \rightarrow \mathbb{R}.$$

사실, 임의의 점  $p$ 에 대해, 우리는  $\alpha(p, -)$ 가 벡터에 대해 선형 함수일 것을 요구할 것입니다: 즉 예를 들어  $\alpha(p, 2v) = 2\alpha(p, v)$ 이기를 원합니다. 그래서  $\alpha$ 를 다음과 같이 생각하는 것이 더 관계적입니다:

**정의 44.1.2.** 1-형식  $\alpha$ 는 매끄러운 함수

$$\alpha: U \rightarrow V^\vee.$$

$Df$ 의 경우처럼,  $\alpha(p)$  대신  $\alpha_p$ 를 사용하겠습니다. 그래서 모든 점  $p$ 에서,  $\alpha_p$ 는  $p$ 에서의 접벡터를 받아 실수 하나를 내놓는 어떤 선형 범함수입니다. 따라서 우리는  $\alpha_p$ 를  $V^\vee$ 의 원소로 생각합니다;

$$\alpha_p \in V^\vee.$$

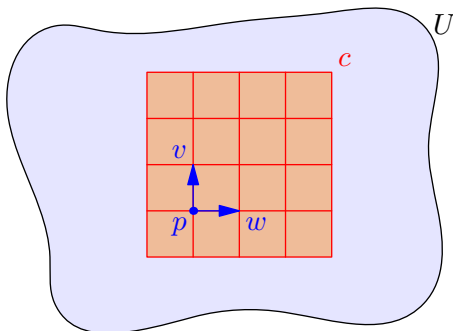
**비고 44.1.3 (경고: 호의 길이는 1-형식이 아닙니다)** — 고등학교 미적분학에서, “호 길이 요소”  $ds$ 를 곡선을 따라 적분할 수 있었다는 것을 기억할 것입니다:  $\int_c ds$ 는 곡선  $c$ 의 길이입니다.

이것은 1-형식이 아닙니다! 이에 관해서는 나중에 더 다루겠습니다. (간단히 말하자면: 근본적으로 문제는 그것이 선형 함수가 아니라는 것입니다. 어떤 곳에서는  $ds = \sqrt{dx^2 + dy^2}$ 라고 구어적으로 쓰인 것을 볼 수 있는데, 이는  $ds$ 가  $dx$ 와  $dy$ 에 대해 선형적인 것처럼 행동하지 않는다는 느낌을 줄 것입니다.)

다음으로, 2-형식의 그림을 그려봅시다. 이는 예를 들어 다음과 같은 형태의 덩어리(이른바 2-세포)에 대해 적분할 수 있게 해주어야 합니다

$$c: [0, 1] \times [0, 1] \rightarrow U$$

즉, 예를 들어  $U$  안의 정사각형입니다. 이전의 1-형식 예제에서는 곡선  $c$ 에 대한 접벡터를 살펴보았습니다. 이번에는 점들에서  $U$  안의 접벡터의 쌍을 살펴볼 것입니다: 많은 접벡터가 곡선 전체를 근사하는 것과 같은 의미로, 많은 작은 정사각형이  $U$  안의 큰 정사각형을 근사할 것입니다.



그렇다면 2-형식  $\beta$ 는 어떠해야 할까요? 이전과 마찬가지로, 점  $p \in U$ 를 받는 것으로 시작해야 하므로,  $\beta_p$ 는 이제 선형 범함수입니다: 하지만 이번에는 두 벡터  $v$ 와  $w$ 에 대한 선형 사상이어야 합니다. 여기서  $v$ 와  $w$ 는 접한다기보다는, 그것들의 생성 공간이 작은 평행사변형을 잘라낸다고 보아야 합니다. 그래서 옳은 방법은 사실 다음을 고려하는 것입니다

$$\beta_p \in V^\vee \wedge V^\vee.$$

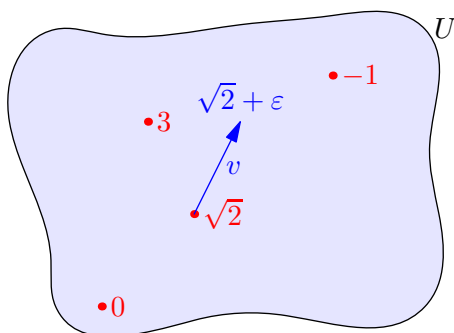
즉, 썬기곶을 사용하여  $v$ 와  $w$ 가 평행사변형을 생성한다는 발상을 다루는 것입니다. 또 다른 타당한 선택은  $(V \wedge V)^\vee$ 였을 것입니다; 실제로 이 둘은 동형이지만,<sup>1</sup> 전자로 쓰는 것이 더 편리할 것입니다.<sup>2</sup>

## §44.2 외미분의 그림

다음 질문:

0-형식으로부터 1-형식을 어떻게 만들 수 있을까요?

$f$ 를  $U$  위의 0-형식이라고 합시다. 즉, 함수  $f: U \rightarrow \mathbb{R}$ 가 주어집니다. 그러면 사실  $f$ 로부터 나오는 매우 자연스러운  $U$  위의 1-형식이 있으며, 이는 적절하게도  $df$ 라고 불립니다. 즉, 점  $p$ 와 접벡터  $v$ 가 주어졌을 때, 미분 형식  $(df)_p$ 는  $v$ 를 따른  $f$ 의 변화량을 반환합니다. 다시 말해, 이는 단지 전미분  $(Df)_p(v)$ 입니다.



따라서  $df$ 는 “ $f$ 의 변화량”을 측정합니다.

이제, 아직 적분을 정의하지 않았더라도, 점  $a$ 에서  $b$ 로 가는 곡선  $c$ 가 주어졌을 때, 다음이

$$\int_c df$$

무엇과 같아야 한다고 생각하십니까?  $df$ 는 “ $f$ 의 무한소 변화량”을 측정하는 1-형식임을 기억하십시오. 그러므로  $a$ 에서  $b$ 로 가는 경로를 따라  $f$ 의 모든 변화량을 더하면, 얻어지는 답은 단지

$$\int_c df = f(b) - f(a).$$

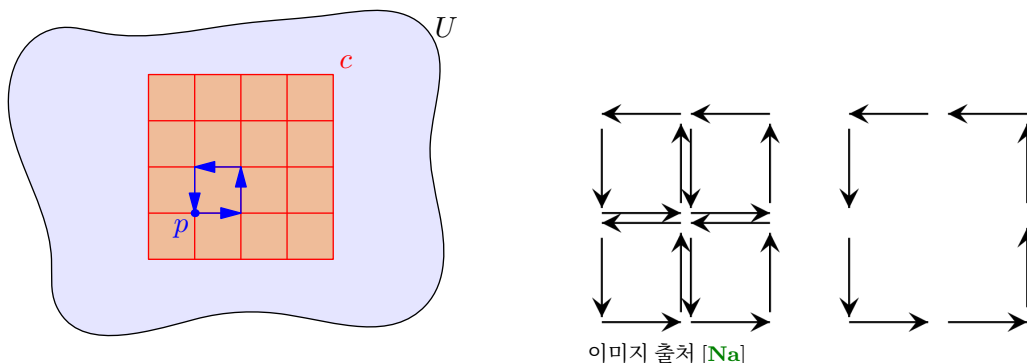
이것이 우리가 스톡스 정리라고 부르는 것의 첫 번째 경우입니다.

일반화하여, 1-형식에서 2-형식으로는 어떻게 가야 할까요? 각 점  $p$ 에서, 2-형식  $\beta$ 는 “평행사변형”을 입력받아 실수를 반환하는  $\beta_p$ 를 줍니다. 이제 1-형식  $\alpha$ 가 있다고 합시다. 그러면 평행사변형의 각 변을 따라, 적절한 부호 규약과 함께 1-형식  $\alpha$ 는 우리에게 실수를 줍니다. 그러므로 1-형식  $\alpha$ 가 주어졌을 때,  $d\alpha$ 를  $v$ 와  $w$ 가 펼치는 평행사변형을 입력받아 **경계를 따른  $\alpha$ 의 측도를 반환하는 2-형식으로 정의합니다.**

<sup>1</sup>우리는 유한 차원  $V$ 만을 고려합니다.

<sup>2</sup>절 44.5을 보십시오.

이제, 전체 정사각형  $c$ 를 따라  $d\alpha$ 를 적분하면 무슨 일이 일어날까요? 올바른 그림은, 각각의 작은 정사각형들이 모여 큰 정사각형을 이룬다고 생각하면, 인접한 경계들은 서로 상쇄되고, 남는 것은 주 경계뿐이라는 것입니다. 이것 역시 이른바 스톡스 정리의 한 경우일 뿐입니다.



### §44.3 미분 형식

**이 절의 대표적인 예:** 대수적으로는  $f\mathbf{e}_1^\vee \wedge \mathbf{e}_2^\vee + \dots$ 와 같은 형태이고, 기하학적으로는 이전 절을 참고하십시오.

이제  $dx$ 가 무엇을 의미하는지 파악해 봅시다. 차원이  $n$ 인 실벡터 공간  $V$ 를 고정하고,  $\mathbf{e}_1, \dots, \mathbf{e}_n$ 을 표준 기저라고 합시다.  $U$ 를 열린집합이라고 합시다.

**정의 44.3.1.**  $U$  위의 **미분  $k$ -형식**  $\alpha$ 를 매끄러운(무한히 미분 가능한) 사상  $\alpha: U \rightarrow \wedge^k(V^\vee)$ 로 정의합니다. (여기서  $\wedge^k(V^\vee)$ 는 켤레곱입니다.)

$Df$ 의 경우와 마찬가지로,  $\alpha(p)$  대신  $\alpha_p$ 를 사용하겠습니다.

**예제 44.3.2** ( $k = 0, 1$ 일 때의  $k$ -형식)

- (a) 0-형식은 그저 함수  $U \rightarrow \mathbb{R}$ 입니다.
- (b) 1-형식은 함수  $U \rightarrow V^\vee$ 입니다. 예를 들어, 함수  $V \rightarrow \mathbb{R}$ 의 전미분  $Df$ 는 1-형식입니다.
- (c)  $V = \mathbb{R}^3$ 이고 표준 기저를  $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ 이라고 합시다. 그러면 전형적인 2-형식은 다음으로 주어집니다

$$\alpha_p = f(p) \cdot \mathbf{e}_1^\vee \wedge \mathbf{e}_2^\vee + g(p) \cdot \mathbf{e}_1^\vee \wedge \mathbf{e}_3^\vee + h(p) \cdot \mathbf{e}_2^\vee \wedge \mathbf{e}_3^\vee \in \wedge^2(V^\vee)$$

여기서  $f, g, h: V \rightarrow \mathbb{R}$ 는 매끄러운 함수입니다.

이제, 사영 원리(정리 43.2.1)에 의해 우리는  $\wedge^k(V^\vee)$ 의  $\binom{n}{k}$ 개 기저 원소 각각에 대해서만 함수를 지정하면 됩니다. 그러므로  $V$ 의 임의의 기저  $\{\mathbf{e}_i\}$ 를 취하고,  $\wedge^k(V^\vee)$ 의 통상적인 기저인 다음 원소들을 취합니다

$$\mathbf{e}_{i_1}^\vee \wedge \mathbf{e}_{i_2}^\vee \wedge \dots \wedge \mathbf{e}_{i_k}^\vee.$$

따라서 일반적인  $k$ -형식은 다음과 같은 형태를 취합니다

$$\alpha_p = \sum_{1 \leq i_1 < \dots < i_k \leq n} f_{i_1, \dots, i_k}(p) \cdot \mathbf{e}_{i_1}^\vee \wedge \mathbf{e}_{i_2}^\vee \wedge \dots \wedge \mathbf{e}_{i_k}^\vee.$$

이것을 쓰는 것은 몹시 성가신 일이므로, 우리는 이를 다음과 같이 줄여 쓰겠습니다

$$\alpha = \sum_I f_I \cdot de_I$$

여기서 합은  $I = (i_1, \dots, i_k)$ 에 걸쳐 이루어지며,  $de_I$ 는  $e_{i_1}^\vee \wedge \dots \wedge e_{i_k}^\vee$ 를 나타내는 것으로 이해합니다.

이제  $\wedge^k(V^\vee)$ 의 원소를 얻었으니, 이것이 무엇을 할 수 있을까요? 자, 먼저 정의를 제시한 다음, 그것이 무엇을 하는지 말씀드리겠습니다.

**정의 44.3.3** (한 점에서 미분 형식을 계산하는 방법). 선형 함수  $\xi_1, \dots, \xi_k \in V^\vee$ 와 벡터  $v_1, \dots, v_k \in V$ 에 대해, 다음과 같이 설정합니다

$$(\xi_1 \wedge \dots \wedge \xi_k)(v_1, \dots, v_k) := \det \begin{bmatrix} \xi_1(v_1) & \dots & \xi_1(v_k) \\ \vdots & \ddots & \vdots \\ \xi_k(v_1) & \dots & \xi_k(v_k) \end{bmatrix}.$$

예를 들어  $v \wedge w = -w \wedge v$  등을 통해 이것이 잘 정의됨을 확인할 수 있습니다.

**예제 44.3.4** (미분 형식의 계산)

$V = \mathbb{R}^3$ 이라고 합시다. 어떤 점  $p$ 에서 2-형식  $\alpha$ 가 다음을 반환한다고 가정합니다

$$\alpha_p = 2e_1^\vee \wedge e_2^\vee + e_1^\vee \wedge e_3^\vee.$$

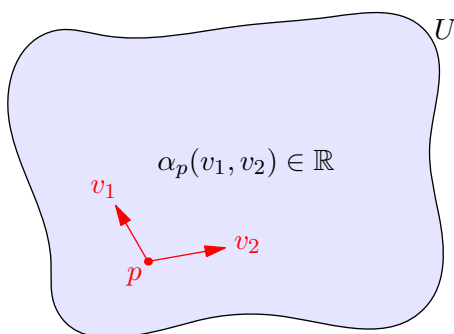
$v_1 = 3e_1 + e_2 + 4e_3$ 이고  $v_2 = 8e_1 + 9e_2 + 5e_3$ 이라고 합시다. 그러면

$$\alpha_p(v_1, v_2) = 2 \det \begin{bmatrix} 3 & 8 \\ 1 & 9 \end{bmatrix} + \det \begin{bmatrix} 3 & 8 \\ 4 & 5 \end{bmatrix} = 21.$$

이 정의는 무엇을 의미합니까? 이를 설명하는 한 가지 방법은 다음과 같습니다

제가 점  $p \in U$ 로 걸어가면,  $k$ -형식  $\alpha$ 는  $k$ 개의 벡터  $v_1, \dots, v_k$ 를 받아들여서 (부호가 있는) 부피로 해석될 수 있는 하나의 수를 내놓습니다.

그림:



다시 말해, 모든 점  $p$ 에서 함수  $\alpha_p$ 를 얻습니다. 그러면  $\alpha_p$ 에  $k$ 개의 벡터를 넣어서 하나의 수를 얻을 수 있는데, 이는  $\{v_i\}$ 들이 펼치는 평행육면체의 부호가 있는 부피로 (예를 들어 힘장의 플럭스와 같은 방식으로) 해석됩니다. 바로 이 때문에 "함수"로서의  $\alpha_p$ 가 썩기곱 안에 놓이도록 고안된 것입니다. 이는 "부피"라는 개념이 의미를 갖도록 보장하며, 그 결과 예를 들어 등식  $\alpha_p(v_1, v_2) = -\alpha_p(v_2, v_1)$ 가 성립합니다.

이것이 바로 미분 형식이 적분에 그토록 적합한 이유입니다.

## §44.4 외미분

**이 절의 대표적인 예:** 아마도  $(dx_1)_p = \mathbf{e}_1^\vee$  일 것입니다.

이제 이 장의 시작 부분에서 그림으로 보여드렸던 외미분<sup>3</sup>  $df$ 를 정의하겠습니다. 명시적인 좌표가 주어지면 외미분은 계산하기 쉬운 것으로 밝혀집니다.

먼저, 함수  $f: U \rightarrow \mathbb{R}$ 의 외미분을 다음과 같이 정의합니다

$$df := Df = \sum_i \frac{\partial f}{\partial \mathbf{e}_i} \mathbf{e}_i^\vee$$

특히,  $V = \mathbb{R}^n$ 이고  $f(x_1, \dots, x_n) = x_1$  (즉  $f = \mathbf{e}_1^\vee$ )이라고 합시다. 그러면

**질문 44.4.1.** 임의의  $p \in U$ 에 대해

$$(d(\mathbf{e}_1^\vee))_p = \mathbf{e}_1^\vee.$$

임을 보이십시오.

**표기의 남용 44.4.2.** 안타깝게도, 어딘가의 누군가는  $\mathbf{e}_1^\vee$ 를 나타내기 위해 “ $x_1$ ”을 사용하는 것이 좋은 생각이라고 결정했고(왜냐하면 당연히<sup>4</sup>  $x_1$ 은 “ $(x_1, \dots, x_n) \in \mathbb{R}^n$ 을  $x_1$ 으로 보내는 함수”를 의미하기 때문입니다) 그런 다음

$$dx_1 := d(\mathbf{e}_1^\vee).$$

라고 정하기로 결정했습니다. 이 표기법은 너무나 깊이 뿌리박혀 있어서 저로서는 마지못해 받아들이는 수밖에 없습니다. 엄밀히 말하면  $(dx_1)_p = \mathbf{e}_1^\vee$ 이므로 이것조차 옳지 않다는 점에 유의하십시오.  $dx_1$ 은 1-형식입니다.

**비고 44.4.3 —** 이것이 바로 오늘날 미적분학에서  $\frac{df}{dx}$ 라는 표기법을 사용하는 이유입니다: 예를 들어  $f(x) = x^2$ 로 정의되는  $f: \mathbb{R} \rightarrow \mathbb{R}$ 가 주어졌을 때, 다음이 실제로 성립합니다

$$df = 2x \cdot \mathbf{e}_1^\vee = 2x \cdot dx$$

그래서 (더 나아간) 표기법의 남용을 통해 우리는  $df/dx = 2x$ 라고 씁니다.

더 일반적으로, 우리의 기저  $\mathbf{e}_1, \dots, \mathbf{e}_n$ 을 이용하여 외미분을 다음과 같이 정의할 수 있습니다

**정의 44.4.4.**  $\alpha = \sum_I f_I d\mathbf{e}_I$ 라면, **외미분**을 다음과 같이 정의합니다

$$d\alpha := \sum_I df_I \wedge d\mathbf{e}_I = \sum_I \sum_j \frac{\partial f_I}{\partial \mathbf{e}_j} d\mathbf{e}_j \wedge d\mathbf{e}_I.$$

이는 기저의 선택에 의존하지 않는 것으로 밝혀집니다; 이 절의 끝부분에서 기저에 무관한 정의를 언급하겠습니다.

<sup>3</sup>“외미분”이라는 이름은 췌기곱  $\wedge$ 가 외적(exterior product)이라고도 불리는 데서 유래합니다.

<sup>4</sup>반어법입니다.

**예제 44.4.5 (외미분 몇 가지 계산하기)**

$V = \mathbb{R}^3$ 에 표준 기저  $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ 가 있다고 합시다.  $f(x, y, z) = x^4 + y^3 + 2xz$ 라고 합시다. 그러면 다음과 같이 계산합니다

$$df = Df = (4x^3 + 2z) dx + 3y^2 dy + 2x dz.$$

다음으로, 지시된 대로  $d(df)$ 를 계산할 수 있습니다. 이는

$$\begin{aligned} d^2 f &= (12x^2 dx + 2dz) \wedge dx + (6y dy) \wedge dy + 2(dx \wedge dz) \\ &= 12x^2(dx \wedge dx) + 2(dz \wedge dx) + 6y(dy \wedge dy) + 2(dx \wedge dz) \\ &= 2(dz \wedge dx) + 2(dx \wedge dz) \\ &= 0. \end{aligned}$$

놀랍게도,  $d^2 f$ 는 영사상입니다. 여기서 우리는  $dx, dy, dz$ 를 쓰면서 처음으로 **표기의 남용 44.4.2**를 이용했습니다.

그리고 실제로, 이는 일반적으로 항상 참입니다:

**정리 44.4.6 (외미분은 소멸합니다)**

$\alpha$ 를 임의의  $k$ -형식이라 합시다. 그러면  $d^2(\alpha) = 0$ 입니다. 더 간결하게는,

$$d^2 = 0.$$

증명은 **문제 44B**로 남겨둡니다.

**연습문제 44.4.7.**  $d^2 = 0$ 이라는 명제를 이 장 시작 부분에서 주어진 2-형식의 기하학적 그림과 비교해 보십시오. 왜 이것이 직관적으로 타당한지 생각해 보십시오.

다음은  $d$ 의 다른 몇 가지 성질입니다:

- 방금 보았듯이,  $d^2 = 0$ 입니다.
- $k$ -형식  $\alpha$ 와  $\ell$ -형식  $\beta$ 에 대해, 다음을 보일 수 있습니다

$$d(\alpha \wedge \beta) = d\alpha \wedge \beta + (-1)^k(\alpha \wedge d\beta).$$

- $f: U \rightarrow \mathbb{R}$ 가 매끄럽다면,  $df = Df$ 입니다.

사실, 위에서 정의된  $df$ 가 이러한 성질을 갖는 유일한 사상, 즉  $k$ -형식을  $(k+1)$ -형식으로 보내는 사상임을 보일 수 있습니다. 따라서  $df$ 를 정의하는 한 가지 방법은, 위의 나열된 성질들을 공리로 삼고  $d$ 를 이 함수 방정식의 유일한 해로 선언하는 것입니다. 어느 쪽이든, 이는  $d$ 에 대한 우리의 정의가 선택된 기저에 의존하지 않음을 말해줍니다.

$df$ 가 경계의 변화를 측정한다는 것을 상기하십시오. 그런 의미에서,  $d^2 = 0$ 은 "경계의 경계는 비어 있다"와 같은 것을 말하고 있습니다. 다음 장에서 스톡스 정리를 볼 때 이를 정확하게 다듬을 것입니다.

**§44.5 여담:  $\wedge^k(V^\vee)$  대  $(\wedge^k(V))^\vee$** 

앞서 우리는  $\wedge^k(V^\vee) \cong (\wedge^k(V))^\vee$ 가 표준적으로 성립한다고 언급했지만, 편의상 전자를 사용합니다.

전자의 표기법이 실제로 더 편리하지만(두 미분 형식의 켤레가 자연스럽습니다), **정의 44.3.3**이 왜 그런 방식으로 정의되었는지는 명확하지 않습니다.

만약 대신  $(\wedge^k(V))^\vee$ 를 사용했다면, 미분 형식을 계산하는 것은 자명합니다:  $f \in (\wedge^k(V))^\vee$ 와 벡터  $v_1, \dots, v_k \in V$ 에 대해, 다음과 같습니다

$$f(v_1, \dots, v_k) := f(v_1 \wedge \dots \wedge v_k).$$

이는  $f$ 가 자연스럽게  $\wedge^k(V)$ 의 원소를 받아 실수를 반환하기 때문입니다.

하지만 이제,  $f \in (\wedge^1(V))^\vee$ 와  $g \in (\wedge^1(V))$ 를 받아서  $f \wedge g \in (\wedge^2(V))^\vee$ 와 같은 것을 반환하는 방법이 명확하지 않습니다: 자연스러운 선택인  $(v \wedge w \mapsto f(v)g(w))$ 조차 잘 정의되지 않습니다!<sup>5</sup>

무엇을 해야 할지 알아내려면, 한 걸음 물러나 텐서곱을 고려해야 합니다. 벡터 공간  $V$ 에 대해,  $T^k(V) = \underbrace{V \otimes V \otimes \dots \otimes V}_{k\text{번}}$ 로 정의합니다.

다음과 같은 도식이 있습니다:

$$\begin{array}{ccc} T^k(V^\vee) & \xrightarrow{\phi} & (T^k(V))^\vee \\ \downarrow q & & \uparrow q^\vee \\ \wedge^k(V^\vee) & & (\wedge^k(V))^\vee \end{array}$$

무슨 일이 일어나고 있는 것일까요?

먼저, 다음과 같이 주어지는 자연스러운 사상  $T^k(V^\vee) \rightarrow (T^k(V))^\vee$ 이 있습니다

$$\phi(\xi_1 \otimes \dots \otimes \xi_k) = v_1 \otimes \dots \otimes v_k \mapsto \xi_1(v_1)\xi_2(v_2)\dots\xi_k(v_k)$$

그리고 이는 자명한 방식으로 선형성에 의해  $T^k(V^\vee)$  전체로 확장됩니다.

위의 켤레 상황과 달리, 이 사상은 실제로 잘 정의됩니다.

약간의 수작업을 거치면  $\phi$ 가 단사임을 확인할 수 있습니다.  $T^k(V^\vee)$ 와  $(T^k(V))^\vee$  모두 차원이  $(\dim V)^k$ 이므로,  $\phi$ 는 전단사입니다.

다음으로,  $\wedge^k(V)$ 는 그저 " $T^k(V)$ 에 더 많은 관계를 부여한 것"에 불과하므로, 자연스러운 몫 사상  $q: T^k(V) \twoheadrightarrow \wedge^k(V)$ 가 존재함에 주목하십시오. 따라서 텐서들은 동치류로 나뉩니다.

#### 예제 44.5.1

$V = \mathbb{R}^2$ 이면,  $T^2(V)$ 는  $\mathbf{e}_1 \otimes \mathbf{e}_1$ ,  $\mathbf{e}_1 \otimes \mathbf{e}_2$  또는  $-\mathbf{e}_2 \otimes \mathbf{e}_1$ 과 같은 원소들을 갖게 됩니다. 이 원소들을  $\wedge^2(V)$ 로 사상하면,  $\mathbf{e}_1 \wedge \mathbf{e}_1 = 0$ 이고  $\mathbf{e}_1 \wedge \mathbf{e}_2 = -\mathbf{e}_2 \wedge \mathbf{e}_1$ 을 얻습니다. 즉,  $\mathbf{e}_1 \otimes \mathbf{e}_2$ 와  $-\mathbf{e}_2 \otimes \mathbf{e}_1$ 은 같은 동치류에 속합니다.

사상  $q$ 는 쌍대 사상  $q^\vee: (\wedge^k(V))^\vee \rightarrow (T^k(V))^\vee$ 를 유도합니다.

**질문 44.5.2.** 함수  $f \in (T^k(V))^\vee$ 가  $\text{im } q^\vee$ 에 속하는 것은  $f$ 가 위에서 정의된 각 동치류 내의 모든 원소에 대해 동일한 값을 부여하는 경우, 그리고 오직 그 경우뿐임을 스스로 확인해 보십시오.

따라서, 동형사상  $q \circ \phi^{-1} \circ q^\vee: (\wedge^k(V))^\vee \rightarrow \wedge^k(V^\vee)$ 를 얻습니다.<sup>6</sup>

<sup>5</sup> $f = \mathbf{e}_1^\vee$ 와  $g = \mathbf{e}_2^\vee$ 로 시도해 보고, 이를 우리가 서로 같음을 아는  $\mathbf{e}_1 \wedge \mathbf{e}_2$ 와  $-\mathbf{e}_2 \wedge \mathbf{e}_1$ 에서 계산해 보십시오.

<sup>6</sup>여기서  $q$ 는 사상  $T^k(V) \rightarrow \wedge^k(V)$ 와  $T^k(V^\vee) \rightarrow \wedge^k(V^\vee)$  모두를 가리키는 데 표기를 남용하여 사용하고 있습니다.

이것이 실제로 동형사상임을 확인하기 위해, 그 역사상을 구성해 보겠습니다. 위에서 정의한 대로,  $T^k(V^\vee)$  안의 각 동치류(즉  $g \in \wedge^k(V^\vee)$ )의 올은 여러 원소를 가지지만, 다음과 같은 방법으로 그 정준적인 원소를 찾을 수 있습니다:

**정의 44.5.3.** 벡터 공간  $V$ 와 원소  $f = f_1 \otimes f_2 \otimes \cdots \otimes f_k \in T^k(V)$ 에 대해,  $f$ 의 교대화(alternation)를 다음과 같이 정의합니다:

$$\text{Alt } f = \frac{1}{k!} \sum_{\sigma \in S_k} \text{sgn}(\sigma) \cdot (f_{\sigma(1)} \otimes f_{\sigma(2)} \otimes \cdots \otimes f_{\sigma(k)})$$

그리고 이를  $T^k(V)$  전체로 확장합니다.

여기서  $S_k$ 는 순열군입니다. 행렬식의 정의와의 유사성에 주목하십시오.

#### 예제 44.5.4

위와 마찬가지로,  $V = \mathbb{R}^2$ 이라 합시다. 그러면 다음을 얻습니다:

$$\text{Alt}(\mathbf{e}_1 \otimes \mathbf{e}_2) = \frac{\mathbf{e}_1 \otimes \mathbf{e}_2 - \mathbf{e}_2 \otimes \mathbf{e}_1}{2}.$$

$\mathbf{e}_1 \otimes \mathbf{e}_2$ 의 첫 번째 성분과 두 번째 성분을 맞바꾸면, 원래 텐서와 별 관계가 없는  $\mathbf{e}_2 \otimes \mathbf{e}_1$ 을 얻는다는 점에 주목하십시오. 그러나  $\frac{\mathbf{e}_1 \otimes \mathbf{e}_2 - \mathbf{e}_2 \otimes \mathbf{e}_1}{2}$ 의 첫 번째 성분과 두 번째 성분을 맞바꾸면,  $\frac{\mathbf{e}_2 \otimes \mathbf{e}_1 - \mathbf{e}_1 \otimes \mathbf{e}_2}{2}$ 를 얻는데, 이는 정확히 원래 텐서의 부호를 반대로 한 것입니다!

$\text{Alt } f$ 가  $f$ 의 동치류를 대표하는 바람직한 원소인 이유는 다음과 같습니다:

- $\text{Alt}(\text{Alt } f) = \text{Alt } f$ ;
- $q$ 가 몫 사상  $T^k(V) \twoheadrightarrow \wedge^k(V)$ 일 때,  $q(f) = q(\text{Alt } f)$ 입니다;
- $\text{Alt } f$ 는 교대 텐서입니다 — 즉, 각 순수 텐서에 대해  $\text{Alt } f$ 의 인접한 두 성분을 맞바꾸면, 전체 텐서의 부호가 반대로 바뀝니다.

따라서 각 원소를  $T^k(V^\vee)$  안의 교대 텐서로 보내는 사상  $\iota: \wedge^k(V^\vee) \hookrightarrow T^k(V^\vee)$ 를 정의하는 것이 타당합니다.

#### 예제 44.5.5

위와 같은 예시로,  $V = \mathbb{R}^2$ 이라 하면 다음을 얻습니다

$$\iota(\mathbf{e}_1 \wedge \mathbf{e}_2) = \text{Alt}(\mathbf{e}_1 \otimes \mathbf{e}_2) = \frac{\mathbf{e}_1 \otimes \mathbf{e}_2 - \mathbf{e}_2 \otimes \mathbf{e}_1}{2}.$$

마지막으로,

**연습문제 44.5.6.**  $\text{im}(\phi \circ \iota) = \text{im } q^\vee$ 이며,  $\iota^\vee \circ \phi \circ \iota$ 와  $q \circ \phi^{-1} \circ q^\vee$ 가 서로의 역사상임을 보이십시오.

$\mathbf{e}_1^\vee \wedge \mathbf{e}_2^\vee$ 가  $\mathbf{e}_1 \wedge \mathbf{e}_2$ (즉,  $\mathbf{e}_1$ 과  $\mathbf{e}_2$ 로 이루어진 정사각형)를 입력으로 받아 1을 반환하도록 썬기곱을 정의하고자 하는 것이 흔한 표기법입니다. 그러나 위의 방법으로 썬기곱을 자연스럽게 정의하면, 다음을 얻습니다

$$\iota(\mathbf{e}_1^\vee \wedge \mathbf{e}_2^\vee) = \frac{\mathbf{e}_1^\vee \otimes \mathbf{e}_2^\vee - \mathbf{e}_2^\vee \otimes \mathbf{e}_1^\vee}{2}$$

이는 다음을 의미합니다

$$\phi(\iota(\mathbf{e}_1^\vee \wedge \mathbf{e}_2^\vee))(\mathbf{e}_1, \mathbf{e}_2) = \frac{1 \cdot 1 - 0 \cdot 0}{2} = \frac{1}{2}.$$

따라서, 보정 계수  $k!$ 가 필요합니다.

두 번째 표기법을 사용할 경우 썬기곱이 얼마나 “어려운지” 확인하기 위해,  $V = \mathbb{R}^3$ ,  $\alpha = dx \wedge dy \in \wedge^2(V^\vee)$ ,  $\beta = dz \in \wedge^1(V^\vee)$ 로 놓겠습니다.

그러면 다음이 성립함을 알 수 있습니다.

- $\alpha(\mathbf{e}_1 \wedge \mathbf{e}_2) = 1$ .
- $\beta(\mathbf{e}_3) = 1$ .
- $(\alpha \wedge \beta)(\mathbf{e}_1 \wedge \mathbf{e}_2 \wedge \mathbf{e}_3) = 1$ 이 성립해야 합니다.

썬기곱을 사상  $\wedge: \wedge^2(V^\vee) \times \wedge^1(V^\vee) \rightarrow \wedge^3(V^\vee)$ 로 정의한다면 마지막 부분은 자명합니다.

하지만  $\alpha$ 와  $\beta$ 가 각각  $(\wedge^2(V))^\vee$ 와  $(\wedge^1(V))^\vee$ 의 원소로 주어진다면(즉,  $v, w \in V$ 에 대해  $\alpha$ 를  $v \wedge w$ 에서만 계산할 수 있고,  $v \in V$ 에 대해  $\beta$ 를  $v$ 에서만 계산할 수 있다면),  $\alpha \wedge \beta$ 가 어떠한지 하는지 적어내는 것이 훨씬 더 어려워집니다. 실제로,

$$(\alpha \wedge \beta)(v_1 \wedge v_2 \wedge v_3) = \alpha(v_1 \wedge v_2)\beta(v_3) - \alpha(v_1 \wedge v_3)\beta(v_2) + \alpha(v_2 \wedge v_3)\beta(v_1).$$

이것이 교대화 연산자(또는 평가 연산)의 변형이며,  $\alpha \wedge \beta$ 가 교대적이 되도록 가중평균을 계산하는 것임을 알 수 있습니다.

## §44.6 결가지 언급: 호의 길이 $ds$ 는 1-형식이 아닙니다

앞서 언급했듯이, 호의 길이  $ds$ 는 1-형식이 아닙니다.<sup>7</sup>

앞서 미분 형식은 적분할 수 있는 대상이라고 말했습니다.  $ds$ 를 분명히 적분할 수 있지만, 이는 1-형식으로 간주되지 않습니다!

$ds$ 가 선형이 아님을 정의에 비추어 쉽게 확인할 수 있지만(문제 45E), 그럼에도 불구하고 왜 미분 형식을 정의할 때  $ds$ 를 제외하고 싶은지 의문이 생깁니다. 여기서 무슨 일이 벌어지고 있는 것일까요?

사실 진짜 이야기는, 매끄러운 곡선 위에서 적분 가능한 대상은 1-밀도라는 것입니다. 이는 나중에 정의하겠습니다.

간단히 하기 위해, 이 절에서는  $\mathbb{R}^2$  위에서 다루겠습니다. 매끄러운 곡선  $c$  위에서 적분할 수 있는 (매끄러운) 1-밀도  $\omega$ 가 주어졌을 때, 적분  $\int_c \omega$ 가 다음 성질들을 만족하기를 바랍니다.

- 이는 가법적입니다. 즉,  $c$ 가 두 곡선  $c_1$ 과  $c_2$ 의 이어붙임이라면,  $\int_c \omega = \int_{c_1} \omega + \int_{c_2} \omega$ 입니다.
- 모든 것이 매끄럽기 때문에,  $c$ 가 아주 작은 선분이라면  $c$ 를 같은 길이의 두 선분  $c_1$ 과  $c_2$ 로 나눌 경우 실제로  $\int_{c_1} \omega \approx \int_{c_2} \omega$ 가 될 것으로 기대할 수 있습니다.

따라서  $c$ 의 길이가 충분히 작을 때  $\int_c \omega$ 가 “근사적으로 선형”이도록 요구하는 것이 자연스럽습니다.

기호로 나타내면:  $\varepsilon > 0$ 에 대해,  $c_\varepsilon$ 를 곡선  $c$ 의 길이  $\varepsilon$ 인 시작 부분 선분이라 하면,

$$\lim_{\varepsilon \rightarrow 0^+} \frac{\int_{c_\varepsilon} \omega}{\varepsilon} = h$$

어떤 유한한 상수  $h$ 에 대해 성립합니다.

<sup>7</sup><https://mathoverflow.net/q/90455>에 이에 대한 논의가 있습니다.

물론 1-밀도  $\omega$ 를, 매끄러운 곡선  $c$ 를 받아 위의 두 조건을 만족하는 값  $\int_c \omega$ 를 반환하는 함수로 단순히 형식화할 수도 있지만, 이 정의는 어색합니다.

더 나은 방법은, 아주 작은 곡선  $c$ 에 대해  $\int_c \omega$ 를 알고 있다면 임의의 매끄러운 곡선  $c$ 를 작은 곡선들로 잘게 쪼개어  $\omega$ 를 적분할 수 있다는 사실을 관찰하는 것입니다. 하지만 이는 완전히 형식적이지는 않습니다 — 물론 곡선의 길이가 0으로 갈수록 적분  $\int_c \omega$  역시 0으로 가기 때문입니다 — 그래서 대신 위의 극한을 고려합니다.

$$\lim_{\varepsilon \rightarrow 0^+} \frac{\int_{c_\varepsilon} \omega}{\varepsilon}.$$

**질문 44.6.1.** 같은 점  $c(0) = c_2(0) = p$ 에서 시작하여 같은 방향  $c'(0) = c_2'(0) = v$ 로 나아가는 두 곡선  $c: [0, 1] \rightarrow \mathbb{R}^2$ 와  $c_2: [0, 1] \rightarrow \mathbb{R}^2$ 가 주어졌을 때,  $\int_c \omega$ 의 기본적인 매끄러움 조건에 의해 위 극한이 동일함이 보장된다는 것을 스스로 확인해 보십시오.

따라서,

1-밀도  $\omega$ 를, 점  $p$ 와 (점  $p$ 에서  $\mathbb{R}^2$ 의 접벡터로 이해되는) 시작 방향  $v \in \mathbb{R}^2$ 를 입력받아 그 극한을 반환하는 함수로 정의할 수 있습니다.

형식적으로:

**정의 44.6.2** (1-밀도). 1-밀도  $\omega$ 는  $\mathbb{R}^2 \times \mathbb{R}^2 \rightarrow \mathbb{R}$ 인 함수입니다.

$\omega_p(v) \in \mathbb{R}$ 로 씁니다.

방향만이 중요하므로,  $\lambda \geq 0$ 에 대해  $\omega$ 가  $\omega_p(\lambda v) = \lambda \omega_p(v)$ 를 만족하도록 하는 것이 타당합니다. 특히  $\omega_p(0) = 0$ 입니다.

그러면  $ds$ 는  $ds_p(v) = \|v\|$ 인 1-밀도입니다. 곡선 위에서 적분하는 방법을 아직 엄밀하게 정의하지는 않았지만(다음 장에서 다루겠습니다), 이것이 어떻게 작동하는지 직관적으로 알 수 있습니다.

이 정의에 따르면, 1-형식은 추가로 두 번째 인자에 대해 선형인 1-밀도일 뿐입니다 —  $\omega_p(v + w) = \omega_p(v) + \omega_p(w)$ .

그렇다면 미분 형식이 갖는 특별한 성질은 무엇입니까? 우선,  $\omega$ 가 미분 형식이면 다음이 성립합니다:

$c: [0, 1] \rightarrow \mathbb{R}^2$ 를 매끄러운 곡선이라 하면,  $c$ 에 균등 수렴하는 매끄러운 곡선들의 임의의 수열  $c_k$ 에 대해  $\int_{c_k} \omega$ 는  $\int_c \omega$ 로 수렴합니다.

$ds$ 에 대해서는 이것이 어떻게 성립하지 않을 수 있는지 쉽게 상상할 수 있습니다 — 수평 선과 수직선으로만 이루어진 조각별 매끄러운 곡선들의 수열은 원을 근사할 수 있지만, 이 들쭉날쭉한 곡선들의 호의 길이는 결코 원의 둘레로 수렴할 수 없습니다.<sup>8</sup>

## §44.7 닫힌 형식과 완전 형식

$\alpha$ 를  $k$ -형식이라 합시다.

**정의 44.7.1.**  $d\alpha = 0$ 이면  $\alpha$ 가 **닫혀 있다**고 말합니다.

**정의 44.7.2.** 어떤  $(k-1)$ -형식  $\beta$ 에 대해  $d\beta = \alpha$ 이면  $\alpha$ 가 **완전하다**고 말합니다.  $k=0$ 인 경우,  $\alpha$ 는  $\alpha=0$ 일 때만 완전합니다.

<sup>8</sup>사실 같은 논증을 사용하면, 반대로 후자의 성질을 만족하는 매끄러운 밀도는 실제로 선형이어야 함을 증명할 수도 있습니다!

**질문 44.7.3.** 완전 형식은 닫혀 있음을 보이십시오.

자연스러운 질문이 떠오릅니다: 닫혀 있지만 완전하지 않은 형식이 존재할까요? 놀랍게도 이 질문에 대한 답은 위상수학과 연결되어 있습니다. 여기 중요한 예시가 하나 있습니다.

**예제 44.7.4 (각 형식)**

$U = \mathbb{R}^2 \setminus \{0\}$ 라 하고,  $\theta(p)$ 를  $x$ 축과 원점에서  $p$ 로 향하는 직선이 이루는 각도라 하겠습니다.

다음과 같이 정의되는 1-형식  $\alpha: U \rightarrow (\mathbb{R}^2)^\vee$ 는

$$\alpha = \frac{-y \, dx + x \, dy}{x^2 + y^2}$$

**각 형식**이라 불리며,  $p \in U$ 가 주어졌을 때 접벡터를 따른 각도  $\theta(p)$ 의 변화를 측정합니다. 그러므로 직관적으로는 “ $\alpha = d\theta$ ”인 셈입니다. 실제로 각 형식이 닫혀 있음을 직접 확인할 수 있습니다.

그러나  $\alpha$ 는 완전하지 않습니다:  $\alpha$ 를 도함수로 갖는 전역 매끄러운 함수  $\theta: U \rightarrow \mathbb{R}$ 는 존재하지 않습니다. 이는 원점 주위로 실제로  $2\pi$  전체 회전을 수행할 수 있다는 사실, 즉  $\theta$ 가  $2\pi$ 를 법으로 해서만 의미를 갖는다는 사실을 반영합니다. 따라서 각도 형식  $\alpha$ 의 존재는 원점 주위를 “감는” 가능성을 반영합니다.

그러므로 핵심 아이디어는, 닫힌 형식이 완전하지 못하다는 사실이 공간 안의 “구멍”과 상당히 잘 대응된다는 것입니다: 이는 호모토피 군과 호몰로지 군이 포착하려는 것과 같은 정보입니다. 또 다른 비유를 들자면, 복소해석학에서 코시-구르사 정리는  $U$ 가 단순 연결일 때에만 성립합니다.  $U$  안의 “구멍”은 형식  $\alpha$ 의 존재를 통해 감지되고 있는 것입니다. 이른바 드 램 코호몰로지가 이 관계를 명시적으로 드러내 줄 것입니다.

## §44.8 생각해 볼 만한 조금 더 어려운 문제

**문제 44A.** 각 형식이

$$\alpha = \frac{-y \, dx + x \, dy}{x^2 + y^2}$$

닫혀 있음을 직접 보이십시오.

**문제 44B.**  $d^2 = 0$ 임을 서술하는 정리 44.4.6를 증명하십시오.

# 45 미분 형식 적분하기

이제 셀 위에서 미분 형식을 적분하는 방법을 보이고, 이러한 맥락에서 스토크스 정리를 서술합니다. 이 장에서는 모든 벡터 공간이 유한 차원이고 실수입니다.

## §45.1 동기: 선적분

함수  $g: [a, b] \rightarrow \mathbb{R}$ 가 주어졌을 때, 미적분학의 기본정리에 의해 다음을 알 수 있습니다.

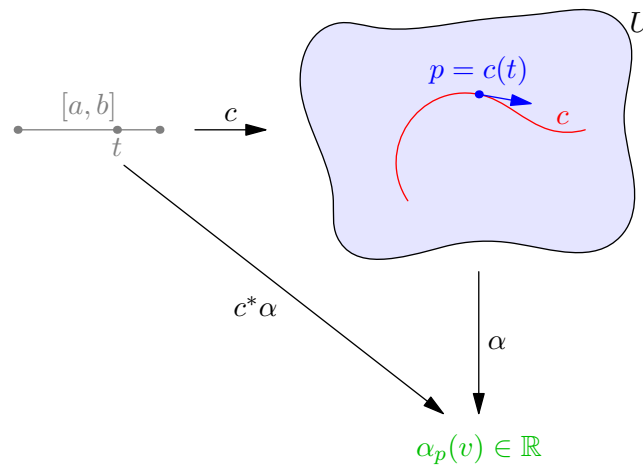
$$\int_{[a,b]} g(t) dt = f(b) - f(a)$$

여기서  $f$ 는  $g = df/dt$ 를 만족하는 함수입니다. 동등하게,  $f: [a, b] \rightarrow \mathbb{R}$ 에 대해서는

$$\int_{[a,b]} g dt = \int_{[a,b]} df = f(b) - f(a)$$

여기서  $df$ 는 앞서 정의한 외미분입니다.

좋습니다, 이제  $[a, b]$  위에서 적분을 할 수 있습니다. 이제 더 일반적으로, 실수 벡터 공간  $V$ 의 열린 부분집합  $U$ 와 1-형식  $\alpha: U \rightarrow V^\vee$ 가 있다고 합시다. **매개변수화된 곡선 (parametrized curve)**, 즉 매끄러운 함수  $c: [a, b] \rightarrow U$ 를 생각해봅시다. 그림:



다음을 만족하는  $\int_c \alpha$ 를 정의하고자 합니다.

**적분  $\int_c \alpha$ 는 곡선  $c$ 를 따라 모든  $\alpha$ 를 더한 것이어야 합니다.**

우리의 미분 형식  $\alpha$ 는 먼저 점  $p$ 를 받아  $\alpha_p \in V^\vee$ 를 얻습니다. 그다음, 곡선  $c$ 에 대한 접벡터  $v \in V$ 를 받아들여 마침내 실수  $\alpha_p(v) \in \mathbb{R}$ 를 내놓습니다. 우리는  $[a, b]$  위에서의 적분이라는 개념만을 사용하여 "이 모든 수들을 더하고" 싶습니다.

**연습문제 45.1.1.** 적분의 정의가 무엇이어야 할지 추측해보십시오. (형식 검사만으로도, 합리적인 답은 하나뿐입니다.)

따라서, 우리가 제시하는 정의는 다음과 같습니다.

$$\int_c \alpha := \int_{[a,b]} \alpha_{c(t)}(c'(t)) dt.$$

여기서  $c'(t)$ 는  $(Dc)_t(1)$ 의 약칭입니다. 이는 시각  $t$ 에서, 점  $p = c(t)$ 에서의 곡선  $c$ 의 접벡터를 나타냅니다. (여기서는  $[a, b]$ 가 1차원이라는 사실을 이용하고 있습니다.)

이제 그 정의는 쓰기가 번거로우므로,  $[a, b]$  위에 미분 1-형식  $c^*\alpha$ 를 정의하여 그 전체를 삼키도록 하겠습니다. 구체적으로, 이 경우 우리는  $c^*\alpha$ 를 다음과 같이 정의합니다.

$$(c^*\alpha)_t(\varepsilon) = \alpha_{c(t)} \cdot (Dc)_t(\varepsilon)$$

(여기서  $\varepsilon$ 는 시간상의 어떤 변위입니다.) 따라서, 더 간결하게 다음과 같이 쓸 수 있습니다.

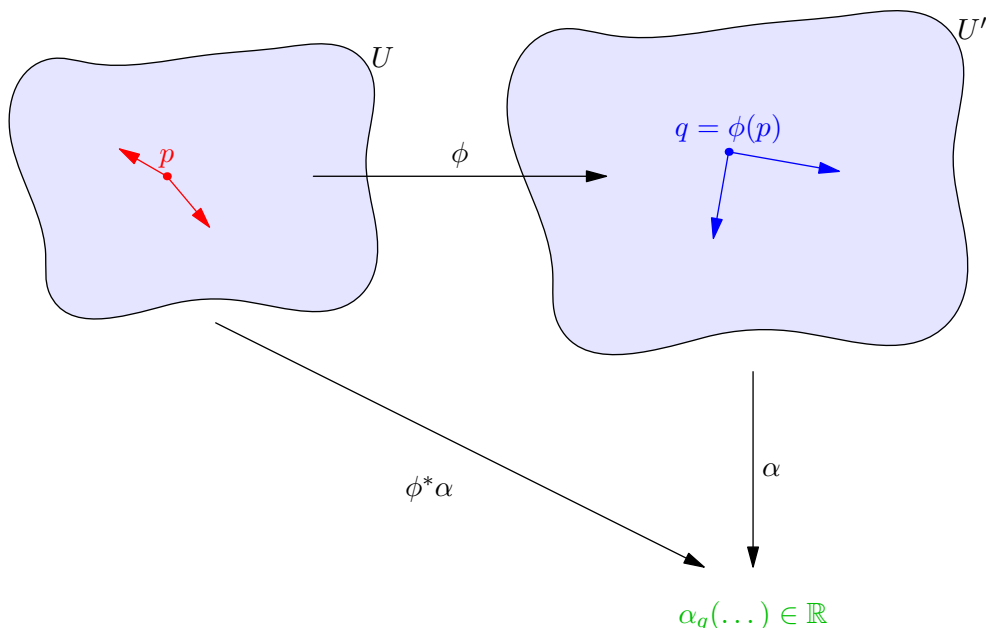
$$\int_c \alpha := \int_{[a,b]} c^*\alpha.$$

이는 당겨오기(*pullback*)의 특수한 경우입니다. 대략적으로,  $\phi: U \rightarrow U'$  ( $U \subseteq V, U' \subseteq V'$ ) 일 때,  $U'$  위의 임의의 미분  $k$ -형식  $\alpha$ 를  $U$  위의  $k$ -형식으로 바꿀 수 있습니다. 특히,  $U = [a, b]$  인 경우,<sup>1</sup> 우리는 기존의 적분 정의로 돌아갈 수 있습니다. 이제 이것을 완전히 일반적으로 해봅시다.

## §45.2 당겨오기

$V$ 와  $V'$ 를 유한 차원 실수 벡터 공간(차원이 다를 수도 있음)이라 하고,  $U$ 와  $U'$ 가 각각의 열린 부분집합이라 합시다. 다음으로,  $U'$  위의  $k$ -형식  $\alpha$ 를 생각해봅시다.

사상  $\phi: U \rightarrow U'$ 가 주어졌을 때, 이제 이전과 거의 같은 방식으로 당겨오기를 정의하고자 합니다. 그림:



음, 우리가 할 수 있는 일은 대략 한 가지뿐입니다. 구체적으로:  $\alpha$ 는  $U'$  안의 점 하나와  $V'$  안의 접벡터  $k$ 개를 받아, 실수를 반환합니다. 우리는  $\phi^*\alpha$ 가  $p \in U$  안의 점과  $V$  안의 접벡터  $v_1, \dots, v_k$   $k$ 개를 받아, 그에 대응하는 정보를  $\alpha$ 에 넘겨주기를 원합니다.

명백히 우리는 점  $q = \phi(p)$ 를 넘겨줍니다. 접벡터에 대해서는, 우리가 부피에 관심이 있으므로  $p$ 에서  $\phi$ 의 미분  $(D\phi)_p$ 를 취하는데, 이는 우리의 각 벡터  $v_i$ 를 목표 공간  $V'$  안의 어떤 벡터로 스케일링할 것입니다. 결론부터 말하면 다음과 같습니다.

<sup>1</sup>네,  $[a, b]$ 는 사실 열린집합이 아닙니다, 죄송합니다.  $(a - \varepsilon, b + \varepsilon)$  같은 것을 썼어야 합니다.

**정의 45.2.1.**  $\phi: U \rightarrow U'$ 와  $k$ -형식  $\alpha$ 가 주어졌을 때, **당겨오기(pullback)**를 다음과 같이 정의합니다.

$$(\phi^* \alpha)_p(v_1, \dots, v_k) := \alpha_{\phi(p)}((D\phi)_p(v_1), \dots, (D\phi)_p(v_k)).$$

기저를 사용하여 당겨오기를 정의하는 더 구체적인 방법이 있습니다.  $w_1, \dots, w_n$ 을  $V'$ 의 기저라 하고  $e_1, \dots, e_m$ 을  $V$ 의 기저라 합시다. 그러면 사영 원리(정리 43.2.1)에 의해 사상  $\phi: V \rightarrow V'$ 는 다음과 같이 생각할 수 있습니다.

$$\phi(v) = \phi_1(v)w_1 + \dots + \phi_n(v)w_n$$

여기서 각  $\phi_i$ 는  $v \in V$ 를 받아서 실수를 반환합니다. 또한  $\alpha$ 는 구체적으로 다음과 같이 쓸 수 있다는 것을 알고 있습니다.

$$\alpha = \sum_{I \subseteq \{1, \dots, n\}} f_I dw_I.$$

그러면, 다음과 같이 정의합니다.

$$\phi^* \alpha = \sum_{I \subseteq \{1, \dots, n\}} (f_I \circ \phi)(D\phi_{i_1} \wedge \dots \wedge D\phi_{i_k}).$$

성실한 독자라면 이 정의들이 동치임을 확인할 수 있습니다.

#### 예제 45.2.2 (당겨오기의 계산)

$V = \mathbb{R}^2$ 이 기저  $\mathbf{e}_1$ 과  $\mathbf{e}_2$ 를 가진다고 하고,  $\phi: V \rightarrow V'$ 가 다음과 같이 보낸다고 합시다.

$$\phi(a\mathbf{e}_1 + b\mathbf{e}_2) = (a^2 + b^2)w_1 + \log(a^2 + 1)w_2 + b^3w_3$$

여기서  $w_1, w_2, w_3$ 은  $V'$ 의 기저입니다.  $f: V' \rightarrow \mathbb{R}$ 일 때, 형식  $\alpha_q = f(q)w_1^\vee \wedge w_3^\vee$ 를 생각해 봅시다. 그러면

$$(\phi^* \alpha)_p = f(\phi(p)) \cdot (2a\mathbf{e}_1^\vee + 2b\mathbf{e}_2^\vee) \wedge (3b^2\mathbf{e}_2^\vee) = f(\phi(p)) \cdot 6ab^2 \cdot \mathbf{e}_1^\vee \wedge \mathbf{e}_2^\vee.$$

당겨오기는 기본적으로 가능한 한 좋은 성질을 가지는 것으로 밝혀졌는데, 예를 들면

- $\phi^*(c\alpha + \beta) = c\phi^*\alpha + \phi^*\beta$  (선형성)
- $\phi^*(\alpha \wedge \beta) = (\phi^*\alpha) \wedge (\phi^*\beta)$
- $\phi_1^*(\phi_2^*(\alpha)) = (\phi_2 \circ \phi_1)^*(\alpha)$  (자연성)

하지만 여기서는 이것들을 확인하는 데 시간을 들이지 않겠습니다 (기저로 전개하면 모두 검증할 수 있습니다).

## §45.3 세포

**이 절의 대표적인 예:**  $\mathbb{R}^2$ 의 원판은  $(r, \theta) \mapsto (r \cos \theta)\mathbf{e}_1 + (r \sin \theta)\mathbf{e}_2$ 에 의한 세포  $[0, R] \times [0, 2\pi] \rightarrow \mathbb{R}^2$ 로 생각할 수 있습니다.

이제 당겨오기의 개념을 갖게 되었으므로, 더 일반적인 공간에 대한 적분의 개념을 정의할 수 있습니다. 구체적으로, 앞서 다뤘던 적분의 개념을 일반화하기 위해서는 다음과 같이 합니다:

**정의 45.3.1.**  $k$ -세포란 매끄러운 함수  $c: [a_1, b_1] \times [a_2, b_2] \times \dots [a_k, b_k] \rightarrow V$ 를 말합니다.

**예제 45.3.2 (셀의 예시)**

편의를 위해  $V = \mathbb{R}^2$ 이라 합시다.

- (a) 0-셀은 하나의 점으로 이루어집니다.
- (b) 앞서 보았듯이, 1-셀은 임의의 곡선입니다.
- (c) 2-셀은 2차원 곡면에 대응합니다. 예를 들어, 사상  $c: [0, R] \times [0, 2\pi] \rightarrow V$ 를 다음과 같이 정의하면

$$c: (r, \theta) \mapsto (r \cos \theta, r \sin \theta)$$

반지름  $R$ 인 원판으로 생각할 수 있습니다.

이제 정의를 제시할 수 있습니다.

**정의 45.3.3** (미분  $k$ -형식을 적분하는 방법). 미분  $k$ -형식  $\alpha$ 와  $k$ -셀  $c: [0, 1]^k \rightarrow V$ 를 취합시다. 당겨오기를 이용하여 적분  $\int_c \alpha$ 를 다음과 같이 정의합니다.

$$\int_c \alpha := \int_{[0,1]^k} c^* \alpha.$$

$c^* \alpha$ 는  $k$ 차원 단위 상자 위의  $k$ -형식이므로,  $f(x_1, \dots, x_k) dx_1 \wedge \dots \wedge dx_k$ 로 쓸 수 있습니다. 따라서 위 적분은 다음과 같이도 쓸 수 있습니다.

$$\int_0^1 \dots \int_0^1 f(x_1, \dots, x_k) dx_1 \wedge \dots \wedge dx_k.$$

**예제 45.3.4 (원의 넓이)**

$V = \mathbb{R}^2$ 을 생각하고, 앞서와 같이  $[0, R] \times [0, 2\pi]$  위에서  $c: (r, \theta) \mapsto (r \cos \theta) \mathbf{e}_1 + (r \sin \theta) \mathbf{e}_2$ 라 합시다. 모든 점  $p$ 에서  $\alpha_p = \mathbf{e}_1^\vee \wedge \mathbf{e}_2^\vee$ 를 주는 2-형식  $\alpha$ 를 취합시다. 그러면

$$\begin{aligned} c^* \alpha &= (\cos \theta dr - r \sin \theta d\theta) \wedge (\sin \theta dr + r \cos \theta d\theta) \\ &= r(\cos^2 \theta + \sin^2 \theta)(dr \wedge d\theta) \\ &= r dr \wedge d\theta \end{aligned}$$

따라서,

$$\int_c \alpha = \int_0^R \int_0^{2\pi} r dr \wedge d\theta = \pi R^2$$

이것이 바로 원의 넓이입니다.

무슨 일이 일어나고 있는지에 대한 기하학적 직관을 소개하겠습니다.  $V$  안의  $k$ -cell이 주어졌을 때, 미분  $k$ -형식  $\alpha$ 는 점  $p$ 와 접벡터  $v_1, \dots, v_k$ 를 받아 숫자  $\alpha_p(v_1, \dots, v_k)$ 를 내놓는데, 이는 앞서와 마찬가지로 부호가 있는 초부피로 볼 수 있습니다. 그러면 적분은 이 모든 무한소들을 전체 cell에 걸쳐 합산합니다. 특히  $V = \mathbb{R}^k$ 이고 형식  $\alpha: p \mapsto \mathbf{e}_1^\vee \wedge \dots \wedge \mathbf{e}_k^\vee$ 를 취하면, 이  $\alpha$ 들이 주는 것은 그 cell의  $k$ 번째 초부피입니다. 이러한 이유로 이  $\alpha$ 는  $\mathbb{R}^k$  위의 **부피 형식**이라고 불립니다.

여기서 제가 "cell"이라는 용어를 다소 느슨하게 사용하기 시작했다는 것을 눈치채셨을 것입니다. cell  $c: [0, R] \times [0, 2\pi] \rightarrow \mathbb{R}^2$ 는 원래 함수여야 하지만, 저는 이를 (즉 그 상의 관점에서) 단위 원판으로 생각하라고 계속 말해왔습니다. 같은 맥락에서, 곡선  $[0, 1] \rightarrow V$ 는 시간에 대한 함수라기보다는 공간 속의 곡선으로 생각해야 합니다.

이 오류는 무해한 것으로 밝혀집니다.  $\alpha$ 를  $U$  위의  $k$ -형식이라 하고  $c: [a_1, b_1] \times \cdots \times [a_k, b_k] \rightarrow U$ 를  $k$ -cell이라 합시다.  $\phi: [a'_1, b'_1] \times \cdots \times [a'_k, b'_k] \rightarrow [a_1, b_1] \times \cdots \times [a_k, b_k]$ 라 합시다.  $\phi$ 가 전단사이고  $(D\phi)_p$ 가 항상 가역이면 (변수 변환이라고 생각하십시오) 이를 **재매개화**라고 합니다. 따라서

$$c \circ \phi: [a'_1, b'_1] \times \cdots \times [a'_k, b'_k] \rightarrow U$$

역시  $k$ -cell입니다. 그러면 모든  $p$ 에 대해  $\det(D\phi)_p > 0$ 이면 **방향을 보존한다**고 하고, 모든  $p$ 에 대해  $\det(D\phi)_p < 0$ 이면 **방향을 뒤집는다**고 합니다.

**연습문제 45.3.5.** 왜 이 두 경우 중 정확히 하나만 일어나야 할까요?

#### 정리 45.3.6 (변수 변환은 적분에 영향을 주지 않는다)

$c$ 를  $k$ -cell,  $\alpha$ 를  $k$ -형식,  $\phi$ 를 재매개화라 합시다. 그러면

$$\int_{c \circ \phi} \alpha = \begin{cases} \int_c \alpha & \phi \text{ 방향을 보존합니다} \\ - \int_c \alpha & \phi \text{ 방향을 뒤집습니다.} \end{cases}$$

증명. 당겨오기의 자연성을 이용하여 이를 일반 미적분학의 대응하는 정리로 환원하십시오.  $\square$

예를 들어, 단위원을  $[0, 1] \times [0, 1] \rightarrow \mathbb{R}^2$ 로  $(r, t) \mapsto R \cos(2\pi t)\mathbf{e}_1 + R \sin(2\pi t)\mathbf{e}_2$ 에 의해 매개화했다면, 우리는 같은 결과에 도달했을 것입니다. 그러므로 우리는 정말로  $k$ -cell을 그것이 지정하는 점들만으로 생각할 수 있습니다.

## §45.4 경계

**이 절의 대표적인 예:**  $[a, b]$ 의 경계는  $\{b\} - \{a\}$ 입니다. 정사각형의 경계는 그 가장자리를 반시계 방향으로 돕니다.

먼저, 여러 cell을 동시에 고려할 수 있게 해주는 전문 용어를 소개하겠습니다.

**정의 45.4.1.**  $k$ -사슬  $U$ 는  $U$  위의  $k$ -cell들의 형식적 선형결합, 즉 다음과 같은 형태의 합입니다.

$$c = a_1 c_1 + \cdots + a_m c_m$$

여기서 각  $a_i \in \mathbb{R}$ 이고  $c_i$ 는  $k$ -cell입니다. 우리는  $\int_c \alpha = \sum_i a_i \int_{c_i} \alpha$ 로 정의합니다.

특히, 0-사슬은 각각 주어진 가중치를 가진 여러 점들로 이루어집니다.

이제, 경계를 어떻게 정의할까요? 1-cell  $[a, b] \rightarrow U$ 에 대해, 앞서 암시했듯이 답이 0-사슬  $\{c(b)\} - \{c(a)\}$ 이기를 원합니다. 일반적인 경우에는 다음과 같이 합니다.

**정의 45.4.2.**  $c: [0, 1]^k \rightarrow U$ 가  $k$ -cell이라 합시다. 그러면  $\partial c: [0, 1]^{k-1} \rightarrow U$ 로 표기되는  $c$ 의 **경계**는 다음과 같이 정의되는  $(k-1)$ -사슬입니다. 각  $i = 1, \dots, k$ 에 대해 다음으로  $(k-1)$ -사슬들을 정의합니다.

$$\begin{aligned} c_i^{\text{시작}}: (t_1, \dots, t_{k-1}) &\mapsto c(t_1, \dots, t_{i-1}, 0, t_i, \dots, t_{k-1}) \\ c_i^{\text{정지}}: (t_1, \dots, t_{k-1}) &\mapsto c(t_1, \dots, t_{i-1}, 1, t_i, \dots, t_{k-1}). \end{aligned}$$

그러면

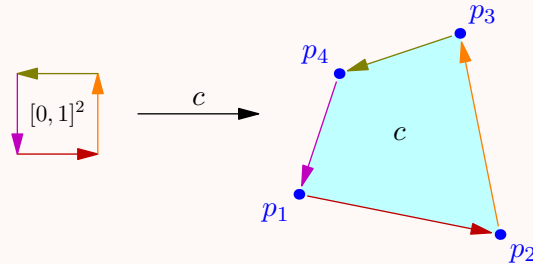
$$\partial c := \sum_{i=1}^k (-1)^{i+1} (c_i^{\text{정지}} - c_i^{\text{시작}}).$$

마지막으로, 사슬의 경계는 각 cell의 경계들의 합입니다(적절한 가중치와 함께). 즉,  $\partial(\sum a_i c_i) = \sum a_i \partial c_i$ 입니다.

**질문 45.4.3.** 이 정의가  $[0, 1]^k \rightarrow V$ 가 아니라  $c: [a_1, b_1] \times \cdots \times [a_k, b_k] \rightarrow V$ 로 정의된  $k$ -cell  $c$ 로 확장될 수 있음을 스스로 확인해 보십시오.

#### 예제 45.4.4 (경계의 예)

아래에 나타난 2-cell  $c: [0, 1]^2 \rightarrow \mathbb{R}^2$ 를 생각해 봅시다.



여기서  $p_1, p_2, p_3, p_4$ 는 각각  $(0, 0), (1, 0), (1, 1), (0, 1)$ 의 상입니다. 형식적으로  $\partial c$ 는 다음과 같이 주어집니다.

$$\partial c = (t \mapsto c(1, t)) - (t \mapsto c(0, t)) - (t \mapsto c(t, 1)) + (t \mapsto c(t, 0)).$$

인라인 함수로 인한 눈에 거슬리는 표기에 대해 사과드립니다. 이를 개선하여 그냥 다음과 같이 써봅시다.

$$\partial c = [p_2, p_3] - [p_1, p_4] - [p_4, p_3] + [p_1, p_2]$$

여기서 각 "구간"은 부호를 반영한 후 오른쪽에 붉은 화살표로 표시된 1-cell을 나타냅니다. 이것의 경계 또한 취할 수 있으며, 다음과 같이 빈 사슬을 얻습니다.

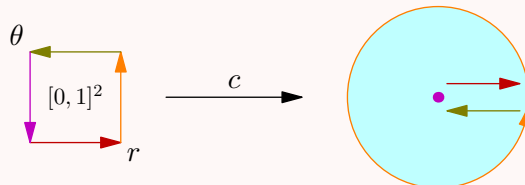
$$\partial(\partial c) = \sum_{i=1}^4 \{p_{i+1}\} - \{p_i\} = 0.$$

#### 예제 45.4.5 (단위 원판의 경계)

다음으로 주어진 단위 원판을 생각해 봅시다.

$$c: [0, 1] \times [0, 1] \rightarrow \mathbb{R}^2 \quad \text{에 의해} \quad (r, \theta) \mapsto r \cos(2\pi\theta)\mathbf{e}_1 + r \sin(2\pi\theta)\mathbf{e}_2.$$

경계의 네 부분은 아래 그림에 나타나 있습니다:



화살표 중 두 개는 적분될 때 서로 거의 상쇄된다는 점에 주목하십시오. 더욱이 흥미롭게도 원의 중심에 퇴화된 1-cell이 있습니다; 이는 항상 원점을 내놓는 상수 함수  $[0, 1] \rightarrow \mathbb{R}^2$ 입니다.

$d^2 = 0$ 과 유사한 필수 정리이며, 문제로 남겨둡니다.

**정리 45.4.6** (경계의 경계는 공집합입니다)

$\partial^2 = 0$ , 즉 임의의  $k$ -사슬  $c$ 에 대해  $\partial^2(c) = 0$ 이라는 의미입니다.

## §45.5 스토크스 정리

**이 절의 대표적인 예:**  $\int_{[a,b]} dg = g(b) - g(a)$ .

이제 cell에 대한 스토크스 정리를 서술하는 데 필요한 모든 재료가 준비되었습니다.

**정리 45.5.1** (cell에 대한 스토크스 정리)

평소와 같이  $U \subseteq V$ 를 취하고,  $c: [0, 1]^k \rightarrow U$ 를  $k$ -cell이라 하고,  $\alpha: U \rightarrow \bigwedge^{k-1}(V^\vee)$ 를  $(k-1)$ -형식이라 합시다. 그러면

$$\int_c d\alpha = \int_{\partial c} \alpha.$$

특히,  $d\alpha = 0$ 이면 좌변은 사라집니다.

예를 들어,  $c$ 가 구간  $[a, b]$ 이면  $\partial c = \{b\} - \{a\}$ 이며, 이로부터 미적분학의 기본정리를 얻습니다.

## §45.6 다시 현실로: 벡터 미적분학에서 배운 내용과의 비교

지금까지 모든 것을 추상적으로 다루었으니, 이제 일반적인 대학교에서 벡터 미적분학 강의를 듣는다면  $\mathbb{R}^3$ 에서 보게 될 내용과 우리가 배운 것을 비교해 봅시다.

**그림 45.1**에서는 제가 2024년 가을 MIT의 18.02 강의를 위해 그렸던 그림을 옮겨왔습니다. 이 강의는 많은 1학년 학생들이 수강하는 다변수 미적분학 강의입니다.  $0 \leq d \leq n \leq 3$ 인 각 경우(단,  $d = n = 0$ 은 제외)에 대해, 정의역이  $\mathbb{R}^n$ 인 함수의  $d$ 차원 적분을 수행할 때 그 강의에서 어떤 종류의 적분이 등장했는지를 보여줍니다. 이 그림의 모든 적분은 실숫값을 갖는다는 점에 유의하십시오.

저는 의도적으로 MIT에서 실제로 사용되었던 표기법을 사용했으며, 이를 18.02 표기법이라고 부르겠습니다. 이는 위키백과 및 다른 여러 곳에서 보게 될 표기법과 유사하기 때문입니다. 이 절의 목표는 18.02 표기법에서 낯선 표기법으로의 변환 체계를 제공하는 것입니다. (이 절 전체에서  $\mathbb{R}^n$ 은 노름 벡터 공간으로 취급되므로,  $\mathbf{e}_1 \mapsto \mathbf{e}_1^\vee$  등의 식별은 표준적입니다.)

**그림 45.1**에는 많은 내용이 담겨 있으므로, 하나씩 나누어 살펴보겠습니다.

**0-형식.** 0-형식은 그저 함수와 같으므로, 0차원 적분 열은 이해하기 쉬운 것입니다: 이는 단지 한 점에서의 값, 또는 여러 점에서의 값의 합일 뿐입니다.

**$n$ -형식.** The case  $n = d$  is also easy:  $\mathbb{R}^n$ 에서  $n$ -형식을 적분하여 하나의 수를 얻는 것이 가능함을 우리는 알고 있습니다. 즉:

- 통상적인 적분  $\int_a^b dx$ 는 1-cell  $[a, b]$ 에서 1-형식  $f \cdot \mathbf{e}_1^\vee$ 를 적분한 것입니다.
- 면적분  $\int_{a_1}^{b_1} \int_{a_2}^{b_2} f(x, y) dx dy$ 는 2-형식  $f \cdot \mathbf{e}_1^\vee \wedge \mathbf{e}_2^\vee$ 를 적분하는 것에 해당합니다.

## 18.02 도표.

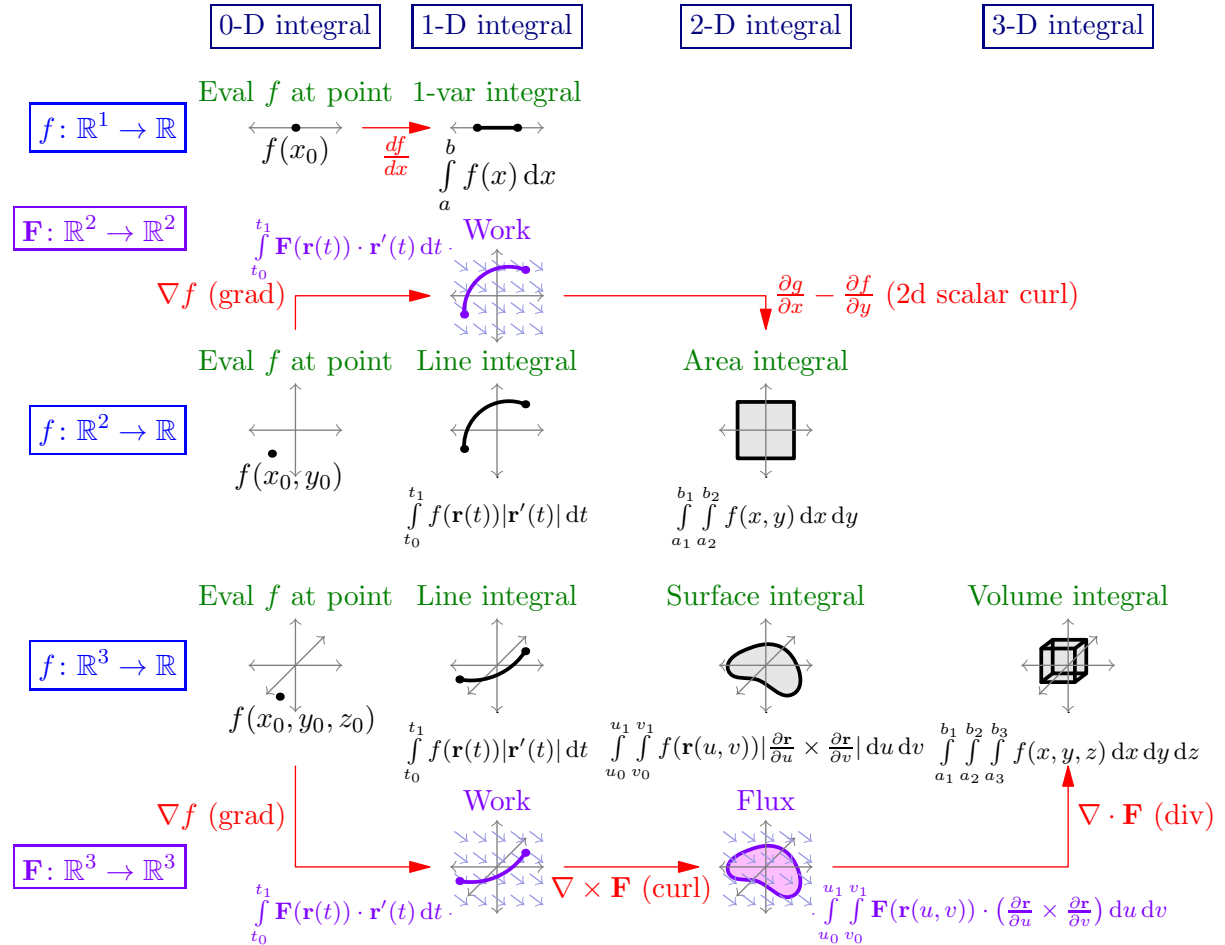


그림 45.1: 대학 1학년으로의 회귀인가요? 고해상도 버전은 <https://web.evanchen.cc/textbooks/poster-stokes.pdf>에서 확인할 수 있습니다.

- 부피적분  $\int_{a_1}^{b_1} \int_{a_2}^{b_2} \int_{a_3}^{b_3} f(x, y, z) dx dy dz$ 는 3-형식  $f \cdot \mathbf{e}_1^\vee \wedge \mathbf{e}_2^\vee \wedge \mathbf{e}_3^\vee$ 를 적분하는 것에 해당합니다.

이로써 대각선 위에 있는 초록색으로 표시된 것들을 처리했습니다.

**나머지 세 개의 초록색 그림은 해석할 수 없습니다!** 까다로운 부분은  $0 < d < n < 3$ 인 상황들입니다. 이런 것이 세 가지 있는데,  $d = 1$ 이고  $n \in \{2, 3\}$ 일 때의 두 선적분과  $d = 2$ 이고  $n = 3$ 일 때의 면적분입니다.

사실 이것들은 우리의 미분 형식 이론으로 다뤄지지 않습니다! 실제로  $f = 1$ 이 상수 함수인 특수한 경우조차, 선적분은 사실상 호의 길이이며, [절 44.6](#)에서 언급했듯이 그 적분은 어떤 미분 형식의 적분으로도 볼 수 없습니다. 마찬가지로 표면적도 미분 형식이 아닙니다.

**1-형식과 2-형식입니다.** 하지만 (벡터장에 대한) 세 개의 자주색 적분은 우리의 틀 안에서 볼 수 있습니다.

- $d = 1$ 이고  $n = 3$ 인 경우, 즉 3차원 선적분을 생각해 봅시다. 입력으로 벡터값 함수  $\mathbf{F}: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ 이 주어집니다. 사영 원리([정리 43.2.1](#))에 의해, 이는 다음 데이터와 동일합니다

$$\mathbf{F}(p) = F_1(p)\mathbf{e}_1 + F_2(p)\mathbf{e}_2 + F_3(p)\mathbf{e}_3$$

$i = 1, 2, 3$ 에 대한 세 함수  $F_i: \mathbb{R}^3 \rightarrow \mathbb{R}$ 에 대해서입니다.

18.02 표기법  $\mathbf{F}(p)$ 를 뱉킨 표기법으로 변환하기 위해,  $\mathbf{F}$ 를 다음 미분 형식과 동일시합니다

$$\alpha_p = F_1(p)\mathbf{e}_1^\vee + F_2(p)\mathbf{e}_2^\vee + F_3(p)\mathbf{e}_3^\vee.$$

한편, 시간  $t \in [t_0, t_1]$ 으로 매개변수화된 경로  $\mathbf{r}(t)$ 는 1-형식  $c: [t_0, t_1] \rightarrow \mathbb{R}^3$ 의 개념과 일치합니다. 적분에서의 "일"은 다음과 같이 씁니다

$$\mathbf{F}(\mathbf{r}(t)) \cdot \mathbf{r}'(t)$$

하지만 그 내적은 정확히 당겨오기  $c^*\alpha$ 입니다.

- $d = 1$ 이고  $n = 2$ 인 경우는 3을 2로 바꾼 것과 정확히 동일합니다.
- 가장 이상한 경우는  $d = 2$ 이고  $n = 3$ 인 유량 적분입니다. 매개변수화  $\mathbf{r}(u, v)$ 는 문제없으며, 이는 2-세포  $c$ 에 대응합니다. 하지만  $\mathbf{F}(p)$ 는 타입이 맞지 않는 것처럼 보입니다. 하지만 다시 다음과 같이 써 봅시다

$$\mathbf{F}(p) = F_1(p)\mathbf{e}_1 + F_2(p)\mathbf{e}_2 + F_3(p)\mathbf{e}_3.$$

이를 뱉킨 표기법으로 변환하는 데는 상당히 이상한 편법이 사용되는데, 원하는 형식은 다음과 같습니다

$$\alpha_p = F_1(p)\mathbf{e}_2^\vee \wedge \mathbf{e}_3^\vee + F_2(p)\mathbf{e}_3^\vee \wedge \mathbf{e}_1^\vee + F_3(p)\mathbf{e}_1^\vee \wedge \mathbf{e}_2^\vee.$$

네, 그것이 정말로 그 동일시입니다! 이 정의가 가능하려면 다음 사실을 이용해야 했습니다

$$\begin{pmatrix} 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 2 \end{pmatrix}.$$

즉 삼차원 공간  $\wedge^2(\mathbb{R}^3)$ 이 마침  $\wedge^1(\mathbb{R}^3) \cong \mathbb{R}^3$ 과 같은 개수의 기저 원소를 가지므로, 다음 사상은

$$\begin{aligned} \star: \wedge^2(\mathbb{R}^3) &\rightarrow \mathbb{R}^3 \\ \mathbf{e}_1 \wedge \mathbf{e}_2 &\mapsto \mathbf{e}_3 \\ \mathbf{e}_2 \wedge \mathbf{e}_3 &\mapsto \mathbf{e}_1 \\ \mathbf{e}_3 \wedge \mathbf{e}_1 &\mapsto \mathbf{e}_2 \end{aligned}$$

실제로 동형사상인데, 이는 기저 원소를 기저 원소로 대응시키기 때문입니다. 이 사상을  $\star$ 로 표기하는데, 이는 이 사상이 고차원에서 이른바 호지 스타 연산자로 일반화되기 때문입니다.

지금까지 의도적으로 피해 왔던 외적에 대해 이야기할 차례입니다. 외적은  $\mathbb{R}^3$ 의 두 벡터를 입력받아  $\mathbb{R}^3$ 의 벡터를 출력하는 이상한 연산입니다. 구체적으로,  $\mathbf{v} = x\mathbf{e}_1 + y\mathbf{e}_2 + z\mathbf{e}_3$ 이고  $\mathbf{w} = x'\mathbf{e}_1 + y'\mathbf{e}_2 + z'\mathbf{e}_3$ 일 때, 학교에서 배우는 외적의 정의는 다음과 같습니다

$$\mathbf{v} \times \mathbf{w} := (yz' - y'z)\mathbf{e}_1 + (zx' - xz')\mathbf{e}_2 + (xy' - x'y)\mathbf{e}_3.$$

이것은 어디서 나온 것일까요? 답은  $\star(\mathbf{v} \wedge \mathbf{w})$ 가 다음과 같기 때문입니다

$$\begin{aligned} \mathbf{v} \wedge \mathbf{w} &= (x\mathbf{e}_1 + y\mathbf{e}_2 + z\mathbf{e}_3) \wedge (x'\mathbf{e}_1 + y'\mathbf{e}_2 + z'\mathbf{e}_3) \\ &= (xy' - x'y)\mathbf{e}_1 \wedge \mathbf{e}_2 + (yz' - y'z)\mathbf{e}_2 \wedge \mathbf{e}_3 + (zx' - xz')\mathbf{e}_3 \wedge \mathbf{e}_1 \\ \star(\mathbf{v} \wedge \mathbf{w}) &\mapsto (xy' - x'y)\mathbf{e}_3 + (yz' - y'z)\mathbf{e}_1 + (zx' - xz')\mathbf{e}_2. \end{aligned}$$

이를 정리하고 나면, 이상한 내적-외적

$$\mathbf{F}(\mathbf{r}(u, v)) \cdot (\mathbf{r}_u \times \mathbf{r}_v) du dv$$

은 이제 당겨오기  $c^*\alpha$ 에 대응하도록 조작되어 있습니다. 그래서 이 호지 스타를 사용하면, 유량이 실제로는 2-형식의 적분임을 알 수 있습니다.

**외미분** 그림 45.1의 모든 빨간 화살표는 해당 형식의 외미분에 대응합니다. 즉:

- "grad" 연산은 0-형식  $f$ 를 입력받아 1-형식  $df$ 에 대응하는 벡터장을 출력합니다.
- "curl" 연산은 1-형식  $\alpha$ 를 입력받아 2-형식  $d\alpha$ 에 대응하는 벡터장을 출력합니다.  $n = 3$ 일 때 이는 잘 맞아떨어지는데, 1-형식의 공간이  $\binom{3}{1}$ 차원이고 2-형식의 공간이  $\binom{3}{2}$ 차원이며, 다행히도  $\binom{3}{1} = 3 = \binom{3}{2}$ 이기 때문입니다.

이상해 보이는 표기  $\nabla \times \mathbf{F}$ 는 외미분에 대응함을 확인할 수 있습니다. 18.02 쪽에서는 다음과 같은 것이 있다면

$$\mathbf{F} = F_1 \mathbf{e}_1 + F_2 \mathbf{e}_2 + F_3 \mathbf{e}_3$$

curl에 대한 18.02의 정의는 다음과 같습니다

$$\text{curl}(\mathbf{F}) := \nabla \times \mathbf{F} := \left( \frac{\partial F_3}{\partial y} - \frac{\partial F_2}{\partial z} \right) \mathbf{e}_1 + \left( \frac{\partial F_1}{\partial z} - \frac{\partial F_3}{\partial x} \right) \mathbf{e}_2 + \left( \frac{\partial F_2}{\partial x} - \frac{\partial F_1}{\partial y} \right) \mathbf{e}_3$$

$\nabla \times$ 라는 말도 안 되는 표기의 이유는, 정말로 표기를 남용한다면 이것을 벡터  $\nabla = \left\langle \frac{\partial}{\partial x}, \frac{\partial}{\partial y}, \frac{\partial}{\partial z} \right\rangle$ 와 벡터  $\mathbf{F} = \langle F_1, F_2, F_3 \rangle$ 의 외적으로 거의 생각할 수 있다는 데 있습니다.

이제  $\mathbf{F}$ 를 뺀 표기법으로 변환하기 위해, 우리가  $\mathbf{F}$ 를 다음 미분 형식과 동일시했다는 것을 기억하십시오

$$\alpha = F_1 \mathbf{e}_1^\vee + F_2 \mathbf{e}_2^\vee + F_3 \mathbf{e}_3^\vee.$$

**정의 44.4.4**에서의 외미분 공식을 따르면 다음을 얻습니다

$$\begin{aligned} d\alpha &= dF_1 \wedge \mathbf{e}_1^\vee + dF_2 \wedge \mathbf{e}_2^\vee + dF_3 \wedge \mathbf{e}_3^\vee \\ &= \left( \frac{\partial F_1}{\partial x} \mathbf{e}_1^\vee + \frac{\partial F_1}{\partial y} \mathbf{e}_2^\vee + \frac{\partial F_1}{\partial z} \mathbf{e}_3^\vee \right) \wedge \mathbf{e}_1^\vee \\ &\quad + \left( \frac{\partial F_2}{\partial x} \mathbf{e}_1^\vee + \frac{\partial F_2}{\partial y} \mathbf{e}_2^\vee + \frac{\partial F_2}{\partial z} \mathbf{e}_3^\vee \right) \wedge \mathbf{e}_2^\vee \\ &\quad + \left( \frac{\partial F_3}{\partial x} \mathbf{e}_1^\vee + \frac{\partial F_3}{\partial y} \mathbf{e}_2^\vee + \frac{\partial F_3}{\partial z} \mathbf{e}_3^\vee \right) \wedge \mathbf{e}_3^\vee \\ &= \left( \frac{\partial F_3}{\partial y} - \frac{\partial F_2}{\partial z} \right) \mathbf{e}_2^\vee \wedge \mathbf{e}_3^\vee + \left( \frac{\partial F_1}{\partial z} - \frac{\partial F_3}{\partial x} \right) \mathbf{e}_3^\vee \wedge \mathbf{e}_1^\vee + \left( \frac{\partial F_2}{\partial x} - \frac{\partial F_1}{\partial y} \right) \mathbf{e}_1^\vee \wedge \mathbf{e}_2^\vee. \end{aligned}$$

호지 스타를 취한 후 모든  $\vee$ 를 없애면  $\nabla \times \mathbf{F}$ 와 같은 것을 얻으며, 이로써 18.02 표기법과 뺀 표기법 사이의 대응이 완성됩니다.

- 18.02 용어로, 발산  $\text{div}$ 는 다음과 같이 정의됩니다

$$\text{div}(\mathbf{F}) := \nabla \cdot \mathbf{F} := \frac{\partial F_1}{\partial x} + \frac{\partial F_2}{\partial y} + \frac{\partial F_3}{\partial z}$$

이는 입력점  $p \in \mathbb{R}^3$ 에 대한 스칼라 값 함수입니다. 이 문제는 **문제 45C**에서 직접 풀어보도록 남겨두겠습니다.

$\nabla$ 라는 말도 안 되는 표기의 이유는, 정말로 표기를 남용한다면 이것을 벡터  $\nabla = \left\langle \frac{\partial}{\partial x}, \frac{\partial}{\partial y}, \frac{\partial}{\partial z} \right\rangle$ 와 벡터  $\mathbf{F} = \langle F_1, F_2, F_3 \rangle$ 의 내적으로 거의 생각할 수 있다는 데 있습니다.

**이중 미분** 우리는  $d^2 = 0$ 임을 알고 있으며, 이는 **그림 45.1**에서 두 화살표를 합성하면 영이 됨을 의미합니다. 18.02에서는 이것을 다음과 같이 보게 됩니다

- 기울기의 curl은 영입니다.
- curl의 플럭스는 영입니다.

하지만 실제로는 이 둘이 같은 정리입니다.

**스토크스 정리** 각 붉은 화살표 역시 셀에 대한 스토크스 정리의 한 사례를 제공합니다. 따라서 셀에 대한 스토크스 정리조차도 정말 훌륭한데, 여섯 개의 18.02 정리를 특수한 경우로 얻게 되기 때문입니다!

- 0차원 적분에서 1차원 적분으로 가는 세 개의 화살표는 모두 "미적분학의 기본 정리"라고 불립니다. 몇몇 저자들은  $n > 1$ 인 경우에는 대신 "선적분에 대한 미적분학의 기본 정리"라고 말할 것입니다.
- $n = 2$ 일 때, 다른 붉은 화살표는 "그린 정리"라고 불리며, 이를 **문제 45A<sup>†</sup>**에서 직접 풀어보도록 남겨두겠습니다.
- $n = 3$ 일 때, work에서 flux로 가는 화살표는 헛갈리게도 마찬가지로 "스토크스 정리"라고 불리며, 이는 2차원 곡면의 플럭스가 1차원 경계 위의 work와 같다는 것을 말합니다.
- $n = 3$ 에 대한 가장 오른쪽의 붉은 화살표는 "발산 정리"라고 불리며, 이는 3차원 부피의 발산이 2차원 경계 곡면의 플럭스와 같다는 것을 말합니다.

## §45.7 생각해 볼 만한 조금 더 어려운 문제

**문제 45A<sup>†</sup>** (그린 정리).  $f, g: \mathbb{R}^2 \rightarrow \mathbb{R}$ 를 매끄러운 함수라 하고  $c$ 를 2-셀이라 합시다. 다음을 증명하십시오

$$\int_c \left( \frac{\partial g}{\partial x} - \frac{\partial f}{\partial y} \right) dx \wedge dy = \int_{\partial c} (f dx + g dy).$$

**문제 45B.**  $\partial^2 = 0$ 임을 보이십시오.

**문제 45C.** 18.02 표기법과 뱀킨 표기법의 대응을 완성하십시오. 즉,  $\mathbf{F}: \mathbb{R}^3 \rightarrow \mathbb{R}^3$ 를 벡터장이라 하고,  $\alpha$ 를 뱀킨 버전에서 이에 대응하는 2-형식이라 합시다. 다음과 같이 정의되는 스칼라값 함수가

$$\operatorname{div}(\mathbf{F}) := \nabla \cdot \mathbf{F} := \frac{\partial F_1}{\partial x} + \frac{\partial F_2}{\partial y} + \frac{\partial F_3}{\partial z}$$

3-형식  $d\alpha$ 에서의 평갯값과 일치함을 보이십시오.

**문제 45D** (당겨오기와  $d$ 는 가환합니다).  $U$ 와  $U'$ 를 벡터 공간  $V$ 와  $V'$ 의 열린집합이라 하고,  $\phi: U \rightarrow U'$ 를 이들 사이의 매끄러운 사상이라 합시다.  $U'$  위의 임의의 미분 형식  $\alpha$ 에 대해 다음이 성립함을 증명하십시오.

$$\phi^*(d\alpha) = d(\phi^*\alpha).$$

**문제 45E** (호의 길이는 형식이 아닙니다).  $\mathbb{R}^2$  위에 1-형식  $\alpha$ 가 존재하여, 곡선  $c: [0, 1] \rightarrow \mathbb{R}^2$ 에 대해 적분  $\int_c \alpha$ 가  $c$ 의 호의 길이를 주는 그러한  $\alpha$ 가 존재하지 않음을 보이십시오.

**문제 45F. 완전**  $k$ -형식  $\alpha$ 란 어떤  $\beta$ 에 대해  $\alpha = d\beta$ 를 만족하는 것입니다. 다음을 증명하십시오.

$$\int_{C_1} \alpha = \int_{C_2} \alpha$$

여기서  $C_1$ 과  $C_2$ 는 평면 위의 임의의 동심원이고  $\alpha$ 는 어떤 완전 1-형식입니다.



# 46 다양체에 대한 약간의 이야기

지난 장에서 우리는 세포(cell)에 대한 스토크스 정리를 서술했습니다. 이것이 성립하는 훨씬 더 큰 부류의 공간, 이른바 매끄러운 다양체가 존재한다는 것이 밝혀집니다.

불행히도 매끄러운 다양체의 정의는 완전히 엉망이므로, 미분 형식과 방향을 정의하고 나면 그 위의 적분이 실제로 무엇인지 정의하기에는 너무 게을러질 것이고, 그저 대충 넘어가며 스토크스 정리를 서술할 것입니다.

## §46.1 위상 다양체

**이 절의 대표적인 예:**  $S^2$ : “지구는 평평해 보입니다”.

오래전 사람들은 지구가 평평하다고, 즉 평면과 위상동형이라고 생각했으며, 특히  $\pi_2(\text{지구}) = 0$ 이라고 생각했습니다. 하지만 실제로는 우리 대부분이 알듯이 지구는 사실 구이며, 이는 수축 가능하지 않고 특히  $\pi_2(\text{지구}) \cong \mathbb{Z}$ 입니다. 이 관찰이 다양체의 정의의 바탕이 됩니다:

**$n$ -다양체란 국소적으로  $\mathbb{R}^n$ 처럼 보이는 공간입니다.**

사실 위상 다양체  $M$ 을 생각하는 방법에는 두 가지가 있습니다:

- “국소적으로”: 모든 점  $p \in M$ 에서,  $p$ 의 어떤 열린 근방은  $\mathbb{R}^n$ 의 열린집합처럼 보입니다. 예를 들어, 지구 표면에 서 있는 사람에게 지구는  $\mathbb{R}^2$ 와 매우 비슷하게 보입니다.
- “전역적으로”: 열린집합  $\{U_i\}_i$  (무한히 많을 수도 있음)로 이루어진  $M$ 의 열린 덮개가 존재하여, 각  $U_i$ 가  $\mathbb{R}^n$ 의 어떤 열린 부분집합과 위상동형이 되도록 할 수 있습니다. 예를 들어 우주에서 보면 지구는 두 개의 반구형 팬케이크로 덮을 수 있습니다.

**질문 46.1.1.** 이 둘이 동치임을 확인하십시오.

첫 번째 것이 예시에 대한 가장 좋은 동기를 제공하는 반면, 두 번째 것은 형식적으로 사용하기가 더 쉽습니다.

**정의 46.1.2. 위상  $n$ -다양체**  $M$ 이란  $\mathbb{R}^n$ 의 부분집합과 위상동형인 집합들로 이루어진 열린 덮개  $\{U_i\}$ 를 갖는 하우스도르프 공간이며, 그 위상동형사상을 다음과 같이 나타냅니다

$$\phi_i: U_i \xrightarrow{\cong} E_i \subseteq \mathbb{R}^n$$

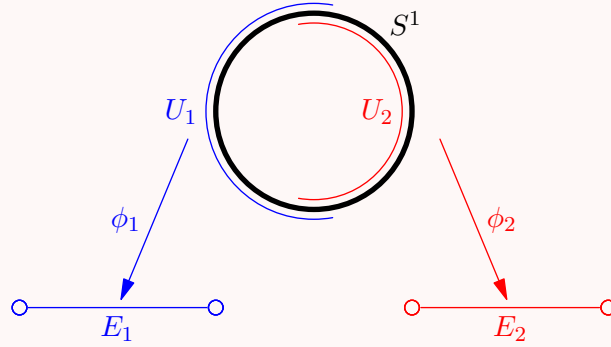
여기서 각  $E_i$ 는  $\mathbb{R}^n$ 의 열린 부분집합입니다. 각  $\phi_i: U_i \rightarrow E_i$ 는 **좌표계**(chart)라고 불리며, 이들이 함께 이른바 **좌표 모음집**(atlas)을 이룹니다.

**비고 46.1.3** — 여기서 “ $E$ ”는 “유클리드적(Euclidean)”을 의미합니다. 이 표기법은 표준적이지 않다고 생각하며, 보통 사람들은 그냥  $\phi_i(U_i)$ 라고 씁니다.

**비고 46.1.4** — 이 정의가 좋은 이유는 매장(embedding)에 의존하지 않기 때문입니다: 다양체는 어떤  $N$ 에 대한  $\mathbb{R}^N$ 의 부분집합이 아니라 내재적인 공간  $M$ 입니다. 비유하자면: 추상적인 군  $G$ 는  $S_n$ 의 부분군이 아니라 내재적인 대상입니다.

**예제 46.1.5** ( $S^1$  위의 좌표 모음집)

다음은 두 개의 열린집합을 가진  $S^1$ 의 좌표 모음집을 그림으로 나타낸 것입니다.



**질문 46.1.6.** “chart”와 “atlas”라는 단어가 어디에서 왔다고 생각하십니까?

**예제 46.1.7** (위상 다양체의 몇 가지 예)

- (a) 길게 논의했듯이, 구  $S^2$ 는 2-다양체입니다: 구 위의 모든 점은  $D^2$ 처럼 보이는 작은 열린 근방을 가집니다. 지구는 단 두 개의 반구로 덮을 수 있으며, 각 반구는 원판과 위상동형입니다.
- (b) 원  $S^1$ 은 1-다양체입니다; 모든 점은 열린 구간처럼 보이는 열린 근방을 가집니다.
- (c) 원환면, 클라인 병,  $\mathbb{RP}^2$ 는 모두 2-다양체입니다.
- (d)  $\mathbb{R}^n$ 은 자명하게 다양체이며, 그 열린집합들 또한 마찬가지입니다.

$\mathbb{R}^n$ 을 제외하면 이 모든 공간은 콤팩트합니다.

다양체가 아닌 예로  $D^n$ 이 있는데, 이는 경계를 가지기 때문입니다. 경계 위의 점들은 유클리드 공간처럼 보이는 열린 근방을 갖지 않습니다.

## §46.2 매끄러운 다양체

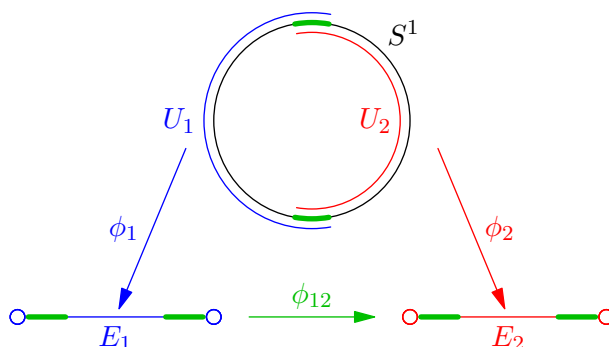
**이 절의 대표적인 예:** 모든 위상 다양체.

$M$ 을 아틀라스  $\{U_i \xrightarrow{\phi_i} E_i\}$ 를 갖는 위상  $n$ -다양체라고 합시다.

**정의 46.2.1.**  $U_i \cap U_j \neq \emptyset$ 인 모든  $i, j$ 에 대해, **전이 사상**  $\phi_{ij}$ 는 다음과 같이 합성된 사상입니다

$$\phi_{ij}: E_i \cap \phi_i^{\text{img}}(U_i \cap U_j) \xrightarrow{\phi_i^{-1}} U_i \cap U_j \xrightarrow{\phi_j} E_j \cap \phi_j^{\text{img}}(U_i \cap U_j).$$

표기가 조밀해서 죄송합니다, 설명해 드리겠습니다. 상  $\phi_i^{\text{img}}(U_i \cap U_j)$ 와 상  $\phi_j^{\text{img}}(U_i \cap U_j)$ 의 교집합은 이 사상이 잘 정의되고 위상동형사상이 되도록 만들기 위한 표기상의 번거로움입니다. 전이 사상은 그저  $E_i \rightarrow E_j$ 로 가는 자연스러운 방식을, 겹치는 부분으로 제한한 것일 뿐입니다. 아래 그림에서 교집합은 각  $E_1$ 과  $E_2$ 의 초록색 부분입니다:



미분 형식을 사용할 수 있도록 충분한 구조를 추가하고자 합니다.

**정의 46.2.2.**  $M$ 의 모든 전이 사상이 매끄러우면  $M$ 을 **매끄러운 다양체**라고 합니다.

이 정의는 타당한데,  $\mathbb{R}^n$ 의 두 열린집합 사이의 사상이 미분 가능하다는 것이 무엇을 의미하는지 우리가 알고 있기 때문입니다.

매끄러운 다양체를 이용하면  $\mathbb{R}^n$ 에 대해 구축한 정의들을 우리의 다양체로 이식해 볼 수 있습니다. 그래서 일반적으로, 매끄러운 다양체와 관련된 모든 정의는 각 좌표 조각에서의 어떤 것으로, 호환 조건과 함께 귀결됩니다.

예시로, 다음은 "매끄러운 사상"의 정의입니다:

**정의 46.2.3.** (a)  $M$ 을 매끄러운 다양체라 합시다. 연속 함수  $f: M \rightarrow \mathbb{R}$ 가 **매끄럽다**는 것은 다음 합성이

$$E_i \xrightarrow{\phi_i^{-1}} U_i \hookrightarrow M \xrightarrow{f} \mathbb{R}$$

가 함수  $E_i \rightarrow \mathbb{R}$ 로서 매끄러우면 **매끄럽다**고 합니다.

(b)  $M$ 과  $N$ 을 아틀라스  $\{U_i^M \xrightarrow{\phi_i} E_i^M\}_i$ 와  $\{U_j^N \xrightarrow{\phi_j} E_j^N\}_j$ 를 갖는 매끄러운 다양체라 합시다. 사상  $f: M \rightarrow N$ 이 **매끄럽다**는 것은 모든  $i$ 와  $j$ 에 대해 다음 합성 사상이

$$E_i \xrightarrow{\phi_i^{-1}} U_i \hookrightarrow M \xrightarrow{f} N \twoheadrightarrow U_j \xrightarrow{\phi_j} E_j$$

이 함수  $E_i \rightarrow E_j$ 로서 매끄러우면 **매끄럽다**고 합니다.

## §46.3 정칙값 정리

**이 절의 대표적인 예:**  $x^2 + y^2 = 1$ 은 원입니다!

일반적인 다양체에 대해 이렇게 많이 써 왔음에도 불구하고, 원  $x^2 + y^2 = 1$ 이  $\mathbb{R}^2$ 에 매장된 1차원 다양체의 훌륭한 예라는 것을 알고 있으면서도 실제로 다양체를 어떻게 구성하는지 제대로 알려드리지 않고 여러분을 여기 남겨두는 것은 다소 매정한 일일 것입니다.

### 정리 46.3.1 (정칙값 정리)

$V$ 를  $n$ 차원 실수 노름 벡터 공간이라 하고,  $U \subseteq V$ 를 열린집합이라 하며,  $f_1, \dots, f_m: U \rightarrow \mathbb{R}$ 을 매끄러운 함수들이라고 합시다.  $M$ 을  $f_1(p) = \dots = f_m(p) = 0$ 을 만족하는 점  $p \in U$ 들의 집합이라고 합시다.

$M$ 이 공집합이 아니고 사상

$$V \rightarrow \mathbb{R}^m \quad \text{에 의해} \quad v \mapsto ((Df_1)_p(v), \dots, (Df_m)_p(v))$$

모든 점  $p \in M$ 에서 계수(rank)  $m$ 을 가집니다. 그러면  $M$ 은 차원  $n - m$ 의 다양체입니다.

증명은 [Sj05, 정리 6.3]를 참고하십시오.

매우 흔한 특수한 경우 하나는 위에서  $m = 1$ 로 두는 것입니다.

### 따름정리 46.3.2 (수준 초곡면)

$V$ 를 유한 차원 실수 노름 벡터 공간이라 하고,  $U \subseteq V$ 를 열린집합,  $f: U \rightarrow \mathbb{R}$ 를 매끄러운 함수라 합시다.  $M$ 을  $f(p) = 0$ 을 만족하는 점  $p \in U$ 들의 집합이라 합시다. 만약  $M \neq \emptyset$ 이고 임의의  $p \in M$ 에 대해  $(Df)_p$ 가 영사상이 아니라면,  $M$ 은 차원  $\dim V - 1$ 의 다양체입니다.

### 예제 46.3.3 (원 $x^2 + y^2 - c = 0$ )

$f(x, y) = x^2 + y^2 - c$ ,  $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ 라 합시다. 여기서  $c$ 는 양의 실수입니다. 다음을 주목하십시오.

$$Df = 2x \cdot dx + 2y \cdot dy$$

이는 특히  $(x, y) \neq (0, 0)$ 인 한, 즉  $c \neq 0$ 인 한 0이 아닙니다. 따라서:

- $c > 0$ 일 때, 결과로 얻어지는 곡선 — 반지름이  $\sqrt{c}$ 인 원 — 은 우리가 이미 알고 있었듯이 1차원 다양체입니다.
- $c = 0$ 일 때는 이 결과가 성립하지 않습니다. 실제로  $M$ 은 단 하나의 점이며, 이는 사실 0차원 다양체입니다!

여러분이 실제 구체적인 예시를 작성할 수 있는 능력을 기르도록 그저 지나가며 언급하는 것이므로 더 이상의 예시는 제시하지 않겠습니다. (하지만 [Sj05, 제6.2장]에는 아름답게 그려진 더 많은 예시가 있습니다.)

## §46.4 다양체 위의 미분 형식

열린집합  $U \subseteq \mathbb{R}^n$  위에서 미분 형식이 무엇인지는 이미 알고 있습니다. 따라서 자연스럽게 이 정의를 각 부분집합으로 옮겨오되, 호환성 조건을 추가하고자 합니다.

$M$ 을 아틀라스  $\{U_i \xrightarrow{\phi_i} E_i\}_i$ 를 가진 매끄러운 다양체라 합시다.

**정의 46.4.1.** 매끄러운 다양체  $M$  위의 **미분  $k$ -형식**  $\alpha$ 란, 각  $E_i$  위의 미분  $k$ -형식들의 모임  $\{\alpha_i\}_i$ 로서, 임의의  $j$ 와  $i$ 에 대해 다음이 성립하는 것을 말합니다.

$$\alpha_j = \phi_{ij}^*(\alpha_i).$$

말로 풀어 쓰면: 각 좌표계 위에 미분 형식을 하나씩 지정하되, 전이 사상들의 당겨오기 아래에서 호환되도록 지정합니다.

## §46.5 방향

**이 절의 대표적인 예:** 왼쪽 대 오른쪽, 시계 방향 대 반시계 방향.

이것으로는 아직 다양체 위에서 적분하기에 충분하지 않습니다. 방향이라는 정의가 하나 더 필요합니다.

주된 문제는 표준 미적분학에서의 다음 관찰입니다.

$$\int_a^b f(x) dx = - \int_b^a f(x) dx.$$

그렇다면 구간과 위상동형인 공간  $M$ 을 생각해 봅시다. 1-형식  $\alpha$ 가 있다면, 이를  $M$  위에서 어떻게 적분할까요?  $M$ 은  $(\mathbb{R}$ 의 부분집합이 아니라) 단지 위상 공간일 뿐이므로, 우리가 고를 수 있는 기본값으로서의 "왼쪽"이나 "오른쪽"이 존재하지 않습니다. 또 다른 예로,  $M = S^1$ 이 원이라면,  $M$ 을  $\mathbb{R}^2$ 에 매장하기로 결정하지 않는 한 기본값으로서의 "시계 방향"이나 "반시계 방향"이 존재하지 않습니다.

이를 우회하려면 실제로 우리의 다양체에 대해 추가적인 가정을 세워야 합니다.

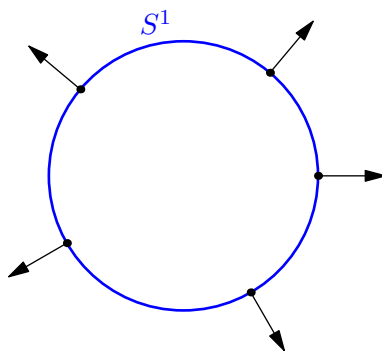
**정의 46.5.1.** 매끄러운  $n$ -다양체가 **방향 가능**하다는 것은,  $M$  위에 미분  $n$ -형식  $\omega$ 가 존재하여 모든  $p \in M$ 에 대해 다음이 성립함을 뜻합니다.

$$\omega_p \neq 0.$$

여기서  $\omega_p$ 는  $\wedge^n(V^V)$ 의 원소임을 상기하십시오. 이 경우  $\omega$ 를  $M$ 의 **부피 형식**이라고 부릅니다.

이 정의를 어떻게 그림으로 그려볼 수 있을까요? 미분 형식이란  $M$ 의 접벡터를 받아 실수를 반환하는 것임을 상기해 봅시다. 이를 위해, 각 점  $p \in M$ 이  $n$ 차원인 **접평면**  $T_p(M)$ 을 가진다고 생각할 수 있습니다. 이제 부피 형식  $\omega$ 가  $n$ 차원이므로, 이는  $T_p(M)$ 의 기저 전체를 받아 실수를 하나 내놓습니다. 따라서 다양체가 방향 가능하다는 것은, 다양체의 모든 점에서 접벡터들의 기저에 대해 일관된 부호 선택이 존재함을 뜻합니다.

"매장된 다양체"의 경우, 이는 각 점  $p \in M$ 에 대해 0이 아닌 법선 벡터장을 선택할 수 있음을 의미할 뿐입니다. 예를 들어,  $S^1$ 은 이러한 방식으로 방향 가능합니다.



마찬가지로, 중심에서 멀어지는(또는 중심을 향하는) 벡터장을 가짐으로써 구  $S^2$ 에 방향을 줄 수 있습니다. 접평면  $T_p(M)$ 을 정의하지 않았으므로 이는 전혀 엄밀하지 않습니다.  $M$ 은 일반적으로 내재적인 대상이기 때문에  $T_p(M)$ 을 정의하려면 상당히 우회적인 방법을 써야 합니다(다만 이는 뒤의 선택 절에서 다루겠습니다). 어쨌든, 요점은 공간의 방향 가능성에 대한 추측이 대체로 옳을 가능성이 높다는 것입니다.

#### 예제 46.5.2 (방향 가능한 곡면)

- (a) 구  $S^n$ , 평면, 그리고 원환면  $S^1 \times S^1$ 은 방향 가능합니다.
- (b) 뫼비우스 띠와 클라인 병은 *orientable*하지 않습니다: 이들은 "한쪽만 있는" 곡면입니다.
- (c)  $\mathbb{CP}^n$ 은 임의의  $n$ 에 대해 방향을 줄 수 있습니다.
- (d)  $\mathbb{RP}^n$ 은  $n$ 이 홀수일 때만 방향을 줄 수 있습니다.

## §46.6 다양체에 대한 스토크스 정리

일반적인 경우의 스토크스 정리는 **경계가 있는 다양체**(manifold with boundary)  $M$ 이라는 개념에 기반을 두고 있는데, 이를 정의하지는 않겠지만 그 경계  $\partial M$ 이  $n-1$ 차원 다양체이며

$M$ 이 방향이 주어져 있으면 그 경계도 방향이 주어진다라는 것만 언급하겠습니다. 한 예로  $M = D^2$ 가 있는데, 이는 경계  $\partial M = S^1$ 을 가집니다.

다음으로,

**정의 46.6.1.**  $M$  위의 미분 형식  $\alpha$ 의 **지지집합**(support)이란 다음 집합의 폐포입니다

$$\{p \in M \mid \alpha_p \neq 0\}.$$

이 지지집합이 위상 공간으로서 콤팩트하면,  $\alpha$ 가 **콤팩트 지지**(compactly supported)를 갖는다고 말합니다.

**비고 46.6.2** — 예를 들어, 부피 형식은  $M$  전체에서 지지됩니다.

이제 방향이 주어진 다양체 위에서 적분을 정의할 수 있지만, 그 정의가 정말로 끔찍하기 때문에 여기서는 정의하지 않겠습니다. 그러면 스토크스 정리는 다음과 같이 말합니다

**정리 46.6.3 (다양체에 대한 스토크스 정리)**

$M$ 을 경계가 있는 매끄러운 방향  $n$ -다양체라 하고  $\alpha$ 를 콤팩트 지지를 갖는  $(n-1)$ -형식이라 합시다. 그러면

$$\int_M d\alpha = \int_{\partial M} \alpha.$$

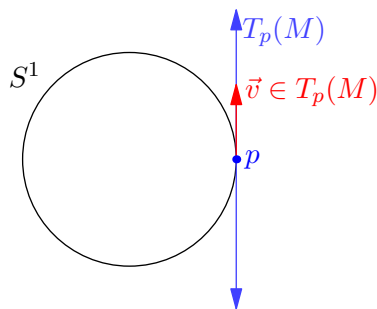
생략된 모든 세부 사항은 [Sj05]에서 완전히 전개되어 있습니다.

## §46.7 (선택) 접공간과 여접공간

**이 절의 대표적인 예:** 원에 접하는 직선, 또는 구에 접하는 평면을 그려보십시오.

$M$ 을 매끄러운 다양체라 하고  $p \in M$ 을 한 점이라 합시다. 앞에서  $T_p(M)$ 의 정의를 생략했었는데, 이제 실제로 정의하고자 합니다.

앞서 말했듯이, 기하학적으로 우리에게 익숙한 예시들에서 이것이 어떤 모습이어야 하는지는 이미 알고 있습니다. 예를 들어,  $M = S^1$ 이  $\mathbb{R}^2$ 에 埋め込まれた 원이라면, 점  $p$ 에서의 접벡터는 그저 원에 접하며 뻗어나가는 벡터처럼 보여야 합니다. 마찬가지로, 구  $M = S^2$ 가 주어졌을 때, 구를 따라 점  $p$ 에서의 접공간은  $p$ 에서  $M$ 에 접하는 평면처럼 보일 것입니다.



그러나 이 모든 다양체 이론의 요점 중 하나는, 다양체를  $\mathbb{R}^n$ 에 埋め込まれた 것으로서가 아니라 그 자체로 내재적 대상(intrinsic object)으로 보고자 한다는 것입니다.<sup>1</sup> 따라서 우

<sup>1</sup>이는 케일리의 정리가 모든 군이 치환군의 부분군이라고 알려주지만, 그럼에도 우리가 군을 그 자체로 추상적인 대상으로 생각하는 방식과 유사하다고 볼 수 있습니다.

이것이 항상 그랬던 것은 아니라는 점에 유의하십시오! 19세기 동안 군은 문자 그대로  $GL(n)$  또는  $S_n$ 의 부분집합으로 정의되었습니다. 실제로 실로우는 "군"이라는 단어 없이도 자신의 정리들을 전개했습니다. 훨씬 나중에야  $S_n$ 으로의 어떠한 매장(embedding)과도 무관한 추상 집합  $G$ 로서, 그 자체로 독립적인 대상인 군의 추상적 정의가 주어졌습니다.

리는 접벡터라는 개념이 주변 공간을 참조하지 않고, 오직 문제가 되는 다양체  $M$ 의 내재적 성질만을 참조하기를 바랍니다.

### §46.7.i 접공간

이 구성을 동기 부여하기 위해, 이미 답을 알고 있는 埋め込まれた 경우인 구에서부터 시작해봅시다.

$f: S^2 \rightarrow \mathbb{R}$ 가 구 위의 함수라 하고, 점  $p$ 를 택합시다. 점  $p$  근처에서  $f$ 는 원점의 어떤 열린 근방 위의 함수처럼 보입니다. 따라서 상상 속의 접평면 안에서 벡터  $\vec{v}$ 를 따라 방향 미분(directional derivative)을 취하는 것을 생각해볼 수 있습니다(즉, 어떤 편미분입니다). 고정된  $\vec{v}$ 에 대해 이 편미분은 하나의 선형 사상입니다

$$D_{\vec{v}}: C^\infty(M) \rightarrow \mathbb{R}.$$

이는 반대 방향으로도 성립함이 밝혀집니다:  $D_{\vec{v}}$ 가 모든 매끄러운 함수에 대해 무엇을 하는지 안다면,  $\vec{v}$ 를 복원할 수 있습니다. 이것이 접공간을 만들기 위해 우리가 사용하는 요령입니다. 벡터  $\vec{v}$ 를 직접 명시하려 하는 대신(주변 공간이 없으므로 이는 할 수 없습니다),

**벡터란 편미분과 유사한 사상입니다.**

좀 더 형식적으로, 다음과 같은 내용이 있습니다.

**정의 46.7.1.**  $p$ 에서의 **미분**  $D$ 란 다음의 라이프니츠 규칙을 만족시키는 선형 사상  $D: C^\infty(M) \rightarrow \mathbb{R}$  (즉, 모든 매끄러운  $f$ 에 실수를 대응시키는 사상)입니다: 임의의  $f, g$ 에 대해 다음 등식이 성립합니다.

$$D(fg) = f(p) \cdot D(g) + g(p) \cdot D(f) \in \mathbb{R}.$$

이는 단지 “곱 규칙”일 뿐입니다. 그러면 접공간은 쉽게 정의할 수 있습니다:

**정의 46.7.2.** **접벡터**란 단지  $p$ 에서의 derivation이며, **접공간**  $T_p(M)$ 은 이러한 접벡터들 전체의 집합일 뿐입니다.

이렇게 하여 접공간을 구성하였습니다.

### §46.7.ii 쌍대접공간

실제로,  $D$ 에 대한 곱 규칙은 다음 세 조건과 동치임을 보일 수 있습니다:

1.  $D$ 는 선형입니다. 즉  $D(af + bg) = aD(f) + bD(g)$ 입니다.
2.  $D(1_M) = 0$ 이며, 여기서  $1_M$ 은  $M$  위의 상수 함수입니다.
3.  $f(p) = g(p) = 0$ 일 때마다  $D(fg) = 0$ 입니다. 직관적으로, 이는 함수  $h = fg$ 가  $p$ 에서 이차로 소멸한다면  $D$ 를 따른 그 미분값은 0이어야 함을 의미합니다.

이는 세 번째 동치인 정의를 시사합니다: 다음을 정의한다고 합시다

$$\mathfrak{m}_p := \{f \in C^\infty M \mid f(p) = 0\}$$

이는  $p$ 에서 소멸하는 함수들의 집합입니다 (이를  $p$ 에서의 극대 아이디얼이라고 부릅니다). 이 경우,

$$\mathfrak{m}_p^2 = \left\{ \sum_i f_i \cdot g_i \mid f_i(p) = g_i(p) = 0 \right\}$$

은  $p$ 에서 이차로 소멸하는 함수들의 집합입니다. 따라서, 접벡터란 실제로는 단지 다음과 같은 선형 사상일 뿐입니다

$$\mathfrak{m}_p/\mathfrak{m}_p^2 \rightarrow \mathbb{R}.$$

다시 말해, 접공간은 사실  $\mathfrak{m}_p/\mathfrak{m}_p^2$ 의 쌍대 공간이며, 이러한 이유로 공간  $\mathfrak{m}_p/\mathfrak{m}_p^2$ 는 **여접공간** (접공간의 쌍대)으로 정의됩니다. 이 정의는 위의 미분(derivation)을 이용한 정의보다 훨씬 더 추상적이지만, 다음과 같은 좋은 성질들을 가지고 있습니다:

- 좌표에 무관하다는 점과,
- 매끄러운 함수  $M \rightarrow \mathbb{R}$ 만을 이용하여 정의된다는 점인데, 이는 이후 대수기하학에서 다양체나 스킴을 다루며 이 정의를 그대로 반복할 때 상당히 유용할 것입니다.

### §46.7.iii 타당성 검증

이렇게 동치인 정의들을 모두 살펴본 후, 마지막으로 해야 할 일은 이 접공간의 정의가 실제로 차원  $n$ 인 벡터 공간을 준다는 것을 확인하는 것입니다. 이를 위해서는  $\mathbb{R}^n$ 의 열린 부분 집합에 대해서만 이를 확인하면 충분한데, 이는 일반적인 다양체  $M$ (국소적으로  $\mathbb{R}^n$ 의 열린 부분집합인)에 대한 결과를 함의할 것입니다. 실해석학의 몇 가지 도구를 사용하면, 다음 결과를 증명할 수 있습니다:

#### 정리 46.7.3

$M \subset \mathbb{R}^n$ 이 열려 있고  $0 \in M$ 이라고 합시다. 그러면

$$\mathfrak{m}_0 = \{\text{매끄러운 함수 } f \mid f(0) = 0\}$$

$$\mathfrak{m}_0^2 = \{\text{매끄러운 함수 } f \mid f(0) = 0, (\nabla f)_0 = 0\}.$$

다시 말해  $\mathfrak{m}_0^2$ 는 0에서 소멸하고  $f$ 의 모든 1계 도함수가 영점에서 소멸하는 함수들의 집합입니다.

따라서, 다음과 같은 동형사상이 존재함을 알 수 있습니다

$$\mathfrak{m}_0/\mathfrak{m}_0^2 \cong \mathbb{R}^n \quad \text{에 의해} \quad f \mapsto \left[ \frac{\partial f}{\partial x_1}(0), \dots, \frac{\partial f}{\partial x_n}(0) \right]$$

그러므로 여접공간, 즉 접공간은 실제로 차원  $n$ 을 가집니다.

### §46.8 생각해 볼 만한 조금 더 어려운 문제

**문제 46A.** 매끄러운 다양체  $M$  위의 미분 0-형식이 매끄러운 함수  $M \rightarrow \mathbb{R}$ 와 동일한 것임을 보이십시오.

여기서 정칙값 정리(regular value theorem)의 몇 가지 응용

# XIII

리만 곡면

## 제XIII부: 목차

---

|           |                                          |            |
|-----------|------------------------------------------|------------|
| <b>47</b> | <b>리만 곡면의 기본 정의</b>                      | <b>495</b> |
| 47.1      | 복소 구조 . . . . .                          | 495        |
| 47.2      | 리만 곡면 . . . . .                          | 497        |
| 47.3      | 복소 다양체 . . . . .                         | 498        |
| 47.4      | 리만 곡면의 예 . . . . .                       | 498        |
| <b>48</b> | <b>리만 곡면 사이의 사상</b>                      | <b>501</b> |
| 48.1      | 정의 . . . . .                             | 501        |
| 48.2      | 리만 구면으로 가는 함수 . . . . .                  | 501        |
| 48.3      | 그 밖의 몇 가지 좋은 성질들 . . . . .               | 502        |
| 48.4      | 사상의 중복도 . . . . .                        | 504        |
| 48.5      | 유리형 함수의 위수의 합 . . . . .                  | 505        |
| 48.6      | 후르비츠 공식 . . . . .                        | 505        |
| 48.7      | 항등 정리 . . . . .                          | 505        |
| <b>49</b> | <b>아핀 평면 곡선과 사영 평면 곡선</b>                | <b>507</b> |
| 49.1      | 아핀 평면 곡선 . . . . .                       | 507        |
| 49.2      | 사영직선 $\mathbb{CP}^1$ . . . . .           | 512        |
| 49.3      | 사영 평면 곡선 . . . . .                       | 513        |
| 49.4      | 구멍 매우기 . . . . .                         | 514        |
| 49.5      | 평면 곡선의 마디점 . . . . .                     | 515        |
| <b>50</b> | <b>미분 형식</b>                             | <b>517</b> |
| 50.1      | $\mathbb{C}$ 위의 미분 형식 . . . . .          | 517        |
| 50.2      | 미분 형식의 시각화 . . . . .                     | 517        |
| <b>51</b> | <b>리만-로흐 정리</b>                          | <b>521</b> |
| 51.1      | 동기 . . . . .                             | 521        |
| 51.2      | 인자 . . . . .                             | 523        |
| 51.3      | 제수의 차수 . . . . .                         | 524        |
| 51.4      | 유리형 함수의 주인자(principal divisor) . . . . . | 524        |
| 51.5      | 리만-로흐 정리 . . . . .                       | 525        |
| <b>52</b> | <b>선다발</b>                               | <b>527</b> |
| 52.1      | 개요 . . . . .                             | 527        |
| 52.2      | 정의 . . . . .                             | 527        |
| 52.3      | 선다발 시각화하기 . . . . .                      | 528        |
| 52.4      | 선다발 사이의 사상 . . . . .                     | 534        |
| 52.5      | 가역층과의 관계 . . . . .                       | 534        |

---

# 47 리만 곡면의 기본 정의

대략적으로 말하면, 리만 곡면 이론은 미분기하학의 아이디어를 사용한 복소해석학의 일반화에 불과합니다: 2-다양체가 실평면  $\mathbb{R}^2$ 의 조각들을 매끄럽게 접합하여 더 복잡한 대상을 이루는 것으로 볼 수 있는 것처럼, 우리는 복소평면  $\mathbb{C}$ 의 “조각”들을 해석적으로 접합합니다.

정칙 함수의 이론이 매우 좋다는 것은 이미 알고 있습니다 — 그것들은 모두 해석적입니다! 여기서도 같은 정도의 경직성을 기대할 수 있습니다.

실제로 콤팩트 리만 곡면 위에서는, 이론이 정칙 함수의 경우보다 더욱 좋아집니다! 예를 들면:

- $Y$ 가 콤팩트인 두 리만 곡면  $X$ 와  $Y$ 에 대해, 임의의 유리형 함수  $f: X \rightarrow Y$ 는 사실 정칙이어야 합니다. 즉, 모든 곳에서 정의됩니다.
- $X$ 가 콤팩트 리만 곡면이면, 정칙 함수  $f: X \rightarrow \mathbb{C}$ 는 상수입니다.
- 위와 같은 설정에서, 더 나아가  $g: X \rightarrow \mathbb{C}$ 가 유리형 함수이면,  $g$ 의 영점의 개수는 중복도를 포함하여  $g$ 의 극점의 개수와 같습니다.

**비고 47.0.1** (왜 우리는 이러한 좋은 성질들을 가지는 것일까요?) — 대략적으로 말하면,  $\mathbb{C}$ 는 콤팩트하지 않습니다 — 이는 구멍이 제거된 리만 구와 동형입니다. 구멍을 메움으로써, 우리는 이전에 극점이었던 곳에서 값  $\infty$ 를 취하도록 유리형 함수를 확장할 수 있습니다.

방향 가능한 2-다양체로서, 우리는 리만 곡면의 **종수**를 정의할 수 있습니다 — 이는 순전히 위상적인 개념이지만, 매우 놀라운 방식으로 여러 대수적 불변량과 결정적으로 연결되어 있습니다. 암호학에서 타원 곡선에 대해 들어본 적이 있을 것입니다 — 이것들 또한 리만 곡면으로 나타나며, 그 일반화인 **초타원 곡선**은 임의의 종수  $\geq 2$ 를 가지는 리만 곡면의 족을 이룹니다!

## §47.1 복소 구조

이전 장들에서의 정의를 상기해봅시다:

- 위상  $n$ -다양체는 하우스도르프 공간으로서, 각각이  $\mathbb{R}^n$ 과 동형인 피복  $\{U_i\}$ 를 가집니다.
- 매끄러운  $n$ -다양체는 모든 전이 사상이 매끄러운 위상  $n$ -다양체입니다.

이들의 공통점은 무엇일까요? 겉보기에는 그리 많지 않아 보입니다. 하지만 본질적으로, 이들은 모두 같은 철학을 설명하고 있습니다:

우리는 가산 개의 조각  $\{U_i\}$ 를 취하여, 근본적인 구조를 유지하면서 이들을 접합합니다.

여기서, 위상 다양체는 위상적 구조를 가지며, 매끄러운 다양체는 매끄러운 구조를 가집니다. 비슷한 방식으로, 복소 다양체는 복소 구조를 가집니다.

여기서 “구조”란 무엇을 의미할까요?

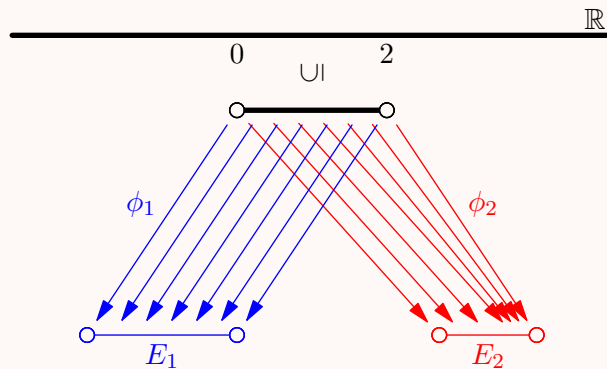
먼저, 위상적 구조는 여러분에게 익숙합니다 — 그것은 그저 위상입니다. 형식적으로, 위상은 열린집합들의 모임으로 정의되지만, 위상적 구조의 실제 의미는 다음을 결정합니다:

- 어떤 집합이 열려있다고 또는 닫혀있다고 간주되는지,
- 점들의 수열이 주어진 점으로 수렴하는지,
- 사상  $X \rightarrow Y$  또는  $Y \rightarrow X$ 가 연속인지 ( $Y$ 가 또 다른 위상 공간으로 주어졌을 때),
- 등입니다.

기존의 (하우스도르프) 위상을 가진 위상  $n$ -다양체가 주어졌을 때, 우리는 국소 좌표계가 위상적 구조를 존중하는지, 즉 동형사상인지 여부를 판별할 수 있습니다.

**예제 47.1.1** ( $(0, 2)$ 는 위상 1-다양체입니다)

$\mathbb{R}$ 에 포함된 열린 구간  $(0, 2)$ 는 위상 다양체로 간주될 수 있습니다.



이 공간에 대한 두 가지 가능한 좌표계,  $\phi_1$ 과  $\phi_2$ 가 나타나 있습니다.

이들의 공식은  $\phi_1: (0, 2) \rightarrow (0, 2), \phi_1(x) = x$ 와  $\phi_2: (0, 2) \rightarrow (0, 1.3), \phi_2(x) = x + 0.35 \cdot (1 - x - |1 - x|)$ 입니다.

위의 예시에서, 좌표계  $\phi_2$ 가 위상동형사상임에도 불구하고 매끄러워 보이지 않는다는 것을 알아차렸을 것입니다. 그래서 매끄러운 2-다양체를 다음과 같은 식으로 정의하고 싶어집니다:

곡면  $S \subseteq \mathbb{R}^3$ 이 매끄러운 2-다양체라는 것은, 각  $p \in S$ 에 대해  $E \subseteq \mathbb{R}^2$ 와 미분 동형인 열린 근방  $V \subseteq S$ 가 존재한다는 것입니다.

실제로 이것이 고전 미분기하학에서의 실제 정의입니다 — 물론 이것이 완전히 일반적이지는 않은데, 예를 들어 클라인 병은  $\mathbb{R}^3$ 에 매장될 수 없다는 것을 우리는 알고 있습니다.

그렇다면 우리는 왜 정의 46.2.2에서 이와 비슷한 것을 정의하지 않았을까요? 문제는, 미분동형사상이라는 개념이 하우스도르프 위상 공간 위에서 정의되지 않는다는 것입니다 — 사실 정의될 수가 없는데, 바로 위의 예시에서 미분동형사상이 아닌 위상동형사상을 볼 수 있습니다 — 다시 말해, 하나의 위상 공간에 서로 다른 매끄러운 구조가 부여될 수 있다는 것입니다.

그러므로 정의 46.2.2이 하고 있는 일의 본질은, 각 조각  $E_i \subseteq \mathbb{R}^n$ 으로부터 위상 공간  $M$ 으로 매끄러운 구조를 유도함으로써 매끄러운 구조가 무엇을 의미하는지를 암묵적으로 정의하는 것입니다. 전이 함수가 매끄러워야 한다는 조건은, 물론, 서로 다른  $\phi_i$ 에 의해  $M$  위에 유도된 매끄러운 구조들이 동일함을 보장하기 위한 것입니다.

완전히 같은 방식으로, 우리는 정의 46.1.2를 다음과 같이 대체할 수도 있었을 것입니다:

위상  $n$ -다양체  $M$ 이란,  $M$ 을 덮는 부분집합들의 모임  $\{U_i\}$ 를 갖춘 집합으로서, 각  $U_i$ 에 대해  $\mathbb{R}^n$ 의 부분집합으로 가는 전단사 사상이 존재하며, 이를

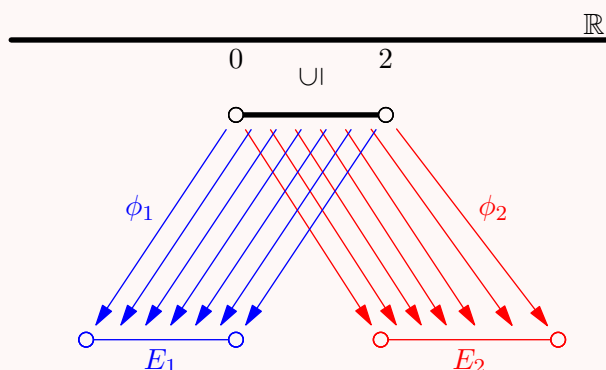
$$\phi_i: U_i \rightarrow E_i \subseteq \mathbb{R}^n$$

이라 할 때, 각  $E_i$ 는  $\mathbb{R}^n$ 의 열린집합이며, 모든 전이 사상이 위상적 위상동형사상이라는 조건을 만족시킵니다.

여기서  $\phi_i$ 는 "집합 동형사상"이며, 정의 46.2.2에서의 위상동형사상과 비슷한 역할을 하고, 위상 공간 구조 역시 조각  $E_i$ 로부터 유사하게 유도됩니다.

**예제 47.1.2** ( $(0, 2)$ 는 매끄러운 1-다양체입니다)

위와 마찬가지로,  $\mathbb{R}$ 에 포함된 열린 구간  $(0, 2)$  또한 매끄러운 다양체로 간주될 수 있습니다.



이번에는  $\phi_1$ 은 위와 동일하지만,  $\phi_2: (0, 2) \rightarrow (0, 2 + \frac{1}{e})$ 는 다음과 같이 정의됩니다

$$\phi_2(x) = \begin{cases} x & \text{만약 } x \leq 1 \\ x + e^{-1/(x-1)} & \text{그렇지 않으면.} \end{cases}$$

$\phi_1$ ,  $\phi_2$ , 그리고 이들의 역함수가 모두 매끄러운 함수이므로, 전이 사상  $\phi_1 \circ \phi_2^{-1}$ 와  $\phi_2 \circ \phi_1^{-1}$  역시 매끄러우며, 따라서 정의 46.2.2의 가정을 만족시킵니다.

이 개념을 잠시 곰곰이 생각해 볼 필요가 있습니다 —  $\mathbb{R}^n$  위의 매끄러운 함수는 너무나 자연스러운 것이기에, 매끄러운 다양체가 단순한 위상 이상의 구조를 지닌다는 사실을 잊기 쉽습니다.

다시 한번, 위의 예시에서 보았듯이,  $\mathbb{R}^n$ 은 단순히 매끄럽다는 것 이상의 구조를 가지고 있습니다 — 바로 해석적 구조입니다. 좌표계  $\phi_2$ 는 이 구조를 보존하지 않습니다.

그러므로 리만 곡면에 대해서는 다음과 같이 정의하겠습니다:

**리만 곡면이란, 국소적으로  $\mathbb{C}$ 처럼 보이며 복소-매끄러운 구조를 지니는 매끄러운 (실) 2-다양체입니다.**

물론, 복소해석학의 기적 덕분에 — 정칙 함수는 해석적입니다! — 이는 리만 곡면이 복소해석적 구조를 지닌다고 말하는 것과 동치입니다.

## §47.2 리만 곡면

**이 절의 대표적인 예:** 리만 구, 또는  $\{z \in \mathbb{C} \mid |z| < 1\}$ 과 같은  $\mathbb{C}$ 의 임의의 열린집합.

위의 동기로부터, 리만 곡면의 정의가 자연스럽게 도출됩니다:

**정의 47.2.1** (리만 곡면). **리만 곡면**  $X$ 란 가산 개의 집합으로 이루어진 열린 덮개  $\{U_i\}$ 를 가지는 제2가산 연결 하우스도르프 공간이며, 이 집합들은 동형사상에 의해  $\mathbb{C}$ 의 열린 부분

집합들과 위상동형인 것을 말합니다,

$$\phi_i: U_i \xrightarrow{\cong} E_i \subseteq \mathbb{C}$$

다음과 같이 정의되는 **전이 사상**  $\phi_{ij}$ 가

$$\phi_{ij}: E_i \cap \phi_i^{\text{img}}(U_i \cap U_j) \xrightarrow{\phi_i^{-1}} U_i \cap U_j \xrightarrow{\phi_j} E_j \cap \phi_j^{\text{img}}(U_i \cap U_j).$$

해석함수가 되도록 하는 것입니다. 각  $\phi_i$ 를 **복소 좌표계**라 부르며, 이들을 함께 모으면 **복소 아틀라스**를 이룹니다.

복소 아틀라스가 하우스도르프 공간에 **복소 구조**를 부여한다고 말합니다. 따라서 다시 말해, 리만 곡면은 복소 구조를 갖는 (제2가산, 연결, 하우스도르프) 위상 공간입니다.

[Mi95]에는 극대 복소 아틀라스에 의한 다른 정의가 있습니다. 두 정의는 동일하지만, 실제로는 무한히 많은 복소 좌표계를 지정하는 것보다 유한히 많은 복소 좌표계를 지정하는 것이 더 쉽습니다.

복소 좌표계  $U_i \rightarrow E_i$ 는  $U_i$  위에 **국소 좌표**를 부여하는 것으로 생각해야 합니다. 형식적으로는:

**정의 47.2.2.** 점  $p \in X$ , 열린집합  $U \subseteq X$ , 그리고 복소 좌표계  $\phi: U \rightarrow \mathbb{C}$ 에 대해, 각  $x \in U$ 마다  $z = \phi(x)$ 라 하면,  $z$ 를 **국소 좌표**라 부릅니다.  $\phi(p) = 0$ 이면 이 국소 좌표가  $p$ 에 **중심을 둔다**고 말합니다.

### §47.3 복소 다양체

실  $n$ -다양체의 정의와 유사하게, 복소 다양체를 정의할 수 있습니다. 위에서와 마찬가지로, 이 구조는 매끄러운 곡면보다 훨씬 더 강한 경직성을 가집니다.

**정의 47.3.1** (복소  $n$ -다양체). **복소  $n$ -다양체**란 가산 개의 집합으로 이루어진 열린 덮개  $\{U_i\}$ 를 가지는 하우스도르프 공간이며, 이 집합들은 동형사상에 의해  $\mathbb{C}^n$ 의 열린 부분집합들과 위상동형인 것을 말합니다,

$$\phi_i: U_i \xrightarrow{\cong} E_i \subseteq \mathbb{C}^n$$

**전이 사상**  $\phi_{ij}$ 가 해석 함수가 되도록 합니다.

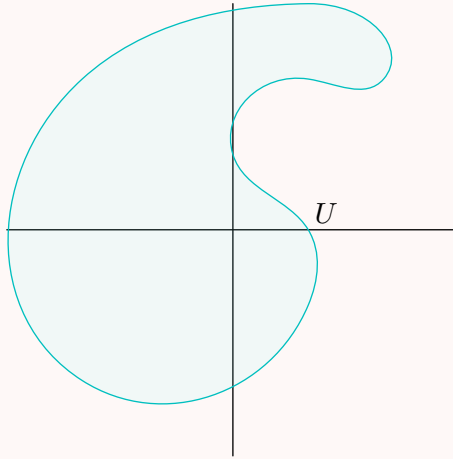
물론, 복소  $n$ -다양체는 자연스럽게 매끄러운 (실)  $2n$ -다양체가 됩니다.

### §47.4 리만 곡면의 예

이 장에서는 몇 가지 예가 제시될 것입니다.

#### 예제 47.4.1 ( $\mathbb{C}$ 의 열린 부분집합)

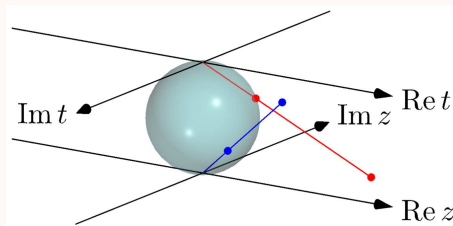
연결된 열린 부분집합  $U \subseteq \mathbb{C}$ 는 어느 것이든 리만 곡면입니다.



이는 지루한 예시입니다 (전체가 어떠한 집합도 없이 정의될 수 있습니다), 하지만 계속 진행해 봅시다.

#### 예제 47.4.2 (리만 구면)

리만 구면  $\mathbb{C}_\infty$ 는 매끄러운 2-다양체로서 그저 하나의 구면입니다.



그 복소 구조는 다음과 같이 정의됩니다:

$N = (0, 0, 1)$ 과  $S = (0, 0, 0)$ 이 두 대척점이 되도록 구면을  $\mathbb{R}^3$ 에 매장합니다.

$E_1$ 을  $xy$ -평면이라 하고,  $E_2$ 를  $z = 1$ 인 점들의 집합이라 합시다.

그러면  $\phi_1: \mathbb{C}_\infty \setminus \{N\} \rightarrow E_1$ 을 (점  $N$ 을 제외한) 구에서 점  $N$ 을 지나  $E_1$ 로 향하는 입체 사영이라 하고,  $\phi_2: \mathbb{C}_\infty \setminus \{S\} \rightarrow E_2$ 를 (점  $S$ 을 제외한) 구에서 점  $S$ 을 지나  $E_2$ 로 향하는 입체 사영이라 합시다.

$E_1$ 과  $E_2$ 를  $z \mapsto (\operatorname{Re} z, \operatorname{Im} z, 0) \in E_1$ 과  $t \mapsto (\operatorname{Re} t, -\operatorname{Im} t, 1) \in E_2$ 에 의해  $\mathbb{R}^3$ 에 매장된 복소평면의 사본으로 생각합니다. 그러면  $\phi_1$ 과  $\phi_2$ 는  $\mathbb{C}_\infty$ 의 복소 좌표계입니다.

$\phi_1$ 과  $\phi_2$ 의 정의역은  $\mathbb{C}_\infty$ 를 덮습니다.  $\mathbb{C}_\infty$ 를 복소다양체로 만들려면,  $\phi_1$ 과  $\phi_2$ 에 의해 유도되는 복소 구조가 동일함을 확인해야 합니다 — 실제로,  $N$ 도  $S$ 도 포함하지 않는 임의의 열린집합  $U$  위에서, 이 사영들은 모든  $p \in U$ 에 대해  $\phi_1(p) = \frac{1}{\phi_2(p)}$ 의 관계를 만족합니다.

이는 또한  $t \mapsto (\operatorname{Re} t, -\operatorname{Im} t, 1)$ 에서 왜 음의 부호가 필요한지 설명해줍니다 — 그렇지 않으면 이 사영들은  $\phi_1(p) = \frac{1}{\phi_2(p)}$ 의 관계를 만족하게 되는데, 이는 해석적이지 않습니다.

우리는 리만 구를 빠진 점  $\infty$ 를 "채우기" 위해  $\mathbb{C}$ 의 두 사본을 용접하여 얻은 결과로 생각할 수 있습니다.

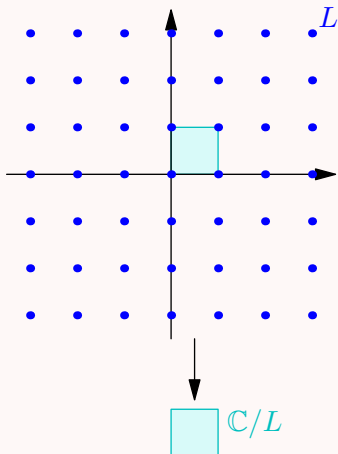
위의 예에서,  $\phi_1$ 이 주는 국소 좌표는  $S$ 를 중심으로 하고,  $\phi_2$ 가 주는 국소 좌표는  $N$ 을 중심으로 합니다. 점  $\phi_1^{-1}(4)$ 는 좌표계  $\phi_1$  아래에서 국소 좌표  $z = 4$ 를 가지며, 좌표계  $\phi_2$

아래에서는 국소 좌표  $t = \frac{1}{4}$ 를 가지게 됩니다.

#### 예제 47.4.3 (복소 원환면)

$L$ 을  $\mathbb{C}$ 의 실부와 허부가 모두 정수인 복소수들의 집합  $\mathbb{Z}[i]$ 라고 합시다. 그러면  $L$ 은  $\mathbb{C}$ 의 덧셈 부분군을 이룹니다.

몫  $\mathbb{C}/L$ 을 생각해봅시다. 몫사상  $\mathbb{C} \rightarrow \mathbb{C}/L$ 은  $\mathbb{C}/L$  위에 자연스러운 복소 구조를 유도합니다.



여기서는  $\mathbb{C}/L$ 을 정사각형으로 그리지만, 위쪽 변과 아래쪽 변, 그리고 왼쪽 변과 오른쪽 변이 매끄럽게 용접되어 있다고 상상해야 합니다.

원환면의 각 작은 조각에 대해, 몫사상의 원상 중 적절한 성분을 취함으로써 이를  $\mathbb{C}$ 로 동형적으로 대응시킬 수 있습니다 — 사영의 서로 다른 선택들은  $a \in L$ 에 대한 전이 함수  $\phi_{ij}(x) = x + a$ 로 관계되며, 이는 해석적입니다.

복소 원환면은 콤팩트하므로,  $\mathbb{C}/L$  위의 임의의 정칙 함수는 상수입니다. 유리형 함수는 더 흥미로우며, 구성하기도 더 어렵습니다.

그리고 몇 가지 반례들입니다.

#### 예제 47.4.4

두 리만 구의 서로소 합집합은 연결되어 있지 않으므로 리만 곡면이 아닙니다.

리만 곡면이 연결되어야 한다는 조건은 정리들이 깔끔하게 성립하도록 하기 위한 단순한 기술적 조건에 불과합니다 — 복소 구조를 갖는 임의의 위상 공간은 각 연결 성분마다 하나씩 대응하는 리만 곡면들의 서로소 합집합으로 분해될 수 있기 때문에, 이 조건을 요구한다고 해서 잃는 것은 그리 많지 않습니다.

# 48 리만 곡면 사이의 사상

## §48.1 정의

이 정의는 우리가 예상하는 그대로입니다 — 리만 곡면의 주요 특징이 복소 구조이므로, 사상  $f: \mathbb{C} \rightarrow \mathbb{C}$ 가 리만 곡면 사이의 사상이 되는 것은 그것이 정칙일 때, 그리고 오직 그때 뿐입니다.

**정의 48.1.1.**  $X$ 와  $Y$ 를 리만 곡면이라 합시다. 사상  $f: X \rightarrow Y$ 가  $p \in X$ 에서 정칙인 것은,  $p \in U_1$ 을 만족하는  $X$  위의 차트  $\phi_1: U_1 \rightarrow E_1$ 과  $f(p) \in U_2$ 를 만족하는  $Y$  위의 차트  $\phi_2: U_2 \rightarrow E_2$ 가 존재하여 합성  $\phi_2 \circ f \circ \phi_1^{-1}$ 가  $\phi_1(p)$ 에서 정칙이 될 때, 그리고 오직 그때 뿐입니다.  $f$ 가  $X$ 의 모든 점에서 정칙일 때, 그리고 오직 그때에만  $f$ 를 **리만 곡면 사이의 사상**이라고 합니다.

다시 말해:  $f$ 가 정칙인 것은 국소 좌표 사이를 대응시키는 함수로서 정칙일 때, 그리고 오직 그때뿐입니다.

### 예제 48.1.2

몇 가지 예시를 들어보겠습니다.

- $f(x) = x^3$ 으로 정의되는 함수  $f: \mathbb{C} \rightarrow \mathbb{C}$ 는 사상입니다.  
이 함수는 전단사가 아님에 유의하십시오.  $p \neq 0$ 인 각 점에서는  $f$ 가 역함수를 갖는 열린 근방이 존재하지만, 0에서는  $f$ 가 역함수를 갖지 않습니다.
- 복소평면을 리만 구면에 내포시키는 사상  $\mathbb{C} \hookrightarrow \mathbb{C}_\infty$ 는 사상입니다.

## §48.2 리만 구면으로 가는 함수

**이 절의 대표적인 예:** 유리형 함수  $\frac{1}{z}$ 는 정칙  $\mathbb{C} \rightarrow \mathbb{C}_\infty$  함수로 만들 수 있습니다.

이 절에서는 리만 구면  $\mathbb{C}_\infty$ 를 “무한대의 점이 추가된  $\mathbb{C}$ ”로 볼 수 있음을 살펴보겠습니다. 이러한 해석을 통해 유리형 함수  $f: X \rightarrow \mathbb{C}$ 를 정칙 사상  $g: X \rightarrow \mathbb{C}_\infty$ 로 해석할 수 있으며, 이는 유리형 함수를 훨씬 더 잘 다룰 수 있게 해줍니다 — 더 이상 특이점이 존재하지 않으며, 결과 함수  $g$ 는 어디서나 정칙입니다!

먼저,  $\mathbb{C}_\infty$ 가 자연스럽게 점 하나가 추가된  $\mathbb{C}$ 로 해석될 수 있음을 살펴봅시다: **예제 47.4.2**에서와 같은 표기법을 사용하여,  $\mathbb{C}_\infty \setminus \{N\}$ 을 사상  $\phi_1$ 을 통해  $E_1$ 과 (따라서  $\mathbb{C}$ 와) 동일시하고,  $\infty$ 를 점  $N$ 이라 합시다.

**질문 48.2.1.** 이 점을  $\infty$ 라고 부르는 것이 타당함을 스스로 확인해 보십시오 —  $|z_i| \rightarrow +\infty$ 를 만족하는  $\mathbb{C}$  위의 점들의 모든 수열  $\{z_i\}$ 에 대해, 위상 공간으로서의  $\mathbb{C}_\infty$ 에서  $\phi_1^{-1}(z_i) \rightarrow \infty$ 가 성립합니다.

그러면,  $X$ 를 리만 곡면이라 하고,  $f: X \rightarrow \mathbb{C}$ 를  $X$  위의 유리형 함수라 합시다. 자연스럽게,  $g$ 는 다음과 같이 정의될 수 있습니다

$$g(z) = \begin{cases} f(z) & \text{만약 } f(z) \neq \infty \\ \infty & \text{만약 } f(z) = \infty. \end{cases}$$

그러면  $g$ 는 연속입니다 — 그뿐만 아니라, 해석적이기도 합니다.

**질문 48.2.2.** 분명히,  $g(z) \neq \infty$ 인 점  $z \in X$ 에서는  $g$ 가 해석적입니다.  $g(z) = \infty$ 인  $z \in X$ 에서도  $g$ 가 해석적임을 스스로 확인해 보십시오. (예제 47.4.2에서와 같은 표기법을 사용하여, 작은 열린집합  $U \subseteq X$ 를 취하고,  $g^{\text{img}}(U) \subseteq \mathbb{C}_\infty$ 를  $t = 1/z$ 로 재매개변수화해 보십시오.)

따라서,

### 명제 48.2.3

$g$ 가 항등적으로  $\infty$ 가 아닌 유리형 함수  $f: X \rightarrow \mathbb{C}$ 와 정칙 사상  $g: X \rightarrow \mathbb{C}_\infty$  사이에는 일대일 대응이 존재합니다.

또는, 좀 더 편하게 말하면,

$\mathbb{C}$ 의  $\infty$ 에 있는 구멍을 메움으로써, 유리형 함수를 어디에서나 정칙인  $\mathbb{C} \cup \infty$  사이의 사상으로 해석적으로 확장할 수 있게 됩니다.

## §48.3 그 밖의 몇 가지 좋은 성질들

지난 절에서 우리는 리만 구면  $\mathbb{C}_\infty$ 가 유리형 함수의 특이점을 제거할 수 있게 해준다는 것을 방금 살펴보았습니다.

비형식적으로 말하면, 이는  $\mathbb{C}_\infty$ 가  $\mathbb{C}$ 의 "콤팩트화"이기 때문입니다 — 콤팩트하게 만들기 위해 한 점을 추가한 것입니다 — 그리고 콤팩트 리만 곡면은 여러 좋은 성질을 가집니다.

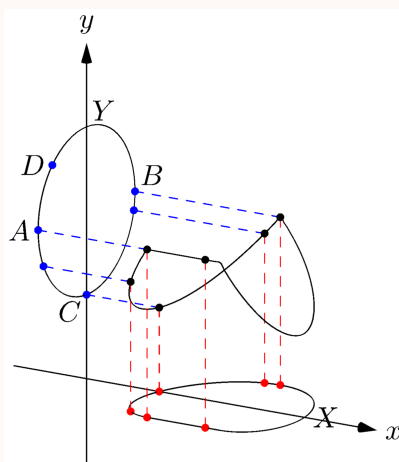
### 명제 48.3.1

$X$ 와  $Y$ 가 콤팩트하고,  $f: X \rightarrow Y$ 가 정칙이며 상수가 아니라고 합시다. 각 점  $y \in Y$ 에 대해,  $d_y$ 를  $y$ 의 원상에 속한 점들의 중복도의 총합으로 정의합니다. 그러면,  $d_y$ 는 잘 정의되어 있으며 상수입니다.

이 명제가 왜 놀라운지 알 수 있습니다:

### 예제 48.3.2 (이 명제는 매끄러운 콤팩트 다양체에 대해서는 성립하지 않습니다)

콤팩트 매끄러운 실 1-다양체 사이의 다음 함수  $f: X \rightarrow Y$ 를 생각해 봅시다. 이는  $x$ 축과  $y$ 축을 가진 그래프로 나타내었습니다. (콤팩트한 1-다양체는  $\mathbb{R}$ 에 매장될 수 없다는 점에 유의하십시오. 왜냐하면  $\mathbb{R}$ 의 콤팩트 부분집합은 닫혀 있고 유계이므로 반드시 경계를 가지기 때문입니다. 제대로 된 그래프는 4차원 공간에 존재해야 하는데, 이는 시각화하기가 상당히 어려우므로, 근사적인 표현으로 만족하겠습니다.)



여기서,  $X$ 와  $Y$ 는 모두 단위원과 동형사상 관계에 있습니다.  
 $Y$ 의 각 점 위에 있는 올(fiber)의 점의 개수를 세어 봅시다:

- 점  $A$  위에는, 무한히 많은 점이 있습니다.
- 점  $B$  위에는, 오직 한 점만 있습니다. (다만 이 점이 "중복도 2"를 가진다고 주장할 수 있습니다)
- 점  $C$  위에는, 두 점이 있습니다.
- 점  $D$  위에는, 올이 공집합입니다.

**정의 48.3.3.** 위의 값  $d_y$ 는 사상  $f$ 의 **차수**라고 불리며,  $\deg(f)$ 로 씁니다.

#### 예제 48.3.4

사상  $z \mapsto z^k$ 를  $\mathbb{C}_\infty \rightarrow \mathbb{C}_\infty$  사상으로 확장하면, 차수  $k$ 를 가집니다.

$t \neq 0$ 이면,  $t$ 가 서로 다른  $k$ 개의  $k$ 제곱근을 가진다는 것을 알고 있습니다. 하지만  $t = 0$ 이면, 그 원상은 오직 점 0만으로 이루어져 있습니다 — 이 경우, 우리는  $z = 0$ 이 "중복점"이라고 말하고 싶습니다 — 다음 절에서 사상의 중복도를 정의할 때 이를 엄밀하게 formalize하겠습니다.

**절 74.1**를 읽으셨다면, 이는 사실  $X$ 와  $Y$ 가 모두 리만 구인 경우의 호몰로지에서의 차수 개념과 동일합니다 — 이는  $\text{im } f$ 가 몇 개의 구형 자루로 이루어져 있는지를 세는 것입니다. 하지만, 이 경우에는, 이론이 특별히 더 좋습니다 — 그래프가 각 점을  $d$ 번 덮는 것과 호모토피 동치일 뿐만 아니라, 각 점이 실제로 정확히  $d$ 번 덮이기 때문입니다!

이 주제는 복소해석학과 리만 곡면에서 반복적으로 나타날 것입니다. 기본적으로:

**"것들"을 제대로 세면, 공식이 매우 깔끔합니다.**

이 명제의 증명은 어렵지 않습니다 — 핵심 관찰은 정리가  $f(z) = z^n$  형태의 함수에 대해 참이며, 각 점  $p \in X$  주변에서 국소적으로  $f$ 가 동형사상이거나 위의 형태를 가진다는 것입니다. 따라서  $d_y$ 는 국소적으로 상수이며,  $Y$ 가 연결되어 있으므로 상수가 됩니다.

## §48.4 사상의 중복도

**이 절의 대표적인 예:**  $f(x) = (x - 3)^2$ 는  $\text{mult}_3(f) = 2$ 를 가집니다.

이전 절에서, 우리는 한 점에서의 사상의 중복도에 대해 비형식적으로 이야기했습니다. 이 절에서 이를 엄밀하게 정의하겠습니다.

### 예제 48.4.1

$f(z) = z^5 + 1$ 로 주어진 사상  $f: \mathbb{C} \rightarrow \mathbb{C}$ 를 생각해 봅시다.

각 점  $y \in \mathbb{C}$  위에서, 올  $f^{\text{pre}}(y)$ 는 5개의 점을 가집니다 —  $y = 1$ 인 경우는 예외로, 이때  $f^{\text{pre}}(1) = \{0\}$ 는 오직 1개의 점만을 가집니다.

이러한 동작은 바람직하지 않으며, 우리는 함수  $f$ 가 점 0의 “동일한 사본” 5개를 점 1로 보낸다고 말하고 싶습니다. (다른 관점으로 보면, 1로 수렴하는 각 수열  $\{y_i\}$ 에 대해, 각  $i$ 마다  $f(x_i) = y_i$ 를 만족하며 0으로 수렴하는 서로 다른 수열  $\{x_i\}$ 가 5개 존재합니다.)

이에 영감을 받아, 다음과 같은 방식으로 중복도를 정의하겠습니다:

- $z \mapsto z^m$ 은 정수  $m \geq 1$ 에 대해 중복도  $m$ 을 가집니다.
- 정의역이나 공역에 대해 정칙 재매개화를 수행하더라도, 차수는 변하지 않습니다.

이 두 성질이 차수를 완전히 정의한다는 것이 밝혀졌습니다! 다음이 성립합니다.

### 명제 48.4.2

$f: X \rightarrow Y$ 를  $p \in X$ 에서 정의된 상수가 아닌 정칙 사상이라 합시다. 그러면,  $f(p)$ 를 중심으로 하는  $Y$  위의 모든 좌표계  $\phi_2: U_2 \rightarrow V_2$  (즉,  $\phi_2(f(p)) = 0$ )에 대해,  $p$ 를 중심으로 하는  $X$  위의 좌표계  $\phi_1: U_1 \rightarrow V_1$ 이 존재하여, 유도된 사상  $\phi_2 \circ f \circ \phi_1^{-1}: V_1 \rightarrow V_2$ 가  $z \mapsto z^m$ 의 형태를 가지도록 하는 유일한 정수  $m \geq 1$ 이 존재합니다.

다시 말해,  $Y$ 의 좌표계를 고정하면,  $X$ 의 (열린 부분집합의) 좌표계가 존재하여  $\mathbb{C}$ 의 열린 부분집합 사이에 유도된 사상이 거듭제곱 사상이 되도록 할 수 있으며, 더 나아가 그 지수는 선택에 무관합니다.

**모든 사상은 국소적으로  $z \mapsto z^m$ 처럼 보입니다.**

증명. 본질적으로, 테일러 전개를 이용하여  $m$ 을 결정하면,  $\phi_1$ 의 선택은 그 제약 조건들에 의해 거의 고정됩니다.  $\square$

**정의 48.4.3.** 위의 값  $m$ 은 점  $p$ 에서  $f$ 의 **중복도**이며,  $\text{mult}_p(f)$ 로 표기합니다.

### 예제 48.4.4 (점에서의 사상의 중복도에 대한 더 많은 예시)

몇 가지 예시를 살펴보겠습니다.

- $\mathbb{C} \rightarrow \mathbb{C}_\infty$  사상으로 확장된 함수  $z \mapsto z^{-2}$ 는 점 0에서 중복도 2를 가집니다 — 점 0의 “두 사본”이 점  $\infty$ 로 사상됩니다.
- 함수  $f(z) = (z - 1)(z - 2)^5$ 는  $\text{mult}_2(f) = 5$ 를 가집니다 — 더 일반적으로,  $p$ 가  $f$ 의 근이라면,  $\text{mult}_p(f)$ 는 그 근의 중복도입니다.
- 함수  $z \mapsto z + 1$ 은 모든 곳에서 중복도 1을 가집니다 — 사실, 상수가 아닌 사상의

“대부분의” 점에서의 중복도는 1이 됩니다.

이것들이 공식 용어입니다:

**정의 48.4.5.**  $\text{mult}_p(f) > 1$ 인 점  $p$ 를 **분기점**이라 부릅니다. 이 경우, 점  $f(p)$ 를 **가지점**이라 부릅니다.

## §48.5 유리형 함수의 위수의 합

우리가 좋은 공식을 얻는 또 다른 경우입니다.

### 예제 48.5.1

( $\mathbb{C} \rightarrow \mathbb{C}$  함수를 자명한 방식으로 확장하여 정의된) 몇 가지 유리형  $\mathbb{C}_\infty \rightarrow \mathbb{C}_\infty$  함수를 고려하고, 그 영점과 극점을 (중복도와 함께) 나열해 보겠습니다.

| 함수                | 영점               | 극점               |
|-------------------|------------------|------------------|
| 5                 | 없음               | 없음               |
| $(x+1)^2$         | -1, -1           | $\infty, \infty$ |
| $\frac{1}{x^2+1}$ | $\infty, \infty$ | $i, -i$          |
| $\frac{x+1}{x+2}$ | -1               | -2               |

매번, 영점의 개수는 극점의 개수와 같습니다. 이것은 우연이 아닙니다!

### 명제 48.5.2

$f: X \rightarrow \mathbb{C}$ 를 콤팩트 리만 곡면  $X$  위의 상수가 아닌 유리형 함수라 합시다. 그러면

$$\sum_p \text{ord}_p(f) = 0.$$

이 성립합니다.

물론,  $X$ 가 콤팩트여야 합니다 — 영점은 여러 개 있지만 극점은 없는  $\mathbb{C} \rightarrow \mathbb{C}$  함수가 분명히 존재합니다.

증명.  $f$ 를  $X \rightarrow \mathbb{C}_\infty$  함수로 확장하면, 0의 울에 속한 점들의 중복도의 합은  $\infty$ 의 울에 속한 점들의 중복도의 합과 같습니다.  $\square$

## §48.6 후르비츠 공식

이것을 작성하십시오. 사실 꽤 멋진입니다

## §48.7 항등 정리

다음 명제들은 예상되는 바입니다 — 정칙 함수를 다루는 복소해석학에서도 동일한 현상이 나타납니다.

**정리 48.7.1**

$f, g: X \rightarrow Y$ 를 리만 곡면 사이의 정칙 사상이라 합시다.  $X$ 의 공집합이 아닌 열린집합 위에서  $f = g$ 이면,  $f = g$ 입니다.

이는 **문제 31C\***의 유사물입니다. 여기서  $X$ 가 연결되어 있다는 가정이 사용됨에 주목하십시오 —  $\mathbb{C}$ 의 두 사본의 분리합집합은 매끄러운 2-다양체이지만, 리만 다양체는 아닙니다. 즉,

정칙 사상은 경직되어 있습니다 — 함수의 값이 아주 작은 부분집합에서 결정되면 그 함수의 값은 어디서나 결정됩니다.

# 49 아핀 평면 곡선과 사영 평면 곡선

이 장에서는 아핀 평면 곡선과 사영 평면 곡선을 정의합니다. 여기에는 두 가지 목적이 있습니다:

- $\mathbb{R}^2$ 의 많은 흥미로운 곡선들은 다항식의 근의 집합으로 정의될 수 있습니다. 이는 단지 자연스러운 일반화일 뿐입니다.
- 사실, 모든 콤팩트 리만 곡면이 사영 곡선으로 쓰일 수 있음을 보게 될 것입니다! 따라서 사영 곡선을 연구함으로써, 우리는 실제로 모든 콤팩트 리만 곡면을 연구한 셈이 됩니다.

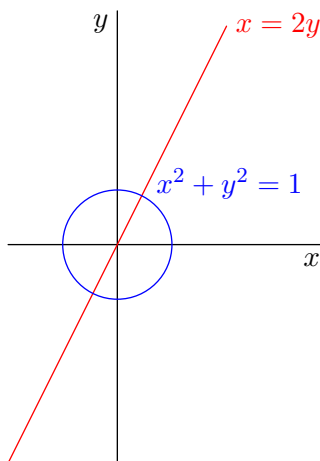
다음 절들에서 이것들이 의미하는 바를 살펴보겠습니다.

## §49.1 아핀 평면 곡선

평면 위의 몇 가지 친숙한 곡선들을 생각해 봅시다.

- 직선은 방정식  $y = ax + b$ , 또는  $x = c$ 로 나타낼 수 있습니다.
- 원은  $-1 \leq x \leq 1$ 에 대해  $y = \pm\sqrt{1-x^2}$ 의 집합으로 쓸 수 있습니다.

지금까지는 별다른 내용이 없지만, 여기 그림이 있습니다.



보시다시피, 위의 정의들은 사실 상당히 투박합니다. 곡선 위의 점들을 암묵적으로 정의함으로써 더 낮게 할 수 있습니다:

- 직선은  $ax + by + c = 0$ 을 만족하는  $(x, y)$ 의 집합으로 나타낼 수 있습니다.
- 원은  $x^2 + y^2 = 1$ 을 만족하는  $(x, y)$ 의 집합으로 나타낼 수 있습니다.

물론, 이 방식으로는 점의 좌표를 계산적으로 구하기가 더 어렵지만, 정의는 더 깔끔합니다. 요점은 다음과 같습니다:

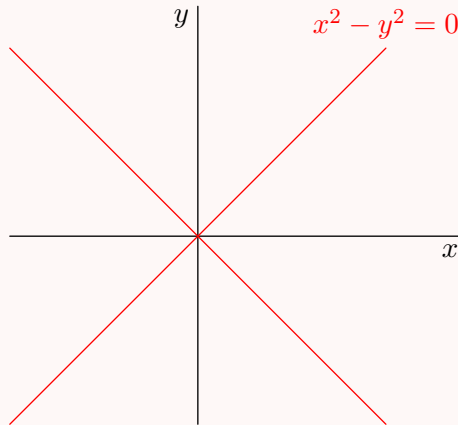
**흥미로운 곡선들 중 많은 경우가 다항식의 근의 집합으로 쓰일 수 있습니다.**

그래서 우리는 여기서도 같은 것을 시도해 볼 것입니다 — 직관적으로, 복소 차원 2에서 시작하여 다항식 하나를 지정하면, 남은 부분은 복소 차원 1을 갖게 됩니다, 즉 리만 곡면이 됩니다.

먼저, 우리가 해결해야 할 기술적인 세부사항이 하나 있습니다 — 다항식의 근의 집합이 매끄러운 곡선일 필요는 없다는 점입니다.

### 예제 49.1.1

$\mathbb{R}^2$ 에서  $x^2 - y^2 = 0$ 의 근의 집합은 원점 근처에서 곡선이 아닙니다 — 서로 교차하는 두 개의 곡선이 있습니다.



이는 다항식에 제약을 줌으로써 쉽게 처리할 수 있습니다.  $f(x, y)$ 를 다항식이라 하고,  $X = \{(x, y) \in \mathbb{R}^2 \mid f(x, y) = 0\}$ 라 합시다. 그러면:

### 정리 49.1.2

$\frac{\partial f}{\partial x}$ 와  $\frac{\partial f}{\partial y}$ 가 둘 다 소멸하지는 않는 점  $(x, y) \in X$ 에 대해,  $X$ 는  $(x, y)$  근처에서 매끄럽습니다.

$\frac{\partial f}{\partial x} \neq 0$  또는  $\frac{\partial f}{\partial y} \neq 0$ 인 점  $(x, y) \in X$ 에서, 우리는  $X$ 가  $(x, y)$ 에서 **매끄럽다** 또는 **비특이적이다**라고 말합니다.

사실, 우리에게는 더 많은 것이 있습니다. 위와 같은 표기법으로,  $(x, y) \in X$ 라 하면, 다음이 성립합니다:

- $\frac{\partial f}{\partial x} \neq 0$ 이라 가정하면, 점  $(x, y)$  근처에서  $X$ 는 어떤 해석적 함수  $g$ 에 대해  $x = g(y)$ 로 매개변수화될 수 있습니다.
- $\frac{\partial f}{\partial y} \neq 0$ 이라고 가정하면, 점  $(x, y)$  근방에서  $X$ 는 어떤 해석 함수  $h$ 에 대해  $y = h(x)$ 로 매개변수화될 수 있습니다.

이 모든 것은 그저 음함수 정리일 뿐입니다.

**연습문제 49.1.3.** 원  $x^2 + y^2 = 1$  위에서 점  $(0, 1)$ 과  $(1, 0)$ 에 대해 위의 명제를 확인해 보십시오.

$\mathbb{R}^2$ 를  $\mathbb{C}^2$ 로 바꾸어도 정확히 동일한 명제가 성립합니다.

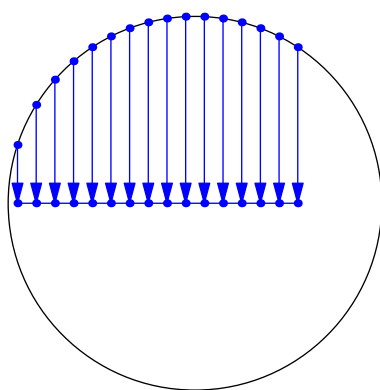
다음으로, 근의 집합  $X$ 가 단순히  $\mathbb{C}^2$  안의 점들의 집합이 아니라 실제로 리만 곡면이 되기를 원합니다. 따라서  $X$  위에 적절한 해석적 구조를 찾아야 합니다.

위의 원에서 적절한 해석적 구조는 무엇일까요? 한 가지 가능한 생각은 원을 호의 길이에 따라 펼쳐서  $\mathbb{R}$  위로 사상하는 것이지만, 리만 곡면에 대해서는 이것조차 잘 정의되지 않습니다 — 예를 들어 구면을 평면 위로 어떻게 펼치겠습니까?

또 다른 가능성은, 위의 음함수 정리의 진술을 바탕으로 다음과 같이 선언하는 것입니다:

- $U$  안의 모든 점에서  $\frac{\partial f}{\partial x} \neq 0$ 인 열린집합  $U \subseteq X$  위에서,  $U$ 가 충분히 작아서  $X$ 가 어떤 해석 함수  $g$ 에 대해  $x = g(y)$ 로 매개변수화될 수 있다고 가정하면,  $\phi(x, y) = \phi(g(y), y) = y$ 인 사상  $\phi$ 는 복소 좌표계입니다.
- $\frac{\partial f}{\partial y} \neq 0$ 인 경우도 마찬가지입니다.

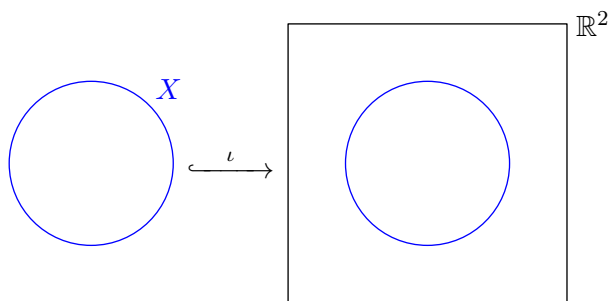
가능한 복소 좌표계 하나가 아래에 그려져 있습니다. 직관적으로, 두 점  $(1, 0)$ 과  $(-1, 0)$ 에서  $\frac{\partial f}{\partial y} = 0$ 이라는 사실은 이 "x로의 투영" 복소 좌표계가 이 점들에서 사용될 수 없음을 반영합니다.



사실 실해석적인 경우에는 위의 두 정의가 동치입니다. 원한다면 아래 연습문제를 풀어볼 수 있습니다.

**연습문제 49.1.4.** 위의 원에 대해 이를 보이십시오. (한 가지 가능한 방법은 호의 길이에 대한 명시적인 공식을 적고 그것이 해석적임을 보이는 것입니다)

이 정의가 이미 어느 정도 자연스럽기는 하지만, 여기에는 그 이상의 것이 있습니다. 범주론에서는 대상들 사이의 사상을 연구함으로써 대상들의 성질을 연구합니다. 위의 집합  $X$ 는 자연스러운 사상을 가지고 있습니다 —  $\mathbb{R}^2$ 로의 포함 사상이며,  $\mathbb{R}^2$ 는 명백히 이미 존재하는 해석적 구조를 가지고 있습니다.



위에서 정의한 해석적 구조는 다음과 같은 의미에서 자연스럽습니다:

- $Y \xrightarrow{g} X \xrightarrow{\iota} \mathbb{R}^2$ 인 함수  $g$ 에 대해,  $g$ 가 해석적인 것과  $\iota \circ g$ 가 해석적인 것은 동치입니다.
- $X \xrightarrow{\iota} \mathbb{R}^2 \xrightarrow{g} Y$ 인 함수  $g$ 에 대해,  $g$ 가 해석적인 것과  $g \circ \iota$ 가 해석적인 것은 동치입니다.

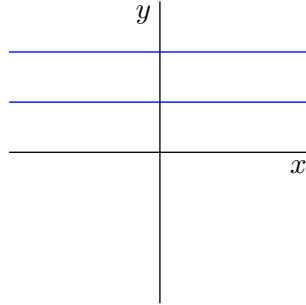
- $X \hookrightarrow \mathbb{R}^2$ 일 때,  $\iota$ 는 해석적이며,  $\iota'$ 이 해석적인 임의의 다른 복소 구조  $X' \xrightarrow{\iota'} \mathbb{R}^2$ 에 대해, 유일한 해석적 사상  $X' \rightarrow X$ 가 존재합니다.

실제로 위의 각 항목은  $X$  위의 복소 구조를 유일하게 결정합니다.

어떤 의미에서 이것은 우리의 자연스러운 해석적 구조에 대한 보편 성질과 같은 것입니다.

물론 우리는 해석적 실다양체가 무엇인지 정의하지 않았습니다. 용감한 독자는 이 모든 개념을 엄밀하게 형식화하고 위의 명제를 증명해 볼 수 있습니다.

정리해야 할 또 다른 기술적 세부사항이 있습니다.  $f(x, y) = (y-1)(y-2)$ 의 영점 집합은 다음과 같습니다:



이는 분명히 매끄럽습니다 — 하지만 연결되어 있지 않습니다. 우리는 리만 곡면이 연결되어 있을 것을 요구했습니다.

이 두 가지 문제를 제외하면, 우리의 최종 명제는 다음과 같습니다:

**정의 49.1.5.** 다항식  $f(z, w) \in \mathbb{C}[z, w]$ 가 주어졌을 때,  $f$ 의 근의 집합을  $X = \{(z, w) \in \mathbb{C}^2 \mid f(z, w) = 0\}$ 라고 합시다.  $X$ 가 연결되어 있고, 모든  $(z, w) \in X$ 에 대해  $f$ 가  $(z, w)$ 에서 매끄럽다고(즉,  $\frac{\partial f}{\partial z} \neq 0$ 이거나  $\frac{\partial f}{\partial w} \neq 0$ 이라고) 가정합시다. 그러면  $X$ 는 리만 곡면입니다 — 우리는  $X$ 를 **(매끄러운) 아핀 평면 곡선**이라고 부르며, 복소 좌표계는 다음과 같이 정의됩니다:

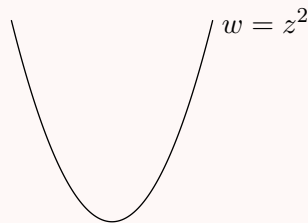
- $U$  위의 모든 점에서  $\frac{\partial f}{\partial z} \neq 0$ 인 열린집합  $U$ 에서,  $\phi: U \rightarrow \mathbb{C}$ ,  $\phi(z, w) = w$ 는 복소 차트입니다.
- $U$  위의 모든 점에서  $\frac{\partial f}{\partial w} \neq 0$ 인 열린집합  $U$ 에서,  $\phi: U \rightarrow \mathbb{C}$ ,  $\phi(z, w) = z$ 는 복소 차트입니다.

어떤 의미에서 더 “휘어진” 사영평면  $\mathbb{CP}^2$ 와 달리, 평면은 “평평하기” 때문에 이를 아핀이라고 부릅니다.

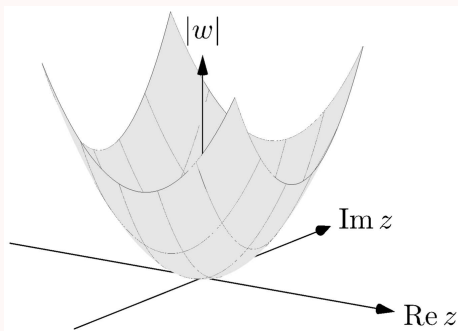
물론 예시가 몇 가지 있어야 할 것입니다 — 이러한 도구들을 갖추면, 우리는 (아핀) 타원 곡선과 다른 아핀 곡선들을 정의할 수 있는 위치에 있습니다.

#### 예제 49.1.6 (포물선)

$w = z^2$ 로 잘라낸 리만 곡면을 생각해봅시다. 그 실수부는 포물선처럼 생겼습니다:



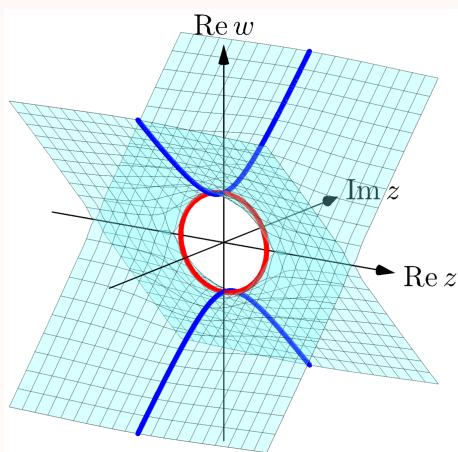
4차원의 그래프를 그리는 것은 어려우므로, 리만 곡면을 3차원으로 사영할 것입니다. 그 결과는 다음과 같습니다:



이 리만 곡면은 사실  $(z, w) \mapsto z$ 에 의해 복소평면  $\mathbb{C}$ 와 동형입니다.

#### 예제 49.1.7 (원)

원의 실수부가 어떤 모습인지는 모두 알고 있습니다. 그러나 리만 곡면 전체를 시각화하는 것은 다소 더 어렵습니다.



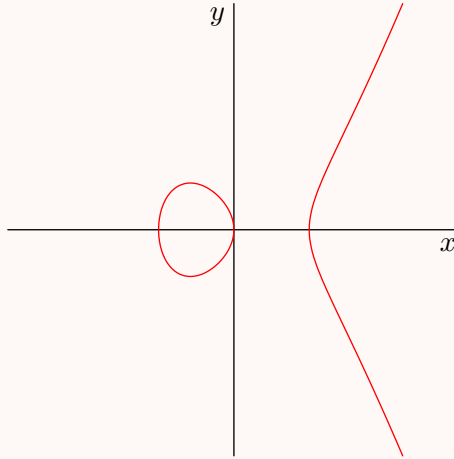
강조 표시된 빨간 원이 실수부입니다. 평면이 자기 자신과 교차하는 것처럼 보이는 것은 단지 사영에 의한 산물일 뿐이라는 점에 유의하십시오.

원은 복소평면  $\mathbb{C}$ 와 동형이 아니지만(이는 당분간 증명할 수 없을 것입니다<sup>a</sup>), 사실 변환  $y \mapsto y \cdot i$ 에 의해 쌍곡선  $x^2 - y^2 = 1$ 과 동형입니다. 또 다른 회전과 상수 곱셈을 거치면, 이는 다시 쌍곡선  $xy = 1$ 과 동형이 되는데, 이는 점  $(0, 0)$  하나가 빠진 직선  $x = y$ 와 “거의” 동형입니다.

<sup>a</sup>호모토피 장을 읽었다면, 이 리만 곡면은 그 실수부인 원으로의 변형 수축을 가지므로 원과 호모토픽합니다. 반면 복소평면  $\mathbb{C}$ 는 널호모토픽하다는 것을 우리는 알고 있습니다.

#### 예제 49.1.8 (타원곡선 $y^2 = x^3 - x$ )

실수부는 이렇게 생겼습니다. (이번에는 복소부는 그리지 않았습니다.)



이는 당분간 증명할 수 없겠지만, 유한개의 점을 제거하는 것을 허용하더라도 이 리만 곡면은  $\mathbb{C}$ 와 동형이 아니라는 것이 밝혀집니다.

## §49.2 사영직선 $\mathbb{CP}^1$

사영직선을 정의할 것입니다 — 앞으로 밝혀지겠지만, 이는 우리가 이미 정의한 리만 구  $\mathbb{C}_\infty$ 와 동형입니다. 따라서 이 절은 단지 우리의 도구가 어떻게 작동하는지를 보여주는 것일 뿐입니다.

이름에서 짐작하셨을 수도 있듯이: 점들의 집합으로서,  $\mathbb{CP}^1$ 은 점들의 집합  $\mathbb{C}^2 \setminus \{0\}$ 을, 임의의  $\lambda \in \mathbb{C} \setminus \{0\}$ 에 대한 관계  $(x, y) \sim (\lambda x, \lambda y)$ 로 나눈 몫입니다.

위상적 복소 다양체로서는, 다행히도 여전히 쉽습니다 —  $\mathbb{C}^2 \setminus \{0\}$ 은 자연스러운 위상을 가지며,  $\mathbb{CP}^1$ 은 몫위상을 얻습니다.

**연습문제 49.2.1.** 공간  $\mathbb{RP}^1$  위의 위상도 유사하게 정의하십시오.

**연습문제 49.2.2.**  $X \subseteq \mathbb{R}^2$ 를 점  $(0, 0)$ 을 지나지 않는 직선이라고 합시다.  $X \xrightarrow{f} \mathbb{R}^2 \xrightarrow{q} \mathbb{RP}^1$ 가 매장, 즉  $X \xrightarrow{q \circ f} \text{im}(q \circ f) \subseteq \mathbb{RP}^1$ 가 위상동형사상임을 보이십시오.

리만 곡면으로서, 일반적인 교과서적 정의는 다음과 같습니다:

**정의 49.2.3** ( $\mathbb{CP}^1$ 의 복소 구조).  $\mathbb{CP}^1$ 을 두 개의 열린집합으로 덮읍시다.  $U_1$ 은  $x$  좌표가 0이 아닌 점들로 이루어지고,  $U_2$ 는  $y$  좌표가 0이 아닌 점들로 이루어집니다. 그러면  $\phi_1(x, y) = y/x$ 로 주어진 복소 차트  $\phi_1: U_1 \rightarrow \mathbb{C}$ 와  $\phi_2(x, y) = x/y$ 로 주어진 복소 차트  $\phi_2: U_2 \rightarrow \mathbb{C}$  두 개가 복소 구조를 결정합니다.

그리고 이어서 두 열린집합이 실제로  $\mathbb{CP}^1$  전체를 덮고, 값  $y/x$ 가 잘 정의되며, 전이 사상 이 정칙임을 증명합니다.

위의 정의는 초등적이지만 통찰을 주지는 못합니다. 복소 좌표계는 어디에서 오는 것일까요?

앞 장에서 우리가 한 작업을 고려하면, 여기서 어디로 나아가야 할지는 명백해야 합니다. 시도해 볼 만한 두 가지가 있습니다:

- $X$ 를 점 0을 포함하지 않는  $\mathbb{C}^2$  안의 아핀 평면 곡선이라 합시다. 그러면 사상  $X \hookrightarrow \mathbb{C}^2 \twoheadrightarrow \mathbb{CP}^1$ 은 어떤 특정한 도함수가 소멸하지 않는 한 동형사상이어야 합니다.

- 사상을 이용할 수도 있습니다: 복소 구조는,  $Y \xrightarrow{f} \mathbb{C}^2 \xrightarrow{q} \mathbb{CP}^1$  또는  $\mathbb{C}^2 \xrightarrow{q} \mathbb{CP}^1 \xrightarrow{g} Y$ 가 주어졌을 때,  $f$ 가 해석적인 것과  $q \circ f$ 가 해석적인 것이 동치이고,  $g$ 가 해석적인 것과  $g \circ q$ 가 해석적인 것이 동치가 되도록 하는 것입니다.

둘 다 위의 정의와 동치입니다 — 사실 이 정의는 첫 번째 항목의 특수한 경우일 뿐이며, 여기서  $X$ 는 각각 직선  $x = 1$ 과  $y = 1$ 로 취해집니다. 우연히도, 이렇게 얻어지는 2개의 복소 좌표계는 대수적으로 가장 간단하게 쓸 수 있는 것이고, 이미  $\mathbb{CP}^1$  전체를 덮으므로 흔히 이것이 정의로 채택됩니다. 그러나 반드시 이 2개의 직선이어야 할 이유는 없습니다 —  $x + y = 1$ 과  $x - y = 1$ 을 사용해도 무방합니다.

### §49.3 사영 평면 곡선

이번에는 아핀 평면 곡선  $X \subseteq \mathbb{C}^2$ 를 사용하는 대신, 사영 평면 곡선  $X \subseteq \mathbb{CP}^2$ 를 정의하겠습니다.

“또 하나의 예시의 원천”이라는 점을 제외하면, 사영 평면 곡선에는 뚜렷한 이점이 있습니다 — 콤팩트하다는 것입니다! 이 덕분에 여러 좋은 성질들이 성립할 수 있으며, 지난 장에서 몇 가지를 살펴본 바 있습니다.

먼저 **사영 평면**  $\mathbb{CP}^2$ 를 정의하는 것으로 시작하겠습니다. 물론 이것은  $\mathbb{C}^3 \setminus \{0\}$ 을 관계  $(x, y, z) \sim (\lambda x, \lambda y, \lambda z)$ 로 몫을 취한 것입니다. 이는 몫사상에 의해  $\mathbb{C}^3$ 으로부터 유도되는 자연스러운 2차원 복소 구조를 가집니다.

위의 정의는 자연스럽지만 추상적입니다. 구체적으로는 다음과 같이 쓸 수 있습니다:

**질문 49.3.1.** (그것들이 잘 정의되는 열린집합 위에서) 세 개의 복소다양체 좌표계를 다음과 같이 정의합니다:

$$\phi_0(x, y, z) = (y/x, z/x)$$

$$\phi_1(x, y, z) = (x/y, z/y)$$

$$\phi_2(x, y, z) = (x/z, y/z).$$

이 복소다양체 구조가 올바른 것임을 스스로 확인해 보십시오.

그러면 사영 평면 곡선  $X$ 는  $f(x, y, z) = 0$ 을 만족하는 점  $(x, y, z)$ 들의 집합으로 정의됩니다 — 마찬가지로 어떤 매끄러움 및 연결성 조건을 만족해야 합니다. 안타깝게도, 만약 다항식이 예컨대  $f(x, y, z) = x - 1$ 이라면, 이는 잘 정의되지 않을 것입니다. 왜냐하면  $f(1, 0, 0) = 0$ 이지만  $f(2, 0, 0) = 1$ 이기 때문입니다. 그래서 우리는  $f$ 가 동차식일 것을 요구합니다 — 그렇게 하면  $f(x, y, z)$  자체는 여전히 잘 정의되지 않지만, 적어도  $f(x, y, z) = 0$ 인지 아닌지는 알 수 있습니다.

사영 평면 곡선 위의 복소 구조도 마찬가지로 보편 성질에 의해 정의됩니다.

이 정의는 간결하고 자연스럽지만 추상적입니다. 더 구체적인 정의는 아래에 주어집니다.

**질문 49.3.2.** 위와 같은 표기법 하에서,  $U_0, U_1, U_2$ 를 각각  $\phi_0, \phi_1, \phi_2$ 의 정의역으로 정의합니다.  $U_i \xrightarrow{\phi_i} \mathbb{C}^2$ 가  $U_i$ 와 아핀 평면  $\mathbb{C}^2$  사이의 동형사상을 준다는 점에 유의하십시오.

사영 평면 곡선  $X$ 와  $U_i$  중 하나의 교집합이,  $\mathbb{C}^2$ 로 사상되었을 때 (공집합일 수도 있는) 아핀 평면 곡선이 되며, 모든 사상이 동형사상임을 스스로 확인해 보십시오.

몇 가지 예시가 필요합니다.

#### 예제 49.3.3 (리만 구, 다시 한번)

리만 구는 대안적으로  $\mathbb{CP}^2$ 에서  $z = 0$ 인 점들의 집합으로 정의될 수 있습니다.

이것에는 특별히 흥미로운 점이 없습니다 — 우리는 이미 이 리만 곡면이 어떻게 생겼는지 알고 있습니다. 그저 자명한 예시로 쓰일 뿐입니다.

#### 예제 49.3.4 (타원 곡선, 다시 한번)

$f(x, y) = x^3 - x - y^2$ 라 합시다. 아핀 평면  $\mathbb{C}^2$ 에서  $f$ 의 근들의 집합이 타원 곡선임을 알고 있습니다.

$\mathbb{C}^2$ 를  $U_2$ 와 동일시하면,  $\mathbb{CP}^2$ 의 대부분의 점은  $(x, y, 1)$ 로 쓸 수 있습니다. 우리는  $\mathbb{CP}^2$ 에서의 근의 집합을  $U_2$ 로 제한했을 때 타원 곡선과 같아지는 다항식  $g(x, y, z)$ 를 찾고자 합니다.

직관적으로, 항등 정리에 의해 이것으로 리만 곡면을 유일하게 결정하기에 충분할 것입니다. 실제로, 우리가 찾는 다항식  $g$ 는 다음과 같습니다:

$$g(x, y, z) = x^3 - xz^2 - y^2z.$$

이는 다항식  $f$ 를 동차화하는 가장 게으른 방법일 뿐으로, 결과가 동차 다항식이 되도록  $z$ 의 최소 거듭제곱을 곱하는 것이며,  $g(x, y, 1) = f(x, y)$ 가 됩니다.

$\mathbb{CP}^2$ 는 콤팩트이고  $g$ 의 근의 집합은 닫혀 있으므로, 그 결과로 얻어지는 리만 곡면은 콤팩트입니다! 약속드린 대로입니다.

visualize this

밝혀진 바로는, 리만 구면과 달리 위의 타원 곡선으로 정의되는 리만 곡면은 종수 1을 가집니다! 우리는 리만 구면과 확실히 다른 첫 번째 예를 얻은 것입니다.

**연습문제 49.3.5.** 위의 예에서,  $z$ 의 더 큰 거듭제곱을 곱하면 어떻게 될까요? 예를 들어

$$g(x, y, z) = x^3z - xz^2 - y^2z.$$

#### 예제 49.3.6 (초타원 곡선)

$f(x, y) = (x - x_1)(x - x_2) \cdots (x - x_{2k+1}) - y^2$ 라 하되,  $x_1, \dots, x_{2k+1}$ 은 모두 서로 다른 복소수라고 합시다.

$f$ 를 동차화하면  $g(x, y, z) = (x - x_1z)(x - x_2z) \cdots (x - x_{2k+1}z) - y^2z^{2k-1}$ 을 얻습니다. 위와 마찬가지로,  $\mathbb{CP}^2$ 에서  $g$ 의 근의 집합은 리만 곡면을 잘라내며 — 이번에도 이는 종수  $k$ 를 가집니다!

따라서 우리는 단순히  $k$ 의 값을 다르게 선택함으로써 모든 종수의 콤팩트 리만 곡면의 예를 살펴본 셈입니다.

우리가 그 곡면 자체를 "보았다"고 말하는 것은 그다지 정확하지 않습니다 — 하지만 타원 곡선을 시각화한 것과 같은 방식으로 이러한 초타원 곡선을 시각화해 볼 수 있습니다.

## §49.4 구멍 메우기

**이 절의 대표적인 예:** 리만 구면은 복소평면  $\mathbb{C}$ 에 있는 하나의 구멍을 메움으로써 형성됩니다.

이것을 작성하십시오

### §49.5 평면 곡선의 마디점

이 절의 대표적인 예: 방정식  $x^2 - y^2 = 0$ 으로 정의되는 집합은 단순 마디점을 가집니다.



# 50 미분 형식

## §50.1 $\mathbb{C}$ 위의 미분 형식

이 절에서는 경로 적분이 가능한 대상의 정의를 일반화하겠습니다.

**정의 50.1.1** ( $\mathbb{C}$  위의 미분 1-형식). 열린집합  $U \subseteq \mathbb{C}$  위의 1-형식  $\omega$ 는  $f(z)d\operatorname{Re} + g(z)d\operatorname{Im}$  꼴의 식이며, 여기서  $f(z)$ 와  $g(z)$ 는 매끄러운  $U \rightarrow \mathbb{C}$  함수입니다.

여기서 매끄럽다는 것은  $\mathbb{R}^2 \rightarrow \mathbb{R}^2$  함수로 해석했을 때 무한히 미분 가능함을 의미합니다. 이는  $\mathbb{R}^2$  위의 1-형식의 정의와 거의 동일합니다! 여기서  $\operatorname{Re}$ 와  $\operatorname{Im}$ 은 자연스러운 방식으로  $e_1^\vee$ 와  $e_2^\vee$ 의 역할을 합니다.

유일한 차이는, 보다시피  $f(z)$ 와  $g(z)$ 가 실수가 아닌 복소수를 반환한다는 점입니다 — 하지만 이는 대체로 큰 문제가 되지 않는데, 사영 원리(정리 43.2.1)에 의해 1-형식  $\omega$ 는 실숫값 1-형식의 쌍  $(\operatorname{Re}\omega, \operatorname{Im}\omega)$ 와 동치이기 때문입니다.

우리가 이렇게 하고자 하는 이유는 단순히 편의를 위한 것입니다 — 표기를 남용하여,  $z$ 를 함수  $z \mapsto z$ 라고 하면,  $dz$ 가  $z$ 의 변화량을 반환하는 1-형식이 되기를 원합니다.

## §50.2 미분 형식의 시각화

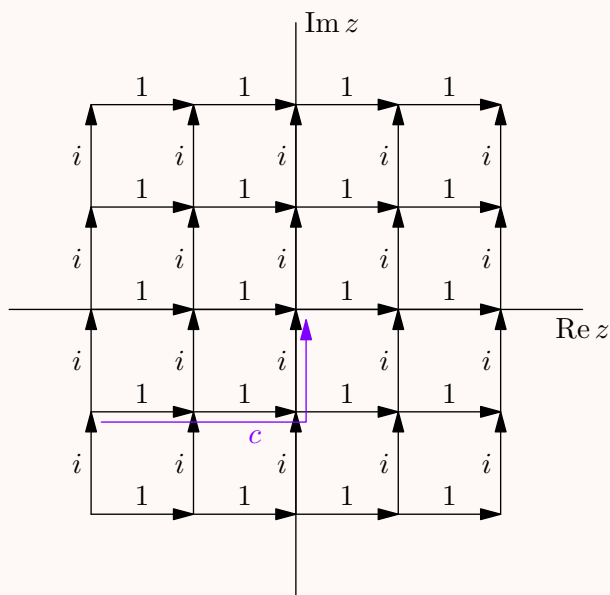
$\omega$ 는 한 점을 입력받아 점공간으로부터의  $\mathbb{R}$ -선형 사상을 반환하므로, 이를 시각화하는 자연스러운 방법은 화살표 도식(quiver diagram)을 그리는 것입니다 — 각 점에 대해, 벡터  $v$ 에 대한 값  $\omega_p(v)$ 를 표시하며, 이는 "점  $p$  근처에서  $v$  방향으로,  $v$ 의 길이와 대략 같은 길이의 곡선  $c$ 를 따라 적분하면, 그 결과는 대략 표시된 값과 같다"로 해석합니다.

미분 형식  $\omega$ 를 곡선  $c$ 를 따라 적분하려면, 도식에 나타난  $c$ 의 이동 방향에 대응하는 숫자들을 단순히 합산하면 됩니다.

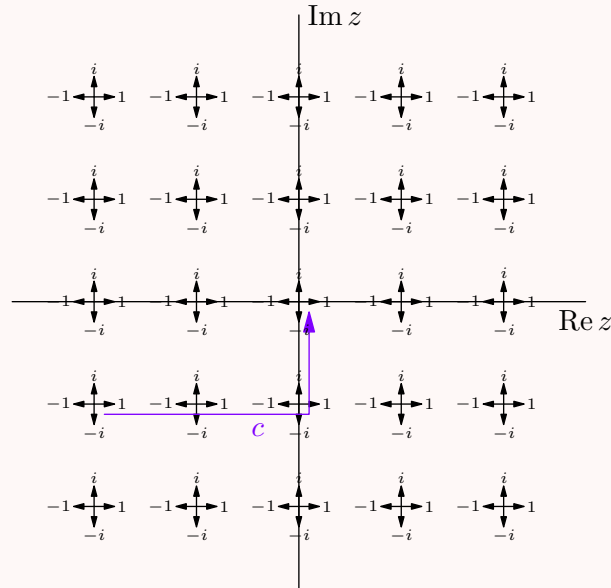
이러한 시각화를 바탕으로, 몇 가지 예를 살펴보겠습니다.

### 예제 50.2.1 (1-형식 $dz$ )

단지  $z$ 의 변화량일 뿐인  $dz$ 를 다음과 같이 시각화할 수 있습니다.

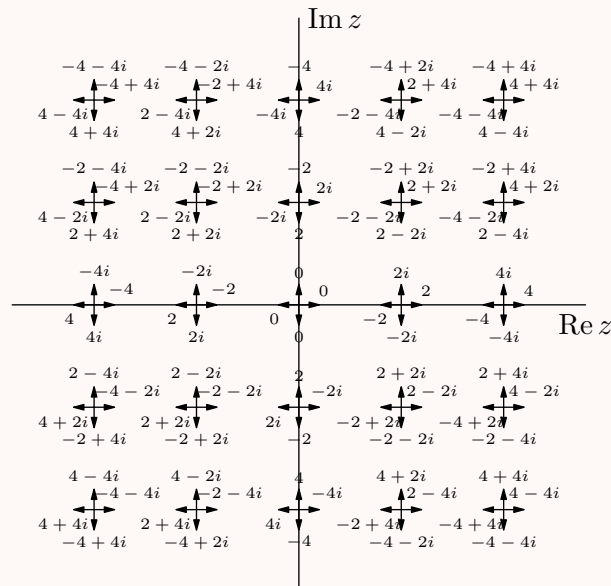


적분  $\int_C dz$ 는 벡터들의 값을 모두 더하여 계산할 수 있으며, 그 결과  $2+i$ 를 얻습니다 — 이는 실제로 곡선을 따라 이동할 때의  $z$ 의 변화량인  $0 - (-2-i) = 2+i$ 와 일치합니다. 화살표를 전체 길이만큼 늘어뜨리면 혼란스러울 수 있으므로, 다음과 같이 화살표를 짧게 표시하겠습니다.



### 예제 50.2.2 (또 다른 정칙 1-형식: $d(z^2) = 2z \cdot dz$ )

정칙 1-형식이 무엇인지 아직 정의한 적은 없지만, 만약  $f(z)$ 가 정칙이면  $df(z)$ 가 정칙 1-형식이어야 한다는 것이 그 정의가 만족해야 할 직관적으로 타당한 성질입니다. 어쨌든, 위와 같은 절차를 수행하여 점벡터들을 따라  $z^2$ 의 미분 변화량을 계산하면, 다음과 같은 결과를 얻습니다.



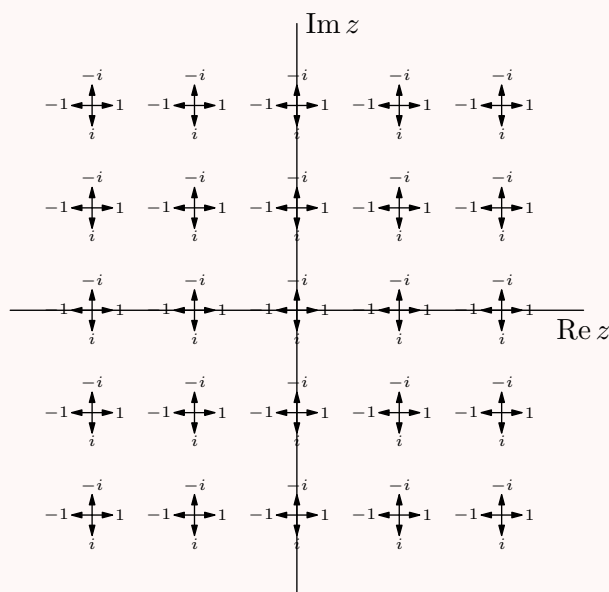
안타깝게도, 여전히 다소 복잡해 보입니다. 어쨌든, 보다시피 각 점  $z$ 에서 각 방향을 따라 1-형식  $d(z^2)$ 의 값은 1-형식  $dz$ 의 대응하는 값의  $2z$ 배이며, 따라서  $d(z^2) = 2z \cdot dz$ 가 되도록 곱셈을 정의하는 것이 타당합니다.

**예제 50.2.3 (정칙이 아닌 형식:  $d\bar{z}$ )**

위의 두 예 모두에서, 각 점  $z$ 에 대해  $\omega_z(\mathbf{e}_2) = i \cdot \omega_z(\mathbf{e}_1)$ 임을 알 수 있으며, 여기서  $\mathbf{e}_1 = (1, 0)$ 이고  $\mathbf{e}_2 = (0, 1)$ 입니다 — 다시 말해, 벡터를 반시계 방향으로 90 deg 회전시키면 미분 형식의 값에  $i$ 를 곱한 것과 같습니다.

자연스럽게 드는 의문은, 이것이 모든 1-형식의 성질인가 하는 것입니다. 결론적으로는 그렇지 않습니다. (나중에 우리는 이것이 모든 정칙 1-형식, 더 일반적으로는 모든  $(1, 0)$ 형 1-형식의 공통된 성질임을 보게 될 것입니다.)

다음 예를 생각해 봅시다:  $\omega = d\bar{z}$  라고 하면 — 이는 그저  $\bar{z}$  값의 변화일 뿐입니다.

**예제 50.2.4 (또 다른 비정칙 형식:  $\bar{z} \cdot dz$ )**

매끄러운 함수  $f(z)$ 가 복소미분가능일 때에만 정칙인 것과 마찬가지로, 매끄러운 1-형식  $\omega$ 가 그 미분  $d\omega$ 를 계산할 수 있을 때에만 정칙이 되도록 정칙 1-형식을 정의해야 합니다.

우리는 아직 2-형식을 정의하지 않았을뿐더러, 1-형식  $\omega$ 를 미분하여 2-형식으로 만든다는 것이 무엇을 의미하는지도 정의하지 않았습니다.

**§50.2.i 정칙 형식**

위의 예들을 염두에 두고, 다음과 같이 정의합니다:

**정의 50.2.5** (복소평면 위의 정칙 1-형식). 1-형식  $\omega$ 는 어떤 정칙 함수  $f$ 에 대해  $f(z) \cdot dz$ 로 쓸 수 있을 때에만 정칙입니다.

그리고 몇 가지 다른 유형들도 있습니다.

**정의 50.2.6** (유형  $(1, 0)$ 과 유형  $(0, 1)$ 의 1-형식). 1-형식은 매끄러운  $f$ 에 대해 국소적으로  $f(z)dz$ 의 형태일 때 **유형  $(1, 0)$** 입니다. 마찬가지로, 1-형식은 매끄러운  $f$ 에 대해 국소적으로  $f(z)d\bar{z}$ 의 형태일 때 **유형  $(0, 1)$** 입니다.

**예제 50.2.7 (몇 가지 유형  $(1, 0)$ 의 1-형식)**

위의 예들을 살펴봅시다:

- 정칙 형식인  $dz$ 나  $2z \cdot dz$ 는 당연히 유형  $(1, 0)$ 입니다.
- $\bar{z} \cdot dz$ 는 정칙은 아니지만 여전히 유형  $(1, 0)$  형식입니다.
- 그러나  $d\bar{z}$ 는 유형  $(1, 0)$  형식이 아닙니다.

왜 이것이 중요할까요? 위의 정의가 잘 정의되어 있다는 것은 자명하지 않다는 점에 주목하십시오 — 이는 정칙 함수가 모든 방향을 동일한 양만큼 스케일링하기 때문에 성립하는 것입니다!

직관적으로,

$(1, 0)$  형식  $\omega$ 는  $\omega_p(\mathbf{e}_2) = \omega_p(\mathbf{e}_1) \cdot i$ 를 만족하는 형식입니다.

### §50.2.ii 조각들을 종합하여: 리만 곡면 위의 1-형식

놀랍지 않게도, 이제 우리는 리만 곡면 위에서 1-형식을 정의할 수 있습니다.

이것을 작성합니다

# 51 리만-로흐 정리

## §51.1 동기

복소해석학의 기본적인 사실을 상기해 봅시다:

정칙  $\mathbb{C} \rightarrow \mathbb{C}$  함수는 원점에서의 테일러 급수 전개에 의해 유일하게 결정됩니다.

실수 매끄러운 함수의 경우와 비교하면, 이는 이미 매우 강한 제약입니다 — 원점의 작은 근방에서의 함수값이 모든 곳에서의 함수값을 결정합니다 — 하지만 함수를 명시하려면 여전히 무한히 많은 좌표가 필요합니다!

한편, 리우빌 정리가 있습니다:

유계인 정칙  $\mathbb{C} \rightarrow \mathbb{C}$  함수는 상수입니다.

앞서 배웠듯이, 이 정리를 리만 곡면의 관점에서 서술하면 다음과 같이 더 우아하게 다시 쓸 수 있습니다:

정칙  $\mathbb{C}_\infty \rightarrow \mathbb{C}$  함수는 상수입니다.

다시 말해, 정칙  $\mathbb{C}_\infty \rightarrow \mathbb{C}$  함수를 명시하려면 복소수 하나만 있으면 됩니다! 즉,  $\mathbb{C}$ -벡터 공간  $\text{Hom}(\mathbb{C}_\infty, \mathbb{C})$ 의 차원은 1입니다.

당연히, "그 사이에 무언가가 있는가"라고 물을 수 있습니다. 있습니다! 그리고 리만-로흐 정리는 이러한 것들이 어떻게 작동하는지 이해하기 위한 핵심 재료입니다.

그렇다면, 이를 어떻게 정의할 것인가? 위의 두 상황을 비교해 보면, 정칙  $\mathbb{C} \rightarrow \mathbb{C}$  함수는 유리형  $\mathbb{C}_\infty \rightarrow \mathbb{C}$  함수이되,  $\infty$ 에서만 극을 가질 수 있고 다른 곳에서는 가질 수 없는 함수입니다.

그러므로,

"임의 차수의 극을 허용함"과 "반드시 정칙이어야 함" 사이를 매끄럽게 보간함으로써, 여러 흥미로운 함수 공간을 만들어 낼 수 있습니다.

편리하게도, 앞서 장 32에서 우리는 영점의 **중복도**와 유리형 함수의 극의 **차수**를 정의한 바 있습니다. 따라서 이 두 극단 사이의 자연스러운 지점은 차수가 최대  $d$ 인 극을 허용하는 것입니다.

표기의 편의를 위해 다음과 같이 정의합니다:

**정의 51.1.1** (유리형 함수의 차수).  $f$ 가  $p$ 에서 유리형이라고 합시다.  $\text{ord}_p(f)$ 를 다음과 같이 정의합니다:

- $f$ 가  $p$ 에서 중복도  $d$ 인 영점을 가지면  $d$ ;
- $f$ 가  $p$ 에서 차수  $d$ 인 극을 가지면  $-d$ ;
- 그 외의 경우 0.

**예제 51.1.2** ( $\mathbb{C}_\infty$  위에서 차수가 최대 4인 극을 갖는 함수들의 공간)

$L(4 \cdot \infty)$ 를  $\infty$ 를 제외한 모든 곳에서 정칙이고  $\infty$ 에서 차수가 최대 4인 극을 갖는 유

리형  $\mathbb{C}_\infty \rightarrow \mathbb{C}$  함수들의 집합이라고 합시다 — 다시 말해,

$$L(4 \cdot \infty) = \{\mathbb{C}_\infty \text{ 위에서 유리형인 } f \mid \mathbb{C}_\infty \setminus \{\infty\} \text{ 위에서 정의된 } f, \text{ord}_\infty(f) \geq -4\}.$$

(표기  $L(-)$ 는 나중에 설명하겠습니다.)

당연히, 이는 자연스러운  $\mathbb{C}$ -벡터 공간을 이룹니다.

원점에서 임의의  $f \in L(4 \cdot \infty)$ 의 테일러 급수를 생각해 봅시다:

$$f(z) = \frac{c_{-m}}{z^m} + \frac{c_{-m+1}}{z^{m-1}} + \cdots + \frac{c_{-1}}{z} + c_0 + c_1 z + \cdots$$

당연히,  $f$ 가 원점에서 정의되므로  $m > 0$ 에 대해 0이 아닌 계수  $c_{-m}$ 을 가질 수 없습니다. 하지만 더 중요한 것은,  $m > 4$ 에 대해서도 0이 아닌 계수  $c_m$ 을 가질 수 없다는 점입니다!<sup>a</sup>

여기서 무슨 일이 일어났는지 보셨습니까? 우리는 함수가 해석적이면서 너무 심하게 발산하지 않아야 한다는 요구에서 출발했지만, 결국 순전히 대수적인 함수 — 즉 다항식에 도달하게 되었습니다!

특히,  $L(4 \cdot \infty)$ 는 차수가  $\leq 4$ 인 다항식들로 이루어지며,

$$\dim L(4 \cdot \infty) = 5$$

$\mathbb{C}$ -벡터 공간으로서 그러합니다.

<sup>a</sup>그 이유는 사실 그리 간단하지 않지만, 스스로 확인해 볼 수 있습니다: 0이 아닌 항이 유한 개만 있다면,  $\infty$ 에서의 극의 위수 ( $-\text{ord}_\infty(f)$ )는 정확히 0이 아닌 최고차 계수의 차수가 됩니다.

### 예제 51.1.3 (더 복잡한 $L(-)$ 공간)

$\infty$ 에서 발산하는 함수만을 고려할 이유는 없습니다 — 앞으로 보게 되겠지만, 극의 위수를 제한하는 한, 더 일반적인 유리형 함수도 고려할 수 있습니다.

$L(-1 \cdot 3 + 4 \cdot i + 5 \cdot \infty)$ 를 다음 조건을 만족하는 유리형 함수  $f: \mathbb{C}_\infty \rightarrow \mathbb{C}$ 들의 집합이라고 합시다:

- $\mathbb{C}_\infty$ 의 모든 곳에서 정칙이되, 점 3,  $i$ ,  $\infty$ 에서는 예외일 수 있습니다;
- 3에서는 위수가  $\geq 1$ 인 근을 가져야 합니다;
- $i$ 에서는 위수가 4를 넘는 극을 가질 수 없습니다;
- $\infty$ 에서는 위수가 5를 넘는 극을 가질 수 없습니다.

그러므로, 예를 들어  $(z \mapsto z - 3)$ ,  $(z \mapsto \frac{(z-3)^3}{(z-i)^2})$ , 또는  $(z \mapsto (z-3)^4)$ 는 이 집합에 속하는 함수이지만,  $(z \mapsto (z-3)^2 + 1)$ 이나  $(z \mapsto (z-3)^7)$ 은 그렇지 않습니다. 앞서와 마찬가지로, 이것 역시  $\mathbb{C}$ -벡터 공간이며, 나아가 유한 차원이기도 합니다! 그 차원은 얼마여야 할까요?

자, 함수  $f \in L(-1 \cdot 3 + 4 \cdot i + 3 \cdot \infty)$ 와 함수  $g \in L(-1 \cdot 3 + 7 \cdot \infty)$  사이에 1-1 전단사가 다음과 같이 존재함을 주목하십시오.

$$g = \Phi(f) = (z \mapsto f(z) \cdot (z-i)^4),$$

여기서, 이제쯤 아마 짐작하셨겠지만,  $L(-1 \cdot 3 + 7 \cdot \infty)$ 는 3에서 적어도 하나의 영점을 가지고  $\infty$ 에서 많아야 위수 7의 극을 가지는 유리형 함수들의 공간입니다.

이 정보를 이용하면, 그 차원이 7이어야 함을 이해하는 것은 그리 어렵지 않을 것입니다.

또 다른 동기 부여로: 이후에 우리는 **인자**(divisor)와 **선다발**(line bundle)이라는 개념도 정의할 것입니다. 만약 대수기하학의 맥락에서 이 개념들을 배운 적이 있다면, 이것들이 실제로 무엇에 관한 것인지 알게 되는 것이 흥미로울 수 있습니다; 그렇지 않더라도, 이러한 정리들이 완전히 대수적인 설정으로 자연스럽게 일반화될 수 있다는 것, 그리고 해석적 다양체의 경우에서 얻은 직관이 거의 그대로 통한다는 것은 여전히 매우 놀라운 사실입니다 — 실제로,  $\mathbb{Q}[\sqrt{2}]$ 와 같은 수체의 종수(genus)까지도 정의할 수 있습니다!

## §51.2 인자

**이 절의 대표적인 예:**  $(-3) \cdot i + (-4) \cdot \infty$ 는  $\mathbb{C}_\infty$  위의 인자입니다.

위의 개념들에 대해 편리한 표기법을 정의하는 것으로 시작해 봅시다.

먼저, “ $f$ 는 원점에서 위수가 많아야 4인 영점을 가져야 한다”는 조건이 다음과 같이 편리하게 쓰일 수 있음을 관찰하십시오

$$z^4 \mid f.$$

다시 말해,  $z^4$ 는  $f$ 의 **인자**여야 합니다.

$f$ 가 다항식인 경우 이 표기법은 작동하는데, 두 다항식이 서로를 나눈다는 것이 무엇을 의미하는지는 이미 알고 있기 때문입니다.

일반화하면, “ $f$ 는 점  $i$ 에서 차수가 3보다 큰 극을 가질 수 없고,  $f$ 는 점  $\infty$ 에서 차수가 4보다 큰 극을 가질 수 없다”라고 다음과 같이 말할 수 있습니다.

$$(z - i)^{-3} \cdot (z - \infty)^{-4} \mid f.$$

물론 이 시점에서 이 표기법은 순전히 형식적인 것으로, 예를 들어 식  $(z - \infty)$ 에 부여할 수 있는 “함수”로서의 해석은 존재하지 않습니다.

이러한 대상들은 적절하게도 **제수**(divisor)라고 불립니다. 그러면 이제 형식적 정의로 들어가 봅시다:

**정의 51.2.1 (제수).**  $X$ 를 리만 다양체라고 합시다. 그러면  $X$  위의 제수  $D$ 는 함수  $D: X \rightarrow \mathbb{Z}$ 로서, 점들의 이산 집합 위에서만 0이 아닌 값을 가집니다.

위의 형식적 대상  $(z - i)^{-3} \cdot (z - \infty)^{-4}$ 를 이제부터는 다음과 같이 함수  $D: \mathbb{C}_\infty \rightarrow \mathbb{Z}$ 로 간주하겠습니다.

$$D(z) = \begin{cases} -3 & z = i \\ -4 & z = \infty \\ 0 & \text{그렇지 않으면.} \end{cases}$$

**표기의 남용 51.2.2.** 점  $p \in X$ 에 대해,  $p$ 에서 값 1을 취하고 그 외의 곳에서는 0을 취하는 제수를 나타내기 위해  $p$ 라고 씁니다.

제수는 정수값 함수이므로, 두 제수를 더하거나 제수에 정수를 곱할 수 있으며, 그 결과는 정수가 됩니다. 따라서,

**예제 51.2.3 (제수로서의  $(z - i)^{-3} \cdot (z - \infty)^{-4}$ )**

위의 형식적 대상  $(z - i)^{-3} \cdot (z - \infty)^{-4}$ 에 대응하는 제수  $D$ 는  $(-3) \cdot i + (-4) \cdot \infty$ 로 쓸 수 있습니다.

### §51.3 제수의 차수

**이 절의 대표적인 예:**  $\deg((-3) \cdot i + (-4) \cdot \infty) = -7$ .

곡면  $X$ 가 콤팩트하다면, 점들의 임의의 이산 집합은 유한합니다. 따라서  $X$  위의 제수  $D$ 는 유한한 지지집합을 가집니다.

이로써 제수의 차수를 정의할 수 있습니다:

**정의 51.3.1** (제수의 차수). 콤팩트 곡면  $X$  위의 제수  $D$ 에 대해, 그 차수는  $\sum_{p \in X} D(p)$ 입니다.

물론 유한 개의 항만이 0이 아니므로 이 합은 잘 정의됩니다.

### §51.4 유리형 함수의 주인자(principal divisor)

**이 절의 대표적인 예:**  $\operatorname{div} \frac{(z-3)^2}{z-i} = 2 \cdot 3 + (-1) \cdot i + (-1) \cdot \infty$  는 차수 0을 갖습니다.

인자(divisor)를 정의한 후, 앞서 인자가 함수를 “나눈다”라고 했던 모호한 표현을 형식화할 편리한 표기법을 원합니다.

**정의 51.4.1** (유리형 함수의 인자(divisor)).  $f$ 를 리만 곡면  $X$  위의 유리형 함수라고 합시다. 그러면  $f$ 의 제수  $\operatorname{div}(f)$ 는 다음과 같습니다.

$$\operatorname{div}(f)(p) = \operatorname{ord}_p(f).$$

이를 형식적인 합으로도 쓸 수 있습니다:  $\operatorname{div}(f) = \sum_p \operatorname{ord}_p(f) \cdot p$  — 위에서의 표기법 남용에 의해,  $f$ 가 유한 개의 근과 극을 가진다면 이는 실제 합이 될 것입니다.

어떤 제수  $D$ 가 어떤  $f$ 에 대해  $\operatorname{div}(f)$ 와 같다면,  $D$ 를 **주제수(principal divisor)**라고 부릅니다. (이를 하나의 원소로 생성되는 아이디얼인 주 아이디얼과 비교해 보십시오!)

이 절의 대표적인 예시를 살펴보면, 리만 구에 대해 다음을 추측했을 수도 있습니다. 실제로는 훨씬 더 많은 것이 성립합니다:

#### 명제 51.4.2

콤팩트 곡면  $X$  위의 인자  $D$ 가 주인자(principal)라면,  $\deg D = 0$ 입니다.

극이 유계인 함수들의 공간을 다루기 위한 편리한 표기법을 정의한다는 목표를 잊지 맙시다. 위에서 정의한 표기법을 사용하면,  $f = z$ 일 때  $\operatorname{div} f = 1 \cdot 0 + (-1) \cdot \infty$ 이며, 우리는  $f$ 가 인자  $(-1) \cdot \infty$ 를 “나눈다”고 말하고 싶습니다. 자연스러운 정의는 다음과 같을 것입니다:

**정의 51.4.3** (인자의 부분 순서). 모든  $p \in X$ 에 대해  $D(p) \geq 0$ 이면  $D \geq 0$ 이라고 씁니다. 두 인자  $D_1$ 과  $D_2$ 에 대해,  $D_1 - D_2 \geq 0$ 이면  $D_1 \geq D_2$ 라고 씁니다.

그리고 마지막으로,

**정의 51.4.4.**  $D$ 를 리만 곡면  $X$  위의 인자라고 합시다. 그러면 극이  $D$ 로 유계인 유리형 함수들의 공간은 다음과 같습니다

$$L(D) = \{X \text{ 위에서 유리형인 } f \mid \operatorname{div}(f) \geq -D\}.$$

**연습문제 51.4.5.** 이 연습문제는 여러분이 표기법에 익숙해지도록 하기 위한 것입니다. 다음을 보이십시오:

- 두 인자  $D_1 \leq D_2$ 에 대해,  $L(D_1) \subseteq L(D_2)$ 입니다.

- $X$ 가 콤팩트이면,  $L(0) \cong \mathbb{C}$ 입니다.
- $X$ 가 콤팩트이고  $\deg D < 0$ 이면,  $L(D) = \{0\}$ 입니다.

## §51.5 리만-로흐 정리

표준 인자  
(canonical  
divisor)를 설  
명하십시오

### 정리 51.5.1 (리만-로흐 정리)

$D$ 를 종수(genus)  $g$ 인 대수 곡선  $X$  위의 인자라 하고,  $K$ 를  $X$  위의 표준 인자(canonical divisor)라고 합시다. 그러면

$$\dim L(D) - \dim L(K - D) = \deg(D) + 1 - g.$$

몇 가지 응용  
을 나열하십  
시오



# 52 선다발

## §52.1 개요

선다발에 대해 들어보셨을 수도 있는데, 이는 어떤 식으로든 “각 점의 원상이 하나의 직선이 되는 사상  $\pi: L \rightarrow X$ 를 갖춘 집합  $L$ ”을 의미합니다. 그리고 대수기하학 절에서, 단지 함수처럼 보이는 “절단”이라는 개념을 마주치게 됩니다.

그렇듯하게 들리지만, “그래서 뭐 어떻다는 것인가? 그렇다면 이는  $X$ 보다 차원이 하나 더 많은 또 다른 복소다양체에 불과한 것 아닌가? 그냥 복소다양체를 공부하면 안 되는 것인가?”라고 물으실 수도 있습니다.

사실이긴 하지만, 선다발에는 더 많은 구조가 있습니다:

- 두 선다발의 곱을 취할 수 있는데, 이는 어떤 식으로든 두 선다발의 “뒤틀림을 더하는” 것입니다.
- 단면은 단순한 함수가 아닙니다 — “그래프 용지” 자체가 평평한 특수한 경우에는 단면을 함수의 그래프로 생각할 수 있지만, 만약 그것이 뫼비우스(Möbius) 띠처럼 휘어져 있다면, “그래프 용지”의 각 점에 “함숫값”을 대응시킬 방법이 없다는 것을 알게 될 것입니다 — 이러한 상황을 우리는 “선다발이 자명하지 않다”라고 부를 것입니다.

다시 말해, 선다발은 “함수의 그래프의 공간”을 크게 일반화한 것입니다.

나중에는 선다발과 인자의 선형 동치류 사이의 깊이 숨겨진 연관성을 보게 될 것이고, 그것들이 어떻게 모두 이른바 피카르 군을 통해 연결되는지 보게 될 것입니다.

## §52.2 정의

$X$ 를 리만 곡면이라 합시다.

이 절에서는  $X$ 를 단지 곡선으로 — 즉 2차원 대상이 아니라 1차원 대상으로 — 보겠습니다. 왜냐하면:

- 3차원 공간에 매장될 수 있는 대상은 시각화하기가 더 쉽기 때문입니다. (실수부와 허수부를 모두 가진 ...의 그래프를 그려보십시오, 그러면 제가 무슨 말을 하는지 아시게 될 것입니다!)
- 우리가 관심을 갖는 모든 함수는 해석적이므로, 함수의 다른 곳에서의 거동은 실수축 위에서의 값에 의해 결정됩니다.

그러나 실수부만 보면 직관을 놓치는 경우가 있습니다 — 예를 들어, 원  $x^2 + y^2 = 1$ 과 쌍곡선  $x^2 = 1 + y^2$ 이  $\mathbb{C}^2$ 에서 같은 모양의 리만 곡면을 잘라낸다는 것을 간과하기 쉽고, 함수  $\frac{1}{x^2+1}$ 이  $x = \pm i$ 에서 극을 갖는다는 것도 간과하기 쉽습니다. 그러니 주의하십시오.

**정의 52.2.1. 선다발**  $L$ 은 다음을 함께 갖춘 집합입니다:

- 사상 사상  $\pi: L \rightarrow X$ ,
- $X$ 의 열린 덮개  $\{U_i\}$ ,
- 각  $U_i$ 에 대해,  $\pi^{-1}(p)$ 의 각 점을  $\mathbb{C} \times p$ 의 한 점으로 전단사적으로 대응시키는 **선다발 차트**  $\phi: \pi^{-1}(U) \rightarrow \mathbb{C} \times U$ ,
- 두 열린집합  $U_1$ 과  $U_2$ 에 대해, **전이 함수**  $\phi_2 \circ \phi_1^{-1}: \mathbb{C} \times U_1 \rightarrow \mathbb{C} \times U_2$ 는 각 점  $p \in U_1 \times U_2$ 에 대해  $\mathbb{C} \times p \rightarrow \mathbb{C} \times p$ 로 제한했을 때  $\mathbb{C}$ -벡터 공간 동형사상이어야 하며, 그 비례계수는  $U$  위에서 해석적 함수여야 합니다.

**비고 52.2.2 (주의)** — 보통 우리는 함수  $f(x)$ 의 그래프를  $y = f(x)$ 인 점  $(x, y)$ 들의 집합으로 그립니다.

이번에는 [Mi95]의 표기법을 사용합니다 — 선다발 차트의 목표 공간이  $U \times \mathbb{C}$ 가 아니라  $\mathbb{C} \times U$ 입니다 — 그러므로 절단을 함수의 일반화로 본다면, 좌표는 대신  $(y, x)$ 처럼 보일 것입니다.

이 정의는 압축적이지만, 본질적으로는 다음과 같습니다:

**선다발(line bundle)은 해석적 구조와 1차원 벡터 공간 구조로 이루어진 선다발 구조를 갖춘 집합입니다.**

전이 사상(transition map)은 [장 47](#)에서 리만 곡면의 조각들을 이어 붙였던 것과 마찬가지로, 단순히 선다발의 조각들을 이어 붙이는 것입니다.

또 다른 정의도 있는데, 이것은 나중에 설명하겠습니다.

**정의 52.2.3 (선다발의 절단).**  $L$ 을 선다발이라 합시다. 열린집합  $U$  위의 **절단**(section)이란  $\pi \circ f$ 가  $U$  위의 항등 사상이 되는 사상  $f: U \rightarrow L$ 을 말합니다.

절단  $f: X \rightarrow L$ 을 **전역 절단**(global section)이라 부릅니다.

절단  $f: U \rightarrow L$ 이 **해석적 절단**(analytic section)이라는 것은, 선다발 도표  $\phi: \pi^{-1}(U_1) \rightarrow \mathbb{C} \times U_1$ 가 존재하는 모든  $U_1 \subseteq U$ 에 대해  $\phi \circ f|_{U_1}: U_1 \rightarrow \mathbb{C} \times U_1$ 가 해석적임을 의미합니다.

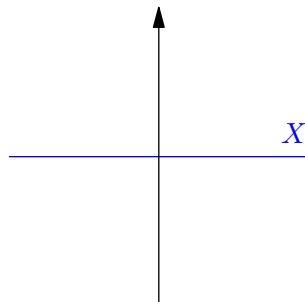
이 정의는 대수기하학, [정의 82.2.2](#)에서 나중에 다시 보게 될 것입니다.

**비고 52.2.4** — 대부분의 책에서는 먼저 층(sheaf)이 무엇인지 정의한 다음, "해석적 절단" 대신 "해석적 함수 층의 절단"(또는 정칙 함수 등)이라고 말합니다.

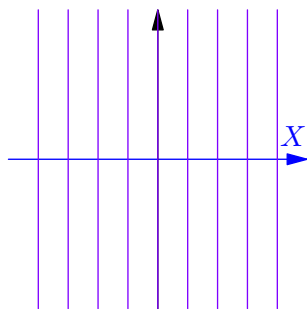
## §52.3 선다발 시각화하기

리만 구  $\mathbb{C}_\infty$ 의 모든 정보를, 구를 시각화하는 것만으로 (표면 위의 어떤 "호환되는 격자"로 해석적 구조를 바라보면서) 한꺼번에 머릿속에 담아둘 수 있는 것처럼, 적어도 가장 단순한 경우에는 선다발의 모든 정보도 한꺼번에 머릿속에 담아둘 수 있어야 합니다.

먼저,  $X = \mathbb{C}$ 일 때  $\mathbb{C} \times X$ 를 시각화해봅시다. 실수부만 살펴보면, 이는 평면처럼 보입니다.

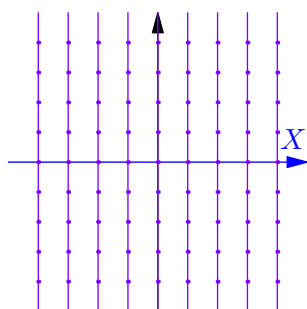


선다발로서, 각 점의 원상은 하나의 직선입니다.

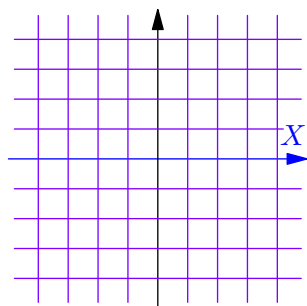


**질문 52.3.1.** 기호로 나타내면, 수직선은  $\mathbb{C} \times X$ 의 어떤 부분집합에 대응합니까?

그런데 이들은 단순히 서로 무관한 직선들이 아닙니다 — 두 가지 구조가 더 있습니다. 첫 번째는 벡터 공간 구조입니다 — 물론  $\mathbb{C}$ -벡터 공간으로서  $\mathbb{C}$ 의 차원은 1입니다. 우리는 직선 위에  $1, 2, 3, \dots$ 인 점들을 표시함으로써 이를 시각화할 수 있습니다.

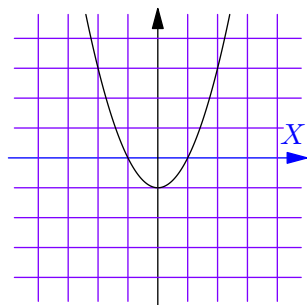


다른 구조는  $p$ 가  $X$  위를 변화함에 따라 직선들이 "매끄럽게 변화"해야 한다는 것입니다. 우리는 이를, 그렇습니다, 격자를 그림으로써 시각화합니다.



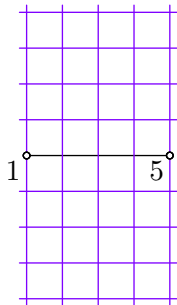
**질문 52.3.2.** 격자 그림은 선다발 도표의 형식적 정의와 어떻게 대응합니까? (힌트: 선다발 도표  $\phi: L \rightarrow \mathbb{C} \times U$  (여기서  $U \subseteq X$ )에 대해 수직선  $x = c$ 와 수평선  $y = c$ 의 원상을 취한 다음,  $X$  위의 해석적 구조를 사용하여  $U$ 의 열린 부분집합을  $\mathbb{C}$ 의 열린 부분집합과 동일시하십시오.)

지금까지는 놀라운 것이 없습니다 — 이는 그저 보통의 격자 그래프이며, 여기에  $y = x^2 - 1$ 과 같은 함수를 그릴 수 있고, 함수가 격자에 대해 해석적이면 그 함수는 해석적입니다.

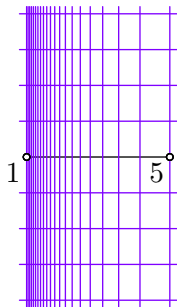


물론, 함수 대신 이것을 절단이라고 부릅니다. 이 특정한 절단은 예상하시는 대로 실제로 해석적입니다.

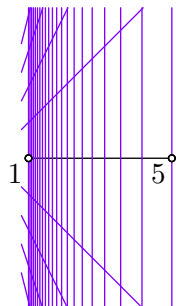
어떤 "격자"들이 동일한 선다발 구조를 나타내는지 살펴봅시다. 이 부분에서는  $\{z \in \mathbb{C} \mid |z - 3| < 2\}$ 를 살펴볼 것이며, 그 실수부는  $(1, 5)$ 입니다.



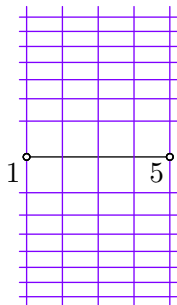
선분  $(1, 5)$  위에 해석적 재매개변수화를 적용한다면 — 예를 들어  $t = 25/x$ 라 두면, 격자는 다음과 같이 됩니다. 이는 여전히 동일한 선다발 구조를 나타냅니다 — 다시 말해, 두 도표는 서로 호환됩니다.



해석적으로 변화하는 함수로 수직 방향을 재조정하더라도, 이는 여전히 동일한 선다발 구조를 나타냅니다.



그러나 선형이 아닌 무언가로 수직 방향을 재조정하면, 벡터 공간 구조가 바뀌게 됩니다. 다음 격자는 동일한 선다발 구조를 나타내지 않습니다:



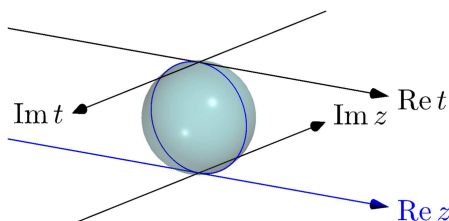
직관적으로 이는 타당합니다 — 벡터 공간에서는 두 원소를 더하여 또 다른 원소를 얻을 수 있습니다 — 우리의 경우,  $a, b \in L$ 이고  $\pi(a) = \pi(b)$ 라면,  $c = a + b$ 를 계산하여  $\pi(c) = \pi(a) = \pi(b)$ 인 또 다른 원소  $c \in L$ 을 얻을 수 있습니다. 수직 방향을 비선형적으로 재조정하면, 원소  $c$ 가 바뀌게 됩니다.

마지막으로,  $L$ 이 여전히 해석적 구조를 가지고 있다는 것을 잊지 마십시오 — 단면이 반드시 함수일 필요는 없지만, 우리는 여전히 단면이 언제 해석적인지 말할 수 있습니다.

**질문 52.3.3.** 위에서 설명한 모든 것이 형식적 정의와 일치하는지 확인하십시오. (이것은 중요합니다! 흐릿한 그림은 개념을 이해하는 데 도움이 되지 않으며, 여러분의 직관이 불완전하거나 부정확하다면 이후 부분을 이해하는 데 큰 어려움을 겪게 될 것입니다.)

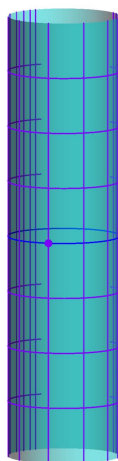
지금까지는 모든 것이 그저 모눈종이처럼 보였고, 그 위에서 단면은 마치 함수처럼 보였습니다.<sup>1</sup> 좀 더 복잡한 공간  $X$  — 리만 구를 생각해 봅시다.

우리는 실수부만을 보고 있으므로, 다시 한번  $\mathbb{C}_\infty$ 는 그저 원처럼 보입니다.



이전처럼, 곡면 위의 점들을 매개변수화하기 위해  $z$ 와  $t$ 를 두며, 둘 다 정의되는 곳에서는  $t = \frac{1}{z}$ 입니다.

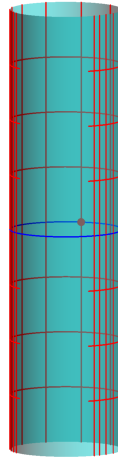
그럼에도 원을 매립하려면 2차원이 필요합니다. 따라서  $\mathbb{C} \times \mathbb{C}_\infty$ 의 실수부는 다음과 같이 보일 수 있습니다:



격자선이 그려져 있고, 원점  $z = 0$ 은 점으로 표시되어 있습니다. 세로선은  $z = 0$ ,  $z = \frac{1}{2}$ ,  $z = 1$ ,  $z = \frac{3}{2}$ , ...의 위치를 나타냅니다.

반대편에서는 다음과 같은 모습을 볼 수 있습니다. 세로선은  $t = 0$ ,  $t = \frac{1}{2}$ ,  $t = 1$ ,  $t = \frac{3}{2}$ , ...의 위치를 나타냅니다.

<sup>1</sup>위에서 경고했듯이, "그래프 좌표"는  $(y, x)$ 로 씁니다.

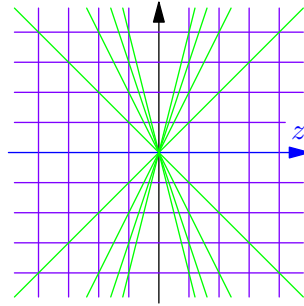


**질문 52.3.4.** 0도  $\infty$ 도 포함하지 않는 임의의 열린집합  $U \subseteq \mathbb{C}_\infty$ 에 대해,  $\mathbb{C} \times U$  위에서 위의 두 선다발 좌표계가 동일한 선다발 구조를 정의함을 확인하십시오. (전이 함수는 무엇입니까?)

이렇게 해서, 우리는 소위 자명한 선다발  $\mathbb{C} \times \mathbb{C}_\infty$ 를 갖게 됩니다.

약속했던 대로, 여기에는 자명하지 않은 선다발도 존재합니다.

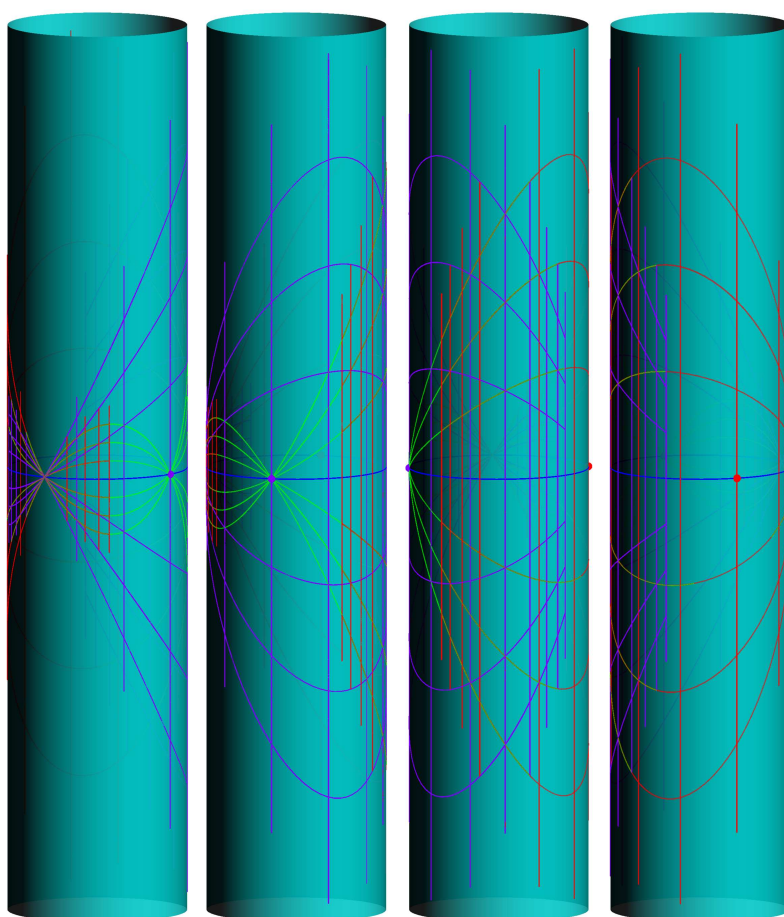
먼저, 위 절에서 다음을 상기하십시오: 0도  $\infty$ 도 포함하지 않는 임의의 열린집합  $U$  위에서, 세로 방향을  $z$ 배로 스케일링하는 또 다른 선다발 좌표계를 생각할 수 있으며, 이는  $U$  위에서 동일한 선다발 구조를 유도합니다.



**질문 52.3.5.**  $\phi_p$ 와  $\phi_g$ 를 각각 보라색 격자와 초록색 격자에 대응하는 선다발 좌표계라 합시다.  $q \in L$ 인 점이  $z \notin \{0, \infty\}$ 에 대해  $\phi_p(q) = (y, z)$ 를 만족한다면,  $\phi_g(q) = (\frac{y}{z}, z)$ 가 됨을 확인하십시오.

이제 — 위의 자명한 선다발  $\mathbb{C} \times \mathbb{C}_\infty$ 는 두 조각을 용접하여, 각  $y$ 에 대해 보라색 선  $(y, z)$ 가 빨간색 선  $(y, t)$ 에 용접되도록 한 것으로 볼 수 있음에 주목하십시오. 그러나 우리가 그 특정한 용접 방식에 제한될 이유는 전혀 없습니다 — 이번에는, 각  $y$ 에 대해 초록색 선  $(\frac{y}{z}, z)$ 를 빨간색 선  $(y, t)$ 에 용접해 보겠습니다.

그 결과물은 다음과 같이 보일 것입니다. 상당히 복잡해 보이므로, 이번에는 4개의 시점을 보여드립니다.



이번에 원기둥은 오직 예시를 위한 것입니다. 무슨 일이 일어나고 있는지 살펴봅시다.

- 먼저, 보라색 점과 빨간색 점 근처에서는 그래프 선들이 우리에게 익숙한 상황처럼 보입니다.

$t = \frac{1}{z}$ 이기 때문에, 바깥에서 볼 때 빨간색 좌표선들은 뒤집힌 것처럼 보일 것임에 주목하십시오.

- 양의 쪽( $z > 0$ 이고  $t > 0$ )에서는 문제가 없습니다 — 그림에 나타난 대로, 보라색 선들을 더 가깝게 밀착시키기만 하면 됩니다.

- 그러나 음의 쪽에서는 — 초록색 선  $(\frac{y}{z}, z)$ 가  $y$ 가 증가할 때 아래쪽으로 움직임에 주목하십시오, 따라서 그것이 위로 가도록 하려면 "모눈종이를 비틀" 필요가 있습니다.

그림에서는 이것이 모든 가로선들이 교차하는 특이점으로 묘사되어 있지만, 실제로는 우리가 "모눈종이"를 180도로 비틀어서 다른 부분에 용접하는 것으로 생각해야 합니다.

이것이 바로 Möbius 띠입니다!

따라서, "동형"이 무엇을 의미하든 간에, 이 선다발이 자명한 것과 동형이 아니라는 것은 분명해 보입니다.

**질문 52.3.6.** 위에서 한 작업이  $y, z, t$ 가 실수가 아닐 때도 성립하는지 확인하십시오 — 특히,  $\mathbb{R} \setminus \{0\}$ 와 달리  $\mathbb{C} \setminus \{0\}$ 는 연결 집합입니다. 이번에는 아마 "그래프 용지"를 시각화할 수 없을 것입니다 (4차원이기 때문입니다!). 따라서 직관은 실수부에 국한시키고 나머지는 대수를 이용해야 합니다.

## §52.4 선다발 사이의 사상

두 선다발이 동형이라는 것이 무엇을 의미하는지 형식적으로 정의하려면, 사상을 정의할 수 있어야 합니다. 이는 정확히 예상하시는 바와 같습니다 — 즉  $L_1$ 과  $L_2$  위의 선다발 구조(즉 벡터 공간 구조와 해석적 구조)를 보존해야 합니다.

**정의 52.4.1.**  $\pi_1: L_1 \rightarrow X$ 와  $\pi_2: L_2 \rightarrow X$ 를 선다발이라 합시다. 선다발 사상  $\alpha: L_1 \rightarrow L_2$ 는 다음을 만족하는 집합 사상입니다:

- $\pi_2 \circ \alpha = \pi_1$  이고,
- $\phi_1: \pi_1^{-1}(U_1) \rightarrow \mathbb{C} \times U_1$ 와  $\phi_2: \pi_2^{-1}(U_2) \rightarrow \mathbb{C} \times U_2$ 가 선다발 차트라면, 그 합성이

$$\phi_2 \circ \alpha \circ \phi_1^{-1}: \mathbb{C} \times (U_1 \cap U_2) \rightarrow \mathbb{C} \times (U_1 \cap U_2)$$

$(s, p) \mapsto (f(p) \cdot s, p)$ 의 형태를 가지며, 여기서  $f$ 는  $U_1 \cap U_2$  위에서 정칙입니다.

**연습문제 52.4.2.** 위의 함수  $f(p)$ 는 모든  $p \in U_1 \cap U_2$ 에 대해 0이 아니어야 합니다. 왜 그럴까요? (힌트:  $\phi_1$ 과  $\phi_2$ 의 역할을 바꾸어 함수를 뒤집어 보십시오.)

**질문 52.4.3.** 위의 정의가 다음과 동치임을 확인하십시오:  $\alpha$ 가 선다발 사상인 것은 다음과 동치입니다

- 점  $q \in \pi_1^{-1}(x)$ 를 어떤 점  $\alpha(q) \in \pi_2^{-1}(x)$ 로 보내며(즉 각 올이 대응하는 올로 사상되며), 그리고
- 열린집합  $U \subseteq X$  위의 모든 정칙 단면  $s: U \rightarrow L_1$ 에 대해,  $\alpha(s)$ 가 정칙 단면  $s: U \rightarrow L_2$ 가 됩니다.

### 예제 52.4.4

$X = \mathbb{C}$ 라 합시다. 그러면  $\alpha(y, x) = (y \cdot x^2, x)$ 로 정의된  $\alpha: \mathbb{C} \times X \rightarrow \mathbb{C} \times X$ 는 선다발 준동형사상입니다.

이 선다발 준동형사상은 동형사상이 아닌데, 모든 점  $(y, 0)$ 이  $(0, 0)$ 으로 사상되기 때문입니다.

선다발 동형사상의 정의는 예상하시는 바와 같습니다.

**정의 52.4.5** (선다발의 동형사상). 두 선다발  $L_1$ 과  $L_2$ 는, 서로 역인 선다발 동형사상  $\alpha: L_1 \rightarrow L_2$ 와  $\beta: L_2 \rightarrow L_1$ 이 존재하면 **동형**입니다.

## §52.5 가역층과의 관계

쓸 것입니다  
(사실 층도 아직 정의하지 않았습니)

# XIV

## 대수적 정수론 I: 정수환

## 제XIV부: 목차

---

|           |                                                          |            |
|-----------|----------------------------------------------------------|------------|
| <b>53</b> | <b>대수적 정수</b>                                            | <b>537</b> |
| 53.1      | 고등학교 대수학으로부터의 동기 . . . . .                               | 537        |
| 53.2      | 대수적 수와 대수적 정수 . . . . .                                  | 538        |
| 53.3      | 수체 . . . . .                                             | 540        |
| 53.4      | 원시원소 정리, 그리고 단생성 확대 . . . . .                            | 540        |
| 53.5      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                           | 541        |
| <b>54</b> | <b>정수환</b>                                               | <b>543</b> |
| 54.1      | 노름과 자취 . . . . .                                         | 543        |
| 54.2      | 정수 환 . . . . .                                           | 547        |
| 54.3      | 단생성 확대에 대하여 . . . . .                                    | 550        |
| 54.4      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                           | 551        |
| <b>55</b> | <b>유일 인수분해 (드디어!)</b>                                    | <b>553</b> |
| 55.1      | 동기 . . . . .                                             | 553        |
| 55.2      | 아이디얼 산술 . . . . .                                        | 554        |
| 55.3      | 데데킨트 정역 . . . . .                                        | 555        |
| 55.4      | 유일 인수분해가 성립합니다 . . . . .                                 | 557        |
| 55.5      | 인수분해 알고리즘 . . . . .                                      | 559        |
| 55.6      | 분수 아이디얼 . . . . .                                        | 562        |
| 55.7      | 아이디얼 노름 . . . . .                                        | 563        |
| 55.8      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                           | 564        |
| <b>56</b> | <b>민코프스키 경계와 유상군</b>                                     | <b>567</b> |
| 56.1      | 유상군 . . . . .                                            | 567        |
| 56.2      | 수체의 판별식 . . . . .                                        | 568        |
| 56.3      | 수체의 시그니처 . . . . .                                       | 571        |
| 56.4      | 민코프스키 정리 . . . . .                                       | 573        |
| 56.5      | 함정 상자 . . . . .                                          | 574        |
| 56.6      | 민코프스키 경계 . . . . .                                       | 575        |
| 56.7      | 유수군은 유한합니다 . . . . .                                     | 576        |
| 56.8      | 유수의 계산 . . . . .                                         | 577        |
| 56.9      | 선택: $\mathcal{O}_K$ 가 자유 $\mathbb{Z}$ -가군임을 증명 . . . . . | 580        |
| 56.10     | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                           | 585        |
| <b>57</b> | <b>판별식의 추가 성질</b>                                        | <b>587</b> |
| 57.1      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                           | 587        |
| <b>58</b> | <b>보너스: 펠 방정식을 풀어봅시다!</b>                                | <b>589</b> |
| 58.1      | 단위 . . . . .                                             | 589        |
| 58.2      | 디리클레 단위 정리 . . . . .                                     | 590        |
| 58.3      | 기본 단위 찾기 . . . . .                                       | 591        |
| 58.4      | 펠 방정식 . . . . .                                          | 592        |
| 58.5      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                           | 593        |

---

# 53 대수적 정수

대수적 수론의 첫 맛보기입니다.

이는 올림피아드와 고등 수학의 경계에 매우 가까운 내용입니다. 여러분은 항상  $a + \sqrt{2}b$ 가 “노름”(norm)  $a^2 - 2b^2$ 를 가지며, 이 노름이 어떤 식으로든 곱셈적이라는 것을 알고 있었을 것입니다. 또한 근이 켄레쌍으로 나타난다는 것도 항상 알고 있었을 것입니다. 최소다항식에 대해 들어본 적은 있어도 그다지 잘 알지는 못할 수도 있습니다.

이 장과 다음 장은 이러한 모호한 개념들을 정확하게 만들어 줄 것입니다. 이 내용은 주로 [Og10]의 첫 장에서 가져온 것입니다.

## §53.1 고등학교 대수학으로부터의 동기

이는 제 블로그 압도적인 힘<sup>1</sup>에서 각색한 것입니다.

고등학교 미적분 예비과정에서는 정수 계수를 갖는 어떤 다항식의 근을 구하라는 문제를 자주 접하게 됩니다. 예를 들면,

$$x^3 - x^2 - x - 15 = (x - 3)(x^2 + 2x + 5)$$

근으로 3,  $-1 + 2i$ ,  $-1 - 2i$ 를 갖습니다. 또 다른 예로는,

$$x^3 - 3x^2 - 2x + 2 = (x + 1)(x^2 - 4x + 2)$$

근으로  $-1$ ,  $2 + \sqrt{2}$ ,  $2 - \sqrt{2}$ 를 갖습니다.  $-1 \pm 2i$ 나  $2 \pm \sqrt{2}$ 와 같은 무리수 근들이 쌍으로 나타난다는 것을 알아차릴 수 있습니다. 실제로, 미적분 예비과정에서는 복소수 근이 켄레쌍으로 나타난다고 명시적으로 알려줄 것입니다. 더 일반적으로,  $a + b\sqrt{c}$  형태의 모든 근은 “켄레쌍”으로 나타나는 것처럼 보입니다. 그리고 그 이유도 알 수 있을 것입니다.

하지만 다음과 같은 다항식은

$$x^3 - 8x + 4$$

유리수 근을 갖지 않습니다. (이 다항식의 근은 대략  $-3.0514$ ,  $0.51730$ ,  $2.5341$ 입니다.) 혹은 더 간단한 예로,

$$x^3 - 2$$

실근을 단 하나,  $\sqrt[3]{2}$ 만 갖습니다. 이 근들은 무리수임에도 불구하고 “켄레”쌍을 갖지 않습니다. 정말 그럴까요?

정확히 무슨 일이 일어나고 있는지 알아보시다.  $\alpha$ 를 임의의 복소수라 합시다.  $\mathbb{Q}$  위에서  $\alpha$ 의 **최소다항식**을 다음 조건을 만족하는 다항식으로 정의합니다.

- $P(x)$ 는 유리수 계수를 가지며, 최고차항의 계수는 1입니다.
- $P(\alpha) = 0$ .
- $P$ 의 차수는 가능한 한 작습니다.  $\deg P$ 를  $\alpha$ 의 **차수**라고 부릅니다.

### 예제 53.1.1 (최소다항식의 예)

(a)  $\sqrt{2}$ 의 최소다항식은  $x^2 - 2$ 입니다.

(b) 허수 단위  $i = \sqrt{-1}$ 의 최소다항식은  $x^2 + 1$ 입니다.

<sup>1</sup>URL: <https://blog.evanchen.cc/conjugate/>

(c)  $p$ 가 소수일 때, 원시  $p$ 차 단위근  $\zeta_p = e^{\frac{2\pi i}{p}}$ 의 최소다항식은  $x^{p-1} + x^{p-2} + \cdots + 1$ 입니다.

$100x^2 - 200$  역시  $\sqrt{2}$ 를 근으로 갖는 같은 차수의 다항식이라는 점에 주목하십시오. 바로 이 때문에 다항식이 모닉(mononic)일 것을 요구하고자 하는 것입니다. 또한 바로 이 때문에 유리수 범위에서 작업하기로 선택하는 것입니다. 그렇게 하면 정수가 아닌 값이 나올 걱정 없이 최고차항의 계수로 나눌 수 있습니다.

왜 이것이 중요할까요? 요점은 다음과 같습니다:  $A(\alpha) = 0$ 을 만족하는 또 다른 다항식  $A(x)$ 가 있다고 합시다. 그러면  $P(x)$ 가 실제로  $A(x)$ 를 나눈다고 주장할 수 있습니다! 이는  $P$ 의 다른 모든 근 역시  $A$ 의 근이 된다는 것을 의미합니다.

증명은 귀류법으로 진행됩니다. 만약 그렇지 않다면, 다항식의 긴 나눗셈에 의해 다음을 만족하는 몫  $Q(x)$ 와 나머지  $R(x)$ 를 찾을 수 있습니다.

$$A(x) = Q(x)P(x) + R(x)$$

그리고  $R(x) \neq 0$ 입니다.  $x = \alpha$ 를 대입해 보면  $R(\alpha) = 0$ 임을 알 수 있습니다. 하지만  $\deg R < \deg P$ 이고,  $P(x)$ 는 최소다항식이어야 했습니다. 이는 불가능합니다!

이로부터 최소다항식이 유일하다는 것(존재할 경우)이 모닉성과 함께 따라 나오므로, 실제로는 그 최소다항식이라고 부르는 것이 더 낫습니다.

**연습문제 53.1.2.**  $\mathbb{C}$ 에서 최소 다항식이 없는 원소를 찾을 수 있습니까?

더 구체적인 예를 살펴봅시다. 처음에 나왔던  $A(x) = x^3 - 3x^2 - 2x + 2$ 를 생각해 봅시다.  $2 + \sqrt{2}$ 의 최소 다항식은  $P(x) = x^2 - 4x + 2$ 입니다(왜일까요?). 이제  $2 + \sqrt{2}$ 가 근이라면  $A(x)$ 는  $P(x)$ 로 나누어떨어진다는 것을 알고 있습니다. 그리고 이것이 바로  $2 + \sqrt{2}$ 가  $A$ 의 근이라면  $2 - \sqrt{2}$ 도 근이어야 함을 아는 방법입니다.

또 다른 예로,  $\sqrt[3]{2}$ 의 최소 다항식은  $x^3 - 2$ 입니다. 따라서  $\sqrt[3]{2}$ 는 실제로 두 개의 켄레를 가지는데, 즉  $\alpha = \sqrt[3]{2}(\cos 120^\circ + i \sin 120^\circ)$ 와  $\beta = \sqrt[3]{2}(\cos 240^\circ + i \sin 240^\circ)$ 입니다. 따라서  $\sqrt[3]{2}$ 에서 소멸하는 임의의 다항식은  $\alpha$ 와  $\beta$ 도 근으로 가집니다!

**질문 53.1.3** (중요하지만 항진명제: 기약  $\iff$  최소).  $\alpha$ 를 다항식  $P(x)$ 의 근이라 합시다.  $P(x)$ 가 최소 다항식인 것과 기약인 것이 동치임을 보이십시오.

## §53.2 대수적 수와 대수적 정수

**이 절의 대표적인 예:**  $\sqrt{2}$ 는 대수적 정수입니다 ( $x^2 - 2$ 의 근),  $\frac{1}{2}$ 는 대수적 수이지만 대수적 정수는 아닙니다 ( $x - \frac{1}{2}$ 의 근).

이제 훨씬 더 넓은 일반성 속에서 다루어 봅시다. 먼저 위에서 논의한 새로운 수들에 이름을 붙여 봅시다.

**정의 53.2.1.** **대수적 수**는  $\mathbb{Q}$ 의 계수를 가지는 어떤 다항식의 근이 되는 임의의  $\alpha \in \mathbb{C}$ 입니다. 대수적 수의 집합은  $\overline{\mathbb{Q}}$ 로 표기합니다.

**비고 53.2.2** —  $\mathbb{Q}[x]$ 의 임의의 다항식은  $\mathbb{Z}[x]$ 의 다항식으로 스케일링할 수 있으므로, 대수적 수는 ( $\mathbb{Q}$ 가 아니라)  $\mathbb{Z}$ 의 계수를 가지는 어떤 다항식의 근인 수라고 똑같이 말할 수도 있습니다.

**정의 53.2.3.** 대수적 수  $\alpha$ 와 그 최소 다항식  $P$ (모닉이며 유리수 계수를 가짐)를 생각해 봅시다.  $P$ 의 계수가 정수로 밝혀지면,  $\alpha$ 를 **대수적 정수**라고 부릅니다.

대수적 정수의 집합은  $\mathbb{Z}$ 로 표기합니다.

**비고 53.2.4** — 가우스 보조정리를 사용하면,  $\alpha$ 가 정수 계수를 가지는 임의의 모닉 다항식의 근이라면  $\alpha$ 는 대수적 정수임을 보일 수 있습니다. 그래서 실제로는,  $\sqrt{2} + \sqrt{3}$ 가 대수적 정수임을 증명하고 싶다면, 그것이 최소임을 확인할 필요 없이 "다항식  $(x^2 - 5)^2 - 24$ 가 작동합니다"라고만 말하면 됩니다.

때로는 명확성을 위해  $\mathbb{Z}$ 의 원소를 **유리 정수**라고 부릅니다.

**예제 53.2.5** (대수적 정수의 예)

다음 수들은

$$4, i = \sqrt{-1}, \sqrt[3]{2}, \sqrt{2} + \sqrt{3}$$

모두 대수적 정수인데, 모닉 다항식  $x - 4$ ,  $x^2 + 1$ ,  $x^3 - 2$ ,  $(x^2 - 5)^2 - 24$ 의 근이기 때문입니다.

수  $\frac{1}{2}$ 은 최소 다항식  $x - \frac{1}{2}$ 을 가지므로, 대수적 수이지만 대수적 정수는 아닙니다. (사실 유리근 정리도 임의의 모닉 정수 다항식이  $\frac{1}{2}$ 을 근으로 가지지 않음을 직접적으로 함의합니다!)

처음부터 언급하고 싶은 두 가지 성질이 있습니다. 이는 절의 끝부분에 나오는 까다롭지만 좋은 문제들에서 폭넓게 사용될 것이기 때문입니다. 첫 번째는 매우 쉬우므로 지금 증명합니다:

**명제 53.2.6** (유리 대수적 정수는 유리 정수입니다)

대수적 정수가 유리수인 것은 그것이 유리 정수인 것과 필요충분조건입니다. 기호로 나타내면

$$\bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}.$$

입니다.

**증명.**  $\alpha$ 를 유리수라 합시다.  $\alpha$ 가 정수라면 그것은  $x - \alpha$ 의 근이므로, 역시 대수적 정수입니다.

역으로,  $P$ 가 정수 계수를 가지는 모닉 다항식이고  $P(\alpha) = 0$ 이라면 (예컨대 유리근 정리에 의해)  $\alpha$ 는 반드시 정수여야 함이 따라 나옵니다.  $\square$

다른 하나는 다음과 같습니다.

**명제 53.2.7** ( $\mathbb{Z}$ 는 환이고  $\mathbb{Q}$ 는 체)

대수적 정수  $\mathbb{Z}$ 는 환을 이룹니다. 대수적 수  $\mathbb{Q}$ 는 체를 이룹니다.

원한다면 지금 이를 증명할 수도 있지만, 다음 장의 결과가 거의 대신해 줄 것이므로, 잠시 이를 그대로 받아들이기로 합시다.

**비고 53.2.8** — 최소다항식  $P$ 를 갖는 대수적 정수  $\alpha$ 에 대해,  $P$ 의 다른 모든 근 역시 대수적 정수라는 것은 정의상 명백합니다. (위의 두 성질과 더불어) 이 성질이 대수적

정수의 집합을 특징짓는다는 것을 확인할 수 있습니다. 이러한 관점에서, 대수적 정수는 정수환  $\mathbb{Z} \subseteq \mathbb{Q}$ 를 모든 대수적수의 체  $\mathbb{Q}$ 로 내재적으로 정의된 방식으로 일반화한 것으로 생각할 수 있습니다.

### §53.3 수체

**이 절의 대표적인 예:**  $\mathbb{Q}(\sqrt{2})$ 는 전형적인 수체입니다.

임의의 대수적수  $\alpha$ 가 주어지면,  $\mathbb{Q}(\alpha)$  형태의 체를 생각할 수 있습니다. 좀 더 완전한 버전을 적어봅시다.

**정의 53.3.1. 수체**  $K$ 는  $\mathbb{Q}$ 를 부분체로 포함하며 유한 차원  $\mathbb{Q}$ -벡터 공간인 체입니다.  $K$ 의 **차수**는 그 차원입니다.

**예제 53.3.2 (전형적인 예)**

다음 체를 생각해봅시다

$$K = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

이는  $\mathbb{Q}$ 의 체 확대이며, 차수는 2입니다 (기저는 1과  $\sqrt{2}$ 입니다).

$\mathbb{Q}[\sqrt{2}]$  대신  $\mathbb{Q}(\sqrt{2})$  (분모를 허용해야 하는 표기)를 쓴 것에 혼란스러울 수 있습니다. 하지만 **예제 5.5.4**를 읽어보면, 분모는 사실 별로 중요하지 않다는 것을 알 수 있습니다: 예를 들어 어차피  $\frac{1}{3-\sqrt{2}} = \frac{1}{7}(3 + \sqrt{2})$ 입니다. 지금 일반적으로 이를 확인해보거나, 아니면 그 구별을 무시하고 제가 어디서나 대괄호를 쓴 것처럼 여기시면 됩니다.

**연습문제 53.3.3** (중요하지 않음).  $\alpha$ 가 대수적수이면  $\mathbb{Q}(\alpha) \cong \mathbb{Q}[\alpha]$ 임을 보이십시오.

**예제 53.3.4 (대수적수 첨가)**

$\alpha$ 를 어떤 기약다항식  $P(x) \in \mathbb{Q}[x]$ 의 근이라 합시다. 체  $\mathbb{Q}(\alpha)$  역시 체 확대이며, 기저는  $1, \alpha, \alpha^2, \dots, \alpha^{m-1}$ 입니다. 여기서  $m = \deg P$ 입니다. 특히,  $\mathbb{Q}(\alpha)$ 의 차수는  $P$ 의 차수입니다.

**예제 53.3.5 (수체가 아닌 예)**

$\mathbb{R}$ 과  $\mathbb{C}$ 는 유한한  $\mathbb{Q}$ -기저가 없으므로 수체가 아닙니다.

### §53.4 원시원소 정리, 그리고 단생성 확대

**이 절의 대표적인 예:**  $\mathbb{Q}(\sqrt{3}, \sqrt{5}) \cong \mathbb{Q}(\sqrt{3} + \sqrt{5})$ 입니다. 왜 그런지 알 수 있습니까?

이 정리를 여기 실은 이유는 오직 그것이 참이라고 아무도 말해주지 않은 것에 화가 났기 때문이며 (이는 매우 자연스러운 추측입니다), 저는 독자에게 같은 일을 반복하고 싶지 않습니다. 다만 이후에는 이를 사용하지 않을 것입니다.

**정리 53.4.1 (아르틴의 원시원소 정리)**

모든 수체  $K$ 는 어떤 대수적수  $\alpha$ 에 대해  $\mathbb{Q}(\alpha)$ 와 동형입니다.

증명은 **문제 59F**로 남겨둡니다. 이를 증명하려면 먼저 체 확대에 대해 이야기해야 하기 때문입니다.

전형적인 예

$$\mathbb{Q}(\sqrt{3}, \sqrt{5}) \cong \mathbb{Q}(\sqrt{3} + \sqrt{5})$$

를 보면 왜 이 정리가 그리 놀랍지 않아야 하는지 명확해집니다.

**§53.5 생각해 볼 만한 조금 더 어려운 문제**

**문제 53A.**  $\sqrt{2} + \sqrt[3]{3}$ 를 근으로 갖는 정수 계수 다항식을 찾으십시오.



**문제 53B** (브라질 2006).  $p$ 를  $\mathbb{Q}[x]$ 에서 차수가 1보다 큰 기약다항식이라 합시다.  $p$ 가 곱이 1인 두 근  $r$ 과  $s$ 를 가지면  $p$ 의 차수가 짝수임을 증명하십시오.

**문제 53C\***.  $n$ 개의 단위근  $\varepsilon_1, \dots, \varepsilon_n$ 을 생각합니다. 평균  $\frac{1}{n}(\varepsilon_1 + \dots + \varepsilon_n)$ 이 대수적 정수라고 가정합니다. 평균이 0이거나  $\varepsilon_1 = \dots = \varepsilon_n$ 임을 증명하십시오. (**보조정리 22.2.2**에서 사용됩니다.)



**문제 53D<sup>†</sup>.** 어떤 유리수  $q$ 가  $\cos(q\pi) \in \mathbb{Q}$ 를 만족합니까?

**문제 53E** (MOP 2010). 원형으로 배열된  $n > 2$ 개의 램프가 있으며, 처음에는 하나만 켜져 있고 나머지는 꺼져 있습니다. 우리는 꼭짓점들이 램프들 중에 있는 임의의 정다각형을 선택하여 모든 램프의 상태를 동시에 전환할 수 있습니다. 모든 램프를 끄는 것이 불가능함을 보이십시오.



**문제 53F** (크로네커의 정리).  $\alpha$ 가 대수적 정수라고 하십시오. 이것의 모든 갈루아 켤레의 절댓값이 1이라고 가정하십시오. 어떤 양의 정수  $N$ 에 대해  $\alpha^N = 1$ 임을 증명하십시오.



**문제 53G.** 절댓값이 1이면서 단위근이 아닌 대수적 정수가 존재합니까?

**문제 53H.** 대수적 정수의 환은 뇌터 환입니까?



# 54 정수환

## §54.1 노름과 자취

**이 절의 대표적인 예:**  $\mathbb{Q}(\sqrt{2})$ 의 원소로서의  $a + b\sqrt{2}$ 는 노름  $a^2 - 2b^2$ 과 자취  $2a$ 를 가집니다.

올림피아드를 하던 시절,  $a^2 + b^2$ 가  $a + bi$ 의 “노름”이었던 것을 기억하십니까? 좋습니다, 실제로 무슨 일이 일어나고 있는지 알려드리겠습니다.

먼저, 켈레의 개념을 정확히 해보겠습니다.

**정의 54.1.1.**  $\alpha$ 를 대수적 수라 하고,  $P(x)$ 를 그것의 최소다항식이라 하되 차수는  $m$ 이라 합시다. 그러면  $P$ 의  $m$ 개의 근은  $\alpha$ 의 (갈루아) **켈레**입니다.

이 시점에서 중복된 켈레가 없다는 것을 보여줄 가치가 있습니다.

### 보조정리 54.1.2 (기약다항식은 서로 다른 근을 가집니다)

$\mathbb{Q}[x]$ 의 기약다항식은 복소수 중근을 가질 수 없습니다.

**증명.**  $f(x) \in \mathbb{Q}[x]$ 를 기약다항식이라 하고, 이것이 중근  $\alpha$ 를 가진다고 가정합시다. **도함수  $f'(x)$ 를 취합니다.** 이 도함수는 세 가지 흥미로운 성질을 가집니다.

- $f'$ 의 차수는  $f$ 의 차수보다 하나 작습니다.
- 다항식  $f$ 와  $f'$ 는 인수  $x - \alpha$ 를 공유하기 때문에 서로소가 아닙니다.
- $f'$ 의 계수 또한  $\mathbb{Q}$ 에 속합니다.

$g = \gcd(f, f')$ 를 생각해봅시다. 유클리드 호제법에 의해  $g \in \mathbb{Q}[x]$ 여야 합니다. 하지만  $f'$ 에 대한 앞의 두 사실은  $g$ 가 상수가 아니며  $\deg g < \deg f$ 임을 보장합니다. 그런데  $g$ 는  $f$ 를 나누므로, 이는  $f$ 가 기약이어야 한다는 사실에 모순됩니다.  $\square$

따라서  $\alpha$ 는 정확히  $\alpha$ 의 차수만큼의 켈레를 가집니다.

이제, 어떤 원소의 노름  $N(\alpha)$ 를 그것의 켈레들의 곱으로 정의하고 싶습니다. 예를 들어,  $2+i$ 가 노름  $(2+i)(2-i) = 5$ 를 갖고, 일반적으로  $a+bi$ 가 노름  $a^2+b^2$ 을 갖기를 원합니다. 노름이 곱셈적이라면 정말 멋진 것입니다. 복소수에서는 이것이 성립함을 이미 알고 있습니다!

안타깝게도 이것은 그다지 잘 작동하지 않습니다. 다음을 생각해봅시다.

$$N(2+i) = 5 \text{ 그리고 } N(2-i) = 5.$$

하지만  $(2+i)(2-i) = 5$ 이고, 이는 우리가 원하는 것처럼 노름 25를 갖지 않습니다. 왜냐하면 5는 차수가 1이고 켈레를 전혀 갖지 않기 때문입니다. 이러한 “나쁜” 일이 일어나는 이유는, 우리가 원소의 노름을 정의하려 하고 있지만, 실제로는 특정한  $K$ 에 대한 원소의 노름을 정의해야 하기 때문입니다.

제가 말하려는 것은, 노름이 어느 체에 있는지에 따라 다른 의미를 가져야 한다는 것입니다. 5를  $\mathbb{Q}$ 의 원소로 생각하면 그 노름은 5입니다. 하지만  $\mathbb{Q}(i)$ 의 원소로 생각하면 그 노름은 실제로 25여야 합니다. 이를 실현해봅시다:  $K$ 를 수체라 할 때, 이제  $N_{K/\mathbb{Q}}(\alpha)$ 를 다음과 같이  $K$ 에 대한  $\alpha$ 의 노름으로 정의하겠습니다.

**정의 54.1.3.**  $\alpha \in K$ 가 차수  $n$ 을 가진다고 합시다. 그러면  $\mathbb{Q}(\alpha) \subseteq K$ 이고,  $k = (\deg K)/n$ 이라 둡시다.  $\alpha$ 의 **노름**은 다음과 같이 정의됩니다

$$N_{K/\mathbb{Q}}(\alpha) := \left( \prod \alpha \text{의 갈루아 켤레} \right)^k.$$

**자취**는 다음과 같이 정의됩니다

$$\text{Tr}_{K/\mathbb{Q}}(\alpha) := k \cdot \left( \sum \alpha \text{의 갈루아 켤레} \right).$$

$k$ 의 지수는 5를  $\mathbb{Q}$ 의 원소가 아니라  $\mathbb{Q}(i)$ 의 원소로 볼 때 5의 노름을  $5^2 = 25$ 로 만들어주는 “보정 계수”입니다.  $K$ 의 “일반적인” 원소에 대해서는  $k = 1$ 일 것으로 예상됩니다.

**연습문제 54.1.4.** 중첩된 벡터 공간에 대해 알고 있는 것을 이용하여  $k$ 가 실제로 정수임을 스스로 확인해보십시오.

**예제 54.1.5** ( $a + b\sqrt{2}$ 의 노름)

$\alpha = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2}) = K$ 라고 합시다.  $b \neq 0$ 이면,  $\alpha$ 와  $K$ 는 차수 2를 갖습니다. 따라서  $\alpha$ 의 켤레는 오직  $a - b\sqrt{2}$ 뿐이며, 이로부터 노름

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2,$$

을 얻습니다. 대각합은  $(a - b\sqrt{2}) + (a + b\sqrt{2}) = 2a$ 입니다. 신기하게도, 공식  $a^2 - 2b^2$ 와  $2a$ 는  $b = 0$ 인 경우에도 성립합니다.

**예제 54.1.6** ( $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ 의 노름)

$\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2}) = K$ 라고 합시다. 위와 마찬가지로,  $b \neq 0$ 이거나  $c \neq 0$ 이면,  $\alpha$ 와  $K$ 는 같은 차수 3을 갖습니다.  $\alpha$ 의 켤레는  $a + b\sqrt[3]{2}\omega + c\sqrt[3]{4}\omega^2$ 와  $a + b\sqrt[3]{2}\omega^2 + c\sqrt[3]{4}\omega$ 이며, 우리는  $N_{K/\mathbb{Q}}(\alpha) = a^3 + 2b^3 + 4c^3 - 6abc$ 와  $\text{Tr}_{K/\mathbb{Q}}(\alpha) = 3a$ 를 계산할 수 있습니다.

이 경우에는  $\alpha$ 의 켤레가 체  $K$  안에 놓여 있지 않다는 점에 유의하십시오!

중요한 것은 다음과 같습니다:

**명제 54.1.7** (노름과 트레이스는 유리 정수입니다)

$\alpha$ 가 대수적 정수이면, 그 노름과 트레이스는 유리 정수입니다.

**질문 54.1.8.** 증명해 보십시오. (비에트 공식.)

훌륭하지만, 이는 한 가지 의문을 남깁니다: 노름은 왜 곱셈적입니까? 이를 위해서는, 노름과 대각합에 대한 새로운 정의를 제시해야 합니다.

**비고 54.1.9** — ”보정 계수”를 자동으로 더하는 또 다른 방법은  $K$ 에서  $\mathbb{C}$ 로의 매장을 이용하는 것입니다.

이후 **정리 59.3.1**에서 보게 되겠지만,  $K$ 에서  $\mathbb{C}$ 로의 매장은 정확히  $d = \deg K$ 개 존재하며, 이를  $\sigma_1, \dots, \sigma_d$ 라고 합시다. 그러면,  $\text{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^d \sigma_i(\alpha)$ 이고  $N_{K/\mathbb{Q}}(\alpha) =$

$\prod_{i=1}^d \sigma_i(\alpha)$ 입니다.

**정리 54.1.10** (노름과 대각합에 대한 본질적으로 올바른 정의)

$K$ 를 차수  $n$ 인 수체라 하고,  $\alpha \in K$ 라고 합시다.  $\mu_\alpha: K \rightarrow K$ 를

$$x \mapsto \alpha x$$

로 정의되는 사상이라 하고, 이를  $\mathbb{Q}$ -벡터 공간의 선형 사상으로 봅시다. 그러면,

- $\alpha$ 의 노름은 행렬식  $\det \mu_\alpha$ 와 같으며,
- $\alpha$ 의 대각합은 대각합  $\text{Tr } \mu_\alpha$ 와 같습니다.

행렬식의 정의에는 명백한 기하학적 해석이 있습니다:  $K \cong \mathbb{Q}^n$ 을 벡터 공간으로 볼 때, 행렬식은  $\alpha$ 를 곱했을 때  $\mathbb{Q}^n$ 이 얼마나 늘어나는지를 나타냅니다. 즉,  $\mathbb{Q}^n$  안에 부피가  $v$ 인 평행육면체가 주어졌을 때, 변환  $\mu_\alpha$  아래에서 이는 부피가  $|N(\alpha)|v$ 인 평행육면체로 변환됩니다.

대각합과 행렬식은 기저의 선택에 의존하지 않으므로, 원하는 아무 기저나 골라서 고등학교 때 배운 정의를 그대로 사용해도 됩니다. 멋지지 않습니까?

**예제 54.1.11** ( $a + b\sqrt{2}$ 에 대한 행렬의 명시적 계산)

$K = \mathbb{Q}(\sqrt{2})$ 라 하고,  $1, \sqrt{2}$ 를  $K$ 의 기저라고 합시다.

$$\alpha = a + b\sqrt{2}$$

(심지어  $b = 0$ 일 수도 있습니다)라고 하면, 다음을 확인할 수 있습니다.

$$(a + b\sqrt{2})(x + y\sqrt{2}) = (ax + 2yb) + (bx + ay)\sqrt{2}.$$

이를 행렬 형태로 다시 쓰면 다음과 같습니다.

$$\begin{bmatrix} a & 2b \\ b & a \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax + 2yb \\ bx + ay \end{bmatrix}.$$

결과적으로,  $\mu_\alpha$ 를 다음 행렬로 해석할 수 있습니다.

$$\mu_\alpha = \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}.$$

물론 다른 기저를 고르면 행렬은 달라지지만, 행렬식과 대각합은 달라지지 않습니다. 이들은 항상 다음과 같이 주어집니다.

$$\det \mu_\alpha = a^2 - 2b^2 \text{ 그리고 } \text{Tr } \mu_\alpha = 2a.$$

이 해석은  $b = 0$ 인 경우에도 왜  $a + b\sqrt{2}$ 에 대해 같은 공식이 성립해야 하는지를 설명해 줍니다.

증명. 노름에 대해서만 결과를 증명하겠습니다; 대각합은 비슷하게 따라 나옵니다. 다음과

같이 놓읍시다

$$n = \deg \alpha, \quad kn = \deg K.$$

증명은  $k = 1$ 인지 아닌지에 따라 두 부분으로 나눕니다.

$k = 1$ 일 때의 증명.  $n = \deg \alpha = \deg K$ 로 놓읍시다. 따라서 노름은 실제로 갈루아 켈레들의 곱입니다. 또한

$$\{1, \alpha, \dots, \alpha^{n-1}\}$$

는  $K$ 에서 선형독립이며, 따라서 ( $\dim K = n$ 이므로) 기저가 됩니다. 이를  $\mu_\alpha$ 의 기저로 사용합시다.

$$x^n + c_{n-1}x^{n-1} + \dots + c_0$$

를  $\alpha$ 의 최소다항식이라 합시다. 따라서  $\mu_\alpha(1) = \alpha$ ,  $\mu_\alpha(\alpha) = \alpha^2$ 이고 이런 식으로 계속되지만,  $\mu_\alpha(\alpha^{n-1}) = -c_{n-1}\alpha^{n-1} - \dots - c_0$ 입니다. 그러므로  $\mu_\alpha$ 는 다음 행렬로 주어집니다

$$M = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & 0 & \dots & 0 & -c_1 \\ 0 & 1 & 0 & \dots & 0 & -c_2 \\ \vdots & \vdots & \vdots & \ddots & 0 & -c_{n-2} \\ 0 & 0 & 0 & \dots & 1 & -c_{n-1} \end{bmatrix}.$$

따라서

$$\det M = (-1)^n c_0$$

이며, 비에트의 공식에 의해 증명이 끝납니다. ■

$k > 1$ 일 때의 증명. 다음과 같이 중첩된 벡터 공간들이 있습니다

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K.$$

$e_1, \dots, e_k$ 를  $K$ 의  $\mathbb{Q}(\alpha)$ -기저라 합시다 (즉,  $K$ 를  $\mathbb{Q}(\alpha)$  위의 벡터 공간으로 해석하고, 그 기저를 택합니다).  $\{1, \alpha, \dots, \alpha^{n-1}\}$ 가  $\mathbb{Q}(\alpha)$ 의  $\mathbb{Q}$  기저이므로, 다음 원소들은

$$\begin{array}{cccc} e_1, & e_1\alpha, & \dots, & e_1\alpha^{n-1} \\ e_2, & e_2\alpha, & \dots, & e_2\alpha^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ e_k, & e_k\alpha, & \dots, & e_k\alpha^{n-1} \end{array}$$

$K$ 의  $\mathbb{Q}$ -기저를 이룹니다. 이 기저를 사용하면, 사상  $\mu_\alpha$ 는 다음과 같이 보입니다

$$\underbrace{\begin{bmatrix} M & & & \\ & M & & \\ & & \ddots & \\ & & & M \end{bmatrix}}_{k\text{번}}$$

여기서  $M$ 은 위와 같은 행렬입니다: 각  $e_i$ 마다 우리의 기존 행렬 한 벌씩을 얻게 될 뿐입니다. 따라서 필요한 대로  $\det \mu_\alpha = (\det M)^k$ 입니다. ■

**질문 54.1.12.** 대각합에 대해서도 결과를 확인해 보십시오. □

이로부터 다음이 즉시 따라옵니다

$$N_{K/\mathbb{Q}}(\alpha\beta) = N_{K/\mathbb{Q}}(\alpha) N_{K/\mathbb{Q}}(\beta)$$

왜냐하면 정의에 의해 다음을 갖기 때문입니다

$$\mu_{\alpha\beta} = \mu_{\alpha} \circ \mu_{\beta},$$

그리고 행렬식이 곱셈적이라는 사실입니다. 같은 방식으로, 대각합은 덧셈적입니다.

## §54.2 정수 환

**이 절의 대표적인 예:**  $K = \mathbb{Q}(\sqrt{2})$ 이면  $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ 입니다. 그러나  $K = \mathbb{Q}(\sqrt{5})$ 이면  $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ 입니다.

$\mathbb{Z}$ 는  $\mathbb{Q}$ 보다 더 나은 수론을 제공합니다. 마찬가지로,  $K$ 의 대수적 정수에 초점을 맞추면 정말 좋은 구조를 얻을 수 있으며, 여기서 그렇게 하겠습니다.

**정의 54.2.1.** 수체  $K$ 가 주어졌을 때, 우리는

$$\mathcal{O}_K := K \cap \overline{\mathbb{Z}}$$

를  $K$ 의 **정수환**이라 정의합니다; 다시 말해  $\mathcal{O}_K$ 는  $K$ 의 대수적 정수들로 이루어집니다.

이제 이차체의 고전적인 예를 다루겠습니다. 진행하기 전에, 사소한 정수론 사실 하나를 적어야 합니다.

**연습문제 54.2.2** (성가시지만 단순한).  $a$ 와  $b$ 를 유리수라 하고,  $d$ 를 제곱인수가 없는 양의 정수라 합시다.

- $d \equiv 2, 3 \pmod{4}$ 이면,  $2a, a^2 - db^2 \in \mathbb{Z}$ 인 것과  $a, b \in \mathbb{Z}$ 인 것이 동치임을 증명하십시오.
- $d \equiv 1 \pmod{4}$ 에 대해,  $2a, a^2 - db^2 \in \mathbb{Z}$ 인 것과  $a, b \in \mathbb{Z}$ 이거나  $a - \frac{1}{2}, b - \frac{1}{2} \in \mathbb{Z}$ 인 것이 동치임을 증명하십시오.

4로 나눈 나머지를 취해야 할 것입니다.

**예제 54.2.3** ( $K = \mathbb{Q}(\sqrt{3})$ 의 정수환)

$K$ 를 위와 같다고 합시다. 우리는

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{3}] = \{m + n\sqrt{3} \mid m, n \in \mathbb{Z}\}.$$

임을 주장합니다.  $\alpha = a + b\sqrt{3}$ 로 놓습니다. 그러면 최소 다항식이 정수 계수를 가질 때  $\alpha \in \mathcal{O}_K$ 입니다.

$b = 0$ 이면 최소 다항식은  $x - \alpha = x - a$ 이고, 따라서  $\alpha$ 는 정수일 때에만 성립합니다.  $b \neq 0$ 이면 최소 다항식은

$$(x - a)^2 - 3b^2 = x^2 - 2a \cdot x + (a^2 - 3b^2).$$

연습문제로부터, 이는 정확히  $a, b \in \mathbb{Z}$ 일 때 성립합니다.

**예제 54.2.4** ( $K = \mathbb{Q}(\sqrt{5})$ 의 정수환)

이 경우에는

$$\mathcal{O}_K = \mathbb{Z} \left[ \frac{1 + \sqrt{5}}{2} \right] = \left\{ m + n \cdot \frac{1 + \sqrt{5}}{2} \mid m, n \in \mathbb{Z} \right\}.$$

증명은 정확히 동일하되, 연습문제에서  $b \neq 0$ 일 때  $a, b \in \mathbb{Z}$ 이거나  $a, b \in \mathbb{Z} - \frac{1}{2}$ 인 두 가지 가능성이 모두 있음을 알려준다는 점만 다릅니다. 이는  $\frac{1+\sqrt{5}}{2}$ 가  $x^2 - x - 1 = 0$ 의 근이라는 사실을 반영하며,  $\sqrt{3}$ 의 경우에는 이러한 일이 불가능합니다.

일반적으로  $K = \mathbb{Q}(\sqrt{d})$ 의 정수환은

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \pmod{4} \\ \mathbb{Z} \left[ \frac{1+\sqrt{d}}{2} \right] & d \equiv 1 \pmod{4}. \end{cases}$$

우리가 보이고자 하는 것은  $\mathcal{O}_K$ 가  $K$  안에서 정수가  $\mathbb{Q}$  안에서 행동하는 것과 매우 비슷하게 행동한다는 것입니다. 먼저  $K$ 가  $\mathcal{O}_K$ 의 원소들의 몫으로 이루어져 있음을 보입니다. 사실, 더 강한 결과를 얻을 수 있습니다:

**예제 54.2.5** (분모의 유리화)

예를 들어,  $K = \mathbb{Q}(\sqrt{3})$ 을 생각해봅시다. 수  $x = \frac{1}{4+\sqrt{3}}$ 는  $K$ 의 원소이지만, "분모를 유리화"함으로써 다음과 같이 쓸 수 있습니다

$$\frac{1}{4 + \sqrt{3}} = \frac{4 - \sqrt{3}}{13}.$$

그러므로 사실  $x$ 는  $\mathcal{O}_K$ 에 속하는 어떤 정수의  $\frac{1}{13}$ 임을 알 수 있습니다.

이 정리는 더 일반적으로도 성립합니다.

**정리 54.2.6** ( $K = \mathbb{Q} \cdot \mathcal{O}_K$ )

$K$ 를 수체라 하고,  $x \in K$ 를 임의의 원소라 합시다. 그러면  $nx \in \mathcal{O}_K$ 가 되도록 하는 정수  $n$ 이 존재합니다; 다시 말해, 어떤  $\alpha \in \mathcal{O}_K$ 에 대해

$$x = \frac{1}{n} \alpha$$

입니다.

**연습문제 54.2.7.** 이를 직접 증명해보십시오. ( $x$ 가 유리수 계수를 갖는 최소 다항식을 가진다는 사실을 이용하는 것으로 시작하십시오. 또는 노름을 취하십시오.)

이제  $\mathcal{O}_K$ 가 환임을 보이려고 합니다; 덧셈과 곱셈에 대해 닫혀 있음을 확인할 것입니다. 이를 위한 가장 쉬운 방법은:

**보조정리 54.2.8** ( $\alpha \in \overline{\mathbb{Z}} \iff \mathbb{Z}[\alpha]$ 가 유한생성)

$\alpha \in \overline{\mathbb{Q}}$ 라 합시다. 그러면  $\alpha$ 가 대수적 정수인 것은 아벨 군  $\mathbb{Z}[\alpha]$ 가 유한생성인 것과 동치입니다.

증명.  $\alpha$ 가 대수적 정수인 것은 정수 계수를 갖는 어떤 0이 아닌 모닉 다항식의 근인 것과 동치임에 유의하십시오. 먼저 다음을 가정합시다

$$\alpha^N = c_{N-1}\alpha^{N-1} + c_{N-2}\alpha^{N-2} + \cdots + c_0.$$

그러면 집합  $1, \alpha, \dots, \alpha^{N-1}$ 가  $\mathbb{Z}[\alpha]$ 를 생성합니다. 왜냐하면  $\alpha$ 의 모든 거듭제곱이  $N$ 보다 작아질 때까지  $\alpha^N$ 을 반복적으로 대체할 수 있기 때문입니다.

역으로,  $\mathbb{Z}[\alpha]$ 가 어떤  $b_1, \dots, b_m$ 에 의해 유한생성된다고 가정합시다.  $b_i$ 들을  $\alpha$ 에 대한 다항식으로 보면, 큰 정수  $N$ 을 선택하여 (예컨대  $N = \deg b_1 + \cdots + \deg b_m + 2015$ )  $\alpha^N$ 을  $b_i$ 들로 표현하여 다음을 얻을 수 있습니다

$$\alpha^N = c_1 b_1(\alpha) + \cdots + c_m b_m(\alpha).$$

위의 결과는  $\alpha$ 에 대한 모닉 다항식을 우리에게 주며,  $N$ 의 선택은 그것이 0이 아님을 보장합니다. 따라서  $\alpha$ 는 대수적 정수입니다.  $\square$

**예제 54.2.9** ( $\frac{1}{2}$ 은 대수적 정수가 아님)

우리는 이미  $\frac{1}{2}$ 이 대수적 정수가 아님을 알고 있습니다. 따라서 우리는

$$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{ \frac{a}{2^m} \mid a, m \in \mathbb{Z} \text{ 그리고 } m \geq 0 \right\}$$

이 유한생성이 아닐 것으로 예상하며, 실제로 그러합니다.

**질문 54.2.10.** 마지막 예를 구체적으로 만들기 위해:  $\mathbb{Z}[\frac{1}{2}]$ 의 원소들 중 다음의 정수 곱합으로 쓸 수 없는 모든 원소들을 나열해보십시오

$$\left\{ \frac{1}{2}, \frac{7}{8}, \frac{13}{64}, \frac{2015}{4096}, \frac{1}{1048576} \right\}$$

이제 정리를 서술할 수 있습니다.

**정리 54.2.11** (대수적 정수는  $+$ 와  $\times$ 에 대해 닫혀 있습니다)

집합  $\overline{\mathbb{Z}}$ 는 덧셈과 곱셈에 대해 닫혀 있습니다. 즉 이는 환입니다. 특히,  $\mathcal{O}_K$  또한 임의의 수체  $K$ 에 대해 환입니다.

증명.  $\alpha, \beta \in \overline{\mathbb{Z}}$ 라고 합시다. 그러면  $\mathbb{Z}[\alpha]$ 와  $\mathbb{Z}[\beta]$ 는 유한 생성됩니다. 따라서  $\mathbb{Z}[\alpha, \beta]$ 도 그렇습니다. (세부 사항:  $\mathbb{Z}[\alpha]$ 가  $\mathbb{Z}$ -기저  $a_1, \dots, a_m$ 을 가지고  $\mathbb{Z}[\beta]$ 가  $\mathbb{Z}$ -기저  $b_1, \dots, b_n$ 을 가진다면,  $mn$ 개의 원소  $a_i b_j$ 를 취하십시오.)

이제  $\mathbb{Z}[\alpha \pm \beta]$ 와  $\mathbb{Z}[\alpha\beta]$ 는  $\mathbb{Z}[\alpha, \beta]$ 의 부분집합이므로 이들 또한 유한 생성됩니다. 따라서  $\alpha \pm \beta$ 와  $\alpha\beta$ 는 대수적 정수입니다.  $\square$

사실, 더 좋은 것이 성립합니다. 보았듯이,  $\mathbb{Q}(\sqrt{3})$ 에 대해서는  $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$ 이었습니다. 다시 말해,  $\mathcal{O}_K$ 는 1과  $\sqrt{3}$ 에 의해 생성되었습니다.  $\mathbb{Q}(\sqrt{5})$ 에 대해서도 비슷한 것이 성립했습니다. 사실 일반적인 그림도 정확히 이와 같다고 주장합니다.

**정리 54.2.12** ( $\mathcal{O}_K$ 는 계수  $n$ 의 자유  $\mathbb{Z}$ -가군입니다)

$K$ 를 차수  $n$ 의 수체라고 합시다. 그러면  $\mathcal{O}_K$ 는 계수  $n$ 의 자유  $\mathbb{Z}$ -가군입니다. 즉, 아벨 군으로서  $\mathcal{O}_K \cong \mathbb{Z}^{\oplus n}$ 입니다. 다시 말해,  $\mathcal{O}_K$ 는 다음과 같이  $n$ 개의 원소로 이루어진  $\mathbb{Z}$ -기저를 가집니다

$$\mathcal{O}_K = \{c_1\alpha_1 + \cdots + c_{n-1}\alpha_{n-1} + c_n\alpha_n \mid c_i \in \mathbb{Z}\}$$

여기서  $\alpha_i$ 는  $\mathcal{O}_K$ 의 대수적 정수입니다.

증명은 이후 장으로 미루겠습니다.

이 마지막 정리는 여러 면에서  $\mathcal{O}_K$ 가  $K$  안의 "격자"임을 보여줍니다. 즉, 수체  $K$ 에 대해  $\mathcal{O}_K$  안에서  $\alpha_1, \dots, \alpha_n$ 을 찾을 수 있어 다음이 성립합니다

$$\begin{aligned}\mathcal{O}_K &\cong \alpha_1\mathbb{Z} \oplus \alpha_2\mathbb{Z} \oplus \cdots \oplus \alpha_n\mathbb{Z} \\ K &\cong \alpha_1\mathbb{Q} \oplus \alpha_2\mathbb{Q} \oplus \cdots \oplus \alpha_n\mathbb{Q}\end{aligned}$$

아벨 군으로서.

**§54.3 단생성 확대에 대하여**

수체  $K$ 가 모두 어떤  $\alpha$ 에 대해  $\mathbb{Q}(\alpha)$ 로 표현될 수 있다는 것을 상기하십시오. 정수환에 대해서도 비슷한 것이 성립하기를 바랄 수 있습니다. 즉,

$$\mathcal{O}_K = \mathbb{Z}[\theta]$$

로 쓸 수 있기를 바라는 것이며, 이 경우  $\{1, \theta, \dots, \theta^{n-1}\}$ 은  $K$ 의 기저이자  $\mathcal{O}_K$ 의  $\mathbb{Z}$ -기저 역할을 동시에 합니다(여기서  $n = [K : \mathbb{Q}]$ ). 다시 말해,  $\mathcal{O}_K$ 의 기저가 실제로 "거듭제곱 기저"이기를 바랍니다.

이는 우리가 사용하는 가장 흔한 예들에 대해서는 성립합니다:

- 이차체, 그리고
- [문제 54E](#)에서의 원분체.

안타깝게도, 일반적으로는 성립하지 않습니다: 첫 번째 반례는  $X^3 - X^2 - 2X - 8$ 의 근  $\alpha$ 에 대한  $K = \mathbb{Q}(\alpha)$ 입니다.

이러한 좋은 성질을 가진 확대를 **단생성**이라고 부릅니다. 나중에 보게 되겠지만, 단생성 확대는 정말 좋은 인수분해 알고리즘을 가지고 있습니다, [정리 55.5.4](#).

**비고 54.3.1** ( $\mathcal{O}_K$ 에서 무엇이 잘못되었는가?) — 앞서 언급했듯이, 아벨 군으로서  $\mathcal{O}_K \cong \mathbb{Z}^3$ 이므로, 이는 유한히 많은 원소에 의해 생성됩니다.

사실,  $\{1, \alpha, \beta\}$ 는  $\mathcal{O}_K$ 의 기저이며, 여기서  $\beta = \frac{\alpha + \alpha^2}{2}$ 입니다.  $\{1, \alpha, \alpha^2\}$ 에 의해 생성되는 군은  $\mathcal{O}_K$ 에서 지표 2를 가집니다 — 즉,  $|\mathcal{O}_K / \langle 1, \alpha, \alpha^2 \rangle| = 2$ 이며,  $\beta$ 를 놓치게 됩니다.

대신  $\{1, \beta, \beta^2\}$ 를 기저로 선택하려 하면, 다시  $|\mathcal{O}_K / \langle 1, \beta, \beta^2 \rangle| = 2$ 를 얻게 되며,  $\alpha$ 를 놓치게 됩니다. 명시적으로 계산해 보면  $\beta^2 = \frac{3\alpha^2 + 7\alpha}{2} + 6 = 3\beta + 2\alpha + 6$ 을 얻을 수 있습니다.

이것이 이 확대가 단생성이 아니라는 증명은 아니지만,  $\mathcal{O}_K$ 의 구조에 대한 느낌을 주기를 바랍니다.

## §54.4 생각해 볼 만한 조금 더 어려운 문제

**문제 54A\***.  $\alpha$ 가  $\mathcal{O}_K$ 의 단위원( $\alpha^{-1} \in \mathcal{O}_K$ 를 의미함)인 것과  $N_{K/\mathbb{Q}}(\alpha) = \pm 1$ 인 것이 동치임을 보이십시오.

**문제 54B\***.  $K$ 를 수체라고 합시다.  $\mathcal{O}_K$ 의 분수체는 무엇입니까?

**문제 54C** (러시아 올림피아드 1984). 다음을 만족하는 모든 정수  $m$ 과  $n$ 을 구하십시오.

$$(5 + 3\sqrt{2})^m = (3 + 5\sqrt{2})^n.$$

**문제 54D** (미국 TST 2012). 다음을 만족하는  $a, b, c > 2010$ 이 존재하는지 판별하십시오.

$$a^3 + 2b^3 + 4c^3 = 6abc + 1.$$



**문제 54E<sup>†</sup>** (원분체).  $p$ 를 홀수인 유리 소수라 하고  $\zeta_p$ 를 1의 원시  $p$ 제곱근이라 합시다.  $K = \mathbb{Q}(\zeta_p)$ 라 합시다.  $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$ 임을 증명하십시오. (사실  $p$ 가 소수가 아니어도 이 결과는 성립합니다.)



# 55 유일 인수분해 (드디어!)

오래도 걸렸습니다.

## §55.1 동기

디오판토스 방정식  $n = x^2 + 5y^2$ 에서, 주어진  $n$ 에 대한 해에 관심이 있다고 합시다. 아이디얼  $n$ 을  $\mathbb{Z}[\sqrt{-5}]$ 에서 “인수분해”해 보는 것으로, 예를 들면

$$6 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

하지만 안타깝게도 이것은 그리 간단하지 않은데, 앞서 말했듯이 우리는 원소의 유일 인수분해를 갖지 않기 때문입니다:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

이것이 통하지 않는 한 가지 이유는 우리에게 최대공약수라는 개념이 없기 때문입니다.  $(35, 77) = 7$ 이라고 쓸 수는 있지만,  $(3, 1 + \sqrt{-5})$ 는 어떻게 이해해야 할까요?

요령은 아이디얼을 “일반화된 최대공약수”로 사용하는 것입니다.  $(a, b)$ 라는 표기로 제가 의미하는 것은 아이디얼  $\{ax + by \mid x, y \in \mathbb{Z}[\sqrt{-5}]\}$ 임을 기억하십시오.  $(35, 77) = (7)$ 임을 알 수 있지만,  $(3, 1 + \sqrt{-5})$ 는 환 안의 실제 값을 나타내지 않으므로 “단순화되지 않은” 채로 남게 됩니다. 이러한 집합(아이디얼)을 원소처럼 사용하면, 소인수분해의 완전한 이론을 전개할 수 있음이 밝혀지며, 이 장에서 바로 그것을 다룹니다.

다시 말해, 우리는 아이디얼  $(a_1, \dots, a_m)$ 을 사용해  $a_1, \dots, a_m$ 의 “일반화된 최대공약수”를 해석합니다. 특히 표현하고자 하는 수  $x$ 가 있다면, 이를 그냥  $(x)$ 로 부호화합니다.

다시 6의 예로 돌아가서,

$$(6) = (2) \cdot (3) = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

실제로 (6)을 소 아이디얼로 완전히 인수분해하면 다음과 같다는 것을 제 말대로 믿어 주십시오.

$$(6) = (2, 1 - \sqrt{-5})^2 (3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) = \mathfrak{p}^2 \mathfrak{q}_1 \mathfrak{q}_2.$$

실제로  $(2) = \mathfrak{p}^2$ ,  $(3) = \mathfrak{q}_1 \mathfrak{q}_2$ ,  $(1 + \sqrt{-5}) = \mathfrak{p} \mathfrak{q}_1$ ,  $(1 - \sqrt{-5}) = \mathfrak{p} \mathfrak{q}_2$ 입니다. 따라서 6은 원소로는 인수분해되지 않더라도 아이디얼로는 실제로 유일하게 인수분해됩니다.

위에서 볼 수 있듯이, 아이디얼 인수분해는 원소 인수분해보다 더 정교합니다. 아이디얼로의 인수분해를 얻고 나면, 거기서부터 원소로의 모든 인수분해를 복원할 수 있습니다. 이것의 요점은,  $n$ 을  $x^2 + 5y^2$ 로 쓰고 싶다면  $n$ 을 아이디얼로 인수분해하기만 하면 되고, 거기서부터 원소로의 모든 인수분해를 복원할 수 있으며, 결국  $n$ 을  $x^2 + 5y^2$ 로 쓰는 모든 방법을 얻을 수 있다는 것입니다. 우리는 이미  $n$ 을 유리 소인수로 분해할 수 있으므로(위의 예  $6 = 2 \cdot 3$ 처럼), 각 유리 소수  $p \mid n$ 이 어떻게 분해되는지만 알아내면 됩니다. 이를 위한 방법이 있는데, 바로 정리 55.5.4입니다! 실제로 이 특수한 경우에 그것이 무엇을 말하는지도 알려드리겠습니다:

- 만약  $t^2 + 5$ 가  $(t + c)(t - c) \pmod{p}$ 로 인수분해되면,  $(p) = (p, c + \sqrt{-5})(p, c - \sqrt{-5})$ 입니다.
- 그렇지 않으면  $(p)$ 는 소 아이디얼입니다.

이 장에서는 유일 인수분해 이론을 완전히 일반적인 형태로 전개하겠습니다.

**비고 55.1.1** — 이 장에서는  $\mathfrak{a}$ ,  $\mathfrak{b}$ ,  $\mathfrak{p}$ ,  $\mathfrak{q}$  라는 문자를  $\mathcal{O}_K$ 의 아이디얼을 나타내는 데 사용하겠습니다. 분수 아이디얼이 등장할 때는  $I$ 와  $J$ 를 사용하겠습니다.

## §55.2 아이디얼 산술

**이 절의 대표적인 예:**  $(x)(y) = (xy)$ 이고,  $(x) + (y) = (\gcd(x, y))$ 입니다. 어느 경우든 생성원의 관점에서 생각하십시오.

먼저 두 아이디얼  $\mathfrak{a}$ 와  $\mathfrak{b}$ 를 더하고 곱하는 방법을 알려드려야 합니다.

**정의 55.2.1.** 환  $R$ 의 두 아이디얼  $\mathfrak{a}$ 와  $\mathfrak{b}$ 가 주어졌을 때, 다음과 같이 정의합니다

$$\begin{aligned}\mathfrak{a} + \mathfrak{b} &:= \{a + b \mid a \in \mathfrak{a}, b \in \mathfrak{b}\} \\ \mathfrak{a} \cdot \mathfrak{b} &:= \{a_1 b_1 + \cdots + a_n b_n \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}.\end{aligned}$$

(일반적인 환에서는 무한합이 의미가 없으므로,  $\mathfrak{a} \cdot \mathfrak{b}$ 에서 유한 개의 항 이후로 합을 끊는다는 점에 유의하십시오.) 이것들이 실제로 아이디얼임을 쉽게 확인할 수 있습니다. 이 정의는  $\mathfrak{a}$ 와  $\mathfrak{b}$ 의 생성원의 관점에서 생각하면 더 자연스럽습니다.

### 명제 55.2.2 (생성원을 통한 아이디얼 연산)

$\mathfrak{a} = (a_1, a_2, \dots, a_n)$ 이고  $\mathfrak{b} = (b_1, \dots, b_m)$ 이 환  $R$ 의 아이디얼이라고 합시다. 그러면

- (a)  $\mathfrak{a} + \mathfrak{b}$ 는  $a_1, \dots, a_n, b_1, \dots, b_m$ 으로 생성되는 아이디얼입니다.
- (b)  $\mathfrak{a} \cdot \mathfrak{b}$ 는  $1 \leq i \leq n$ 이고  $1 \leq j \leq m$ 인  $a_i b_j$ 로 생성되는 아이디얼입니다.

증명. 꽤 간단하니, 이 결과가 옳다는 것을 스스로 확인해 보십시오. □

다시 말해, 합에 대해서는 두 생성원 집합을 이어 붙이고, 곱에 대해서는 생성원들의 곱을 취합니다. 주 아이디얼의 경우 이는 “보통의” 곱셈과 일치한다는 점에 주목하십시오. 예를 들어

$$(3) \cdot (5) = (15)$$

$\mathbb{Z}$ 에서 말입니다.

**비고 55.2.3** — 아이디얼  $\mathfrak{a}$ 와 원소  $c$ 에 대해, 집합

$$c\mathfrak{a} = \{ca \mid a \in \mathfrak{a}\}$$

은  $(c) \cdot \mathfrak{a}$ 와 같다는 점에 주목하십시오. 따라서 “스케일링”과 “주 아이디얼을 곱하는 것”은 같은 것입니다. 이는 중요한데, 앞으로 두 개념을 서로 바꾸어 사용할 것이기 때문입니다.

**비고 55.2.4** — 두 아이디얼의 덧셈은 원소들의 덧셈에 대응하지 않습니다 — 예를 들어,  $(4) + (6) = (4, 6) = (2)$ 이지만,  $4 + 6 = 10$ 입니다.

이것이 우리가 기대할 수 있는 최선입니다 — 아이디얼에 대해서는 원소들의 덧셈이 의미를 가지지 않습니다 — 예를 들어,  $1 + 1 = 2$ 이고  $1 + (-1) = 0$ 이지만, 아이디얼로서는  $(1) = (-1)$ 입니다.

사실, 아이디얼의 덧셈은 원소들의 gcd를 직관적으로 일반화한 것입니다 — 위의 예에서 확인할 수 있듯이,  $\gcd(4, 6) = 2$ 입니다.

그럼에도 불구하고,  $a + b$ 가  $(a, b)$ 와 같은 표기보다 자연스러운 표기라는 데 동의하기를 바랍니다.  
 인수분해는 아이디얼들을 더하는 것이 아니라 곱하는 것을 수반하므로, 당분간은  $a + b$ 라는 표기를 사용할 필요가 없을 것입니다.

마지막으로, 인수분해를 하고자 한다면 나눗셈이라는 개념이 있어야 합니다. 그래서 다음과 같이 정의합니다:

**정의 55.2.5.**  $a$ 가  $b$ 를 나눈다고 말하며,  $a \geq b$ 이면  $a \mid b$ 라고 씁니다.

포함관계가 뒤집힌다는 점에 주목하십시오! 따라서 (3)은 (15)를 나누는데, 이는 (15)가 (3)에 포함되기 때문입니다. 즉, 15의 모든 배수는 3의 배수입니다. 그리고 앞 절의 예시로부터:  $\mathbb{Z}[\sqrt{-5}]$ 에서,  $(3, 1 - \sqrt{-5})$ 는 (3)과  $(1 - \sqrt{-5})$ 를 나눕니다.

마지막으로, **소 아이디얼**은 **정의 5.3.1**에서와 같이 정의됩니다:  $xy \in \mathfrak{p}$ 가  $x \in \mathfrak{p}$  또는  $y \in \mathfrak{p}$ 를 함의하면  $\mathfrak{p}$ 는 소 아이디얼입니다. 이는 나눗셈의 정의와 부합합니다:

**연습문제 55.2.6.** 영이 아닌 진 아이디얼  $\mathfrak{p}$ 가 소 아이디얼인 것은,  $\mathfrak{p}$ 가  $ab$ 를 나눌 때마다  $\mathfrak{p}$ 가  $a$  또는  $b$  중 하나를 나누는 것과 동치입니다.

**비고 5.3.3**에서 언급했듯이, 이는 또한 우리가 단원에 의한 곱셈을 무시할 수 있게 해줍니다:  $(-3) = (3)$ .

## §55.3 데데킨트 정역

**이 절의 대표적인 예:** 어떠한  $\mathcal{O}_K$ 이든 데데킨트 정역입니다.

이제 데데킨트 정역을 다음과 같이 정의합니다.

**정의 55.3.1.** 정역  $\mathcal{A}$ 는, 뇌터 환이고 정수적으로 닫혀 있으며  $\mathcal{A}$ 의 영이 아닌 모든 소 아이디얼이 실제로 극대 아이디얼일 때, **데데킨트 정역**입니다. (마지막 조건이 중요한 조건입니다.)

**비고 55.3.2** — 우리는 곧 임의의 수체  $K$ 에 대해  $\mathcal{O}_K$ 가 데데킨트 정역임을 증명할 것입니다. 이는 사실 Napkin에서 우리가 사용할 유일한 경우입니다. 그러므로 "데데킨트 정역"이라는 용어를 도입하는 것은, 우리가 실제로 다른 종류의 데데킨트 정역을 마주치게 될 것이기 때문이 아니라, 주로 유일 인수분해를 위해  $\mathcal{O}_K$ 의 어떤 성질들이 사용되는지 강조하기 위함입니다.

여기서 새로 정의해야 할 단어가 하나 있지만, 이를 그리 많이 사용하지는 않을 것입니다.

**정의 55.3.3.**  $R$ 을 정역이라 하고,  $K$ 를 그 분수체라 합시다.  $R$  위의 모닉 다항식의 근이 되는  $K$ 의 원소  $a \in K$ 가 오직  $R$ 의 원소(즉 자명한  $x - r$  다항식의 근)뿐일 때,  $R$ 이 **정수적으로 닫혀 있다**고 합니다.

데데킨트 정역의 정의에서 흥미로운 조건은 마지막 조건입니다: 소 아이디얼과 극대 아이디얼이 동일하다는 것입니다. 다른 조건들은 그저 기술적인 사항일 뿐이지만, "소 아이디얼은 극대 아이디얼이다"라는 조건은 실질적인 내용을 담고 있습니다.

**예제 55.3.4 ( $\mathbb{Z}$ 는 데데킨트 정역입니다)**

환  $\mathbb{Z}$ 는 데데킨트 정역입니다. 다음을 유의하십시오.

- $\mathbb{Z}$ 는 (자명한 이유로) 뇌터입니다.
- $\mathbb{Z}$ 의 분수체는  $\mathbb{Q}$ 입니다.  $f(x) \in \mathbb{Z}[x]$ 가 모닉이면, 유리근 정리에 의해 모든 유리 근은 정수입니다(이는  $\mathbb{Z} \cap \mathbb{Q} = \mathbb{Z}$ 의 증명과 동일합니다). 따라서  $\mathbb{Z}$ 는 정수적으로 닫혀 있습니다.
- $\mathbb{Z}$ 의 영이 아닌 소 아이디얼은  $(p)$ 이며, 이는 극대 아이디얼이기도 합니다.

우리가 관심을 갖는 경우는 인수분해를 하고자 하는 환  $\mathcal{O}_K$ 입니다. 이제 임의의 수체  $K$ 에 대해 환  $\mathcal{O}_K$ 가 데데킨트 정역임을 보이겠습니다. 먼저, 지루한 부분부터 시작합니다.

**명제 55.3.5 ( $\mathcal{O}_K$ 는 정수적으로 닫혀 있고 뇌터적입니다)**

임의의 수체  $K$ 에 대해, 환  $\mathcal{O}_K$ 는 정수적으로 닫혀 있고 뇌터적입니다.

증명. 지루하지만, 완전성을 위해 여기 제시합니다.

$\mathcal{O}_K \cong \mathbb{Z}^{\oplus n}$ 이므로,<sup>1</sup> 이것이 뇌터임을 알 수 있습니다.

이제  $\mathcal{O}_K$ 가 정수적으로 닫혀 있음을 보이겠습니다.  $\eta \in K$ 가  $\mathcal{O}_K$ 의 원소들을 계수로 갖는 어떤 다항식의 근이라고 가정합시다. 따라서

$$\eta^n = \alpha_{n-1} \cdot \eta^{n-1} + \alpha_{n-2} \cdot \eta^{n-2} + \cdots + \alpha_0$$

여기서  $\alpha_i \in \mathcal{O}_K$ 입니다. 우리는  $\eta \in \mathcal{O}_K$  역시 성립함을 보이고자 합니다.

위로부터,  $\mathcal{O}_K[\eta]$ 는 유한 생성이며... 따라서  $\mathbb{Z}[\eta] \subseteq \mathcal{O}_K[\eta]$ 는 유한 생성입니다. 그러므로  $\eta \in \mathbb{Z}$ 이며, 따라서  $\eta \in K \cap \mathbb{Z} = \mathcal{O}_K$ 입니다.  $\square$

이제 재미있는 부분을 해보겠습니다. 반복적으로 다시 등장하게 될 더 강한 결과를 증명하겠습니다.

**정리 55.3.6 (중요: 소 아이디얼은 유리 소수를 나눕니다)**

$\mathcal{O}_K$ 를 정수환이라 하고,  $\mathfrak{p}$ 를 그 안의 영이 아닌 소 아이디얼이라 합시다. 그러면  $\mathfrak{p}$ 는 어떤 유리 소수  $p$ 를 포함합니다. 더욱이  $\mathfrak{p}$ 는 극대 아이디얼입니다.

구체적인 예로,  $\mathbb{Z}[i]$  안의  $(2+i) \subseteq \mathbb{Z}[i]$ 를 생각해 봅시다. 이 경우  $p = 5$ 이며,  $p \in (2+i)$ 이기 때문에 격자가 두 방향 모두에서 주기 5로 주기적이 됨을 알 수 있고, 이는  $\{a+bi \mid 0 \leq a, b \leq 4, a, b \in \mathbb{Z}\}$  안의 유한히 많은 점들만으로 아이디얼에 대한 모든 잉여류를 덮기에 충분함을 함의합니다.

여기서 몫이 유한함을 보이는 증명은, 다음 절에서 다룰 격자의 메시가 유한하다는 명제와 밀접하게 관련되어 있습니다.

증명.  $\mathfrak{p}$  안의 임의의  $\alpha \neq 0$ 을 취합시다. 그 갈루아 켈레들은 대수적 정수이므로, 그들의 곱  $N(\alpha)/\alpha$ 는  $\mathcal{O}_K$  안에 있습니다(비록 각각의 켈레가 개별적으로는  $K$  안에 있을 필요가 없더라도 말입니다). 결과적으로  $N(\alpha) \in \mathfrak{p}$ 이며, 우리는  $\mathfrak{p}$ 가 어떤 정수를 포함함을 결론짓습니다.

그런 다음  $\mathfrak{p}$  안에서 가장 작은 양의 정수를  $p$ 라고 합시다.  $p$ 는 유리 소수여야 하는데, 그렇지 않다면  $\mathfrak{p} \ni p = xy$ 이므로  $x, y \in \mathfrak{p}$  중 하나가 성립하기 때문입니다. 이것으로 첫 번째 부분이 증명됩니다.

<sup>1</sup>정리 54.2.12에 의함.

이제  $\mathfrak{p}$ 가 극대 아이디얼임을 보이기 위해 다소 교묘한 작업을 해보겠습니다.  $\mathcal{O}_K/\mathfrak{p}$ 를 살펴봅시다;  $\mathfrak{p}$ 가 소 아이디얼이므로 이는 정역이어야 하지만... 우리는 이것이 실제로 유한하다고 주장합니다! 이를 위해, 우리는  $\mathcal{O}_K$  위에서 곱셈을 할 수 있다는 사실을 잊습니다.  $\mathcal{O}_K \cong \mathbb{Z}^{\oplus n}$ 이 아벨 군으로서 성립함을 상기하면, 우리는 다음과 같은 사상을 얻습니다.

$$\mathbb{F}_p^{\oplus n} \cong \mathcal{O}_K/(p) \twoheadrightarrow \mathcal{O}_K/\mathfrak{p}.$$

따라서  $|\mathcal{O}_K/\mathfrak{p}| \leq p^n$ 은 유한합니다. 유한 정역은 체이므로(문제 5D\*) 증명이 완료됩니다.  $\square$

영이 아닌 모든 소 아이디얼  $\mathfrak{p}$ 가 극대 아이디얼이므로, 우리는 이제  $\mathcal{O}_K$ 가 데데킨트 정역을 알게 되었습니다. 이 교묘한 증명은 본질적으로 문제 5G<sup>†</sup>의 풀이에서 영감을 받았음을 유의하십시오.

**비고 55.3.7** — 첫 번째 부분에 대한 대안적인 증명은 다음과 같습니다:  $\mathfrak{p}$ 가 아이디얼이므로  $\alpha \cdot \mathcal{O}_K \subseteq \mathfrak{p}$ 이지만,  $\alpha \cdot \mathcal{O}_K$ 는 계수  $n$ 인 자유  $\mathbb{Z}$ -가군이므로,  $\mathfrak{p}$ 는 계수  $n$ 인 두 자유  $\mathbb{Z}$ -가군 사이에 끼어 있으며, 정리 18.1.5에 의해  $\mathfrak{p}$  역시 계수  $n$ 인 자유 가군이어야 합니다. 따라서  $\mathfrak{p}$ 는 유한하며, 그다음 보조정리 56.8.8을 사용합니다.

## §55.4 유일 인수분해가 성립합니다

좋습니다, 이제 말씀드리겠습니다!

**유일 인수분해는 데데킨트 정역에서 완벽하게 성립합니다!**

**비고 55.4.1 (데데킨트 정역과 UFD의 비교)** — 뇌터 조건과 정수 폐포 조건을 잠시 잊는다면, 다음이 성립합니다:

- 소원소와 기약원소가 같다면, 그 정역은 원소의 유일 인수분해를 허용합니다.
- 소 아이디얼과 극대 아이디얼이 같다면, 그 정역은 아이디얼의 유일 인수분해를 허용합니다.

유사성에 주목하십시오 — 어느 경우든, 뇌터 조건은 소인수를 계속 추출할 때 유한한 시간 안에 끝난다는 것을 보장하기 위한 것에 “불과합니다”.

**예제 55.4.2** ( $\mathcal{A}$ 가 정수적으로 닫혀 있지 않으면 무엇이 잘못될까요?)

$\mathbb{Z}$ 의 아이디얼인  $\mathcal{A} = 2\mathbb{Z}$ 를 생각해 봅시다. 분명히, 0이 아닌 모든 소 아이디얼은 극대 아이디얼입니다.

그럼에도 불구하고,  $\mathcal{A}$ 에서  $(2 \cdot 3 \cdot 5) = (60)$ 는 소 아이디얼이 아니며 (따라서 물론 극대 아이디얼도 아닙니다), 이를 예를 들어  $(2 \cdot 3) \cdot (5)$ 로 분해할 수 없습니다.

**정리 55.4.3 (소인수분해가 작동합니다)**

$\mathcal{A}$ 를 데데킨트 정역  $\mathcal{A}$ 의 0이 아닌 진 아이디얼이라 합시다. 그러면  $\mathfrak{a}$ 는 0이 아닌 소 아이디얼  $\mathfrak{p}_i$ 들의 유한 곱으로 다음과 같이 쓸 수 있습니다,

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \dots \mathfrak{p}_g^{e_g}$$

그리고 이 인수분해는  $\mathfrak{p}_i$ 의 순서를 제외하면 유일합니다.

더욱이,  $\mathfrak{a}$ 가  $\mathfrak{b}$ 를 나눈다는 것은 모든 소 아이디얼  $\mathfrak{p}$ 에 대해  $\mathfrak{a}$ 에서  $\mathfrak{p}$ 의 지수가  $\mathfrak{b}$ 에서 그에 대응하는 지수보다 작거나 같다는 것과 동치입니다.

증명을 다 쓰지는 않겠지만, 기본적인 공략법을 설명하겠습니다. [U108]의 3절에서 이를 잘 설명하고 있습니다. 산술의 기본정리를 증명할 때, 기본적인 줄거리는 다음과 같았습니다:

- (1)  $p$ 가 유리 소수<sup>2</sup>라면,  $p \mid bc$ 는  $p \mid b$  또는  $p \mid c$ 를 의미함을 보이십시오. (이는 유클리드 보조정리라 불립니다.)
- (2) 강한 귀납법을 사용하여 모든  $N > 1$ 이 소수들의 곱으로 표현될 수 있음을 보이십시오 (쉽습니다).
- (3) 어떤 소수들에 대해  $p_1 \dots p_m = q_1 \dots q_n$ 이면(반드시 유일할 필요는 없습니다),  $p_1 = q_i$ 인  $i$ 가 존재함을 보이십시오. 예컨대  $q_1$ 이라 합시다.
- (4) 양변을  $p_1$ 으로 나누고 귀납법을 사용하십시오.

여기서 이 증명을 반복하려고 하면 어떻게 될까요? 우리는 1단계를 공짜로 얻습니다. 왜냐하면 더 나은 "소수"의 정의를 사용하고 있기 때문입니다. 3단계도 할 수 있는데, 이는 1단계로부터 따라 나오기 때문입니다. 그러나 2단계는 작동하지 않는데, 추상적인 데데킨트 정역에 대해서는 크기라는 개념이 실제로 없기 때문입니다. 그리고 4단계도 작동하지 않는데, 아직 소 아이디얼의 역원이 무엇인지에 대한 개념이 없기 때문입니다.

그런데 실제로는 아이디얼의 역원  $\mathfrak{a}^{-1}$ 를 정의할 수 있으며, 이 장이 끝날 때까지 그렇게 할 것입니다. 그러면  $\mathfrak{a} \cdot \mathfrak{a}^{-1} = (1) = \mathcal{A}$ 임을 확인해야 합니다. 사실 이것조차 쉽지 않습니다. 먼저 소 아이디얼  $\mathfrak{p}$ 에 대해 이것이 참임을 확인하고, 그런 다음 소인수분해를 증명하고, 그다음에 이것이 참임을 증명해야 합니다. 더욱이  $\mathfrak{a}^{-1}$ 는 실제로는 아이디얼이 아니므로,  $\mathcal{A}$  대신 분수체  $K$ 에서 작업해야 합니다.

그러므로 새로운 상황에서의 주요 단계들은 다음과 같습니다.

- (1) 먼저, 모든 아이디얼  $\mathfrak{a}$ 가 유한한 소수들의 모임  $\mathfrak{p}_1 \dots \mathfrak{p}_g$ 를 나눴음을 보이십시오. (이는 초론의 보조정리의 응용입니다.)
- (2)  $\mathfrak{p}^{-1}$ 를 정의하고  $\mathfrak{p}\mathfrak{p}^{-1} = (1)$ 임을 보이십시오.
- (3) 인수분해가 존재함을 보이십시오(다시 초론의 보조정리를 사용합니다).
- (4) 우리가 정의한 새로운 역원을 사용하여 그것이 유일함을 보이십시오.

마지막으로,  $\mathcal{A}$ 가 (예를 들어  $\mathbb{Z}$ 와 같은) 주 아이디얼 정역(PID)인 경우 이것이 얼마나 멋진지 언급하겠습니다. 그러면 모든 원소  $a \in \mathcal{A}$ 는 아이디얼  $(a)$ 와 직접 대응됩니다. 이제  $(a)$ 가 아이디얼들의 곱  $\mathfrak{p}_i = (p_i)$ 로 인수분해된다고 가정해봅시다.

$$(a) = (p_1)^{e_1} (p_2)^{e_2} \dots (p_n)^{e_n}.$$

<sup>2</sup>소수에 대한 유클리드 수준의 정의는 " $p$ 가 두 개의 더 작은 정수의 곱이 아니다"라는 것임에 주의하십시오. 이는 소수의 올바른 정의가 아닙니다: 소수의 정의는  $p \mid bc$ 이면  $p \mid b$  또는  $p \mid c$ 라는 것입니다. 유클리드 수준의 정의는 "기약"이라 불리는 것입니다. 다행히도,  $\mathbb{Z}$ 에서는 소수와 기약원소가 같은 것이므로, 여러분의 "소수" 정의가 틀렸다고 아무도 말해주지 않았던 것입니다.

이는 문자 그대로

$$a = up_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$$

으로 읽히며, 여기서  $u$ 는 어떤 단위입니다(정의 4.4.1을 상기하십시오). 따라서 PID인 데데킨트 정역은  $\mathbb{Z}$ 에서와 마찬가지로 원소들에 대한 유일 인수분해를 만족합니다. (사실 이것의 역도 참입니다.)

## §55.5 인수분해 알고리즘

이차체(quadratic field)에서 몇 가지 예를 살펴보겠습니다.  $K = \mathbb{Q}(\sqrt{d})$ 이면 다음과 같음을 기억하십시오.

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \pmod{4}. \end{cases}$$

또한  $a + b\sqrt{-d}$ 의 노름은  $a^2 + db^2$ 로 주어짐을 기억하십시오.

**예제 55.5.1** ( $\mathbb{Q}(\sqrt{-5})$ 의 정수환에서 6을 인수분해하기)

$K = \mathbb{Q}(\sqrt{-5})$ 로부터 나오는  $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ 를 생각합시다. 우리는 이미

$$(6) = (2) \cdot (3) = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

그리고 이 주 아이디얼들로는 더 이상 나아갈 수 없습니다. 하지만 다음과 같이 둡시다.

$$\mathfrak{p} = (1 + \sqrt{-5}, 2) = (1 - \sqrt{-5}, 2) \quad \text{그리고} \quad \mathfrak{q}_1 = (1 + \sqrt{-5}, 3), \mathfrak{q}_2 = (1 - \sqrt{-5}, 3).$$

그러면  $(6) = \mathfrak{p}^2 \mathfrak{q}_1 \mathfrak{q}_2$ 임이 밝혀집니다. 더 구체적으로는  $(2) = \mathfrak{p}^2$ ,  $(3) = \mathfrak{q}_1 \mathfrak{q}_2$ 이며,  $(1 + \sqrt{-5}) = \mathfrak{p} \mathfrak{q}_1$ 이고  $(1 - \sqrt{-5}) = \mathfrak{p} \mathfrak{q}_2$ 입니다. (증명은 곧 하겠습니다.)

우리의 모든 아이디얼이  $\mathcal{O}_K$ 에 대해 계산된다는 점을 강조하고 싶습니다. 예를 들어,

$$(2) = \{2x \mid x \in \mathcal{O}_K\}.$$

이 예에서  $\mathfrak{p}$ 가 소 아이디얼/극대 아이디얼임을 어떻게 알 수 있을까요? (다시 말하지만, 우리는 데데킨트 정역에 있으므로 이 둘은 같습니다.) 답:  $\mathcal{O}_K/\mathfrak{p}$ 를 살펴보고 그것이 체인지 확인하십시오. 여기에는 요령이 있습니다: 우리는 다음과 같이 나타낼 수 있습니다.

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[x]/(x^2 + 5).$$

따라서 그것을  $\mathfrak{p}$ 로 나눈 나머지를 취하면, 다음을 얻습니다.

$$\mathcal{O}_K/\mathfrak{p} = \mathbb{Z}[x]/(x^2 + 5, 2, 1 + x) \cong \mathbb{F}_2[x]/(x^2 + 5, x + 1)$$

환으로서.

**질문 55.5.2.**  $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_2$ 임을 결론짓고,  $\mathfrak{q}_1$ 과  $\mathfrak{q}_2$  또한 극대 아이디얼임을 스스로 확인해 보십시오.

아이디얼 곱셈의 명시적인 예를 하나 들어야겠습니다. 다음을 계산해봅시다.

$$\begin{aligned} \mathfrak{q}_1 \mathfrak{q}_2 &= ((1 + \sqrt{-5})(1 - \sqrt{-5}), 3(1 + \sqrt{-5}), 3(1 - \sqrt{-5}), 9) \\ &= (6, 3 + 3\sqrt{-5}, 3 - 3\sqrt{-5}, 9) \\ &= (6, 3 + 3\sqrt{-5}, 3 - 3\sqrt{-5}, 3) \\ &= (3) \end{aligned}$$

여기서 우리는 먼저  $9 - 6 = 3$ 을 계산했고(유클리드 알고리즘을 떠올리십시오!), 그다음 다른 모든 생성원들이 3으로 이미 가진 것 외에 아무것도 기여하지 않음을 확인했습니다(이 아이디얼들 역시  $\mathcal{O}_K$ 에서 계산된 것입니다).  $\mathfrak{p}^2$ ,  $\mathfrak{p}\mathfrak{q}_1$ ,  $\mathfrak{p}\mathfrak{q}_2$ 에 대해서도 같은 방식으로 계산할 수 있습니다.

마지막으로, 어떤  $x$ 에 대해서도  $\mathfrak{p} \neq (x)$ 임을, 즉  $\mathfrak{p}$ 가 주 아이디얼이 아님을 빠르게 확인해볼 가치가 있습니다. 모순을 위해 그렇다고 가정합시다. 그러면  $x$ 는  $1 + \sqrt{-5}$ 와 2를 모두 나누는데, 이는 어떤  $\alpha_1, \alpha_2 \in \mathcal{O}_K$ 에 대해  $1 + \sqrt{-5} = \alpha_1 x$ 이고  $2 = \alpha_2 x$ 라는 의미입니다. (주 아이디얼은 정확히  $x$ 의 "배수"들이므로  $(x) = x\mathcal{O}_K$ 입니다.) 노름을 취하면,  $N_{K/\mathbb{Q}}(x)$ 가 다음 둘을 모두 나눌 수 있습니다.

$$N_{K/\mathbb{Q}}(1 + \sqrt{-5}) = 6 \quad \text{그리고} \quad N_{K/\mathbb{Q}}(2) = 4.$$

$\mathfrak{p} \neq (1)$ 이므로  $x$ 는 단위일 수 없으며, 따라서 그 노름은 2여야 합니다. 그러나  $\mathcal{O}_K$ 에는 노름이  $2 = a^2 + 5b^2$ 인 원소가 존재하지 않습니다.

### 예제 55.5.3 ( $\mathbb{Q}(\sqrt{-17})$ 의 정수환에서 3을 인수분해하기)

$\mathcal{O}_K = \mathbb{Z}[\sqrt{-17}]$ 가  $K = \mathbb{Q}(\sqrt{-17})$ 로부터 나온다고 합시다. 우리는  $\mathcal{O}_K \cong \mathbb{Z}[x]/(x^2 + 17)$ 임을 알고 있습니다. 이제

$$\mathcal{O}_K/3\mathcal{O}_K \cong \mathbb{Z}[x]/(3, x^2 + 17) \cong \mathbb{F}_3[x]/(x^2 - 1).$$

이는 이미 (3)이 소(즉 극대) 아이디얼이 될 수 없음을 보여주는데, 그렇지 않다면 우리의 결과가 체(field)여야 하기 때문입니다. 어쨌든 우리는 다음과 같은 사영을 갖습니다.

$$\mathcal{O}_K \twoheadrightarrow \mathbb{F}_3[x]/((x-1)(x+1)).$$

$\mathfrak{q}_1$ 을 그 상(image)에서  $(x-1)$ 의 원상(pre-image)이라 합시다. 즉,

$$\mathfrak{q}_1 = (3, \sqrt{-17} - 1).$$

마찬가지로,

$$\mathfrak{q}_2 = (3, \sqrt{-17} + 1).$$

우리는  $\mathcal{O}_K/\mathfrak{q}_1 \cong \mathbb{F}_3$ 임을 알고 있으므로,  $\mathfrak{q}_1$ 은 극대(소) 아이디얼입니다. 마찬가지로  $\mathfrak{q}_2$ 도 소 아이디얼입니다. 신기하게도, 다음을 명시적으로 확인할 수 있습니다.

$$\mathfrak{q}_1 \mathfrak{q}_2 = (3).$$

따라서 이것이 (3)의 소 아이디얼로의 인수분해입니다.

$q_1 q_2 = (3)$ 이라는 사실은 신기해 보이지만, 실제로 참입니다.

$$\begin{aligned} q_1 q_2 &= (3, \sqrt{-17} - 1)(3, \sqrt{-17} + 1) \\ &= (9, 3\sqrt{-17} + 3, 3\sqrt{-17} - 3, 18) \\ &= (9, 3\sqrt{-17} + 3, 6) \\ &= (3, 3\sqrt{-17} + 3, 6) \\ &= (3). \end{aligned}$$

사실 이것은 일반적으로 항상 성립하는 것으로 밝혀졌습니다. 유리 소수  $p$ 가 주어지면,  $\mathbb{Z}[\theta]$  형태의 임의의  $\mathcal{O}_K$ 에서  $p$ 를 인수분해하는 알고리즘이 존재합니다.

#### 정리 55.5.4 (소인수분해 알고리즘 / 데데킨트-쿠머 정리)

$K$ 를 대수적 수체라 합시다.  $\theta \in \mathcal{O}_K$ 가  $|\mathcal{O}_K/\mathbb{Z}[\theta]| = j < \infty$ 를 만족한다 하고,  $p$ 를  $j$ 를 나누지 않는 소수라 합시다. 그러면  $(p) = p\mathcal{O}_K$ 는 다음과 같이 인수분해됩니다:

$f$ 를  $\theta$ 의 최소다항식이라 하고,  $\bar{f}$ 를 법  $p$ 로 다음과 같이 인수분해합시다

$$\bar{f} \equiv \prod_{i=1}^g (\bar{f}_i)^{e_i} \pmod{p}.$$

그러면 각  $i$ 에 대해  $\mathfrak{p}_i = (f_i(\theta), p)$ 는 소 아이디얼이며,  $(p)$ 의 인수분해는 다음과 같습니다

$$\mathcal{O}_K \supseteq (p) = \prod_{i=1}^g \mathfrak{p}_i^{e_i}.$$

특히,  $K$ 가  $\mathcal{O}_K = \mathbb{Z}[\theta]$ 인 단생성체(monogenic)라면  $j = 1$ 이며, 이 정리는 모든 소수  $p$ 에 대해 적용됩니다.

이 책의 거의 모든 응용에서  $K$ 는 단생성체, 즉  $j = 1$ 일 것입니다. 여기서  $\bar{\psi}$ 는 다항식  $\psi \in \mathbb{Z}[x]$ 가  $\mathbb{F}_p[x]$ 에서 갖는 상을 나타냅니다.

**질문 55.5.5.** 우리가 선택할 수 있는 원상  $f_i$ 는 여러 가지가 있을 수 있습니다 (예를 들어  $\bar{f}_i = x^2 + 1 \pmod{3}$ 이라면,  $f_i = x^2 + 3x + 7$ 을 선택할 수도 있습니다.) 이것이  $\mathfrak{p}_i$ 의 값에 영향을 주지 않는 이유는 무엇입니까?

앞서 우리는 특정한 경우에 대해 이 인수분해가 성립하는지 확인할 수 있었음에 유의하십시오. 이것이 성립한다는 증명도 이와 거의 같지만, 아이디얼 노름이라는 도구가 하나 더 필요합니다. 그 이후에는 이 명제를 **문제 55E**로 남겨둡니다.

이 알고리즘은  $\mathcal{O}_K = \mathbb{Z}[\theta]$ 인 임의의 단생성 대수적 수체에서  $(p)$ 의 소인수분해를 계산하는 구체적인 방법을 제공합니다. 그 절차를 요약하면 다음과 같습니다:

1.  $\theta$ 의 최소다항식을 구하고, 이를  $f \in \mathbb{Z}[x]$ 라 합시다.
2.  $f$ 를 법  $p$ 로 기약다항식들  $\bar{f}_1^{e_1} \bar{f}_2^{e_2} \dots \bar{f}_g^{e_g}$ 로 인수분해합니다.
3. 각  $i$ 에 대해  $\mathfrak{p}_i = (f_i(\theta), p)$ 를 계산합니다.

그러면  $(p) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$ 입니다.

혹은 더 짧게:

$\mathbb{Z}[x]/(f(x))$ 에서  $p$ 를 인수분해하는 대신,  $\mathbb{Z}[x]/(p)$ 에서  $f(x)$ 를 인수분해할 수 있습니다.

두 방법 모두  $\mathbb{Z}[x]/(f(x), p)$ 에서 0을 인수분해하는 것과 동치입니다 — 다시 말해,  $\mathbb{Z}[x]/(f(x), p)$ 를  $\mathbb{Z}[x]$ -가군의 직합으로 쓰는 것입니다.

**연습문제 55.5.6.** 위의 알고리즘을 사용하여  $\mathbb{Z}[i]$ 에서 (29)를 인수분해하십시오.

## §55.6 분수 아이디얼

**이 절의 대표적인 예:**  $\mathbb{Z}$ 에 대한  $\mathbb{Q}$ 의 유사물로, 아이디얼의 역원을 취할 수 있게 해줍니다. 소인수분해가 가장 좋은 방식으로 작동합니다.

이제 정수를 인수분해하는 것과 마찬가지로  $\mathcal{A}$ 의 아이디얼을 인수분해하는 깔끔한 이론을 갖추었습니다. 이제  $\mathbb{Z}$ 의 인수분해가 자연스럽게  $\mathbb{Q}$ 의 원소를 인수분해하는 방법을 제공합니다. 다는 점에 주목하십시오. 분자와 분모를 각각 인수분해하면 됩니다.

유사성을 더 명확히 해봅시다. 유리수의 유사물은 다음과 같습니다.

**정의 55.6.1.**  $\mathcal{A}$ 를 분수체  $K$ 를 갖는 데데킨트 정역이라 합시다.  $K$ 의 **분수 아이디얼**  $J$ 란 다음과 같은 형태의 집합입니다

$$J = \frac{1}{x} \cdot \mathfrak{a} \quad \text{여기서 } x \in \mathcal{A} \text{이고, } \mathfrak{a} \text{는 정수 아이디얼입니다.}$$

강조를 위해,  $\mathcal{A}$ 의 아이디얼을 때때로 **정수 아이디얼**이라 부르기도 합니다.

이 정의가 다소 의외라고 느껴질 수도 있습니다: 분수 아이디얼이 어떤 정수 아이디얼  $\mathfrak{a}$ ,  $\mathfrak{b}$ 에 대해  $\frac{\mathfrak{a}}{\mathfrak{b}}$ 의 형태여야 한다고 예상할 법도 합니다. 하지만 실제로는 분모에  $x \in \mathcal{A}$ 만 있으면 충분합니다. 이는 우리가  $\mathcal{O}_K$ 를 살펴볼 때, 정수 분모만 있으면 충분하다는 것을 발견했던 것과 같은 유비입니다:  $\frac{1}{4-\sqrt{3}} = \frac{1}{13}(4+\sqrt{3})$ . 이와 마찬가지로 여기서도  $\frac{\mathfrak{a}}{\mathfrak{b}}$  대신  $\frac{1}{x} \cdot \mathfrak{a}$ 만 살펴보면 충분하다는 것이 밝혀질 것이며, 그래서 처음부터 이런 식으로 정의합니다. 다른 동치인 정의는 **문제 55D<sup>†</sup>**를 참고하십시오.

**예제 55.6.2** ( $\frac{5}{2}\mathbb{Z}$ 는 분수 아이디얼입니다)

집합

$$\frac{5}{2}\mathbb{Z} = \left\{ \frac{5}{2}n \mid n \in \mathbb{Z} \right\} = \frac{1}{2}(5)$$

은  $\mathbb{Z}$ 의 분수 아이디얼입니다.

이제 앞서 규정한 대로, 분수 아이디얼은 곱셈에 대한 군을 이룹니다:

**정리 55.6.3** (분수 아이디얼은 군을 이룹니다)

$\mathcal{A}$ 를 데데킨트 정역이라 하고  $K$ 를 그 분수체라 합시다. 임의의 정수 아이디얼  $\mathfrak{a}$ 에 대해, 집합

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq (1) = \mathcal{A}\}$$

은  $\mathfrak{a}\mathfrak{a}^{-1} = (1)$ 을 만족하는 분수 아이디얼입니다.

(이 결과는 자명하지 않습니다.  $\mathfrak{a}\mathfrak{a}^{-1} = (1)$ 을 증명하는 한 가지 방법은, 먼저  $\mathfrak{a}$ 가 소 아이디얼인 경우에 대해 증명한 다음,  $\mathfrak{a}$ 의 소 아이디얼로의 분해를 고려하는 것입니다.)

**정의 55.6.4.** 따라서  $K$ 의 0이 아닌 분수 아이디얼들은 항등원  $(1) = \mathcal{A}$ 를 갖는 곱셈 군을 이룹니다. 이 **아이디얼 군**은  $J_K$ 로 표기합니다.

**예제 55.6.5** ( $\mathbb{Z}$ 에서의  $(3)^{-1}$ )

$\mathbb{Z}$ 에서 다음이 성립함을 확인해 보십시오

$$(3)^{-1} = \left\{ \frac{1}{3}n \mid n \in \mathbb{Z} \right\} = \frac{1}{3}\mathbb{Z}.$$

이로부터 모든 분수 아이디얼  $J$ 는 다음과 같이 유일하게 표현될 수 있음이 따라옵니다

$$J = \prod_i \mathfrak{p}_i^{n_i} \cdot \prod_i \mathfrak{q}_i^{-m_i}$$

여기서  $n_i$ 와  $m_i$ 는 양의 정수입니다. 실제로  $\mathfrak{a}$ 가 정수 아이디얼인 것은, 정수의 경우와 마찬가지로, 그 모든 지수가 음이 아닌 경우와 동치입니다. 그러므로 분수 아이디얼을 생각하는 아마도 더 나은 방법은, 음의 지수를 가질 수도 있는 소 아이디얼들의 곱으로 보는 것입니다.

## §55.7 아이디얼 노름

마지막 도구는 아이디얼 노름으로, 이는 아이디얼의 "크기"에 대한 개념을 제공합니다.

**정의 55.7.1.** 0이 아닌 아이디얼  $\mathfrak{a} \subseteq \mathcal{O}_K$ 의 **아이디얼 노름**(또는 절대 노름)은  $|\mathcal{O}_K/\mathfrak{a}|$ 로 정의되며  $N(\mathfrak{a})$ 로 표기합니다.

**예제 55.7.2** (가우스 정수에서  $(5)$ 의 아이디얼 노름)

$K = \mathbb{Q}(i)$ ,  $\mathcal{O}_K = \mathbb{Z}[i]$ 라 합시다.  $\mathcal{O}_K$ 에서의 아이디얼  $(5)$ 를 생각해 봅시다. 다음이 성립합니다

$$\mathcal{O}_K/(5) \cong \{a + bi \mid a, b \in \mathbb{Z}/5\mathbb{Z}\}$$

따라서  $(5)$ 는 아이디얼 노름 25를 가지며, 이는  $\mathcal{O}_K/(5)$ 가  $5^2 = 25$ 개의 원소를 가진다는 사실에 대응됩니다.

**예제 55.7.3** (가우스 정수에서  $(2+i)$ 의 아이디얼 노름)

$$\mathcal{O}_K/(2+i) \cong \mathbb{F}_5$$

임을 알 수 있는데, 이는  $2+i$ 를 법으로 할 때  $5 \equiv 0$ 이고  $i \equiv -2$ 이기 때문입니다. (실제로  $(2+i)$ 가 소 아이디얼이므로 체를 얻는 것이 당연합니다!) 따라서  $N((2+i)) = 5$ 이며, 마찬가지로  $N((2-i)) = 5$ 입니다.

따라서 아이디얼 노름은 그 아이디얼이 얼마나 "여유로운지"를 측정합니다: 즉,  $(5)$ 는  $\mathbb{Z}$ 에서보다  $\mathbb{Z}[i]$ 에서 훨씬 더 넓게 퍼져 있습니다. (이 직관은 나중에  $\mathcal{O}_K$ 를 실제로 격자로 볼 때 중요해질 것입니다.)

**질문 55.7.4.** 아이디얼 노름이 1인 아이디얼은 무엇입니까?

$(5)$ 를 이용한 우리의 예시는 아이디얼 노름의 여러 성질을 시사하는데, 이는 실제로 참임이 밝혀집니다:

**보조정리 55.7.5 (절대 노름의 성질)**

$\mathfrak{a}$ 를  $\mathcal{O}_K$ 의 0이 아닌 아이디얼이라 합시다.

- (a)  $N(\mathfrak{a})$ 는 유한합니다.
- (b) 다른 임의의 영이 아닌 아이디얼  $\mathfrak{b}$ 에 대해,  $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$ 입니다.
- (c)  $\mathfrak{a} = (a)$ 가 주 아이디얼이면,  $N(\mathfrak{a}) = |N_{K/\mathbb{Q}}(a)|$ 입니다.

아쉽게도 이 성질들을 증명하지는 않겠지만,  $\mathcal{O}_K$ 가 데데킨트 정역임을 증명할 때 이미 (a)를 증명했습니다.

원소의 노름의 경우와 마찬가지로, 아이디얼 노름 또한 기하학적 해석을 가집니다:  $\mathfrak{a} = (a)$  일 때  $\mu_a$ 를  $a$ -곱하기 사상이라 하면,  $N_{K/\mathbb{Q}}(a) = |\det \mu_a|$ 는  $K$ 를  $\mathbb{Q}$ -벡터 공간으로 볼 때  $\mu_a$  아래에서  $K$ 가 얼마나 늘어나는지를 측정한다는 것을 상기하십시오.

**연습문제 55.7.6.**  $\mu_a(\mathcal{O}_K) \subseteq \mathcal{O}_K$ 이면,  $|\mathcal{O}_K/a\mathcal{O}_K|$ 가 정확히  $|\det \mu_a|$ 와 같음을 스스로 확인해 보십시오.

이는 왜  $N(\mathfrak{a}) = |N_{K/\mathbb{Q}}(a)|$ 인지를 설명해 주지만,  $\mathfrak{a} = (a) = (-a)$ 이므로  $a$ -곱하기 사상이 유일할 필요는 없다는 점에 유의하십시오.

$N$ 이 완전히 곱셈적이라는 사실 덕분에, 자연스러운 확장을 통해 분수 아이디얼  $J$ 의 노름도 생각할 수 있습니다

$$J = \prod_i \mathfrak{p}_i^{n_i} \cdot \prod_i \mathfrak{q}_i^{-m_i} \implies N(J) := \frac{\prod_i N(\mathfrak{p}_i)^{n_i}}{\prod_i N(\mathfrak{q}_i)^{m_i}}.$$

따라서  $N$ 은  $J_K \rightarrow \mathbb{Q}^\times$ 인 자연스러운 군 준동형사상입니다.

**§55.8 생각해 볼 만한 조금 더 어려운 문제**

**문제 55A.**  $K = \mathbb{Q}(\sqrt{-13})$ 일 때,  $\mathcal{O}_K$ 에서 77의 서로 다른 인수분해가 세 가지 존재함을 보이십시오.

**문제 55B.**  $K = \mathbb{Q}(\sqrt[3]{2})$ 라 하고,  $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$ 임을 주어진 것으로 받아들이십시오.  $\mathcal{O}_K$ 에서 (5)의 인수분해를 구하십시오.

**문제 55C (페르마의 소정리).**  $\mathfrak{p}$ 를 어떤 정수환  $\mathcal{O}_K$ 의 소 아이디얼이라 하십시오.  $\alpha \in \mathcal{O}_K$ 에 대해 다음을 보이십시오,

$$\alpha^{N(\mathfrak{p})} \equiv \alpha \pmod{\mathfrak{p}}.$$

**문제 55D<sup>†</sup>.**  $\mathcal{A}$ 를 분수체  $K$ 를 갖는 데데킨트 정역이라 하고,  $J \subseteq K$ 를 택하십시오.  $J$ 가 분수 아이디얼인 것과 다음이 동치임을 보이십시오

- (i)  $J$ 가 덧셈 및  $\mathcal{A}$ 의 원소에 의한 곱셈에 대해 닫혀 있고, 또한
- (ii)  $J$ 가 아벨 군으로서 유한 생성됩니다.

더 간결하게 말하면:  $J$ 가 분수 아이디얼인 것  $\iff J$ 가 유한 생성  $\mathcal{A}$ -가군인 것입니다.

**문제 55E.** 정리 55.5.4의 표기법에서,  $I = \prod_{i=1}^g \mathfrak{p}_i^{e_i}$ 라 하십시오. 간단히 하기 위해  $K$ 가 단생성이어서  $\mathcal{O}_K = \mathbb{Z}[\theta]$ 라고 가정합니다.

- (a) 각  $\mathfrak{p}_i$ 가 소 아이디얼임을 증명하십시오.

(b)  $(p)$ 가  $I$ 를 나눈다는 것을 보이십시오.

(c) 노름을 사용하여  $(p) = I$ 임을 보이십시오.



**문제 55F** (USEMO 2025).  $k$ 를 6으로 나누어떨어지지 않는 양의 정수라 합시다.  $p$ 가  $2025^k - 1$ 과  $2026^k - 1$ 을 모두 나누는 소수  $p$ 가 존재한다고 가정합시다.  $p < 3^k$ 임을 증명하십시오.



# 56 민코프스키 경계와 유상군

우리는 이제 아이디얼의 유일 인수분해에 관한 훌륭한 이론을 갖추었습니다. PID의 경우, 이것은 실제로 우리에게 UFD를 제공합니다. 좋습니다.

잠시 후,  $\mathcal{O}_K$ 가 PID로부터 얼마나 멀리 떨어져 있는지를 측정하는 유상군이라는 것을 정의할 것입니다; 유상군이 클수록  $\mathcal{O}_K$ 는 PID로부터 더 멀리 떨어져 있습니다. 특히,  $\mathcal{O}_K$ 는 유상군이 자명하면 PID입니다.

그런 다음 유상군에 제약을 가할 수 있게 해 주는 몇 가지 부등식을 제시할 것입니다; 예를 들어, 이것은 어떤 경우에는 유상군이 반드시 자명해야 함을 보이는 데 사용될 것입니다. 놀랍게도, 그 증명은 기하학의 결과인 민코프스키 정리를 사용할 것입니다.

## §56.1 유상군

이 절의 대표적인 예: PID는 자명한 유상군을 가집니다.

$K$ 를 수체라 하고,  $J_K$ 를  $\mathcal{O}_K$ 의 분수 아이디얼로 이루어진 곱셈군이라 합시다.  $P_K$ 를 **주 분수 아이디얼**로 이루어진 곱셈군, 즉 어떤  $x \in K$ 에 대해  $(x) = x\mathcal{O}_K$  꼴인 것들의 군이라 합시다.

**질문 56.1.1.**  $P_K$  역시 곱셈군임을 확인하십시오. (이것은 정말 쉽습니다:  $x\mathcal{O}_K \cdot y\mathcal{O}_K$ 와  $(x\mathcal{O}_K)^{-1}$ 를 명명해 보십시오.)

$J_K$ 가 아벨 군이므로, 우리는 이제 **유상군**(또는 **아이디얼 유상군**)을 다음 몫으로 정의할 수 있습니다

$$\text{Cl}_K := J_K / P_K.$$

$\text{Cl}_K$ 의 원소들을 **류**라고 부릅니다.  
동등하게,

**유상군  $\text{Cl}_K$ 는  $K$ 에서의 상수배에 대해 법(modulo)을 취한, 영이 아닌 분수 아이디얼들의 집합입니다.**

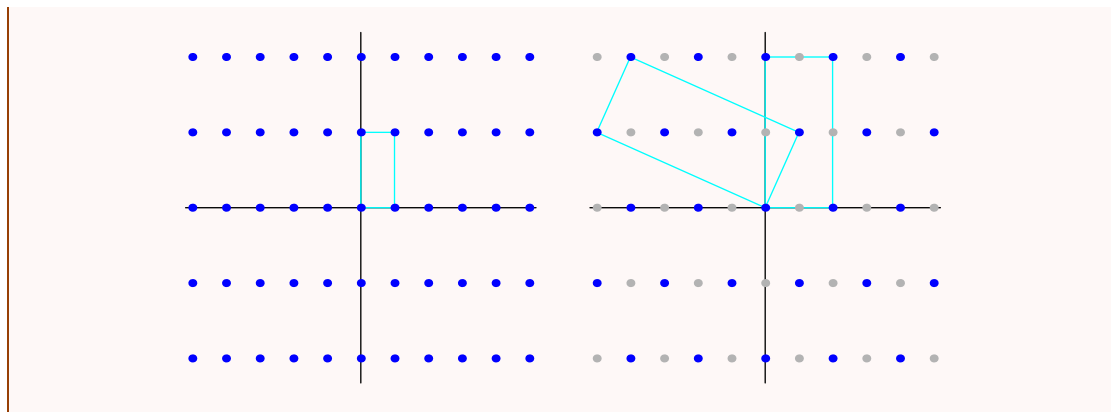
두 아이디얼이  $\mathcal{O}_K$ -가군으로서 동형사상일 때에만 같은 류에 속하므로, 류를 아이디얼들의 "모양"으로 생각할 수도 있습니다.

### 예제 56.1.2 ( $\mathbb{Q}(\sqrt{-5})$ 에서의 아이디얼 류)

만약 체가 허수 이차체라면, 아이디얼의 류를 시각화하는 것은 정말 쉽습니다: 복소수를 곱하는 것은 스케일링과 회전의 조합에 대응하므로(즉, 각도를 보존하므로), 두 아이디얼이 닮음일 때, 즉 회전과 스케일링을 사용하여 하나를 다른 하나 위에 겹칠 수 있을 때 같은 류에 속합니다.

체가  $K = \mathbb{Q}(\sqrt{-5})$ 일 때, 정수환은  $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ 입니다.

아래의 첫 번째 그림은 아이디얼  $(1) \subseteq \mathcal{O}_K$ 를 나타냅니다. 두 번째 그림은 주 아이디얼이 아닌  $(2, 1 + \sqrt{-5}) \subseteq \mathcal{O}_K$ 를 나타냅니다.



특히, 영이 아닌 주 아이디얼들은 스케일링을 제외하면 동일하므로, 모든 아이디얼이 주 아이디얼이면  $\text{Cl}_K$ 는 자명합니다.

유상군의 크기를 **유상수**라고 부릅니다. 유상수가 항상 유한하다는 것은 아름다운 정리이며, 이 장의 대부분은 이 결과를 향해 쌓아 나갈 것입니다. 이를 위해서는 여러 가지 요소가 필요합니다.

## §56.2 수체의 판별식

이 절의 대표적인 예: 이차체.

$K = \mathbb{Q}(\sqrt{2})$ 라고 합시다. 앞서 보았듯이, 이는  $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ 임을 의미하며, 다음을 뜻합니다

$$\mathcal{O}_K = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}.$$

이제 핵심적인 통찰은 이것을 격자로 생각할 수 있다는 것입니다: 기하학적으로, 우리는 이것을  $\mathbb{Z}^2$ 를 생각하는 것과 같은 방식으로 생각하고자 합니다.

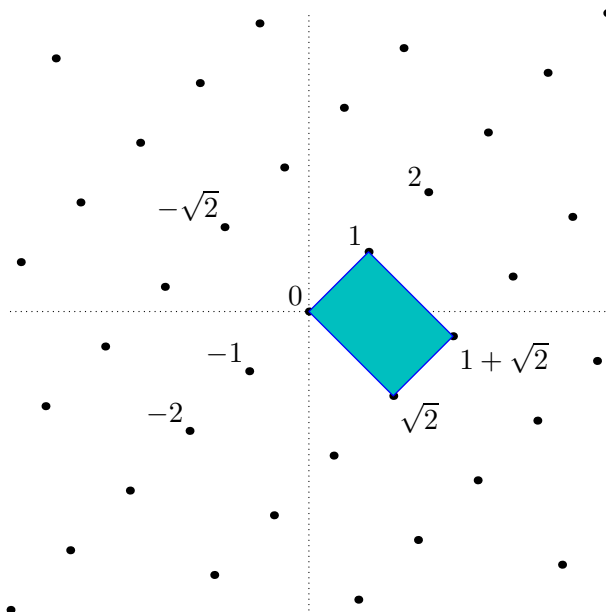
짓궁게도, 우리는  $a + b\sqrt{2}$ 를  $(a, b)$ 로 보냄으로써 이것을  $\mathbb{Q}^2$ 에 매장하려 할 수 있습니다. 하지만 이는 조금 어리석은데, 어떤 의미에서  $\mathbb{R}$  안에 살면서 "일차원적"인  $K$ 를 무례하게 이차원 공간으로 만들어 버리기 때문입니다. 또한 이는 우리가 좋아하지 않는, 기저의 선택에 의존합니다. 더 나은 방법은 항등사상과 켤레, 즉 두 개의 매장  $\sigma_1: K \rightarrow \mathbb{C}$ 와  $\sigma_2: K \rightarrow \mathbb{C}$ 가 존재한다는 사실을 생각하는 것입니다:

$$\begin{aligned}\sigma_1(a + b\sqrt{2}) &= a + b\sqrt{2} \\ \sigma_2(a + b\sqrt{2}) &= a - b\sqrt{2}.\end{aligned}$$

다행히도 이 두 매장은 모두 실수 상(image)을 가집니다. 이로부터 우리는 다음과 같은 점들의 집합을 생각하게 됩니다

$$(\sigma_1(\alpha), \sigma_2(\alpha)) \in \mathbb{R}^2 \quad \text{로써} \quad \alpha \in K.$$

이를 통해  $\mathcal{O}_K$ 가  $\mathbb{R}^2$ 에서 어떤 모습인지 시각화할 수 있습니다.  $K$ 의 점들은  $\mathbb{R}^2$ 에서 조밀하지만,  $\mathcal{O}_K$ 의 점들은 격자를 이룹니다.



격자가 얼마나 큰지 알아보기 위해,  $\mathcal{O}_K$ 의 생성원인  $\{1, \sqrt{2}\}$ 가 어떻게 작용하는지 살펴봅시다. 격자에서  $a + b\sqrt{2}$ 에 대응하는 점은

$$a \cdot (1, 1) + b \cdot (\sqrt{2}, -\sqrt{2}).$$

격자의 **메시**<sup>1</sup>는 위에서 파란색으로 칠한 "기본 평행육면체"의 초부피로 정의됩니다. 이 특정한 경우, 이것은 그 평행사변형의 넓이와 같아야 하며, 그 값은

$$\det \begin{bmatrix} 1 & -\sqrt{2} \\ 1 & \sqrt{2} \end{bmatrix} = 2\sqrt{2}.$$

판별식의 정의는 정확히 이것이지만, 여기에 제곱 인자가 추가됩니다(위 행렬에서 행의 치환이 부호 변화를 일으킬 수 있기 때문입니다). **문제 57B\***는 제곱을 취함으로써  $\Delta_K$ 가 정수가 됨을 보여줍니다.

다음 정의를 내리기 위해, 우리는 다음을 인용합니다:

#### 정리 56.2.1 (대수체의 $n$ 개의 매장)

$K$ 를 차수가  $n$ 인 대수체라고 합시다. 그러면  $\mathbb{Q}$ 를 고정하는 체 준동형사상  $K \hookrightarrow \mathbb{C}$ 가 정확히  $n$ 개 존재하며, 이를  $\sigma_1, \dots, \sigma_n$ 이라고 합시다.

증명. 갈루아 이론의 도구를 갖춘 뒤, **정리 59.3.1**로 미룹니다. □

실제로 **정리 59.3.4**에서,  $\alpha \in K$ 에 대해  $i = 1, \dots, n$ 일 때  $\sigma_i(\alpha)$ 가  $\alpha$ 의 켤레들을 모두 훑는다는 것을 보게 됩니다. 이로부터 다음이 성립합니다

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha) \quad \text{그리고} \quad N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha).$$

이를 통해 우리는 다음과 같이 정의할 수 있습니다:

<sup>1</sup>대부분의 저자는 이것을 부피라고 부르지만, 나는 이것이 올바른 용어가 아니라고 생각합니다 – 격자는 그저 점들의 모음이므로 "부피"가 0입니다! 반면 영어 단어 "mesh"는 실제로 "틈"의 폭을 가리킵니다.

**정의 56.2.2.**  $\alpha_1, \dots, \alpha_n$ 이  $\mathcal{O}_K$ 의  $\mathbb{Z}$ -기저라고 합시다. 대수체  $K$ 의 **판별식**은 다음과 같이 정의됩니다

$$\Delta_K := \det \begin{bmatrix} \sigma_1(\alpha_1) & \dots & \sigma_n(\alpha_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \dots & \sigma_n(\alpha_n) \end{bmatrix}^2.$$

이것은  $\{\alpha_i\}$ 의 선택에 의존하지 않습니다; 여기서는 이를 증명하지 않겠습니다.

**예제 56.2.3** ( $K = \mathbb{Q}(\sqrt{2})$ 의 판별식)

$\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ 이며, 위에서 논의한 바와 같이 판별식은

$$\Delta_K = (-2\sqrt{2})^2 = 8.$$

**예제 56.2.4** ( $\mathbb{Q}(i)$ 의 판별식)

$K = \mathbb{Q}(i)$ 라고 합시다.  $\mathcal{O}_K = \mathbb{Z}[i] = \mathbb{Z} \oplus i\mathbb{Z}$ 입니다. 매장은 항등사상과 복소켈레이며, 1을  $(1, 1)$ 로,  $i$ 를  $(i, -i)$ 로 보냅니다. 따라서

$$\Delta_K = \det \begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix}^2 = (-2i)^2 = -4.$$

이 예는 복소평면으로 들어가는 대수체의 경우 판별식이 양수일 필요가 없음을 보여줍니다(격자 그림은 덜 완벽한 비유가 됩니다). 하지만 다시, 문제에서 증명하게 되듯이 판별식은 항상 정수입니다.

**예제 56.2.5** ( $\mathbb{Q}(\sqrt{5})$ 의 판별식)

$K = \mathbb{Q}(\sqrt{5})$ 라고 합시다. 이번에는  $\mathcal{O}_K = \mathbb{Z} \oplus \frac{1+\sqrt{5}}{2}\mathbb{Z}$ 이므로, 판별식은 조금 다르게 보일 것입니다. 매장은 여전히  $a + b\sqrt{5} \mapsto a + b\sqrt{5}, a - b\sqrt{5}$ 입니다.

이를  $\mathbb{Z}$ -기저  $\{1, \frac{1+\sqrt{5}}{2}\}$ 에 적용하면, 다음을 얻습니다

$$\Delta_K = \det \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{bmatrix}^2 = (-\sqrt{5})^2 = 5.$$

**연습문제 56.2.6.** 이를 모두 확장하여,  $d \neq 1$ 이 제곱인수가 없는 정수일 때  $K = \mathbb{Q}(\sqrt{d})$ 이면 다음이 성립함을 보이십시오

$$\Delta_K = \begin{cases} d & \text{만약 } d \equiv 1 \pmod{4} \\ 4d & \text{만약 } d \equiv 2, 3 \pmod{4}. \end{cases}$$

사실, 흥미로운 점을 하나 지적하고자 합니다:  $Ax^2 + Bx + C$ 의 다항식 판별식이  $B^2 - 4AC$ 임을 상기하십시오. 그러면:

- $d \equiv 1 \pmod{4}$ 인 경우,  $\Delta_K$ 는  $x^2 - x - \frac{d-1}{4}$ 의 판별식이며, 이는  $\frac{1}{2}(1 + \sqrt{d})$ 의 최소다항식입니다. 물론  $\mathcal{O}_K = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{d})]$ 입니다.
- $d \equiv 2, 3 \pmod{4}$ 인 경우,  $\Delta_K$ 는  $x^2 - d$ 의 판별식이며, 이는  $\sqrt{d}$ 의 최소다항식입니다.

이번에도 마찬가지로  $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ 입니다.

이는 우연이 아닙니다! **문제 57C\***는 이것이 일반적으로 참임을 주장하며, 따라서 "판별식"이라는 이름이 붙었습니다.

### §56.3 수체의 시그니처

**이 절의 대표적인 예:**  $\mathbb{Q}(\sqrt[100]{2})$ 의 시그니처는  $(2, 49)$ 입니다.

$K = \mathbb{Q}(i)$ 의 예에서, 우리는 대체로  $K$ 를 공간  $\mathbb{C}$ 에 매입했습니다. 그러나  $K$ 는 2차 확대이므로, 우리가 정말로 하고 싶은 것은 이를  $\mathbb{R}^2$ 에 매입하는 것입니다. 이를 위해 복소켈레를 활용하려고 합니다.

$K$ 를 수체라 하고  $\sigma_1, \dots, \sigma_n$ 을 그 매입들이라 합시다. 우리는 **실 매입**(전체  $K$ 를  $\mathbb{R}$ 로 보내는 것)과 **복소 매입**( $K$ 의 일부를  $\mathbb{R}$  밖으로 보내는 것)을 구별합니다.  $\sigma$ 가 복소 매입이면 그 켤레  $\bar{\sigma} \neq \sigma$  역시 복소 매입임에 주목하십시오. 따라서 복소 매입은 쌍으로 나타납니다.

**정의 56.3.1.**  $K$ 를 차수  $n$ 인 수체라 하고, 다음과 같이 둡시다

$$r_1 = \text{실 매장의 개수}$$

$$r_2 = \text{복소 매장 쌍의 개수.}$$

$K$ 의 **시그니처**는 순서쌍  $(r_1, r_2)$ 입니다.  $r_1 + 2r_2 = n$ 임을 관찰하십시오.

#### 예제 56.3.2 (시그니처의 기본 예시)

(a)  $\mathbb{Q}$ 의 시그니처는  $(1, 0)$ 입니다.

(b)  $\mathbb{Q}(\sqrt{2})$ 의 시그니처는  $(2, 0)$ 입니다.

(c)  $\mathbb{Q}(i)$ 의 시그니처는  $(0, 1)$ 입니다.

(d)  $K = \mathbb{Q}(\sqrt[3]{2})$ 라 하고,  $\omega$ 를 1의 세제곱근이라 합시다.  $K$ 의 원소들은 다음과 같습니다

$$K = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}.$$

그러면 시그니처는  $(1, 1)$ 인데, 세 매입이 다음과 같기 때문입니다

$$\sigma_1: \sqrt[3]{2} \mapsto \sqrt[3]{2}, \quad \sigma_2: \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega, \quad \sigma_3: \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2.$$

이 중 첫 번째는 실 매입이고 나머지 두 개는 켤레 쌍입니다.

#### 예제 56.3.3 (더 많은 시그니처)

같은 맥락으로  $\mathbb{Q}(\sqrt[99]{2})$ 와  $\mathbb{Q}(\sqrt[100]{2})$ 는 각각 시그니처  $(1, 49)$ 와  $(2, 49)$ 를 가집니다.

**질문 56.3.4.** 위의 두 수체의 시그니처를 검증하십시오.

지금부터, 우리는  $K$ 의 매입들에 다음과 같이 번호를 매길 것입니다.

$$\sigma_1, \sigma_2, \dots, \sigma_{r_1}$$

은 실 매입이고, 한편

$$\sigma_{r_1+1} = \overline{\sigma_{r_1+2r_2+1}}, \quad \sigma_{r_1+2} = \overline{\sigma_{r_1+2r_2+2}}, \quad \dots, \quad \sigma_{r_1+r_2} = \overline{\sigma_{r_1+2r_2}}.$$

은  $r_2$ 개의 복소 매입 쌍입니다. 우리는  $K$ 의 **정준 매입**을 다음과 같이 정의합니다

$$K \xhookrightarrow{\ell} \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \quad \text{에 의해} \quad \alpha \mapsto (\sigma_1(\alpha), \dots, \sigma_{r_1}(\alpha), \sigma_{r_1+1}(\alpha), \dots, \sigma_{r_1+r_2}(\alpha)).$$

우리가 한 일은 복소인 경우 각 켤레 쌍에서 두 번째 매입을 생략한 것뿐입니다. 이는 별일 아닌데, 이들은 단지 켤레일 뿐이므로 위의 튜플이 우리가 필요로 하는 모든 정보이기 때문입니다.

잠시 후 명확해질 이유로,  $\tau$ 가 다음 동형사상을 나타내도록 하겠습니다

$$\tau: \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \xrightarrow{\sim} \mathbb{R}^{r_1+2r_2} = \mathbb{R}^n$$

각 복소수를 실수부와 허수부로 나눔으로써, 다음과 같이

$$\begin{aligned} \alpha \mapsto & (\sigma_1(\alpha), \dots, \sigma_{r_1}(\alpha), \\ & \operatorname{Re} \sigma_{r_1+1}(\alpha), \operatorname{Im} \sigma_{r_1+1}(\alpha), \\ & \operatorname{Re} \sigma_{r_1+2}(\alpha), \operatorname{Im} \sigma_{r_1+2}(\alpha), \\ & \dots, \\ & \operatorname{Re} \sigma_{r_1+r_2}(\alpha), \operatorname{Im} \sigma_{r_1+r_2}(\alpha)). \end{aligned}$$

#### 예제 56.3.5 (정준 매입의 예시)

전과 같이  $K = \mathbb{Q}(\sqrt[3]{2})$ 라 하고 다음과 같이 둡시다

$$\sigma_1: \sqrt[3]{2} \mapsto \sqrt[3]{2}, \quad \sigma_2: \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega, \quad \sigma_3: \sqrt[3]{2} \mapsto \sqrt[3]{2}\omega^2$$

여기서  $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ 이며, 우리가 이미 지표를  $\sigma_1 = \operatorname{id}$ 이 실수이고  $\sigma_2$ 와  $\sigma_3$ 가 켤레 쌍이 되도록 배열했다는 점에 유의하십시오. 따라서 매장  $K \xhookrightarrow{\ell} \mathbb{R} \times \mathbb{C} \xrightarrow{\sim} \mathbb{R}^3$ 은 다음과 같이 주어집니다

$$\alpha \xhookrightarrow{\ell} (\sigma_1(\alpha), \sigma_2(\alpha)) \xrightarrow{\tau} (\sigma_1(\alpha), \operatorname{Re} \sigma_2(\alpha), \operatorname{Im} \sigma_2(\alpha)).$$

구체적으로,  $\alpha = 9 + \sqrt[3]{2}$ 로 두면 다음을 얻습니다

$$\begin{aligned} 9 + \sqrt[3]{2} & \xhookrightarrow{\ell} (9 + \sqrt[3]{2}, 9 + \sqrt[3]{2}\omega) \\ & = \left( 9 + \sqrt[3]{2}, 9 - \frac{1}{2}\sqrt[3]{2} + \frac{\sqrt[6]{108}}{2}i \right) \in \mathbb{R} \times \mathbb{C} \\ & \xrightarrow{\tau} \left( 9 + \sqrt[3]{2}, 9 - \frac{1}{2}\sqrt[3]{2}, \frac{\sqrt[6]{108}}{2} \right) \in \mathbb{R}^3. \end{aligned}$$

이제, 이 모든 것의 핵심은 우리가  $\mathcal{O}_K$ 를 취할 때 생기는 격자를 살펴보고자 한다는 것입니다. 실제로 다음이 성립합니다:

#### 보조정리 56.3.6

매장  $K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \xrightarrow{\sim} \mathbb{R}^n$ 의 합성을 생각해 봅시다. 그러면 앞서와 마찬가지로  $\mathcal{O}_K$ 는  $\mathbb{R}^n$  안의 격자  $L$ 이 되며, 그 메시는 다음과 같습니다

$$\frac{1}{2^{r_2}} \sqrt{|\Delta_K|}.$$

증명. 재미있는 선형대수 문제입니다(행렬식을 다룰 줄만 알면 됩니다). 문제 56D로 남겨둡니다.  $\square$

이로부터 다음을 유도할 수 있습니다:

### 보조정리 56.3.7

매장  $K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \xrightarrow{\sim} \mathbb{R}^n$ 의 합성을 생각해 봅시다.  $\mathfrak{a}$ 를  $\mathcal{O}_K$ 의 아이디얼이라 합시다. 그러면  $\mathfrak{a}$ 의 상은  $\mathbb{R}^n$  안의 격자  $L_{\mathfrak{a}}$ 가 되며, 그 메시는 다음과 같습니다

$$\frac{N(\mathfrak{a})}{2^{r_2}} \sqrt{|\Delta_K|}.$$

증명 스케치.

$$d = N(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}|.$$

라고 합시다. 그러면 격자  $L_{\mathfrak{a}}$ 에서는 어찌 보면 격자  $L$ 에 나타나는 점들 중  $\frac{1}{d}$ 만을 취하게 되는데, 이것이 바로 넓이가  $N(\mathfrak{a})$ 배만큼 커지는 이유입니다. 이를 모두 엄밀하게 다루려면 이 장에서 할애할 수 있는 지면보다 훨씬 더 많은 격자와 기하학 내용이 필요하므로, 세부 사항은 생략하겠습니다. 하지만 이것이 직관적으로 왜 참인지는 이해하시리라 생각합니다.  $\square$

## §56.4 민코프스키 정리

이제 제가 왜  $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ 에서  $\mathbb{R}^n$ 으로 옮겨 갈 것을 고집했는지 말씀드릴 수 있습니다. 기하학에는 다음과 같은 정말 멋진 민코프스키의 정리가 있습니다.

### 정리 56.4.1 (민코프스키)

$S \subseteq \mathbb{R}^n$ 을 0을 포함하며 중심 대칭인(즉,  $x \in S \iff -x \in S$ 인) 볼록집합이라 합시다.  $L$ 을 메시가  $d$ 인 격자라 합시다. 만약

- (a)  $S$ 의 부피가  $2^n d$ 를 초과하거나,
- (b)  $S$ 의 부피가  $2^n d$ 와 같고  $S$ 가 콤팩트하면,

$S$ 는  $L$ 의 0이 아닌 격자점을 포함합니다.

**질문 56.4.2.** 조건  $0 \in S$ 가 사실상 불필요함을, 즉 공집합이 아닌 임의의 볼록·중심 대칭 집합은 원점을 포함함을 보이십시오.

증명 스케치. (a) 부분은 놀랍도록 간단하며 매우 올림피아드스러운 풀이를 가지고 있습니다: 본질적으로 넓이에 대한 비둘기집 원리입니다. 간단히 하기 위해 특수한 경우  $n = 2$ ,  $L = \mathbb{Z}^2$ 에 대해 (a) 부분을 증명하겠습니다. 이 증명은 임의의 격자와 임의의  $n$ 으로 쉽게 일반화될 수 있습니다. 따라서 넓이가 4보다 큰 그러한 볼록집합  $S$ 는 격자점을 포함함을 보이고자 합니다.

평면을  $2 \times 2$  정사각형들로 분할합니다

$$[2a - 1, 2a + 1] \times [2b - 1, 2b + 1]$$

그리고 이 모든 정사각형들을 서로 겹쳐 놓습니다. 비둘기집 원리에 의해, 같은 점으로 대응되는 서로 다른 두 점  $p \neq q \in S$ 가 존재함을 알 수 있습니다.  $S$ 가 대칭이므로  $-q \in S$ 입니다. 그러면  $\frac{1}{2}(p - q) \in S$ 이고(볼록성에 의해), 이는 0이 아닌 격자점입니다.

(b) 부분을 간단히 스케치해 보겠습니다: 아이디어는  $\varepsilon > 0$ 에 대해  $(1 + \varepsilon)S$ (이는 " $S$ 를 작은 배율  $1 + \varepsilon$ 만큼 확대한 것")를 고려하는 것입니다. 이는 조건 (a)를 만족합니다. 따라서 각  $\varepsilon > 0$ 에 대해  $(1 + \varepsilon)S$  안의 0이 아닌 격자점들의 집합, 이를  $S_\varepsilon$ 라 하면, 이는 (이산적인) 점들의 유한한 공집합이 아닌 집합입니다("유한"이라는 부분은  $(1 + \varepsilon)S$ 가 유계라는 사실로부터 따라옵니다). 따라서 모든  $\varepsilon > 0$ 에 대해  $S_\varepsilon$ 에 속하는 어떤 점이 존재해야 하며(왜 그럴까요?), 이는 그 점이  $S$ 에 속함을 함의합니다.  $\square$

## §56.5 합정 상자

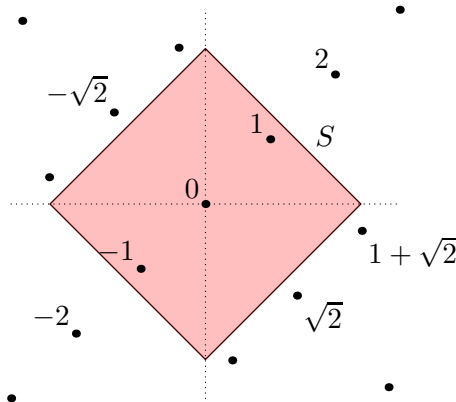
우리에게 필요한 마지막 재료는 민코프스키 정리를 적용할 집합입니다. 다음을 제안합니다:

**정의 56.5.1.**  $M$ 을 양의 실수라 합시다.  $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ 에서, 다음 조건을 만족하는 점  $(x_1, \dots, x_{r_1}, z_1, \dots, z_{r_2})$ 들의 집합으로 상자  $S$ 를 정의합니다

$$\sum_{i=1}^{r_1} |x_i| + 2 \sum_{j=1}^{r_2} |z_j| \leq M.$$

이는  $M$ 의 값에 따라 달라진다는 점에 유의하십시오.

이 상자를 쥐뿔이라고 생각해 보십시오: 여기에 빠지는 것은 무엇이든 노름이 작을 것이고, 우리의 목표는 민코프스키를 이용해 0이 아닌 어떤 원소를 그 안으로 유인하는 것입니다.



즉,  $\alpha \in \mathfrak{a}$ 가 위에서 정의한 상자 안에 빠진다고 가정하면, 이는 다음을 의미합니다

$$M \geq \sum_{i=1}^{r_1} |\sigma_i(\alpha)| + 2 \sum_{i=r_1+1}^{r_1+r_2} |\sigma_i(\alpha)| = \sum_{i=1}^n |\sigma_i(\alpha)|,$$

여기서 마지막 몇 개의  $\sigma$ 들이 켈레쌍으로 나타난다는 점을 기억하고 있습니다. 이것은 대각합처럼 보이지만, 절댓값이 방해가 됩니다. 그래서 대신 AM-GM을 적용하여 다음을 얻습니다:

### 보조정리 56.5.2 (쥐뿔의 효과)

$\alpha \in \mathcal{O}_K$ 이고,  $\iota(\alpha)$ 가  $S$  안에 있다고 가정합시다 (여기서  $\iota: K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ 는 평소와 같습니다). 그러면

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^n |\sigma_i(\alpha)| \leq \left(\frac{M}{n}\right)^n.$$

마지막으로 해야 할 단계는 상자의 부피를 계산하는 것입니다. 이 역시 제가 직접 하지는 않을 기하학이지만, 제 말을 믿어주십시오:

### 보조정리 56.5.3 (쥐뿔의 크기)

앞서와 같이  $\tau: \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \xrightarrow{\sim} \mathbb{R}^n$ 이라 합시다. 그러면  $\tau$ 에 의한  $S$ 의 상은 볼록하고, 콤팩트하며, 중심 대칭인 집합으로, 그 부피는 다음과 같습니다

$$2^{r_1} \cdot \left(\frac{\pi}{2}\right)^{r_2} \cdot \frac{M^n}{n!}.$$

**질문 56.5.4.** (건전성 검사)  $n = 2$ 일 때 가능한 시그니처인  $(r_1, r_2) = (2, 0)$ 과  $(r_1, r_2) = (0, 1)$ 에 대해 위 내용이 맞는지 확인하십시오.

## §56.6 민코프스키 경계

이제 지금까지의 모든 것을 종합하여 위대한 민코프스키 경계를 얻을 수 있습니다.

### 정리 56.6.1 (민코프스키 경계)

$\mathfrak{a} \subseteq \mathcal{O}_K$ 를 0이 아닌 임의의 아이디얼이라 합시다. 그러면 다음을 만족하는  $0 \neq \alpha \in \mathfrak{a}$ 가 존재합니다

$$N_{K/\mathbb{Q}}(\alpha) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|\Delta_K|} \cdot N(\mathfrak{a}).$$

**증명.** 이는 우리가 가진 모든 재료를 한데 모으는 문제입니다. 이미 정의한 것들을 살펴봅시다:

$$K \xhookrightarrow{\iota} \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \xrightarrow{\tau} \mathbb{R}^n$$

$$\text{box } S \longmapsto \tau^{\text{img}}(S) \quad \text{with volume } 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{M^n}{n!}$$

$$\mathcal{O}_K \longmapsto \text{Lattice } L \quad \text{with mesh } 2^{-r_2} \sqrt{|\Delta_K|}$$

$$\mathfrak{a} \longmapsto \text{Lattice } L_{\mathfrak{a}} \quad \text{with mesh } 2^{-r_2} \sqrt{|\Delta_K|} N(\mathfrak{a})$$

$L_{\mathfrak{a}}$ 의 메시(mesh)가 상자 부피의  $2^{-n}$ 과 같아지도록  $M$ 의 값을 선택하십시오. 그러면 민코프스키 정리에 의해 어떤  $0 \neq \alpha \in \mathfrak{a}$ 가 상자 안에 들어가게 됩니다 — 쥐뿔은  $N_{K/\mathbb{Q}}(\alpha) \leq \frac{1}{n^n} M^n$ 을 강제하도록 설정되어 있습니다.  $M$ 의 올바른 선택은

$$M^n = M^n \cdot 2^n \cdot \frac{\text{메시}}{\text{vol box}} = 2^n \cdot \frac{n!}{2^{r_1} \cdot \left(\frac{\pi}{2}\right)^{r_2}} \cdot 2^{-r_2} \sqrt{|\Delta_K|} N(\mathfrak{a})$$

이는 약간의 계산을 거치면 그 경계를 줍니다. □

## §56.7 유수군은 유한합니다

**정의 56.7.1.** 간결함을 위해  $M_K = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|\Delta_K|}$ 라 합시다. 이는  $K$ 에 의존하는 상수라는 점에 유의하십시오.

그것도 멋지긴 하지만, 우리가 정말 보이고 싶었던 것은 유수군이 유한하다는 것이었습니다. 민코프스키 경계가 어떻게 도움이 될 수 있을까요? 핵심 아이디어는 다음과 같습니다:

**$\alpha$ 의 유수는  $(\alpha) \cdot \mathfrak{a}^{-1}$ 에 의해 전적으로 결정됩니다.**

**질문 56.7.2.** 이를 확인하십시오. (즉,  $\mathfrak{a}$ 와  $\mathfrak{b}$ 가 어떤  $\alpha \in \mathfrak{a}, \beta \in \mathfrak{b}$ 에 대해  $(\alpha) \cdot \mathfrak{a}^{-1} = (\beta) \cdot \mathfrak{b}^{-1}$ 를 만족한다면, 어떤  $\gamma \in K$ 에 대해  $\mathfrak{a} = (\gamma)\mathfrak{b}$ 임을 증명하십시오.)

### 예제 56.7.3

이 예제를 떠올려 보십시오:

$$(6) = (2, 1 - \sqrt{-5})^2 (3, 1 + \sqrt{-5}) (3, 1 - \sqrt{-5}) = \mathfrak{p}^2 \mathfrak{q}_1 \mathfrak{q}_2.$$

$\mathfrak{a} = (2)$ 가 주 아이디얼인 경우를 생각해 봅시다.  $\alpha = 2$ 를 택하면  $(\alpha) \cdot \mathfrak{a}^{-1} = (1)$ 입니다.  $(\alpha) \cdot \mathfrak{a}^{-1} = (1)$  (또는  $(2)$ , 또는 주 아이디얼인 무엇이든)이면,  $\mathfrak{a}$ 가 반드시 주 아이디얼이어야 함을 알 수 있습니다.

반면,  $\mathfrak{q}_1 = (3, 1 + \sqrt{-5})$ 는 주 아이디얼이 아니며,  $\alpha = 3$ 을 택합니다.  $(3) = \mathfrak{q}_1 \mathfrak{q}_2$ 임을 알고 있으므로,  $(\alpha) \cdot \mathfrak{q}_1^{-1} = \mathfrak{q}_2 \neq (1)$ 입니다.

위 두 예시 모두에서  $\mathfrak{a} \mid (\alpha)$ 이므로, 그 몫은 “정수”여야 합니다. 실제로:

**질문 56.7.4.**  $(\alpha) \cdot \mathfrak{a}^{-1}$ 가 정수 아이디얼임을 보이십시오. (정의를 풀어 쓰십시오.)

민코프스키 경계를 다시 써서 다음과 같이 말할 수 있음을 눈치챌 수도 있습니다

$$N((\alpha) \cdot \mathfrak{a}^{-1}) \leq M_K$$

여기서  $M_K$ 는  $K$ 에 의존하는 어떤 상수입니다.

이 진술은 유용한데, 실제로 노름이  $\leq M_K$ 인 정수 아이디얼은 유한히 많기 때문입니다.

### 따름정리 56.7.5 (유군의 유한성)

유군은 항상 유한합니다.

**증명.** 위와 같은 정수 아이디얼이 유한히 많다는 것만 보이면 되며, 이는 류가 유한히 많다는 것을 의미합니다.

그런 아이디얼  $\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_m^{e_m}$ 을 만들고 싶다고 합시다. 소 아이디얼  $\mathfrak{p}_i$ 는 그 안에 어떤 유리 소수  $p$ 를 가져야 함을 상기하십시오. 이는  $\mathfrak{p}_i$ 가  $(p)$ 를 나누고  $p$ 가  $N(\mathfrak{p}_i)$ 를 나눈다는 것을 의미합니다. 그러므로  $\mathfrak{a}$ 를 만들기 위해 사용할 모든  $\mathfrak{p}_i$ 를 그것들이 어느  $(p)$ 에서 왔는지에 따라 묶어봅시다.

$$\begin{array}{cccc}
 (2) & (3) & (5) & \dots \\
 \vdots & \vdots & \vdots & \\
 \vdots & \vdots & \vdots & \\
 \vdots & \vdots & \vdots & 
 \end{array}$$

좀 더 극적으로 표현하자면: 여러분에게 체리나무가 있다고 상상해 보십시오. 각 가지는 소수  $(p)$ 에 대응하며,  $(p)$ 의 인수들(유한히 많음)을 체리(소 아이디얼)로서 담고 있습니다. 여러분의 바구니(만들고 있는 아이디얼  $\mathfrak{a}$ )는 총 무게(노름)  $M_K$ 만큼만 담을 수 있습니다. 그러므로  $M_K$ 보다 높은 가지에는 손도 댈 수 없습니다. 체리를 중복해서 담을 수는 있지만 (이런), 가지  $(p)$ 에 달린 체리의 무게는 반드시  $\geq p$ 이므로, 이 모든 것은  $\mathfrak{a}$ 를 만드는 방법의 수가 유한함을 의미합니다.  $\square$

## §56.8 유수의 계산

**정의 56.8.1.**  $\text{Cl}_K$ 의 위수를  $K$ 의 **유수**라고 부릅니다.

**비고 56.8.2** — 만약  $\text{Cl}_K = 1$ 이면,  $\mathcal{O}_K$ 는 PID이며 따라서 UFD입니다.

$M_K$ 의 실제 값을 계산함으로써, 우리는 앞선 증명에서 언급한 “체리나무” 전체를 말 그대로 만들어 낼 수 있습니다. 어떻게 하는지 예를 들어봅시다!

### 명제 56.8.3

체  $\mathbb{Q}(\sqrt{-67})$ 의 유수는 1입니다.

**증명.**  $K = \mathbb{Q}(\sqrt{-67})$ 의 부호수가  $(0, 1)$ 이고 판별식이  $\Delta_K = -67$ 이므로  $(-67 \equiv 1 \pmod{4})$ 이기 때문에, 우리는 다음을 계산할 수 있습니다

$$M_K = \left(\frac{4}{\pi}\right)^1 \cdot \frac{2!}{2^2} \sqrt{67} \approx 5.2.$$

이는 (2), (3), (5) 이후로 체리나무를 잘라낼 수 있음을 의미하는데, 이 가지들 위의 체리들은 반드시 노름이  $\geq M_K$ 이기 때문입니다. 이제 이것들 각각을  $\mathcal{O}_K = \mathbb{Z}[\theta]$ 에서 인수분해하고자 하는데, 여기서  $\theta = \frac{1+\sqrt{-67}}{2}$ 는 최소다항식  $x^2 - x + 17$ 을 갖습니다. 그런데 놀라운 일이 일어납니다:

- $x^2 - x + 17 \pmod{2}$ 를 줄여보면, 기약다항식  $x^2 - x + 1$ 을 얻습니다. 인수분해 알고리즘(**정리 55.5.4**)에 의해 이는 (2)가 소 아이디얼임을 의미합니다.
- 마찬가지로, 법 3으로 줄이면  $x^2 - x + 2$ 를 얻는데, 이는 기약다항식입니다. 이는 (3)이 소 아이디얼임을 의미합니다.
- 마지막으로, 같은 이유로 (5)는 소 아이디얼입니다.

오늘은 운이 좋은 날입니다. 아이디얼 (2), (3), (5) 모두 소 아이디얼(이미 주 아이디얼)입니다. 다르게 말하면, 세 가지 각각에는 오직 하나의 (큰) 체리만 달려 있습니다. 이는 노름이  $\leq M_K$ 인 정수 아이디얼을 만들 때마다 그것이 실제로 주 아이디얼임을 의미합니다. 사실, 이들은 각각 노름 4, 9, 25를 가지므로... (3)과 (5)에는 손도 댈 수 없고, 얻을 수 있는 아이디얼은 (노름 1과 4를 갖는) (1)과 (2)뿐입니다.

이제 우리는 이것이 전부라고 주장합니다.  $N(\mathfrak{b}) \leq M_K$ 인 정수 아이디얼  $\mathfrak{b}$ 가 있다고 합시다. 위의 논의에 의해,  $\mathfrak{b} = (1)$ 이거나  $\mathfrak{b} = (2)$ 이며, 둘 다 주 아이디얼이므로  $\text{Cl}_K$ 에서 자명합니다. 그러므로 필요한 대로  $J$  역시  $\text{Cl}_K$ 에서 자명합니다.  $\square$

몇 개 더 해봅시다.

**정리 56.8.4** (가우스 정수  $\mathbb{Z}[i]$ 는 UFD를 이룹니다)

체  $\mathbb{Q}(i)$ 의 유수는 1입니다.

증명. 이것은  $K = \mathbb{Q}(i)$ 일 때의  $\mathcal{O}_K$ 이므로, 우리는 그저  $\text{Cl}_K$ 가 자명하기를 원합니다.  $M_K = \frac{2}{\pi}\sqrt{4} < 2$ 입니다. 따라서 모든 류는 다음을 만족하는 노름  $\mathfrak{b}$ 의 정수 아이디얼을 가집니다

$$N(\mathfrak{b}) \leq \left(\frac{4}{\pi}\right)^1 \cdot \frac{2!}{2^2} \cdot \sqrt{4} = \frac{4}{\pi} < 2.$$

흠, 그건 시시합니다: 우리는 고를 가지가 아예 없습니다. 다시 말해,  $\mathfrak{b} = (1)$ 일 수밖에 없습니다.  $\square$

여전히 유일 인수분해로 밝혀지는 또 다른 예가 있습니다만, 이번에는 우리의 뱃나무에 실제로 딸 수 있는 벚꽃이 열릴 것입니다.

**명제 56.8.5** ( $\mathbb{Z}[\sqrt{7}]$ 는 UFD입니다)

체  $\mathbb{Q}(\sqrt{7})$ 의 유수는 1입니다.

증명. 먼저 민코프스키 경계를 계산합니다.

**질문 56.8.6.**  $M_K \approx 2.646$ 임을 확인하십시오.

그러므로 이번에는 유일한 가지는 (2)입니다. 평소처럼 (2)를 인수분해해 봅시다: 다항식  $x^2 + 7$ 은  $(x-1)(x+1) \pmod{2}$ 로 축약되므로

$$(2) = (2, \sqrt{7} - 1)(2, \sqrt{7} + 1).$$

이런! 이제 우리는 두 개의 체리를 가지게 되었고, 둘 다 그럴듯해 보입니다. 하지만 실제로는 다음이 성립한다고 주장합니다

$$(2, \sqrt{7} - 1) = (3 - \sqrt{7}).$$

**질문 56.8.7.** 이를 증명하십시오.

그러므로 두 체리 모두 주 아이디얼이며, 앞서와 마찬가지로  $\text{Cl}_K$ 가 자명하다고 결론지을 수 있습니다. 다만 이번에는 소 아이디얼 (2)가 실제로 분해된다는 점에 유의하십시오. 두 체리가 주 아이디얼이었던 것은 운이 좋았던 것이며, 이런 방식이 항상 통하지는 않습니다.  $\square$

자명하지 않은 류군은 어떨까요? 먼저, 뱃나무에서의 작업을 줄여 나가는 데 도움이 될 보조정리를 하나 사용하겠습니다.

**보조정리 56.8.8** (아이디얼은 자신의 노름을 나눕니다)

$N(\mathfrak{b}) = n$ 인 정수 아이디얼  $\mathfrak{b}$ 가 있다고 합시다. 그러면  $\mathfrak{b}$ 는 아이디얼  $(n)$ 을 나눕니다.

증명. 정의에 의해  $n = |\mathcal{O}_K/\mathfrak{b}|$ 입니다.  $\mathcal{O}_K/\mathfrak{b}$ 를 (덧셈적) 아벨 군으로 취급하고 라그랑주 정리를 사용하면, 다음을 얻습니다

$$0 \equiv \underbrace{\alpha + \cdots + \alpha}_{n\text{곱하기}} = n\alpha \pmod{\mathfrak{b}} \quad \text{모든 } \alpha \in \mathcal{O}_K \text{에 대하여}$$

따라서  $(n) \subseteq \mathfrak{b}$ 이며, 증명이 끝났습니다.  $\square$

다른 방법으로, **장 59**를 읽으셨다면: 확장  $K/\mathbb{Q}$ 가 갈루아 확장인 경우, **비고 54.1.9**와 유사하게  $\prod_{\sigma \in \text{Gal}(K/\mathbb{Q})} \sigma(\mathfrak{b}) = (n)$ 임을 실제로 증명할 수 있으며, 이는 결과  $\mathfrak{b} \mid (n)$ 을 함의합니다.

이제 그러한 예를 하나 들어보겠습니다.

**명제 56.8.9** ( $\mathbb{Q}(\sqrt{-17})$ 의 이데알류군)

수체  $K = \mathbb{Q}(\sqrt{-17})$ 의 이데알류군은  $\mathbb{Z}/4\mathbb{Z}$ 입니다.

이 증명은 다소 지저분하므로, 전체를 상세히 읽으실 필요는 없습니다. 요점은 류군에서 자명하지 않은 체리가 몇 개 있다는 것입니다.

증명.  $\Delta_K = -68$ 이므로, 민코프스키 경계를 계산합니다

$$M_K = \frac{4}{\pi} \sqrt{17} < 6.$$

이제 (2), (3), (5)로 인수분해하는 것으로 충분합니다.  $\sqrt{-17}$ 의 최소다항식은  $x^2 + 17$ 이므로, 늘 하던 대로

$$\begin{aligned} (2) &= (2, \sqrt{-17} + 1)^2 \\ (3) &= (3, \sqrt{-17} - 1)(3, \sqrt{-17} + 1) \\ (5) &= (5) \end{aligned}$$

이는  $x^2 + 17$ 을 2, 3, 5 각각으로 나눈 나머지에 따른 인수분해에 대응합니다.  $\mathfrak{p} = (2, \sqrt{-17} + 1)$ 이라 하고,  $\mathfrak{q}_1 = (3, \sqrt{-17} - 1)$ ,  $\mathfrak{q}_2 = (3, \sqrt{-17} + 1)$ 이라 합시다. 다음을 계산할 수 있습니다

$$N(\mathfrak{p}) = 2 \quad \text{그리고} \quad N(\mathfrak{q}_1) = N(\mathfrak{q}_2) = 3.$$

특히 이들은 주 아이디얼이 아닙니다. 아이디얼 (5)는 논외입니다; 이는 노름이 25입니다. 따라서 세 체리는  $\mathfrak{p}$ ,  $\mathfrak{q}_1$ ,  $\mathfrak{q}_2$ 입니다.

노름  $\leq 5$  인 아이디얼로 이 체리들을 배열하는 가능한 방법은 다음과 같습니다

$$\{(1), \mathfrak{p}, \mathfrak{q}_1, \mathfrak{q}_2, \mathfrak{p}^2\}.$$

그러나

$$\mathfrak{p}^2 = (2)$$

임을 계산할 수 있으므로  $\mathfrak{p}^2$  와 (1) 은 같은 유수군에 속합니다. 즉, 이들은 자명합니다. 특히, 유수군은 위수가 최대 4 입니다.

지금부터  $[\mathfrak{a}]$  가  $\mathfrak{a}$  가 속한 클래스(유수군의 원소)를 나타내도록 합시다.  $\mathfrak{p}$  가 주 아이디얼이 아니므로  $[\mathfrak{p}] \neq [(1)]$ ,  $\mathfrak{p}$  는 위수가 2임이 따라옵니다. 따라서 라그랑주 정리에 의해  $\text{Cl}_K$  의 위수는 2 또는 4 입니다.

이제  $[\mathfrak{q}_1]^2 \neq [(1)]$  임을 주장하는데, 이는  $\mathfrak{q}_1$  이 2 보다 큰 위수를 가짐을 의미합니다. 그렇지 않다면,  $\mathfrak{q}_1^2$  은 주 아이디얼입니다.  $N(\mathfrak{q}_1) = 3$  임을 알고 있으므로, 이는 오직  $\mathfrak{q}_1^2 = (3)$

인 경우에만 일어날 수 있습니다. 이는  $q_1 = q_2$  를 강제합니다. 그러나  $q_1 + q_2 = (1)$  이므로 이는 불가능합니다.

따라서  $q_1$  은 2 보다 큰 짝수 위수를 가집니다. 그러므로 위수는 4 여야 합니다. 이로부터

$$\text{Cl}_K \cong \mathbb{Z}/4\mathbb{Z}. \quad \square$$

임을 유도할 수 있습니다.

**비고 56.8.10** — 하버드에서 Math 129 수업 중 이 작업을 했을 때, 학생들이 (농담 삼아)  $\frac{4}{\pi}\sqrt{17}$ 을 계산하는 어려움에 대해 불평하는 5분간의 소동이 있었습니다. 발췌:

“시험에 소형 계산기를 가져와도 됩니까?” – 학생 1  
 “크기가 무슨 상관입니까? 애플 위치를 가지고 있을 수도 있습니다” – 교수  
 “ $\pi \geq 3$ 이라는 사실을 그냥 이용하십시오” – 나  
 “[다른 교수]님도 그것을 모르는데, 저희가 어떻게 알겠습니까?” – 학생 2  
 “이것은 스스로 해야 합니다!” – 교수  
 “이것은 말도 안 됩니다.” – 학생 1

## §56.9 선택: $\mathcal{O}_K$ 가 자유 $\mathbb{Z}$ -가군임을 증명

이제 정리 54.2.12 을 증명할 적절한 도구를 갖추었습니다.

$\mathcal{O}_K$  가 환임을 알고 있으므로, 이는 당연히  $\mathbb{Z}$ -가군이여야 합니다. 이것이 차수  $n = [K : \mathbb{Q}]$  의 자유  $\mathbb{Z}$ -가군이 아니라고 가정해봅시다. 무엇이 잘못될 수 있을까요?

- 먼저,  $\mathbb{Q}$  나 환 확장  $\mathbb{Z}[\frac{1}{2}]$  처럼 조밀할 수 있으며(이는 유한 생성이 아니고 자유롭지도 않게 만듭니다), 이러한 경우가 발생할 수 있습니다.
- 그렇지 않더라도, 계수가  $n$  보다 작을 수 있습니다.

두 번째 가능성은 훨씬 쉽게 배제할 수 있습니다.  $\alpha_1, \dots, \alpha_n$  을  $K$  의 기저라고 합시다. 정리 54.2.6 을 이용하면,  $d_1\alpha_1, \dots, d_n\alpha_n \in \mathcal{O}_K$  가 되는 양의 정수  $d_1, \dots, d_n$  이 존재합니다.  $\alpha_1, \dots, \alpha_n$  이 선형독립이므로, 이는  $\text{rank } \mathcal{O}_K \geq n$  을 의미합니다.

반대 방향은 더 어렵습니다.  $\mathcal{O}_K$  가 어떤 의미에서 ”이산적”임을 증명하고자 합니다.

지금부터  $\alpha_i$  를  $d_i\alpha_i$  로 대체하면, 이들은 여전히  $\mathbb{Q}$ -벡터 공간  $K$  의 기저이면서, 더 나아가 이제  $\mathcal{O}_K$  에 속하게 됩니다.

세 가지 서로 다른 증명이 제시될 것입니다.

### §56.9.i 첫 번째 증명

$\mathcal{O}_K$  가 계수  $n$  인 어떤 자유  $\mathbb{Z}$ -가군에 포함됨을 보이겠습니다.

구체적으로, 어떤 정수  $d \neq 0$  에 대해  $\mathcal{O}_K \subseteq \langle \frac{1}{d}\alpha_1, \dots, \frac{1}{d}\alpha_n \rangle$  임을 보이겠습니다.

$\mathcal{O}_K$  가 계수  $n$  인 자유  $\mathbb{Z}$ -가군임을 이미 알고 있다고 가정해봅시다.  $d$  를 어떻게 계산할 수 있을까요?

**연습문제 56.9.1.** 다음은  $d$  를 계산하려는 몇 가지 소박한 시도들이지만, 안타깝게도 이들은 성립하지 않습니다.  $\langle 1, 1 + 2i \rangle \subseteq \mathbb{Z}[i]$  에서 이를 확인해보십시오.

- $d$  를  $\langle \alpha_1, \dots, \alpha_n \rangle$  에 속하는 첫 번째 양의 정수로 잡습니다. (정리 55.3.6 에서 영감을 받은 시도입니다.)
- $d$  를  $\alpha_1, \dots, \alpha_n$  의 노름의 곱으로 잡습니다.

대신, 격자의 메시를 계산하는 방식에서 영감을 받은 아이디어를 이용하여  $d$ 를 계산하겠습니다.  $A = \langle \alpha_1, \dots, \alpha_n \rangle$  이라 하면, 이는 격자이며 계수  $n$ 인 자유  $\mathbb{Z}$ -가군입니다.

**연습문제 56.9.2.**  $\mathcal{O}_K$ 가 계수  $n$ 의 자유 가군임을 이미 알고 있다고 가정합니다.  $|\mathcal{O}_K/A|$ 가 유한함을 보이십시오. 모든  $x \in \mathcal{O}_K$ 에 대해  $|\mathcal{O}_K/A| \cdot x \in A$ 임을 결론지으십시오.

**문제 57B\***와 동일한 논증을 사용하면,  $\alpha_1, \dots, \alpha_n$ 이 생성하는 격자의 "판별식"(제공 메시)이 정수임을 증명할 수 있습니다. 공식적으로, 다음과 같이 놓습니다:

$$d := \det \begin{bmatrix} \sigma_1(\alpha_1) & \dots & \sigma_n(\alpha_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \dots & \sigma_n(\alpha_n) \end{bmatrix}^2.$$

**연습문제 56.9.3.** (적어도 모든 매장이 실수인 경우에는)  $\mathcal{O}_K$ 와  $A$ 의 메시 비율이 정확히 몫 아벨 군  $\mathcal{O}_K/A$ 의 크기, 즉  $\left| \frac{d}{\Delta_K} \right| = |\mathcal{O}_K/A|^2$ 임을 스스로 납득해 보십시오. 모든  $x \in \mathcal{O}_K$ 에 대해  $d \cdot x \in A$ 임을 결론지으십시오.

이는  $\mathcal{O}_K \subseteq \langle \frac{1}{d}\alpha_1, \dots, \frac{1}{d}\alpha_n \rangle$ 을 함의하며, 이는 계수  $n$ 의 또 다른 자유  $\mathbb{Z}$ -가군입니다.

그러나 위 논증은  $\Delta_K$ 가 존재함을 가정하므로 순환 논법입니다(이는 값  $d$ 가 어디서 비롯되는지에 대한 동기 부여로만 사용될 수 있습니다). 실제 증명은 다음과 같습니다.

**문제 57B\***와 유사하게, 다음과 같이 정의합니다

$$d := \det[\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j)]_{i,j}.$$

그러면,  $\{\alpha_i\}_i$ 가  $K$ 를  $\mathbb{Q}$ -벡터 공간으로서 생성하므로, 다음을 만족하는 어떤  $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{Q}^{\oplus n}$

이 존재합니다

$$\begin{bmatrix} \alpha_1 & \dots & \alpha_n \end{bmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (x).$$

이는 다음을 의미합니다

$$\begin{bmatrix} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1 \alpha_1) & \dots & \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1 \alpha_n) \\ \vdots & \ddots & \vdots \\ \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_n \alpha_1) & \dots & \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_n \alpha_n) \end{bmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1 x) \\ \vdots \\ \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_n x) \end{pmatrix}.$$

즉, 간단히 말하면,

$$(\text{행렬식이 } d \text{인 어떤 행렬} \in \mathrm{Mat}_n(\mathbb{Z})) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (\text{어떤 벡터} \in \mathbb{Z}^{\oplus n}).$$

**질문 56.9.4.**  $d \cdot x \in A$ 라는 증명을 마무리하십시오. (크라메르 공식. 또는 수반행렬을 취하십시오.)

마지막으로,  $\mathcal{O}_K$ 가 계수  $n$ 의 두 자유  $\mathbb{Z}$ -가군 사이에 끼어 있으므로, 이 또한 계수  $n$ 의 자유 가군임을 얻습니다.<sup>2</sup>

<sup>2</sup>비고 55.3.7에서 유사한 작업을 한 바 있습니다.

**질문 56.9.5.** 이를 마무리하십시오. (정리 18.1.5을 여기서 사용할 수 있습니다.)

### §56.9.ii 두 번째 증명

이번에는  $d$ 로 나누는 대신, 쌍대 격자를 취합니다.

쌍대 격자란 무엇이며, 왜 이를 사용할 생각을 하게 될까요? 이 증명에 대한 동기를 부여하는 한 가지 방법은 아이디얼의 역원을 살펴보는 것입니다. 만약  $(1) \mid \mathfrak{a}$ 라면(즉  $\mathfrak{a}$ 가 정수 아이디얼이라면),  $\mathfrak{a}^{-1} \mid (1)$ 입니다.

여기서  $\mathfrak{a}^{-1} := \{x \in K \mid xa \in \mathcal{O}_K \text{ 모든 } a \in \mathfrak{a}\}$ 입니다.

이와 비슷한 것을 해볼 수 있다고 생각할 수 있는데, 다음을 고려하는 것입니다

$$\{x \in K \mid xa \in \mathcal{O}_K \text{ 모든 } a \in \langle \alpha_1, \dots, \alpha_n \rangle\}.$$

이 집합은 실제로 계수  $n$ 의 격자이지만, 이는 논증을 증명하는 데 통하지 않습니다! 우리는 애초에  $\mathcal{O}_K$ 가 "이산적"임을 증명하려는 것인데, 만약  $\mathcal{O}_K = K$ 라면 위의 집합 역시  $K$ 와 같아질 것입니다.

대신, 우리는 이미 알고 있는 것 — 즉  $\mathbb{Z}$ 의 이산성 — 에 의존해야 합니다. 다음과 같이 정의합니다

$$S := \{x \in K \mid \text{Tr}_{K/\mathbb{Q}}(xa) \in \mathbb{Z} \text{ 모든 } a \in \langle \alpha_1, \dots, \alpha_n \rangle\}.$$

이 집합은 이전 집합보다 조금 더 큼니다.

**질문 56.9.6.** 이 집합이 이전 집합의 상위집합임을 확인하십시오. 그런 다음  $\mathcal{O}_K \subseteq S$ 임을 결론지으십시오.

**연습문제 56.9.7.**  $\langle 1, 2i \rangle \subseteq \mathbb{Z}[i]$ 을 고려해 보십시오. 이때 집합  $S$ 는 무엇이 될까요? ( $\mathbb{C}$ 에서의 대각합은 실수부의 두 배임을 기억하십시오.)

$S$ 는 여전히 계수  $n$ 의 격자입니다 — 그리고 이번에는 실제로 이를 증명할 수 있습니다! 우리는 이미  $\mathbb{Z}$ 가 이산적임을 알고 있기 때문입니다.

이번에는 순수하게 대수적인 문제이며, 여기서는 벡터 공간에 대한 지식만 사용하면 됩니다.  $x \in K$ 인 각 원소는 벡터로 나타낼 수 있습니다.

$$F(x) := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{Q}^{\oplus n}$$

기저  $\{\alpha_1, \dots, \alpha_n\}$ 을 사용한다면 말입니다.

**연습문제 56.9.8.**  $(x, y) \mapsto \text{Tr}_{K/\mathbb{Q}}(x \cdot y)$ 가 그러면  $\text{GL}_n(\mathbb{Q})$ 에서 가역인 행렬로 쓰일 수 있음을 보이십시오 — 구체적으로,  $\text{Tr}_{K/\mathbb{Q}}(x \cdot y) = F(x)^\top M F(y)$ 를 만족하는  $M \in \text{GL}_n(\mathbb{Q})$ 가 존재하며, 여기서  $F(x)^\top$ 는  $F(x)$ 의 전치입니다.

이는  $(x, y) \mapsto \text{Tr}_{K/\mathbb{Q}}(x \cdot y)$ 를 거의 내적으로 만듭니다(장 13 참고). 다만 양의 정부호가 아니라는 점만 다릅니다(예를 들어,  $\mathbb{C}$ 에서  $\text{Tr}((1+i)^2) = 0$ 입니다). 하지만 행렬이 가역이라는 사실만으로도 다음을 하기에 충분합니다:

**연습문제 56.9.9.** 증명을 완성하십시오. (힌트: 행렬  $[F(\alpha_1) \cdots F(\alpha_n)] \in GL_n(\mathbb{Q})$ 을 고려하십시오.  $x \in S$ 가 되기 위한  $F(x)$ 에 대한 조건은 무엇입니까?)

### §56.9.iii 세 번째 증명

$\mathcal{O}_K$ 가 계수  $n$ 의 자유  $\mathbb{Z}$ -가군임을 증명하고자 한다는 것을 상기하십시오. 이를 위해, 이것이  $n$ 개의 원소로 생성될 수 없다고 가정한 다음,  $\mathcal{O}_K$ 가 이산적이지 않음을 보이는데, 이는 노름이 연속임을 알고 있기 때문에 문제를 일으킵니다.

**연습문제 56.9.10.**  $K \cong \mathbb{Q}^{\oplus n}$ 을 생각해 보십시오, 이는  $K$  위에 위상을 부여합니다.  $x \mapsto |N(x)|$ 가 실제로 연속임을 확인하십시오.

모든  $x \in \mathcal{O}_K$ 에 대해  $|N(x)| \in \mathbb{Z}$ 임을 알고 있습니다.

**연습문제 56.9.11.** 위의 위상에서 0을 제외하고는  $\mathcal{O}_K$ 의 어떤 원소도 포함하지 않는 공  $B(0, r)$ 이 존재함을 결론지으십시오.

자,  $\mathcal{O}_K$ 가  $n$ 개의 원소로 생성될 수 없다면 무엇이 잘못될까요? 문제는 빠르게 발생합니다:

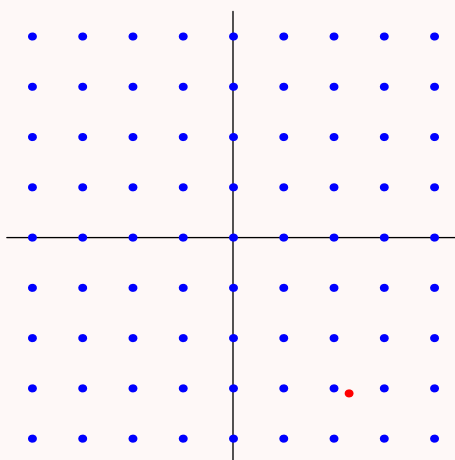
**연습문제 56.9.12.**  $\langle \alpha_1, \dots, \alpha_n \rangle$ 가  $K$ 를  $\mathbb{Q}$ -벡터 공간으로서 생성한다고 합시다.  $x \in \mathcal{O}_K$ 인  $x$ 가  $\{\alpha_1, \dots, \alpha_n\}$ 의  $\mathbb{Z}$ -선형 결합이 아니라고 합시다. 모두 0은 아닌  $z_1, \dots, z_n \in [-\frac{1}{2}, \frac{1}{2}]$ 가 존재하고,  $\{\alpha_1, \dots, \alpha_n\}$ 의  $\mathbb{Z}$ -선형 결합인  $z$ 가 존재하여  $x + z = \sum_{i=1}^n z_i \alpha_i$ 가 성립함을 보이십시오.

**연습문제 56.9.13.** 위와 같은 표기로,  $z_1 \neq 0$ 이라고 가정하십시오.  $\alpha_1$ 을  $z_1$ 로 바꾸면, 새로운 집합  $\{z_1, \alpha_2, \dots, \alpha_n\}$ 이 여전히  $K$ 를  $\mathbb{Q}$ -벡터 공간으로서 생성하며, 나아가 격자의 메시가 적어도 절반 감소함을 보이십시오.

### 예제 56.9.14

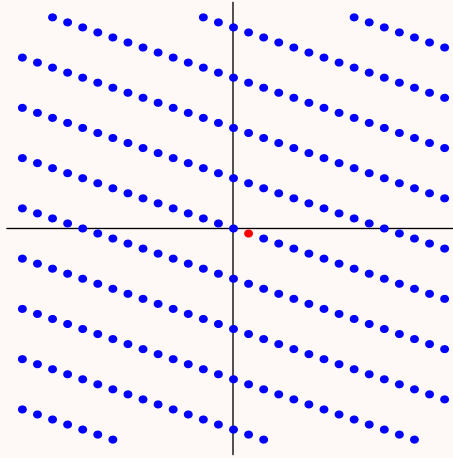
$A \subseteq \mathbb{C}$ 가 격자라고 가정하십시오.  $1 \in A$ 이고  $i \in A$ 임을 알고 있으므로,  $\mathbb{Z}[i] \subseteq A$ 입니다.

추가로  $2.3 - 3.1i \in A$ 임을 안다고 가정하십시오.



$A$ 가 덧셈에 대해 닫혀 있으므로,  $(2.3 - 3.1i) + (-2 + 3i) = 0.3 - 0.1i \in A$ 임을 알

수 있습니다. 기저에서 1을  $0.3 - 0.1i$ 로 바꿉니다. 그러면 격자  $\langle i, 0.3 - 0.1i \rangle \subseteq A$ 는 예상대로  $\langle 1, i \rangle$ 보다 작은 메시를 가집니다.

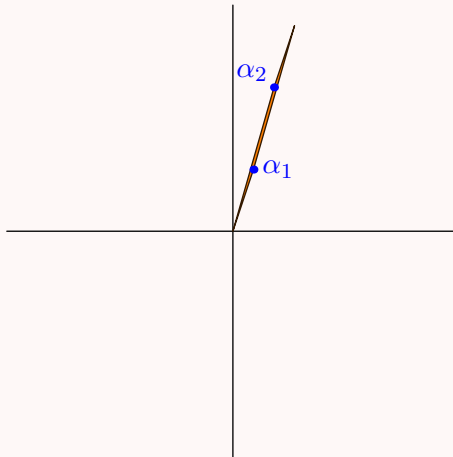


이를 무한히 계속할 수 있으므로 ( $\mathcal{O}_K$ 는 결코 생성되지 않습니다), 메시는 빠르게 0으로 감소합니다.

그럼, 끝난 걸까요? 메시가 0으로 가니, 어쩌면 어떤  $\alpha_i$ 의 최소 거리도 0으로 가지 않을까요? 거의 맞지만, 완전히는 아닙니다:

#### 예제 56.9.15

$\alpha_1 = 1 + 3i$ 와  $\alpha_2 = 2 + 7i$ 를 생각해 보십시오.



$\alpha_1$ 과  $\alpha_2$ 가 생성하는 격자의 메시는 1이지만,  $\alpha_1$ 도  $\alpha_2$ 도 원점에 특별히 가깝지 않습니다.

여기서 다시 민코프스키 경계를 적용해야 합니다: 메시가  $d$ 라고 가정하면, 원점을 중심으로 하고 부피가  $2^n d$ 인 정육면체는 0이 아닌 격자점을 포함합니다.<sup>3</sup> 이 점의 거리는 원점으로부터  $\sqrt[n]{n} \cdot \sqrt[n]{d}$ 보다 멀 수 없습니다.

<sup>3</sup>구를 사용하면 물론 더 나은 경계를 얻겠지만, 그 부피는 계산하기가 조금 더 어렵습니다.

**비고 56.9.16** — 이와 관련하여, LLL 격자 기저 축소 알고리즘은 실제로 원점에 충분히 가까운 격자 위의 점을 찾는 데 사용될 수 있습니다.

$d$ 가 충분히 작으면,  $\sqrt{n} \cdot \sqrt[n]{d} < r$ 이 성립하는데, 여기서  $r$ 은 위에서 보인 격자점이 없는 공이며, 이는 모순을 줍니다. 그러므로 증명이 끝났습니다!

## §56.10 생각해 볼 만한 조금 더 어려운 문제

**문제 56A.**  $K = \mathbb{Q}(\sqrt{-163})$ 가 자명한 유형군을 가지며, 따라서  $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right]$ 가 UFD임을 보이십시오.<sup>4</sup>

**문제 56B.**  $\mathbb{Q}(\sqrt{-31})$ 의 유수군을 결정하십시오.

**문제 56C** (China TST 1998).  $n$ 을 양의 정수라 합시다. 평면 위의 (반드시 볼록일 필요는 없는) 다각형의 넓이가  $n$ 보다 크다고 합시다. 이를 평행이동하여 적어도  $n+1$ 개의 격자점을 포함하도록 할 수 있음을 증명하십시오.

**문제 56D** (보조정리 56.3.6). 매장  $K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \xrightarrow{\sim} \mathbb{R}^n$ 의 합성을 생각하십시오.  $\mathcal{O}_K \subseteq K$ 의 상이 다음과 같은 메쉬를 가짐을 보이십시오.

$$\frac{1}{2^{r_2}} \sqrt{|\Delta_K|}.$$

**문제 56E.**  $p \equiv 1 \pmod{4}$ 인 소수  $p$ 가 있다고 합시다.  $a^2 + b^2 = p$ 를 만족하는 정수  $a > b > 0$ 이 유일하게 존재함을 보이십시오.

**문제 56F** (한국 국가수리올림피아드 2014).  $p$ 를 홀수 소수,  $k$ 를  $p \mid k^2 + 5$ 를 만족하는 양의 정수라 합시다.  $p^2 = m^2 + 5n^2$ 을 만족하는 양의 정수  $m, n$ 이 존재함을 증명하십시오.

**문제 56G.**  $K$ 를 수체라 하고  $\mathfrak{p}$ 를 임의의 0이 아닌 소 아이디얼이라 합시다. 다른 임의의 소 아이디얼  $\mathfrak{q}$ 에 대해  $x \notin \mathfrak{q}$ 이면서  $x \in \mathfrak{p}$ 인  $x$ 가 존재함을 증명하십시오.

<sup>4</sup>사실,  $n = 163$ 은  $\mathbb{Q}(\sqrt{-n})$ 이 자명한 유형군을 가지는 가장 큰 수입니다. 완전한 목록은 1, 2, 3, 7, 11, 19, 43, 67, 163이며, 이를 **히그너 수**라고 부릅니다. 위 문제를 풀 때 오일러의 소수 생성 다항식  $t^2 + t + 41$ 을 눈치챘을지도 모릅니다. 우연이 아닙니다!



# 57 판별식의 추가 성질

수체  $K$ 의 판별식은 다음과 같이 주어짐을 상기시켜 드립니다

$$\Delta_K := \det \begin{bmatrix} \sigma_1(\alpha_1) & \dots & \sigma_n(\alpha_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(\alpha_n) & \dots & \sigma_n(\alpha_n) \end{bmatrix}^2$$

여기서  $\alpha_1, \dots, \alpha_n$ 은  $K$ 의  $\mathbb{Z}$ -기저이며,  $\sigma_i$ 는  $K$ 에서  $\mathbb{C}$ 로의  $n$ 개의 매장입니다. 몇 가지 예시, 성질, 그리고 동치인 정의들이 이어집니다.

## §57.1 생각해 볼 만한 조금 더 어려운 문제

**문제 57A\*** (원분체의 판별식).  $p$ 를 홀수 유리 소수라 하고  $\zeta_p$ 를 1의 원시  $p$ 제곱근이라 합시다.  $K = \mathbb{Q}(\zeta_p)$ 라 합시다. 다음을 보이십시오.

$$\Delta_K = (-1)^{\frac{p-1}{2}} p^{p-2}.$$



**문제 57B\*** ( $\Delta_K$ 의 대각합 표현).  $\alpha_1, \dots, \alpha_n$ 을  $\mathcal{O}_K$ 의 기저라 합시다. 다음을 증명하십시오

$$\Delta_K = \det \begin{bmatrix} \text{Tr}_{K/\mathbb{Q}}(\alpha_1^2) & \text{Tr}_{K/\mathbb{Q}}(\alpha_1\alpha_2) & \dots & \text{Tr}_{K/\mathbb{Q}}(\alpha_1\alpha_n) \\ \text{Tr}_{K/\mathbb{Q}}(\alpha_2\alpha_1) & \text{Tr}_{K/\mathbb{Q}}(\alpha_2^2) & \dots & \text{Tr}_{K/\mathbb{Q}}(\alpha_2\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ \text{Tr}_{K/\mathbb{Q}}(\alpha_n\alpha_1) & \text{Tr}_{K/\mathbb{Q}}(\alpha_n\alpha_2) & \dots & \text{Tr}_{K/\mathbb{Q}}(\alpha_n\alpha_n) \end{bmatrix}.$$

특히,  $\Delta_K$ 는 정수입니다.

**문제 57C\*** ( $\Delta_K$ 의 근 표현). 이차 다항식  $Ax^2 + Bx + C$ 의 판별식은  $B^2 - 4AC$ 로 정의됩니다. 더 일반적으로, 차수가  $n$ 인 다항식  $f \in \mathbb{Z}[x]$ 의 다항식 판별식은

$$\Delta(f) := c^{2n-2} \prod_{1 \leq i < j \leq n} (z_i - z_j)^2$$

여기서  $z_1, \dots, z_n$ 은  $f$ 의 근이고,  $c$ 는  $f$ 의 최고차항 계수입니다.

$K$ 가 모노제닉이고  $\mathcal{O}_K = \mathbb{Z}[\theta]$ 라고 합시다.  $f$ 를  $\theta$ 의 최소다항식이라고 합시다(따라서 모닉입니다). 다음을 보이십시오.

$$\Delta_K = \Delta(f).$$

**문제 57D.**  $K \neq \mathbb{Q}$ 가 수체이면  $|\Delta_K| > 1$ 임을 보이십시오.

**문제 57E** (Brill의 정리). 서명이  $(r_1, r_2)$ 인 수체  $K$ 에 대해,  $\Delta_K > 0$ 인 것과  $r_2$ 가 짝수인 것이 동치임을 보이십시오.



**문제 57F** (Stickelberger 정리).  $K$ 를 수체라 하자.

$$\Delta_K \equiv 0 \text{ 또는 } 1 \pmod{4}$$

임을 증명하십시오.



# 58 보너스: 펠 방정식을 풀어봅시다!

이는 선택적으로 읽을 수 있는 부록이며, 안전하게 건너뛰어도 됩니다. (반면 꽤 짧습니다.)

## §58.1 단위

이 절의 대표적인 예:  $\pm 1$ , 단위근,  $3 - 2\sqrt{2}$ 와 그 거듭제곱.

문제 54A\*에 따르면  $\alpha \in \mathcal{O}_K$ 가 가역인 것과

$$N_{K/\mathbb{Q}}(\alpha) = \pm 1.$$

인 것이 동치임을 상기하십시오.  $\mathcal{O}_K^\times$ 가  $\mathcal{O}_K$ 의 단위들의 집합을 나타내도록 합시다.

**질문 58.1.1.**  $\mathcal{O}_K^\times$ 가 곱셈에 대해 군을 이룸을 보이십시오. 따라서 이를  $\mathcal{O}_K$ 의 **단위원**이라 부릅니다.

단위의 예로는 어떤 것들이 있습니까?

### 예제 58.1.2 (수체에서 단위의 예시)

1.  $\pm 1$ 은 확실히 단위이며, 임의의 수체에 존재합니다.
2.  $\mathcal{O}_K$ 가 단위근  $\omega$ 를 포함한다면 (즉  $\omega^n = 1$ ),  $\omega$ 는 단위입니다. (사실  $\pm 1$ 은 이의 특수한 경우입니다.)
3. 물론  $\mathcal{O}_K$ 의 모든 단위가 단위근인 것은 아닙니다. 예를 들어  $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$  ( $K = \mathbb{Q}(\sqrt{3})$ 로부터 나온 것)이라면, 수  $2 + \sqrt{3}$ 은 단위인데, 그 노름이

$$N_{K/\mathbb{Q}}(2 + \sqrt{3}) = 2^2 - 3 \cdot 1^2 = 1.$$

또는, 단순히 그 역원  $2 - \sqrt{3} \in \mathcal{O}_K$  역시 성립함을 확인해도 됩니다:

$$(2 - \sqrt{3})(2 + \sqrt{3}) = 1.$$

어느 쪽이든,  $2 - \sqrt{3}$ 은 단위입니다.

4. 임의의 단위  $u \in \mathcal{O}_K^\times$ 에 대해, 그 모든 거듭제곱 역시 단위입니다. 예를 들어  $(3 - 2\sqrt{2})^n$ 은 임의의  $n$ 에 대해 항상  $\mathbb{Z}[\sqrt{2}]$ 의 단위입니다.  $u$ 가 단위근이 아니라면, 이는  $\mathcal{O}_K^\times$ 에서 무한히 많은 새로운 단위들을 생성합니다.

**질문 58.1.3.** 다음 주장들을 확인하십시오:

- (a) 단위근은 단위이다, 그리고
- (b) 단위원의 거듭제곱은 단위원입니다.

정의로부터 출발하거나,  $N_{K/\mathbb{Q}}(\alpha) = \pm 1$ 이라는 특징을 사용할 수 있습니다. 한쪽 정의가 더 자연스럽게 느껴진다면, 다른 쪽을 사용해 보십시오.

## §58.2 디리클레 단위 정리

이 절의 대표적인 예:  $\mathbb{Z}[\sqrt{3}]$ 의 단위들은  $\pm(2 + \sqrt{3})^n$ 입니다.

**정의 58.2.1.**  $\mu(\mathcal{O}_K)$ 가 수체  $K$ 에 (동치로,  $\mathcal{O}_K$ 에) 포함된 단위근들의 집합을 나타내도록 합시다.

**예제 58.2.2** ( $\mu(\mathcal{O}_K)$ 의 예)

(a)  $K = \mathbb{Q}(i)$ 이면,  $\mathcal{O}_K = \mathbb{Z}[i]$ 입니다. 따라서

$$\mu(\mathcal{O}_K) = \{\pm 1, \pm i\} \quad \text{여기서 } K = \mathbb{Q}(i).$$

(b)  $K = \mathbb{Q}(\sqrt{3})$ 이면,  $\mathcal{O}_K = \mathbb{Z}[\sqrt{3}]$ 입니다. 따라서

$$\mu(\mathcal{O}_K) = \{\pm 1\} \quad \text{여기서 } K = \mathbb{Q}(\sqrt{3}).$$

(c)  $K = \mathbb{Q}(\sqrt{-3})$ 이면,  $\mathcal{O}_K = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{-3})]$ 입니다. 따라서

$$\mu(\mathcal{O}_K) = \left\{ \pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2} \right\} \quad \text{여기서 } K = \mathbb{Q}(\sqrt{-3})$$

여기서 두 번째 항의  $\pm$ 들은 서로 독립적일 필요가 없습니다. 다시 말해  $\mu(\mathcal{O}_K) = \{z \mid z^6 = 1\}$ 입니다.

**연습문제 58.2.3.**  $\mu(\mathcal{O}_K)$ 가 항상 어떤 정수  $n$ 에 대해  $x^n - 1$ 의 근들로 이루어짐을 보이십시오. (먼저 그것이 곱셈에 대해 유한군임을 보이십시오.)

이제 증명 없이 소위 디리클레 단위정리를 인용하겠습니다. 이 정리는  $\mathcal{O}_K$ 의 단위들이 무엇인지에 대해 훨씬 더 완전한 그림을 제공합니다. 전설에 따르면 디리클레는 시스티나 성당에서 열린 부활절 연주회 중에 이 정리의 증명을 발견했다고 합니다.

**정리 58.2.4** (디리클레의 단위 정리)

$K$ 를 시그니처  $(r_1, r_2)$ 를 갖는 수체라 하고 다음과 같이 놓습니다

$$s = r_1 + r_2 - 1.$$

그러면 모든 단위  $\alpha \in \mathcal{O}_K^\times$ 가 다음 형태로 유일하게 쓰일 수 있도록 하는 단위  $u_1, \dots, u_s$ 가 존재합니다

$$\alpha = \omega \cdot u_1^{n_1} \dots u_s^{n_s}$$

여기서  $\omega \in \mu(\mathcal{O}_K)$ 는 단위근이고,  $n_1, \dots, n_s \in \mathbb{Z}$ 입니다.

더 간결하게 말하면:

$$\mathcal{O}_K^\times \cong \mathbb{Z}^{r_1+r_2-1} \times \mu(\mathcal{O}_K) \text{입니다.}$$

$u_1, \dots, u_s$ 의 선택을 **기본 단위**의 선택이라 부릅니다.

몇 가지 응용 예시를 살펴보겠습니다.

### 예제 58.2.5 (몇몇 단위군)

- (a)  $K = \mathbb{Q}(i)$ 가 시그니처  $(0, 1)$ 을 갖는다고 합시다. 그러면  $s = 0$ 이 되므로, 디리클레의 단위정리에 따르면 단위군 외에 다른 단위는 존재하지 않습니다. 따라서

$$\mathcal{O}_K^\times = \{\pm 1, \pm i\} \quad \text{여기서 } K = \mathbb{Q}(i).$$

이는 놀랍지 않은데,  $a + bi \in \mathbb{Z}[i]$ 가 단위인 것과  $a^2 + b^2 = 1$ 인 것이 동치이기 때문입니다.

- (b)  $K = \mathbb{Q}(\sqrt{3})$ 이 시그니처  $(2, 0)$ 을 갖는다고 합시다. 그러면  $s = 1$ 이므로 정확히 하나의 기본 단위를 기대합니다. 기본 단위는 노름이 1인  $2 + \sqrt{3}$  (또는 그 역원인  $2 - \sqrt{3}$ )이며, 따라서 다음을 얻습니다

$$\mathcal{O}_K^\times = \{\pm(2 + \sqrt{3})^n \mid n \in \mathbb{Z}\}.$$

- (c)  $K = \mathbb{Q}(\sqrt[3]{2})$ 가 시그니처  $(1, 1)$ 을 갖는다고 합시다. 그러면  $s = 1$ 이므로 정확히 하나의 기본 단위를 기대합니다. 선택은  $1 + \sqrt[3]{2} + \sqrt[3]{4}$ 입니다. 따라서

$$\mathcal{O}_K^\times = \{\pm(1 + \sqrt[3]{2} + \sqrt[3]{4})^n \mid n \in \mathbb{Z}\}.$$

이것들이 실제로 기본 단위임을 아직 보여드리지 않았는데, 실제로 기본 단위를 계산하는 것은 일반적으로 어렵습니다.

## §58.3 기본 단위 찾기

다음은 몇몇 기본 단위들을 담은 표입니다.

| $d$      | 단위                          |
|----------|-----------------------------|
| $d = 2$  | $1 + \sqrt{2}$              |
| $d = 3$  | $2 + \sqrt{3}$              |
| $d = 5$  | $\frac{1}{2}(1 + \sqrt{5})$ |
| $d = 6$  | $5 + 2\sqrt{6}$             |
| $d = 7$  | $8 + 3\sqrt{7}$             |
| $d = 10$ | $3 + \sqrt{10}$             |
| $d = 11$ | $10 + 3\sqrt{11}$           |

일반적으로 기본 단위를 결정하는 것은 계산상 어렵습니다.

그러나 일단 기본 단위가 무엇인지 알려드리면, 그것을 검증하는 일은 (적어도  $s = 1$ 인 경우에는) 그리 나쁘지 않습니다. 예를 들어,  $K = \mathbb{Q}(\sqrt{11})$ 의 정수환이  $\mathbb{Z}[\sqrt{11}]$ 일 때  $10 + 3\sqrt{11}$ 이  $K$ 의 기본 단위임을 보이고자 한다고 합시다. 만약 그렇지 않다면, 어떤  $n > 1$ 에 대해 다음이 성립해야 할 것입니다

$$10 + 3\sqrt{11} = \pm(x + y\sqrt{11})^n.$$

이런 일이 일어나려면, 최소한  $|y| < 3$ 이어야 합니다. 또한  $x^2 - 11y^2 = \pm 1$ 이어야 합니다. 따라서 ( $y = 1, 2$ 를 이용하여) 이것이 성립하지 않음을 그냥 확인할 수 있습니다.

요점은 이렇습니다:  $(10, 3)$ 이  $x^2 - 11y^2 = \pm 1$ 의 정수해 중 ( $|y|$ 의 의미에서) 가장 작은 해이므로, 이는 기본 단위여야 합니다. 이는 더 일반적으로 성립하지만,  $d \equiv 1 \pmod{4}$ 인 경우에는  $x, y$ 가 (예를 들어  $\frac{1}{2}(1 + \sqrt{5})$ 처럼) 반정수일 수 있으므로 수정이 필요합니다.

**정리 58.3.1 (펠 방정식의 기본 단위)**

$d$ 를 제곱인수가 없는 정수라고 가정합니다.

- (a)  $d \equiv 2, 3 \pmod{4}$ 이고,  $(x, y)$ 가  $x^2 - dy^2 = \pm 1$ 의 최소 정수 해라면,  $x + y\sqrt{d}$ 는 기본 단위입니다.
- (b)  $d \equiv 1 \pmod{4}$ 이고,  $(x, y)$ 가  $x^2 - dy^2 = \pm 1$ 의 최소 반정수 해라면,  $x + y\sqrt{d}$ 는 기본 단위입니다. (동등하게,  $a^2 - db^2 = \pm 4$ 의 최소 정수 해는  $\frac{1}{2}(a + b\sqrt{d})$ 를 줍니다.)

(“최소”에 대한 어떤 합리적인 정의든 작동합니다, 예를 들어  $|y|$ 로 정렬하는 것처럼 말입니다.)

**§58.4 펠 방정식**

이러한 부류의 결과는 펠 방정식을 완전히 소거합니다. 결국,

$$a^2 - d \cdot b^2 = \pm 1$$

을 푸는 것은 노름이  $\pm 1$ 인  $\mathbb{Z}[\sqrt{d}]$ 의 원소를 찾는 것에 해당합니다.  $d \equiv 1 \pmod{4}$ 인 경우에는 조금 더 이상합니다, 왜냐하면 이 경우  $K = \mathbb{Q}(\sqrt{d})$ 는  $\mathcal{O}_K = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{d})]$ 를 주므로, 기본 단위가 실제로는 해가 아닐 수도 있기 때문입니다. (예를 들어,  $d = 5$ 일 때, 해  $(\frac{1}{2}, \frac{1}{2})$ 를 얻습니다.) 그럼에도 불구하고, 모든 정수 해는 결국 생성됩니다.

이 모든 것을 구체적으로 만들기 위해, 여기 간단한 예시가 있습니다.

**예제 58.4.1 ( $x^2 - 5y^2 = \pm 1$ )**

$K = \mathbb{Q}(\sqrt{5})$ 로 설정하면,  $\mathcal{O}_K = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{5})]$ 입니다. 디리클레 단위 정리에 의해,  $\mathcal{O}_K^\times$ 는 하나의 원소  $u$ 에 의해 생성됩니다. 다음의 선택은

$$u = \frac{1}{2} + \frac{1}{2}\sqrt{5}$$

$a^2 - 5b^2 = \pm 4$ 에 대해 더 작은 정수 해가 없으므로, 기본 단위로 사용됩니다.  $u$ 의 처음 몇 거듭제곱은 다음과 같습니다

| $n$ | $u^n$                         | 노름 |
|-----|-------------------------------|----|
| -2  | $\frac{1}{2}(3 - \sqrt{5})$   | 1  |
| -1  | $\frac{1}{2}(1 - \sqrt{5})$   | -1 |
| 0   | 1                             | 1  |
| 1   | $\frac{1}{2}(1 + \sqrt{5})$   | -1 |
| 2   | $\frac{1}{2}(3 + \sqrt{5})$   | 1  |
| 3   | $2 + \sqrt{5}$                | -1 |
| 4   | $\frac{1}{2}(7 + 3\sqrt{5})$  | 1  |
| 5   | $\frac{1}{2}(11 + 5\sqrt{5})$ | -1 |
| 6   | $9 + 4\sqrt{5}$               | 1  |

첫 번째 정수 해는  $(2, 1)$ 이며, 이는  $-1$ 을 준다는 것을 알 수 있습니다.  $+1$ 을 주는 첫 번째 해는  $(9, 4)$ 입니다. 이 패턴을 계속하면,  $u$ 의 세제곱마다 정수 해를 준다는 것을 알 수 있으며(또한 **문제 58B** 참조), 홀수 번째는  $x^2 - 5y^2 = -1$ 의 해를 주고 짝수 번째는  $x^2 - 5y^2 = +1$ 의 해를 줍니다. 모든 해는 (부호  $\pm u^{\pm n}$ 을 고려함으로써)  $\pm$  부호를 제외하면 이런 방식으로 생성됩니다.

## §58.5 생각해 볼 만한 조금 더 어려운 문제

**문제 58A** (헤이스팅스 전투에 관한 허구의 기록). 다음 전투에서 병사의 수를 구하십시오:

해럴드의 병사들은 늘 그랬듯이 함께 굳건히 서서 열세 개의 정사각형 대형을 이루었으며, 각 정사각형마다 같은 수의 병사가 있었고, 그들의 진지에 감히 발을 들이려는 대담한 노르만인에게는 화가 있을지언다. 색슨 전투 도끼의 일격 한 번이면 그의 창을 부러뜨리고 사슬 갑옷을 갈랐기 때문이다. . . . 해럴드가 몸소 전장에 뛰어들었을 때 색슨인들은 하나의 거대한 정사각형 병력이 되어 "우트!", "올리크로세!", "고데마이트!"라는 함성을 외쳤다.

**문제 58B.**  $d > 0$ 을 제곱나눴수가 없는 정수라 하고,  $u$ 를  $\mathbb{Q}(\sqrt{d})$ 의 기본 단위라 하십시오.  $u \in \mathbb{Z}[\sqrt{d}]$ 이거나, 혹은  $u^n \in \mathbb{Z}[\sqrt{d}] \iff 3 \mid n$ 임을 보이십시오.

**문제 58C.** 다음에 대해 정수 해가 없음을 보이십시오

$$x^2 - 34y^2 = -1$$

$-1$ 이 34를 법으로 이차잉여라는 사실에도 불구하고 그렇습니다.



# XV

## 대수적 정수론 II: 갈루아 이론과 분기 이론

## 제XV부: 목차

---

|           |                                         |            |
|-----------|-----------------------------------------|------------|
| <b>59</b> | <b>갈루아에 관한 것들</b>                       | <b>597</b> |
| 59.1      | 동기 . . . . .                            | 597        |
| 59.2      | 체 확대, 대수적 확대, 분해체 . . . . .             | 598        |
| 59.3      | 수체의 대수적 폐포로의 매장 . . . . .               | 599        |
| 59.4      | 모두가 표수 2를 싫어하는 이유: 분리 가능 대 기약 . . . . . | 600        |
| 59.5      | 자기동형사상군과 갈루아 확대 . . . . .               | 602        |
| 59.6      | 갈루아 이론의 기본 정리 . . . . .                 | 605        |
| 59.7      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .          | 606        |
| 59.8      | (선택) 갈루아 확장이 분해체임의 증명 . . . . .         | 607        |
| <br>      |                                         |            |
| <b>60</b> | <b>유한체</b>                              | <b>609</b> |
| 60.1      | 유한체의 예 . . . . .                        | 609        |
| 60.2      | 유한체는 소수의 거듭제곱 위수를 가짐 . . . . .          | 610        |
| 60.3      | 모든 유한체는 동형입니다 . . . . .                 | 611        |
| 60.4      | 유한체의 갈루아 이론 . . . . .                   | 612        |
| 60.5      | 추가: 유한체의 곱셈군 . . . . .                  | 613        |
| 60.6      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .          | 614        |
| <br>      |                                         |            |
| <b>61</b> | <b>분지 이론</b>                            | <b>615</b> |
| 61.1      | 분지된 / 비환성 / 분할 소수 . . . . .             | 615        |
| 61.2      | 소수는 $\Delta_K$ 를 나눌 때에만 분지됩니다 . . . . . | 616        |
| 61.3      | 관성차수 . . . . .                          | 616        |
| 61.4      | 갈루아 확장의 마법 . . . . .                    | 617        |
| 61.5      | (선택) 분해군과 관성군 . . . . .                 | 620        |
| 61.6      | 결가지 소견: 더 일반적인 갈루아 확장 . . . . .         | 622        |
| 61.7      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .          | 623        |
| <br>      |                                         |            |
| <b>62</b> | <b>프로베니우스 원소</b>                        | <b>625</b> |
| 62.1      | 프로베니우스 원소들 . . . . .                    | 625        |
| 62.2      | 컬레류 . . . . .                           | 627        |
| 62.3      | 체보타레프 밀도 정리 . . . . .                   | 628        |
| 62.4      | 예시: 원분체의 프로베니우스 원소 . . . . .            | 629        |
| 62.5      | 프로베니우스 원소는 제한 사상과 잘 어울립니다 . . . . .     | 629        |
| 62.6      | 응용: 이차 상호법칙 . . . . .                   | 630        |
| 62.7      | 프로베니우스 원소는 인수분해를 통제합니다 . . . . .        | 632        |
| 62.8      | 응용 예시: IMO 2003 문제 6 . . . . .          | 635        |
| 62.9      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .          | 636        |
| <br>      |                                         |            |
| <b>63</b> | <b>보너스: 아르틴 상호법칙에 대하여</b>               | <b>639</b> |
| 63.1      | 개요 . . . . .                            | 639        |
| 63.2      | 무한 소수 . . . . .                         | 640        |
| 63.3      | 무한 소수를 이용한 모듈러 산술 . . . . .             | 640        |
| 63.4      | 확장에서의 무한 소수 . . . . .                   | 642        |
| 63.5      | 프로베니우스 원소와 아르틴 기호 . . . . .             | 643        |
| 63.6      | 아르틴 상호법칙 . . . . .                      | 645        |
| 63.7      | 응용: 두 제곱수의 합의 일반화 . . . . .             | 648        |
| 63.8      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .          | 652        |

---

# 59 갈루아에 관한 것들

## §59.1 동기

이 절의 대표적인 예:  $\mathbb{Q}(\sqrt{2})$ 과  $\mathbb{Q}(\sqrt[3]{2})$ .

갈루아 이론의 핵심 아이디어는 매장이라는 개념으로, 이는 앞서 설명한 "켈레"라는 개념에 도달하는 또 다른 방법을 제공합니다.

$K$ 를 수체라고 합시다. **매장**  $\sigma: K \hookrightarrow \mathbb{C}$ 는 단사 체 준동형사상입니다. 즉 덧셈과 곱셈을 보존해야 하며, 특히 1을 고정해야 합니다.

**질문 59.1.1.** 이러한 맥락에서 임의의 유리수  $q$ 에 대해  $\sigma(q) = q$ 임을 보이십시오.

### 예제 59.1.2 (매장의 예시)

- (a)  $K = \mathbb{Q}(i)$ 인 경우,  $K$ 에서  $\mathbb{C}$ 로의 두 매장은  $z \mapsto z$ (항등사상)와  $z \mapsto \bar{z}$ (복소켈레)입니다.
- (b)  $K = \mathbb{Q}(\sqrt{2})$ 인 경우,  $K$ 에서  $\mathbb{C}$ 로의 두 매장은  $a + b\sqrt{2} \mapsto a + b\sqrt{2}$ (항등사상)와  $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ (켈레)입니다.
- (c)  $K = \mathbb{Q}(\sqrt[3]{2})$ 인 경우, 세 가지 매장이 있습니다:
  - $1 \mapsto 1$ 과  $\sqrt[3]{2} \mapsto \sqrt[3]{2}$ 를 보내는 항등 매장.
  - $1 \mapsto 1$ 과  $\sqrt[3]{2} \mapsto \omega \sqrt[3]{2}$ 를 보내는 매장으로, 여기서  $\omega$ 는 1의 세제곱근입니다. 이것만으로도 매장의 나머지 부분이 결정되기에 충분함을 유의하십시오.
  - $1 \mapsto 1$ 과  $\sqrt[3]{2} \mapsto \omega^2 \sqrt[3]{2}$ 를 보내는 매장.

이러한 매장들에 대해 몇 가지 관찰을 하고자 하며, 이는 갈루아 이론의 핵심 아이디어를 이룰 것입니다. 여기에 주의를 기울이십시오!

- 먼저, 근들 사이에 일종의 쌍대성이 있음을 알아챌 수 있습니다: 첫 번째 예시에서  $i$ 는  $\pm i$ 로 보내지고,  $\sqrt{2}$ 는  $\pm\sqrt{2}$ 로 보내지며,  $\sqrt[3]{2}$ 는  $x^3 - 2$ 의 다른 근들로 보내집니다. 이는 우연이 아니며, 일반적으로 이러한 현상이 발생함을 보일 수 있습니다. 구체적으로,  $\alpha$ 의 최소다항식이 다음과 같다고 합시다

$$0 = c_n \alpha^n + c_{n-1} \alpha^{n-1} + \cdots + c_1 \alpha + c_0$$

여기서  $c_i$ 는 유리수입니다. 그러면 양변에 임의의 매장  $\sigma$ 를 적용하면 다음을 얻습니다

$$\begin{aligned} 0 &= \sigma(c_n \alpha^n + c_{n-1} \alpha^{n-1} + \cdots + c_1 \alpha + c_0) \\ &= \sigma(c_n) \sigma(\alpha)^n + \sigma(c_{n-1}) \sigma(\alpha)^{n-1} + \cdots + \sigma(c_1) \sigma(\alpha) + \sigma(c_0) \\ &= c_n \sigma(\alpha)^n + c_{n-1} \sigma(\alpha)^{n-1} + \cdots + c_1 \sigma(\alpha) + c_0 \end{aligned}$$

여기서 마지막 단계에서는  $c_i \in \mathbb{Q}$ 이므로  $\sigma$ 에 의해 고정된다는 사실을 사용하였습니다. 따라서 최소다항식의 근들은 그 다항식의 다른 근들로 갑니다.

- 다음으로, 두 번째와 세 번째 예시 사이의 대조를 이끌어내고자 합니다. 구체적으로,  $K = \mathbb{Q}(\sqrt{2})$ 에서  $\mathbb{C}$ 로의 매장을 고려하는 예시 (b)에서, 이 매장들의 상은 전적으로  $K$

안에 들어갑니다: 즉  $K \rightarrow \mathbb{C}$ 를 살펴보는 대신  $K \rightarrow K$ 를 살펴보아도 마찬가지였을 것입니다. 그러나 (c)에서는 이것이 성립하지 않습니다: 실제로  $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ 이지만, 항등사상이 아닌 매장들은 복소수 출력값을 가집니다!

핵심적인 차이는 다시 켄네를 생각해보는 것입니다. 핵심 관찰:

체  $K = \mathbb{Q}(\sqrt[3]{2})$ 는 "결핍"되어 있는데, 이는 최소다항식  $x^3 - 2$ 가  $K$ 에 포함되지 않은 다른 두 근  $\omega\sqrt[3]{2}$ 와  $\omega^2\sqrt[3]{2}$ 를 가지기 때문입니다.

반면  $K = \mathbb{Q}(\sqrt{2})$ 는  $x^2 - 2$ 의 두 근 모두가  $K$  안에 포함되어 있으므로 아무 문제가 없습니다. 마지막으로,  $K = \mathbb{Q}(\sqrt[3]{2})$ 의 결핍은 이를 완비하여 체  $\mathbb{Q}(\sqrt[3]{2}, \omega)$ 로 만듦으로써 실제로 해결할 수 있습니다.  $\mathbb{Q}(i)$ 나  $\mathbb{Q}(\sqrt{2})$ 처럼 "자체 완결적"인 체들은 갈루아 확대라고 불리며, 이는 곧 설명하겠습니다.

- 마지막으로, 위의 예시들에서  $K$ 에서  $\mathbb{C}$ 로의 매장의 개수가 마침  $K$ 의 차수와 같다는 것을 알아챌 수 있습니다. 이는 중요한 정리로, **정리 59.3.1**입니다.

이 장에서는  $\mathbb{Q}$  이외의 임의의 체에 대해 이러한 아이디어들을 완전히 일반적인 형태로 전개하겠습니다.

## §59.2 체 확대, 대수적 확대, 분해체

**이 절의 대표적인 예:**  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 는 확대이며,  $\mathbb{C}$ 는 임의의 수체의 대수적 확대입니다.

먼저, 수체의 개념을 일반화하기 위해 한 체가 다른 체 안에 들어있다는 개념을 정의합니다.

**정의 59.2.1.**  $K$ 와  $F$ 를 체라고 합시다.  $F \subseteq K$ 이면  $K/F$ 라고 쓰고  $K$ 를  $F$ 의 **체 확대**라고 합니다.

따라서  $K$ 는 자동으로  $F$ -벡터 공간이 됩니다 ( $\mathbb{Q}(\sqrt{2})$ 가 자동으로  $\mathbb{Q}$ -벡터 공간이 되는 것과 마찬가지입니다). **차수**는 이 공간의 차원이며,  $[K : F]$ 로 표기합니다.  $[K : F]$ 가 유한하면  $K/F$ 를 **유한 (체) 확대**라고 합니다.

이게 정말 전부입니다. 까다로운 부분은 전혀 없습니다.

**질문 59.2.2.**  $\mathbb{Q}$ 의 유한 확대를 뭐라고 부를까요?

유한 확대의 차수는 곱셈적입니다.

**정리 59.2.3** (체 확대는 곱셈적 차수를 가집니다)

$F \subseteq K \subseteq L$ 을 체라고 하고,  $L/K$ ,  $K/F$ 가 유한하다고 합시다. 그러면

$$[L : K][K : F] = [L : F].$$

증명. 기저 계산:  $K$  위에서  $L$ 의 기저를 찾은 다음, 이를 확장하여  $F$  위에서  $L$ 의 기저로 만들 수 있습니다. (성실한 독자라면 세부사항을 채워 넣을 수 있습니다.)  $\square$

다음으로, ( $\mathbb{Q}(\sqrt[3]{2})$ 과 같은) 체가 주어졌을 때 그것을 매장할 대상(우리 경우에는  $\mathbb{C}$ )이 필요합니다. 즉 모든 다항식의 모든 근을 포함하는 체가 필요할 뿐입니다. 체  $E$ 가 **대수적으로 닫혀 있다**고 하는 것은  $E$ 의 계수를 갖는 모든 다항식이  $E$ 에서 일차다항식들의 곱으로 분해되는 경우로 약속합니다. 고전적인 예는 다음과 같습니다:

**예제 59.2.4 (C)**

$\mathbb{C}$ 는 대수적으로 닫혀 있습니다.

중요한 정리는 임의의 체  $F$ 를 대수적으로 닫힌 체  $\bar{F}$ 로 확대할 수 있다는 것입니다.  $\bar{F}[x]$ 의 다항식의 모든 근은  $\bar{F}$ 에 있으므로, 특히  $F[x]$ 의 다항식의 모든 근도 그러합니다. 결과는 다음과 같습니다:

**정리 59.2.5 (대수적 폐포)**

임의의 체  $F$ 는 대수적으로 닫힌 체 확대를 가집니다. 사실, 포함 관계에 대해 극소인 이러한 확대는 유일하게 존재하며, 이를 **대수적 폐포**라고 하고  $\bar{F}$ 로 표기합니다. (여기서 “극소”란  $F$ 의 다른 임의의 대수적으로 닫힌 확대가  $\bar{F}$ 와 동형인 사본을 포함한다는 뜻입니다.) 이는  $\bar{F}$ 의 모든 원소가 실제로  $F$ 의 계수를 갖는 어떤 다항식의 근이라는 성질을 가집니다.

**예제 59.2.6 ( $\mathbb{R} = \bar{\mathbb{C}} = \mathbb{C} \supsetneq \mathbb{Q}$ )**

$\mathbb{C}$ 는  $\mathbb{R}$ 의 (그리고 자기 자신의) 대수적 폐포입니다. 하지만  $\mathbb{Q}$ 의 대수적 폐포  $\bar{\mathbb{Q}}$  (즉, 대수적 수의 집합)는  $\mathbb{C}$ 의 진부분체입니다 (일부 복소수는 유리수 계수 다항식의 근이 아닙니다).

보통 이러한 확대가 어떤 모습인지는 별로 신경 쓰지 않고, 그저 존재한다는 사실에 만족합니다. 종종 대수적 폐포조차 사용하지 않고, 단지 충분히 큰 아무 체나 사용합니다. 예를 들어  $\mathbb{Q}$ -계수를 갖는 다항식  $f$ 를 다룰 때,  $\mathbb{C}$  대신 더 작은  $\bar{\mathbb{Q}}$ 를 사용하는 편이 덜 낭비적일 수 있음에도 불구하고, 편의와 구체성을 위해 단순히  $f$ 의 근을  $\mathbb{C}$ 의 원소로 간주합니다.

## §59.3 수체의 대수적 폐포로의 매장

이제 이 모든 재료를 정의했으니, 다음을 증명할 수 있습니다:

**정리 59.3.1 (수체의  $n$ 개의 매장)**

$K$ 를 차수  $n$ 의 수체라고 합시다. 그러면  $\mathbb{Q}$ 를 고정하는 체 준동형사상  $K \hookrightarrow \mathbb{C}$ 가 정확히  $n$ 개 존재하며, 이를  $\sigma_1, \dots, \sigma_n$ 이라고 합시다.

**비고 59.3.2** — 체의 자명하지 않은 준동형사상은 반드시 단사임에 유의하십시오(핵이 아이디얼이기 때문입니다). 이는 “ $\hookrightarrow$ ”의 사용을 정당화하며, 우리는 각  $\sigma_i$ 를  $K$ 에서  $\mathbb{C}$ 로의 **매장**(매장)이라고 부릅니다.

증명. 이것은 사실 꽤 재미있습니다!  $\mathbb{Q}$  위의 임의의 기약다항식은 서로 다른 근을 가진다는 것을 기억하십시오 (**보조정리 54.1.2**). 우리는 원소  $\alpha_1, \alpha_2, \dots, \alpha_m$ 을 한 번에 하나씩  $\mathbb{Q}$ 에 첨가하여, 결국  $K$  전체를 얻을 것입니다. 즉,

$$K = \mathbb{Q}(\alpha_1, \dots, \alpha_m).$$

도식으로 나타내면, 이는

$$\begin{array}{ccccccc}
 \mathbb{Q} & \hookrightarrow & \mathbb{Q}(\alpha_1) & \hookrightarrow & \mathbb{Q}(\alpha_1, \alpha_2) & \hookrightarrow & \dots \hookrightarrow K \\
 \downarrow \text{id} & & \downarrow \tau_1 & & \downarrow \tau_2 & & \downarrow \tau_m = \sigma \\
 \mathbb{C} & \longrightarrow & \mathbb{C} & \longrightarrow & \mathbb{C} & \longrightarrow & \dots \longrightarrow \mathbb{C}
 \end{array}$$

먼저,  $\tau_1$ 을 선택하는 방법이 정확히

$$[\mathbb{Q}(\alpha_1) : \mathbb{Q}]$$

가지임을 주장합니다.  $\tau_1$ 은 그것이  $\alpha_1$ 을 어디로 보내는지에 의해 결정된다는 점에 주목하십시오( $\mathbb{Q}$ 를 고정해야 하기 때문입니다).  $p_1$ 을  $\alpha_1$ 의 최소 다항식이라 하면,  $\tau_1$ 에 대해  $\deg p_1$ 가지 선택지가 있으며, 이는  $p_1$ 의 (서로 다른) 근 각각에 대응합니다. 이로써 주장이 증명됩니다.

마찬가지로,  $\tau_1$ 의 선택이 주어지면

$$[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)]$$

$\tau_2$ 를 선택하는 방법의 가짓수입니다. (조금 다릅니다:  $\tau_1$ 이 항등원일 필요는 없습니다. 하지만  $\tau_2$ 가 그것이  $\alpha_2$ 를 어디로 보내는지에 의해 결정된다는 것은 여전히 참이며, 앞서와 마찬가지로  $[\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}(\alpha_1)]$ 가지의 가능한 방법이 있습니다.)

이들을 모두 곱하면 원하는  $[K : \mathbb{Q}]$ 가 나옵니다.  $\square$

**비고 59.3.3** — 원시원소 정리는 사실  $m = 1$ 이면 충분함을 함의합니다. 즉 탑 전체를 세울 필요가 없습니다. 이는 증명을 다소 단순화합니다.

” $K$ 를 차수  $n$ 인 수체라 하고,  $\sigma_1, \dots, \sigma_n$ 을 그것의  $n$ 개의 매장이라 하자”와 같은 표현을 더 이상의 설명 없이 보는 것은 흔한 일입니다. 이러한 매장과 갈루아 켄레 사이의 관계는 다음과 같이 주어집니다.

#### 정리 59.3.4 (매장은 켄레들에 고르게 분포합니다)

$K$ 를 차수  $n$ 인 수체로 두고 그  $n$ 개의 매장을  $\sigma_1, \dots, \sigma_n$ 이라 하며,  $\alpha \in K$ 가  $\mathbb{Q}$  위에서  $m$ 개의 갈루아 켄레를 갖는다고 합시다.

그러면  $\sigma_j(\alpha)$ 는 이  $m$ 개의 켄레 각각에 ”고르게 분포”합니다: 임의의 갈루아 켄레  $\beta$ 에 대해, 정확히  $\frac{n}{m}$ 개의 매장이  $\alpha$ 를  $\beta$ 로 보냅니다.

증명. 앞선 증명에서, 먼저  $\alpha_1 = \alpha$ 를 첨가하십시오.  $\square$

이제 우리는  $\mathbb{Q}$  위에서 대각합과 노름을 다음과 같이 좋은 방식으로 정의할 수 있습니다: 수체  $K$ 가 주어졌을 때, 다음과 같이 둡니다

$$\text{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha) \quad \text{그리고} \quad N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha)$$

여기서  $\sigma_i$ 는  $K$ 에서  $\mathbb{C}$ 로 가는  $n$ 개의 매장입니다.

## §59.4 모두가 표수 2를 싫어하는 이유: 분리 가능 대 기약

**이 절의 대표적인 예:**  $\mathbb{Q}$ 는 표수 0을 가지므로, 기약 다항식은 분리 가능합니다.

이제 우리는 위 정리를 임의의 체  $F$ 에 대해 성립하는 형태로 만들고자 합니다. 증명을 읽어보면, 체  $\mathbb{Q}$ 에 대해 사용되는 유일한 성질은 보조정리 54.1.2이며, 여기서 우리는 다음 사실을 사용한다는 것을 알 수 있습니다

$F$  위의 기약 다항식은 이중근을 갖지 않습니다.

이중근을 갖지 않는 다항식을 **분리 가능**하다고 부릅니다. 따라서 우리는 기약 다항식이 분리 가능하기를 원합니다. 지난 장에서 우리는  $\mathbb{Q}$ 에 대해 도함수를 취함으로써 이를 해냈습니다. 임의의 체에 대해서도 통해야 하지 않을까요?

아닙니다.  $2x^3 + 24x + 9$ 와 같은 다항식의 도함수를 취했다고 합시다. 즉  $6x^2 + 24$ 입니다.  $\mathbb{C}$ 에서는 상수가 아닌 다항식의 도함수  $f'$ 가 영이 아니라는 것이 자명합니다. 하지만 위 다항식을  $\mathbb{F}_3$ 에서의 다항식, 즉 3을 법으로 하여 생각했다고 합시다. 그러면 도함수는 영이 됩니다. 이런!

우리는 이런 일이 일어나는 것을 막는 조건을 부과해야 합니다.

**정의 59.4.1.** 체  $F$ 에 대해,  $F$ 의 **표수**란 다음을 만족시키는 가장 작은 양의 정수  $p$ 입니다,

$$\underbrace{1_F + \cdots + 1_F}_{p \text{ 번}} = 0$$

또는 그러한 정수  $p$ 가 존재하지 않으면 영입니다.

#### 예제 59.4.2 (체의 표수)

오랜 친구인  $\mathbb{R}$ ,  $\mathbb{Q}$ ,  $\mathbb{C}$ 는 모두 표수 0을 갖습니다. 하지만  $p$ 를 법으로 하는 정수들인  $\mathbb{F}_p$ 는 표수  $p$ 인 체입니다.

**연습문제 59.4.3.**  $F$ 를 표수  $p$ 인 체라 합시다.  $p > 0$ 이면  $p$ 가 소수임을 보이십시오. (증명은 다음 장에서 주어집니다.)

표수가 0이라는 가정 하에서, 앞서의 증명이 그대로 작동합니다.

#### 보조정리 59.4.4 (표수 0에서의 분리가능성)

표수 0인 체 위의 모든 기약 다항식은 분리가능합니다.

안타깝게도 이 보조정리는 "표수 0" 조건을 빼면 성립하지 않습니다.

**비고 59.4.5** — 이것이 분리가능이라고 불리는 이유는 (제 생각에는) 다음과 같은 그림 때문입니다: 다항식이 하나 있고 이를 기약인 부분들로 쪼개고 싶습니다. 보통 다항식에 중근이 있다면, 이는 그것이 기약이 아니라는 뜻입니다. 하지만 표수  $p > 0$ 에서는 이것이 성립하지 않습니다. 그래서 분리불가능한 다항식은 생각해 보면 이상합니다: 어쩐지 서로 분리될 수 없는 중근을 갖게 되는 것입니다.

분리가능성이 문제가 되지 않는 어떠한 체 확대에 대해서도 이것이 작동하도록 만들 수 있습니다.

**정의 59.4.6. 분리가능 확대**  $K/F$ 란 각  $\alpha \in K$ 에 대해  $F$  위에서의  $\alpha$ 의 최소다항식이 분리가능한 경우를 말합니다(예를 들어  $F$ 의 표수가 0인 경우가 그렇습니다). 체  $F$ 는 임의의 유한 체 확대  $K/F$ 가 분리가능하면 **완전체**라고 합니다.

실제로 다음 장에서 보게 되듯이:

#### 정리 59.4.7 (유한체는 완전체이다)

$F$ 가 유한개의 원소를 갖는 체라고 합시다. 그러면 이는 완전체입니다.

따라서 냅킨에서 등장하는 모든 체는 유한체이거나 표수 0이므로, 우리는 분리가능성에 대해 거의 걱정할 필요가 없을 것입니다. 그러므로 "분리가능"이라는 단어를 포함시키는 것은 대체로 형식적인 것에 지나지 않습니다.

계속 나아가면 다음을 얻습니다

**정리 59.4.8 (임의의 분리가능 확대의  $n$ 개의 매장)**

$K/F$ 가 차수  $n$ 인 분리가능 확대이고  $\bar{F}$ 가  $F$ 의 대수적 폐포라고 합시다. 그러면  $F$ 를 고정하는 체 준동형사상  $K \hookrightarrow \bar{F}$ 가 정확히  $n$ 개 존재하며, 이를  $\sigma_1, \dots, \sigma_n$ 이라 합시다.

어쨌든 이를 통해 임의의 분리가능 정규 확대에 대해 자취를 정의할 수 있습니다.

**정의 59.4.9.**  $K/F$ 가 차수  $n$ 인 분리가능 확대이고,  $\sigma_1, \dots, \sigma_n$ 이  $F$ 의 대수적 폐포의  $n$ 개의 매장이라고 합시다. 그러면 다음과 같이 정의합니다

$$\mathrm{Tr}_{K/F}(\alpha) = \sum_{i=1}^n \sigma_i(\alpha) \quad \text{그리고} \quad N_{K/F}(\alpha) = \prod_{i=1}^n \sigma_i(\alpha).$$

$F = \mathbb{Q}$ 이고 대수적 폐포가  $\mathbb{C}$ 일 때, 이는 앞서의 정의와 일치합니다!

## §59.5 자기동형사상군과 갈루아 확대

**이 절의 대표적인 예:**  $\mathbb{Q}(\sqrt{2})$ 는 갈루아이지만  $\mathbb{Q}(\sqrt[3]{2})$ 는 그렇지 않습니다.

이제 이 절의 시작에서 언급했던,  $\mathbb{Q}(\sqrt[3]{2})$ 가  $\mathbb{Q}(\sqrt{2})$ 는 그렇지 않은 방식으로 결핍되어 있다는 발상으로 돌아가고자 합니다.

먼저 "내부" 자기동형사상을 정의합니다.

**정의 59.5.1.**  $K/F$ 가 유한 확대라고 합시다. 그러면  $\mathrm{Aut}(K/F)$ 는  $F$ 를 고정하는 체 동형사상  $\sigma: K \rightarrow K$ 들의 집합입니다. 기호로 나타내면

$$\mathrm{Aut}(K/F) = \{\sigma: K \rightarrow K \mid \sigma \text{는 } F \text{ 위에서 항등입니다}\}.$$

이는 함수 합성에 대해 군을 이룹니다!

이번에는  $\sigma$ 에 의해  $F$ 가 고정된다는 조건이 있음에 유의하십시오. (앞서  $F = \mathbb{Q}$ 를 고려했을 때는 이 조건이 저절로 성립했기 때문에 이것이 없었습니다.)

**예제 59.5.2 (자기동형사상군의 예전 예시들)**

새로운 표기법으로 이 장 시작 부분의 예를 다시 살펴보면 다음과 같습니다:

(a)  $\mathrm{Aut}(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ 이며, 원소는  $z \mapsto z$ 와  $z \mapsto \bar{z}$ 입니다.

(b) 같은 방식으로  $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ 입니다.

(c)  $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ 는 자명군이며, 항등 임베딩만을 가집니다!

**예제 59.5.3 ( $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ 의 자기동형사상군)**

새로운 예를 들어보겠습니다:  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ 라고 합시다.  $\mathrm{Aut}(K/\mathbb{Q}) =$

$\{1, \sigma, \tau, \sigma\tau\}$ 임이 밝혀지며, 여기서

$$\sigma : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \quad \text{그리고} \quad \tau : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}.$$

다시 말해,  $\text{Aut}(K/\mathbb{Q})$ 는 클라인 4원군입니다.

먼저, 이러한 임베딩들이 근들을 뒤섞는다는 관찰(서론의 첫 번째 관찰과 유사한)의 증명을 반복해 봅시다:

#### 보조정리 59.5.4 ( $\text{Aut}(K/F)$ 에서의 근의 뒤섞임)

$f \in F[x]$ 라 하고,  $K/F$ 가 유한 확대라 가정하며,  $\alpha \in K$ 가  $f$ 의 근이라고 가정합니다. 그러면 임의의  $\sigma \in \text{Aut}(K/F)$ 에 대해,  $\sigma(\alpha)$  또한  $f$ 의 근입니다.

증명.  $f(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0$ 라 하고, 여기서  $c_i \in F$ 입니다. 따라서,

$$0 = \sigma(f(\alpha)) = \sigma(c_n \alpha^n + \cdots + c_0) = c_n \sigma(\alpha)^n + \cdots + c_0 = f(\sigma(\alpha)). \quad \square$$

특히,  $f$ 를  $\alpha$ 의 최소다항식으로 취하면 다음을 유도할 수 있습니다

**임베딩  $\sigma \in \text{Aut}(K/F)$ 는  $\alpha \in K$ 를 그것의 여러 갈루아 켄레( $F$  위에서의) 중 하나로 보냅니다.**

다음으로, 특정 체들의 “결핍”을 다시 살펴봅시다.  $K = \mathbb{Q}(\sqrt[3]{2})$ 를 봅시다. 그러면, 역시  $K/\mathbb{Q}$ 는 두 가지 이유로 결핍되어 있습니다. 첫째,  $\mathbb{Q}(\sqrt[3]{2}) \hookrightarrow \mathbb{C}$ 인 사상이 세 개 있지만, 그중 오직 하나만이  $\text{Aut}(K/\mathbb{Q})$ 에 속하며, 그것은 바로 항등사상입니다. 다시 말해,  $|\text{Aut}(K/\mathbb{Q})|$ 가 너무 작습니다. 둘째,  $K$ 에는 몇몇 갈루아 켄레( $\omega\sqrt[3]{2}$ 와  $\omega^2\sqrt[3]{2}$ )가 빠져 있습니다.

빠진 갈루아 켄레가 있다는 사실을 포착하는 방법이 바로 분해체라는 개념입니다.

**정의 59.5.5.**  $F$ 를 체라 하고  $p(x) \in F[x]$ 를 차수  $n$ 인 다항식이라 합시다. 그러면  $p(x)$ 는  $F$ 의 대수적 폐포 안에 근  $\alpha_1, \dots, \alpha_n$ 을 가집니다.  $F$  위에서의  $p(x)$ 의 **분해체**는  $F(\alpha_1, \dots, \alpha_n)$ 로 정의됩니다.

다시 말해, 분해체는  $p(x)$ 가 분해되는 가장 작은 체입니다.

#### 예제 59.5.6 (분해체의 예)

- (a)  $\mathbb{Q}$  위에서의  $x^2 - 5$ 의 분해체는  $\mathbb{Q}(\sqrt{5})$ 입니다. 이는 차수 2의 확대입니다.
- (b)  $\mathbb{Q}$  위에서의  $x^2 + x + 1$ 의 분해체는  $\mathbb{Q}(\omega)$ 이며, 여기서  $\omega$ 는 1의 세제곱근입니다. 이는 차수 2의 확대입니다.
- (c)  $x^2 + 3x + 2 = (x+1)(x+2)$ 의 분해체는 그냥  $\mathbb{Q}$ 입니다! 할 일이 없습니다.

#### 예제 59.5.7 (분해체: 주의해야 할 사례)

$\mathbb{Q}$  위에서의  $x^3 - 2$ 의 분해체는 사실

$$\mathbb{Q}(\sqrt[3]{2}, \omega)$$

단순히  $\mathbb{Q}(\sqrt[3]{2})$ 가 아닙니다! 정말로 모든 근을 첨가해야 하며, 이 근들이 서로를 생성하는 경우가 반드시 성립하는 것은 아닙니다.

명확히 하자면:

- $x^2 - 5$ 의 경우,  $\sqrt{5}$ 를 첨가하면 이는 자동으로  $-\sqrt{5}$ 를 포함하게 됩니다.
- $x^2 + x + 1$ 의 경우,  $\omega$ 를 첨가하면 다른 근  $\omega^2$ 도 공짜로 얻습니다.
- 하지만  $x^3 - 2$ 의 경우,  $\sqrt[3]{2}$ 를 첨가하더라도  $\omega\sqrt[3]{2}$ 와  $\omega^2\sqrt[3]{2}$ 를 공짜로 얻지는 못합니다. 실제로  $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ 입니다!

특히  $\mathbb{Q}$  위에서  $x^3 - 2$ 의 분해체는 삼차가 아니라 육차라는 점에 주목하십시오.

일반적으로, 다항식의 분해체는 최대  $n!$ 차까지의 확장이 될 수 있습니다. 그 이유는  $p(x)$ 가  $n$ 개의 근을 가지고 그 사이에 어떠한 "우연한" 관계도 없다면 근들의 어떤 치환이든 성립하기 때문입니다.

이제 다음을 얻습니다:

#### 정리 59.5.8 (갈루아 확장은 분해체입니다)

유한 확장  $K/F$ 에 대해,  $|\text{Aut}(K/F)|$ 는  $[K : F]$ 를 나누며, 등호는  $K$ 가  $F$ 에 계수를 갖는 어떤 분리 다항식의 분해체일 때 그리고 그때만 성립합니다.

이에 대한 증명은 이 장의 끝에 있는 선택적 절로 미룹니다.  $K/F$ 가 유한 확장이고  $|\text{Aut}(K/F)| = [K : F]$ 이면, 확장  $K/F$ 를 **갈루아**라고 부릅니다. 이 경우,  $\text{Aut}(K/F)$  대신  $\text{Gal}(K/F)$ 로 표기하고 이를  $K/F$ 의 **갈루아 군**이라고 부릅니다.

#### 예제 59.5.9 (갈루아 확장의 예와 비예)

- 확장  $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 는 갈루아 확장인데, 이는  $\mathbb{Q}$  위에서  $x^2 - 2$ 의 분해체이기 때문입니다. 갈루아 군은 위수 2를 가지며,  $\sqrt{2} \mapsto \pm\sqrt{2}$ 입니다.
- 확장  $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ 는 갈루아 확장인데, 이는  $\mathbb{Q}$  위에서  $(x^2 - 5)^2 - 24$ 의 분해체이기 때문입니다. 앞서 논의했듯이, 갈루아 군은  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 입니다.
- 확장  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ 는 갈루아 확장이 아닙니다.

마지막으로 한 번 더  $\mathbb{Q}(\sqrt[3]{2})$ 를 탐구해 봅시다:

#### 예제 59.5.10 (갈루아 폐포, 그리고 $\mathbb{Q}(\sqrt[3]{2}, \omega)$ 의 자기동형사상군)

체  $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ 로 돌아가 봅시다. 이는  $[K : \mathbb{Q}] = 6$ 인 체입니다. 다음 두 자기동형사상을 생각해 봅시다:

$$\sigma : \begin{cases} \sqrt[3]{2} & \mapsto \omega\sqrt[3]{2} \\ \omega & \mapsto \omega \end{cases} \quad \text{그리고} \quad \tau : \begin{cases} \sqrt[3]{2} & \mapsto \sqrt[3]{2} \\ \omega & \mapsto \omega^2. \end{cases}$$

$\sigma^3 = \tau^2 = \text{id}$ 임에 주목하십시오. 이로부터  $K$ 의 자기동형사상 군은 위수가 6이어야 함을 알 수 있습니다(위수는 확실히  $\leq 6$ 입니다; 이제 라그랑주 정리를 사용하십시오).

따라서  $K/\mathbb{Q}$ 는 갈루아입니다! 실제로 다음을 명시적으로 확인할 수 있습니다

$$\text{Gal}(K/\mathbb{Q}) \cong S_3$$

3개의 원소에 대한 대칭군이며, 위수는  $3! = 6$ 입니다.

이 예는 비갈루아 체 확장이 주어졌을 때, 빠진 켤레들을 "추가"하여 갈루아 확장으로 만들 수 있다는 사실을 보여줍니다. 이를 **갈루아 폐포**를 취한다고 부릅니다.

## §59.6 갈루아 이론의 기본 정리

갈루아 이론에 관한 이 모든 내용을 다룬 후, 증명은 하지 않겠지만 기본 정리를 알려드리는 것이 좋겠습니다. 기본적으로, 이 정리는  $K/F$ 가 갈루아 군  $G$ 를 갖는 갈루아 확장이라면 다음이 성립한다는 것을 말합니다:

**$G$ 의 부분군은  $F \subseteq E \subseteq K$ 를 만족하는 체  $E$ 와 정확히 대응합니다.**

이 전단사가 어떻게 이루어지는지 말씀드리려면, 고정체를 정의해야 합니다.

**정의 59.6.1.**  $K$ 를 체,  $H$ 를  $\text{Aut}(K/F)$ 의 부분군이라 합시다.  $H$ 의 **고정체**를  $K^H$ 로 표기하며, 다음과 같이 정의합니다

$$K^H := \{x \in K : \sigma(x) = x \ \forall \sigma \in H\}.$$

**질문 59.6.2.**  $K^H$ 가 실제로 체임을 빠르게 확인해 보십시오.

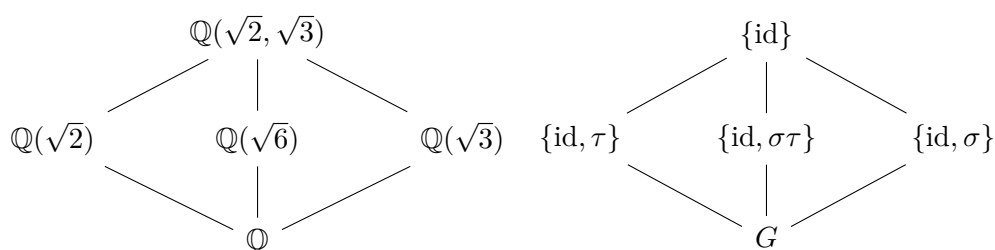
이제 다시 예시를 살펴봅시다.  $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ 를 생각해 보면,

$$G = \text{Gal}(K/\mathbb{Q}) = \{\text{id}, \sigma, \tau, \sigma\tau\}$$

는 클라인 사원군입니다 (여기서  $\sigma(\sqrt{2}) = -\sqrt{2}$ 이지만  $\sigma(\sqrt{3}) = \sqrt{3}$ 이며,  $\tau$ 는 그 반대 방향으로 작용합니다).

**질문 59.6.3.**  $H = \{\text{id}, \sigma\}$ 라 합시다.  $K^H$ 는 무엇입니까?

이 경우,  $\mathbb{Q}$ 와  $K$  사이의 체 도식은 다음과 같이  $G$ 의 부분군과 정확히 일치합니다.



부분군이 고정체에 대응함을 알 수 있습니다. 이 사실은, 그리고 그보다 훨씬 많은 것이, 일반적으로 성립합니다.

**정리 59.6.4 (갈루아 이론의 기본 정리)**

$K/F$ 를 갈루아 군  $G = \text{Gal}(K/F)$ 를 갖는 갈루아 확대라 합시다.

(a) 체 탑  $F \subseteq E \subseteq K$ 와 부분군  $H \subseteq G$  사이에는 전단사가 존재합니다.

$$\left\{ \begin{array}{c} K \\ | \\ E \\ | \\ F \end{array} \right\} \Longleftrightarrow \left\{ \begin{array}{c} 1 \\ | \\ H \\ | \\ G \end{array} \right\}$$

이 전단사는  $H$ 를 그 고정체  $K^H$ 로 보내며, 따라서 포함 관계를 뒤집습니다.

(b) 이 전단사 아래,  $[K : E] = |H|$ 이고  $[E : F] = |G/H|$ 입니다.

(c)  $K/E$ 는 항상 갈루아 확대이며, 그 갈루아 군은  $\text{Gal}(K/E) = H$ 입니다.

(d)  $E/F$ 가 갈루아 확대인 것은  $H$ 가  $G$ 의 정규부분군인 것과 동치입니다. 그러한 경우,  $\text{Gal}(E/F) = G/H$ 입니다.

**연습문제 59.6.5.** 이 정리를 다음의 경우에 적용해 봅시다

$$K = \mathbb{Q}(\sqrt[3]{2}, \omega).$$

$E = \mathbb{Q}(\sqrt[3]{2})$ 가 갈루아 확대가 아니라는 사실이  $S_3$ 가 위수 2인 정규부분군을 갖지 않는다는 사실에 대응함을 확인하십시오.

**§59.7 생각해 볼 만한 조금 더 어려운 문제**

**문제 59A\*** (원분체의 갈루아 군).  $p$ 를 홀수인 유리소수라 하고  $\zeta_p$ 를  $p$ 차 원시근이라 합시다.  $K = \mathbb{Q}(\zeta_p)$ 라 합시다. 다음을 보이십시오.

$$\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times.$$

**문제 59B.**  $\mathbb{Q}$ 의 3차 갈루아 확대의 예를 하나 드십시오.

**문제 59C** (그리스 작도). 세 가지 그리스 작도가

- (a) 정육면체의 배적,
- (b) 원의 정사각형화, 그리고
- (c) 각의 삼등분이

모두 불가능함을 증명하십시오. ( $\pi$ 가 초월수라고 가정하십시오.)



**문제 59D** (중국 홍콩 수학 올림피아드). 다음을 만족하는 유리수  $p, q, r$ 이 존재하지 않음을 증명하십시오.

$$\cos\left(\frac{2\pi}{7}\right) = p + \sqrt{q} + \sqrt[3]{r}.$$

**문제 59E.**  $\mathbb{R}$ 의 유일한 자기동형사상이 항등사상임을 보이십시오. 따라서  $\text{Aut}(\mathbb{R}/\mathbb{Q})$ 는 자명군입니다.



**문제 59F** (아르틴의 원시원소 정리).  $K$ 를 수체라고 합시다. 어떤  $\gamma$ 에 대해  $K \cong \mathbb{Q}(\gamma)$ 임을 보이십시오.

## §59.8 (선택) 갈루아 확장이 분해체임의 증명

정리 59.5.8를 증명합니다. 먼저, 기본 정리로부터 유용한 조각을 추출합니다.

### 정리 59.8.1 (고정체 정리)

$K$ 를 체라 하고  $G$ 를  $\text{Aut}(K)$ 의 부분군이라 합시다. 그러면  $[K : K^G] = |G|$ 입니다.

부등식 자체는 어렵지 않습니다:

**연습문제 59.8.2.**  $[K : F] \geq |\text{Aut}(K/F)|$ 임을 보이고, 모든  $\sigma \in \text{Aut}(K/F)$ 에 의해 고정되는 원소들의 집합이 정확히  $F$ 일 때에만 등호가 성립함을 보이십시오. (정리 59.8.1를 사용하십시오.)

등호가 성립하는 경우는 더 까다롭습니다.

더 쉬운 방향은  $K$ 가 분해체인 경우입니다.  $K = F(\alpha_1, \dots, \alpha_n)$ 가  $n$ 개의 서로 다른 근  $\alpha_1, \dots, \alpha_n$ 을 갖는 어떤 분리다항식  $p \in F[x]$ 의 분해체라고 합시다. 이들을 하나씩 첨가합니다:

$$\begin{array}{ccccccc} F & \hookrightarrow & F(\alpha_1) & \hookrightarrow & F(\alpha_1, \alpha_2) & \hookrightarrow & \dots \hookrightarrow K \\ \text{id} \downarrow & & \tau_1 \downarrow & & \tau_2 \downarrow & & \downarrow \tau_n = \sigma \\ F & \hookrightarrow & F(\alpha_1) & \hookrightarrow & F(\alpha_1, \alpha_2) & \hookrightarrow & \dots \hookrightarrow K \end{array}$$

(이 도식이 익숙해 보입니까?)  $F$ 를 고정하는 모든 사상  $K \rightarrow K$ 는 위의 가환 도식에 대응됩니다. 이전과 마찬가지로,  $\tau_1$ 을 선택하는 방법은 정확히  $[F(\alpha_1) : F]$ 가지입니다. (이를 위해서는  $\alpha_1$ 의 최소다항식  $p_1$ 이 분리다항식이라는 사실이 필요합니다:  $p_1$ 을 대응시킬 서로 다른 근이 정확히  $\deg p_1 = [F(\alpha_1) : F]$ 개 있어야 합니다.) 마찬가지로,  $\tau_1$ 의 선택이 주어지면,  $\tau_2$ 를 선택하는 방법은  $[F(\alpha_1, \alpha_2) : F(\alpha_1)]$ 가지입니다. 이들을 모두 곱하면 원하는  $[K : F]$ 가 나옵니다.

이제  $K/F$ 가 갈루아라고 가정합시다. 먼저, 다음을 서술합니다:

### 보조정리 59.8.3

$K/F$ 가 갈루아 확대이고  $p \in F[x]$ 가 기약이라고 합시다. 만약  $p$ 의 (근이  $\bar{F}$ 에 있는) 근 하나가  $K$ 에 속한다면, 모든 근이  $K$ 에 속하며, 실제로  $p$ 는 분리가능합니다.

증명.  $\alpha \in K$ 를 주어진 근이라 합시다. 다음 집합을 생각합니다

$$S = \{\sigma(\alpha) \mid \sigma \in \text{Gal}(K/F)\}.$$

( $\text{Gal}(K/F) \ni \text{id}$ 이므로  $\alpha \in S$ 임에 유의하십시오.) 구성상, 임의의  $\tau \in \text{Gal}(K/F)$ 는  $S$ 를 고정합니다. 그러므로 다음을 구성하면

$$\tilde{p}(x) = \prod_{\beta \in S} (x - \beta),$$

비에트의 공식에 의해,  $\tilde{p}$ 의 모든 계수가  $\sigma$ 의 원소들에 의해 고정됨을 알 수 있습니다. 연습문제에서 명시한 등호가 성립하는 경우에 의해,  $\tilde{p}$ 가  $F$ 에 계수를 갖는다는 것이 따라 나옵니다! (바로 이 지점에서 그 조건을 사용합니다.) 또한, 보조정리 59.5.4에 의해  $\tilde{p}$ 는  $p$ 를 나눕니다.

그런데  $p$ 는 기약다항식이었으므로, 이는  $F[x]$ 에서  $\alpha$ 의 최소다항식이며, 따라서  $p$ 가  $\hat{p}$ 를 나누어야 합니다. 그러므로  $p = \hat{p}$ 입니다.  $\hat{p}$ 가 분리다항식이 되도록 구성되었으므로,  $p$ 도 분리다항식입니다.  $\square$

이제 거의 다 끝났습니다 –  $K/F$ 의 기저  $\omega_1, \dots, \omega_n$ 을 선택하고,  $p_i$ 를 이들의 최소다항식이라고 합시다. 위의 사실에 의해,  $K$  바깥에서는 근을 얻지 않습니다.  $P = p_1 \dots p_n$ 을 생각하되, 반복되는 인수는 제거합니다.  $P$ 의 근은  $\omega_1, \dots, \omega_n$ 과  $K$  안의 다른 몇몇 원소입니다. 따라서  $K$ 는  $P$ 의 분해체입니다.

# 60 유한체

이 짧은 장에서는 원소가 유한개인 모든 체를 분류하고 갈루아 군을 계산합니다. 여기 나오는 내용은 그리 어렵지 않으므로 대부분의 증명은 개요만 제시합니다. 원한다면 세부 사항을 직접 확인해 보십시오.

이 장의 요점은 다음을 증명하는 것입니다:

- 유한체  $F$ 의 위수는 반드시  $p^n$ 이어야 하며, 이때  $p$ 는 소수이고  $n$ 은 정수입니다.
- 이 경우  $F$ 의 표수는  $p$ 입니다.
- 이러한 모든 체는 서로 동형이므로, 동형사상까지만 신경 쓴다면 위수  $p^n$ 의 “유일한” 유한체를 나타내는 데  $\mathbb{F}_{p^n}$ 이라는 표기를 관례적으로 사용합니다.
- 확장  $F/\mathbb{F}_p$ 는 갈루아 확장이며,  $\text{Gal}(F/\mathbb{F}_p)$ 는 위수  $n$ 인 순환군입니다. 생성원은 다음의 자기동형사상입니다.

$$\sigma: F \rightarrow F \quad \text{에 의해} \quad x \mapsto x^p.$$

급하다면 이 결과들만 기억하고 다음 장으로 넘어가도 됩니다.

## §60.1 유한체의 예

본격적으로 다루기 전에, 몇 가지 예를 들어보겠습니다.

체  $F$ 의 표수란 다음을 만족시키는 가장 작은 양의 정수  $p$ 임을 상기하십시오.

$$\underbrace{1_F + \cdots + 1_F}_{p \text{ 번}} = 0$$

그러한 정수  $p$ 가 존재하지 않으면 0입니다.

### 예제 60.1.1 (기저체)

$\mathbb{F}_p$ 가  $p$ 를 법으로 하는 정수들의 체를 나타낸다고 합시다. 이는 원소가  $p$ 개인 체이며, 표수는  $p$ 입니다.

### 예제 60.1.2 (원소 아홉 개짜리 유한체)

다음과 같이 둡시다

$$F \cong \mathbb{F}_3[X]/(X^2 + 1) \cong \mathbb{Z}[i]/(3).$$

그 원소들을 다음과 같이 생각할 수 있습니다.

$$\{a + bi \mid 0 \leq a, b \leq 2\}.$$

$\mathbb{Q}(i)$ 의 정수환인  $\mathbb{Z}[i]$ 에서  $(3)$ 이 소원소이므로,  $F$ 는 그 안에  $3^2 = 9$ 개의 원소를 가진 체임을 알 수 있습니다. 이 체는 원소가 9개이지만, 모든 원소  $x$ 가 다음의 성질을 가짐에 유의하십시오.

$$3x = \underbrace{x + \cdots + x}_{3 \text{ 번}} = 0.$$

특히  $F$ 의 표수는 3입니다.

## §60.2 유한체는 소수의 거듭제곱 위수를 가짐

### 보조정리 60.2.1

체  $F$ 의 표수가 0이 아니라면, 그것은 소수여야 합니다.

증명. 그렇지 않다고 가정합시다. 그러면  $a, b < n$ 에 대해  $n = ab$ 입니다. 이제 다음과 같이 둡시다

$$A = \underbrace{1_F + \cdots + 1_F}_{a\text{번}} \neq 0$$

그리고

$$B = \underbrace{1_F + \cdots + 1_F}_{b\text{번}} \neq 0.$$

그러면  $AB = 0$ 이 되어,  $F$ 가 체라는 사실에 모순됩니다.  $\square$

표수가 0인 체를 선호하지만, 불행히도 유한체의 경우에는 표수가 0이 아닐 수밖에 없습니다.

### 보조정리 60.2.2 (유한체는 소수 거듭제곱 위수를 가집니다)

$F$ 를 유한체라고 합시다. 그러면

- (a) 그 표수는 0이 아니며, 따라서 어떤 소수  $p$ 입니다.
- (b) 체  $F$ 는  $\mathbb{F}_p$ 의 유한 확대이며, 특히  $\mathbb{F}_p$ -벡터 공간입니다.
- (c) 어떤 소수  $p$ 와 정수  $n$ 에 대해  $|F| = p^n$ 입니다.

증명. 이는 쉬우므로 아주 간단히 설명하겠습니다:

- (a)  $(F, +)$ 에 라그랑주 정리(또는 비둘기집 원리!)를 적용하면 표수가 0이 아님을 얻습니다.
- (b)  $1_F$ 로 생성된  $(F, +)$ 의 덧셈 부분군은  $\mathbb{F}_p$ 의 동형인 사본입니다.
- (c) 체 확대이므로,  $F$ 는  $\mathbb{F}_p$  위의 유한 차원 벡터 공간이며, 어떤 기저  $e_1, \dots, e_n$ 을 가집니다. 따라서  $F$ 의 원소는  $p^n$ 개입니다.  $\square$

**비고 60.2.3** — (c)에 대한 재미있는 다른 증명은 모순에 의한 것입니다: 만약 소수  $q \neq p$ 가  $|F|$ 를 나눈다면,  $(F, +)$ 에 대한 코시 정리(문제 17A\*)에 의해 위수가  $q$ 인 (0이 아닌) 원소  $x$ 가 존재합니다. 그러면 명백히

$$x \cdot \underbrace{(1_F + \cdots + 1_F)}_{q\text{번}} = 0$$

이지만,  $x \neq 0$ 이므로,  $F$ 의 표수 또한  $q$ 를 나누게 되는데, 이는 불가능합니다.

위 증명에서 중요한 점은

**보조정리 60.2.4** (유한체는  $\mathbb{F}_p$ 의 체 확대입니다)

$|F| = p^n$ 인 유한체  $F$ 가 있다면,  $F$  내부에  $\mathbb{F}_p$ 의 동형인 사본이 존재합니다. 따라서  $F$ 는  $\mathbb{F}_p$ 의 체 확대입니다.

앞으로 이  $\mathbb{F}_p$ 의 사본을 자주 참조하고자 하므로, 이후에는:

**표기의 남용 60.2.5.** 모든 정수  $n$ 은  $F$ 의 원소로 동일시될 수 있으며, 즉

$$n := \underbrace{1_F + \cdots + 1_F}_{n \text{ 번}}$$

(예상대로) 이는 오직  $n \pmod{p}$ 에만 의존함에 유의하십시오.

이 표기법을 사용하면 다음과 같은 명제를 생각하기가 더 쉬워집니다.

**정리 60.2.6** (신입생의 꿈)

임의의  $a, b \in F$ 에 대해 다음이 성립합니다

$$(a + b)^p = a^p + b^p.$$

증명. 이항 정리와,  $0 < i < p$ 일 때  $\binom{p}{i}$ 가  $p$ 로 나누어떨어진다는 사실을 사용하십시오.  $\square$

**연습문제 60.2.7.** 이 증명이 성립함을 스스로 확인해 보십시오.

## §60.3 모든 유한체는 동형입니다

이제 "페르마의 소정리"를 증명해 보겠습니다:

**정리 60.3.1** (유한체에서의 페르마의 소정리)

$F$ 를 위수  $p^n$ 인 유한체라고 합시다. 그러면 모든 원소  $x \in F$ 는 다음을 만족합니다

$$x^{p^n} - x = 0.$$

증명.  $x = 0$ 이면 자명하게 성립합니다. 그렇지 않다면, 아벨 군  $(F, \times)$ 에 라그랑주 정리를 적용하여  $x^{p^n-1} = 1_F$ 를 얻습니다.  $\square$

이제 유한체에 관한 "주된 놀라운 사실", 즉 각 크기마다 동형사상까지 유일한 유한체가 존재한다는 다음 결과를 증명할 수 있습니다.

**정리 60.3.2** (유한체의 완전한 분류)

체  $F$ 가  $p^n$ 개의 원소를 갖는 유한체인 것은 그것이  $\mathbb{F}_p$  위에서  $x^{p^n} - x$ 의 분해체인 것과 동치입니다.

증명. "페르마의 소정리"에 의해,  $F$ 의 모든 원소는 이 다항식을 만족합니다. 따라서 우리는 이 다항식의 근들이 서로 다르다는 것(즉 그것이 분리가능하다는 것)만 보이면 됩니다.

이를 위해, 우리는 다시 미분 트릭을 사용합니다: 이 다항식의 도함수는 다음과 같습니다

$$p^n \cdot x^{p^n-1} - 1 = -1$$

이는 전혀 근을 갖지 않으므로, 이 다항식은 어떠한 중근도 가질 수 없습니다.  $\square$

**정의 60.3.3.** 이러한 이유로,  $p^n$ 개의 원소를 갖는 그 체를  $\mathbb{F}_{p^n}$ 으로 표기하는 것이 관례입니다.

다항식  $x^{p^n} - x \pmod{p}$ 는 결코 기약다항식이 아니지만, 위의 계산은 그것이 분리가능함을 보여줍니다.

**예제 60.3.4** (아홉 개의 원소를 갖는 유한체, 다시 한번)

다항식  $x^9 - x$ 는 법 3에 대해 분리가능하며 다음과 같이 인수분해됩니다

$$x(x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2) \pmod{3}.$$

따라서  $F$ 가 위수 9를 갖는다면, 우리는 직관적으로 그것이 모든 근들을 첨가하여 생성된 체일 것이라 기대합니다: 0, 1, 2, 그리고  $\pm i$ ,  $1 \pm i$ ,  $2 \pm i$ . 실제로 그것이 이 장의 처음에 다루었던 예제입니다.

(여기서  $i$ 는  $i^2 = -1$ 을 만족하는  $\mathbb{F}_9$ 의 한 원소를 나타냅니다. 이 표기법은 일반적인 허수 단위와 의도적으로 유사하게 되어 있습니다.)

## §60.4 유한체의 갈루아 이론

이제 (앞서와 같이  $F$  대신)  $\mathbb{F}_{p^n}$ 이라는 표기법을 유지합니다. 위의 정리에 의해, 그것은 분리가능 다항식의 분해체이므로, 우리는  $\mathbb{F}_{p^n}/\mathbb{F}_p$ 가 갈루아 확대임을 압니다. 우리는 갈루아 군을 구하고자 합니다.

사실, 우리는 매우 운이 좋습니다: 그것은 순환군입니다. 먼저, 우리는 그러한 원소 하나를 제시합니다:  $\sigma_p \in \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$

**정리 60.4.1** ( $p$ 제곱 자기동형사상)

다음과 같이 정의되는 사상  $\sigma_p: \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ 은

$$\sigma_p(x) = x^p$$

자기동형사상이며, 더욱이  $\mathbb{F}_p$ 를 고정합니다.

이것은 프로베니우스 자기동형사상이라 불리며, [장 62](#)에서 다시 등장할 것입니다.

증명. 이는 1을 고정하고, 곱셈을 보존하며, 덧셈을 보존하므로 준동형사상입니다.

**질문 60.4.2.** 왜 그것이 덧셈을 보존할까요?

다음으로, 우리는 그것이 단사 사상임을 주장합니다. 이를 확인하기 위해, 다음을 유의하십시오

$$x^p = y^p \iff x^p - y^p = 0 \iff (x - y)^p = 0 \iff x = y.$$

여기서 우리는 또다시 신입생의 꿈을 사용했습니다.  $\mathbb{F}_{p^n}$ 이 유한하므로, 이 단사 사상은 자동으로 전단사가 됩니다. 그것이  $\mathbb{F}_p$ 를 고정한다는 사실은 페르마의 소정리입니다.  $\square$

이제 우리는 끝났습니다:

**정리 60.4.3 (확대  $\mathbb{F}_{p^n}/\mathbb{F}_p$ 의 갈루아 군)**

$\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$ 이며, 생성원은  $\sigma_p$ 입니다.

증명.  $[\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ 이므로, 갈루아 군  $G$ 는 위수  $n$ 을 가집니다. 따라서  $\sigma_p \in G$ 가 위수  $n$ 을 가짐을 보이기만 하면 됩니다.

$\sigma_p$ 를  $k$ 번 적용하면  $x \mapsto x^{p^k}$ 가 됨에 주목하십시오. 따라서  $\mathbb{F}_{p^n}$ 의 모든 원소가  $x^{p^n} = x$ 를 만족하므로,  $\sigma_p$ 를  $n$ 번 적용하면 항등원이 됩니다. 하지만  $k < n$ 이면,  $\sigma_p$ 를  $k$ 번 적용한 것은 항등원이 될 수 없는데, 그렇지 않다면  $x^{p^k} = x$ 가 너무 많은 근을 가지게 되기 때문입니다.  $\square$

위수 9인 유한체를 통해 이러한 예를 다시 살펴볼 수 있습니다.

**예제 60.4.4 (위수 9인 유한체의 갈루아 군)**

$\mathbb{F}_9$ 를 위수 9인 유한체라 하고, 이를  $\mathbb{F}_9 = \mathbb{Z}[i]/(3)$ 로 구체적으로 나타내겠습니다.  $\sigma_3: \mathbb{F}_9 \rightarrow \mathbb{F}_9$ 를  $x \mapsto x^3$ 라 하겠습니다. 아홉 개 원소 모두의 행방을 살펴볼 수 있습니다:

$$\begin{array}{cccccc} 0 & 1 & 2 & i & 1+i & 2+i \\ & & & \updownarrow \sigma & \updownarrow \sigma & \updownarrow \sigma \\ & & & -i & 1-i & 2-i \end{array}$$

(주장한 대로, 0, 1, 2는 고정점이므로 이들에 대해서는 화살표를 그리지 않았습니다.)  
예상한 대로, 갈루아 군은 위수 2를 가집니다:

$$\text{Gal}(\mathbb{F}_9/\mathbb{F}_3) = \{\text{id}, \sigma_3\} \cong \mathbb{Z}/2\mathbb{Z}.$$

이로써 이 장의 시작 부분에서 언급한 모든 결과의 증명이 마무리됩니다.

## §60.5 추가: 유한체의 곱셈군

이 절에서는 이후 장들에서 사용되지는 않지만 그 자체로 흥미로운 결과를 증명하겠습니다. 위수  $p = 17$ 인 체  $F$ 를 생각해 봅시다.  $F$ 에 대해 다음과 같은 질문을 던져 볼 수 있습니다:

- $F$ 의 0이 아닌 원소 중 이차 잉여(즉,  $F$ 의 다른 원소의 제곱으로 나타낼 수 있는 것)는 몇 개입니까?
- $F$ 에서  $x^2 = -1$ 을 만족하는 원소  $x$ 가 존재합니까?

다음 명제를 이용하면 위 질문들이 쉬워집니다.

**명제 60.5.1**

$F$ 를 유한체라 하면, 곱셈군  $F^\times$ 는 순환군입니다.

본질적으로 이는 곱셈군  $F^\times$ 가 최대한 좋은 성질을 가진다는 것을 말해줍니다 — 순환군은 가장 단순한 아벨 군입니다!

위의 예들을 다시 살펴보면, 이러한 지식이 어떻게 도움이 되는지 알 수 있습니다.

**예제 60.5.2** ( $\mathbb{F}_{17}$ 의 곱셈군)

군  $F^\times$ 는 위수 16의 순환군이므로,  $F$ 의 모든 원소가 다음과 같이 나타나도록 하는 어떤 원소  $g \in F^\times$ 가 존재합니다

$$0, g^0 = 1, g^1, g^2, \dots, g^{15}.$$

이 지식을 이용하여 0이 아닌 원소들을 제공해 보면, 그 결과가 다음과 같음을 쉽게 알 수 있습니다 (여기서  $g^{16} = g^0 = 1$ 임에 유의하십시오):

$$g^0, g^2, g^4, \dots, g^{14}, g^0, g^2, \dots, g^{14}.$$

이와 같이,  $F^\times$ 의 원소 중 정확히 절반 — 8개의 원소 — 이 이차 잉여입니다!  $x^2 = -1$ 을 만족하는 원소  $x$ 가 존재하는지 확인하는 것도 그리 어렵지 않습니다. 먼저, 수열  $\{g^0, g^1, \dots, g^{15}\}$ 에서  $-1$ 은 어디에 나타날 수 있습니까?  $g$ 의 구체적인 값을 구해 보면 (예를 들어  $g = 3$ 을 선택할 수 있습니다)  $g^8 = -1$ 임을 알 수 있습니다. 하지만 구체적인 계산 없이도 다음과 같이 알 수 있습니다:

**질문 60.5.3.** 방정식  $x^2 = 1$ 은 오직 2개의 근, 1과  $-1$ 만을 가짐에 유의하십시오. 군  $F^\times$ 에서의 군 연산을 이용하면, 이 방정식은 무엇을 말해줍니까?

$g^8 = -1$ 이므로,  $(g^4)^2 = (g^{12})^2 = -1$ 이고, 따라서 증명이 완료됩니다.

그렇다면 이 명제는 왜 참입니까? 위수가 소수의 거듭제곱  $q$ 인 유한체  $F$ 를 생각해 봅시다. 먼저, 위와 유사한 아이디어를 이용하면 다음을 얻습니다:

**질문 60.5.4.** 임의의 양의  $d < |F^\times| = q-1$ 에 대해,  $x^d = 1$ 을 만족하는 원소  $x$ 는 최대  $d$ 개임을 보이십시오.

나머지는 군론을 이용하여 쉽게 처리할 수 있습니다. **정리 18.1.5**로부터,  $F^\times$ 는 유한 아벨 군이므로 특히 유한 생성이고, 다음과 같은 형태로 쓸 수 있음을 상기하십시오.

$$F^\times \cong \mathbb{Z}^{\oplus r} \oplus \mathbb{Z}/q_1\mathbb{Z} \oplus \mathbb{Z}/q_2\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/q_m\mathbb{Z}.$$

물론, 여기서  $r = 0$ 입니다.

이제  $F^\times$ 가 순환군이 아니라고 가정하면, 모든  $q_i$  값의 최소공배수는  $|F^\times|$ 보다 작습니다. 그러면 모든  $x \in F^\times$ 에 대해  $x^{\text{lcm}(q_1, \dots, q_m)} = 1$ 이 되어 모순이 발생합니다.

**비고 60.5.5** —  $p$ 를 법으로 하는 이차 잉여가 정확히  $\frac{p-1}{2}$ 개 존재하는 이유에 대한 초등적인 증명을 찾아본다면, 대부분의 경우 위 증명과 비슷하게 “ $x^d = 1$ 은 근을 최대  $d$ 개 가진다”라는 논증을 얻게 되지만, 끝까지 나아가 곱셈군의 구조를 보여주지 않음으로써 실제로 무슨 일이 벌어지고 있는지의 본질을 감추게 됩니다.

위의 명제는 한 걸음 더 나아갑니다 — 이제 아무런 계산 없이도, 예를 들어 유한체  $\mathbb{F}_{17^2}$ 가 정확히  $\frac{17^2-1}{2} = 144$ 개의 0이 아닌 이차 잉여를 가짐을 알 수 있습니다.

## §60.6 생각해 볼 만한 조금 더 어려운 문제



**문제 60A<sup>†</sup>** (HMMT 2017). 127을 법으로 한 피보나치 수열의 주기는 무엇입니까?

# 61 분지 이론

우리는 유리 소수  $p$ 가 더 큰 수체  $K$ 에서 어떻게 인수분해되는지에 큰 관심을 가지고 있습니다. 이러한 행동의 몇 가지 예로,  $\mathbb{Z}[i]$ (이는 UFD입니다!)에서 다음과 같은 인수분해를 가집시다

$$\begin{aligned}(2) &= (1+i)^2 \\ (3) &= (3) \\ (5) &= (2+i)(2-i).\end{aligned}$$

이번 장에서는 소수가 더 큰 수체에 던져졌을 때 어떻게 분해되는지에 대해 더 배워보겠습니다. 갈루아 이론의 무기를 사용하여, 이는 이차 상호법칙의 증명으로 절정에 이를 것입니다.

## §61.1 분지된 / 비활성 / 분할 소수

**이 절의 대표적인 예:**  $\mathbb{Z}[i]$ 에서, 2는 분지되고, 3은 비활성이며, 5는 분할됩니다.

$p$ 를 유리 소수라 하고, 이를  $\mathcal{O}_K$ 에 던져 넣습니다. 그러면 소 아이디얼로의 인수분해를 얻습니다

$$p \cdot \mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}.$$

우리는 각  $\mathfrak{p}_i$ 가  $(p)$ 의 **위에**<sup>1</sup> 있다고 말합니다. 그림으로는 다음과 같이 그릴 수 있습니다:

$$\begin{array}{ccccc} K & & \supset & & \mathcal{O}_K & & \mathfrak{p}_i \\ | & & & & | & & | \\ \mathbb{Q} & & \supset & & \mathbb{Z} & & (p)\end{array}$$

일어날 수 있는 다양한 행동에 대한 몇 가지 이름:

- 우리는 어떤  $i$ 에 대해  $e_i > 1$ 이면  $p$ 가 **분지되었다**고 말합니다. 예를 들어 2는  $\mathbb{Z}[i]$ 에서 분지됩니다.
- 우리는  $g = 1$ 이고  $e_1 = 1$ 이면  $p$ 가 **비활성**이라고 말합니다. 즉  $(p)$ 가 소 아이디얼로 남는 경우입니다. 예를 들어 3은  $\mathbb{Z}[i]$ 에서 비활성입니다.
- 우리는  $g > 1$ 이면  $p$ 가 **분할**된다고 말합니다. 예를 들어 5는  $\mathbb{Z}[i]$ 에서 분할됩니다.

**질문 61.1.1.** 더 일반적으로,  $\mathbb{Z}[i]$ 에서 소수  $p$ 에 대해:

- $p$ 가 분지되는 것은 정확히  $p = 2$ 일 때입니다.
- $p$ 가 비활성인 것은 정확히  $p \equiv 3 \pmod{4}$ 일 때입니다.
- $p$ 가 분할되는 것은 정확히  $p \equiv 1 \pmod{4}$ 일 때입니다.

이를 증명하십시오.

<sup>1</sup> $p \cdot \mathcal{O}_K$ 와  $(p)$ 는 같은 것을 의미한다는 점을 상기시켜 드리며, 저는 이 둘을 서로 바꾸어 사용할 것입니다.

## §61.2 소수는 $\Delta_K$ 를 나눌 때에만 분지됩니다

가장 특이한 경우는 분지입니다: 임의로 선택된 다항식이 중근을 가질 것이라고 기대하지 않는 것처럼, 우리는 임의로 선택된 소수가 분지될 것이라고 기대하지 않습니다. 사실, 분지를 이해하는 열쇠는 판별식입니다.

논의를 위해,  $K$ 가 단생성이고,  $\mathcal{O}_K = \mathbb{Z}[\theta]$ 이며,  $\theta$ 가 최소다항식  $f$ 를 가진다고 가정합니다.  $p$ 를 우리가 인수분해하고자 하는 유리 소수라 합시다. 만약  $f$ 가  $f_1^{e_1} \dots f_g^{e_g}$ 로 인수분해된다면,  $(p)$ 의 소 아이디얼 인수분해는 다음과 같이 주어진다 것을 알고 있습니다

$$p \cdot \mathcal{O}_K = \prod_i (p, f_i(\theta))^{e_i}.$$

특히,  $p$ 가 분지되는 것은 정확히  $f$ 가 법  $p$ 에서 중근을 가질 때입니다! 이런 일이 일어나는지 탐지하기 위해, 우리는  $f$ 의 다항식 판별식을 살펴봅니다, 즉

$$\Delta(f) = \prod_{i < j} (z_i - z_j)^2$$

그리고 이것이 법  $p$ 에서 영인지 확인합니다 – 따라서  $p$ 는 이것이 참일 때에만 분지됩니다.

$\Delta(f)$ 를  $K$ 의 판별식  $\Delta_K$ 로 그저 대체하면 임의의 수체에 대한 순진한 일반화가 통한다는 것이 밝혀집니다(단일생성  $\mathcal{O}_K$ 의 경우 이 둘이 같다는 것은 **문제 57C\***에 의합니다). 즉,

### 정리 61.2.1 (판별식은 분지를 탐지한다)

$p$ 를 유리 소수,  $K$ 를 수체라 합시다. 그러면  $p$ 가 분지되는 것은 정확히  $p$ 가  $\Delta_K$ 를 나눌 때입니다.

### 예제 61.2.2 (가우스 정수에서의 분지)

$K = \mathbb{Q}(i)$ 라고 하면  $\mathcal{O}_K = \mathbb{Z}[i]$ 이고  $\Delta_K = -4$ 입니다. 예측한 대로,  $\mathbb{Z}[i]$ 에서 분기하는 유일한 소수는  $\Delta_K$ 의 유일한 소인수인 2입니다.

특히, 오직 유한히 많은 소수만이 분기합니다.

## §61.3 관성차수

**이 절의 대표적인 예:**  $\mathbb{Z}[i]$ 에서 (7)은 관성차수 2를 가지며,  $(2+i)$ 는  $\mathbb{Z}[i]$ 에서 관성차수 1을 가집니다.

아이디얼  $\mathfrak{a}$ 가 얼마나 “넓은지”를 측정하는 아이디얼 노름  $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$ 를 정의할 수 있었음을 상기하십시오. 예를 들어,  $\mathbb{Z}[i]$ 에서 (5)는 아이디얼 노름  $5^2 = 25$ 를 가지는데, 그 이유는

$$\mathbb{Z}[i]/(5) \cong \{a + bi \mid a, b \in \mathbb{Z}/5\mathbb{Z}\}$$

$5^2 = 25$ 개의 원소를 가지기 때문입니다.

이제, 다음을 살펴봅시다

$$p \cdot \mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$$

$K$ 가 차수  $n$ 을 가지는  $\mathcal{O}_K$ 에서 말입니다. 양변의 아이디얼 노름을 취하면, 다음을 얻습니다

$$p^n = N(\mathfrak{p}_1)^{e_1} \dots N(\mathfrak{p}_g)^{e_g}.$$



$\sigma$ 들이 모두 전단사(이들은 자기동형사상이기 때문입니다!)이므로, 같은 궤도에 속한 소 아이디얼들이 밀접하게 관련되어 있다는 것은 그리 놀랍지 않을 것입니다. 하지만 놀랍게도, 궤도는 오직 하나뿐임이 밝혀집니다!

#### 정리 61.4.2 (갈루아 군은 추이적으로 작용한다)

$K/\mathbb{Q}$ 가  $G = \text{Gal}(K/\mathbb{Q})$ 인 갈루아 확장이라 합시다.  $\{\mathfrak{p}_i\}$ 를  $p \cdot \mathcal{O}_K$ 의 ( $\mathcal{O}_K$ 에서의) 인수분해에 나타나는 서로 다른 소 아이디얼들의 집합이라 합시다. 그러면  $G$ 는  $\mathfrak{p}_i$ 에 추이적으로 작용합니다: 모든  $i$ 와  $j$ 에 대해,  $\sigma \mathfrak{p}_i = \mathfrak{p}_j$ 가 되는  $\sigma$ 를 찾을 수 있습니다.

다시 말해,

**모든  $\{\mathfrak{p}_i\}$ 는 서로 갈루아 켄레입니다.**

이를 증명하기 전에, 원소로의 인수분해라는 더 쉬운 문제를 생각해 봅시다.

$\mathcal{O}_K$ 가 UFD이고,  $p$ 가  $\mathcal{O}_K$ 에서  $up_1p_2 \cdots p_n$ 으로 인수분해된다고 합시다. 여기서  $p_i$ 는 기약원이고  $u$ 는 단원입니다.  $p_i$ 들이 단원 곱을 제외하면 모두 서로 켄레임을 보이십시오.

**질문 61.4.3.** 아래를 읽기 전에 먼저 증명해 보십시오. (힌트: 갈루아 이론. 또는  $p_1$ 의 노름을 취해 보십시오.)

증명.  $q = N_{K/\mathbb{Q}}(p_1)$ 을  $p_1$ 의 모든 켄레의 곱이라 하면,  $q \in \mathbb{Q}$ 입니다. 따라서  $p \mid q$ 이므로, 각  $p_i$ 는  $q$ 의 인수이며, 유일 인수분해에 의해 증명이 끝납니다.  $\square$

안타깝게도, 아이디얼  $\mathfrak{p}_1$ 의 모든 켄레의 곱이 반드시  $p \cdot \mathcal{O}_K$  꼴인 것은 아닙니다(예를 들어,  $K = \mathbb{Q}[i]$ 이고  $(1+i)$ 는 다른 켄레를 갖지 않습니다). 그래서 증명에서는  $\mathfrak{p}_1$ 의 "대표원"이 되는  $x$ 를 선택합니다.

**정리 61.4.2**의 증명.  $\mathfrak{p}_i$ 가 서로 다른 소 아이디얼이므로, 중국인의 나머지 정리에 의해 다음을 만족하는  $x \in \mathcal{O}_K$ 를 찾을 수 있습니다

$$\begin{aligned} x &\equiv 0 \pmod{\mathfrak{p}_1} \\ x &\equiv 1 \pmod{\mathfrak{p}_i} \quad i \geq 2 \text{에 대해} \end{aligned}$$

그런 다음, 노름을 계산하면

$$N_{K/\mathbb{Q}}(x) = \prod_{\sigma \in \text{Gal}(K/\mathbb{Q})} \sigma(x).$$

$K/\mathbb{Q}$ 가 갈루아이므로 각  $\sigma(x)$ 는  $K$ 에 속합니다!

$N_{K/\mathbb{Q}}(x)$ 는 정수이고  $\mathfrak{p}_1$ 로 나누어떨어지므로,  $N_{K/\mathbb{Q}}(x)$ 는  $p$ 로도 나누어떨어져야 합니다. 따라서  $\mathfrak{p}_2$ 로도 나누어떨어져야 합니다. 그러므로 어떤  $\sigma \in \text{Gal}(K/\mathbb{Q})$ 에 대해  $\sigma(x)$ 가  $\mathfrak{p}_2$ 로 나누어떨어지고, 이는 곧  $x$ 가  $\sigma^{-1}\mathfrak{p}_2$ 로 나누어떨어짐과 동치입니다. 그러나  $x$ 를 선택한 방식에 의해,  $p$ 의 인수들 중에서  $x$ 는 오직  $\mathfrak{p}_1$ 로만 나누어떨어집니다! 따라서  $\sigma^{-1}\mathfrak{p}_2 = \mathfrak{p}_1$ 이고, 증명이 끝났습니다.  $\square$

**정리 61.4.4** (잉여차수와 분기지수는 모두 같습니다)

$K/\mathbb{Q}$ 가 갈루아라고 합시다. 그러면 임의의 유리 소수  $p$ 에 대해 다음이 성립합니다

$$p \cdot \mathcal{O}_K = (\mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_g)^e$$

어떤  $e$ 에 대해, 여기서  $\mathfrak{p}_i$ 는 동일한 잉여차수  $f$ 를 갖는 서로 다른  $s$  아이디얼입니다. 따라서

$$[K : \mathbb{Q}] = efg.$$

증명. 잉여차수들이 같음을 보이려면, 각  $\sigma$ 가 다음과 같은 동형사상을 유도함에 주목하십시오

$$\mathcal{O}_K/\mathfrak{p} \cong \mathcal{O}_K/\sigma(\mathfrak{p}).$$

작용이 추이적이므로, 모든  $f_i$ 는 같습니다.

**연습문제 61.4.5.**  $\sigma \in \text{Gal}(K/\mathbb{Q})$ 라는 사실을 이용하여, 다음을 보이십시오

$$\sigma^{\text{img}}(p \cdot \mathcal{O}_K) = p \cdot \sigma^{\text{img}}(\mathcal{O}_K) = p \cdot \mathcal{O}_K.$$

따라서 모든  $\sigma$ 에 대해,  $p \cdot \mathcal{O}_K = \prod \mathfrak{p}_i^{e_i} = \prod (\sigma \mathfrak{p}_i)^{e_i}$ 가 성립합니다. 작용이 추이적이므로, 모든  $e_i$ 는 같습니다.  $\square$

이에 대한 예시를 살펴봅시다.

**예제 61.4.6** (갈루아/비갈루아 확대에서 5를 인수분해하기)

$p = 5$ 를 소수라 합시다.

- (a)  $E = \mathbb{Q}(\sqrt[3]{2})$ 라 합시다.  $\mathcal{O}_E = \mathbb{Z}[\sqrt[3]{2}]$ 임을 보일 수 있으므로, 최소다항식  $x^3 - 2$ 에 대해 인수분해 알고리즘을 사용합니다.  $x^3 - 2 \equiv (x - 3)(x^2 + 3x + 9) \pmod{5}$ 가 기약 인수분해이므로, 다음을 얻습니다

$$(5) = (5, \sqrt[3]{2} - 3)(5, \sqrt[3]{4} + 3\sqrt[3]{2} + 9)$$

이들은 각각 잉여차수 1과 2를 갖습니다. 이것이 균일하지 않다는 사실은  $E$ 가 갈루아가 아님을 반영합니다.

- (b) 이제  $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ 라 합시다. 이는  $\mathbb{Q}$  위에서  $x^3 - 2$ 의 분해체이며, 이제  $K$ 는 갈루아입니다. 다음이 성립함이 밝혀집니다

$$\mathcal{O}_K = \mathbb{Z}[\varepsilon] \quad \text{여기서} \quad \varepsilon \text{의 근임} t^6 + 3t^5 - 5t^3 + 3t + 1.$$

(이를 얻는 데는 많은 작업이 필요하므로 여기서는 하지 않겠습니다). 5로 나눈 나머지로 보면 이는  $(x^2 + x + 2)(x^2 + 3x + 3)(x^2 + 4x + 1) \pmod{5}$ 라는 기약 인수분해를 가지므로, 인수분해 알고리즘에 의해

$$(5) = (5, \varepsilon^2 + \varepsilon + 2)(5, \varepsilon^2 + 3\varepsilon + 3)(5, \varepsilon^2 + 4\varepsilon + 1).$$

이번에는 정리가  $K$ 가 갈루아일 때 예측하는 대로, 모든 관성차수가 2입니다.

## §61.5 (선택) 분해군과 관성군

$p$ 를 유리 소수라 합시다. 그러면

$$p \cdot \mathcal{O}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^e$$

그리고 모든  $\mathfrak{p}_i$ 는 관성차수  $f$ 를 가집니다.  $\mathfrak{p}$ 가  $\mathfrak{p}_i$  중 하나의 선택을 나타내도록 합시다.

우리는 체  $\mathcal{O}_K/\mathfrak{p}$ 와  $\mathbb{Z}/p = \mathbb{F}_p$ 를 모두 살펴볼 수 있습니다. 자연스럽게,  $\mathcal{O}_K/\mathfrak{p}$ 가 유한체이므로 이를  $\mathbb{F}_p$ 의 체 확장으로 볼 수 있습니다. 따라서 다음 도식을 얻을 수 있습니다

$$\begin{array}{ccccc} K & \supset & \mathcal{O}_K & \mathfrak{p} & \mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^f} \\ | & & | & | & | \\ \mathbb{Q} & \supset & \mathbb{Z} & (p) & \mathbb{F}_p \end{array}$$

맨 오른쪽에는 유한체 확장이 있는데, 이것이 정말로 잘 작동한다는 것을 우리는 알고 있습니다. 그래서 우리는 다음을 묻습니다:

$\text{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p)$ 와  $\text{Gal}(K/\mathbb{Q})$ 는 어떤 관계가 있습니까?

먼저, 모든  $\sigma \in \text{Gal}(K/\mathbb{Q})$ 는  $\mathcal{O}_K$ 의 자기동형사상을 유도하며, 이는 다음과 같이 사상  $\mathcal{O}_K \rightarrow \mathcal{O}_K/\mathfrak{p}$ 를 유도합니다

$$\alpha \mapsto \sigma(\alpha) \pmod{\mathfrak{p}}.$$

이것이  $\text{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p)$ 에서의 사상을 유도하려면,  $\sigma(\mathfrak{p}) \subseteq \mathfrak{p}$ 일 필요가 있습니다. 그래서 우리는  $\mathfrak{p}$ 를 고정하는 자기동형사상들의 부분집합을 고려합니다:

**정의 61.5.1.**  $D_{\mathfrak{p}} \subseteq \text{Gal}(K/\mathbb{Q})$ 를  $\mathfrak{p}$ 의 안정자군이라 합시다. 즉

$$D_{\mathfrak{p}} := \{\sigma \in \text{Gal}(K/\mathbb{Q}) \mid \sigma\mathfrak{p} = \mathfrak{p}\}.$$

우리는  $D_{\mathfrak{p}}$ 를  $\mathfrak{p}$ 의 **분해군**이라 부릅니다.

이 정의는 사실  $\sigma(\mathfrak{p}) \subseteq \mathfrak{p}$ 인  $\sigma$ 들의 집합과 동치임에 유의하십시오. 왜냐하면 체 동형사상은 아이디얼 노름  $N(\mathfrak{p})$ 을 고정하기 때문입니다.

그러므로 다음과 같은 자연스러운 사상이 있습니다

$$D_{\mathfrak{p}} \xrightarrow{\theta} \text{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p)$$

$\theta(\sigma)$ 를 단순히 " $\sigma \pmod{\mathfrak{p}}$ "로 선언함으로써입니다.  $\sigma \in D_{\mathfrak{p}}$ 라는 사실(즉  $\sigma$ 가  $\mathfrak{p}$ 를 고정한다는 사실)이 이 사상이 잘 정의됨을 보장합니다.

놀랍게도,  $\text{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p)$ 의 모든 원소는 이러한 방식으로  $K$ 의 어떤 체 자기동형사상으로부터 나옵니다.

### 정리 61.5.2 (분해군과 갈루아군)

$\theta$ 를 위와 같이 정의합시다. 그러면

- $\theta$ 는 전사이며,
- 그 핵은 위수  $e$ 인 군이며, 이는 분기 지수입니다.

특히,  $p$ 가 비분기이면  $D_{\mathfrak{p}} \cong \text{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p)$ 입니다.

(증명은 어렵지 않지만 다소 길고, 제 생각에는 그다지 계몽적이지 않습니다.)

$p$ 가 비분기이면,  $\mathfrak{p}$ 를 법으로 취함으로써  $D_{\mathfrak{p}} \cong \text{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p)$ 를 얻습니다.

$\text{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p)$ 이 정확히 무엇인지 우리는 이미 알고 있습니다! 이미  $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^f}$ 임을 알고 있으며, 갈루아 군은

$$\text{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p) \cong \text{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p) \cong \langle x \mapsto x^p \rangle \cong \mathbb{Z}/f\mathbb{Z}.$$

따라서

$$D_{\mathfrak{p}} \cong \mathbb{Z}/f\mathbb{Z}$$

역시 성립합니다.

이제 다시

$$D_{\mathfrak{p}} \xrightarrow{\theta} \text{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p).$$

$\theta$ 의 핵은 **관성군**이라 불리며  $I_{\mathfrak{p}} \subseteq D_{\mathfrak{p}}$ 로 표기하고, 위수  $e$ 를 가집니다.

이로써 부분군의 아주 멋진 수열  $\{1\} \subseteq I \subseteq D \subseteq G$ 을 얻습니다. 여기서  $G$ 는 갈루아 군입니다 (이제부터는  $\mathfrak{p}$ -첨자를 생략하겠습니다). 갈루아 이론의 기본 정리를 통해 대응하는 고정체를 살펴봅시다. 그림으로 나타내면:

$$\begin{array}{ccccc} \mathfrak{p} \subset \mathcal{O}_K \subset & K & \longleftrightarrow & \{1\} \\ & \uparrow \text{Ramify} & & \downarrow e \\ & K^I & & I \\ & \uparrow \text{Inert} & & \downarrow f \\ & K^D & & D \\ & \uparrow \text{Split} & & \downarrow g \\ (p) \subset \mathbb{Z} \subset & \mathbb{Q} & \longleftrightarrow & G \end{array}$$

흥미로운 일이 일어납니다:

- $D \leq G$ 일 경우,  $(p)$ 를  $K^D$ 로 끌어올리면 완전히 갈라져서  $g$ 개의 비분기 소 아이디얼이 됩니다. 이들 각각은 관성차수가 1입니다.
- $I \leq G$ 이기도 하다면,  $K^D$ 의 소 아이디얼들을  $K^I$ 로 끌어올릴 때 그것들은 관성 상태를 유지하며, 이제 관성차수가  $f$ 가 됩니다.
- 그런 다음  $K$ 로 끌어올리면, 그것들은 지수  $e$ 로 분기됩니다 (그러나 전혀 갈라지지는 않습니다).

다시 말해, 1에서  $efg$ 로 가는 과정은 위의 세 단계로 아주 깔끔하게 나눌 수 있습니다. 이를 그림으로 그리면 다음과 같습니다

$$(p) \longrightarrow \mathfrak{p}'_1 \dots \mathfrak{p}'_g \longrightarrow \mathfrak{p}''_1 \dots \mathfrak{p}''_g \longrightarrow (\mathfrak{p}_1 \dots \mathfrak{p}_g)^e$$

$$\{f_i\}: \quad 1, \dots, 1 \quad f, \dots, f \quad f, \dots, f$$

$$\mathbb{Q} \xrightarrow{\text{Split}} K^D \xrightarrow{\text{Inert}} K^I \xrightarrow{\text{Ramify}} K$$

어쨌든, 분기가 없는 "일반적인" 경우에는 그저  $K^I = K$ 가 됩니다.

**예제 61.5.3** (소 아이디얼이 관성 상태로 남기 전에 먼저 갈라지는 경우)

$\zeta_5$ 가 원시 5차 단위근인  $K = \mathbb{Q}[\zeta_5]$ 라 합시다. **문제 59A\***로부터, 갈루아 군  $\text{Gal}(K/\mathbb{Q})$ 가  $(\mathbb{Z}/5\mathbb{Z})^* \cong \mathbb{Z}/4\mathbb{Z}$ 와 동형임을 알고 있습니다.

$p = 19$ 라 합시다.  $K$ 에서  $p$ 는  $19 = (2\sqrt{5}+1)(2\sqrt{5}-1)$ 로 인수분해되며, 운 좋게도  $\mathcal{O}_K$ 는 주 아이디얼 정역이므로, 이는 아이디얼  $(19) = \mathfrak{p}_1\mathfrak{p}_2 = (2\sqrt{5}+1)(2\sqrt{5}-1)$ 로 인수분해됨을 의미합니다.

이 경우,  $K^{D_{\mathfrak{p}_1}} = K^D = \mathbb{Q}[\sqrt{5}]$ 이고  $K^I = K$ 이며, 실제로:

- $(19)$ 를  $K^D$ 로 끌어올리면, 이미  $(2\sqrt{5}+1)(2\sqrt{5}-1)$ 로 갈라집니다 — 왜냐하면  $2\sqrt{5}+1 \in K^D$ 이기 때문입니다.  $[K^D : \mathbb{Q}] = 2$ 이고  $(19)$ 가 이미 2개의 소 아이디얼로 갈라졌으므로, 각 소 아이디얼은 필연적으로 관성차수가 1이어야 합니다.
- $(2\sqrt{5}+1)$ 과  $(2\sqrt{5}-1)$  각각을  $K^D$ 에서  $K$ 로 끌어올리면, 그것들은 관성 상태를 유지합니다. 다시,  $[K : K^D] = 2$ 이므로 관성차수는 반드시 2여야 합니다.

정리의 일부는 아주 쉽게 확인할 수 있습니다: 갈루아 이론의 기본 정리에 의해,  $D$ 의 모든 체 자기동형사상이  $2\sqrt{5}+1$ 을 고정하므로, 동어반복적으로  $2\sqrt{5}+1$ 은  $D$ 의 고정체에 속해야 합니다! 다시 말해,  $2\sqrt{5}+1 \in K^D$ 이며, 이는  $p$ 가  $K^D$ 로 끌어올려질 때 이미 갈라짐을 의미합니다.

$\mathfrak{p}'_1 = \mathfrak{p}_1 \cap K^D$ 가  $K^D$ 에서  $K$ 로 끌어올려질 때 갈라지지 않음을 보이려면 논증을 약간만 수정하면 됩니다: 확장  $K/K^D$ 가 갈루아 확장이므로, 갈루아 군  $\text{Gal}(K/K^D)$ 는  $\mathfrak{p}'_1 = (2\sqrt{5}+1) \subseteq K^D$  위에 있는 소 아이디얼들  $\mathfrak{p}_i$ 에 추이적으로 작용하지만,  $D$ 의 정의에 의해 이번에도  $\mathfrak{p}_1$ 이 그 궤도에서 유일한 소 아이디얼입니다.

**예제 61.5.4** (서로 다른 소 아이디얼은 서로 다른  $K^D$ 를 가짐)

$D \nsubseteq G$ 일 때는,  $p$ 가 그 체로 끌어올려질 때  $\mathfrak{p}_1 \dots \mathfrak{p}_g$ 로 깔끔하게 갈라지는 단일한 부분체  $K^D$ 가 존재할 필요가 없습니다.

이유는 간단합니다 — 각 소 아이디얼  $\mathfrak{p}_i$ 는 곱에서 자신만의  $K^{D_{\mathfrak{p}_i}}$  안에서 갈라지지만,  $D_{\mathfrak{p}_1}$ 이  $G$ 에서 정규가 아니라면 서로 다른  $D_{\mathfrak{p}_i}$ 들은 서로 같지 않습니다 — 대신, 이들은  $G$ 의 켄레 부분군들입니다.

구체적인 예를 들어봅시다:  $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ 를  $\mathbb{Q}$  위에서  $x^3 - 2$ 의 분해체라 합시다. 유리 소 아이디얼  $p = (5)$ 는  $K$ 에서  $p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ 로 갈라지며, 각각은 관성차수가 2입니다. 따라서 각  $i$ 에 대해  $|D_{\mathfrak{p}_i}| = 2$ 입니다.

$\text{Gal}(K/\mathbb{Q}) \cong S_3$ 임을 알고 있으며,  $S_3$ 에는 위수 2인 정규 부분군이 없으므로,  $D_{\mathfrak{p}_i}$ 가  $G$ 에서 정규가 아님은 명백합니다!

앞서 언급했듯이, 여기서 일어나는 일은 다음과 같습니다:  $p$ 가  $K^{D_{\mathfrak{p}_1}}$ 로 올라갈 때, 이는  $\mathfrak{p}'_1\mathfrak{p}'_{23}$ 로 분해되며,  $\mathfrak{p}_1$ 은  $\mathfrak{p}'_1$  위에 있고  $\mathfrak{p}_2$ 와  $\mathfrak{p}_3$ 는 모두  $\mathfrak{p}'_{23}$  위에 있습니다. 확장  $K^{D_{\mathfrak{p}_1}}/\mathbb{Q}$ 에서  $\mathfrak{p}'_1$ 은 이전과 마찬가지로 관성차수가 1이지만,  $\mathfrak{p}'_{23}$ 은 관성차수가 2입니다.

**§61.6** **결가지 소견: 더 일반적인 갈루아 확장**

갈루아 확장에 관한 모든 논의는  $K/\mathbb{Q}$ 를 다른 갈루아 확장  $L/F$ 로 바꾸어도 그대로 성립합니다. 유리 소수  $p$ 가  $\mathcal{O}_K$ 에서 분해되는 대신,  $F$ 의 소 아이디얼  $\mathfrak{p}$ 가 다음과 같이 분해될 것입니다

$$\mathfrak{p} \cdot \mathcal{O}_L = (\mathfrak{P}_1 \dots \mathfrak{P}_g)^e$$

$\mathcal{O}_L$ 에서, 그러면 모든 결과가 그대로 성립합니다. ( $\mathfrak{p}_i$ 는  $\mathfrak{p}$  위에 있는  $L$ 의 소수들입니다.)  $\mathbb{F}_p$  대신  $\mathcal{O}_F/\mathfrak{p}$ 를 사용하게 될 것입니다.

제가  $F = \mathbb{Q}$ 로 작업하기로 선택한 이유는, 대문자 고딕체  $P(\mathfrak{p})$ 가 정말 무섭게 생겼기 때문입니다.

## §61.7 생각해 볼 만한 조금 더 어려운 문제

더 많은 문제

**문제 61A<sup>†</sup>.** 유리 소수  $p$ 가  $x^3 - 2$ 의 분해체인  $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ 에서 비활성(inert)으로 남을 수 없음을 증명하십시오. 이는 어떻게 일반화되니까?



# 62 프로베니우스 원소

이 장 전체에서  $K/\mathbb{Q}$ 는 갈루아 군  $G$ 를 갖는 갈루아 확장이고,  $p$ 는  $K$ 에서 비분기인 유리 소수이며,  $\mathfrak{p}$ 는 그 위에 있는 소 아이디얼입니다. 그림:

$$\begin{array}{ccccccc} K & \supset & \mathcal{O}_K & \mathfrak{p} & \mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^f} \\ | & & | & | & | \\ \mathbb{Q} & \supset & \mathbb{Z} & (p) & \mathbb{F}_p \end{array}$$

$p$ 제곱 사상  $\sigma: \mathbb{F}_{p^f} \rightarrow \mathbb{F}_{p^f}$ 가 자기동형사상이라는 것을 상기하며, 이는  $\mathbb{F}_{p^f}$  위의 프로베니우스 사상이라고 불립니다. 이 사상을  $\sigma(x) = x^p$ 로 정의하여  $K \rightarrow K$  사상으로 확장하려 시도할 수 있지만, 안타깝게도 이는 체의 자기동형사상이 되지 않습니다.

놀랍게도, 그림에도 불구하고 이를 어떤 체 자기동형사상  $\sigma \in \text{Gal}(K/\mathbb{Q})$ 로 확장하는 것이 가능합니다.

$p$ 가 비분기라면, 모든  $\alpha \in \mathcal{O}_K$ 에 대해  $\sigma(\alpha) \equiv \alpha^p \pmod{\mathfrak{p}}$ 를 만족하는 유일한  $\sigma \in \text{Gal}(K/\mathbb{Q})$ 가 존재함을 보일 수 있습니다.

## §62.1 프로베니우스 원소들

**이 절의 대표적인 예:**  $\mathbb{Z}[i]$ 에서의  $\text{Frob}_{\mathfrak{p}}$ 는  $p \pmod{4}$ 에 따라 달라집니다.

여기 정리 진술을 다시 적습니다:

### 정리 62.1.1 (프로베니우스 원소)

$K/\mathbb{Q}$ 가 갈루아 군  $G$ 를 갖는 갈루아 확장이라고 가정합니다.  $p$ 를  $K$ 에서 비분기인 유리 소수로,  $\mathfrak{p}$ 를 그 위에 있는 소 아이디얼로 둡니다. 모든  $\alpha \in \mathcal{O}_K$ 에 대해 다음 성질을 갖는 유일한 원소  $\text{Frob}_{\mathfrak{p}} \in G$ 가 존재합니다,

$$\text{Frob}_{\mathfrak{p}}(\alpha) \equiv \alpha^p \pmod{\mathfrak{p}}.$$

이는  $\mathfrak{p}$ 에서의 **프로베니우스 원소**라고 불리며, 위수  $f$ 를 갖습니다.

유일성 부분이 상당히 중요합니다: 이는 주어진  $\sigma \in \text{Gal}(K/\mathbb{Q})$ 가 위의 함수 방정식을 만족한다는 것만 관찰함으로써 그것이 프로베니우스 원소임을 보일 수 있게 해줍니다.

이에 대한 예를 살펴봅시다:

### 예제 62.1.2 (가우스 정수의 프로베니우스 원소들)

$\mathcal{O}_K = \mathbb{Z}[i]$ 를 갖는  $K = \mathbb{Q}(i)$ 에 대해 실제로 몇 가지 프로베니우스 원소를 계산해봅시다. 이는 갈루아 확장이며,  $G = (\mathbb{Z}/2\mathbb{Z})^\times$ 는 항등원과 복소켈레에 대응합니다.  $p$ 가 그 위에  $\mathfrak{p}$ 를 갖는 홀수 소수라면,  $\text{Frob}_{\mathfrak{p}}$ 는 다음을 만족하는 유일한 원소입니다

$$(a + bi)^p \equiv \text{Frob}_{\mathfrak{p}}(a + bi) \pmod{\mathfrak{p}}$$

$\mathbb{Z}[i]$ 에서. 특히,

$$\text{Frob}_{\mathfrak{p}}(i) = i^p = \begin{cases} i & p \equiv 1 \pmod{4} \\ -i & p \equiv 3 \pmod{4}. \end{cases}$$

이로부터  $p \equiv 1 \pmod{4}$ 일 때  $\text{Frob}_p$ 는 항등원이고,  $p \equiv 3 \pmod{4}$ 일 때  $\text{Frob}_p$ 는 복소켈레임을 알 수 있습니다.

우리가 실제로  $i$ 에서만  $\text{Frob}_p$ 를 계산하면 되었다는 점에 주목하십시오. 이것이 너무 그럴 듯해서 믿기 어렵게 느껴진다면, 철학적인 이유는  $(x+y)^p \equiv x^p + y^p \pmod{p}$  (따라서  $p$ 를 범으로도 성립)인 "신입생의 꿈"입니다. 그러므로  $\sigma$ 가 생성원들에서 함수 방정식을 만족한다면, 이는 모든 곳에서 함수 방정식을 만족합니다.

우리는 또한 중요한 보조정리를 갖고 있습니다:

### 보조정리 62.1.3 (프로베니우스 원소의 위수)

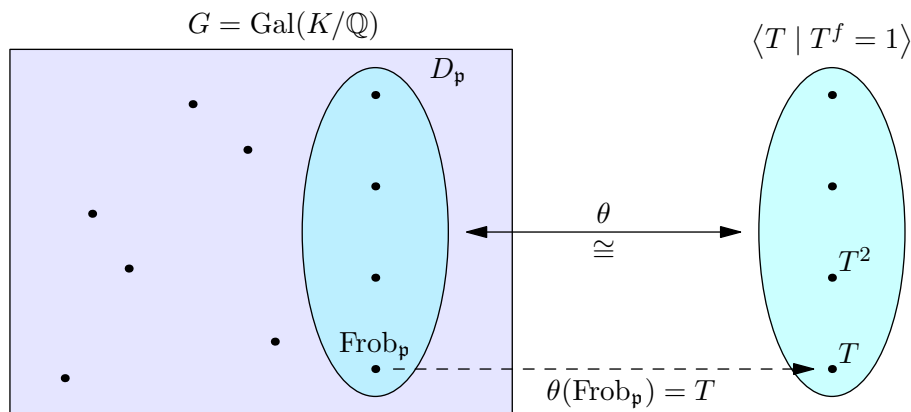
$\text{Frob}_p$ 를 확장  $K/\mathbb{Q}$ 로부터 나온 프로베니우스 원소라고 합니다. 그러면  $\text{Frob}_p$ 의 위수는 관성차수  $f_p$ 와 같습니다. 특히,  $(p)$ 가  $\mathcal{O}_K$ 에서 완전히 분해되는 것은  $\text{Frob}_p = \text{id}$ 일 때이고 오직 그때에만 성립합니다.

이 보조정리는  $\text{Frob}_p$ 를 계산하는 것만으로  $p$ 의 분해 양상을 알 수 있게 해주며, 이는 나중에 [보조정리 62.4.1](#)와 [절 62.6.iii](#)에서 보게 될 것입니다.

**연습문제 62.1.4.**  $\mathcal{O}_K/\mathfrak{p}$ 가 위수  $f_p$ 인 유한체이고, 프로베니우스 원소가 이 체에서 단지  $x \mapsto x^p$ 라는 사실을 이용하여 이 보조정리를 증명하십시오.

이제 주요 정리를 증명해 봅시다. 이는 분해군의 맥락에서만 의미가 있으므로, 그 부분을 건너뛴 독자는 이 증명을 생략해야 합니다.

프로베니우스 원소의 존재성 증명. 이 정리 전체는 앞 절에서 정의된 사상  $\theta$ 가  $p$ 가 비분기일 때 동형사상이라는 사실을 다시 서술한 것에 불과합니다. 그림:



여기서는  $D_p$ 에 주목해도 충분한데,  $\alpha \equiv 0 \pmod{\mathfrak{p}}$ 일 때  $\sigma(\alpha) \equiv 0 \pmod{\mathfrak{p}}$ 이어야 하기 때문입니다. 따라서 다음과 같은 동형사상을 얻습니다

$$D_p \xrightarrow{\theta} \text{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p).$$

하지만 우리는 이미 다음의 동형사상들의 연쇄에 따라  $\text{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p)$ 를 알고 있습니다

$$\text{Gal}((\mathcal{O}_K/\mathfrak{p})/\mathbb{F}_p) \cong \text{Gal}(\mathbb{F}_{p^f}/\mathbb{F}_p) \cong \langle T = x \mapsto x^p \rangle \cong \mathbb{Z}/f\mathbb{Z}.$$

따라서 그러한 유일한 원소는  $\theta$ 에 대한  $T$ 의 원상입니다. □

## §62.2 켈레류

이제  $\mathfrak{p}_1$ 과  $\mathfrak{p}_2$ 가 비분기 유리 소수  $p$  위에 있는 두 소 아이디얼이라고 합시다. 그러면  $\text{Frob}_{\mathfrak{p}_1}$ 과  $\text{Frob}_{\mathfrak{p}_2}$ 를 정의할 수 있습니다. 갈루아 군이 추이적으로 작용하므로, 다음을 만족하는  $\sigma \in \text{Gal}(K/\mathbb{Q})$ 를 선택할 수 있습니다

$$\sigma(\mathfrak{p}_1) = \mathfrak{p}_2.$$

우리는 다음을 주장합니다

$$\text{Frob}_{\mathfrak{p}_2} = \sigma \circ \text{Frob}_{\mathfrak{p}_1} \circ \sigma^{-1}.$$

이는  $G$ 에서의 방정식임에 유의하십시오.

**질문 62.2.1.** 이를 증명하십시오.

더 일반적으로, 주어진 비분기 유리 소수  $p$ 에 대해 다음을 연습니다:

### 정리 62.2.2 (갈루아 군에서의 켈레류)

다음 집합은

$$\{\text{Frob}_{\mathfrak{p}} \mid \mathfrak{p} \text{ 위에서의 } p\}$$

$G$ 의 켈레류 중 하나입니다.

증명. 우리는  $G = \text{Gal}(K/\mathbb{Q})$ 가 추이적이라는 사실을 이용하여,  $\text{Frob}_{\mathfrak{p}_1}$ 과  $\text{Frob}_{\mathfrak{p}_2}$ 가 둘 다  $p$  위에 있을 때 서로 켈레임을 보였습니다. 따라서 그것은 어떤 켈레류에 포함되어 있습니다. 그러므로 남은 것은, 임의의  $\mathfrak{p}$ ,  $\sigma$ 에 대해  $\sigma \circ \text{Frob}_{\mathfrak{p}} \circ \sigma^{-1} = \text{Frob}_{\mathfrak{p}'}$ 가 되는 어떤  $\mathfrak{p}'$ 가 존재함을 확인하는 것입니다. 이를 위해서는 그냥  $\mathfrak{p}' = \sigma\mathfrak{p}$ 로 놓으면 됩니다. 따라서 그 집합은 실제로 켈레류입니다.  $\square$

요약하면,

$\text{Frob}_{\mathfrak{p}}$ 는  $\mathfrak{p}$ 가 유래한 소수  $p$ 에 의해 켈레 관계까지 결정됩니다.

그러므로 고딕 문자가 겹나 보이더라도,  $\text{Frob}_{\mathfrak{p}}$ 의 내용은 사실 더 친숙해 보이는 유리 소수  $p$ 로부터 나오는 것에 불과합니다.

### 예제 62.2.3 ( $\mathbb{Q}(\sqrt[3]{2}, \omega)$ 에서의 프로베니우스 원소)

이러한 언급을 바탕으로, 프로베니우스 사상의 더 복잡한 예를 살펴봅시다.  $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ 를 다음의 분해체라 합시다

$$t^3 - 2 = (t - \sqrt[3]{2})(t - \omega\sqrt[3]{2})(t - \omega^2\sqrt[3]{2}).$$

따라서  $K/\mathbb{Q}$ 는 갈루아입니다. 앞선 예에서 우리는 다음을 보았습니다

$$\mathcal{O}_K = \mathbb{Z}[\varepsilon] \quad \text{여기서 } \varepsilon \text{의 근이다 } t^6 + 3t^5 - 5t^3 + 3t + 1.$$

다음과 같이 인수분해되는(여기서는 그냥 믿어주십시오) 소수 5를 생각해 봅시다

$$(5) = (5, \varepsilon^2 + \varepsilon + 2)(5, \varepsilon^2 + 3\varepsilon + 3)(5, \varepsilon^2 + 4\varepsilon + 1) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3.$$

모든 소 아이디얼의 관성차수가 2임에 유의하십시오. 따라서 각  $i$ 에 대해  $\text{Frob}_{\mathfrak{p}_i}$ 는 위수 2를 갖게 됩니다.

다음에 유의하십시오

$$\text{Gal}(K/\mathbb{Q}) = \text{의 순열} \{ \sqrt[3]{2}, \omega \sqrt[3]{2}, \omega^2 \sqrt[3]{2} \} \cong S_3.$$

이  $S_3$ 에는 위수가 2인 원소가 3개 있는데, 하나의 근을 고정하고 나머지 두 근을 교환하는 것들입니다. 이들은 각각  $\text{Frob}_{p_1}$ ,  $\text{Frob}_{p_2}$ ,  $\text{Frob}_{p_3}$ 에 대응됩니다. 결론적으로, (5)에 결부된 켈레류  $\{\text{Frob}_{p_1}, \text{Frob}_{p_2}, \text{Frob}_{p_3}\}$ 는  $S_3$ 에서 순환 유형  $(\bullet)(\bullet\bullet)$ 입니다.

## §62.3 체보타레프 밀도 정리

자연스러운 질문: 모든 켈레류를 이런 방식으로 나타낼 수 있습니까? 다시 말해,  $G$ 의 모든 원소는 어떤  $p$ 에 대해  $\text{Frob}_p$ 와 같습니까?

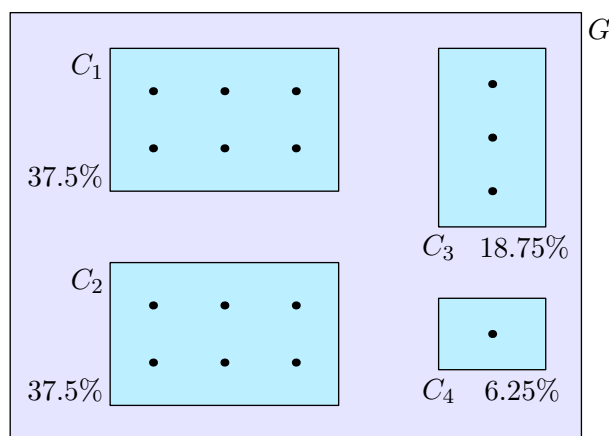
놀랍게도 답은 "예"일 뿐만 아니라, 실제로는 가장 좋은 방식으로 그렇게 됩니다: 임의의  $p$ 를 뽑을 때  $\text{Frob}_p$ 들은 "균등하게 분포"합니다.

### 정리 62.3.1 ( $\mathbb{Q}$ 위의 체보타레프 밀도 정리)

$C$ 를  $G = \text{Gal}(K/\mathbb{Q})$ 의 켈레류라 합시다.  $\{\text{Frob}_p \mid p \text{ 위에서의 } p\} = C$ 를 만족하는 (비분기) 소수  $p$ 들의 밀도는 정확히  $|C|/|G|$ 입니다. 특히, 임의의  $\sigma \in G$ 에 대해  $\text{Frob}_p = \sigma$ 가 되도록  $p$  위에 있는  $\mathfrak{p}$ 를 갖는 유리 소수  $p$ 가 무한히 많이 존재합니다.

여기서 밀도란, 조건을 만족하는 소수  $p \leq x$ 의 비율이  $x \rightarrow \infty$ 일 때  $|C|/|G|$ 에 가까워진다는 뜻입니다.  $K$ 에서 분기되는 소수들은 제외하고 있음에 유의하십시오. 분기되는 소수는 오직  $\Delta_K$ 를 나누는 소수들뿐이고, 이는 유한 개밖에 없으므로 문제가 되지 않습니다.

다시 말해, 무작위로 소수  $p$ 를 뽑아 그 결과로 나오는 켈레류를 살펴보는 것은  $G$ 에 다트를 던지는 것과 매우 비슷합니다: 어떤 켈레류에 맞을 확률은 오직 그 켈레류의 크기에만 좌우됩니다.



**비고 62.3.2** — 다행히도 이 정리(및 앞선 논의)는  $K/\mathbb{Q}$ 를 임의의 갈루아 확장  $K/F$ 로 바꾸어도 그대로 성립합니다; 이 경우 " $p$  위의  $\mathfrak{p}$ "를 " $\mathfrak{p}$  위의  $\mathfrak{P}$ "로 바꿉니다. 이 경우, 밀도를 정의하는 방식으로  $p \leq x$  대신  $N(\mathfrak{p}) \leq x$ 를 사용합니다.

## §62.4 예시: 원분체의 프로베니우스 원소

$q$ 를 소수라 하고,  $\zeta_q$ 를 원시  $q$ 제곱근 단위근이라 할 때  $L = \mathbb{Q}(\zeta_q)$ 를 생각합시다. 여러 별표 문제들로부터 다음을 기억하고 있어야 합니다.

- $\Delta_L = \pm q^{q-2}$ ,
- $\mathcal{O}_L = \mathbb{Z}[\zeta_q]$ 이며,
- 

$$\sigma_n: L \rightarrow L \quad \text{에 의해} \quad \zeta_q \mapsto \zeta_q^n$$

이 사상은  $\gcd(n, q) = 1$ 일 때마다  $L$ 의 자기동형사상이며,  $n \pmod{q}$ 에만 의존합니다. 다시 말해,  $L/\mathbb{Q}$ 의 자기동형사상들은 그저  $q$ 제곱근 단위근들을 뒤섞을 뿐입니다. 실제로 갈루아 군은 정확히 원소들  $\{\sigma_n\}$ 으로 이루어져 있으며, 즉

$$\text{Gal}(L/\mathbb{Q}) = \{\sigma_n \mid n \not\equiv 0 \pmod{q}\}.$$

군으로서,

$$\text{Gal}(L/\mathbb{Q}) = (\mathbb{Z}/q\mathbb{Z})^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}.$$

이는 놀랍도록 좋은데, 왜냐하면  $\text{Gal}(L/\mathbb{Q})$ 의 원소들이 이미 프로베니우스 원소와 매우 비슷하게 생겼기 때문입니다. 구체적으로:

### 보조정리 62.4.1 (원분체 프로베니우스 원소)

원분체 설정  $L = \mathbb{Q}(\zeta_q)$ 에서,  $p$ 를 비분기 유리 소수라 하고 그 위의  $\mathfrak{p}$ 를 생각합시다. 그러면

$$\text{Frob}_{\mathfrak{p}} = \sigma_p.$$

증명.  $\sigma_p$ 가 함수 방정식을 만족함을 관찰하십시오(생성원에서 확인하십시오). 유일성에 의해 증명이 끝납니다.  $\square$

**질문 62.4.2.** 유리 소수  $p$ 가  $\mathcal{O}_L$ 에서 완전히 분해되는 것은 정확히  $p \equiv 1 \pmod{q}$ 일 때임을 결론지으십시오.

## §62.5 프로베니우스 원소는 제한 사상과 잘 어울립니다

$L/\mathbb{Q}$ 와  $K/\mathbb{Q}$ 를 갈루아 확장이라 하고, 다음 설정을 생각합시다

$$\begin{array}{ccc} L & \supset & \mathfrak{P} \cdots \cdots \rightarrow \text{Frob}_{\mathfrak{P}} \in \text{Gal}(L/\mathbb{Q}) \\ | & & | \\ K & \supset & \mathfrak{p} \cdots \cdots \rightarrow \text{Frob}_{\mathfrak{p}} \in \text{Gal}(K/\mathbb{Q}) \\ | & & | \\ \mathbb{Q} & \supset & (p) \end{array}$$

여기서  $\mathfrak{p}$ 는  $(p)$  위에 있고  $\mathfrak{P}$ 는  $\mathfrak{p}$  위에 있습니다. 우리는 다음과 같이 정의할 수 있습니다

$$\text{Frob}_{\mathfrak{p}}: K \rightarrow K \quad \text{그리고} \quad \text{Frob}_{\mathfrak{P}}: L \rightarrow L$$

그리고 이들이 어떻게 관련되는지 알고 싶습니다.

$\text{Frob}_{\mathfrak{p}}$ 와  $\text{Frob}_{\mathfrak{p}}$  두 사상 모두 대응하는 몫체에서  $p$ 의 거듭제곱 사상을 유도하므로, 자연스럽게 이들이 같으리라 예상할 수 있습니다.

### 정리 62.5.1

[프로베니우스 원소의 제한]  $K/\mathbb{Q}$ 와  $L/\mathbb{Q}$ 가 모두 갈루아 확대라고 가정합니다. 위와 같이  $\mathfrak{p}$ 와  $\mathfrak{p}$ 가 비분지라고 합시다. 그러면  $\text{Frob}_{\mathfrak{p}}|_K = \text{Frob}_{\mathfrak{p}}$ 이며, 즉 모든  $\alpha \in K$ 에 대해

$$\text{Frob}_{\mathfrak{p}}(\alpha) = \text{Frob}_{\mathfrak{p}}(\alpha).$$

증명. 먼저,  $K/\mathbb{Q}$ 가 정규 확대이므로  $\text{Frob}_{\mathfrak{p}}$ 는  $K$ 의 상을 고정합니다. 즉,  $\text{Frob}_{\mathfrak{p}}|_K \in \text{Gal}(K/\mathbb{Q})$ 가 잘 정의됩니다.

자연스러운 사상  $\phi: \mathcal{O}_K \rightarrow \mathcal{O}_L \rightarrow \mathcal{O}_L/\mathfrak{p}$ 와 몫 사상  $q: \mathcal{O}_K \rightarrow \mathcal{O}_K/\mathfrak{p}$ 가 있습니다.  $\mathfrak{p} \subseteq \mathfrak{p} \cap \mathcal{O}_K \subseteq \ker \phi$ 이므로,  $\phi$ 는  $q$ 를 통해 인수분해되어 자연스러운 체 준동형사상  $\mathcal{O}_K/\mathfrak{p} \rightarrow \mathcal{O}_L/\mathfrak{p}$ 를 줍니다.

체 준동형사상은 단사이므로,  $\text{Frob}_{\mathfrak{p}}$ 는  $\mathcal{O}_L/\mathfrak{p}$  위에서  $p$ 거듭제곱 사상을 유도하며, 모든 것이 가환이므로 정리가 성립합니다.  $\square$

요컨대, 이 절의 요점은 다음과 같습니다.

**위쪽의 프로베니우스 원소는 아래쪽의 프로베니우스 원소로 제한됩니다.**

## §62.6 응용: 이차 상호법칙

이제 다음을 증명하고자 합니다.

### 정리 62.6.1 (이차 상호법칙)

$p$ 와  $q$ 를 서로 다른 홀수 소수라 합시다. 그러면

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

(이차 상호법칙에 익숙하지 않다면, 예를 들어 이에 대한 설명은 [Le]을 참고하십시오.)

### §62.6.i 1단계: 설정

이 증명을 위해, 먼저 다음을 정의합니다.

$$L = \mathbb{Q}(\zeta_q)$$

여기서  $\zeta_q$ 는 원시  $q$ 차 단위근입니다. 그러면  $L/\mathbb{Q}$ 는 갈루아 확대이며, 갈루아 군은  $G$ 입니다.

**질문 62.6.2.**  $G$ 가 지표 2인 부분군  $H$ 를 유일하게 가짐을 보이십시오.

사실, 이를 정확히 기술할 수 있습니다.  $G \cong (\mathbb{Z}/q\mathbb{Z})^\times$ 로 볼 때, 다음이 성립합니다.

$$H = \{\sigma_n \mid q \text{ 법으로 } n \text{ 이차잉여}\}.$$

갈루아 이론의 기본정리에 의해,  $\mathbb{Q}(\zeta_q)$  안에는  $\mathbb{Q}$ 의 차수 2인 확대(즉, 이차체)가 존재해야 합니다. 이를  $q^*$ 가 제곱인수가 없는 수일 때  $\mathbb{Q}(\sqrt{q^*})$ 라 부릅니다.

$$\begin{array}{ccc}
 L = \mathbb{Q}(\zeta_q) & \longleftrightarrow & \{1\} \\
 \downarrow \frac{q-1}{2} & & \downarrow \\
 K = \mathbb{Q}(\sqrt{q^*}) & \longleftrightarrow & H \\
 \downarrow 2 & & \downarrow \\
 \mathbb{Q} & \longleftrightarrow & G
 \end{array}$$

**연습문제 62.6.3.** 유리 소수  $\ell$ 이  $K$ 에서 분기하면  $L$ 에서도 분기함에 주의하십시오. 이를 이용하여 다음을 보이십시오.

$$q^* = \pm q \text{ 그리고 } q^* \equiv 1 \pmod{4}.$$

이 둘을 종합하면  $q^*$ 의 값이 결정됩니다.

(사실, 탑  $L/K/\mathbb{Q}$ 에서 일반적으로  $\Delta_K$ 가  $\Delta_L$ 을 나눈다는 것이 성립합니다.)

### §62.6.ii 2단계: 재정식화

이제 다음을 증명하고자 합니다.

#### 정리 62.6.4 (이차 상호법칙, 동치인 정식화)

서로 다른 홀수 소수  $p, q$ 에 대해 다음이 성립합니다.

$$\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right).$$

**연습문제 62.6.5.**  $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ 이라는 사실을 이용하여, 이것이 우리가 알고 있는 이차 상호법칙과 동치임을 보이십시오.

$\mathbb{Z}$ 에서 유리 소수  $p$ 를 살펴봅시다. 이는  $K$ 에서 둘로 분해되거나 비활성이 되는데, 어느 경우든  $\mathfrak{p}$ 를 그 결과 분해에서의 소인자라 합시다(즉, 비활성인 경우  $\mathfrak{p}$ 는  $p \cdot \mathcal{O}_K$ 이고, 분해되는 경우에는 그 소인자 중 하나입니다). 그다음  $\mathfrak{p}$  위에 있는 소인자를  $\mathfrak{P}$ 라 합시다. 이는  $K$ 에서도 분해될 수 있습니다. 그림은 다음과 같습니다.

$$\mathcal{O}_L = \mathbb{Z}[\zeta_q] \quad \supset \quad \mathfrak{P} \longrightarrow \mathbb{Z}[\zeta_q]/\mathfrak{P} \cong \mathbb{F}_{p^f}$$

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{q^*}}{2}\right] \quad \supset \quad \mathfrak{p} \longrightarrow \mathbb{F}_p \text{ 또는 } \mathbb{F}_{p^2}$$

$$\mathbb{Z} \quad \supset \quad (p) \longrightarrow \mathbb{F}_p$$

**질문 62.6.6.**  $p$ 가  $K$ 와  $L$  어느 쪽에서도 분기하지 않는 이유는 무엇입니까?

### §62.6.iii 3단계: 프로베니우스 도입하기

이제, 프로베니우스를 취합니다

$$\sigma_p = \text{Frob}_{\mathfrak{P}} \in \text{Gal}(L/\mathbb{Q}).$$

우리는 다음을 주장합니다

$$\text{Frob}_{\mathfrak{p}} \in H \iff K \text{에서 } p \text{가 분해됨.}$$

이를 확인하려면,  $\text{Frob}_{\mathfrak{p}}$ 가  $H$ 에 속하는 것은 그것이  $K$  위에서 항등원으로 작용하는 것과 동치임에 주목하십시오. 그런데  $\text{Frob}_{\mathfrak{p}}|_K$ 는 바로  $\text{Frob}_p$ 입니다! 따라서

$$\text{Frob}_{\mathfrak{p}} \in H \iff \text{Frob}_p = \text{id}_K.$$

마지막으로, 보조정리 62.1.3에 의해,  $\text{Frob}_p$ 의 위수는  $p$ 가 분해될 때( $p$ 의 관성차수가 1일 때) 1이고  $p$ 가 비활성일 때 2입니다. 이로써 주장의 증명이 완료됩니다.

### §62.6.iv 마무리하기

보조정리 62.4.1에 의해  $\text{Frob}_{\mathfrak{p}} = \sigma_p \in H$ 인 것은  $p$ 가 이차 잉여인 것과 동치임을 이미 알고 있습니다. 한편,

**연습문제 62.6.7.**  $p \neq 2$ 라는 사실이 여기서 필요합니다.)  $p$ 가  $\mathcal{O}_K = \mathbb{Z}[\frac{1}{2}(1 + \sqrt{q^*})]$ 에서 분해되는 것은  $\left(\frac{q^*}{p}\right) = 1$ 인 것과 동치임을 보이십시오. (인수분해 알고리즘을 사용하십시오.)

다시 말해,

$$\begin{aligned} \left(\frac{p}{q}\right) = 1 &\iff \sigma_p \in H \\ &\iff \text{Frob}_{\mathfrak{p}} \in H \\ &\iff \text{Frob}_{\mathfrak{p}} = \text{id}_K \\ &\iff \text{ord } \text{Frob}_{\mathfrak{p}} = 1 \\ &\iff f_{\mathfrak{p}} = 1 \\ &\iff p \text{는 } \mathbb{Z} \left[ \frac{1}{2}(1 + \sqrt{q^*}) \right] \text{에서 분해됩니다} \\ &\iff \left(\frac{q^*}{p}\right) = 1. \end{aligned}$$

이로써 증명이 완료됩니다.

### §62.7 프로베니우스 원소는 인수분해를 통제합니다

**이 절의 대표적인 예:** 이차 상호법칙의 증명에서  $\text{Frob}_p$ 는  $p$ 의 분해를 통제하였습니다. 일반적인 경우에도 마찬가지입니다.

이차 상호법칙의 증명에서, 우리는  $p$ 의 분해와  $\text{Frob}_p$ 의 성질을 관련짓기 위해 프로베니우스 원소가 제한과 잘 어울린다는 사실을 사용하였습니다.

사실,  $E/\mathbb{Q}$ 가 갈루아 확대가 아닌 경우에도 성립하는, 임의의 중간체  $\mathbb{Q} \subseteq E \subseteq K$ 에 대한 훨씬 더 강한 명제가 있습니다. 이는 인수분해 패턴이라는 개념에 의존합니다. 그 내용은 다음과 같습니다.

$n = [E : \mathbb{Q}]$ 로 놓고,  $p$ 를  $K$ 에서 비분기인 유리 소수라고 합시다. 그러면  $p$ 는  $E$ 에서 다음과 같이 분해될 수 있습니다

$$p \cdot \mathcal{O}_E = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_g$$

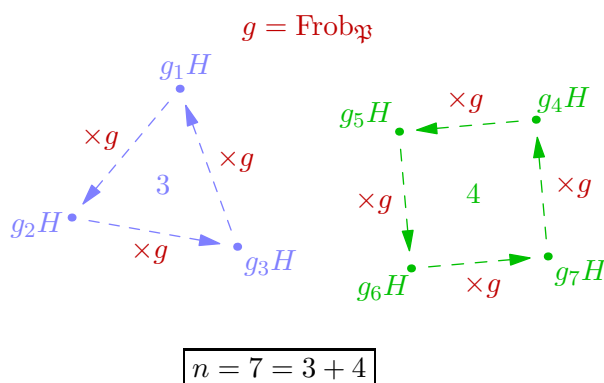
관성차수  $f_1, \dots, f_g$ 와 함께입니다: ( $E/\mathbb{Q}$ 가 갈루아가 아니므로 이 관성차수들은 서로 다를 수 있습니다). 수  $f_1 + \dots + f_g = n$ 은 수  $n$ 의 분할을 이룹니다. 예를 들어, 이차 상호법칙

증명에서는  $n = 2$ 였고, 가능한 분할은 (만약  $p$ 가 분해되었다면)  $1 + 1$ 과 (만약  $p$ 가 비활성이었다면)  $2$ 였습니다. 우리는 이를  $E$ 에서  $p$ 의 **인수분해 패턴**이라고 부릅니다.

다음으로,  $K$  안에서 ( $p$ ) 위에 있는 프로베니우스  $\text{Frob}_{\mathfrak{p}}$ 를 도입합니다; 이는  $G = \text{Gal}(K/\mathbb{Q})$ 의 한 원소입니다. 그리고  $H$ 를 체  $E$ 에 대응하는 군이라고 합시다. 도식:

$$\begin{array}{ccc}
 K & \longleftrightarrow & \{1\} \\
 | & & | \\
 E & \longleftrightarrow & H \\
 n \downarrow & & \downarrow n \\
 \mathbb{Q} & \longleftrightarrow & G
 \end{array}
 \quad
 \begin{array}{ccc}
 & \text{Frob}_{\mathfrak{p}} & \\
 & \mathfrak{p}_1 \dots \mathfrak{p}_g & f_1 + \dots + f_g = n \\
 & \downarrow & \\
 & (p) &
 \end{array}$$

그러면  $\text{Frob}_{\mathfrak{p}}$ 는 좌곱셈에 의해  $n$ 개의 좌잉여류  $gH$ 에 대한 순열을 유도합니다(어쨌든,  $\text{Frob}_{\mathfrak{p}}$  역시  $G$ 의 원소이니깐요!). 다른 모든 순열과 마찬가지로, 우리는 그 결과로 나오는 순환 분해를 살펴볼 수 있는데, 이는 자연스러운 "순환 구조"를 가집니다: 즉  $n$ 의 분할입니다.



정리는 이 둘이 일치한다는 것입니다:

**정리 62.7.1 (프로베니우스 원소가 분해를 결정한다)**

$\mathbb{Q} \subseteq E \subseteq K$ 를 수체의 확대라고 하고  $K/\mathbb{Q}$ 가 갈루아라고 가정합시다(단,  $E/\mathbb{Q}$ 는 그럴 필요가 없습니다). 비분기 유리 소수  $p$ 를 고르고;  $G = \text{Gal}(K/\mathbb{Q})$ ,  $H$ 를 대응하는 중간 부분군이라고 합시다. 마지막으로,  $\mathfrak{p}$ 를  $K$ 에서  $p$  위에 있는 소 아이디얼이라고 합시다.

그러면  $E$ 에서  $p$ 의 인수분해 패턴은  $H$ 의 좌잉여류에 작용하는  $\text{Frob}_{\mathfrak{p}}$ 의 순환 구조로 주어집니다.

흔히, 우리는  $E = K$ 로 취하는데, 이 경우 이는 단지 소수  $p$ 의 분해가 그 위의 프로베니우스 원소에 의해 결정된다는 것을 주장하는 것입니다.

**증명 개요.**  $\alpha$ 를 대수적 정수라 하고  $f$ 를 그 최소다항식(차수  $n$ )이라고 합시다.  $E = \mathbb{Q}(\alpha)$ 로 놓읍시다(이는  $\mathbb{Q}$  위에서 차수  $n$ 을 가집니다). 운 좋게도  $\mathcal{O}_E = \mathbb{Z}[\alpha]$ 라고, 즉  $E$ 가 단생성이라고 가정합시다. 그러면 인수분해 알고리즘에 의해,  $E$ 에서 임의의  $p$ 를 인수분해하려면  $p$ 를 법으로  $f$ 를 인수분해하기만 하면 됨을 알고 있습니다. 왜냐하면  $f = f_1^{e_1} \dots f_g^{e_g} \pmod{p}$ 이면 다음을 얻기 때문입니다

$$(p) = \prod_i \mathfrak{p}_i = \prod_i (f_i(\alpha), p)^{e_i}.$$

이는 분기지수와 관성차수에 대한 완전한 정보를 우리에게 제공합니다;  $e_i$ 는 분기지수이고,  $\deg f_i$ 는 관성차수입니다(왜냐하면  $\mathcal{O}_E/\mathfrak{p}_i \cong \mathbb{F}_p[X]/(f_i(X))$ 이기 때문입니다).

특히  $p$ 가 비분기(unramified)라면 모든  $e_i$ 는 1과 같으며, 다음을 얻습니다

$$n = \deg f = \deg f_1 + \deg f_2 + \cdots + \deg f_g.$$

다시 한 번  $n$ 의 분할을 얻으며, 이를  $f$ 의 법  $p$ 에 대한 **인수분해 패턴**이라고 부릅니다. 따라서  $\mathcal{O}_E$ 에서 비분기 소수  $p$ 의 인수분해 패턴을 보려면,  $f \pmod{p}$ 의 인수분해 패턴만 알면 됩니다.

정리를 증명하기 위해,  $f \pmod{p}$ 의 인수분해 패턴이  $f$ 의 근에 대한  $\text{Frob}_{\mathfrak{p}}$  작용의 순환 분해와 정확히 대응하며,  $f$ 의 근이  $G$ 에서  $H$ 의 잉여류와 정확히 대응함을 보이겠습니다.

이를 위해  $S = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ 을  $f$ 의 근이라 합시다 ( $f$ 가  $\mathbb{Q}$  위에서 기약이므로 서로 다른 근입니다).  $\text{Frob}_{\mathfrak{p}}$ 가  $S$ 에 작용하도록 합시다. 이는  $S$ 를 궤도  $S_1, S_2, \dots, S_k$ 로 분할합니다.  $S_i$ 의 원소를 정확히 근으로 갖는, 계수가  $E$ 에 속하는 다항식  $f_i$ 를 구성합니다. 이는  $E$  위에서  $f$ 의 인수분해를 이루며, 다음과 같이 씁니다

$$f = f_1 f_2 \cdots f_k.$$

우리는 이것이 실제로  $f \pmod{p}$ 의 인수분해를 유도한다고 주장합니다. 이를 확인하기 위해, 몫  $\mathcal{O}_K \rightarrow \mathcal{O}_K/\mathfrak{p}$  아래에서 이 다항식들  $f_i$ 의 상을 생각하고, 이를  $\bar{f}_i$ 로 표기합니다. 그러면  $p$ 가 비분지이므로, 분해군  $D(\mathfrak{p}|p)$ 가 갈루아 군  $\mathcal{G} = \text{Gal}((\mathcal{O}_E/\mathfrak{p})/(\mathbb{Z}/p\mathbb{Z}))$ 와 동형임을 압니다. 따라서  $\text{Frob}_{\mathfrak{p}}$ 는  $\mathcal{G}$ 의 생성원  $\sigma$ 에 대응됩니다.  $f$ 의 근에 대한  $\text{Frob}_{\mathfrak{p}}$ 의 작용이  $\bar{f}$ 의 근에 대한  $\sigma$ 의 작용과 같다는 것은 믿기 어렵지 않습니다.  $f_i$ 의 근들이  $\text{Frob}_{\mathfrak{p}}$ 의 작용 아래 하나의 궤도를 이루므로,  $\bar{f}_i$ 의 근들이  $\sigma$ 의 작용, 따라서  $\mathcal{G}$ 의 작용 아래 하나의 궤도를 이룸을 알 수 있습니다. 이제  $\bar{f}_i$ 가  $\mathbb{F}_p$  위에서 기약다항식이라는 것은 갈루아 이론의 표준적인 사실입니다( $\mathcal{G}$ 에 의해 고정되므로), 따라서 주장이 증명됩니다.

이제  $f$ 의 근이  $H$ 의 잉여류와 대응함을 관찰하기만 하면 되며, 이는 나중에 확립하겠습니다.  $\square$

위에서  $f \pmod{p}$ 의 인수분해 패턴이 주어지면,  $\mathcal{O}_E$ 에서 비분기 소수  $p$ 의 인수분해 패턴을 결정할 수 있음을 보았습니다.

이를 뒤집어 보면,  $f \pmod{p}$ 의 인수분해 패턴을 알고 싶다면,  $p$ 가 어떻게 분해되는지만 알면 됩니다. 그리고 이는  $E$ 가 모노제닉(monogenic)이라는 가정 없이도 일치함이 밝혀집니다.

### 정리 62.7.2 (프로베니우스가 다항식 인수분해를 지배한다)

$\alpha$ 를 최소 다항식  $f$ 를 갖는 대수적 정수라 하고,  $E = \mathbb{Q}(\alpha)$ 라 합시다. 그러면  $f$ 의 분해체  $K$ 에서 비분기인 임의의 소수  $p$ 에 대해, 다음이 서로 일치합니다:

- (i)  $E$ 에서  $p$ 의 인수분해 패턴.
- (ii)  $f \pmod{p}$ 의 인수분해 패턴.
- (iii)  $f$ 의 근에 대한  $\text{Frob}_{\mathfrak{p}} \in \text{Gal}(K/\mathbb{Q})$  작용과 관련된 순환 구조, 여기서  $\mathfrak{p}$ 는  $K$ 에서  $p$  위에 있습니다.

### 예제 62.7.3 ( $x^3 - 2 \pmod{5}$ 인수분해하기)

$\alpha = \sqrt[3]{2}$ 이고  $f = x^3 - 2$ 라 하면,  $E = \mathbb{Q}(\sqrt[3]{2})$ 입니다.  $p = 5$ 로 두고, 마지막으로  $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ 를 분해체라 합시다. 설정:

$$\begin{array}{ccc}
 K = \mathbb{Q}(\sqrt[3]{2}, \omega) & \mathfrak{P} & x^3 - 2 = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\omega)(x - \sqrt[3]{2}\omega^2) \\
 \downarrow 2 & \downarrow & \\
 E = \mathbb{Q}(\sqrt[3]{2}) & \mathfrak{p} & x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4}) \\
 \downarrow 3 & \downarrow & \\
 \mathbb{Q} & (5) & x^3 - 2 \text{ irreducible over } \mathbb{Q}
 \end{array}$$

이제 주장된 세 대상은 모두  $2+1$  모양을 가집니다:

- (i) 인수분해 알고리즘에 의해,  $(5) = (5, \sqrt[3]{2} - 3)(5, 9 + 3\sqrt[3]{2} + \sqrt[3]{4})$ 를 얻습니다.
- (ii)  $x^3 - 2 \equiv (x - 3)(x^2 + 3x + 9) \pmod{5}$ 입니다.
- (iii) 앞서  $\text{Frob}_{\mathfrak{P}} = (\bullet)(\bullet \bullet)$ 임을 보았습니다.

증명 개요.  $n = \deg f$ 라 둡시다.  $H$ 를  $E$ 에 대응하는  $G = \text{Gal}(K/\mathbb{Q})$ 의 부분군이라 하면,  $|G/H| = n$ 입니다. 그림으로 나타내면 다음과 같습니다

$$\begin{array}{ccc}
 K & \{1\} & \mathfrak{P} \\
 \downarrow & \downarrow & \downarrow \\
 E = \mathbb{Q}(\alpha) & H & \mathfrak{p} \\
 \downarrow & \downarrow & \downarrow \\
 \mathbb{Q} & G & (p)
 \end{array}$$

(i), (ii), (iii)이 모두 다음과 동치임을 주장합니다

(iv)  $G/H$ 에 대한  $\text{Frob}_{\mathfrak{P}}$  작용의 패턴.

다시 말해, 잉여류들이  $K$ 에서  $f$ 의  $n$ 개 근과 대응한다고 주장합니다. 실제로  $H$ 는  $\tau(\alpha) = \alpha$ 를 만족하는  $\tau \in G$ 의 집합일 뿐이므로,  $\tau H \mapsto \tau(\alpha)$ 에 의해 근과 잉여류  $G/H$  사이에 전단사가 존재합니다. 이렇게 생각해 봅시다: 만약  $G = S_n$ 이고  $H = \{\tau : \tau(1) = 1\}$ 이라면,  $G/H$ 는 위수  $n!/(n-1)! = n$ 을 가지며 원소  $\{1, \dots, n\}$ 과 대응합니다. 따라서 (iii)에서 (iv)로 가는 자연스러운 전단사가 존재합니다.

(i)가 (iv)와 전단사 관계에 있다는 사실은 이전 정리인 **정리 62.7.1**였습니다. 대응 (i)  $\iff$  (ii)는 갈루아 이론의 사실이므로, 여기서는 증명을 생략합니다.  $\square$

이 모든 것은  $\mathbb{Q}$ 를  $F$ 로 바꾸어 일반적으로도 할 수 있습니다. 예를 들어 [Le02]에서 그러합니다.

## §62.8 응용 예시: IMO 2003 문제 6

이제 우리가 가진 힘을 보여주는 예시로서, 다음을 증명해 봅시다:



**문제 6.**  $p$ 를 소수라고 합시다. 모든 정수  $n$ 에 대해  $n^p - p$ 가  $q$ 로 나누어떨어지지 않는 소수  $q$ 가 존재함을 증명하십시오.

훨씬 더 강하게,  $X^p - p$ 가 법  $q$ 에 대해 기약다항식이 되는 무한히 많은 소수  $q$ 가 존재함을 보이겠습니다.

풀이. 좋습니다! 먼저, 체의 답을 그림니다

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[p]{p}) \subseteq K$$

여기서  $K$ 는  $f(x) = x^p - p$ 의 분해체입니다. 간결함을 위해  $E = \mathbb{Q}(\sqrt[p]{p})$ 라 하고, 이것이  $[E : \mathbb{Q}] = p$ 의 차수를 가짐에 주목하십시오.  $G = \text{Gal}(K/\mathbb{Q})$ 라 합시다.

**질문 62.8.1.**  $p$ 가  $G$ 의 위수를 나눴을 보이십시오. ( $E$ 를 살펴보십시오.)

따라서 코시의 정리(**문제 17A\***, 이는 순수하게 군론적인 사실입니다)에 의해 위수가  $p$ 인  $\sigma \in G$ 를 찾을 수 있습니다. 체보타레프에 의해,  $q$  위에 있는 소 아이디얼  $\Omega \subseteq \mathcal{O}_K$  중  $\text{Frob}_\Omega = \sigma$ 가 되도록 하는, 무한히 많은 (비분기) 유리 소수  $q \neq p$ 가 존재합니다. (네, 이것은 대문자 고딕체  $Q$ 입니다. 죄송합니다.)

이 모든  $q$ 가 원하는 대로 작동함을 주장합니다.

**정리 62.7.2**에 의해,  $f \pmod{q}$ 의 인수분해는  $f$ 의 근들에 대한  $\sigma = \text{Frob}_\Omega$ 의 작용에 의해 제어됩니다. 그런데  $\sigma$ 는  $G$ 에서 소수 위수  $p$ 를 갖습니다! 따라서 순환마디 구조의 모든 길이는  $p$ 를 나누어야 합니다. 그러므로  $f$ 의 가능한 인수분해 패턴은 다음과 같습니다

$$p = \underbrace{1 + 1 + \cdots + 1}_{p\text{번}} \quad \text{또는} \quad p = p.$$

이제 우리는  $p = 1 + \cdots + 1$ 인 경우만 배제하면 됩니다: 이는  $f$ 가 법  $q$ 에서 일차 인수들로 분해될 때만 일어납니다. 직관적으로 이 극단적인 경우는 매우 일어날 법하지 않아 보입니다(우리가  $f$ 가 기약이기를 바랄 때 정말로 운이 나빠서 일차 인수들로 분해되겠습니까?). 그리고 실제로 이는 쉽게 알 수 있습니다: 이는  $\sigma$ 가  $K$  안의  $f$ 의 모든 근을 고정시킨다는 것을 의미하지만, 그렇다면  $\sigma$ 는  $K$  전체를 고정시키게 되므로  $G$ 의 항등원이 되어, 모순입니다.  $\square$

**비고 62.8.2** — 실제로  $K = \mathbb{Q}(\sqrt[p]{p}, \zeta_p)$ 이고,  $|G| = p(p-1)$ 입니다. 조금 더 군론을 사용하면, 실제로 작동하는 소수  $q$ 의 밀도가  $\frac{1}{p}$ 임을 보일 수 있습니다.

## §62.9 생각해 볼 만한 조금 더 어려운 문제

**문제 62A.** 홀수 소수  $p$ 에 대해 다음이 성립함을 보이십시오.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}.$$

**문제 62B.**  $f$ 를 정수 계수를 갖는 비상수 다항식이라 합시다. 충분히 큰 모든 소수  $p$ 에 대해  $f \pmod{p}$ 가 일차 인수들로 완전히 분해된다고 가정합시다.  $f$ 가 일차 인수들로 완전히 분해됨을 보이십시오.

**문제 62C<sup>†</sup>** (등차수열에 관한 디리클레 정리).  $a$ 와  $m$ 을 서로소인 양의 정수라 합시다.  $p \equiv a \pmod{m}$ 인 소수  $p$ 의 밀도가 정확히  $\frac{1}{\phi(m)}$ 임을 보이십시오.

**문제 62D.**  $n$ 을 소수의 거듭제곱이 아닌 홀수라 합시다.  $n$ 번째 원분다항식이 어떤 유리 소수를 법으로 하더라도 기약이 아님을 보이십시오.



**문제 62E** (Putnam 2012 B6).  $p$ 를  $p \equiv 2 \pmod{3}$ 을 만족하는 홀수 소수라 합시다.  $\pi(x) = x^3 \pmod{p}$ 로 정의되는  $\mathbb{F}_p$ 의 순열을  $\pi$ 라 합시다.  $\pi$ 가 짝순열인 것은  $p \equiv 3 \pmod{4}$ 인 것과 동치임을 보이십시오.



# 63 보너스: 아르틴 상호법칙에 대하여

이 장에서는 대역류체론(global class field theory)의 몇 가지 중요한 정리들을 서술하고, 이를 이용하여 크로네커-베버 정리와 힐베르트 류체(Hilbert class field)를 유도하겠습니다. 증명은 없지만, 그럼에도 충분히 흥미할 수 있기를 바랍니다. 전문가를 위해 덧붙이자면: 이것은 이델(idèle)을 사용하지 않는 대역류체론입니다.

요약하자면 다음과 같습니다:  $K$ 를 수체(number field)라 합시다. 그러면 모든 아벨 확장  $L/K$ 는 오직  $K$ 에 내재된 정보만을 이용하여 이해될 수 있는데, 바로 (아이디얼 류군을 일반화한) 사선 류군(ray class group)입니다.

## §63.1 개요

이 절의 끝에서 아벨 체 확장  $L/K$ 에 대해 아르틴 기호(Artin symbol)를 정의하겠습니다

$$\left( \frac{L/K}{\mathfrak{p}} \right),$$

이는 르장드르 기호(Legendre symbol)  $\left( \frac{a}{p} \right)$ 를 일반화한 것입니다:

- 사선 위에는 정수  $a$  대신 체 확장  $L/K$ 가 있습니다.
- 사선 아래에는 유리 소수  $p$  대신  $K$ 의 소 아이디얼  $\mathfrak{p}$ 가 있습니다.

이 기호가 정의되려면  $\mathfrak{p}$ 가 확장  $L/K$ 에서 분기(ramify)하지 않아야 합니다.

그리고 마지막으로, 다음과 같은 형태의 아르틴 상호법칙(Artin reciprocity theorem)을 서술하고자 합니다:

소 아이디얼  $\mathfrak{p}$ 에 대해,  $\left( \frac{L/K}{\mathfrak{p}} \right)$ 는 오직 “ $\mathfrak{p} \pmod{f}$ ”에만 의존합니다.

여기서  $f$ 는 오직 체 확장  $L/K$ 에만 의존하는 “법(modulus)”입니다.

이를 위해서는 먼저 두 아이디얼이 무언가를 법으로 서로소라는 것이 무엇을 의미하는지 정의해야 합니다.  $f$ 와 “서로소”인  $\mathcal{O}_K$ 의 아이디얼들을 “ $f$ 를 법으로 하는 잉여류”(앞으로는 이를 “사선류(ray class)”라 부르겠습니다)로 다음과 같은 방식으로 나눌 것입니다:

- 이는 류군(class group)을 일반화합니다 – 서로 다른 아이디얼 류에 속하는(즉  $\mathcal{O}_K$ -가 균으로서 동형이 아닌) 두 아이디얼은 서로 다른 사선류에 속합니다.
- 이는 곱셈 구조를 보존합니다 – 만약  $\mathfrak{p}$ 가  $\mathfrak{p}'$ 와 같은 사선류에 속하고,  $\mathfrak{q}$ 가  $\mathfrak{q}'$ 와 같은 사선류에 속한다면,  $\mathfrak{p}\mathfrak{q}$ 는  $\mathfrak{p}'\mathfrak{q}'$ 와 같은 사선류에 속합니다.

아이디얼에 대해서는 원소 덧셈에 대응하는 것이 없다는 점에 유의하십시오(예를 들어,  $(1) = (-1)$ 이지만  $(1) + (1) \neq (1) + (-1)$ 입니다). 따라서 이것이 우리가 기대할 수 있는 최선입니다.

다시 말해, 사선류들은 아이디얼 곱셈으로부터 유도된 연산을 갖는 곱셈에 대한 아벨 군을 이룹니다.

- 고정된 법  $f$ 에 대해, 사선류는 오직 유한 개만 존재합니다.

위 절에서는 소 아이디얼  $\mathfrak{p} \in \mathcal{O}_K$ 를, 모든 아이디얼이 그 곱으로 쓰일 수 있는 기약 인수로 생각할 수 있습니다. 그러나 이들은 또한 자연스럽게 법으로도 사용될 수 있습니다:

소 아이디얼  $\mathfrak{p}$ 는  $\mathcal{O}_K$ 의 원소들을, 원소의 덧셈과 곱셈을 보존하는 방식으로 잉여류로 나누는 방법을 제공합니다.

이는  $\mathcal{O}_K$ 의 아이디얼을 사선류로 나누도록 더 일반화될 수 있습니다 – 안타깝게도, [예제 63.3.3](#)에서 나중에 보게 되듯이, 유한 소수만을 사용해서는 우리가 원하는 방식으로 아이디얼을 나누기에 충분하지 않습니다. 따라서 무한 소수를, 아이디얼뿐만 아니라 원소까지도 곱셈 구조를 만족하는 류로 나누기 위해 도입하겠습니다.

## §63.2 무한 소수

**이 절의 대표적인 예:**  $\mathbb{Q}(\sqrt{-5})$ 는 복소 무한 소수를 하나 가지고,  $\mathbb{Q}(\sqrt{5})$ 는 실 무한 소수를 두 개 가집니다.

$K$ 를 차수가  $n$ 이고 서명이  $(r, s)$ 인 수체라고 합시다.  $\mathcal{O}_K$ 의 소 아이디얼이 무엇인지는 이미 알고 있지만, 이제는 소위 무한 소수라는 것도 허용하려고 하며, 이를 매장을 이용해 설명하겠습니다.<sup>1</sup>  $n$ 개의 매장  $\sigma: K \rightarrow \mathbb{C}$ 가 있음을 상기하면, 이는 다음으로 구성됩니다

- $\text{im } \sigma \subseteq \mathbb{R}$ 인 실 매장  $r$ 개, 그리고
- $s$  쌍의 켤레 복소 매장.

따라서  $r + 2s = n$ 입니다. 첫 번째 부류의 매장은 **실 무한 소수**를 이루고, **복소 무한 소수**는 두 번째 유형입니다.  $K$ 의 모든 무한 소수가 실수(각각 복소수)이면  $K$ 를 **완전 실**(각각 **완전 복소**)이라고 합니다.

### 예제 63.2.1 (무한 소수의 예시)

- $\mathbb{Q}$ 는 하나의 실 무한 소수를 가집니다. 이를 흔히  $\infty$ 로 표기합니다.
- $\mathbb{Q}(\sqrt{-5})$ 는 하나의 복소 무한 소수를 가지며, 실 무한 소수는 없습니다. 따라서 완전 복소입니다.
- $\mathbb{Q}(\sqrt{5})$ 는 두 개의 실 무한 소수를 가지며, 복소 무한 소수는 없습니다. 따라서 완전 실입니다.

## §63.3 무한 소수를 이용한 모듈러 산술

$K$ 의 **모듈러스**(또는 **모듈**)는 다음과 같은 형식적 곱입니다

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu(\mathfrak{p})}$$

여기서 곱은 유한 소수와 무한 소수를 모두 포함한 모든 소수에 대해 취해집니다. (여기서  $\nu(\mathfrak{p})$ 는 음이 아닌 정수이며, 그중 유한 개만이 0이 아닙니다.) 또한 다음을 요구합니다

- 임의의 복소 무한 소수  $\mathfrak{p}$ 에 대해  $\nu(\mathfrak{p}) = 0$ 이고,

<sup>1</sup>이것이 정말로 올바른 정의는 아닙니다. 유한이든 무한이든 소수를 생각하는 “올바른” 방법은 부치를 이용하는 것입니다. 하지만 제가 말하고자 하는 정리들을 서술하는 데는 이것으로 충분합니다.

- 임의의 실 무한 소수  $p$ 에 대해  $\nu(p) \leq 1$ 입니다.

당연히, 모든  $m$ 은 유한 소수와 (실) 무한 소수를 분리하여  $m = m_0 m_\infty$ 로 쓸 수 있습니다. 다음의 경우  $a \equiv b \pmod{p}$ 라고 합니다

- $p$ 가 유한 소수이면,  $a \equiv b \pmod{p^{\nu(p)}}$ 는 여러분이 예상하는 바로 그 의미입니다:  $a - b \in p^{\nu(p)}$ .
- $p$ 가 실 무한 소수  $\sigma: K \rightarrow \mathbb{R}$ 이면,  $a \equiv b \pmod{p}$ 는  $\sigma(a/b) > 0$ 임을 의미합니다.

**실 무한 소수  $p = \sigma$ 는  $K^\times$ 의 원소들을 두 부류  $\{k \in K^\times \mid \sigma(k) > 0\}$ 와  $\{k \in K^\times \mid \sigma(k) < 0\}$ 로 나누며, 이 구분은 곱셈 연산을 만족합니다.**

물론,  $a \equiv b \pmod{m}$ 는  $m$ 에 포함된 각 소수 거듭제곱에 대해  $a \equiv b$ 임을 의미합니다. 이를 바탕으로 류군의 일반화를 정의할 수 있습니다:

**정의 63.3.1.**  $m$ 을 수체  $K$ 의 모듈러스라고 합시다.

- $I_K(m)$ 을  $m$ 과 서로소인  $K$ 의 모든 분수 아이디얼의 집합이라고 하며, 이는 아벨 군입니다.
- $P_K(m)$ 을 다음에 의해 생성되는  $I_K(m)$ 의 부분군이라고 합시다

$$\{\alpha \mathcal{O}_K \mid \alpha \in K^\times \text{ 그리고 } \alpha \equiv 1 \pmod{m}\}.$$

이는 때때로 주 아이디얼의 “레이(ray)”라고 불립니다.<sup>2</sup>

마지막으로  $m$ 의 **레이 류군**을  $C_K(m) = I_K(m)/P_K(m)$ 으로 정의합니다.

이 군은 항상 유한하다고 알려져 있습니다. 통상적인 류군은  $C_K(1)$ 임에 유의하십시오. 아르틴 상호법칙 직후에 사용할 마지막 정의는 다음과 같습니다:

**정의 63.3.2.**  $m$ 의 **합동 부분군**(congruence subgroup)은 다음을 만족하는 부분군  $H$ 입니다.

$$P_K(m) \subseteq H \subseteq I_K(m).$$

따라서  $C_K(m)$ 는 다양한 몫  $I_K(m)/H$ 의 격자를 포함하는 군이며, 여기서  $H$ 는 합동 부분군입니다.

이 정의는 익숙해지는 데 시간이 걸리므로, 여기 몇 가지 예시를 제시합니다.

### 예제 63.3.3 ( $\mathbb{Q}$ 에서의 사상류군, 유한 모듈러스)

무한 소수  $\infty$ 를 갖는  $K = \mathbb{Q}$ 를 생각해봅시다. 그러면

- $m = 1$ 로 두면  $I_{\mathbb{Q}}(1)$ 은 모든 분수 아이디얼이고,  $P_{\mathbb{Q}}(1)$ 은 모든 주 분수 아이디얼입니다. 이들의 몫은  $\mathbb{Q}$ 의 통상적인 유수군이며, 이는 자명합니다.
- 이제  $m = 8$ 로 둡니다. 그러면  $I_{\mathbb{Q}}(8) \cong \{\frac{a}{b}\mathbb{Z} \mid a/b \equiv 1, 3, 5, 7 \pmod{8}\}$ 입니다. 더 나아가

$$P_{\mathbb{Q}}(8) \cong \left\{ \frac{a}{b}\mathbb{Z} \mid a/b \equiv 1 \pmod{8} \right\}.$$

얼핏 보면 몫이  $(\mathbb{Z}/8\mathbb{Z})^\times$ 일 것이라 생각할 수 있습니다. 하지만 문제는 우리가

<sup>2</sup>아마도 기하학적 반직선과 마찬가지로, 한 방향으로만 무한히 뻗어나가기 때문일 것입니다 – 적어도 모듈러스  $m$ 에 무한 소수가 있는 경우에는 그렇습니다.

다루고 있는 것이 아이디얼이라는 점입니다: 구체적으로, 우리는 다음을 갖습니다.

$$7\mathbb{Z} = -7\mathbb{Z} \in P_{\mathbb{Q}}(8)$$

왜냐하면  $-7 \equiv 1 \pmod{8}$ 이기 때문입니다. 그래서 실제로는, 우리는 다음을 얻습니다.

$$C_{\mathbb{Q}}(8) \cong \{1, 3, 5, 7\mathbb{Z}\} / \{1, 7\mathbb{Z}\} \cong (\mathbb{Z}/4\mathbb{Z})^{\times}.$$

더 일반적으로,

$$C_{\mathbb{Q}}(m) = (\mathbb{Z}/m\mathbb{Z})^{\times} / \{\pm 1\}.$$

### 예제 63.3.4 ( $\mathbb{Q}$ 에서의 사상류군, 무한 모듈러스)

다시 무한 소수  $\infty$ 를 갖는  $K = \mathbb{Q}$ 를 생각해봅시다.

- 이제  $m = \infty$ 로 둡니다. 앞서와 마찬가지로  $I_{\mathbb{Q}}(\infty) = \mathbb{Q}^{\times}$ 입니다. 이제 정의에 의해 우리는 다음을 갖습니다.

$$P_{\mathbb{Q}}(\infty) = \left\{ \frac{a}{b}\mathbb{Z} \mid a/b > 0 \right\}.$$

얼핏 보면 이것이  $\mathbb{Q}_{>0}$ 일 것이라 생각할 수 있지만, 아이디얼에서의 동일한 현상으로 인해 실제로는  $P_{\mathbb{Q}}(\infty) = \mathbb{Q}^{\times}$ 임이 드러납니다. 따라서 이 경우,  $P_{\mathbb{Q}}(\infty)$ 는 여전히 모든 주 분수 아이디얼을 갖습니다. 그러므로  $C_{\mathbb{Q}}(\infty)$ 는 여전히 자명합니다.

- 마지막으로,  $m = 8\infty$ 로 둡시다. 앞서와 마찬가지로  $I_{\mathbb{Q}}(8\infty) \cong \left\{ \frac{a}{b}\mathbb{Z} \mid a/b \equiv 1, 3, 5, 7 \pmod{8} \right\}$ 입니다. 이제 이 경우:

$$P_{\mathbb{Q}}(8\infty) \cong \left\{ \frac{a}{b}\mathbb{Z} \mid a/b \equiv 1 \pmod{8} \text{ 그리고 } a/b > 0 \right\}.$$

이번에는 정말로  $-7\mathbb{Z} \notin P_{\mathbb{Q}}(8\infty)$ 입니다:  $7 \not\equiv 1 \pmod{8}$ 이고 또한  $-7 < 0$ 이기 때문입니다. 따라서  $7\mathbb{Z}$ 의 생성원 중 어느 것도  $P_{\mathbb{Q}}(8\infty)$ 에 속하지 않습니다. 이렇게 우리는 마침내 다음을 얻습니다.

$$C_{\mathbb{Q}}(8\infty) \cong \{1, 3, 5, 7\mathbb{Z}\} / \{1\mathbb{Z}\} \cong (\mathbb{Z}/8\mathbb{Z})^{\times}$$

여기서 전단사  $C_{\mathbb{Q}}(8\infty) \rightarrow (\mathbb{Z}/8\mathbb{Z})^{\times}$ 는  $a\mathbb{Z} \mapsto |a| \pmod{8}$ 로 주어집니다.

더 일반적으로,

$$C_{\mathbb{Q}}(m\infty) = (\mathbb{Z}/m\mathbb{Z})^{\times}.$$

## §63.4 확장에서의 무한 소수

저는 위의 모든 내용이 특정한 수체  $K$ 에 고유한(intrinsic) 것임을 강조하고 싶습니다. 이 시점 이후로 우리는 확장  $L/K$ 를 고려할 것이지만, 모듈러스와 사상류군이라는 개념이 위의  $L$ 이 아니라 오직  $K$ 로부터만 정의되는 대상이라는 구분을 염두에 두는 것이 중요합니다.

이제 차수  $m$ 의 갈루아(Galois) 확장  $L/K$ 를 생각해봅시다. 우리는 이미  $K$ 의 소 아이디얼  $\mathfrak{p}$ 가  $L$ 의 소 아이디얼  $\mathfrak{P}$ 의 곱으로 좋은 방식으로 분해된다는 것을 알고 있으므로, 무한 소수에 대해서도 같은 것을 하고자 합니다. 이는 간단합니다:  $n$ 개의 무한 소수  $\sigma: K \rightarrow \mathbb{C}$

각각은  $m$ 개의 무한 소수  $\tau: L \rightarrow \mathbb{C}$ 로 들어올려지는데, 이는 다음 도식이

$$\begin{array}{ccc} L & \xrightarrow{\tau} & \mathbb{C} \\ \uparrow & \nearrow \sigma & \\ K & & \end{array}$$

가환임을 의미합니다. 따라서 앞서와 마찬가지로,  $K$ 의 각 무한 소수  $\sigma$ 는 그 위에 놓인  $L$ 의  $m$ 개의 무한 소수  $\tau$ 를 갖습니다.

$K$ 의 실 소수  $\sigma$ 에 대해, 그 위에 놓인 결과  $\tau$  중 어느 것이라도 복소이면, 우리는 소수  $\sigma$ 가 확장  $L/K$ 에서 **분기한다**(ramifies)고 말합니다. 그렇지 않으면  $L/K$ 에서 **비분기**(unramified)라고 합니다.  $K$ 의 무한 소수는  $L/K$ 에서 항상 비분기입니다. 이런 방식으로, 우리는 비분기 갈루아 확장  $L/K$ 에 대해 이야기할 수 있습니다: 이는 모든 소수(유한이든 무한이든)가 비분기인 확장입니다.

#### 예제 63.4.1 ( $\infty$ 의 분기)

$\infty$ 를  $\mathbb{Q}$ 의 실 무한 소수라 합시다.

- $\infty$ 는  $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$ 에서 분기합니다.
- $\infty$ 는  $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ 에서 비분지입니다.

또한  $K$ 가 전복소체이면 임의의 확대  $L/K$ 는 비분지임을 유의하십시오.

### §63.5 프로베니우스 원소와 아르틴 기호

핵심 결과를 상기하십시오:

#### 정리 63.5.1 (프로베니우스 원소)

$L/K$ 를 갈루아 확대라 합시다.  $\mathfrak{p}$ 가  $L/K$ 에서 비분지인 소 아이디얼이고,  $\mathfrak{P}$ 가  $L$ 에서 그 위에 있는 소 아이디얼이면, 다음을 만족하는  $\text{Gal}(L/K)$ 의 유일한 원소가 존재하며, 이를  $\text{Frob}_{\mathfrak{P}}$ 로 표기합니다

$$\text{Frob}_{\mathfrak{P}}(\alpha) \equiv \alpha^{N(\mathfrak{p})} \pmod{\mathfrak{P}} \quad \forall \alpha \in \mathcal{O}_L.$$

예제 62.1.2와 보조정리 62.4.1의 예시들을 상기하십시오.

#### 예제 63.5.2 (프로베니우스 원소의 예)

$L = \mathbb{Q}(i)$ ,  $K = \mathbb{Q}$ 라 합시다.  $\text{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}$ 입니다.

$p$ 가 홀수 소수이고  $\mathfrak{P}$ 가 그 위에 있다면,  $\text{Frob}_{\mathfrak{P}}$ 는 다음을 만족하는 유일한 원소입니다

$$(a + bi)^p \equiv \text{Frob}_{\mathfrak{P}}(a + bi) \pmod{\mathfrak{P}}$$

$\mathbb{Z}[i]$ 에서. 특히,

$$\text{Frob}_{\mathfrak{P}}(i) = i^p = \begin{cases} i & p \equiv 1 \pmod{4} \\ -i & p \equiv 3 \pmod{4}. \end{cases}$$

이로부터  $p \equiv 1 \pmod{4}$ 일 때  $\text{Frob}_{\mathfrak{P}}$ 는 항등원이고,  $p \equiv 3 \pmod{4}$ 일 때  $\text{Frob}_{\mathfrak{P}}$ 는 복소켈레임을 알 수 있습니다.

**예제 63.5.3 (원분 프로베니우스 원소)**

이전 예시를 일반화하여,  $\zeta$ 를  $m$ 차 단위근이라 하고  $L = \mathbb{Q}(\zeta)$ ,  $K = \mathbb{Q}$ 라 합시다.  $L/K$ 가  $\infty$ 와  $m$ 의 소인수를 제외하고는 비분지임은 잘 알려져 있습니다. 더욱이 갈루아 군  $\text{Gal}(L/K)$ 는  $(\mathbb{Z}/m\mathbb{Z})^\times$ 이며, 갈루아 군은 다음 형태의 원소들로 이루어집니다

$$\sigma_n: \zeta \mapsto \zeta^n$$

그리고  $\text{Gal}(L/K) = \{\sigma_n \mid n \in (\mathbb{Z}/m\mathbb{Z})^\times\}$ 입니다.

그러면 이전과 마찬가지로  $p \nmid m$ 인 소수  $p$ 에 대해  $\mathfrak{p}$ 가  $p$  위에 있을 때 다음이 성립합니다

$$\text{Frob}_{\mathfrak{p}} = \sigma_p.$$

여기서 **절 61.6**에서 암시했듯이, 기저체  $K$ 가 반드시  $\mathbb{Q}$ 일 필요는 없는 경우로 이론을 일반화해야 합니다(예를 들어, **예제 63.5.8**에서는  $K = \mathbb{Q}(\omega)$ 가 필요합니다). 이 경우  $p$ 는 반드시 정수일 필요는 없으며, 뒤편에 유도되는 사상은 “ $N(\mathfrak{p})$  거듭제곱” 사상입니다.

**예제 63.5.4 (기저체가  $\mathbb{Q}(\omega)$ 일 때의 프로베니우스 원소)**

$L = \mathbb{Q}(\omega, \sqrt[3]{2})$ ,  $K = \mathbb{Q}(\omega)$ 라 합시다.

$K$ 에서 소 아이디얼인  $\mathfrak{p} = (5)$ 를 생각하면  $N(\mathfrak{p}) = 25$ 입니다. 체  $\mathcal{O}_K/\mathfrak{p}$ 는  $\mathbb{F}_{25}$ 와 동형입니다.  $L$ 에서  $\mathfrak{p}$ 는  $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ 로 분해되며, 각 잉여체  $\mathcal{O}_L/\mathfrak{p}_i$ 는  $\mathbb{F}_{25}$ 와 동형입니다.

프로베니우스 원소  $\text{Frob}_{\mathfrak{p}} \in \text{Gal}(L/K)$ 는 뒤편에서 25제곱 동형사상을 유도하므로, 항등원입니다.

프로베니우스 원소의 중요한 성질은 그 위수가 상위체  $L$ 에서  $\mathfrak{p}$ 의 분해와 가장 이상적인 방식으로 관련되어 있다는 것입니다:

**보조정리 63.5.5 (프로베니우스 원소의 위수)**

확대  $L/K$ 의 프로베니우스 원소  $\text{Frob}_{\mathfrak{p}} \in \text{Gal}(L/K)$ 의 위수는  $\mathfrak{p}$ 의 잉여차수와 같으며, 즉 다음과 같습니다

$$\text{ord } \text{Frob}_{\mathfrak{p}} = f(\mathfrak{p} \mid \mathfrak{p}).$$

특히,  $\text{Frob}_{\mathfrak{p}} = \text{id}$ 인 것과  $\mathfrak{p}$ 가  $L/K$ 에서 완전히 분해되는 것은 동치입니다.

이는 **보조정리 62.1.3**를 자연스럽게 일반화합니다.

증명. 체  $\mathcal{O}_L/\mathfrak{p}$  위에서 사상  $T: x \mapsto x^{N(\mathfrak{p})}$ 의 위수를 이해하고자 합니다. 그런데 후자는 유한체의 갈루아 이론에 의해  $\mathbb{F}_p$ 에서  $X^{N(\mathfrak{p})} - X$ 의 분해체와 동형입니다. 따라서 그 위수는  $\log_{N(\mathfrak{p})}(N(\mathfrak{p})) = f(\mathfrak{p} \mid \mathfrak{p})$ 입니다.  $\square$

갈루아 군은 주어진  $\mathfrak{p}$  위에 있는  $\mathfrak{p}$ 들의 집합에 추이적으로 작용하므로, 다음이 성립합니다

$$\text{Frob}_{\sigma(\mathfrak{p})} = \sigma \circ (\text{Frob}_{\mathfrak{p}}) \circ \sigma^{-1}.$$

따라서  $\text{Frob}_{\mathfrak{p}}$ 는 그 바탕이 되는  $\mathfrak{p}$ 에 의해 켄넬류를 제외하고 결정됩니다.

유체론(class field theory)에서 우리가 관심을 갖는 것은 **아벨 확대**, 즉  $\text{Gal}(L/K)$ 가 아벨 군인 경우입니다. 여기서 이론은 특별히 더 좋아집니다: 켄넬류의 크기가 1이 됩니다.

**정의 63.5.6.**  $L/K$ 가 **아벨** 확대라고 합시다. 그러면  $K$ 에서 주어진 비분지 소 아이디얼  $\mathfrak{p}$ 에 대해, 원소  $\text{Frob}_{\mathfrak{p}}$ 는  $\mathfrak{p}$ 의 선택에 의존하지 않습니다. 우리는 이렇게 얻어지는  $\text{Frob}_{\mathfrak{p}}$ 를

아르틴 기호라고 표기합니다,

$$\left( \frac{L/K}{\mathfrak{p}} \right).$$

아르틴 기호의 정의는 르장드르 기호와 닮아 보이도록 의도적으로 쓰여진 것입니다. 그 이유를 살펴보면:

**예제 63.5.7** (아르틴 기호에 포함되는 르장드르 기호)

$p > 2$ 가 소수일 때  $\left( \frac{2}{p} \right) \equiv 2^{\frac{p-1}{2}}$  을 이해하고자 한다고 합시다. 다음 원소를 생각합시다

$$\left( \frac{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}{p\mathbb{Z}} \right) \in \text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}).$$

이는  $\sqrt{2}$ 를 어디로 보내는지에 의해 유일하게 결정됩니다. 그런데 실제로 다음이 성립합니다

$$\left( \frac{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}{p\mathbb{Z}} \right) (\sqrt{2}) \equiv (\sqrt{2})^p \equiv 2^{\frac{p-1}{2}} \cdot \sqrt{2} \equiv \left( \frac{2}{p} \right) \sqrt{2} \pmod{\mathfrak{p}}$$

여기서  $\left( \frac{2}{p} \right)$ 는 보통의 르장드르 기호이고,  $\mathfrak{p}$ 는  $\mathbb{Q}(\sqrt{2})$ 에서  $p$  위에 있는 소 아이디얼입니다. 따라서 아르틴 기호는 이차 르장드르 기호를 일반화합니다.

**예제 63.5.8** (아르틴 기호에 포함되는 삼차 르장드르 기호)

마찬가지로, 이는 삼차 르장드르 기호도 일반화합니다. 이를 보이기 위해,  $\theta$ 가  $K = \mathbb{Q}(\sqrt[3]{-3}) = \mathbb{Q}(\omega)$ (따라서  $\mathcal{O}_K = \mathbb{Z}[\omega]$ 는 아이젠슈타인 정수입니다)에서 기본(primary) 소수라고 합시다. 그러면 예를 들어

$$\left( \frac{K(\sqrt[3]{2})/K}{\theta\mathcal{O}_K} \right) (\sqrt[3]{2}) \equiv (\sqrt[3]{2})^{N(\theta)} \equiv 2^{\frac{N(\theta)-1}{3}} \cdot \sqrt[3]{2} \equiv \left( \frac{2}{\theta} \right)_3 \sqrt[3]{2} \pmod{\mathfrak{p}}$$

여기서  $\mathfrak{p}$ 는  $K(\sqrt[3]{2})$ 에서  $(\theta)$  위에 있습니다.

## §63.6 아르틴 상호법칙

이제 우리는  $\text{Gal}(L/K)$ 가 아벨 군이라는 사실을 더욱 활용합니다. 간결함을 위해, 앞으로  $\text{Ram}(L/K)$ 가  $L$ 에서 분지되는  $K$ 의 소 아이디얼들(유한이든 무한이든)을 나타낸다고 합시다.

**정의 63.6.1.**  $L/K$ 가 아벨 확대이고  $\mathfrak{m}$ 이  $\text{Ram}(L/K)$ 의 모든 소 아이디얼로 나누어진다고 합시다. 그러면  $L/K$ 가 아벨이므로 우리는 아르틴 기호를 곱셈적으로 확장하여 다음과 같은 사상을 얻을 수 있습니다

$$\left( \frac{L/K}{\bullet} \right) : I_K(\mathfrak{m}) \twoheadrightarrow \text{Gal}(L/K).$$

이를 **아르틴 사상**이라고 부르며, 이는 (예를 들어 체보타레프 밀도 정리에 의해) 전사입니다.  $H(L/K, \mathfrak{m}) \subseteq I_K(\mathfrak{m})$ 가 이 사상의 핵을 나타낸다고 합시다, 그러면

$$\text{Gal}(L/K) \cong I_K(\mathfrak{m})/H(L/K, \mathfrak{m}).$$

이제 우리는 오랫동안 기다려온 아르틴 상호법칙 정리를 제시할 수 있습니다.

### 정리 63.6.2 (아르틴 상호법칙)

$L/K$ 가 아벨 확대라고 합시다. 그러면 정확히  $\text{Ram}(L/K)$ 의 소 아이디얼들로 나누어지는 법(modulus)  $f = f(L/K)$ 가 존재하여,  $\text{Ram}(L/K)$ 의 모든 소 아이디얼로 나누어지는 임의의 법  $m$ 에 대해 다음이 성립합니다

$$P_K(m) \subseteq H(L/K, m) \subseteq I_K(m) \quad \text{일 때, 그리고 오직 그때만} \quad f \mid m.$$

우리는  $f$ 를  $L/K$ 의 **도체(conductor)**라고 부릅니다.

따라서 도체  $f$ 는 판별식과 비슷한 역할을 하며(정확히 분지되는 소 아이디얼들로 나누어짐),  $m$ 이 도체로 나누어질 때  $H(L/K, m)$ 은 합동 부분군(congruence subgroup)이 됩니다.

이것이 "상호법칙"이라고 불리는 이유는 다음과 같습니다. 위 정리를  $m = f$ 에 적용하면  $P_K(f) \subseteq H(L/K, f)$ 임을 알 수 있으며, 따라서 아르틴 사상은 몫사상  $I_K(f) \twoheadrightarrow I_K(f)/P_K(f)$ 를 통해 인수분해됩니다.  $C_K(f) = I_K(f)/P_K(f)$ 임을 상기하면, 우리는 다음과 같은 사상의 열을 얻습니다

$$\begin{array}{ccccc} I_K(f) & \longrightarrow & C_K(f) & \xrightarrow{\left(\frac{L/K}{\bullet}\right)} & \text{Gal}(L/K) \\ & & \searrow & & \nearrow \cong \\ & & I_K(f)/H(L/K, f) & & \end{array}$$

그 결과:

**소 아이디얼  $\mathfrak{p} \in I_K(f)$ 에 대해,  $\left(\frac{L/K}{\mathfrak{p}}\right)$ 는 오직 " $\mathfrak{p} \pmod{f}$ "에만 의존합니다.**

이 결과가 이차 상호법칙과 어떻게 관련되는지 살펴봅시다.

### 예제 63.6.3 (아르틴 상호법칙이 이차 상호법칙을 함의함)

이차 상호법칙의 큰 기적은 다음과 같이 말합니다: 고정된 (제곱인수가 없는)  $a$ 에 대해, 르장드르 기호  $\left(\frac{a}{p}\right)$ 는 오직  $p$ 가 어떤 것을 법으로 한 잉여류에만 의존해야 합니다. 아르틴 상호법칙이 어떻게 이를 선형적으로(*a priori*) 알려주는지 살펴봅시다.  $L = \mathbb{Q}(\sqrt{a})$ ,  $K = \mathbb{Q}$ 라고 합시다. 그러면 아르틴 기호가

$$\left(\frac{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}{\bullet}\right)$$

르장드르 기호의 올바른 일반화임을 이미 살펴보았습니다. 따라서 아르틴 상호법칙은  $\left(\frac{\mathbb{Q}(\sqrt{a})/\mathbb{Q}}{p}\right)$ 가  $f$ 를 법으로 하는  $p$ 의 잉여류에만 의존하도록 하는 도체  $f = f(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$ 가 존재함을 알려주는데, 이것이 바로 우리가 원했던 것입니다.

같은 맥락의 예시가 여기 있습니다.

### 예제 63.6.4 (원분체)

$\zeta$ 를  $m$ 차 원시근이라고 합시다. 소수  $p$ 에 대해,  $\text{Frob}_p \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ 가 "정확히"  $p \pmod{m}$ 임을 알고 있습니다. 이 아이디어를 아르틴 상호법칙의 표기법으로 옮겨봅시다.

우리는 다음을 증명할 것입니다

$$H(\mathbb{Q}(\zeta)/\mathbb{Q}, m\infty) = P_{\mathbb{Q}}(m\infty) = \left\{ \frac{a}{b} \mathbb{Z} \mid a/b \equiv 1 \pmod{m} \right\}.$$

이것은 아르틴 상호법칙에서 하한을 달성하는 일반적인 예시입니다. 이는 또한  $f(\mathbb{Q}(\zeta)/\mathbb{Q}) \mid m\infty$ 임을 함의합니다.

$\mathbb{Q}(\zeta)/\mathbb{Q}$ 가  $m$ 을 나누는 유한 소수를 제외하고는 비분기임은 잘 알려져 있으므로, 아르틴 기호는  $I_K(\mathfrak{m})$  위에서 정의됩니다. 이제 아르틴 사상은 다음과 같이 주어집니다

$$\begin{array}{ccccc} I_{\mathbb{Q}}(\mathfrak{m}) & \xrightarrow{\left(\frac{\mathbb{Q}(\zeta)/\mathbb{Q}}{\bullet}\right)} & \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) & \xrightarrow{\cong} & (\mathbb{Z}/m\mathbb{Z})^{\times} \\ p & \longmapsto & (x \mapsto x^p) & \longmapsto & p \pmod{m}. \end{array}$$

따라서 이 사상의 핵이 자명하다는 것을, 즉 이는 갈루아 군의 항등원으로 주어지며  $1 \pmod{m}$ 에 대응함을 알 수 있습니다. 한편, 우리는  $P_{\mathbb{Q}}(m\infty)$ 도 이미 계산했으므로, 원하는 등식을 얻습니다.

사실, 우리는 다음과 같은 "존재 정리"도 가지고 있습니다:  $m$ 을 고정하면 모든 합동 부분군이 유일하게 나타납니다.

#### 정리 63.6.5 (다카기 존재 정리)

$K$ 를 고정하고  $m$ 을 모듈러스라고 합시다. 임의의 합동 부분군  $H$ 를 고려하되, 즉

$$P_K(\mathfrak{m}) \subseteq H \subseteq I_K(\mathfrak{m}).$$

그러면 유일한 아벨 확대  $L/K$ 에 대해  $H = H(L/K, \mathfrak{m})$ 입니다.

마지막으로, 이러한 부분군들은 가능한 최선의 방식으로 포함관계를 반전시킵니다:

#### 보조정리 63.6.6 (포함관계를 반전시키는 합동 부분군)

모듈러스  $m$ 을 고정합시다.  $L/K$ 와  $M/K$ 를 아벨 확대라고 하고,  $m$ 이  $L/K$ 와  $M/K$ 의 도체로 나누어진다고 합시다. 그러면

$$L \subseteq M \quad \text{일 때, 그리고 오직 그때만} \quad H(M/K, \mathfrak{m}) \subseteq H(L/K, \mathfrak{m}).$$

여기서  $L \subseteq M$ 이란  $L$ 이  $M$ 의 어떤 부분체와 동형임을 의미합니다.

증명 개요. 먼저  $m$ 을 고정한 상태에서 동치성을 증명해봅시다. 한 방향으로,  $L \subseteq M$ 이라고 가정합시다; 정의로부터 다음 도식이

$$\begin{array}{ccc} I_K(\mathfrak{m}) & \xrightarrow{\left(\frac{M/K}{\bullet}\right)} & \text{Gal}(M/K) \\ & \searrow \left(\frac{L/K}{\bullet}\right) & \downarrow \\ & & \text{Gal}(L/K) \end{array}$$

가환임을 확인할 수 있는데, 이는 소수 거듭제곱에 대해서만 검증하면 충분하기 때문이며, 이는 단지 프로베니우스 원소가 제한에 대해 잘 작동한다는 것을 말할 뿐입니다. 그러면 핵의 포함관계가 직접적으로 따라옵니다. 역방향은 본질적으로 다카기 존재 정리입니다.  $\square$

여기서 우리는 항상  $m$ 을 도체들의 곱으로 취할 수 있음에 유의하십시오.

혹시 눈치채지 못하셨다면: 이차 상호법칙을 일반화하는 것과는 별개로, 아르틴 상호법칙과 다카기 존재 정리는 함께 모든 아벨 체 확대를 열거합니다! 이제 체  $K$ 가 주어지고  $K$ 의 모든 (유한) 아벨 체 확대를 나열하고자 한다면,  $K$ 의 모든 모듈러스  $m$ 을 나열하고,  $C_K(m)$ 의 모든 부분군을 나열하면, 각 부분군이 체 확대에 대응됩니다.

(물론, 모듈러스와 합동 부분군이 주어졌을 때 체  $L$ 을 어떻게 계산하는가 하는 문제는 여전히 어렵습니다. 적어도  $K = \mathbb{Q}$ 일 때는 [문제 63A†](#)가 답을 줍니다: 모든 유한 아벨 체 확대  $L/\mathbb{Q}$ 는 어떤 원분체에 포함됩니다.)

마무리로, 에밀 아르틴이 자신의 상호법칙에 대해 남긴 말을 인용하겠습니다:

상호법칙에 관한 이야기를 하나 들려드리겠습니다. 제 학위논문 이후, 저는 비아벨 확대에 대한  $L$ -급수를 정의하겠다는 생각을 하게 되었습니다. 그러나 그것들이 아벨 확대에 대한  $L$ -급수와 일치하려면, 어떤 동형사상이 참여해야 했습니다. 저는 그것이 모든 표준적인 상호법칙들을 함의함을 보일 수 있었습니다. 그래서 저는 그것을 일반 상호법칙이라 불렀고 증명하려 했지만, 여러 번 시도했음에도 불구하고 할 수 없었습니다. 그런 다음 다른 정수론자들에게 보여주었지만, 그들은 모두 그것을 비웃었으며, 특히 하세가 그것이 참일 리가 없다고 말했던 것을 기억합니다.

그럼에도 저는 계속 매달렸지만, 제가 시도한 그 무엇도 통하지 않았습니다. 3년 동안 상호법칙을 증명하려 시도하지 않은 주가 단 한 주도 없었습니다. 그것은 낙담스러운 일이었고, 그 사이 저는 다른 일들로 눈을 돌렸습니다. 그러던 어느 오후 특별히 할 일이 없었기에, 저는 "그래, 상호법칙 증명을 다시 시도해보자"라고 말했습니다. 그래서 저는 밖으로 나가 정원에 앉았습니다. 아시다시피, 저는 처음부터 원분체를 사용하겠다는 생각을 가지고 있었지만, 그것들은 결코 통하지 않았고, 이제 저는 갑자기 그동안 내내 제가 그것들을 잘못된 방식으로 사용해왔음을 깨달았습니다 — 그리고 삼십 분 만에 저는 그것을 얻었습니다.

## §63.7 응용: 두 제곱수의 합의 일반화

다음의 고전적인 정리로 시작합니다:

### 정리 63.7.1 (두 제곱수의 합에 관한 페르마의 정리)

홀수 소수  $p$ 는  $p \equiv 1 \pmod{4}$ 일 때, 그리고 그때만 정수  $x$ 와  $y$ 에 대해  $p = x^2 + y^2$ 로 표현될 수 있습니다.

다음과 같은 형태의 증명을 볼 수도 있습니다. 수론과 이차 상호법칙을 배웠으므로 이는 직관적으로 따라오기 쉬운 것입니다.

증명.  $p = x^2 + y^2$ 이면  $\left(\frac{x}{y}\right)^2 \equiv -1 \pmod{p}$ 이므로, 필요조건은  $-1$ 이  $p$ 를 법으로 하는 이차 잉여라는 것임에 주목하십시오.

이 조건이 충분조건이기도 함을 보이겠습니다.

$a^2 \equiv -1 \pmod{p}$ 를 만족하는  $a \in \mathbb{Z}$ 를 잡습니다.  $N_{\mathbb{Q}(i)/\mathbb{Q}}(a+i) = a^2 + 1$ 이  $p$ 로 나누어 떨어지고,  $N_{\mathbb{Q}(i)/\mathbb{Q}}(p) = p^2$ 임에 주목하십시오.

$p = x^2 + y^2$ 로 쓰는 것이 가능하다고 가정합니다. 그러면  $p$ 는 정수  $x$ 와  $y$ 에 대해  $\mathbb{Z}[i]$ 에서  $(x+yi)(x-yi)$ 로 인수분해될 수 있습니다.

$x + yi = \gcd(p, a + i)$ 로 두면 성립함을 주장합니다. 실제로  $p \mid (a + i)(a - i) = a^2 + 1$ 이지만  $p$ 는 두 인수 중 어느 것도 나누지 못하므로, 이는  $p$ 가  $\mathbb{Z}[i]$ 에서 소수가 아님을 의미하며  $a + i$  또는  $a - i$  중 하나와  $\gcd$ 를 취하면 자명하지 않은 인수를 추출해야 합니다.

$N_{\mathbb{Q}(i)/\mathbb{Q}}(x + yi) = p$ 이므로  $x + yi$ 와  $x - yi$ 는 이미 소수이며, 따라서 위의 인수 추출은 이미 우리가 원하는 소인수를 주는 것이 분명합니다.

마지막으로,  $-1$ 이  $p$ 를 법으로 하는 이차 잉여인 것은 정확히  $p \equiv 1 \pmod{4}$ 일 때임을 알고 있으므로, 이로써 증명이 끝났습니다.  $\square$

이를 신비로운 트릭...으로 치부할 수도 있지만, 이것이 다른 많은 경우에도 완벽하게 일반화될 수 있음을 깨닫기 전까지만 그렇습니다! 같은 방법을 사용하여 다음 정리를 증명해 보십시오.

### 정리 63.7.2

홀수 소수  $p > 7$ 은 정수  $x$ 와  $y$ 에 대해  $p = x^2 + 7y^2$ 로 표현될 수 있는 것은  $-7$ 이  $p$ 를 법으로 하여 이차 잉여인 경우이고 오직 그 경우에만 그러합니다.

이는 이차 상호법칙에 의해  $(p \bmod 7) \in \{1, 2, 4\}$ 인지 여부로 귀결됩니다. 그럼에도 불구하고, 항상 그렇게 잘 되는 것은 아닙니다.

### 예제 63.7.3

$p = 3$ 이라고 합시다. 그러면  $1^2 \equiv -5 \pmod{p}$ 이지만,  $p = x^2 + 5y^2$ 를 만족하는 정수  $x$ 와  $y$ 는 존재하지 않습니다.

**질문 63.7.4.** 아직 시도해 보지 않았다면, 아래의 설명을 읽기 전에 증명에서 무엇이 잘못되었는지 스스로 파악해 보십시오.

물론 그 오류는  $\gcd(p, 1 + \sqrt{-5})$ 가 하나의 원소라고 가정한 데 있습니다 — 즉, 이 경우  $\mathbb{Q}(\sqrt{-5})$ 의 정수환은 유일 인수분해 정역이 아닙니다. 하지만 이를 바로잡을 아이디어 이론의 도구들이 모두 있습니다: 아이디얼  $(p) = (3) \subseteq \mathbb{Q}$ 는  $\mathbb{Q}(\sqrt{-5})$ 로 끌어올렸을 때  $(p) = \mathfrak{p}_1 \mathfrak{p}_2$ 로 분해되며, 여기서  $\mathfrak{p}_1 = (3, 1 + \sqrt{-5})$ 이고  $\mathfrak{p}_2 = (3, 1 - \sqrt{-5})$ 입니다. 따라서,

### 명제 63.7.5

소수  $p \in \mathbb{Q}$ 는  $(p)$ 가  $\mathbb{Q}(\sqrt{-5})$ 로 끌어올렸을 때  $\mathfrak{p}_1 \mathfrak{p}_2$ 로 분해되고  $\mathfrak{p}_1$ 과  $\mathfrak{p}_2$  둘 다 주 아이디얼일 때, 그리고 그때만  $p = x^2 + 5y^2$ 로 쓸 수 있습니다.

바로 여기서 아르틴 상호법칙과 힐베르트 유체가 빛을 발합니다 — 우리는  $\mathfrak{p}_1$ 의 류, 다시 말해  $\mathfrak{p}_1 \pmod{1}$ 을 결정하고자 합니다.

**질문 63.7.6.**  $\mathfrak{p} \subseteq \mathbb{Q}(\sqrt{-5})$ 가 주 아이디얼일 때, 그리고 그때만  $\mathfrak{p} \equiv (1) \pmod{1}$ 임을 확인하십시오. (정의를 따라가는 작업입니다.)

**질문 63.7.7.**  $\mathfrak{p}_1$ 이 주 아이디얼이면 자동으로  $\mathfrak{p}_2$ 도 주 아이디얼이 됩니다. 왜 그렇습니까?

이제부터  $K = \mathbb{Q}(\sqrt{-5})$ 라 하고,  $L$ 을  $K$ 의 어떤 아벨 확대라 합시다.

앞서 군  $H(L/K, \mathfrak{m}) = \ker \left( \frac{L/K}{\bullet} \right)$ 을 정의했음을 상기하십시오. 아르틴 상호법칙의 진술은, 여러 주장 중에서도,  $P_K(\mathfrak{m}) \subseteq H(L/K, \mathfrak{m})$ 임을 주장합니다. 당연히, 우리가 신경 쓰는 것이 " $\left( \frac{L/K}{\mathfrak{p}} \right)$ 이 오직  $\mathfrak{p} \pmod{f}$ 에만 의존한다"는 것뿐이라면, 왜  $H$ 에 대해 또 다른 표기를 정의할 필요가 있는지 궁금할 수 있습니다.

음, 위의 단순화된 버전의 아르틴 상호법칙 정리는  $\mathfrak{p} \pmod{f}$ 를 알기만 하면  $\left( \frac{L/K}{\mathfrak{p}} \right)$ 를 계산할 수 있다고 진술합니다. 물론 그 이상이 있습니다:

$P_K(f) = H(L/K, f)$ 이면,  $\left( \frac{L/K}{\mathfrak{p}} \right)$ 를 알기만 하면  $\mathfrak{p} \pmod{f}$ 를 계산할 수 있습니다.

다시 말해,  $L$ 이 합동 부분군이 "하한"에 도달하는 경우라면, 그 역 또한 성립합니다.

**질문 63.7.8.** 위의 대수 계산이 성립함을 확인해 보십시오.

위에서 우리는 합동 부분군  $H(\mathbb{Q}(\zeta_m)/\mathbb{Q}, m\infty)$ 이 하한  $P_{\mathbb{Q}}(m\infty)$ 과 같은 예시 하나, [예제 63.6.4](#)를 살펴보았습니다. 아래에서 하나 더 살펴보겠습니다.

### 예제 63.7.9

위의 예시에서, 우리는 법  $\mathfrak{m}$ 과  $K$  위의 아벨 체 확장  $L$ 을 모두 변화시켜 서로 다른 합동 부분군을 얻을 수 있습니다. 이는 혼란스러울 수 있으므로, 예를 하나 들어봅시다.

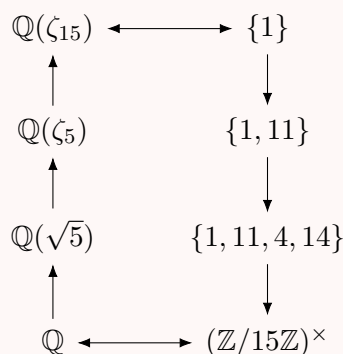
아벨 체 확장  $L/\mathbb{Q}$ 를 생각해 봅시다.  $\mathbb{Q}$ 에서의 법을  $\mathfrak{m} = 15\infty$ 라고 합시다.

선류군  $C_{\mathbb{Q}}(\mathfrak{m})$ 은 물론  $(\mathbb{Z}/15\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ 와 동형입니다.

이 군은 (원소가 8개뿐인) 이렇게 작음에도 불구하고, 부분군이 8개나 있습니다.<sup>a</sup> 그럼에도 불구하고, 우리는 부분군 격자의 관련 부분에만 초점을 맞추겠습니다.

아르틴 상호법칙과 다카기 존재 정리에 의해, 각 합동 부분군은  $L/\mathbb{Q}$  위의 어떤 아벨 확장에 대응합니다.

아래에서 우리는 아벨 체 확장과 합동 부분군  $H(L/\mathbb{Q}, 15\infty)$  사이의 대응관계를,  $H(L/\mathbb{Q}, 15\infty)/P_{\mathbb{Q}}(15\infty)$ 가  $C_{\mathbb{Q}}(15\infty)$ 의 부분군이라는 사실을 이용하여 그립니다. 여기서  $C_{\mathbb{Q}}(15\infty)$ 는  $(\mathbb{Z}/15\mathbb{Z})^\times$ 와 표준적으로 동형입니다.



(위의 도식은 어디서 나온 것일까요? 음, 바탕체가  $\mathbb{Q}$ 라면, [문제 63A<sup>†</sup>](#)이 방법을 제공합니다.)

관심 있는 독자는 아벨 확장의 일반적인 경우에 갈루아 군  $\text{Gal}(L/K)$ 과 선류군  $C_K(\mathfrak{f}(L/K))$  사이의 표준 동형사상을 직접 구해 보고 싶을 수 있습니다.

다음으로, 이것이 다른 법, 예를 들어  $5\infty$ 에 대응하는 아벨 확장들과 어떻게 관련될까요? 직관적으로 말하면, 어떤 아이디얼의 법  $15\infty$ 에서의 값을 안다면, 법  $5\infty$ 에서의

값도 알 수 있을 것입니다. 형식적으로는, 다음과 같은 도식이 있습니다:

$$\begin{array}{ccccc} P_{\mathbb{Q}}(15\infty) & \hookrightarrow & I_{\mathbb{Q}}(15\infty) & \twoheadrightarrow & C_{\mathbb{Q}}(15\infty) \\ \downarrow & & \downarrow & & \downarrow \\ P_{\mathbb{Q}}(5\infty) & \hookrightarrow & I_{\mathbb{Q}}(5\infty) & \twoheadrightarrow & C_{\mathbb{Q}}(5\infty) \end{array}$$

(범주론 장을 읽으셨다면: 짧은 완전열의 사상은 어디에나 나타납니다! 그저 찾아보기만 하면 됩니다.)

즉, 우리는 유도된  $C_{\mathbb{Q}}(15\infty) \twoheadrightarrow C_{\mathbb{Q}}(5\infty)$  사상, 또는 동등하게  $(\mathbb{Z}/15\mathbb{Z})^{\times} \twoheadrightarrow (\mathbb{Z}/5\mathbb{Z})^{\times}$ 를 얻습니다. 이번에는, 법  $5\infty$ 에 대응하는 아벨 체 확장은 다음과 같습니다:

$$\begin{array}{ccc} \mathbb{Q}(\zeta_5) & \longleftrightarrow & \{1\} \\ \uparrow & & \downarrow \\ \mathbb{Q}(\sqrt{5}) & & \{1, 4\} \\ \uparrow & & \downarrow \\ \mathbb{Q} & \longleftrightarrow & (\mathbb{Z}/5\mathbb{Z})^{\times} \end{array}$$

<sup>a</sup><https://beta.lmfdb.org/Groups/Abstract/diagram/8.2>에 도식이 있습니다.

우리의 경우,  $p \in \mathbb{Q}$ 가 소수이고  $K = \mathbb{Q}(\sqrt{-5})$ 로 확장했을 때  $(p) = \mathfrak{p}_1 \mathfrak{p}_2$ 로 인수분해된다고 할 때, 우리는  $\mathfrak{p}_1$ 이 주 아이디얼인지 판정하고자 합니다 — 다시 말해, “ $\mathfrak{p}_1 \pmod{1}$ ”을 계산하고자 합니다. 위의 통찰을 이용하여, 이 조건을 아르틴 기호를 이용해 다시 표현하겠습니다.

$L = K(i)$ 라고 합시다. (나중에,  $L$ 이  $K$ 의 **힐베르트 유체**임을 알게 될 것입니다.) 우리는 다음이 참임을 주장합니다:

- $L/K$ 는 아벨 확장이고,
- 도체는  $f = f(L/K) = 1$ 이며,
- $H(L/K, f) = P_K(f)$ 입니다 — 즉, 이것이 바로  $\left(\frac{L/K}{\mathfrak{p}}\right)$ 를 바탕으로  $\mathfrak{p} \subseteq K$ 에 대해  $\mathfrak{p} \pmod{1}$ 을 결정할 수 있는 바로 그 상황입니다.

(일반적인 경우, 체  $L$ 은 **문제 63B<sup>†</sup>**에 따라 존재합니다.)

그러면, 소 아이디얼  $\mathfrak{p} \subseteq K$ 에 대해, 다음은 서로 동치입니다:

1.  $\mathfrak{p}$ 는 주 아이디얼입니다.
2.  $\left(\frac{L/K}{\mathfrak{p}}\right) = \text{id}$ ;
3.  $\mathfrak{p}$ 는  $L$ 로 올렸을 때 완전히 분해됩니다.

첫 번째 진술과 두 번째 진술의 동치를 증명하기 위해 아벨 확대  $L/K$ 에 대한 아르틴 상호법칙(과 그 “역”)을 사용했음을 주목하십시오.

**연습문제 63.7.10.** 두 번째 진술과 세 번째 진술은 왜 동치입니까? (**문제 63B<sup>†</sup>**.)

따라서 주 아이디얼  $\mathfrak{p}_1$ 과  $\mathfrak{p}_2$ 에 대해  $(p) = \mathfrak{p}_1 \mathfrak{p}_2$ 라는 조건은  $(p) \subseteq \mathbb{Q}$ 가  $L$ 로 올렸을 때 완전히 분해된다는 것과 동치입니다.

아벨 확대  $L/\mathbb{Q}$ 에 대해 위와 유사하게 추론하면, 다음이 동치입니다:

1.  $(p) \subseteq \mathbb{Q}$ 는  $L$ 로 올렸을 때 완전히 분해됩니다.
2.  $\left(\frac{L/\mathbb{Q}}{(p)}\right) = \text{id}$ .

이번에는 첫 번째 항목이 더 이상 없습니다 —  $L$ 은  $\mathbb{Q}$ 의 힐베르트 유체가 아닙니다 — 하지만 아르틴 상호법칙에 의해 다음을 알 수 있습니다:

$\left(\frac{L/\mathbb{Q}}{(p)}\right)$ 의 값은 오직  $(p) \pmod{f(L/\mathbb{Q})}$ 에만 의존합니다.

이 경우, 확대  $L/\mathbb{Q}$ 의 도체는  $f(L/\mathbb{Q}) = 20\infty$ 입니다.  
자, 요약하면:

$$\begin{aligned}
 & p \text{는 } x^2 + 5y^2 \text{로 쓸 수 있습니다} \\
 \iff & \mathbb{Q}(\sqrt{-5}) \text{로 올렸을 때 } (p) = \mathfrak{p}_1 \mathfrak{p}_2 \text{이고 } \mathfrak{p}_1 \text{이 주 아이디얼임} \\
 \iff & (p) = \mathfrak{p}_1 \mathfrak{p}_2 \text{이고, } \mathfrak{p}_1 \subseteq \mathbb{Q}(\sqrt{-5}) \text{가 } \mathbb{Q}(\sqrt{-5}, i) \text{로 올렸을 때 완전히 분해됨} \\
 \iff & (p) \subseteq \mathbb{Q} \text{가 } \mathbb{Q}(\sqrt{-5}, i) \text{로 올렸을 때 완전히 분해됨} \\
 \iff & \left(\frac{\mathbb{Q}(\sqrt{-5}, i)/\mathbb{Q}}{(p)}\right) = \text{id} \\
 \iff & (p \bmod 20) \in \{1, 9\}.
 \end{aligned}$$

다 됐습니다! 정리의 최종 형태는 다음과 같습니다:

#### 정리 63.7.11

$p \nmid 20$ 인 소수  $p$ 가 있다고 합시다. 그러면  $p$ 가  $x^2 + 5y^2$ 로 쓰일 수 있는 것은  $(p \bmod 20) \in \{1, 9\}$ 인 것과 동치입니다.

### §63.8 생각해 볼 만한 조금 더 어려운 문제

**문제 63A<sup>†</sup>.** [크로네커-베버 정리]  $L$ 을  $\mathbb{Q}$ 의 아벨 확대라고 합시다. 그러면  $L$ 은 원분 확대  $\mathbb{Q}(\zeta)$ 에 포함되며, 여기서  $\zeta$ 는 (어떤  $m$ 에 대한)  $m$ 차 단위근입니다.

**문제 63B<sup>†</sup>** (힐베르트 유체).  $K$ 를 임의의 대수적 수체라고 합시다. 그러면 모든 소수(유한 소수든 무한 소수든)에서 비분지이며 다음을 만족하는 유일한 아벨 확대  $E/K$ 가 존재합니다:

- $E/K$ 는 포함 관계상 그러한 확대 중 극대인 확대입니다.
- $\text{Gal}(E/K)$ 는  $K$ 의 유수군과 동형입니다.
- $K$ 의 소 아이디얼  $\mathfrak{p}$ 가  $E$ 에서 완전히 분해되는 것은 그것이  $\mathcal{O}_K$ 의 주 아이디얼인 것과 동치입니다.

우리는  $E$ 를  $K$ 의 **힐베르트 유체**라고 부릅니다.

**문제 63C.** 소수  $p \nmid m$ 이  $p = x^2 + 23y^2$ 으로 쓰일 수 있는지가 오직  $p \bmod m$ 에만 의존하도록 하는 양의 정수  $m$ 은 존재하지 않습니다. 그 이유를 추측해 보십시오.

# XVI

대수적 위상수학 I: 호모토피

## 제XVI부: 목차

---

|           |                                                         |            |
|-----------|---------------------------------------------------------|------------|
| <b>64</b> | <b>몇 가지 위상수학적 구성</b>                                    | <b>655</b> |
| 64.1      | 구 . . . . .                                             | 655        |
| 64.2      | 몹위상 . . . . .                                           | 655        |
| 64.3      | 곱위상 . . . . .                                           | 657        |
| 64.4      | 분리합집합과 켤레 . . . . .                                     | 658        |
| 64.5      | CW 복합체 . . . . .                                        | 659        |
| 64.6      | 원환면, 클라인 병, $\mathbb{R}P^n$ , $\mathbb{C}P^n$ . . . . . | 660        |
| 64.7      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                          | 666        |
| <b>65</b> | <b>기본군</b>                                              | <b>667</b> |
| 65.1      | 경로를 융합하기 . . . . .                                      | 667        |
| 65.2      | 기본군 . . . . .                                           | 668        |
| 65.3      | 기본군은 위상동형사상에 대해 불변입니다 . . . . .                         | 673        |
| 65.4      | 고차 호모토피 군 . . . . .                                     | 673        |
| 65.5      | 호모토피 동치인 공간 . . . . .                                   | 674        |
| 65.6      | 점을 가진 호모토피 범주 . . . . .                                 | 676        |
| 65.7      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                          | 677        |
| <b>66</b> | <b>피복 사영</b>                                            | <b>679</b> |
| 66.1      | 균등 피복과 피복 사영 . . . . .                                  | 679        |
| 66.2      | 올림 정리 . . . . .                                         | 681        |
| 66.3      | 들어올리기 대응 . . . . .                                      | 684        |
| 66.4      | 정칙 피복(Regular coverings) . . . . .                      | 685        |
| 66.5      | 기본군의 대수 . . . . .                                       | 687        |
| 66.6      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                          | 688        |

---

# 64 몇 가지 위상수학적 구성

이 짧은 장에서는 아직 다루지 않은 위상수학의 흔한 공간과 구성 몇 가지를 간략히 설명합니다.

## §64.1 구

다음을 기억하십시오

$$S^n = \{(x_0, \dots, x_n) \mid x_0^2 + \dots + x_n^2 = 1\} \subset \mathbb{R}^{n+1}$$

는  $n$ -구의 표면이며, 반면

$$D^{n+1} = \{(x_0, \dots, x_n) \mid x_0^2 + \dots + x_n^2 \leq 1\} \subset \mathbb{R}^{n+1}$$

는 이에 대응하는 닫힌 공입니다 (예를 들어,  $D^2$ 는 평면 위의 원판이고  $S^1$ 은 단위원입니다.)

**연습문제 64.1.1.** 열린 공  $D^n \setminus S^{n-1}$ 이  $\mathbb{R}^n$ 과 동형사상임을 보이십시오.

특히,  $S^0$ 은 두 점으로 이루어져 있으며,  $D^1$ 은 구간  $[-1, 1]$ 로 생각할 수 있습니다.



## §64.2 몫위상

**이 절의 대표적인 예:**  $D^n/S^{n-1} = S^n$ , 또는 원환면(*torus*)입니다.

공간  $X$ 가 주어지면, 임의의 동치관계  $\sim$ 에 의해 몇몇 점들을 함께 동일시할 수 있습니다;  $x \in X$ 에 대해 그 동치류를  $[x]$ 로 표기합니다. 기하학적으로, 이는  $\sim$  아래에서 동치인 점들을 서로 붙여 접합함으로써 얻어지는 공간입니다.

형식적으로,

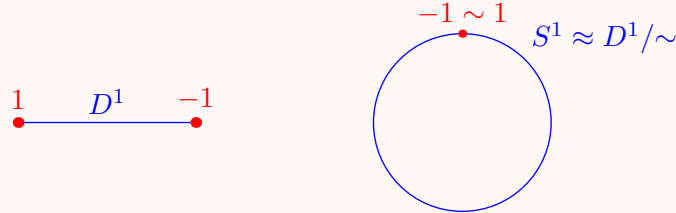
**정의 64.2.1.**  $X$ 를 위상 공간이라 하고,  $\sim$ 를  $X$ 의 점들에 대한 동치관계라 합시다. 그러면  $X/\sim$ 는 다음과 같은 공간입니다

- 점들은  $X$ 의 동치류이며, 그리고
- $U \subseteq X/\sim$ 가 열린집합인 것은  $\{x \in X \text{ 다음을 만족하는 } [x] \in U\}$ 가  $X$ 에서 열린집합인 것과 동치입니다.

제가 알기로, 이 정의는 직관적으로는 대부분 쓸모가 없으므로, 여기 몇 가지 예시를 들어보겠습니다.

**예제 64.2.2 (끝점을 기준으로 한 구간의 몫)**

$D^1 = [-1, 1]$ 을 취하고, 끝점  $-1$ 과  $1$ 을 동일시하는 동치관계로 몫을 취한다고 합시다. (형식적으로,  $x \sim y \iff (x = y) \text{ 또는 } \{x, y\} = \{-1, 1\}$ 입니다.) 이 경우, 우리는 단순히  $S^1$ 을 다시 얻게 됩니다:



몫공간에서  $-1 \sim 1$  주위의 작은 열린 근방이 원래 공간  $D^1$ 에서는  $-1$ 과  $1$ 에서의 두 반구간에 대응함을 관찰하십시오. 이것으로 우리가 제시한 정의가 올바른 것임을 확신할 수 있을 것입니다.

**예제 64.2.3 (더 많은 몫공간들)**

다음을 스스로 확인해 보십시오:

- 앞선 예시를 일반화하면,  $D^n$ 을 그 경계  $S^{n-1}$ 로 몫을 취한 것이  $S^n$ 입니다.
- 정사각형  $ABCD$ 가 주어졌을 때, 변  $AB$ 와  $DC$ 를 함께 동일시한다고 합시다. 그러면 원기둥을 얻게 됩니다. (초등학교 때, 종이 조각들을 테이프로 붙여 원기둥을 만들던 것을 떠올려 보십시오.)
- 앞선 예시에서,  $BC$ 와  $DA$ 도 함께 동일시한다면, 원환면을 얻게 됩니다. (우리의 원기둥을 가져다가 양 끝의 두 원을 서로 붙인다고 상상해 보십시오.)
- $X = \mathbb{R}$ 이라 하고,  $y - x \in \mathbb{Z}$ 이면  $x \sim y$ 라고 합시다. 그러면  $X/\sim$  역시  $S^1$ 입니다.

위에서 다룬 특수한 경우 하나는 다음과 같습니다.

**정의 64.2.4.**  $A \subseteq X$ 라 합시다.  $A$ 의 모든 점들을 서로 동일시하면서 나머지 모든 점들은 동치가 아닌 채로 남겨두는 동치 관계를 생각해 봅시다. (다시 말해,  $x = y$ 이거나  $x, y \in A$ 이면  $x \sim y$ 입니다.) 그러면 결과로 나오는 몫공간을  $X/A$ 로 표기합니다.

그러므로 이 표기법에서,

$$D^n/S^{n-1} = S^n.$$

**표기의 남용 64.2.5.** 저는 일부러 부정확하게 “ $D^n/S^{n-1} = S^n$ ”이라거나 “ $D^n/S^{n-1}$ 은  $S^n$ 입니다”라고 말하고 있는데, 사실은 “ $D^n/S^{n-1}$ 은  $S^n$ 과 동형사상입니다”라고 말해야 합니다. 이는 수학에서 일반적으로 나타나는 주제로서, 동형/동형사상/등등인 대상들은 대체로 서로 세심하게 구별되지 않습니다.

**예제 64.2.6 (더 기이한 몫공간)**

부분집합  $A$ 가  $X$ 에서 닫혀 있지 않다면,  $X/A$ 는 상당히 기이해질 것입니다.

예를 들어,  $X = \mathbb{R}$ 이고  $A = (0, 1)$ 이라 합시다. 그러면 공간  $X/A$ 는 점들  $(-\infty, 0] \cup \{A/A\} \cup [1, \infty)$ 로 이루어집니다. 여기서 점  $0$ 과  $A/A$ 는 서로 다르지만,  $0$ 을 포함하는

모든 열린집합은  $A/A$  또한 포함합니다.  
우리는 이 공간  $X/A$ 가 하우스도르프 공간이 아니라고 말합니다.

### §64.3 곱위상

이 절의 대표적인 예:  $\mathbb{R} \times \mathbb{R}$ 은  $\mathbb{R}^2$ 이고,  $S^1 \times S^1$ 은 토러스입니다.

**정의 64.3.1.** 위상 공간  $X$ 와  $Y$ 가 주어졌을 때,  $X \times Y$  위의 **곱위상**이란 다음과 같은 공간입니다.

- 점들은  $x \in X, y \in Y$ 인 순서쌍  $(x, y)$ 이며,
- 위상은 다음과 같이 주어집니다.  $X \times Y$ 에 대한 위상의 기저는 열린집합  $U \subseteq X$ 와 열린집합  $V \subseteq Y$ 에 대해  $U \times V$ 입니다.

**비고 64.3.2** — 사실  $U$ 와  $V$ 에 대해서는 기저 원소들만 고려해도 충분함을 보이는 어렵지 않습니다. 즉,

$$\{U \times V \mid U, V \text{ 다음에 대한 기저 원소 } X, Y\}$$

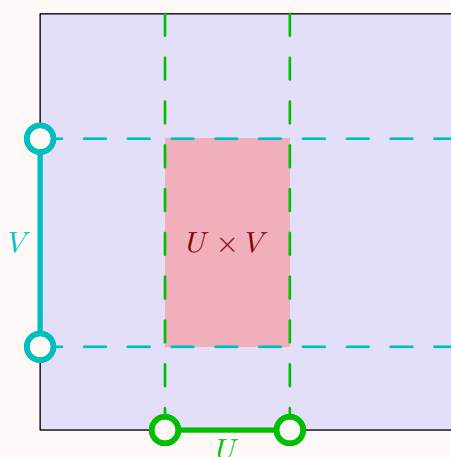
또한  $X \times Y$ 의 기저입니다.

우리는 실제로 기저를 손봐야 합니다.  $\mathbb{R} \times \mathbb{R}$ 에서, 열린 단위 원판은  $U \times V$ 의 형태가 아님에도 불구하고 열린집합이어야 마땅합니다.

이는 여러분이 생각하는 바로 그대로 작동합니다.

#### 예제 64.3.3 (단위 정사각형)

$X = [0, 1]$ 이라 하고  $X \times X$ 를 생각해 봅시다. 우리는 물론 이것이 단위 정사각형이 되기를 기대합니다. 아래 그림은 기저에 속하는  $X \times X$ 의 한 열린집합입니다.



**연습문제 64.3.4.** 이 기저가  $X \times X$  위의 곱 거리로부터 나오는 위상과 동일한 위상을 준다는 것을 스스로 확인해 보십시오. 그러므로 이것이 “올바른” 정의입니다.

**예제 64.3.5 (더 많은 곱공간)**

- (a)  $\mathbb{R} \times \mathbb{R}$ 은 유클리드 평면입니다.
- (b)  $S^1 \times [0, 1]$ 은 원기둥입니다.
- (c)  $S^1 \times S^1$ 은 원환면입니다! (왜 그런지 아시겠습니까?)

**§64.4 분리합집합과 켜기합**

**이 절의 대표적인 예:**  $S^1 \vee S^1$ 은 8자 모양입니다.

두 공간의 분리합집합은 기하학적으로 이름 그대로입니다: 두 공간을 나란히 놓는다고 생각하시면 됩니다. 완결성을 위해 여기에 형식적인 정의를 제시합니다.

**정의 64.4.1.**  $X$ 와  $Y$ 를 두 위상 공간이라 합시다.  $X \amalg Y$ 로 표기되는 **분리합집합**은 다음과 같이 정의됩니다

- 점들은 분리합집합  $X \amalg Y$ 이며, 그리고
- 부분집합  $U \subseteq X \amalg Y$ 가 열린집합인 것은  $U \cap X$ 와  $U \cap Y$ 가 열린집합인 것과 동치입니다.

**연습문제 64.4.2.** 공집합이 아닌 두 공간의 분리합집합이 비연결임을 보이십시오.

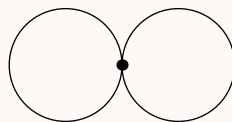
더 흥미로운 것은 켜기합인데, 여기서는 두 위상 공간  $X$ 와  $Y$ 가 하나의 기준점에서만 융합됩니다.

**정의 64.4.3.**  $X$ 와  $Y$ 를 위상 공간이라 하고,  $x_0 \in X$ 와  $y_0 \in Y$ 를 점이라 합시다. 동치 관계  $\sim$ 을  $x_0 \sim y_0$ 만 성립하도록 정의합니다. 그러면 두 공간의 **켄기합**은 다음과 같이 정의됩니다

$$X \vee Y = (X \amalg Y) / \sim.$$

**예제 64.4.4 ( $S^1 \vee S^1$ 은 8자 모양입니다)**

$X = S^1$ 이고  $Y = S^1$ 이라 하고,  $x_0 \in X$ 와  $y_0 \in Y$ 를 임의의 점이라 합시다. 그러면  $X \vee Y$ 는 "8자 모양"입니다: 이는 한 점에서 융합된 두 원입니다.



**표기의 남용 64.4.5.**  $x_0$ 와  $y_0$ 이 자명하거나(또는 무관할 때) 우리는 종종 이를 언급하지 않습니다. 예를 들어, 이제부터는 8자 모양을 그냥  $S^1 \vee S^1$ 로 쓰겠습니다.

**비고 64.4.6** — 성가시게도, L<sup>A</sup>T<sub>E</sub>X에서 `\wedge`는  $\wedge$ 가 아니라  $\vee$ 를 줍니다(전자는 `\vee`입니다). 그러므로 이는 사실 "비 곱(vee product)"이라 불러야 하지만, 이미 늦었습니다.

## §64.5 CW 복합체

이 구성을 이용하여 우리는 몇 가지 공간을 만들어 보기 시작할 수 있습니다. 그렇게 하는 흔한 방법 중 하나는 이른바 **CW 복합체**를 사용하는 것입니다. 직관적으로, CW 복합체는 다음과 같이 만들어집니다:

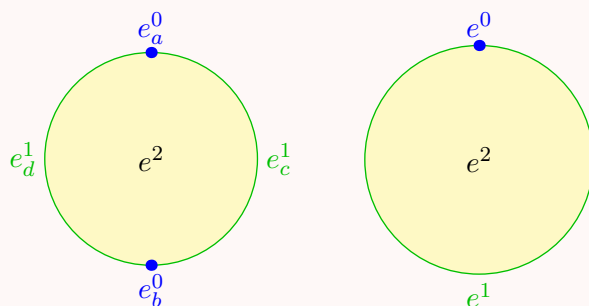
- 점들의 집합  $X^0$ 에서 시작합니다.
- 선분들(즉  $D^1$ 의 복사본들)을 취하여 그 끝점들( $S^0$ 의 복사본들)을  $X^0$ 에 융합시켜  $X^1$ 을 정의합니다.
- $D^2$ (원판)의 복사본들을 취하여 그 경계( $S^1$ 의 복사본)를  $X^1$ 에 용접하여  $X^2$ 를 정의합니다.
- 유한한 단계  $n$ 에 이를 때까지 귀납적으로 반복합니다; 이때  $X$ 는  **$n$ 차원**이라고 합니다.

그 결과로 얻어지는 공간  $X$ 가 CW 복합체입니다. 집합  $X^k$ 는  $X$ 의  **$k$ -골격**이라 불립니다. 각  $D^k$ 는  **$k$ -세포**라고 불리며, 관례적으로  $\alpha$ 가 어떤 첨자일 때  $e_\alpha^k$ 로 표기합니다. 유한히 많은 세포만 사용되었을 경우  $X$ 는 **유한**하다고 합니다.

**표기의 남용 64.5.1.** 엄밀히 말하면, 대부분의 문헌(예를 들어 [Ha02])은 무한 차원 CW 복합체를 구성하는 것도 허용합니다. 뉘킨에서는 그러한 공간을 다루지 않을 것입니다.

### 예제 64.5.2 ( $2 + 2 + 1$ 및 $1 + 1 + 1$ 세포로 이루어진 $D^2$ )

- (a) 먼저, 두 점  $e_a^0$ 과  $e_b^0$ 을 갖는  $X^0$ 에서 시작합니다. 그런 다음, 두 개의 1-세포  $D^1$ (초록색)로 이들을 연결하고, 이를  $e_c^1$ 과  $e_d^1$ 이라 부릅니다. 각 1-세포의 끝점들( $S^0$ 의 복사본)은  $X^0$ 의 서로 다른 점들과 동일시되므로,  $X^1 \cong S^1$ 이 됩니다. 마지막으로, 단 하나의 2-세포  $e^2$ (노란색)를 취하여, 그 경계가 방금 그린  $S^1$ 의 복사본에 들어맞도록 용접합니다. 이렇게 하면 왼쪽 그림이 나옵니다.
- (b) 사실, 단  $1 + 1 + 1 = 3$ 개의 세포만으로도 이를 할 수 있습니다. 하나의 점  $e^0$ 을 갖는  $X^0$ 에서 시작합니다. 그런 다음, 하나의 1-세포  $e^1$ 을 사용하여 그 두 끝점을  $X^0$ 의 그 하나의 점에 융합시킵니다. 그러면 앞서와 같이  $S^1$ 의 복사본을 끼워 넣을 수 있으며, 오른쪽에 있는  $D^2$ 가 됩니다.



### 예제 64.5.3 (CW 복합체로서의 $S^n$ )

- (a)  $S^n$  ( $n \geq 1$ 인 경우)은 단 두 개의 세포만으로 얻을 수 있습니다. 즉,  $X^0$ 에 대해 단일한 점  $e^0$ 을 취하고,  $S^n$ 을 얻기 위해  $D^n$ 을 취하여 그 경계 전체를  $e^0$ 에 용접합니다. 이 예시는 이미 처음에  $n = 2$ 인 경우로 살펴본 적이 있는데, 원판  $D^2$ 의 경계를 함께 융합했을 때 구  $S^2$ 가 그 결과임을 확인했습니다.
- (b) 대안으로, 각 차원마다 두 개의 세포를 사용하여  $S^n$ 을 귀납적으로 구성하는 “반구”

구성을 할 수도 있습니다. 즉  $S^0$ 은 두 점으로 이루어지고,  $S^1$ 은 이 두 점을 두 개의 선분(1-세포)으로 연결하여 얻어지며,  $S^2$ 는  $S^1$ 을 적도로 하는 두 개의 반구(각각 2-세포)를 접합하여 얻어집니다.

**정의 64.5.4.** 형식적으로,  $X^k$ 에 추가하고자 하는 각  $k$ -세포  $e_\alpha^k$ 에 대해, 그 경계  $S_\alpha^{k-1}$ 를 취하여 **부착 사상**(attaching map)  $S_\alpha^{k-1} \rightarrow X^{k-1}$ 을 통해  $X^{k-1}$ 에 용접합니다. 그러면

$$X^k = \left( X^{k-1} \amalg \left( \coprod_\alpha e_\alpha^k \right) \right) / \sim$$

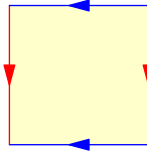
여기서  $\sim$ 은  $e_\alpha^k$ 의 각 경계점을  $X^{k-1}$ 에서의 그 상(image)과 동일시합니다.

## §64.6 원환면, 클라인 병, $\mathbb{RP}^n$ , $\mathbb{CP}^n$

이제 CW 복합체의 가장 중요한 예시 네 가지를 제시하겠습니다.

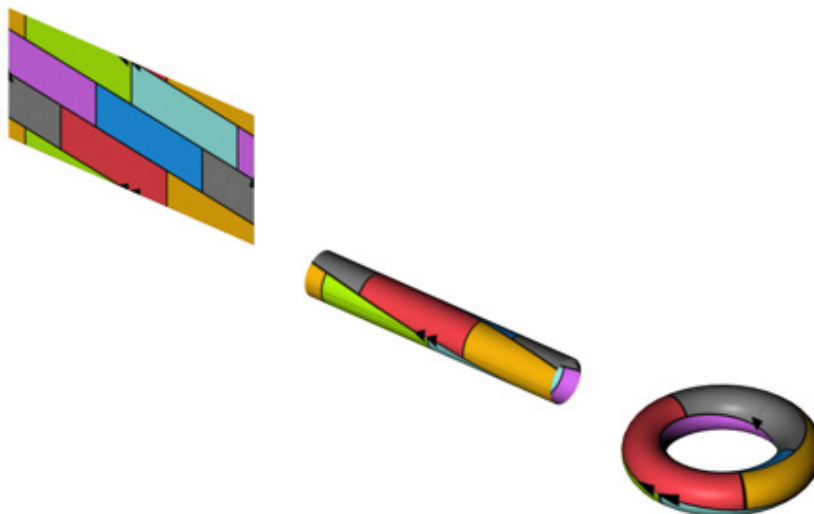
### §64.6.i 원환면

**원환면**(torus)은 정사각형을 취하여 마주보는 변들을 같은 방향으로 동일시함으로써 형성할 수 있습니다. 즉, 오른쪽 변을 걸어 나가면 왼쪽 변의 대응하는 점에서 다시 나타납니다. (아타리(Atari)의 애스터로이드를 떠올려 보십시오!)



따라서 원환면은  $(\mathbb{R}/\mathbb{Z})^2 \cong S^1 \times S^1$ 입니다.

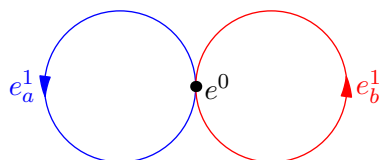
네 개의 모서리가 모두 함께 하나의 점으로 동일시된다는 점에 유의하십시오. 정사각형을 종이 한 장으로 취급하여 왼쪽과 오른쪽(빨간색) 변을 테이프로 붙여 원기둥을 만든 다음, 그 원기둥을 구부려 위쪽과 아래쪽(파란색) 변을 융합함으로써 3차원 공간에서 원환면을 실현할 수 있습니다.



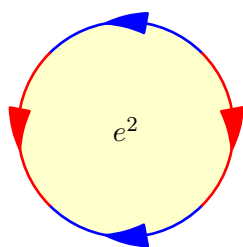
이미지 출처 [To]

원환면은 다음과 같은 CW 복합체로 실현될 수 있습니다.

- 단일한 점으로 이루어진 0-뼈대,
- 두 개의 1-세포  $e_a^1$ ,  $e_b^1$ 로 이루어진 1-뼈대, 그리고



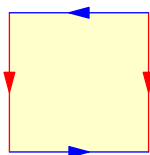
- 단일한 2-세포  $e^2$ 로 이루어진 2-뼈대. 이때 그 둘레는 네 부분으로 나뉘어 “ $aba^{-1}b^{-1}$ 를 통해” 1-뼈대에 용접됩니다. 이는 다음을 의미합니다: 둘레의 4분의 1을  $e_a^1$ 에 감고, 다시 4분의 1을  $e_b^1$ 에 감은 다음, 세 번째 4분의 1을  $e_a^1$ 에 반대 방향으로 감고, 네 번째 4분의 1을 이전과 반대 방향으로  $e_b^1$ 에 다시 감습니다.



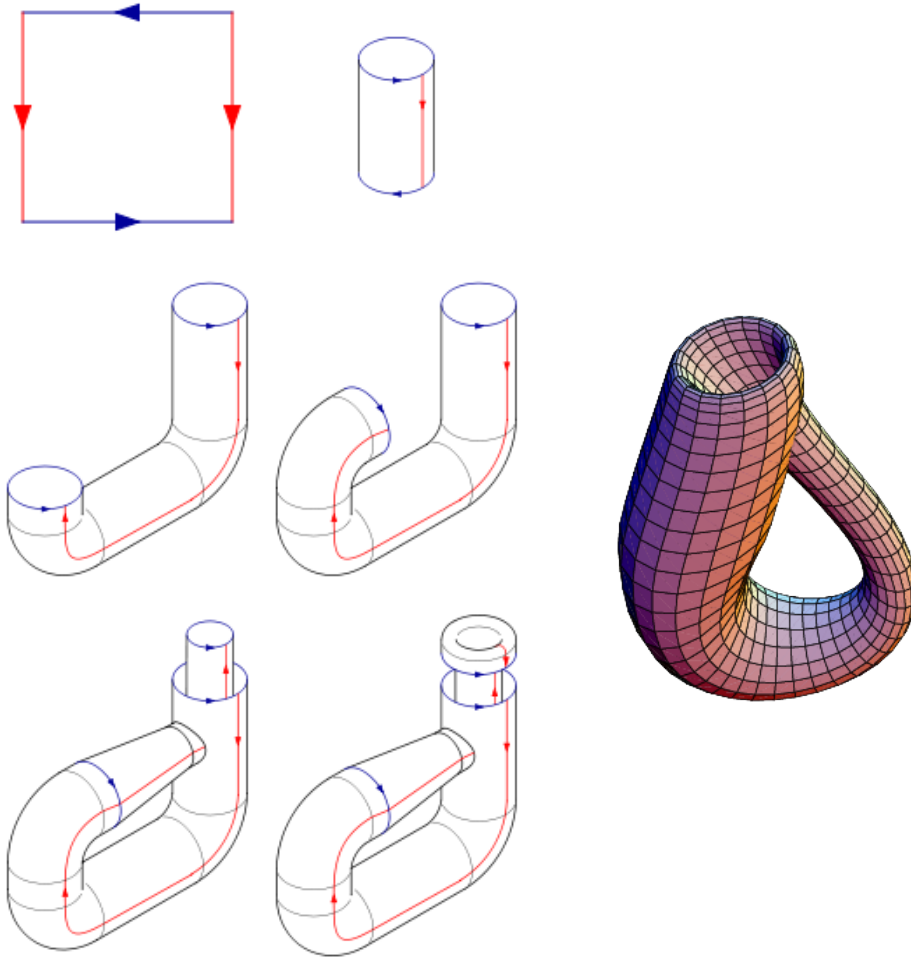
$aba^{-1}b^{-1}$ 를 **부착 단어**(attaching word)라고 부르는데, 이 축약 표기는 이후에 유용할 것입니다.

### §64.6.ii 클라인 병

**클라인 병**(Klein bottle)은 원환면과 유사하게 정의되지만, 그림에서 보듯이 한 쌍의 변이 반대 방식으로 동일시된다는 점만 다릅니다.



원환면과 달리, 이것은 자기 교차 없이 3차원 공간에서 구현할 수 없습니다. 이전과 같이 빨간색 변들을 붙여 원기둥을 얻을 수는 있지만, 그 결과로 생긴 파란색 원들을 서로 반대 방향으로 융합하는 것은 3차원에서 불가능합니다. 그럼에도 불구하고, 우리는 원기둥이 자기 자신과 교차하는 것을 암묵적으로 허용한 채 3차원 공간에서 그림을 그리는 경우가 종종 있습니다.



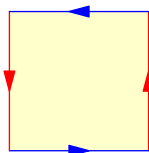
[In; Fr]에서 가져온 이미지

원환면과 마찬가지로, 클라인 병은 다음을 갖는 CW 복합체로 구현됩니다

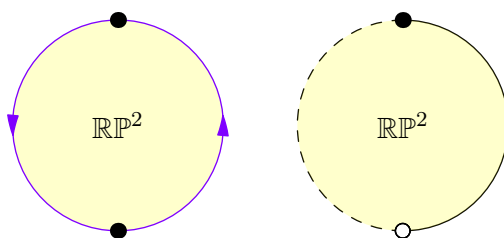
- 하나의 0-세포,
- 두 개의 1-세포  $e_a^1$ 와  $e_b^1$ , 그리고
- 이번에는  $abab^{-1}$  단어를 통해 부착된 단일 2-cell입니다.

### §64.6.iii 실사영 공간

$n = 2$ 부터 시작해봅시다. 공간  $\mathbb{RP}^2$ 는 그림과 같이 이전 정사각형의 양쪽 방향을 모두 뒤집으면 얻어집니다.



그러나 이렇게 하고 나면 원래 다각형이 정사각형이라는 사실은 그다지 중요하지 않습니다. 빨간 변과 파란 변을 합쳐서 하나의 보라색 변으로 만들 수 있습니다. 이는 원둘레의 절반이 나머지 절반과 동일시된 원으로도 동등하게 생각할 수 있습니다:



그 결과로 얻어지는 공간은 사영 (유클리드) 기하학을 다루는 분들에게 익숙할 것입니다. 실제로 여러 가지 기하학적 해석이 가능합니다:

- $\mathbb{RP}^2$ 는  $\mathbb{R}^3$ 에서 원점을 지나는 직선들의 집합으로 생각할 수 있으며, 각 직선이  $\mathbb{RP}^2$ 의 한 점이 됩니다.

물론 각 직선을 단위 구  $S^2$  위의 한 점과 동일시할 수 있는데, 다만 두 대척점이 실제로는 같은 직선에 대응한다는 성질만 예외입니다. 따라서  $\mathbb{RP}^2$ 는 거의 "구의 절반"으로 생각할 수 있습니다. 이를 평평하게 펴면 위의 그림이 됩니다.

- $\mathbb{R}^2$ 에 "무한원점"을 추가한 것을 상상해 보십시오. 이는 직선의 가능한 방향마다 하나씩, "무한히 멀리 있는" 점들을 추가한다는 뜻입니다. 따라서  $\mathbb{RP}^2$ 에서는 임의의 두 직선이 실제로 교차합니다(평행하지 않으면 유클리드 점에서, 평행하면 무한원점에서 교차합니다).

이는  $\mathbb{RP}^2$ 에 대한 하나의 해석을 제공하는데, 경계는 모든 무한원점들을 지나는 무한원 직선을 나타냅니다. 여기서는  $\mathbb{R}^2$ 와  $D^2$ 의 내부가 위상동형이라는 사실을 사용했습니다.

**연습문제 64.6.1.**  $\mathbb{R}^3$ 에서 평면  $z = 1$ 을 고려하고 첫 번째 형식화에서의 각 직선을 이 평면과 교차시킴으로써, 이러한 형식화들이 동등함을 관찰하십시오.

$\mathbb{RP}^2$ 는 좌표를 사용해서도 나타낼 수 있습니다: 이는 스케일링에 대해 모두 0은 아닌 실수의 삼중항  $(x : y : z)$ 들의 집합이며, 이는 다음을 의미합니다

$$(x : y : z) = (\lambda x : \lambda y : \lambda z)$$

임의의  $\lambda \neq 0$ 에 대해서입니다. " $\mathbb{R}^3$ 에서 원점을 지나는 직선"이라는 해석을 사용하면 이 좌표계가 왜 올바른 공간을 나타내는지 명확해집니다. 무한원점은  $z = 0$ 인 점들이며,  $z \neq 0$ 인 임의의 점은 다음과 같은 이유로 데카르트 점을 나타냅니다

$$(x : y : z) = \left( \frac{x}{z} : \frac{y}{z} : 1 \right)$$

따라서 이를 데카르트 점  $(\frac{x}{z}, \frac{y}{z})$ 로 생각할 수 있습니다.

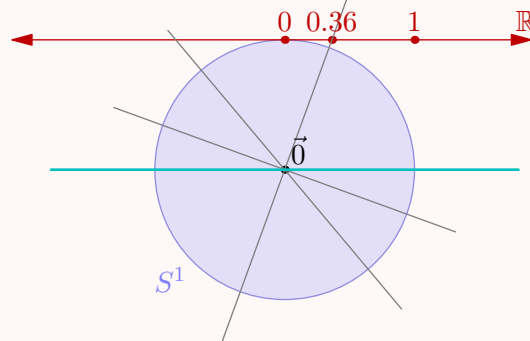
이런 방식으로 우리는 임의의  $n$ 에 대해  **$n$ 차원 실사영 공간**,  $\mathbb{RP}^n$ 을 다음 중 하나로 실제로 정의할 수 있습니다

- $\mathbb{R}^{n+1}$ 에서 원점을 지나는 직선들의 집합,
- 위와 같이  $n + 1$ 개의 좌표를 사용하거나, 또는
- 무한원점이 추가된  $\mathbb{R}^n$ 으로서, 이 무한원점들 자체는  $\mathbb{RP}^{n-1}$ 의 사본을 이룹니다.

도움이 될 만한 예시로,  $\mathbb{RP}^1$ 에 대한 세 가지 그림을 모두 제시합니다.

**예제 64.6.2** (1차원 실사영 공간)

$\mathbb{RP}^1$ 은 대척점들이 동일시되는 관계에 대한  $S^1$ 의 몫으로 생각할 수 있습니다. 접선 위로 사영하면, 아래에 청록색으로 그려진 평행선에 대응하는 무한원점 하나가 추가된  $\mathbb{R}$ 의 사본을 얻게 됨을 알 수 있습니다.



따라서  $\mathbb{RP}^1$ 의 점들은 두 가지 형태를 갖습니다:

- $(x : 1)$ 은 위에서 짙은 빨간색으로 표시된  $x \in \mathbb{R}$ 로 생각하며, 그리고
- $(1 : 0)$ 은 위의 청록색 직선에 대응하는  $1/0 = \infty$ 로 생각합니다.

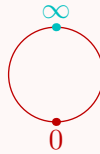
따라서 우리는 말 그대로 다음과 같이 쓸 수 있습니다

$$\mathbb{RP}^1 = \mathbb{R} \cup \{\infty\}.$$

$\mathbb{RP}^1$ 은 또한  $\mathbb{RP}^2$ 의 경계이기도 함에 유의하십시오. 실제로 위상적으로도 다음이 성립함에 유의하십시오

$$\mathbb{RP}^1 \cong S^1$$

”양 끝점이 붙은 실직선”이기 때문입니다.



$\mathbb{RP}^n$ 은 그저 ”경계로  $\mathbb{RP}^{n-1}$ 을 갖는  $\mathbb{R}^n$ (또는  $D^n$ )”이므로, 귀납적으로  $\mathbb{RP}^n$ 을 CW 복합체로 구성할 수 있습니다. 따라서  $\mathbb{RP}^n$ 은 각 차원마다 하나의 세포로 이루어짐에 유의하십시오.

**예제 64.6.3** (세포 복합체로서의  $\mathbb{RP}^n$ )

- $\mathbb{RP}^0$ 은 하나의 점입니다.
- $\mathbb{RP}^1 \cong S^1$ 은 원이며, CW 복합체로서는 0-세포 하나와 1-세포 하나로 이루어집니다.
- $\mathbb{RP}^2$ 는 2-세포 하나를 취하여 그 둘레를  $\mathbb{RP}^1$ 의 사본 주위로 두 번 감아서 만들 수 있습니다.



$\mathbb{CP}^n$ 은 각 짝수 차원마다 하나의 세포로 이루어집니다.

## §64.7 생각해 볼 만한 조금 더 어려운 문제

**문제 64A.** 공간  $X$ 가 하우스도르프 공간인 것과 대각선  $\{(x, x) \mid x \in X\}$ 가 곱공간  $X \times X$ 에서 닫힌집합인 것이 동치임을 보이십시오.

**문제 64B.** 다음 공간들을 CW 복합체로 구현하십시오:

- (a) 뫼비우스 띠(Möbius strip).
- (b)  $\mathbb{R}$ .
- (c)  $\mathbb{R}^n$ .

**문제 64C<sup>†</sup>.** 유한 CW 복합체가 콤팩트함을 보이십시오.

# 65 기본군

위상수학자는 커피잔과 도넛을 구별하지 못합니다. 그렇다면 무엇이든 어떻게 구별할 수 있겠습니까?

이는 답하기 매우 어려운 질문이지만, 이를 답하려 시도할 수 있는 한 가지 방법은 공간의 불변량을 찾는 것입니다. 군의 유비를 들자면, 예를 들어 두 군의 위수가 다르거나, 한쪽은 단순군이고 다른 쪽은 그렇지 않은 경우 등에는 두 군이 동형이 아님이 명백합니다. 우리는 위상 공간에 대해서도 이와 비슷한 성질을 찾아내어 실제로 공간들을 구별할 수 있기를 바랍니다.

공간  $X$ 에 대한 이러한 불변량 두 가지는 다음과 같습니다

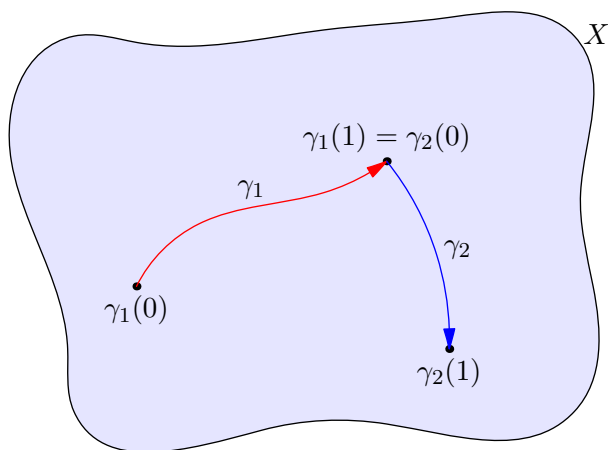
- 호몰로지 군  $H_1(X)$ ,  $H_2(X)$ , ... 정의하기
- 호모토피 군  $\pi_1(X)$ ,  $\pi_2(X)$ , ... 정의하기

호몰로지 군은 정의하기는 어렵지만 일반적으로 계산하기는 더 쉽습니다. 호모토피 군은 정의하기는 더 쉽지만 계산하기는 더 어렵습니다.

이 장은 기본군  $\pi_1$ 에 관한 것입니다.

## §65.1 경로를 융합하기

공간  $X$ 에서의 경로란 함수  $[0, 1] \rightarrow X$ 임을 상기하십시오.  $\gamma_1(1) = \gamma_2(0)$ 을 만족하는 경로  $\gamma_1$ 과  $\gamma_2$ 가 있다고 합시다. 우리는 이들을 융합<sup>1</sup>하여 경로  $\gamma_1 * \gamma_2$ 를 얻고자 합니다. 쉽지 않습니까?



안타깝지만 우리는 정의를 약간 편법적으로 손봐야 합니다. 이상적인 세계라면 경로  $\gamma_1: [0, 1] \rightarrow X$ 와  $\gamma_2: [1, 2] \rightarrow X$ 가 있을 때 이들을 그저 합쳐서  $\gamma_1 * \gamma_2: [0, 2] \rightarrow X$ 를 얻을 수 있을 것입니다. 하지만 여기서 이 “2”는 잘못되었습니다. 해법은 첫 번째 경로에는  $[0, \frac{1}{2}]$ 를, 두 번째 경로에는  $[\frac{1}{2}, 1]$ 을 할당하는 것입니다. 즉 “두 배 빠르게” 진행하는 것입니다.

<sup>1</sup>세상 사람들 거의 모두는 이러한 구성이나 다른 유형의 구성물을 기술할 때 “접합(gluing)”이라는 표현을 사용합니다. 하지만 저는 고등학교 시절 엘머 풀 때문에 트라우마가 생겼는데, 어리석은 “포스터 만들기” 과제가 싫었고 거기에 풀을 써야 하는 것도 싫었기 때문입니다. 그래서 저는 경로들을 “접합한다”고 말하기를 거부하고, 대신 어쨌든 더 멋지게 들리는 “융합한다”라는 표현을 쓰겠습니다.

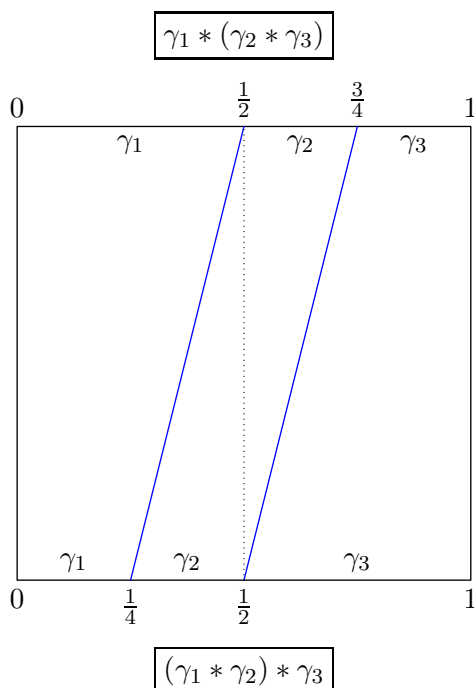
**정의 65.1.1.**  $\gamma_1(1) = \gamma_2(0)$ 을 만족하는 두 경로  $\gamma_1, \gamma_2: [0, 1] \rightarrow X$ 가 주어졌을 때, 경로  $\gamma_1 * \gamma_2: [0, 1] \rightarrow X$ 를 다음과 같이 정의합니다

$$(\gamma_1 * \gamma_2)(t) = \begin{cases} \gamma_1(2t) & 0 \leq t \leq \frac{1}{2} \\ \gamma_2(2t - 1) & \frac{1}{2} \leq t \leq 1. \end{cases}$$

안타깝게도 이 편법은 두 번째 단점을 드러냅니다. 바로 이 “곱”이 결합법칙을 만족하지 않는다는 것입니다. 적절한 경로들에 대해  $(\gamma_1 * \gamma_2) * \gamma_3$ 을 취하면,  $\gamma_1, \gamma_2, \gamma_3$ 에 할당되는 시간은 각각  $[0, \frac{1}{4}]$ ,  $[\frac{1}{4}, \frac{1}{2}]$ ,  $[\frac{1}{2}, 1]$ 입니다.

**질문 65.1.2.**  $\gamma_1 * (\gamma_2 * \gamma_3)$ 에 할당되는 시간은 무엇입니까?

하지만 이 연산이 결합법칙을 만족하지 않는다 해도, 그것이 결합법칙을 만족하지 못하는 이유는 다소 어이없다는 데 동의하시리라 생각합니다. 이는 그저 특정 구간에서 얼마나 빨리 진행하느냐의 문제일 뿐입니다.



따라서 경로들을 융합하는 한, 우리는  $[0, 1]$  자체를 너무 진지하게 받아들이고 싶지 않을 것입니다. 그래서 우리는 모든 것을 (경로) 호모토피 동치까지만 고려합니다. (두 경로  $\alpha$ 와  $\beta$  사이에 경로 호모토피  $F: [0, 1]^2 \rightarrow X$ , 즉  $\alpha$ 에서  $\beta$ 로 가는 연속적인 변형이 존재하면 두 경로는 호모토픽하다는 것을 상기하십시오.) 다음이 확실히 성립합니다

$$(\gamma_1 * \gamma_2) * \gamma_3 \simeq \gamma_1 * (\gamma_2 * \gamma_3).$$

또한  $\alpha_1 \simeq \alpha_2$ 이고  $\beta_1 \simeq \beta_2$ 이면  $\alpha_1 * \beta_1 \simeq \alpha_2 * \beta_2$ 라는 것도 성립합니다.

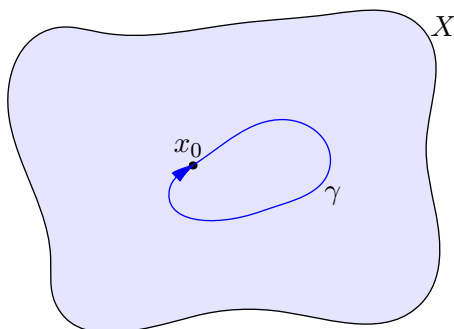
당연히 호모토피는 동치 관계이므로, 경로  $\gamma$ 는 어떤 “호모토피 타입”, 즉  $\simeq$  아래에서의 동치류에 속합니다. 이를  $[\gamma]$ 로 표기하겠습니다. 그러면  $[\alpha] * [\beta]$ 를 이야기하는 것이 의미가 있습니다. 따라서  $*$ 를 호모토피류에 대한 연산으로 생각할 수 있습니다.

## §65.2 기본군

**이 절의 대표적인 예:**  $\pi_1(\mathbb{R}^2)$ 는 자명하며  $\pi_1(S^1) \cong \mathbb{Z}$ 입니다.

이 시점에서 끝점을 계속 추적하는 것이 다소 성가시므로, 이제 특정한 유형의 경로로 논의를 한정하겠습니다.

**정의 65.2.1.** 루프란  $\gamma(0) = \gamma(1)$ 을 만족하는 경로입니다.



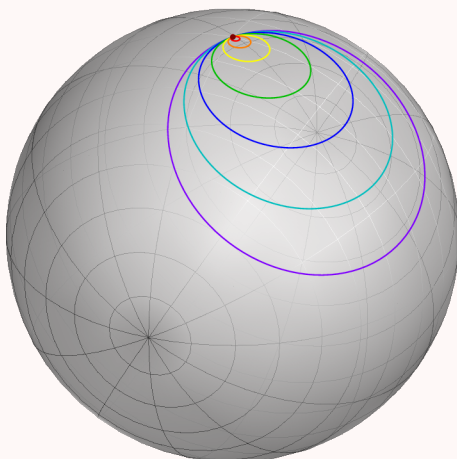
따라서 단일한 점  $x_0$ 에서 시작하는 경로들로 주의를 한정하면, 모든 것이  $x_0$ 에서 시작하고 끝나므로 더 이상 끝점과 시작점을 신경 쓸 필요가 없습니다. 우리에게는 심지어 매우 표준적인 루프도 있습니다. 바로 내내  $x_0$ 에 가만히 서 있는 것으로 주어지는 “아무것도 하지 않는” 루프<sup>2</sup>입니다.

**정의 65.2.2.** 자명한 “아무것도 하지 않는 루프”를 1로 표기하겠습니다. 루프  $\gamma$ 가 1과 호모토픽하면, 즉  $\gamma \simeq 1$ 이면 **널호모토픽**하다고 합니다.

고리(loop)의 호모토피에 대해서는, 고리를 “감아 들이는” 것을 상상하여 하나의 점으로 수축시키는 것으로 시각화할 수 있습니다.

**예제 65.2.3** ( $S^2$ 의 고리는 영호모토픽(nulhomotopic)입니다)

다음 그림이 여러분을 납득시켜 주겠지만, 단일 연결(simply connected) 공간  $S^2$ 의 모든 고리는 영호모토픽입니다.



(보라색 고리에서 시작하여, 적갈색 점으로 수축시킵니다.)

따라서 어떤 공간이 단일 연결임을 보이려면 그 공간의 고리들을 이해하는 것으로 충분합니다. 이제 다음을 제시할 준비가 되었습니다:

<sup>2</sup>똥보.

**정의 65.2.4.** 기점  $x_0$ 을 갖는  $X$ 의 **기본군**은  $\pi_1(X, x_0)$ 으로 표기하며, 호모토피 동치류들의 집합으로

$$\{[\gamma] \mid \gamma x_0 \text{에서의 루프}\}$$

$*$ 를 군 연산으로 갖춘 것입니다.

이것이 군 구조를 이룬다는 사실이 놀랍게 느껴질 수 있습니다. 예를 들어, 역원은 무엇 일까요? 지금 정의해 봅시다.

**정의 65.2.5.** 경로  $\alpha: [0, 1] \rightarrow X$ 가 주어졌을 때, 경로  $\bar{\alpha}$ 를 다음과 같이 정의할 수 있습니다

$$\bar{\alpha}(t) = \alpha(1 - t).$$

이는 실질적으로 " $\alpha$ 를 거꾸로 진행하는" 것입니다.  $\bar{\alpha}$ 는  $\alpha$ 의 끝점에서 시작하여  $\alpha$ 의 시작점에서 끝난다는 점에 유의하십시오.

**연습문제 65.2.6.** 임의의 경로  $\alpha$ 에 대해,  $\alpha * \bar{\alpha}$ 가  $\alpha(0)$ 에서의 "아무것도 하지 않는" 고리와 호모토픽함을 보이십시오. (그림을 그려 보십시오.)

확인해 봅시다.

이것이 군 구조임을 증명. 분명히  $*$ 는  $x_0$ 에서의 두 고리를 받아  $x_0$ 에서의 고리를 내놓습니다. 우리는 또한 이미  $*$ 가 결합적임을 보이는 데 시간을 들였습니다. 따라서 우리는 (i) 항등원이 존재하는지, (ii) 역원이 존재하는지만 확인하면 됩니다.

- 우리는 항등원이 앞서 설명한 "아무것도 하지 않는" 고리 1이라고 주장합니다. 독자는 임의의  $\gamma$ 에 대해 다음을 확인할 수 있습니다,

$$\gamma \simeq \gamma * 1 \simeq 1 * \gamma.$$

- 고리  $\gamma$ 에 대해, 그것의 "역방향" 고리  $\bar{\gamma}$ 를 다음과 같이 정의했음을 다시 상기하십시오

$$\bar{\gamma}(t) = \gamma(1 - t).$$

그러면  $\gamma * \bar{\gamma} = \bar{\gamma} * \gamma = 1$ 이 성립합니다.

따라서  $\pi_1(X, x_0)$ 은 실제로 군입니다. □

더 나아가기 전에 몇 가지 예시를 드는 것이 좋겠습니다.

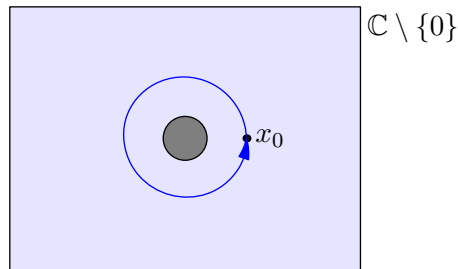
### 예제 65.2.7 (기본군의 예시들)

다음 결과들을 증명하는 것은 결코 자명하지 않다는 점에 유의하십시오. 지금은 그저 주장된 답이 "왜" 옳아야 하는지를 직관적으로 파악해 보십시오.

- $\mathbb{C}$ 의 기본군은 자명군입니다: 평면에서는 모든 고리가 영호모토픽입니다. (증명: 그것이 밧줄 한 조각이라고 상상하고 감아 들이는 것입니다.)
- 반면,  $\mathbb{C} \setminus \{0\}$  (앞서 나온 유성 예시)의 기본군은 어떤 기점을 택하더라도 실제로  $\mathbb{Z}$ 입니다! 이를 증명하기까지는 아직 시간이 걸리겠지만, 본질적으로 고리는 원점을 감는 횟수에 의해 결정되며 – 이를 소위 감김수(winding numbers)라 부릅니다. 한번 생각해 보십시오!
- 마찬가지로, 우리는 곧  $S^1$ (단위원)의 기본군이  $\mathbb{Z}$ 임을 보일 것입니다.

공식적으로는 기점이 무엇인지도 알려드려야 하지만, 이 예시들에서는 대칭성에 의해 그것이 중요하지 않습니다.

다음은 절 7.7의 유성처럼 구멍을 과장하여 나타낸  $\mathbb{C} \setminus \{0\}$ 의 그림입니다.



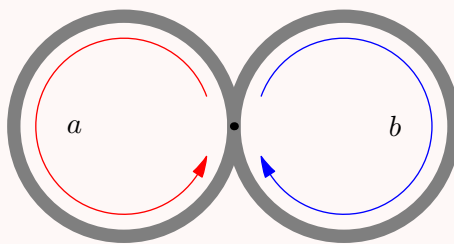
**질문 65.2.8.**  $S^1$ 의 기본군이  $\mathbb{Z}$ 임을 스스로 확인하고, 이를 왜 "감김수(winding numbers)"라고 부르는지 이해하십시오. (이는 이후 장들에서 기본군의 가장 중요한 예시가 될 것이므로, 지금 반드시 파악해 두는 것이 중요합니다.)

**예제 65.2.9 (8자 도형)**

8자 도형  $S^1 \vee S^1$ 을 생각하고,  $x_0$ 를 중심점이라 합시다. 그러면

$$\pi_1(S^1 \vee S^1, x_0) \cong \langle a, b \rangle$$

는 두 문자로 생성된 자유군입니다. 아이디어는 8자 도형의 한쪽 고리가  $a$ 이고 다른 쪽 고리가  $b$ 라는 것이며, 따라서 우리는  $\pi_1$ 이 이 고리들  $a$ 와  $b$ (그리고 그 역원  $\bar{a}$ 와  $\bar{b}$ )에 의해 생성되리라 기대합니다. 이 고리들은 서로 관계가 없습니다.



그래프 이론에서는 보통 그래프가 연결되어 있다고 가정한다는 것을 상기하십시오. 그렇지 않으면 각 연결 성분을 따로따로 고려하면 되기 때문입니다. 마찬가지로 우리는 일반적으로 경로 연결 공간에만 관심을 국한하고자 하는데, 이는 어떤 공간이 경로 연결되어 있지 않다면 여러 개의 "경로 연결 성분"으로 나뉠 수 있기 때문입니다. (이것을 어떻게 정의할지 짐작할 수 있습니까?) 실제로, 제 책상 위의 물건들로 이루어진 (책상 자체는 제외한) 공간  $X$ 를 상상해 볼 수 있습니다. 제 휴대폰의  $\pi_1$ 은 제 머그컵의  $\pi_1$ 과 아무 관계가 없습니다. 이들은 비유적으로도 문자 그대로도 완전히 비연결되어 있습니다.

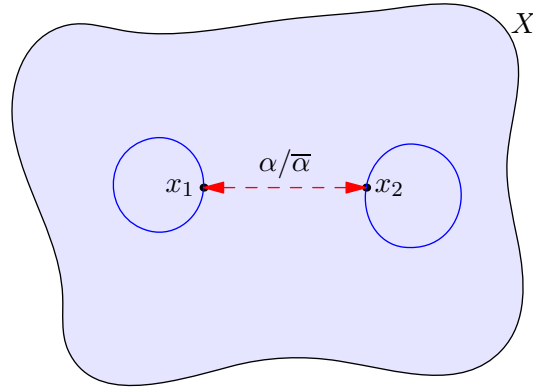
하지만 반대로, 경로 연결 공간에서는 이 군들이 서로 매우 밀접하게 관련되어 있다고 주장합니다!

**정리 65.2.10** (기본군은 기준점에 의존하지 않습니다)

$X$ 를 경로 연결 공간이라 합시다. 그러면 임의의  $x_1 \in X$ 와  $x_2 \in X$ 에 대해 다음이 성립합니다

$$\pi_1(X, x_1) \cong \pi_1(X, x_2).$$

증명을 읽기 전에, 아래 그림만 보고 이 동형사상을 짐작할 수 있는지 시도해 보십시오.



증명.  $\alpha$ 를  $x_1$ 에서  $x_2$ 로 가는 임의의 경로라 하고 (경로 연결성에 의해 가능합니다),  $\bar{\alpha}$ 를 그 역경로라 합시다. 그러면 다음과 같은 사상을 구성할 수 있습니다

$$\pi_1(X, x_1) \rightarrow \pi_1(X, x_2) \text{에 의해 } [\gamma] \mapsto [\bar{\alpha} * \gamma * \alpha].$$

다시 말해,  $x_1$ 에서의 고리  $\gamma$ 가 주어지면,  $x_2$ 에서 시작하여  $\bar{\alpha}$ 를 따라  $x_1$ 로 간 다음  $\gamma$ 를 실행하고, 이어서  $\alpha$ 를 따라 다시  $x_2$ 로 돌아올 수 있습니다. 따라서 이는  $\pi_1(X, x_1)$ 의 모든 고리로부터  $\pi_1(X, x_2)$ 의 고리를 만들어내는 사상입니다. 이것이 군의 준동형사상인 이유는 다음과 같습니다

$$(\bar{\alpha} * \gamma_1 * \alpha) * (\bar{\alpha} * \gamma_2 * \alpha) = \bar{\alpha} * \gamma_1 * \gamma_2 * \alpha$$

$\alpha * \bar{\alpha}$ 가 널호토폭이기 때문입니다.

마찬가지로, 다음과 같은 준동형사상도 존재합니다

$$\pi_1(X, x_2) \rightarrow \pi_1(X, x_1) \text{에 의해 } [\gamma] \mapsto [\alpha * \gamma * \bar{\alpha}].$$

이 두 사상이 서로의 역사상이므로, 이들은 동형사상이어야 함을 알 수 있습니다. 이것으로 끝입니다.  $\square$

이것이 우리가 보통 경로 연결 공간에만 관심을 두는 더 큰 이유입니다.

**표기의 남용 65.2.11.** 경로 연결 공간  $X$ 에 대해서는 어떤  $x_0 \in X$ 를 선택하든 상관없으므로, 흔히  $\pi_1(X, x_0)$ 를 그냥  $\pi_1(X)$ 로 줄여 쓰겠습니다.

마지막으로, 우리가 원래 "단순 연결(simply connected)"을 양 끝점이 같은 임의의 두 경로가 호토폭이라는 뜻으로 정의했음을 상기하십시오. 이 조건을 완화한 다음, 기본군을 이용해 다시 표현하는 것이 가능합니다.

**연습문제 65.2.12.**  $X$ 를 경로 연결 공간이라 합시다.  $X$ 가 **단순 연결**인 것과  $\pi_1(X)$ 가 자명군인 것이 동치임을 증명하십시오. (한쪽 방향은 쉽지만, 다른 쪽 방향은 조금 더 까다롭습니다.)

이것이 단순 연결의 "일반적인" 정의입니다.

### §65.3 기본군은 위상동형사상에 대해 불변입니다

논의를 정리하기 위해 도입할 간단한 표기법이 하나 있습니다

**정의 65.3.1.**  $f: (X, x_0) \rightarrow (Y, y_0)$ 라는 표기는,  $f: X \rightarrow Y$ 가 공간 사이의 연속함수이면서 동시에 점  $x_0$ 를  $y_0$ 로 보낸다는 것을 의미합니다.

$X$ 와  $Y$ 를 위상 공간이라 하고  $f: (X, x_0) \rightarrow (Y, y_0)$ 라 합시다. 이제 우리는  $X$ 와  $Y$ 의 기본군을 서로 연관 짓고자 합니다.

$(X, x_0)$ 에서의 고리  $\gamma$ 란  $\gamma(0) = \gamma(1) = x_0$ 를 만족하는 사상  $\gamma: [0, 1] \rightarrow X$ 임을 상기하십시오. 그러면 다음 합성을 생각해 보면

$$[0, 1] \xrightarrow{\gamma} (X, x_0) \xrightarrow{f} (Y, y_0)$$

바로  $y_0$ 에서의  $Y$ 의 고리를 얻게 됩니다! 이 고리를  $f_{\#}\gamma$ 라고 부르겠습니다.

#### 보조정리 65.3.2 ( $f_{\#}$ 는 호모토피 불변입니다)

$\gamma_1 \simeq \gamma_2$ 가 경로 호모토픽이라면, 실제로

$$f_{\#}\gamma_1 \simeq f_{\#}\gamma_2.$$

증명.  $\gamma_1$ 을  $\gamma_2$ 로 보내는 호모토피  $h$ 를 취하고  $f \circ h$ 를 생각해 보십시오. □

이 시점에서  $X$ 와  $Y$ 가 위상동형이면 그 기본군들이 모두 동형사상 관계에 있다는 점을 짚어줄 만합니다. 실제로  $f: X \rightarrow Y$ 와  $g: Y \rightarrow X$ 를 서로 역인 연속 사상이라 합시다. 그러면  $f_{\#}: \pi_1(X, x_0) \rightarrow \pi_1(Y, y_0)$ 와  $g_{\#}: \pi_1(Y, y_0) \rightarrow \pi_1(X, x_0)$ 가 두 군 사이의 서로 역인 사상임을 확인할 수 있습니다 (단,  $f(x_0) = y_0$ 이고  $g(y_0) = x_0$ 이라고 가정합니다).

### §65.4 고차 호모토피 군

기본군에 왜  $\pi_1$ 이라는 표기를 사용할까요? 그리고  $\pi_2, \dots$ 는 무엇일까요? 그 답은 다음과 같은 재서술에 있습니다:

**질문 65.4.1.** 고리가 연속 함수  $S^1 \rightarrow X$ 와 같은 것임을 스스로 확인해 보십시오.

경로가 아닌 다른 대상에 대해서도 호모토피를 정의할 수 있음이 밝혀졌습니다. 두 함수  $f, g: Y \rightarrow X$ 는  $f$ 를  $g$ 로 연속적으로 변형하는 연속 함수  $Y \times [0, 1] \rightarrow X$ 가 존재하면 **호모토픽**이라고 합니다. 따라서 위에서 했던 모든 것은 그저  $Y = S^1$ 인 특수한 경우였을 뿐입니다.

일반적인  $n$ 에 대해, 군  $\pi_n(X)$ 는 사상  $S^n \rightarrow X$ 의 호모토피 류들로 정의됩니다. 군의 연산은 좀 더 구체적으로 정하기 어렵습니다.  $S^n$ 이 몇몇 끝점들을 붙인  $[0, 1]^n$ 과 위상동형임을 보여야 합니다. 예를 들어  $S^1$ 은 0과 1을 붙인  $[0, 1]$ 입니다. 이러한 정육면체들을 갖추면, 한 면을 따라 서로 합칠 수 있습니다. (다시 말하지만, 저는 일부러 몹시 부정확하게 설명하고 있습니다.)

$n \neq 1$ 일 때,  $\pi_n$ 은  $\pi_1$ 과는 다소 다르게 행동합니다. ( $S^n$ 이  $n \geq 2$ 인 모든 경우에 단일 연결이지만  $n = 1$ 일 때는 그렇지 않으므로, 그리 놀랍지 않을 수도 있습니다.) 특히  $\pi_n(X)$ 는  $n \geq 2$ 인 모든 경우에 아벨 군임이 밝혀졌습니다.

몇 가지 예를 살펴봅시다.

**예제 65.4.2** ( $\pi_n(S^n) \cong \mathbb{Z}$ )

앞서 보았듯이  $\pi_1(S^1) \cong \mathbb{Z}$ 이며, 기준이 되는 원  $S^1$ 이 주어지면 두 번째 원을 그 주위에 원하는 만큼 여러 번 감을 수 있습니다. 일반적으로  $\pi_n(S^n) \cong \mathbb{Z}$ 임이 성립합니다.

**예제 65.4.3** ( $n < m$ 일 때  $\pi_n(S^m)$ 은 자명합니다)

$S^2$  안의 원은 그저 한 점으로 감아 들일 수 있으므로  $\pi_1(S^2) \cong \{1\}$ 임을 보았습니다. 마찬가지로 더 작은  $n$ 차원 구는 더 큰  $m$ 차원 구의 표면 위에서 감아 들일 수 있음이 밝혀졌습니다. 따라서 일반적으로  $n < m$ 일 때  $\pi_n(S^m)$ 은 자명합니다.

그러나 이러한 관찰을 넘어서면, 이 군들은 상당히 기이하게 행동합니다. 다음은  $1 \leq m \leq 8$ 이고  $2 \leq n \leq 10$ 인 범위에서  $\pi_n(S^m)$ 의 표이며, 이를 보면 제가 무엇을 말하는지 알 수 있을 것입니다. (위키백과에서 가져왔습니다.)

| $\pi_n(S^m)$ | 2            | 3            | 4                        | 5                        | 6                         | 7                                           | 8                            | 9                                                      | 10                                                      |
|--------------|--------------|--------------|--------------------------|--------------------------|---------------------------|---------------------------------------------|------------------------------|--------------------------------------------------------|---------------------------------------------------------|
| $m = 1$      | $\{1\}$      | $\{1\}$      | $\{1\}$                  | $\{1\}$                  | $\{1\}$                   | $\{1\}$                                     | $\{1\}$                      | $\{1\}$                                                | $\{1\}$                                                 |
| 2            | $\mathbb{Z}$ | $\mathbb{Z}$ | $\mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/12\mathbb{Z}$ | $\mathbb{Z}/2\mathbb{Z}$                    | $\mathbb{Z}/2\mathbb{Z}$     | $\mathbb{Z}/3\mathbb{Z}$                               | $\mathbb{Z}/15\mathbb{Z}$                               |
| 3            |              | $\mathbb{Z}$ | $\mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/12\mathbb{Z}$ | $\mathbb{Z}/2\mathbb{Z}$                    | $\mathbb{Z}/2\mathbb{Z}$     | $\mathbb{Z}/3\mathbb{Z}$                               | $\mathbb{Z}/15\mathbb{Z}$                               |
| 4            |              |              | $\mathbb{Z}$             | $\mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/2\mathbb{Z}$  | $\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ | $(\mathbb{Z}/2\mathbb{Z})^2$ | $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ | $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ |
| 5            |              |              |                          | $\mathbb{Z}$             | $\mathbb{Z}/2\mathbb{Z}$  | $\mathbb{Z}/2\mathbb{Z}$                    | $\mathbb{Z}/24\mathbb{Z}$    | $\mathbb{Z}/2\mathbb{Z}$                               | $\mathbb{Z}/2\mathbb{Z}$                                |
| 6            |              |              |                          |                          | $\mathbb{Z}$              | $\mathbb{Z}/2\mathbb{Z}$                    | $\mathbb{Z}/2\mathbb{Z}$     | $\mathbb{Z}/24\mathbb{Z}$                              | $\{1\}$                                                 |
| 7            |              |              |                          |                          |                           | $\mathbb{Z}$                                | $\mathbb{Z}/2\mathbb{Z}$     | $\mathbb{Z}/2\mathbb{Z}$                               | $\mathbb{Z}/24\mathbb{Z}$                               |
| 8            |              |              |                          |                          |                           |                                             | $\mathbb{Z}$                 | $\mathbb{Z}/2\mathbb{Z}$                               | $\mathbb{Z}/2\mathbb{Z}$                                |

실제로, 모든  $m$ 과  $n$ 에 대해  $\pi_n(S^m)$ 을 계산할 수 있다면, 사실상 어떠한 호모토피 류도 계산할 수 있음이 밝혀졌습니다. 따라서  $\pi_n(S^m)$ 을 계산하는 것은 일반적으로 일종의 가망 없는 일이며, 위 표에 나타난 혼돈과 패턴의 뒤섞임이 이를 증명하고 있습니다.

**§65.5 호모토피 동치인 공간**

**이 절의 대표적인 예:** 원판은 한 점과 호모토피 동치이고, 환형(*annulus*)은  $S^1$ 과 호모토피 동치입니다.

지금까지 저는 표기를 남용하여 두 경로에 대해 "경로 호모토피"를 그냥 "호모토피"라고 불러왔습니다. 유감스럽게도 앞으로도 계속 그렇게 할 것입니다 (따라서 제가 두 경로가 호모토픽이라고 말할 때는 언제나 "경로 호모토픽"을 의미한다고 가정하시기 바랍니다). 하지만 먼저 호모토피의 일반적인 정의가 무엇인지 말씀드리겠습니다.

**정의 65.5.1.**  $f, g: X \rightarrow Y$ 를 연속 함수라 합시다. **호모토피**란 연속 함수  $F: X \times [0, 1] \rightarrow Y$ 로서,  $s \in [0, 1]$ ,  $x \in X$ 에 대해  $F_s(x)$ 로 쓰며, 다음을 만족하는 것입니다

$$F_0(x) = f(x) \text{ 그리고 } F_1(x) = g(x) \text{ 모든 } x \in X \text{에 대해.}$$

이러한 함수가 존재하면,  $f$ 와  $g$ 는 **호모토픽**이라고 합니다.

직관적으로 이는 다시 한번 " $f$ 를  $g$ 로 변형하는 것"입니다. 이는 경로 호모토피와 거의 똑같은 정의임을 눈치채셨을 텐데, 다만  $f$ 와  $g$ 가 경로가 아니라 임의의 함수이며, 따라서 변형 과정에서 어떤 "끝점"을 고정해야 한다는 제약이 없다는 점이 다릅니다.

이 호모토피는 상당히 극적일 수 있습니다:

**예제 65.5.2**

영함수  $z \mapsto 0$ 과 항등함수  $z \mapsto z$ 는 함수  $\mathbb{C} \rightarrow \mathbb{C}$ 로서 호모토픽입니다. 필요한 변형은

$$[0, 1] \times \mathbb{C} \rightarrow \mathbb{C} \text{에 의해 } (s, z) \mapsto sz.$$

이것을 언급하는 이유는 다음을 정의하고 싶기 때문입니다:

**정의 65.5.3.**  $X$ 와  $Y$ 를 공간이라고 합시다. 다음을 만족하는 연속함수  $f: X \rightarrow Y$ 와  $g: Y \rightarrow X$ 가 존재하면, 이 둘은 **호모토피 동치**입니다.

- (i)  $f \circ g: Y \rightarrow Y$ 는  $Y$  위의 항등사상과 호모토픽하고,
- (ii)  $g \circ f: X \rightarrow X$ 는  $X$  위의 항등사상과 호모토픽합니다.

위상 공간이 한 점과 호모토피 동치이면, 그 공간을 **수축가능**하다고 합니다.

**질문 65.5.4.** 왜 동형인 두 공간은 호모토피 동치이기도 할까요?

직관적으로, 이것은 위상동형사상보다 더 관대한 형태의 늘이기와 구부리기라고 생각할 수 있습니다: 거대한 공간을 하나의 점으로 압축하는 것이 허용됩니다.

**예제 65.5.5** ( $\mathbb{C}$ 는 수축가능합니다)

위상 공간  $\mathbb{C}$ 와 단일 점  $\{0\}$ 으로 이루어진 공간을 생각해봅시다. 우리는 이 두 공간이 호모토피 동치라고 주장합니다 ( $f$ 와  $g$ 가 무엇인지 짐작할 수 있습니까?). 실제로 확인해야 할 두 가지는 다음과 같습니다.

- (i)  $z \mapsto 0 \mapsto 0$ 으로 정의되는  $\mathbb{C} \rightarrow \{0\} \hookrightarrow \mathbb{C}$ 는, 우리가 방금 본 바와 같이  $\mathbb{C}$  위의 항등사상과 호모토피 동치이고,
- (ii)  $0 \mapsto 0 \mapsto 0$ 으로 정의되는  $\{0\} \hookrightarrow \mathbb{C} \rightarrow \{0\}$ 는  $\{0\}$  위의 항등사상 그 자체입니다.

여기서  $\hookrightarrow$ 는 함수가 단순히 "포함사상"인 특수한 경우의  $\rightarrow$ 를 의미합니다.

**비고 65.5.6** —  $\mathbb{C}$ 는 한 점과 위상동형일 수 없는데, 그 이유는 두 집합 사이에 전단사가 존재하지 않기 때문입니다.

**예제 65.5.7** (뚫린 평면은  $S^1$ 과 호모토피 동치입니다)

위상 공간  $\mathbb{C} \setminus \{0\}$ , 즉 **뚫린 평면**과,  $\mathbb{C}$ 의 부분집합으로 간주되는 원  $S^1$ 을 생각해봅시다. 우리는 이 공간들이 실제로 호모토피 동치라고 주장합니다! 필요한 함수는 포함사상과

$$S^1 \hookrightarrow \mathbb{C} \setminus \{0\}$$

다음 함수입니다.

$$\mathbb{C} \setminus \{0\} \rightarrow S^1 \text{ 에 의해 } z \mapsto \frac{z}{|z|}.$$

이들이 요구되는 조건을 만족함을 확인할 수 있습니다.

**비고 65.5.8** — 반면에,  $\mathbb{C} \setminus \{0\}$ 는  $S^1$ 과 위상동형일 수 없습니다. 두 점을 제거하면  $S^1$ 을 비연결로 만들 수 있지만,  $\mathbb{C} \setminus \{0\}$ 에 대해서는 이것이 성립하지 않습니다.

**예제 65.5.9** (원판 = 점, 환형 = 원)

같은 이치로, 원판은 한 점과 호모토픽하며, 환형(annulus)은 원과 호모토픽합니다. (이것은 유한하기 때문에 시각화하기가 조금 더 쉬울 수 있습니다.)

이것을 언급하는 이유는 다음이 성립하기 때문입니다.

**대수적 위상수학은 호모토피 동치인 공간들을 구별할 수 없습니다.**

더 정확히 말하면,

**정리 65.5.10** (호모토피 동치인 공간들은 동형인 기본군을 갖습니다)

$X$ 와  $Y$ 를 경로연결이고 호모토피 동치인 공간이라고 합시다. 그러면 모든 양의 정수  $n$ 에 대해  $\pi_n(X) \cong \pi_n(Y)$ 입니다.

증명.  $\gamma: [0, 1]^n \rightarrow X$ 를 하나의  $S^n$ 이라 합시다.  $f: X \rightarrow Y$ 와  $g: Y \rightarrow X$ 를  $X$ 와  $Y$ 가 호모토피 동치임을 보이는 사상이라 합시다(즉  $f \circ g$ 와  $g \circ f$ 가 각각 항등사상과 호모토픽함을 의미합니다). 그러면 합성

$$[0, 1]^n \xrightarrow{\gamma} X \xrightarrow{f} Y$$

은  $Y$ 에서의  $S^n$ 이며, 따라서  $f$ 는 자연스러운 준동형사상  $\pi_n(X) \rightarrow \pi_n(Y)$ 를 유도합니다. 마찬가지로  $g$ 는 자연스러운 준동형사상  $\pi_n(Y) \rightarrow \pi_n(X)$ 를 유도합니다.  $f$ 와  $g$ 에 대한 조건은 이제 정확히 이 두 준동형사상이 서로 역사상임을 말하며, 이는 곧 이 사상들이 동형사상임을 의미합니다.  $\square$

특히,

**질문 65.5.11.** 수축 가능한 공간의 기본군은 무엇입니까?

이는 예를 들어 대수적 위상수학이  $\mathbb{R}^2$ 의 다음과 같은 호모토픽 부분공간들을 구별할 수 없다는 것을 의미합니다.



## §65.6 점을 가진 호모토피 범주

이 절은 기본적인 범주론을 아는 독자를 위해 쓰였습니다. 그렇지 않은 분들은 [장 67](#) and [68](#)를 읽은 후 돌아오시기 바랍니다. 아는 분들은 범주론적 개념을 이용해 이 장의 내용을 얼마나 간결하게 요약할 수 있는지 즐기실 수 있을 것입니다.

**정의 65.6.1. 점을 가진 호모토피 범주**  $\mathbf{hTop}_*$ 는 다음과 같이 정의됩니다.

- 대상: **점을 가진 공간**; 즉, 구별된 기점  $x_0$ 을 갖는 공간  $X$ 의 쌍  $(X, x_0)$ 이며,
- 사상: 연속함수  $(X, x_0) \rightarrow (Y, y_0)$ 의 호모토피류입니다.

특히, 경로 연결인 두 공간이 이 범주에서 동형사상 관계에 있는 것은 정확히 이들이 호모토피 동치일 때입니다. 그러면 앞서의 여러 결과를 다음과 같이 요약할 수 있습니다:

### 정리 65.6.2 (기본군의 함자적 해석)

다음과 같은 함자가 존재합니다

$$\pi_1: \mathbf{hTop}_* \rightarrow \mathbf{Grp}$$

다음과 같이 대응시키는

$$\begin{array}{ccc} (X, x_0) & \dashrightarrow & \pi_1(X, x_0) \\ f \downarrow & & \downarrow f_{\#} \\ (Y, y_0) & \dashrightarrow & \pi_1(Y, y_0) \end{array}$$

$\pi_1$ 이 각 점을 가진 위상 공간  $(X, x_0)$ 에 어떤 군  $\pi_1(X, x_0)$ 을 단순히 대응시키는 것이 아니라 하나의 함자라는 사실은 자동적으로 여러 좋은 성질들을 함의합니다. 예를 들면:

- 이 함자는  $f_{\#}$ 의 정보를, 그것이 합성을 보존한다는 사실을 포함하여 하나로 묶습니다. 범주론적 언어로 말하면,  $f_{\#}$ 는  $\pi_1(f)$ 입니다.
- 호모토픽인 공간들은 동형인 기본군을 갖습니다(이는 두 공간이  $\mathbf{hTop}$ 에서 동형사상 관계에 있고, 정리 68.2.8에 의해 함자가 동형사상을 보존하기 때문입니다). 실제로 정리 68.2.8과 정리 65.5.10의 증명이 은밀히 서로 동일함을 알아차리실 수 있을 것입니다.
- 사상  $f, g: (X, x_0) \rightarrow (Y, y_0)$ 가 호모토픽하다면,  $f_{\#} = g_{\#}$ 입니다. 이는 기본적으로 보조정리 65.3.2입니다.

**비고 65.6.3** — 사실,  $\pi_1(X, x_0)$ 는  $\mathbf{hTop}_*$ 에서의 화살표  $(S^1, 1) \rightarrow (X, x_0)$ 의 집합이므로, 이는 실제로 대상이  $\mathbf{Set}$  대신  $\mathbf{Grp}$ 인 것을 제외하면 공변 요네다 함자(예제 68.2.6)입니다.

## §65.7 생각해 볼 만한 조금 더 어려운 문제

**문제 65A** (조화 부채꼴). 경로 연결이지만, 점  $p$ 를 찾을 수 있어서  $r < 1$ 인  $p$ 의 임의의  $r$ -근방이 경로 연결이 아니게 되는, 거리 공간  $\mathbb{R}^2$ 의 부분공간  $X$ 를 제시하십시오.



**문제 65B<sup>†</sup>** (자이페르트-반 캄펀의 특수한 경우).  $X$ 를 위상 공간이라 합시다.  $U$ 와  $V$ 가  $X$ 의 연결된 열린집합이고,  $X = U \cup V$ 이며,  $U \cap V$ 가 공집합이 아니고 경로 연결이라고 가정합니다.

$\pi_1(U) = \pi_1(V) = \{1\}$ 이면  $\pi_1(X) = \{1\}$ 임을 증명하십시오.

**비고 65.7.1** — Seifert–van Kampen 정리는  $\pi_1(U)$ 와  $\pi_1(V)$ 가 임의의 군인 경우로 이를 일반화하며,  $\pi_1(U)$ ,  $\pi_1(V)$ ,  $\pi_1(U \cap V)$ 를 이용하여  $\pi_1(X)$ 를 계산하는 공식을 제공합니다. 증명은 거의 동일합니다.

안타깝게도 이는  $\pi_1(S^1)$ 를 계산하는 방법을 제공하지 않는데,  $U \cap V$ 가 연결되도록  $S^1 = U \cup V$ 로 쓰는 것이 불가능하기 때문입니다.



**문제 65C** (RMM 2013).  $n \geq 2$ 인 양의 정수  $n$ 이 주어졌습니다. 정  $2n$ 각형의 각 꼭짓점에 돌이 하나씩 놓여 있습니다. 한 번의 이동은  $2n$ 각형의 변 하나를 선택하여 그 변의 양 끝점에 있는 두 돌을 서로 바꾸는 것으로 이루어집니다. 일련의 이동이 모든 돌의 쌍을 정확히 한 번씩 서로 바꾼다면, 어떤 이동에서도 사용되지 않는 변이 존재함을 증명하십시오. (이 문제는 엄밀히 말해 이 장과는 아무 관련이 없지만, 풀이를 이끄는 “직관”은 매우 유사합니다.)

**문제 65D.** 못 두 개와 끈 하나로, 어느 못을 제거하더라도 액자가 떨어지도록 벽에 액자를 거는 방법은 무엇입니까?

풀이. <https://aamathematics.wordpress.com/2020/05/29/hanging-pictures-with-homotopy/>에 이 문제를 접하게 된 글이 있습니다. □

# 66 피복 사영

몇 챕터 전에 기본군이 무엇인지 이야기했지만, 단순 연결 공간이라는 가장 자명한 경우를 제외하고는 실제로 그것들을 계산하는 방법을 보여주지 않았습니다. 이 장에서는 피복 사영이라는 개념을 소개할 것인데, 이를 통해 이러한 군들 중 일부를 어떻게 찾을 수 있는지 알 수 있게 될 것입니다.

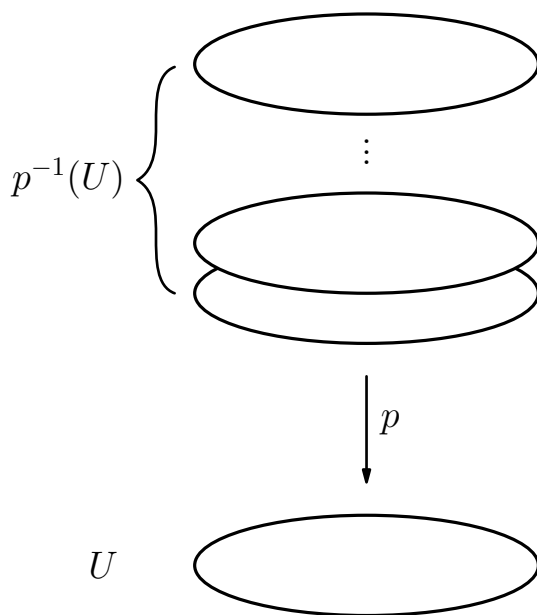
## §66.1 균등 피복과 피복 사영

**이 절의 대표적인 예:**  $\mathbb{R}$ 은  $S^1$ 을 덮습니다.

이제 우리가 원하는 것은, 큰 공간  $E$ , 즉 "피복 공간"을 밑공간  $B$  위로 좋은 방식으로 사영할 수 있게 하는 개념입니다. 여기 그 "좋은"의 개념이 있습니다.

**정의 66.1.1.**  $p: E \rightarrow B$ 를 연속 함수라 합시다.  $U$ 를  $B$ 의 열린집합이라 합시다.  $p^{-1}(U)$ 가  $E$ 의 열린집합들의 서로소 합집합(무한할 수도 있음)이고, 이들 중 어느 것에 제한해도  $p$ 가 위상동형사상이 될 때,  $U$ 를  $p$ 에 의해 **균등하게 피복된다**고 부릅니다.

그림:



우리가 말하고자 하는 것은 단지,  $U$ 의 원상이 그것의 사본들의 모음이면  $U$ 가 균등하게 피복된다는 것입니다. (사실 조금 더 있습니다: 각 팬케이크가  $U$ 와 위상동형이어야 할 뿐만 아니라,  $p$ 가 바로 그 위상동형사상이어야 한다는 것도 요구합니다.)

**정의 66.1.2. 피복 사영**  $p: E \rightarrow B$ 란,  $B$ 의 모든 밑점  $b \in B$ 가  $p$ 에 의해 균등하게 피복되는 열린 근방  $U \ni b$ 를 가지는 전사인 연속 사상을 말합니다.

**연습문제 66.1.3** ( $p$ 의 전사성을 요구하는 것에 대하여).  $p: E \rightarrow B$ 가 이 정의를 만족시키되,  $p$ 가 전사일 필요는 없다고 합시다.  $p$ 의 상이  $B$ 의 연결 성분들의 서로소 합집합임을 보이십시오. 따라서  $B$ 가 연결이고  $E$ 가 공집합이 아니면,  $p: E \rightarrow B$ 는 이미 전사입니다. 이런 이유로 일부 저자들은 보통  $B$ 가 경로 연결이라는 이유로 전사성 가정을 생략합니다.

여기 피복 사영의 가장 시시한 예가 있습니다.

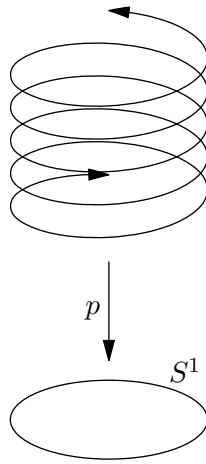
**예제 66.1.4 (항진적 피복 사영)**

임의의 공간  $B$ 의 서로소인  $n$ 개의 사본을 취해봅시다: 형식적으로,  $\{1, \dots, n\}$ 에 이산 위상을 준  $E = B \times \{1, \dots, n\}$ 입니다. 그러면  $(x, m) \mapsto x$ 에 의한 항진적 피복 사영  $E \rightarrow B$ 가 존재합니다; 우리는 그저  $n$ 개의 사본 전부를 사영하는 것입니다. 이것이 피복 사영인 이유는  $B$ 의 모든 열린집합이 균등하게 피복되기 때문입니다.

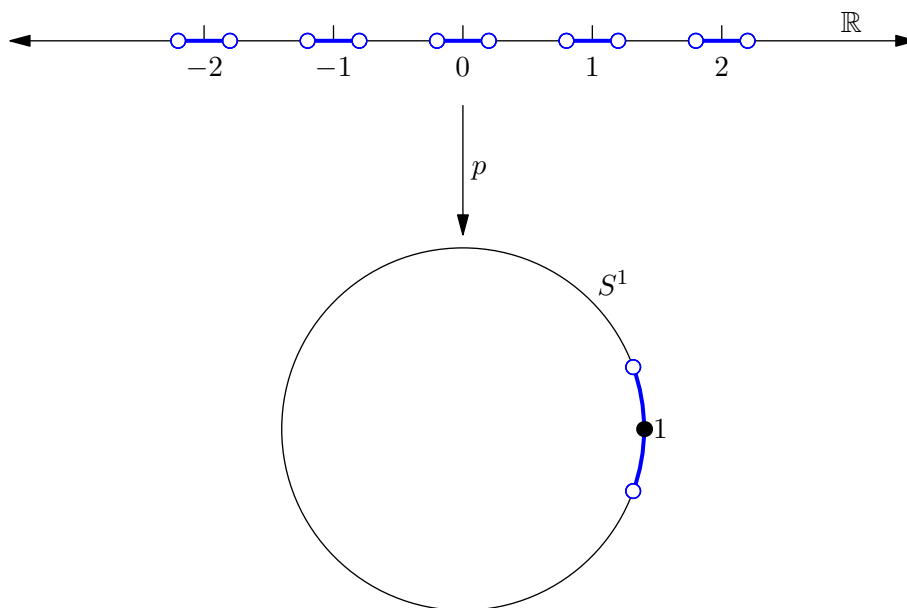
이것은  $B \times [n]$ 이 경로 연결이 아니기 때문에 그다지 흥미롭지는 않습니다. 훨씬 더 흥미로운 예는  $\mathbb{R}$ 과  $S^1$ 의 경우입니다.

**예제 66.1.5 ( $S^1$ 의 피복 사영)**

$\theta \mapsto e^{2\pi i \theta}$ 에 의한  $p: \mathbb{R} \rightarrow S^1$ 을 취합시다. 이것은 본질적으로 실수선을 하나의 나선으로 감아서 아래로 사영하는 것입니다.



우리는 이것이 피복 사영이라고 주장합니다. 실제로, 점  $1 \in S^1$ 을 생각해봅시다(여기서  $S^1$ 을 복소평면 안의 단위원으로 봅니다). 그것의 원상이  $\mathbb{R}$  안의 사본들의 모음이 되는 작은 열린 근방을 그릴 수 있습니다.



이번에는 모든 열린 근방이 통하지는 않는다는 점에 유의하십시오: 특히  $U = S^1$ 은 통하지 않는데, 그 이유는 원상이  $S^1$ 과 위상동형이 아닌  $\mathbb{R}$  전체가 되기 때문입니다.

**예제 66.1.6** ( $S^1$  자기 자신에 의한 피복)

$z \mapsto z^3$ 에 의한 사상  $S^1 \rightarrow S^1$  또한 피복 사영입니다. 그 이유를 알겠습니까?

**예제 66.1.7** ( $\mathbb{C} \setminus \{0\}$ 의 피복 사영)

복소수 연산에 익숙한 분들을 위해,

(a) 지수 사상  $\exp: \mathbb{C} \rightarrow \mathbb{C} \setminus \{0\}$ 은 피복 사영입니다.

(b) 각  $n$ 에 대해,  $n$ 거듭제곱 사상  $z \mapsto z^n: \mathbb{C} \setminus \{0\} \rightarrow \mathbb{C} \setminus \{0\}$ 은 피복 사영입니다.

## §66.2 올림 정리

이 절의 대표적인 예:  $\mathbb{R}$ 는  $S^1$ 을 피복합니다.

이제 핵심 아이디어는 이렇습니다:  $B$ 에서의 루프를  $\mathbb{R}$ 에서의 경로로 해석해보려 합니다. 이는 종종 훨씬 더 간단합니다. 예를 들어, 우리는  $S^1$ 의 기본군을 어떻게 계산해야 할지 전혀 몰랐지만,  $\mathbb{R}$ 의 기본군은 그저 자명군입니다. 따라서  $S^1$ 에서의 루프를  $\mathbb{R}$ 에서의 경로로 해석할 수 있다면, 그것은 (그리고 실제로 그렇습니다!)  $\pi_1(S^1)$ 의 계산을 다루기 쉽게 만들어 줄지도 모릅니다.

**정의 66.2.1.**  $\gamma: [0, 1] \rightarrow B$ 를 경로라 하고  $p: E \rightarrow B$ 를 피복 사영이라 하겠습니다.  $\gamma$ 의 **올림**이란  $p \circ \tilde{\gamma} = \gamma$ 를 만족하는 경로  $\tilde{\gamma}: [0, 1] \rightarrow E$ 입니다.

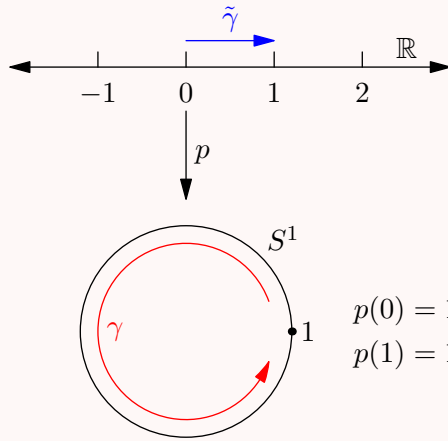
그림:

$$\begin{array}{ccc} & & E \\ & \nearrow \tilde{\gamma} & \downarrow p \\ [0, 1] & \xrightarrow{\gamma} & B \end{array}$$

**예제 66.2.2** (올림의 전형적인 예)

$\theta \mapsto e^{2\pi i \theta}$ 로 주어지는  $p: \mathbb{R} \rightarrow S^1 \subseteq \mathbb{C}$ 를 생각합시다 (여기서  $S^1$ 은 다시 단위원으로 간주됩니다).  $1 \in \mathbb{C}$ 에서 시작하여  $S^1$ 을 반시계 방향으로 한 바퀴 돌아 다시 1에서 끝나는  $S^1$ 에서의 경로  $\gamma$ 를 생각합시다. 기호로 쓰면,  $t \mapsto e^{2\pi i t}$ 로 주어지는  $\gamma: [0, 1] \rightarrow S^1$ 입니다.

그러면 하나의 올림  $\tilde{\gamma}$ 는 0에서 1로 가는 경로입니다. 사실, 임의의 정수  $n$ 에 대해,  $n$ 에서  $n+1$ 로 가는 것도 성립합니다.



마찬가지로,  $1 \in S^1$ 에서  $-1 \in S^1$ 로 가는 반시계 방향 경로도 올림을 가집니다: 어떤 정수  $n$ 에 대해,  $n$ 에서  $n + \frac{1}{2}$ 로 가는 경로입니다.

위는 올림의 주요한 예입니다. 다음과 같은 구조가 있는 것으로 보입니다:  $b_0$ 에서 시작하는  $B$ 에서의 경로  $\gamma$ 가 주어지면, 우리는 섬유  $p^{-1}(b_0)$ 의 임의의 점에서 시작합니다. (우리의 전형적인 예에서는  $B = S^1$ ,  $b_0 = 1 \in \mathbb{C}$ 이며, 이것이 바로 임의의 정수  $n$ 에서 시작하는 이유입니다.) 그다음에는 그저  $B$ 에서의 경로를 따라가기만 하면,  $E$ 에서의 대응하는 경로를 얻게 됩니다.

**질문 66.2.3.**  $\gamma(0) = 1 \in \mathbb{C}$ 인  $S^1$ 에서의 경로  $\gamma$ 를 생각합시다. 정수  $n \in \mathbb{R}$ 을 하나 선택하면,  $n$ 에서 시작하는 올림이 정확히 하나 존재함을 스스로 확인해보십시오.

이는 더 일반적으로도 성립함이 밝혀집니다.

#### 정리 66.2.4 (경로의 올림)

$\gamma: [0, 1] \rightarrow B$ 가  $\gamma(0) = b_0$ 인 경로이고,  $p: (E, e_0) \rightarrow (B, b_0)$ 가 피복 사영이라 합시다. 그러면  $\tilde{\gamma}(0) = e_0$ 를 만족하는 유일한 올림  $\tilde{\gamma}: [0, 1] \rightarrow E$ 가 존재합니다.

**증명.** 각 점  $b \in B$ 에 대해,  $B$ 에서 균등하게 피복된 열린 근방  $U_b$ 를 생각합시다. 그러면 열린집합들의 족

$$\{\gamma^{\text{pre}}(U_b) \mid b \in B\}$$

은  $[0, 1]$ 의 열린 덮개입니다.  $[0, 1]$ 이 콤팩트하므로 유한 부분덮개를 취할 수 있습니다. 따라서  $[0, 1]$ 을 내부가 서로소인 유한 개의 닫힌구간  $[0, 1] = I_1 \sqcup I_2 \sqcup \cdots \sqcup I_N$ 으로 그 순서대로 잘게 나눌 수 있으며, 이때 모든  $I_k$ 에 대해  $\gamma^{\text{img}}(I_k)$ 는 어떤  $U_b$ 에 포함됩니다.

이제  $I_1$ 부터 시작하여 구간별로  $\tilde{\gamma}$ 를 구성하겠습니다. 처음에, 로봇을  $e_0 \in E$ 에 놓고 쥐를  $b_0 \in B$ 에 놓습니다. 각 구간  $I_k$ 에 대해, 쥐는  $\gamma$ 가  $I_k$  위에서 행동하는 대로 움직입니다. 그런데 그 내내 쥐는 어떤 균등하게 피복된  $U_k$  안에 있습니다;  $p$ 가 피복 사영이라는 사실은  $E$  안에  $U_k$ 의 사본이 여러 개 존재함을 말해줍니다. 그중 정확히 하나, 이를  $V_k$ 라 하면, 우리 로봇을 포함합니다. 따라서 로봇은  $I_k$ 의 끝에 도달할 때까지 그저 쥐를 그대로 따라 하기만 합니다. 그러면 쥐는 어떤 새로운 균등하게 피복된  $U_{k+1}$  안에 있게 되고, 이 과정을 반복할 수 있습니다.  $\square$

이 정리는 다음 도식으로 일반화될 수 있습니다

$$\begin{array}{ccc}
 & & (E, e_0) \\
 & \nearrow \tilde{f} & \downarrow p \\
 (Y, y_0) & \xrightarrow{f} & (B, b_0)
 \end{array}$$

여기서  $Y$ 는 충분히 좋은 공간이며, 다음과 같습니다.

**정의 66.2.5.** 공간  $Y$ 가 **국소적으로 경로 연결**이라는 것은, 임의의 점  $x \in Y$ 에서  $x$ 의 모든 열린 근방  $U$ 가 경로 연결인 열린 근방  $V \subseteq U$ 를 포함한다는 뜻입니다.

#### 정리 66.2.6 (일반적인 올림 판정법)

$p: (E, e_0) \rightarrow (B, b_0)$ 를 피복 사영이라 합시다.  $Y$ 가 경로 연결이고 국소적으로 경로 연결인 공간이면, 임의의 연속 함수  $f: (Y, y_0) \rightarrow (B, b_0)$ 에 대해,  $\tilde{f}(y_0) = e_0$ 인 올림  $\tilde{f}$ 가 존재할 필요충분조건은

$$f_{\#}^{\text{img}}(\pi_1(Y, y_0)) \subseteq p_{\#}^{\text{img}}(\pi_1(E, e_0)),$$

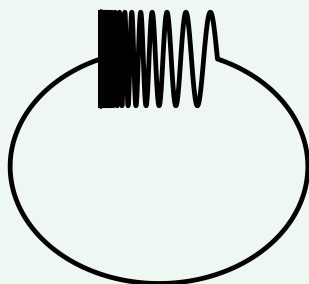
즉,  $f$ 에 의한  $\pi_1(Y, y_0)$ 의 상이  $p$ 에 의한  $\pi_1(E, e_0)$ 의 상에 포함된다는 것입니다 (둘 다  $\pi_1(B, b_0)$ 의 부분군으로 간주합니다). 이 올림이 존재하면, 그것은 유일합니다.

$p_{\#}$ 가 단사 사상이므로, 실제로  $p_{\#}^{\text{img}}(\pi_1(E, e_0)) \cong \pi_1(E, e_0)$ 가 성립합니다. 하지만 이 경우 우리가 관심 있는 것은 군의 동형사상류만이 아니라 실제 원소들입니다.

**질문 66.2.7.**  $Y = [0, 1]$ 로 놓으면 어떻게 될까요?

**비고 66.2.8 (호모토피 들어올리기)** — 여기 또 다른 흥미로운 특수한 경우가 있습니다: 호모토피는 연속함수  $[0, 1] \times [0, 1] \rightarrow X$ 로 부호화될 수 있음을 기억하십시오. 그런데  $[0, 1] \times [0, 1]$  또한 단순 연결입니다. 따라서 밀공간  $B$ 에서의 호모토피  $\gamma_1 \simeq \gamma_2$ 가 주어지면, 이를 들어올려  $E$ 에서의 호모토피  $\tilde{\gamma}_1 \simeq \tilde{\gamma}_2$ 를 얻을 수 있습니다.

**비고 66.2.9 (국소 경로 연결 조건은 실제로 필요합니다)** —  $Y$ 를 바르샤바 원이라 하고, 아래에 그려진 것처럼  $0 < x < 1/\pi$ 에 대한  $y = \sin(1/x)$ 의 그래프, 선분  $\{0\} \times [-1, 1]$ , 그리고 모든 것을 닫아 주는 곡선으로 구성된다고 하겠습니다.



공간  $Y$ 는 단순 연결이므로 들어올리기 판정 기준이 자명하게 만족되지만, 사인 곡선을 수직으로 붕괴시키는 함수  $f: Y \rightarrow S^1$ 은 함수  $\tilde{f}: Y \rightarrow \mathbb{R}$ 로 들어 올려지지 않습니다. 여기서 들어올리기 정리가 적용되지 않는 이유는,  $Y$ 가 원점에서 국소 경로 연결이 아니기 때문입니다.

이 결과의 또 다른 좋은 응용은 **장 33**입니다.

### §66.3 들어올리기 대응

**이 절의 대표적인 예:**  $(\mathbb{R}, 0)$ 은  $(S^1, 1)$ 을 피복합니다.

기본군을 계산하는 작업으로 돌아갑시다. 피복 사영  $p: (E, e_0) \rightarrow (B, b_0)$ 을 생각하십시오.

$B$ 에서의 고리  $\gamma$ 는  $e_0$ 에서 시작하여 섬유  $p^{\text{pre}}(b_0)$  안의 어떤 점  $e$ 에서 끝나는  $E$ 에서의  $\tilde{\gamma}$ 로 유일하게 들어올려질 수 있습니다.  $\gamma$ 와 호모토픽한 다른 경로  $\gamma'$ 를 택하더라도 이  $e \in E$ 가 바뀌지 않음을 쉽게 확인할 수 있습니다.

**질문 66.3.1.** **예제 66.2.2**의 그림을 보십시오.

손가락 하나는  $1 \in S^1$ 에, 다른 손가락 하나는  $0 \in \mathbb{R}$ 에 놓으십시오.  $S^1$ 에서  $\gamma$ 와 호모토픽한 고리를 따라가되(즉, 앞뒤로 갈 수는 있지만 정확히 한 바퀴 반시계 방향으로 끝나야 합니다), 다른 손가락으로는  $\mathbb{R}$ 에서 이를 따라가십시오.

반드시 점  $1 \in \mathbb{R}$ 에서 끝나야 함을 스스로 확인해 보십시오.

따라서  $b_0$ 에서의 고리의 모든 호모토피류(즉,  $\pi_1(B, b_0)$ 의 한 원소)는  $b_0$ 의 섬유 안의 어떤  $e$ 와 연관될 수 있습니다. 아래의 명제는 이것과 그 이상을 정리한 것입니다.

#### 명제 66.3.2

$p: (E, e_0) \rightarrow (B, b_0)$ 을 피복 사영이라 하겠습니다. 그러면 우리는 다음과 같은 집합 사이의 함수를 갖습니다

$$\Phi: \pi_1(B, b_0) \rightarrow p^{\text{pre}}(b_0)$$

$[\gamma] \mapsto \tilde{\gamma}(1)$ 로 정의되며, 여기서  $\tilde{\gamma}$ 는  $e_0$ 에서 시작하는 유일한 들어올림입니다. 더 나아가,

- $E$ 가 경로 연결이면,  $\Phi$ 는 전사 함수입니다.
- $E$ 가 단순 연결이면,  $\Phi$ 는 단사 사상입니다.

**질문 66.3.3.**  $E$ 가 경로 연결이면  $\Phi$ 가 전사 함수임을 증명하십시오. (이것은 정말이지 어이없을 정도로 쉽습니다.)

**증명.** 명제를 증명하기 위해,  $E$ 가 단순 연결이면  $\Phi$ 가 단사 사상을 보이는 것을 제외하고는 모든 것을 마쳤습니다. 이를 위해  $\gamma_1$ 과  $\gamma_2$ 가  $\Phi([\gamma_1]) = \Phi([\gamma_2])$ 를 만족하는 고리라고 가정하십시오.

들어올리기를 적용하면, 둘 다 어떤 점  $e_0 \in E$ 에서 시작하여 어떤 점  $e_1 \in E$ 에서 끝나는 경로  $\tilde{\gamma}_1$ 과  $\tilde{\gamma}_2$ 를 얻습니다.  $E$ 가 단순 연결이므로 이는 둘이 호모토픽하다는 것을 의미하며, 이들을 결합하는 호모토피  $F: [0, 1] \times [0, 1] \rightarrow E$ 를 쓸 수 있습니다. 그러면 이제 다음 사상들의 합성을 생각해 보십시오

$$[0, 1] \times [0, 1] \xrightarrow{F} E \xrightarrow{p} B.$$

$p \circ F$ 가  $\gamma_1$ 에서  $\gamma_2$ 로 가는 호모토피임을 확인할 수 있습니다. 따라서  $[\gamma_1] = [\gamma_2]$ 이며, 증명이 끝났습니다.  $\square$

이는 다음을 동기로 합니다:

**정의 66.3.4.** 공간  $B$ 의 **보편 피복**(universal cover)이란  $E$ 가 단순 연결(특히 경로 연결)인 피복 사영  $p: E \rightarrow B$ 를 말합니다.

**표기의 남용 66.3.5.**  $p$ 가 문맥상 명확할 때는 때때로 그냥  $E$ 가  $B$ 의 보편 피복이라고 말합니다.

### 예제 66.3.6 ( $S^1$ 의 기본군)

우리의 표준적인  $p: \mathbb{R} \rightarrow S^1$ 로 돌아가 봅시다.  $\mathbb{R}$ 이 단순 연결이므로, 이는  $S^1$ 의 보편 피복입니다. 그리고 실제로,  $S^1$ 의 임의의 점의 올(fiber)은 정수의 복사본이며, 이는  $S^1$ 에서의 루프들과 자연스럽게 전단사 관계에 있습니다.

다음의 전단사가

$$\Phi: \pi_1(S^1) \leftrightarrow \mathbb{Z}$$

$\mathbb{Z}$ 에 그 덧셈 군 구조를 부여하면 실제로 군 준동형사상임을 보일 수 있습니다(직관적으로도 명백합니다). 이것이 전단사이므로, 이로부터  $\pi_1(S^1) \cong \mathbb{Z}$ 라는 결론을 얻습니다.

## §66.4 정칙 피복(Regular coverings)

**이 절의 대표적인 예:**  $\mathbb{R} \rightarrow S^1$ 은  $n \cdot x = n + x$ 로부터 나옵니다

피복을 만들어내는 또 다른 방법이 있습니다.  $X$ 를 위상 공간이라 하고  $G$ 를 그 점들에 작용하는 군이라 합시다. 그러면 각  $g$ 에 대해, 다음에 의해 사상  $X \rightarrow X$ 를 얻습니다

$$x \mapsto g \cdot x.$$

우리는 이 사상이 모든  $g \in G$ 에 대해 연속<sup>1</sup>이고,  $X$ 의 각 점의 안정자군(stabilizer)이 자명하다고 요구합니다. 그러면 이 작용의 같은 궤도에 속하는 점들을 융합하여 정의되는 몫공간  $X/G$ 를 생각할 수 있습니다. 따라서  $X/G$ 의 점들은 이 작용의 궤도들과 동일시됩니다. 그러면 우리는 자연스러운 "사영"을 얻습니다

$$X \rightarrow X/G$$

각 점을 그것이 속한 궤도로 그저 보냄으로써 말입니다.

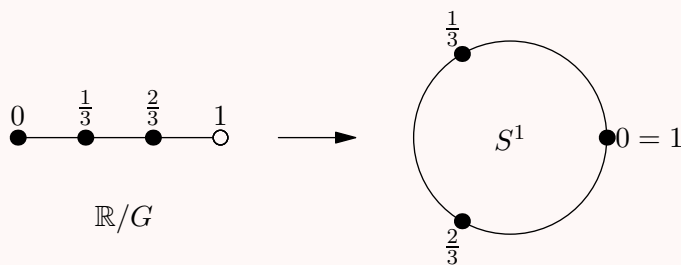
**정의 66.4.1.** 이러한 사영을 **정칙**(regular)이라 부릅니다. (끔찍한 용어지만, 어쩔 수 없습니다.)

### 예제 66.4.2 ( $\mathbb{R} \rightarrow S^1$ 은 정칙입니다)

$G = \mathbb{Z}$ ,  $X = \mathbb{R}$ 이라 하고,  $G$ 의  $X$ 에 대한 군 작용을 다음과 같이 정의합시다

$$n \cdot x = n + x$$

그러면  $X/G$ 를 "1을 법으로 한 실수"라고 생각할 수 있으며,  $[0, 1)$ 이 완전한 대표원 집합이고  $0 \sim 1$ 입니다.



<sup>1</sup>이를 달리 표현하면: 작용을 사상  $G \times X \rightarrow X$ 로 해석했을 때, 이것이 연속이어야 하며, 여기서 왼쪽의  $G$ 는 이산 위상을 갖는 집합으로 해석됩니다.

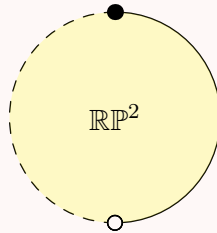
따라서 우리는  $X/G$ 를  $S^1$ 과 동일시할 수 있으며, 이에 연관된 정칙 사영은 바로 우리에게 익숙한  $\exp: \theta \mapsto e^{2i\pi\theta}$ 입니다.

#### 예제 66.4.3 (원환면(The torus))

$G = \mathbb{Z} \times \mathbb{Z}$ 이고  $X = \mathbb{R}^2$ 이라 하고,  $G$ 의  $X$ 에 대한 군 작용을  $(m, n) \cdot (x, y) = (m + x, n + y)$ 로 정의합시다.  $[0, 1)^2$ 이 완전한 대표원 집합이므로, 이를 변들이 동일시된 단위 정사각형으로 생각할 수 있습니다. 우리는 원환면  $S^1 \times S^1$ 과 피복 사영  $\mathbb{R}^2 \rightarrow S^1 \times S^1$ 을 얻습니다.

#### 예제 66.4.4 ( $\mathbb{RP}^2$ )

$G = \mathbb{Z}/2\mathbb{Z} = \langle T \mid T^2 = 1 \rangle$ 이라 하고,  $X = S^2$ 를  $\mathbb{R}^3$ 의 부분집합으로 본 구면이라 합시다. 우리는  $G$ 가  $X$ 에  $T \cdot \vec{x} = -\vec{x}$ 를 보냄으로써 작용하도록 할 것입니다. 따라서 궤도들은 서로 반대되는 점들의 쌍입니다(예: 북극과 남극). 어떤 공간의 그림을 그려봅시다. 모든 궤도의 크기는 2입니다: 적도 아래의 모든 점은 적도 위의 한 점과 융합됩니다. 적도 위의 점들에 대해서는, 우리가 그 절반을 취할 수 있습니다; 나머지 절반은 대응하는 대척점과 융합됩니다. 이제 모든 것을 평평하게 펴면, 그 결과를 경계의 절반을 가진 원판으로 생각할 수 있습니다: 이것이 앞서 나왔던  $\mathbb{RP}^2$ 입니다. 이 결과로 얻어진 공간에는 이름이 있습니다: 실 사영 2차원 공간(real projective 2-space)이라 하며,  $\mathbb{RP}^2$ 로 표기됩니다.



이는 우리에게 피복 사영  $S^2 \rightarrow \mathbb{RP}^2$ 을 줍니다(충분히 작은 조각의 원상은  $S^2$  위에서 단순히 그 조각의 두 복사본임에 유의하십시오).

#### 예제 66.4.5 ( $\mathbb{RP}^2$ 의 기본군)

위에서 보았듯이, 피복 사영  $S^2 \rightarrow \mathbb{RP}^2$ 이 있었습니다. 게다가 임의의 점의 올은 크기가 2입니다.  $S^2$ 가 단순 연결이므로, 우리는  $\pi_1(\mathbb{RP}^2)$ 에서 크기 2인 집합으로 가는 자연스러운 전단사를 갖습니다; 즉,

$$|\pi_1(\mathbb{RP}^2)| = 2.$$

위수가 2인 군은 오직 하나뿐이므로, 이는  $\pi_1(\mathbb{RP}^2) \cong \mathbb{Z}/2\mathbb{Z}$ 인 경우에만 일어날 수 있습니다!

**질문 66.4.6.** 각 연속 사상  $x \mapsto g \cdot x$ 가 실제로 위상동형사상임을 보이십시오. (그 연속 역사상을 밝히십시오.)

## §66.5 기본군의 대수

**이 절의 대표적인 예:** 기본군이  $\mathbb{Z}$ 인  $S^1$ 입니다.

다음으로, 공간 사이의 함수를 기본군의 준동형사상으로 바꿔보겠습니다.

$X$ 와  $Y$ 를 위상 공간이라 하고  $f: (X, x_0) \rightarrow (Y, y_0)$ 이라 합시다. 우리가 다음과 같은 군 준동형사상을 정의했음을 상기하십시오

$$f_{\#}: \pi_1(X, x_0) \rightarrow \pi_1(Y, y_0) \quad \text{에 의해} \quad [\gamma] \mapsto [f \circ \gamma].$$

더 중요하게는, 다음이 성립합니다:

### 명제 66.5.1

$p: (E, e_0) \rightarrow (B, b_0)$ 을 경로 연결 공간들의 피복 사영이라 합시다. 그러면 준동형사상  $p_{\#}: \pi_1(E, e_0) \rightarrow \pi_1(B, b_0)$ 은 단사입니다. 따라서  $p_{\#}^{\text{img}}(\pi_1(E, e_0))$ 은  $\pi_1(B, b_0)$ 의 부분 군으로서  $\pi_1(E, e_0)$ 의 동형인 사본입니다.

증명.  $\ker p_{\#}$ 가 자명함을 보이겠습니다.  $\gamma$ 가  $B$ 에서 영호모토픽 고리라면 그 들어올림도 영호모토픽임을 보이는 것으로 충분합니다.

정의에 의해,  $\gamma$ 를 상수 고리  $1_B$ 로 보내는 호모토피  $F: [0, 1] \times [0, 1] \rightarrow B$ 가 존재합니다. 이를  $\tilde{\gamma} \simeq \tilde{1}_B$ 를 성립시키는 호모토피  $\tilde{F}: [0, 1] \times [0, 1] \rightarrow E$ 로 들어올릴 수 있습니다. 그런데  $1_E$ 는  $1_B$ 의 들어올림이며 (당연하게도) 들어올림은 유일합니다.  $\square$

### 예제 66.5.2 ( $\mathbb{Z}$ 의 부분군)

기본군이  $\mathbb{Z}$ 인 공간  $S^1$ 을 살펴봅시다. 군  $\mathbb{Z}$ 는 두 가지 유형의 부분군을 갖습니다:

- 자명한 부분군입니다. 이는 표준 사영  $\mathbb{R} \rightarrow S^1$ 에 대응하는데,  $\pi_1(\mathbb{R})$ 가 자명군 이므로( $\mathbb{R}$ 은 단순 연결입니다) 그  $\mathbb{Z}$  안에서의 상 또한 자명군이기 때문입니다.
- $n \geq 1$ 에 대한  $n\mathbb{Z}$ 입니다. 이는  $z \mapsto z^n$ 으로 주어지는 피복 사영  $S^1 \rightarrow S^1$ 에 의해 얻어집니다. 피복  $S^1$ 에서의 고리의 상은 밑공간  $S^1$ 에서 “ $n$ 의 배수”가 됩니다.

놀랍게도 이것들이 경로 연결 공간에 의한  $S^1$ 의 유일한 피복 사영입니다. 즉,  $\mathbb{Z}$ 의 각 부분군마다 하나씩 존재합니다. (연결되지 않은 공간은 신경 쓰지 않는데, 다시 말하지만 연결되지 않은 공간을 통한 피복 사영은 그저 서로 무관한 “좋은” 피복들의 모음일 뿐이기 때문입니다.) 이 진술이 의미를 가지려면 두 피복 사영이 동치라는 것이 무엇을 뜻하는지 알려드려야 합니다.

**정의 66.5.3.** 공간  $B$ 를 고정합시다. 두 피복 사영  $p_1: E_1 \rightarrow B$ 와  $p_2: E_2 \rightarrow B$ 가 주어졌을 때, **피복 사영의 사상**이란  $p_2 \circ f = p_1$ 을 만족하는 연속 함수  $f: E_1 \rightarrow E_2$ 입니다.

$$\begin{array}{ccc} E_1 & \xrightarrow{f} & E_2 \\ & \searrow p_1 & \downarrow p_2 \\ & & B \end{array}$$

그러면 두 피복 사영  $p_1$ 과  $p_2$ 는  $f \circ g = \text{id}_{E_1}$ 이고  $g \circ f = \text{id}_{E_2}$ 를 만족하는  $f: E_1 \rightarrow E_2$ 와  $g: E_2 \rightarrow E_1$ 이 존재할 때 동형이라고 합니다.

**비고 66.5.4 (범주론자를 위하여)** — 피복 사영들의 모임은 이러한 방식으로 하나의 범주를 이룹니다.

이것이 더 일반적으로도 성립한다는 것은 그야말로 기적입니다. 피복 공간의 가장 위대한 승리가 바로 다음 결과입니다. 공간  $X$ 가 다음과 같은 좋은 조건들을 만족한다고 합시다:

**정의 66.5.5.** 공간  $X$ 는, 임의의 점  $x \in X$ 와 그것의 열린 근방  $V$ 에 대해  $x \in U \subseteq V$ 를 만족하는 연결된 열린집합  $U$ 가 존재할 때 **국소 연결**이라고 합니다.

**정의 66.5.6.** 공간  $X$ 는, 모든 점  $x \in X$ 에 대해  $U$  안의 모든 고리가 영호모토픽이 되도록 하는 열린 근방  $U$ 가 존재할 때 **준국소 단순 연결**이라고 합니다. (다만 수축이 반드시  $U$  안에서 일어날 필요는 없습니다.)

**예제 66.5.7 (이 조건들은 약합니다)**

지금까지 보여드린 거의 모든 공간이 이 두 성질을 갖습니다. 다시 말해, 이는 상당히 온건한 조건들이며, 그저 “공간이 지나치게 병리적이지는 않다”는 것을 말한다고 생각하셔도 됩니다.

그러면 다음을 얻습니다:

**정리 66.5.8 (피복 공간을 통한 군론)**

$B$ 가 국소 연결이고 준국소 단순 연결인 공간이라고 합시다. 그러면 다음이 성립합니다.

- 모든 부분군  $H \subseteq \pi_1(B)$ 는  $E$ 가 경로 연결인 피복 사영  $p: E \rightarrow B$  하나에 정확히 대응됩니다(동형사상까지 고려하여).  
(구체적으로,  $H$ 는  $p_*$ 를 통한  $\pi_1(E)$ 의  $\pi_1(B)$  내 상입니다.)
- 더 나아가,  $\pi_1(B)$ 의 정규 부분군은 정칙 피복 사영에 정확히 대응됩니다.

따라서  $\pi_1(B)$ 의 군론을 피복 사영의 관점에서 완전히 이해하는 것이 가능합니다.

더 나아가, 이것이 바로 “보편 피복”이라는 이름이 붙은 이유입니다. 보편 피복은  $\pi_1(B)$ 의 자명한 부분군에 대응되는 피복입니다. 실제로,  $p: E \rightarrow B$ 가 또 다른 피복 사영이라면  $E$ 는 다시 이 보편 공간에 의해 피복된다는 의미에서 이것이 정말로 보편적임을 보일 수 있습니다. 더 일반적으로,  $H_1 \subseteq H_2 \subseteq G$ 가 부분군이라면,  $H_2$ 에 대응되는 공간은  $H_1$ 에 대응되는 공간에 의해 피복될 수 있습니다.

## §66.6 생각해 볼 만한 조금 더 어려운 문제

# XVII

범주론

## 제XVII부: 목차

---

|           |                                |            |
|-----------|--------------------------------|------------|
| <b>67</b> | <b>대상과 사상</b>                  | <b>691</b> |
| 67.1      | 동기: 동형사상 . . . . .             | 691        |
| 67.2      | 범주, 그리고 그 예시들 . . . . .        | 691        |
| 67.3      | 범주 안의 특별한 대상들 . . . . .        | 695        |
| 67.4      | 이항 곱 . . . . .                 | 696        |
| 67.5      | 단사 사상과 전사 사상 . . . . .         | 699        |
| 67.6      | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 701        |
| <br>      |                                |            |
| <b>68</b> | <b>함자와 자연 변환</b>               | <b>703</b> |
| 68.1      | 함자의 여러 예 . . . . .             | 703        |
| 68.2      | 공변 함자 . . . . .                | 704        |
| 68.3      | 대상의 색인 족으로서의 공변 함자 . . . . .   | 707        |
| 68.4      | 반변 함자 . . . . .                | 708        |
| 68.5      | 범주의 동치 . . . . .               | 709        |
| 68.6      | (선택) 자연 변환 . . . . .           | 709        |
| 68.7      | (선택) 요네다 보조정리 . . . . .        | 711        |
| 68.8      | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 713        |
| <br>      |                                |            |
| <b>69</b> | <b>범주에서의 극한 (작성 예정)</b>        | <b>715</b> |
| 69.1      | 등화자 . . . . .                  | 715        |
| 69.2      | 당겨오기 사각형 (작성 예정) . . . . .     | 716        |
| 69.3      | 극한 . . . . .                   | 716        |
| 69.4      | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 716        |
| <br>      |                                |            |
| <b>70</b> | <b>아벨 범주</b>                   | <b>717</b> |
| 70.1      | 영 대상, 핵, 여핵, 그리고 상 . . . . .   | 717        |
| 70.2      | 가법 범주와 아벨 범주 . . . . .         | 718        |
| 70.3      | 완전열 . . . . .                  | 720        |
| 70.4      | 프레이드-미첼 매장 정리 . . . . .        | 721        |
| 70.5      | 긴 완전열 쪼개기 . . . . .            | 723        |
| 70.6      | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 723        |

---

# 67 대상과 사상

이 몇 개의 장에서 범주론을 제대로 다루는 것은 도저히 불가능합니다. 따라서 지금까지 만나본 개념들이 어떻게 범주론적 용어로 다시 표현될 수 있는지에 대해 매우 개괄적인 개요만 제시하겠습니다. 그러므로 범주가 무엇인지 말하고, 몇 가지 예를 든 다음, 범주가 할 수 있는 몇 가지 일에 대해 이야기하겠습니다. 예시는 이전의 모든 장에서 가져올 것입니다; 아직 보지 못한 내용에 해당하는 예시는 건너뛰어도 좋습니다.

(저처럼!) 범주론에, 어쩌면 일반적인 범주에 대해 어떤 놀라운 결과들이 성립하는지에 관심이 있다면, [Le14]를 강력히 추천합니다.

## §67.1 동기: 동형사상

앞선 장들에서 두 대상의 동형사상의 정의를 상기해 봅시다:

- 두 군  $G$ 와  $H$ 는 전단사 준동형사상이 존재하면 동형입니다: 이는 동치로,  $\phi \circ \psi = \text{id}_H$  이고  $\psi \circ \phi = \text{id}_G$ 라는 의미에서 서로 역인 준동형사상  $\phi: G \rightarrow H$ 와  $\psi: H \rightarrow G$ 가 존재하기를 원한 것입니다.
- 두 거리 (또는 위상) 공간  $X$ 와  $Y$ 는 연속인 전단사  $f: X \rightarrow Y$ 가 존재하고  $f^{-1}$  역시 연속이면 동형입니다.
- 두 벡터 공간  $V$ 와  $W$ 는 선형 사상인 전단사  $T: V \rightarrow W$ 가 존재하면 동형입니다. 다시 말해, 이는  $T$ 와  $T^{-1}$ 가 선형 사상이라고 다시 표현할 수 있습니다.
- 두 환  $R$ 와  $S$ 는 전단사 환 준동형사상  $\phi$ 가 존재하면 동형입니다; 이 역시 서로 역인 두 환 준동형사상으로 다시 표현할 수 있습니다.

각 경우에서 우리는 대상들의 어떤 모임과 어떤 사상들을 가지고 있으며, 동형사상은 그저 사상으로 볼 수 있습니다. 이를 이용하여 일반적인 범주의 정의에 대한 동기를 부여해 봅시다.

## §67.2 범주, 그리고 그 예시들

**이 절의 대표적인 예:** Grp는 아마도 가장 자연스러운 예시일 것입니다.

**정의 67.2.1. 범주  $\mathcal{A}$ 는 다음으로 구성됩니다:**

- $\text{obj}(\mathcal{A})$ 로 표기되는 **대상**들의 모임.
  - 임의의 두 대상  $A_1, A_2 \in \text{obj}(\mathcal{A})$ 에 대해, 그들 사이의 **화살(사상)** 또는 **맵**이라고도 함)들의 모임. 이 화살들의 집합을  $\text{Hom}_{\mathcal{A}}(A_1, A_2)$ 로 표기하겠습니다.
  - 임의의  $A_1, A_2, A_3 \in \text{obj}(\mathcal{A})$ 에 대해,  $f: A_1 \rightarrow A_2$ 가 화살이고  $g: A_2 \rightarrow A_3$ 가 화살이면, 이 화살들을 합성하여 화살  $g \circ f: A_1 \rightarrow A_3$ 를 얻을 수 있습니다.
- 이를 **가환 도식**으로 나타낼 수 있습니다

$$\begin{array}{ccc} A_1 & \xrightarrow{f} & A_2 \\ & \searrow h & \downarrow g \\ & & A_3 \end{array}$$

여기서  $h = g \circ f$ 입니다. 합성 연산  $\circ$ 는  $\mathcal{A}$ 의 데이터의 일부이며, 결합법칙을 만족해야 합니다. 위 도식에서  $h$ 가  $A_2$ 를 통해 **인수분해**된다고 말합니다.

- 마지막으로, 모든 대상  $A \in \text{obj}(\mathcal{A})$ 는 특별한 **항등 화살**  $\text{id}_A$ 를 가집니다; 그것이 무엇을 하는지 짐작할 수 있을 것입니다.<sup>1</sup>

**표기의 남용 67.2.2.** 지금부터  $A \in \mathcal{A}$ 라고 하면  $A \in \text{obj}(\mathcal{A})$ 를 의미하겠습니다.

**표기의 남용 67.2.3.** "류(class)"는 그냥 "집합(set)"이라고 생각해도 됩니다. "집합"이라는 단어를 사용할 수 없는 이유는 너무 큰 모임과 관련된 몇 가지 역설적인 문제 때문입니다; 칸토어의 역설(Cantor's Paradox)은 모든 집합의 집합은 존재하지 않는다고 말합니다. 따라서 이들을 "류"라고 부르는 것은 이러한 문제들을 우회하는 방법입니다.

지금부터 계속 저는 다소 느슨하게, 저의 모든 범주가 **국소적으로 작다(locally small)**고 가정하겠습니다. 이는 임의의  $A_1, A_2 \in \mathcal{A}$ 에 대해  $\text{Hom}_{\mathcal{A}}(A_1, A_2)$ 가 집합이라는 의미입니다. 따라서  $\mathcal{A}$ 의 원소들은 집합을 이루지 않을 수 있지만, 주어진 두 대상 사이의 사상들의 모임은 항상 집합으로 가정됩니다.

우리가 처음에 시작한 동기를 형식화해 봅시다.

#### 예제 67.2.4 (범주의 기본 예시들)

(a) 군의 범주  $\text{Grp}$ 가 있습니다. 그 데이터는 다음과 같습니다.

- $\text{Grp}$ 의 대상은 군들입니다.
- $\text{Grp}$ 의 사상은 이 군들 사이의 준동형사상들입니다.
- $\text{Grp}$ 에서의 합성  $\circ$ 는 함수 합성입니다.

(b) 같은 방식으로 (가환) 환의 범주  $\text{CRing}$ 을 생각할 수 있습니다.

(c) 마찬가지로, 위상 공간의 범주  $\text{Top}$ 이 있으며, 이 범주의 사상은 연속 사상입니다.

(d) 구별된 기점을 가진 위상 공간의 범주  $\text{Top}_*$ 가 있습니다. 즉,  $x_0 \in X$ 인 순서쌍  $(X, x_0)$ 입니다. 사상은  $f(x_0) = y_0$ 을 만족하는 연속 사상  $f: X \rightarrow Y$ 입니다.

(e) 마찬가지로, 체  $k$  위의 (무한 차원일 수도 있는) 벡터 공간의 범주  $\text{Vect}_k$ 가 있으며, 이 범주의 사상은 선형 사상입니다. 유한 차원 벡터 공간의 범주  $\text{FVect}_k$ 도 있습니다.

(f) 집합의 범주  $\text{Set}$ 가 있으며, 여기서 사상은 임의의 사상입니다.

그리고 물론, 이제 동형사상이 무엇인지 정의할 수 있습니다!

**정의 67.2.5.** 사상  $A_1 \xrightarrow{f} A_2$ 가 **동형사상**이라는 것은,  $f \circ g = \text{id}_{A_2}$ 이고  $g \circ f = \text{id}_{A_1}$ 을 만족하는  $A_2 \xrightarrow{g} A_1$ 이 존재함을 뜻합니다. 이 경우  $A_1$ 과  $A_2$ 가 **동형**이라고 말하며, 따라서  $A_1 \cong A_2$ 입니다.

**비고 67.2.6** —  $\text{Set}$ 에서는  $X \cong Y \iff |X| = |Y|$ 임에 유의하십시오.

**질문 67.2.7.** 범주 내의 모든 대상이 자기 자신과 동형임을 확인하십시오. (이것은 어이없을 정도로 쉽습니다.)

<sup>1</sup>고통스러울 정도로 명시적으로 말하자면:  $f: A' \rightarrow A$ 가 화살이면  $\text{id}_A \circ f = f$ 이고; 마찬가지로  $g: A \rightarrow A'$ 가 화살이면  $g \circ \text{id}_A = g$ 입니다.

더 중요한 점은, 이 정의가 여러분에게 다소 인상적으로 다가와야 한다는 것입니다. 우리는 두 군(환, 공간 등)이 동형인지를 오직 대상들 사이의 함수만으로 정의할 수 있습니다. 실제로, 범주론(그리고 심지어 대수학)의 핵심 주제 중 하나는 다음과 같습니다.

**대상에 대해서는 그 대상들 사이의 함수를 통해 알 수 있습니다. 범주론은 이를 극단까지 밀어붙여, 오직 사상만을 바라보고 대상 자체가 무엇인지는 무시합니다.**

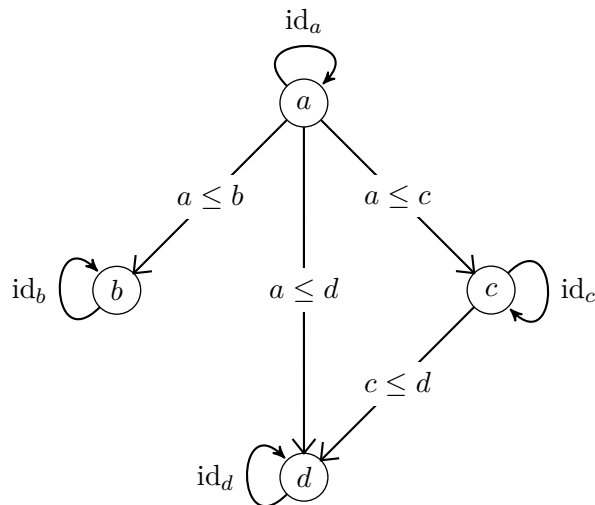
하지만 범주의 더 까다롭고 흥미로운 예시들이 있습니다.

**예제 67.2.8 (순서집합은 범주이다)**

$\mathcal{P}$ 를 부분순서집합이라 합시다. 이에 대해 다음과 같이 범주  $\mathcal{P}$ 를 구성할 수 있습니다.

- $\mathcal{P}$ 의 대상은  $\mathcal{P}$ 의 원소들이 될 것입니다.
- $\mathcal{P}$ 의 사상은 다음과 같이 정의됩니다.
  - 모든 대상  $p \in \mathcal{P}$ 에 대해, 항등 사상  $\text{id}_p$ 를 추가하고,
  - 서로 다른 대상의 쌍  $p \leq q$ 에 대해, 사상  $p \rightarrow q$  하나를 추가합니다.
 다른 사상은 없습니다.
- 합성을 하는 방법은 오직 하나뿐입니다. 그것은 무엇일까요?

예를 들어,  $a \leq b$ 이고  $a \leq c \leq d$ 인 네 대상  $\{a, b, c, d\}$ 로 이루어진 부분순서집합  $\mathcal{P}$ 에 대해서는 다음과 같이 됩니다.



이는 다음과 같은 점을 보여줍니다

**범주의 화살표는 함수와 완전히 다를 수 있습니다.**

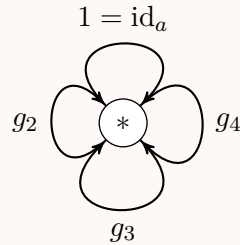
사실 정확하게 표현하자면, “구체적 범주”라는 용어는 화살표가 실제로 Grp, Top, CRing 처럼 “집합 사이의 구조를 보존하는 사상”인 경우를 가리킵니다.

**질문 67.2.9.** 준순서집합의 서로 다른 두 대상은 결코 동형사상이 아님을 확인하십시오.

다음은 구체적이지 않은 범주의 두 번째 중요한 예시입니다.

**예제 67.2.10 (중요: 군은 대상이 하나인 범주입니다)**

군  $G$ 는 대상이 하나  $*$ 이고 모든 화살표가 동형사상인 범주  $\mathcal{G}$ 로 해석될 수 있습니다.



[Le14]에서 말하듯이:

군이 일종의 범주라는 발상을 처음 접하면, 우연이나 트릭으로 치부하고 싶은 유혹이 듭니다. 그렇지 않습니다: 실질적인 내용이 있습니다. 이를 확인하기 위해, 만약 교육 과정이 뒤섞여서 군이 무엇인지 배우기도 전에 범주론 강의를 먼저 들었다고 가정해봅시다. 누군가가 다가와 이렇게 말합니다:

“군’이라 불리는 구조들이 있는데, 그 발상은 이렇습니다: 군이란 주어진 대상의 모든 대칭들을 모아놓은 것입니다.”

“대칭’이라는 게 무슨 뜻인가요?” 당신은 묻습니다.

“음, 대상  $X$ 의 대칭이란  $X$ 를 가역적인 방식으로 변환하거나  $X$  자신으로 사상시키는 방법입니다.”

“아,” 당신이 대답합니다, “그건 제가 전에 접한 발상의 특수한 경우로군요. 범주란 많은 대상들과 그 사이의 사상들 – 반드시 가역적일 필요는 없는 – 로 이루어진 구조입니다. 군은 대상이 단 하나뿐이고 모든 사상이 마침 가역적인 매우 특수한 경우일 뿐이군요.”

**연습문제 67.2.11.** 위의 내용을 검증하십시오! 즉, 모든 사상이 동형사상인 대상 하나짜리 범주의 데이터가 군의 데이터와 동일함을 보이십시오.

마지막으로, 다른 범주들로부터 만들 수 있는 범주의 몇 가지 예시를 소개합니다.

**예제 67.2.12 (범주 유도하기)**

(a) 범주  $\mathcal{A}$ 가 주어지면,  $\mathcal{A}$ 와 같지만 모든 화살표가 뒤집힌 **반대 범주**  $\mathcal{A}^{\text{op}}$ 를 구성할 수 있습니다.

(b) 범주  $\mathcal{A}$ 와  $\mathcal{B}$ 가 주어지면, 다음과 같이 **곱 범주**  $\mathcal{A} \times \mathcal{B}$ 를 구성할 수 있습니다: 대상은  $A \in \mathcal{A}$ 와  $B \in \mathcal{B}$ 에 대한 쌍  $(A, B)$ 이고,  $(A_1, B_1)$ 에서  $(A_2, B_2)$ 로 가는 화살표는 쌍

$$(A_1 \xrightarrow{f} A_2, B_1 \xrightarrow{g} B_2).$$

입니다. 합성과 항등원은 무엇이라고 생각합니까?

### §67.3 범주 안의 특별한 대상들

**이 절의 대표적인 예:** Set은 시작 대상  $\emptyset$ 과 끝 대상  $\{*\}$ 을 가집니다.  $S$ 의 원소는 사상  $\{*\} \rightarrow S$ 에 대응됩니다.

범주 안의 특정 대상들은 특별한 성질을 가집니다. 다음은 그 예시 몇 가지입니다.

#### 예제 67.3.1 (시작 대상)

$\mathcal{A}$ 의 **시작 대상**이란 임의의  $A \in \mathcal{A}$  (경우에 따라  $A = A_{\text{시작 대상}}$ 일 수도 있음)에 대해  $A_{\text{시작 대상}}$ 에서  $A$ 로 가는 화살표가 정확히 하나 존재하는 대상  $A_{\text{시작 대상}} \in \mathcal{A}$ 입니다. 예를 들어,

- (a) Set의 시작 대상은 공집합  $\emptyset$ 입니다.
- (b) Grp의 시작 대상은 자명군  $\{1\}$ 입니다.
- (c) CRing의 시작 대상은 환  $\mathbb{Z}$ 입니다. (환 준동형사상  $R \rightarrow S$ 는  $1_R$ 을  $1_S$ 로 보낸다는 사실을 상기하십시오).
- (d) Top의 시작 대상은 공집합 공간입니다.
- (e) 부분 순서 집합의 시작 대상은, 존재한다면, 그 최소 원소입니다.

우리는 보통 범주의 "그" 시작 대상이라고 지칭할 것인데, 그 이유는 다음과 같습니다:

**연습문제 67.3.2 (중요!).**  $\mathcal{A}$ 의 임의의 두 시작 대상  $A_1, A_2$ 가 유일하게 동형임을, 즉 그들 사이에 유일한 동형사상이 존재함을 보이십시오.

**비고 67.3.3** — 수학에서 우리는 보통 두 대상이 실제로 같은지 혹은 동형인지 알지도 못하고 신경 쓰지도 않습니다. 예를 들어  $\mathbb{R}$ 을 정의하는 여러 경쟁하는 방법이 있지만, 우리는 여전히 그것을 그저 "그" 실수라고 부릅니다. 따라서 범주적 개념을 정의할 때, 우리는 그것들이 동형사상까지 유일한지 확인하고자 합니다. 이는 범주의 언어에서 매우 깔끔하며, 정의는 종종 위와 같은 우아한 이유로 대상이 동형사상까지 유일하게 되도록 만듭니다.

"쌍대" 개념인 끝 대상을 취할 수 있습니다.

#### 예제 67.3.4 (끝 대상)

$\mathcal{A}$ 의 **끝 대상**이란 임의의  $A \in \mathcal{A}$  (가능하다면  $A = A_{\text{종말}}$ )에 대해  $A$ 에서  $A_{\text{종말}}$ 로 가는 화살이 정확히 하나 존재하는 대상  $A_{\text{종말}} \in \mathcal{A}$ 입니다. 예를 들어,

- (a) Set의 끝 대상은 한원소 집합  $\{*\}$ 입니다. (물론 한원소 집합은 많지만, 집합으로서 그것들은 모두 동형입니다!)
- (b) Grp의 끝 대상은 자명군  $\{1\}$ 입니다.
- (c) CRing의 끝 대상은 영환  $0$ 입니다. (환 준동형사상  $R \rightarrow S$ 는 반드시  $1_R$ 을  $1_S$ 로 보내야 함을 기억하십시오).
- (d) Top의 끝 대상은 한 점 공간입니다.

(e) 부분 순서 집합의 끝 대상은, 존재한다면, 그 최대 원소입니다.

다시 말해, 끝 대상은 동형사상까지 유일합니다. 독자는 앞선 연습문제의 증명을 여기서 반복해 보시기 바랍니다. 그러나 우리는 쌍대성 개념을 더 강하게 보여주어 짧은 증명을 제시할 수 있습니다.

**질문 67.3.5.**  $\mathcal{A}$ 의 끝 대상이  $\mathcal{A}^{\text{op}}$ 의 시작 대상과 동치임을 확인하십시오. 따라서  $\mathcal{A}$ 의 끝 대상은 동형사상까지 유일합니다.

일반적으로 이런 방식으로 어떤 범주적 개념의 쌍대도 생각할 수 있습니다:  $\mathcal{A}$ 의 성질은 모두 (흔히 앞에 "쌍대"라는 접두사를 붙여서)  $\mathcal{A}^{\text{op}}$ 의 쌍대 성질로 번역될 수 있습니다.

마지막으로 멋진 구성이 하나 있습니다: 우리가 구체적인 범주에서 작업하고 있다고 가정합시다. 이는 (느슨하게 말해) 대상이 "추가 구조를 갖춘 집합"임을 의미합니다. 이제 여러분이 사상에 지쳐서 그저 이 집합들의 원소에 대해 생각하고 싶다고 가정합시다. 음, 여러분이 범주론 장을 읽고 있으니 그렇게 하도록 두지는 않겠지만, 대신 조언을 하나 드리겠습니다:

- Set에서  $\{*\}$ 에서  $S$ 로 가는 화살은  $S$ 의 원소에 대응합니다.
- Top에서  $\{*\}$ 에서  $X$ 로 가는 화살은  $X$ 의 점에 대응합니다.
- Grp에서  $\mathbb{Z}$ 에서  $G$ 로 가는 화살은  $G$ 의 원소에 대응합니다.
- CRing에서  $\mathbb{Z}[x]$ 에서  $R$ 로 가는 화살은  $R$ 의 원소에 대응합니다.

이런 식으로 계속됩니다. 그러므로 대부분의 구체적인 범주에서, 여러분은 원소를 특수한 집합에서 문제의 집합으로 가는 함수로 생각할 수 있습니다. 이러한 각 경우에 우리는 문제의 대상을 **자유 대상**이라고 부릅니다.

## §67.4 이항 곱

**이 절의 대표적인 예:** 대부분의 구체적인 범주에서  $X \times Y$ 는 집합론적 곱입니다.

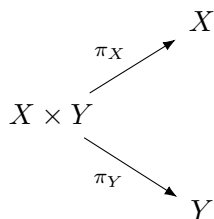
"보편 성질(universal property)"은 대상을 사상의 관점에서 기술하는 방법으로서, 그 대상을 유일한 동형사상까지 결정합니다 (시작 대상 및 끝 대상의 경우와 매우 비슷합니다).

이것이 일반적으로 어떻게 작동하는지 보여드리기 위해, 구체적인 예를 하나 들어보겠습니다. 어떤 범주에 있다고 가정해 봅시다 – 지금은 Set이라고 합시다. 두 집합  $X$ 와  $Y$ 가 있고, 우리가 알고 있는 곱집합  $X \times Y$ 를 구성하고자 합니다. 범주론의 철학은 사상에 대해서만 이야기해야 하며, 집합 자체에 관한 어떤 것도 언급하지 않아야 한다고 지시합니다. 이것을 어떻게 할 수 있을까요?

자,  $X \times Y$ 로 들어가는 사상들에 대해 생각해 봅시다. 핵심 관찰은 다음과 같습니다.

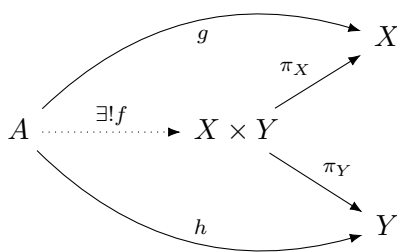
**함수  $A \xrightarrow{f} X \times Y$ 는 함수의 쌍  $(A \xrightarrow{g} X, A \xrightarrow{h} Y)$ 와 대응됩니다.**

달리 말하면,  $X \times Y \rightarrow X$ 와  $X \times Y \rightarrow Y$ 라는 자연스러운 사영 사상이 존재합니다:



(원소가 아니라 사영 사상의 관점에서 이를 다루어야 하는데, 이는 범주론이 우리로 하여금 화살표에 대해 이야기하도록 강제하기 때문입니다.) 이제 이 도식에  $A$ 를 어떻게 추가할까요? 요점은 함수  $A \xrightarrow{f} X \times Y$ 와 함수의 쌍  $(g, h)$  사이에 전단사가 존재한다는 것입니다. 따라서 모든 쌍  $A \xrightarrow{g} X$ 와  $A \xrightarrow{h} Y$ 에 대해 유일한 함수  $A \xrightarrow{f} X \times Y$ 가 존재합니다.

그러나  $X \times Y$ 가 특별한 이유는 그것이 "보편적"이기 때문입니다: 임의의 집합  $A$ 에 대해, 여러분이 함수  $A \rightarrow X$ 와  $A \rightarrow Y$ 를 저에게 준다면, 저는 그것을 이용하여 유일한 함수  $A \rightarrow X \times Y$ 를 만들 수 있습니다. 그림:



이것은 임의의 일반적인 범주에서도 할 수 있으며, 이렇게 정의되는 것을 소위 곱이라고 합니다.

**정의 67.4.1.**  $X$ 와  $Y$ 가 임의의 범주  $\mathcal{A}$ 에서의 대상이라고 합시다. 곱은 대상  $X \times Y$ 와  $X, Y$ 로 향하는 화살표  $\pi_X, \pi_Y$ (사영으로 생각됩니다)로 구성됩니다. 우리는 임의의 대상  $A$ 와 화살표  $A \xrightarrow{g} X, A \xrightarrow{h} Y$ 에 대해, 위 도식이 가환하게 만드는 유일한 함수  $A \xrightarrow{f} X \times Y$ 가 존재할 것을 요구합니다.

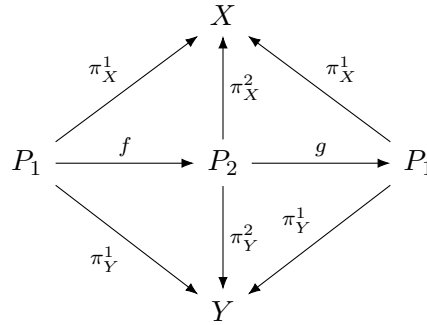
**표기의 남용 67.4.2.** 엄밀히 말하면, 곱은 대상  $X \times Y$ 와 사영 사상  $\pi_X, \pi_Y$ 를 둘 다 포함해야 합니다. 하지만  $\pi_X$ 와  $\pi_Y$ 가 암묵적으로 이해되는 경우, 우리는 흔히  $X \times Y$ 를 그 대상을 가리키는 데 사용하며, 이를 곱이라고도 부릅니다.

곱은 항상 존재하는 것은 아닙니다. 예를 들어, 대상이 딱 두 개만 있고 항등 사상이 아닌 사상은 전혀 없는 범주를 생각해 보십시오. 그럼에도 불구하고:

#### 명제 67.4.3 (곱의 유일성)

곱이 존재할 때, 곱은 동형사상까지 유일합니다:  $X$ 와  $Y$ 의 두 곱  $P_1$ 과  $P_2$ 가 주어지면 두 대상 사이에 동형사상이 존재합니다.

증명. 이는 시작 대상이 유일한 동형사상까지 유일하다는 증명과 매우 유사합니다. 그러한 두 대상  $P_1$ 과  $P_2$ , 그리고 그에 연관된 사영 사상들을 생각해 봅시다. 그러면 다음과 같은 도식이 있습니다.



보편 성질에 따라, 도식 전체를 가환하게 만드는  $P_1$ 과  $P_2$  사이의 유일한 사상  $f$ 와  $g$ 가 존재합니다.

한편,  $g \circ f$ 를 살펴보고 바깥쪽 사각형에만 집중해 봅시다.  $g \circ f$ 는 바깥쪽 사각형을 가환하게 만드는 사상이므로,  $P_1$ 의 보편 성질에 의해 그것이 유일한 것임을 관찰할 수 있습니다. 하지만  $\text{id}_{P_1}$ 도 마찬가지로 작동합니다. 따라서  $\text{id}_{P_1} = g \circ f$ 입니다. 마찬가지로  $f \circ g = \text{id}_{P_2}$ 이므로  $f$ 와  $g$ 는 동형사상입니다.  $\square$

**표기의 남용 67.4.4.** 사실, 이것은 도덕적으로 올바른 정리는 아닌데, 왜냐하면 우리는 대상  $P_1$ 과  $P_2$ 가 동형이라는 것만 보였을 뿐, 사영 사상에 관해서는 어떠한 주장도 하지 않았기 때문입니다. 하지만 저는 곱 전체의 동형사상을 정의하지 않았고 (앞으로도 하지 않을 것이며), 따라서 이후로 " $P_1$ 과  $P_2$ 가 동형이다"라고 말할 때는 정말로 그 대상들이 동형이라는 것만을 의미합니다.

**연습문제 67.4.5.** 실제로, 곱이 유일한 동형사상까지 유일함을 보이겠습니다: 위의  $f$ 와  $g$ 는 사영을 존중하는, 대상  $P_1$ 과  $P_2$  사이의 유일한 동형사상입니다.

이 "보편 성질" 사고방식의 좋은 점은 우리가 명시적인 구성을 제시할 필요가 없다는 것입니다; 존재성을 가정하면, "보편 성질"은 "이러한 성질을 갖는 대상은 유일한 동형사상까지 유일하다"라고 말함으로써 이 모든 작업을 우회할 수 있게 해주며, 따라서 그 성질을 이용하기 위해 그 대상의 내부 작동 방식을 이해할 필요가 없습니다.

물론, 그렇다고 해서 구체적인 예를 들 수 없다는 뜻은 아닙니다.

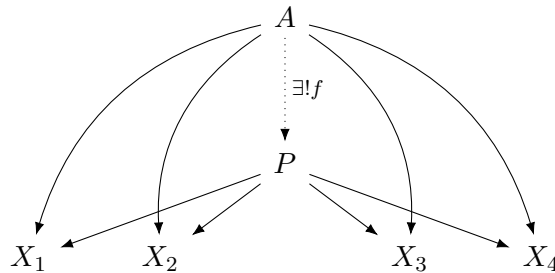
#### 예제 67.4.6 (곱의 예시들)

- (a) Set에서, 두 집합  $X$ 와  $Y$ 의 곱은 그들의 곱집합  $X \times Y$ 입니다.
- (b) Grp에서,  $G$ 와  $H$ 의 곱은 군 곱  $G \times H$ 입니다.
- (c) Vect $_k$ 에서,  $V$ 와  $W$ 의 곱은  $V \oplus W$ 입니다.
- (d) CRing에서,  $R$ 과  $S$ 의 곱은 적절하게도 환 곱  $R \times S$ 입니다.
- (e)  $\mathcal{P}$ 를 범주로 해석된 poset이라 합시다. 그러면 두 대상  $x$ 와  $y$ 의 곱은 **최대 하한**입니다; 예를 들면,
  - poset이  $(\mathbb{R}, \leq)$ 이면 그것은  $\min\{x, y\}$ 입니다.
  - poset이 유한 집합의 부분집합들을 포함관계로 순서 매긴 것이라면, 그것은  $x \cap y$ 입니다.
  - poset이 양의 정수를 나눗셈으로 순서 매긴 것이라면, 그것은  $\gcd(x, y)$ 입니다.

물론, 두 대상보다 더 많은 대상의 곱도 정의할 수 있습니다. 범주  $\mathcal{A}$  안의 대상들의 집합  $(X_i)_{i \in I}$ 을 생각해봅시다.  $X_i$  위의 **원뿔**을 각  $X_i$ 로 가는 몇 개의 "사영" 사상을 가진 대상

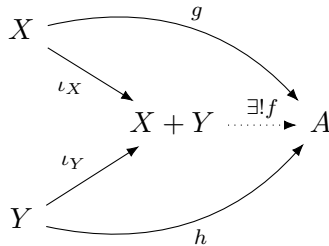
$A$ 로 정의합니다. 그러면 **곱**은 앞서와 같은 의미로 "보편적"인 원뿔  $P$ 입니다: 임의의 다른 원뿔  $A$ 가 주어지면, 도식을 가환하게 만드는 유일한 사상  $A \rightarrow P$ 가 존재합니다. 요컨대, 곱은 "보편 원뿔"입니다.

이것을 그림으로 나타내면 다음과 같습니다



문제 67C도 참고하십시오.

쌍대 구성을 하여 **쌍대곱**을 얻을 수도 있습니다:  $X$ 와  $Y$ 가 주어지면, 그것은 대상  $X+Y$ 와 사상  $X \xrightarrow{\iota_X} X+Y$  및  $Y \xrightarrow{\iota_Y} X+Y$  (이것은 그리스 문자 이오타이며, 포함관계라고 생각하십시오)로 이루어지며, 임의의 대상  $A$ 와 사상  $X \xrightarrow{g} A$ ,  $Y \xrightarrow{h} A$ 에 대해 다음을 만족하는 유일한  $f$ 가 존재합니다



가 가환하는 것입니다. 이번에는 구체적인 예시 몇 가지를 연습문제로 남겨두겠습니다, 예를 들면:

**연습문제 67.4.7.** Set에서 쌍대곱을 묘사하십시오.

예상 가능한 용어입니다: 쌍대곱은 보편 **쌍대원뿔**입니다.

나중을 위한 스포일러: 이 구성은 소위 "극한"으로 크게 일반화될 수 있으며, 나중에 그렇게 할 것입니다.

## §67.5 단사 사상과 전사 사상

화살표가 반드시 함수일 필요는 없으므로, "단사"라는 개념은 임의의 범주에서 의미가 통하지 않습니다. 올바른 범주론적 개념은 다음과 같습니다:

**정의 67.5.1.** 사상  $X \xrightarrow{f} Y$ 가 **모닉**(단사 사상)이라 함은 임의의 가환 도식에 대해

$$A \begin{matrix} \xrightarrow{g} \\ \xrightarrow{h} \end{matrix} X \xrightarrow{f} Y$$

$g = h$ 를 만족해야 한다면 **모닉**(또는 단사 사상)이라 합니다. 다시 말해,  $f \circ g = f \circ h \implies g = h$ 입니다.

**질문 67.5.2.** 구체적 범주에서는 단사  $\implies$  모닉임을 스스로 확인해보십시오. (엄밀히 말하면, 아직 구체적 범주의 formal한 정의를 제시하지 않았습니

**비고 68.2.3**에 도달한 후 이 연습문제를 다시 풀어도 됩니다.)

**질문 67.5.3.** 두 모닉 사상의 합성이 모닉임을 보이십시오.

대부분의 경우, 그러나 전부는 아니지만, 역도 성립합니다.

**연습문제 67.5.4.** Set, Grp, CRing에서 모닉이면 단사임을 보이십시오. ( $A = \{*\}$ ,  $A = \mathbb{Z}$ ,  $A = \mathbb{Z}[x]$ 를 취하십시오.)

더 일반적으로, 앞서 말했듯이 원소로 생각할 수 있는 "자유" 대상을 가진 범주가 많습니다. 집합의 원소는 함수  $1 \rightarrow S$ 이고, 환의 원소는 함수  $\mathbb{Z}[x] \rightarrow R$ 입니다, 기타 등등. 이 모든 범주에서, 모닉의 정의는 문자 그대로 " $f$ 는  $\text{Hom}_A(A, X)$  위에서 단사이다"라고 읽힙니다. 따라서 이러한 범주에서는 "모닉"과 "단사"가 일치합니다.

그렇긴 하지만, 여기 표준적인 반례가 있습니다. 가법 아벨 군  $G = (G, +)$ 는 모든  $x \in G$ 와 정수  $n > 0$ 에 대해  $ny = x$ 를 만족하는  $y \in G$ 가 존재하면 나눗셈가능하다고 합니다. DivAbGrp를 이러한 군들의 범주라 합시다.

**연습문제 67.5.5.** DivAbGrp에서 사영  $\mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z}$ 가 모닉이지만 단사는 아님을 보이십시오.

물론, 쌍대 개념도 취할 수 있습니다.

**정의 67.5.6.** 사상  $X \xrightarrow{f} Y$ 가 다음과 같은 가환 도식에 대해 **전사**(또는 전사 사상)이라는 것은

$$X \xrightarrow{f} Y \xrightleftharpoons[h]{g} A$$

$g = h$ 이어야 한다면 **전사적**(epic, 또는 전사 사상)이라고 합니다. 다시 말해,  $g \circ f = h \circ f \implies g = h$ 입니다.

이는 전사성과 비슷한 개념이지만, 지난번보다는 조금 더 나아간 것입니다. 구체적 범주 (concrete category)에서는 전사  $\implies$  전사적임에 유의하십시오.

**연습문제 67.5.7.** Set, Grp, Ab, Vect<sub>k</sub>, Top에서 전사적임과 전사가 일치함을 보이십시오. (Set의 경우,  $A = \{0, 1\}$ 을 취하십시오.)

그러나 이것이 성립하지 않는 경우가 더 많습니다. 가장 대표적으로는:

**예제 67.5.8** (전사적이지만 전사가 아닌 경우)

(a) 예를 들어 CRing에서, 포함 사상  $\mathbb{Z} \hookrightarrow \mathbb{Q}$ 는 전사적입니다(그리고 전사가 아닙니다). 실제로, 두 준동형사상  $\mathbb{Q} \rightarrow A$ 가 모든 정수에서 일치한다면 이들은 모든 곳에서 일치합니다 (왜 그럴까요?),

(b) 하우스도르프(Hausdorff) 위상 공간(임의의 두 점이 서로소인 열린 근방을 가짐)의 범주에서는, 실제로 전사적임  $\iff$  조밀한 상(像)입니다(예:  $\mathbb{Q} \hookrightarrow \mathbb{R}$ 처럼).

따라서 함수  $f: X \rightarrow Y$ 가  $X$ 의 일부 점들만으로 결정될 수 있을 때 실패가 발생합니다.

## §67.6 생각해 볼 만한 조금 더 어려운 문제

문제 67A. 체  $k$ 에 대한  $k$ -벡터 공간의 범주  $\text{Vect}_k$ 에서, 시작 대상과 끝 대상은 무엇입니까?

문제 67B<sup>†</sup>. 범주  $\text{Vect}_k$ 와 포셋(poset)에서 쌍대곱  $X + Y$ 는 무엇입니까?

문제 67C. 모든 곱이 존재하는 임의의 범주  $\mathcal{A}$ 에서,  $X, Y, Z$ 가 임의의 대상일 때

$$(X \times Y) \times Z \cong X \times (Y \times Z)$$

임을 보이십시오. (여기서 양변은 표기의 남용 67.4.2에서와 같이 대상을 가리킵니다.)



문제 67D. **영 대상**을 갖는 범주  $\mathcal{A}$ 를 생각해 보십시오. 여기서 영 대상이란 시작 대상이면서 동시에 끝 대상인 대상을 의미합니다.  $\mathcal{A}$ 에서 대상  $X$ 와  $Y$ 가 주어졌을 때, 사영  $X \times Y \rightarrow X$ 가 전사 사상임을 증명하십시오.



# 68 함자와 자연 변환

함자는 범주 사이의 사상이며, 자연 변환은 함자 사이의 사상입니다.

## §68.1 함자의 여러 예

이 절의 대표적인 예: 망각 함자; 기본군;  $\bullet^V$ .

함자의 핵심은 다음과 같습니다:

어떤 대상으로부터 다른 대상을 만들어낼 때마다, 거의 항상 함자를 얻게 됩니다.

형식적인 정의를 드리기 전에, (비형식적으로) 몇 가지 예를 나열해 보겠습니다. (몇몇 경우에는 반대 범주  $\mathcal{A}^{\text{op}}$ 가 곳곳에 등장하는 것을 눈치채실 것입니다. 지금은 그것에 대해 걱정하지 마십시오; 잠시 후에 왜 그런지 보시게 될 것입니다.)

- 군  $G$ (또는 벡터 공간, 체, ...)가 주어지면, 우리는 그 바탕이 되는 집합  $S$ 를 취할 수 있습니다. 이는  $\text{Grp} \rightarrow \text{Set}$ 로 가는 함자입니다.
- 집합  $S$ 가 주어지면,  $S$ 를 기저로 갖는 벡터 공간을 생각할 수 있습니다; 이는  $\text{Set} \rightarrow \text{Vect}$ 로 가는 함자입니다.
- 벡터 공간  $V$ 가 주어지면, 그 쌍대 공간  $V^V$ 를 생각할 수 있습니다. 이는 함자  $\text{Vect}_k^{\text{op}} \rightarrow \text{Vect}_k$ 입니다.
- 텐서곱은  $\text{Vect}_k \times \text{Vect}_k \rightarrow \text{Vect}_k$ 로 가는 함자를 줍니다.
- 집합  $S$ 가 주어지면, 그 멍집합을 만들 수 있으며, 이는 함자  $\text{Set} \rightarrow \text{Set}$ 를 줍니다.
- 대수적 위상수학에서는, 위상 공간  $X$ 를 취하여 이와 관련된 여러 군  $H_1(X)$ ,  $\pi_1(X)$  등을 만듭니다. 이러한 모든 군 구성은 함자  $\text{Top} \rightarrow \text{Grp}$ 입니다.
- 준동형사상들의 집합:  $\mathcal{A}$ 를 범주라 합시다.
  - $k$  위의 두 벡터 공간  $V_1$ 과  $V_2$ 가 주어지면, 선형 사상  $V_1 \rightarrow V_2$ 들의 아벨 군을 구성할 수 있습니다. 이는  $\text{Vect}_k^{\text{op}} \times \text{Vect}_k \rightarrow \text{AbGrp}$ 로 가는 함자입니다.
  - 더 일반적으로, 임의의 범주  $\mathcal{A}$ 에 대해 대상들의 쌍  $(A_1, A_2)$ 를 취하여 집합  $\text{Hom}_{\mathcal{A}}(A_1, A_2)$ 를 얻을 수 있습니다. 이는 함자  $\mathcal{A}^{\text{op}} \times \mathcal{A} \rightarrow \text{Set}$ 임이 밝혀집니다.
  - 위의 연산에는 두 개의 "자리"가 있습니다. 첫 번째 자리를 "미리 채우면", 함자  $\mathcal{A} \rightarrow \text{Set}$ 를 얻게 됩니다. 즉,  $A \in \mathcal{A}$ 를 고정함으로써,  $A' \in \mathcal{A}$ 를  $\text{Hom}_{\mathcal{A}}(A, A')$ 로 보내는 함자(이를  $H^A$ 라 부릅니다)를  $\mathcal{A} \rightarrow \text{Set}$ 로부터 얻습니다. 이를 공변 요네다 함자라 부릅니다(나중에 설명합니다).
  - 위에서 보았듯이, 모든  $A \in \mathcal{A}$ 에 대해 함자  $H^A: \mathcal{A} \rightarrow \text{Set}$ 를 얻습니다. 원소가 함자  $\mathcal{A} \rightarrow \text{Set}$ 들인 범주  $[\mathcal{A}, \text{Set}]$ 를 구성할 수 있음이 밝혀지며, 이 경우 이제 함자  $\mathcal{A}^{\text{op}} \rightarrow [\mathcal{A}, \text{Set}]$ 를 갖게 됩니다.

그렇다면, 이제 함수가 아닌 몇 가지 예를 살펴보겠습니다. ” $F$ 는 함수이다” (다시 말해, ” $F$ 는 함수적이다”)라고 말하는 정리를 보게 될 때, 이를 ”이 정리는 자명하다”가 아니라 ” $F$ 는 그 배후에 깊이 숨겨진 대칭성을 가지고 있다! 이는 매우 근사한 일이다!”로 읽으시라는 취지입니다.

그 깊은 대칭성이란 무엇일까요? 계속 읽어 보십시오.

- 군  $G$ 가 주어지면, 그 자기동형사상군  $\text{Aut}(G)$ 를 만들 수 있습니다. 하지만 이는 어떠한 자연스러운 방식으로든 함수가 아닙니다.
- 군  $G$ 가 주어지면, 그 중심  $Z(G)$ , 즉  $G$ 의 모든 원소와 교환하는  $G$ 의 원소들의 집합을 만들 수 있습니다. 이 역시 어떠한 자연스러운 방식으로든 함수가 아닙니다.<sup>1</sup>
- 위에서 본 쌍대 공간을 취하는 연산은 반변 함수  $\text{Vect}_k^{\text{op}} \rightarrow \text{Vect}_k$ 이지만, 공변 함수  $\text{Vect}_k \rightarrow \text{Vect}_k$ 는 아닙니다. (반변 함수가 무엇인지는 지금은 걱정하지 마십시오.)

## §68.2 공변 함수

**이 절의 대표적인 예:** 망각 함수/자유 함수, ...

범주론자들은 늘 ”사상은 무엇인가?”라고 묻으며, 이제 우리는 범주 사이의 사상에 대해 생각해 볼 수 있습니다.

**정의 68.2.1.**  $\mathcal{A}$ 와  $\mathcal{B}$ 를 범주라고 합시다. 물론 **함자**  $F$ 는  $\mathcal{A}$ 의 모든 대상을  $\mathcal{B}$ 의 대상으로 보냅니다. 하지만 이에 더해, 모든 화살표  $A_1 \xrightarrow{f} A_2$ 를 화살표  $F(A_1) \xrightarrow{F(f)} F(A_2)$ 로 보내야 합니다. 이를 다음과 같이 그림으로 나타낼 수 있습니다.

$$\begin{array}{ccc}
 A_1 & & B_1 = F(A_1) \\
 \downarrow f & \xrightarrow{\quad F \quad} & \downarrow F(f) \\
 A_2 & & B_2 = F(A_2)
 \end{array}
 \quad \begin{array}{l} \mathcal{A} \ni \\ \in \mathcal{B} \end{array}$$

(강조를 위해 서로 다른 범주를 가로지르는 함수에는 점선 화살표를 사용하도록 하겠습니까.) 함수는 다음의 ”자연성” 요구 조건을 만족해야 합니다:

- 항등 화살표는 항등 화살표로 보내집니다: 각 항등 화살표  $\text{id}_A$ 에 대해,  $F(\text{id}_A) = \text{id}_{F(A)}$ 가 성립합니다.
- 함수는 합성을 보존합니다:  $A_1 \xrightarrow{f} A_2 \xrightarrow{g} A_3$ 가  $\mathcal{A}$ 의 화살표라면,  $F(g \circ f) = F(g) \circ F(f)$ 가 성립합니다.

그러므로 아이디어는 다음과 같습니다:

$\mathcal{A}$ 의 대상  $A \in \mathcal{A}$ 를  $\mathcal{B}$ 의 대상  $B \in \mathcal{B}$ 로 자연스럽게 대응시킬 때마다, 대개 사상  $A_1 \rightarrow A_2$ 를 사상  $B_1 \rightarrow B_2$ 로 변환하는 자연스러운 방법이 존재합니다.

이에 대한 몇 가지 예시를 살펴보십시오.

<sup>1</sup>함자의 성질—특히 항등 사상이 항등 사상으로 보내진다는 점—에 기반하여 반례를 찾는 것은 쉽습니다. 증명은 <https://math.stackexchange.com/q/158438>을 참고하십시오.

**예제 68.2.2 (자유 함수와 망각 함수)**

이 둘 다 비공식적인 용어이며, 엄밀한 정의를 가지지 않는다는 점에 유의하십시오.

- (a) 앞서 **망각 함수**에 대해 이야기했는데, 이는  $\text{Vect}_k$ 와 같은 범주의 기저 집합을 취하는 함수입니다. 이를  $U: \text{Vect}_k \rightarrow \text{Set}$ 라고 부르도록 합시다.

이제,  $\text{Vect}_k$ 의 사상  $T: V_1 \rightarrow V_2$ 가 주어지면,  $T$ 에 대응하는 집합론적 사상일 뿐인 명백한 사상  $U(T): U(V_1) \rightarrow U(V_2)$ 가 존재합니다.

마찬가지로  $\text{Grp}$ ,  $\text{CRing}$  등에서  $\text{Set}$ 으로 가는 망각 함수들이 있습니다. 심지어  $\text{CRing} \rightarrow \text{Grp}$ 인 망각 함수도 있습니다: 환  $R$ 을 아벨 군  $(R, +)$ 로 보내는 것입니다. 공통된 주제는 원래 범주로부터 구조를 “망각”하고 있다는 점입니다.

- (b) 예시에서 **자유 함수**에 대해서도 이야기했습니다. 자유 함수  $F: \text{Set} \rightarrow \text{Vect}_k$ 는  $F(S)$ 를 기저가  $S$ 인 벡터 공간으로 간주함으로써 얻을 수 있습니다. 이제, 사상  $f: S \rightarrow T$ 가 주어지면,  $F(S) \rightarrow F(T)$ 인 명백한 사상은 무엇일까요? 간단합니다: 각 기저 원소  $s \in S$ 를 기저 원소  $f(s) \in T$ 로 보내면 됩니다.

마찬가지로, 집합  $S$ 에 의해 생성된 자유 군을 취함으로써  $F: \text{Set} \rightarrow \text{Grp}$ 를 정의할 수 있습니다.

**비고 68.2.3** — 함수에 대해서도 (화살표에 관한) “단사”와 “전사”라는 개념이 다음과 같이 존재합니다. 함수  $F: \mathcal{A} \rightarrow \mathcal{B}$ 는, 임의의  $A_1, A_2$ 에 대해  $F: \text{Hom}_{\mathcal{A}}(A_1, A_2) \rightarrow \text{Hom}_{\mathcal{B}}(FA_1, FA_2)$ 가 단사(각각, 전사)일 때 **충실**(각각, **충만**)하다고 합니다.<sup>a</sup> 이를 이용해 구체적인 범주의 정확한 정의를 내릴 수 있습니다: 이는 충실한 (망각) 함수  $U: \mathcal{A} \rightarrow \text{Set}$ 를 갖는 범주입니다.

<sup>a</sup>다시 말하지만, 전문가라면  $\text{Hom}_{\mathcal{A}}(A_1, A_2)$ 나  $\text{Hom}_{\mathcal{B}}(FA_1, FA_2)$ 가 집합이 아니라 고유 모임일 수 있다고 반론할 수 있겠으나, 여기서는 모든 것이 국소적으로 작다고 가정하겠습니다.

**예제 68.2.4 ( $\mathcal{G}$ 로부터의 함수)**

$G$ 를 군이라 하고,  $\mathcal{G} = \{*\}$ 를 그에 대응하는 한 대상 범주라고 합시다.

- (a) 함수  $F: \mathcal{G} \rightarrow \text{Set}$ 를 생각하고,  $S = F(*)$ 라고 합시다. 그러면  $F$ 의 자료는  $S$ 에 대한  $G$ 의 군 작용을 부여하는 것에 대응합니다.
- (b) 함수  $F: \mathcal{G} \rightarrow \text{FDVect}_k$ 를 생각하고,  $V = F(*)$ 가 차원  $n$ 을 가진다고 합시다. 그러면  $F$ 의 자료는  $G$ 를  $n \times n$  행렬들(즉, 선형 사상  $V \rightarrow V$ 들)의 부분군으로 매장하는 것에 대응합니다. 이는 역사적으로 군이 등장하게 된 한 가지 방식이며, 군을 행렬로 보는 이론이 표현론이라는 분야를 이룹니다.
- (c)  $H$ 를 군이라 하고 같은 방식으로  $\mathcal{H}$ 를 구성합시다. 그러면 함수  $\mathcal{G} \rightarrow \mathcal{H}$ 는 준동형 사상  $G \rightarrow H$ 에 대응합니다.

**연습문제 68.2.5.** 위의 군에 기반한 함수들이 광고한 대로 작동하는지 확인해 보십시오.

좀 더 복잡한 예시를 들어보겠습니다. 만약 헛갈린다면, 건너뛰었다가 이것의 반변 버전에 대해 읽은 뒤 다시 돌아오십시오.

**예제 68.2.6 (공변 요네다 함자)**

$A \in \mathcal{A}$  하나를 고정합니다. 범주  $\mathcal{A}$ 에 대해,

$$H^A(A_1) := \text{Hom}_{\mathcal{A}}(A, A_1) \in \text{Set}.$$

로 정의함으로써 **공변 요네다 함자**  $H^A: \mathcal{A} \rightarrow \text{Set}$ 를 정의합니다. 따라서 각  $A_1$ 은  $\mathcal{A}$ 에서  $A_1$ 로 가는 화살표로 보내집니다; 즉  $H^A$ 는  $A$ 가 세상을 어떻게 보는지를 설명합니다.

이제  $H^A$ 가 화살표에 대해 어떻게 작동하는지 명시하고자 합니다. 각 화살표  $A_1 \xrightarrow{f} A_2$ 에 대해,  $\text{Set}$ -사상  $\text{Hom}_{\mathcal{A}}(A, A_1) \rightarrow \text{Hom}_{\mathcal{A}}(A, A_2)$ 를 명시해야 합니다; 다시 말해, 화살표  $A \xrightarrow{p} A_1$ 을 화살표  $A \rightarrow A_2$ 로 보내야 합니다. 이를 수행하는 합리적인 방법은 오직 하나뿐입니다: 합성을 취하는 것입니다

$$A \xrightarrow{p} A_1 \xrightarrow{f} A_2.$$

다시 말해,  $H^A(f)$ 는  $p \mapsto f \circ p$ 입니다. 또 다르게 말하면,  $H^A(f) = f \circ -$ 입니다; 여기서  $-$ 는 입력값이 들어갈 자리입니다.

또 다른 예로:

**질문 68.2.7.**  $\mathcal{P}$ 와  $\mathcal{Q}$ 가 범주로 해석된 순서집합이라면,  $\mathcal{P}$ 에서  $\mathcal{Q}$ 로 가는 함자는 무엇을 나타냅니까?

이제 우리가 왜 이것에 관심을 가져야 하는지 설명하겠습니다. 다음의 "당연한" 사실을 생각해 봅시다:  $G$ 와  $H$ 가 동형인 군이라면, 이들은 크기가 같습니다. 이를 다음과 같이 형식화할 수 있습니다:  $\text{Grp}$ 에서  $G \cong H$ 이고  $U: \text{Grp} \rightarrow \text{Set}$ 이 망각 함자(각 군을 그 기초 집합으로 보내는 함자)라면,  $U(G) \cong U(H)$ 입니다. 범주론의 아름다움이 여기서 드러납니다: 이는 사실 임의의 함자와 범주에 대해서도 성립하며, 그 증명은 오직 화살표만으로 이루어집니다:

**정리 68.2.8 (함자는 동형사상을 보존합니다)**

$A_1 \cong A_2$ 가  $\mathcal{A}$ 에서 동형인 대상이고  $F: \mathcal{A} \rightarrow \mathcal{B}$ 가 함자라면  $F(A_1) \cong F(A_2)$ 입니다.

증명. 직접 시도해 보십시오! 그림은 다음과 같습니다:

$$\mathcal{A} \ni \begin{array}{c} A_1 \\ \uparrow f \\ \text{---} F \text{---} \\ \downarrow g \\ A_2 \end{array} \quad \begin{array}{c} B_1 = F(A_1) \\ \uparrow F(f) \\ \text{---} F(g) \text{---} \\ \downarrow \\ B_2 = F(A_2) \end{array} \in \mathcal{B}$$

함자의 두 가지 핵심 성질을 모두 사용해야 합니다: 함자는 합성과 항등 사상을 보존한다는 것입니다.  $\square$

이는 앞으로 우리에게 훌륭한 직관을 줄 것입니다, 왜냐하면

(i) 우리가 평생 수행하는 거의 모든 연산은 함자일 것이며, 그리고

(ii) 우리는 이제 함자가 동형인 대상을 동형인 대상으로 보낸다는 것을 알고 있습니다.

따라서 우리는 이제 자동으로, 우리가 수행하는 거의 모든 "합리적인" 연산이 동형을 보존한다는 것을 알게 됩니다(여기서 "합리적"이라는 것은 그것이 함자라는 것을 의미합니다). 이는 예를 들어 대수적 위상수학에서 매우 유용합니다; 정리 65.6.2를 참고하십시오, 거기서 우리는 호모토픽한 공간들이 동형인 기본군을 가진다는 것을 공짜로 얻습니다.

**비고 68.2.9** — 이를 통해 대상이 범주이고 화살표가 함자인 범주  $\mathbf{Cat}$ 을 구성할 수 있습니다.

## §68.3 대상의 색인 족으로서의 공변 함자

함자를 함수로 보는 대신, 때로는 함자를 대상(또는 대상의 족)으로 보는 것이 더 편리합니다.

집합  $A$ 와  $B$ 에 대해, 때로는 표기법  $A^B$ 가  $B$ 에서  $A$ 로 가는 모든 함수의 집합인  $\text{Hom}(B, A)$ 를 나타내는 데 사용됩니다. 이 표기법이 자연스러운 이유는, 유한 집합  $A$ 와  $B$ 에 대해  $|\text{Hom}(B, A)| = |A|^{|B|}$ 이기 때문입니다.

그렇긴 하지만, 곱집합  $A \times A$ 도 때로는  $A^2$ 로 표기됩니다. 이들 사이에 관계가 있습니까?

물론입니다! 집합  $\mathbf{2} = \{0, 1\}$ (또는 원소가 두 개인 임의의 집합)을 정의합니다. 그러면  $|\mathbf{2}| = 2$ 입니다.  $A^2$ 와  $\text{Hom}(\mathbf{2}, A)$  사이에 대응이 있음을 확인하는 것은 어렵지 않습니다.

이제  $\mathcal{A}$ 를 범주라 합시다. 범주  $\mathcal{A} \times \mathcal{A} = \mathcal{A}^2$ 를 자명한 방식으로 정의합니다:

- $\mathcal{A}^2$ 의 대상은  $A_1, A_2 \in \mathcal{A}$ 인 대상의 쌍  $(A_1, A_2)$ 입니다,
- 사상은 사상의 쌍입니다...

**연습문제 68.3.1.**  $X, Y \in \mathbf{Top}$ 에 대해, 곱공간  $X \times Y \in \mathbf{Top}$ 을 정의할 수 있습니다. 이는 함자  $\mathbf{Top}^2 \rightarrow \mathbf{Top}$ 을 줍니다. 이를 확인하십시오. ( $\mathbf{Top}^2$ 에서의 사상 쌍  $(f, g) : (X_1, Y_1) \rightarrow (X_2, Y_2)$ 로부터, 어떻게 사상  $X_1 \times Y_1 \rightarrow X_2 \times Y_2$ 를 얻습니까? 이 사상이 연속임을, 즉 실제로  $\mathbf{Top}$ 에서의 사상임을 확인하십시오.)

위와 유사하게,  $\mathcal{A}^2$ 의 각 대상은 어떤 함수  $f : \mathbf{2} \rightarrow \mathcal{A}$ 에 대응해야 합니다. 하지만 함수의 공역은 대상이어야 하는데...  $\mathcal{A}$ 는 범주이므로,  $f$ 는 함자여야 합니다!

그래서 우리는 범주  $\mathbf{2}$ 를 만들 수 있고,  $F : \mathbf{2} \rightarrow \mathcal{A}$ 를 갖게 됩니다. 우리가 원하는 바를 만족하도록  $\mathbf{2}$ 를 정의하는 합리적인 방법은 오직 하나뿐입니다:<sup>2</sup>

- 대상은  $\{0, 1\}$ 입니다;
- $\text{id}_0$ 과  $\text{id}_1$ 을 제외하고는 사상이 없습니다.

더 일반적으로,

**함자  $F : \mathcal{A} \rightarrow \mathcal{B}$ 는 대상들의 인덱스 모음  $\{B_A \in \mathcal{B}\}_{A \in \mathcal{A}}$ 로 볼 수 있습니다.**

이는 전층(presheaf)의 경우 가장 쉽게 확인할 수 있습니다: "반변 함자  $\text{OpenSets}(X)^{\text{op}} \rightarrow \mathbf{Rings}$ "란 " $X$ 의 열린집합으로 인덱스된, 어떤 좋은 조건을 만족하는 환들의 모임"을 의미합니다.

실제로  $\mathcal{A}^2$ 가 범주인 것처럼, 함자  $\mathbf{2} \rightarrow \mathcal{A}$ 들 또한 범주를 이룹니다. 이는 절 68.7에서 살펴보겠습니다.

<sup>2</sup>이는 나중에 자연 변환을 위해 정의할 범주  $\mathbf{2}$ 와는 다릅니다! 주의하십시오.

## §68.4 반변 함자

**이 절의 대표적인 예:** 쌍대 공간, 반변 요네다 함자 등

이제 앞서 반대 범주가 무엇을 하고 있었는지 설명해야겠습니다. 앞선 모든 예시에서, 우리는 화살표  $A_1 \rightarrow A_2$ 를 취하면 그것이 화살표  $F(A_1) \rightarrow F(A_2)$ 가 되었습니다. 그러나 때로는 화살표가 실제로 반대 방향으로 가기도 합니다: 대신 화살표  $F(A_2) \rightarrow F(A_1)$ 을 얻게 됩니다. 다시 말해, 단순히 함자  $\mathcal{A} \rightarrow \mathcal{B}$ 를 얻는 대신 함자  $\mathcal{A}^{\text{op}} \rightarrow \mathcal{B}$ 를 얻게 됩니다.

이러한 함자들에는 이름이 있습니다:

**정의 68.4.1.**  $\mathcal{A}$ 에서  $\mathcal{B}$ 로 가는 **반변 함자**란 함자  $F: \mathcal{A}^{\text{op}} \rightarrow \mathcal{B}$ 를 말합니다. (혼동을 줄 수 있으므로 "반변 함자  $F: \mathcal{A} \rightarrow \mathcal{B}$ "라고는 쓰지 않는다는 점에 유의하십시오; 함수 표기법은 항상 올바른 정의역과 공역을 사용합니다.)

그림으로 나타내면:

$$\begin{array}{ccc}
 & A_1 & B_1 = F(A_1) \\
 & \downarrow f & \uparrow F(f) \\
 \mathcal{A} \ni & \text{-----} F \text{-----} & \in \mathcal{B} \\
 & \downarrow & \downarrow \\
 & A_2 & B_2 = F(A_2)
 \end{array}$$

강조를 위해, 보통의 함자는 종종 **공변 함자**라고 불립니다. ("함자"라는 단어는 별다른 수식어가 없으면 항상 공변 함자를 가리킵니다.)

이런 일이 왜 일어날 수 있는지 살펴봅시다.

### 예제 68.4.2 ( $V \mapsto V^\vee$ 는 반변적입니다)

$V \mapsto V^\vee$ 에 의한 함자  $\text{Vect}_k \rightarrow \text{Vect}_k$ 를 생각해 봅시다.

만약 우리가 공변 함자를 명시하려 한다면, 모든 선형 사상  $T: V_1 \rightarrow V_2$ 에 대해 선형 사상  $T^\vee: V_1^\vee \rightarrow V_2^\vee$ 가 필요할 것입니다. 하지만  $V_1^\vee = \text{Hom}(V_1, k)$ 이고  $V_2^\vee = \text{Hom}(V_2, k)$ 임을 상기해 보십시오: 왼쪽에서 오른쪽으로 가는 명백한 사상을 얻을 쉬운 방법이 없습니다.

하지만 오른쪽에서 왼쪽으로 가는 명백한 사상은 존재합니다:  $\xi_2: V_2 \rightarrow k$ 가 주어지면,  $V_1 \rightarrow k$ 로 가는 사상을 쉽게 줄 수 있습니다: 그냥  $T$ 와 합성하면 됩니다! 다시 말해, 다음 합성에 따라  $V_2^\vee \rightarrow V_1^\vee$ 로 가는 매우 자연스러운 사상이 존재합니다

$$V_1 \xrightarrow{T} V_2 \xrightarrow{\xi_2} k$$

요약하면, 사상  $T: V_1 \rightarrow V_2$ 는 반대 방향으로 사상  $T^\vee: V_2^\vee \rightarrow V_1^\vee$ 를 자연스럽게 유도합니다. 따라서 반변 함자는 다음과 같은 모습입니다:

$$\begin{array}{ccc}
 V_1 & & V_1^\vee \\
 \downarrow T & \text{-----} T^\vee & \uparrow \\
 V_2 & & V_2^\vee
 \end{array}$$

위 예시는 체  $k$ 를 선택된 임의의 대상  $A \in \mathcal{A}$ 로 바꾸어 임의의 범주에서 일반화할 수 있습니다.

**예제 68.4.3 (반변 요네다 함자)**

$\mathcal{A}$  위의 **반변 요네다 함자**(contravariant Yoneda functor)  $H_A: \mathcal{A}^{\text{op}} \rightarrow \text{Set}$ 는  $\mathcal{A}$ 의 대상들이  $A$ 를 어떻게 보는지 기술하는 데 사용됩니다. 각  $X \in \mathcal{A}$ 에 대해

$$H_A(X) := \text{Hom}_{\mathcal{A}}(X, A) \in \text{Set}.$$

로 둡니다.  $\mathcal{A}$ 에서  $X \xrightarrow{f} Y$ 에 대해, 사상  $H_A(f)$ 는 각 화살표  $Y \xrightarrow{p} A \in \text{Hom}_{\mathcal{A}}(Y, A)$ 를 다음으로 보냅니다:

$$X \xrightarrow{f} Y \xrightarrow{p} A \in \text{Hom}_{\mathcal{A}}(X, A)$$

위에서 했던 것처럼 말입니다. 따라서  $H_A(f)$ 는  $\text{Hom}_{\mathcal{A}}(Y, A) \rightarrow \text{Hom}_{\mathcal{A}}(X, A)$ 로 가는 사상입니다. (뒤집힘에 주목하십시오!)

**연습문제 68.4.4.**  $\mathcal{A}^{\text{op}} \times \mathcal{A} \rightarrow \text{Set}$ 가  $(A_1, A_2) \mapsto \text{Hom}(A_1, A_2)$ 로 정의될 때 이것이 실제로 함자라는 주장을 이제 확인해 봅시다.

**§68.5 범주의 동치**

완전충실이며  
본질적으로  
전사

**§68.6 (선택) 자연 변환**

우리는 대상과 사상을 추적하기 위해 범주를 만들었고, 그다음 조금 무모하게 "범주들 사이의 사상은 무엇인가?"라는 질문을 던져 함자를 얻었습니다. 이제 우리는 "함자들 사이의 사상은 무엇인가?"라는 질문을 던져 자연 변환을 얻을 것입니다.

함자들 사이에 화살표를 그린다라는 것이 무섭게 들릴 수도 있지만, 사실 이것은 오래된 발상입니다. 두 경로  $\alpha, \beta: [0, 1] \rightarrow X$ 가 주어졌을 때, 경로  $\alpha$ 를  $\beta$ 로 "연속적으로 변형"하여 경로-호모토피를 만들었던 것을 떠올려 보십시오. 이는 함수  $[0, 1] \times [0, 1] \rightarrow X$ 로 볼 수 있습니다. 자연 변환의 정의도 이와 비슷합니다. 우리는 대상 공간  $\mathcal{B}$  안의 일련의 화살표를 따라  $F$ 를  $G$ 로 끌어당기고자 합니다.

**정의 68.6.1.**  $F, G: \mathcal{A} \rightarrow \mathcal{B}$ 를 두 함자라 합시다.  $F$ 에서  $G$ 로 가는 **자연 변환**  $\alpha$ 는 다음과 같이 표기되며,

$$\begin{array}{ccc} \mathcal{A} & \begin{array}{c} \xrightarrow{F} \\ \Downarrow \alpha \\ \xrightarrow{G} \end{array} & \mathcal{B} \end{array}$$

각  $A \in \mathcal{A}$ 에 대해 사상  $\alpha_A \in \text{Hom}_{\mathcal{B}}(F(A), G(A))$ 로 이루어지고, 이를  $A$ 에서의  $\alpha$ 의 **성분**이라고 부릅니다. 그림으로 나타내면 다음과 같습니다.

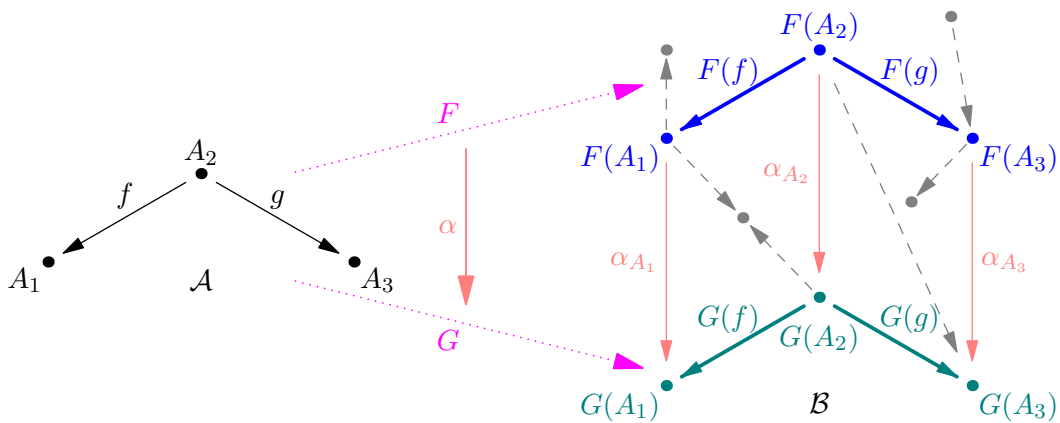
$$\begin{array}{ccc} & F(A) \in \mathcal{B} & \\ & \downarrow \alpha_A & \\ \mathcal{A} \ni A & \begin{array}{c} \xrightarrow{F} \\ \searrow G \end{array} & G(A) \in \mathcal{B} \end{array}$$

이  $\alpha_A$ 들은 임의의  $A_1 \xrightarrow{f} A_2$ 에 대해 다음 도식이 가환한다는 "자연성" 요구 조건을 만족해야 합니다.

$$\begin{array}{ccc}
 F(A_1) & \xrightarrow{F(f)} & F(A_2) \\
 \alpha_{A_1} \downarrow & & \downarrow \alpha_{A_2} \\
 G(A_1) & \xrightarrow{G(f)} & G(A_2)
 \end{array}$$

가환합니다.

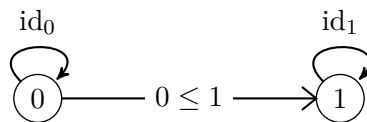
화살표  $\alpha_A$ 는  $F(A)$ 가  $G(A)$ 에 도달하기 위해 취하는 경로를 나타냅니다 (마치  $\alpha$ 에서  $\beta$ 로 가는 경로-호모토피에서 각 점  $\alpha(t)$ 가 연속적으로 점  $\beta(t)$ 로 변형되는 것처럼 말입니다). 그림이 도움이 될 수 있으니 다음을 살펴봅시다.



여기서  $\mathcal{A}$ 는 세 개의 원소와 두 개의 항등이 아닌 화살표  $f, g$ 로 이루어진 작은 범주입니다 (단순화를 위해 항등 화살표는 생략했습니다).  $F$ 와  $G$ 에 의한  $\mathcal{A}$ 의 상은  $\mathcal{B}$ 의 파란색과 초록색 "부분범주"입니다.  $\mathcal{B}$ 가 그 안에 잠재적으로 훨씬 더 많은 대상과 화살표(회색)를 가질 수 있다는 점에 주목하십시오. 자연 변환  $\alpha$ (빨간색)는 각  $F(A)$ 에서 대응하는  $G(A)$ 로 가는  $\mathcal{B}$ 의 화살표를 선택하여,  $F$ 의 상 전체를  $G$ 의 상으로 끌어당깁니다. 마지막으로, 우리는 파란색, 빨간색, 초록색 화살표로 이루어진 어떤 도식이든 가환해야 함을 요구하므로(자연성), 자연 변환은 정말로 "자연스러운" 것입니다.

호모토피와 훨씬 더 비슷해 보이는 두 번째 동치인 정의가 있습니다.

**정의 68.6.2.** 2가 두 원소  $0 \leq 1$ 을 갖는 순서 집합에 의해 생성되는 범주를 나타낸다고 합시다. 즉,



그러면 자연 변환  $\mathcal{A} \begin{matrix} \xrightarrow{F} \\ \Downarrow \alpha \\ \xrightarrow{G} \end{matrix} \mathcal{B}$  은 단지 다음을 만족하는 함수  $\alpha: \mathcal{A} \times \mathbf{2} \rightarrow \mathcal{B}$ 입니다.

$$\alpha(A, 0) = F(A), \quad \alpha(f, 0) = F(f) \quad \text{그리고} \quad \alpha(A, 1) = G(A), \quad \alpha(f, 1) = G(f).$$

더 간결하게 말하면,  $\alpha(-, 0) = F$ ,  $\alpha(-, 1) = G$ 입니다.

이 둘이 동치라는 증명은 연습 문제로 남겨 둡니다.

당연히, 두 자연 변환  $\alpha: F \rightarrow G$ 와  $\beta: G \rightarrow H$ 는 합성될 수 있습니다.

$$\begin{array}{ccc}
 & & F(A) \\
 & \nearrow F & \downarrow \alpha_A \\
 \mathcal{A} \ni A & \xrightarrow{G} & G(A) \\
 & \searrow H & \downarrow \beta_A \\
 & & H(A)
 \end{array}$$

이제  $\alpha_A$ 가 각  $A$ 에 대해 동형사상이 되는 자연 변환  $\alpha$ 가 있다고 합시다. 이런 방식으로, 우리는 이에 대한 역 화살표  $\beta_A$ 를 구성할 수 있습니다.

$$\begin{array}{ccc}
 & & F(A) \in \mathcal{B} \\
 & \nearrow F & \uparrow \alpha_A \\
 \mathcal{A} \ni A & \xrightarrow{G} & G(A) \in \mathcal{B} \\
 & \searrow G & \downarrow \beta_A
 \end{array}$$

이 경우, 우리는  $\alpha$ 를 **자연 동형사상**이라고 부릅니다. 그러면 우리는  $F(A) \cong G(A)$ 가  $A$ 에 대해 **자연스럽게** 성립한다고 말할 수 있습니다. (그리고  $\beta$  역시 동형사상입니다!) 이는 함자  $F$ 와  $G$ 가 "정말로 같다"는 것을 의미합니다. 이들은 대상 수준에서 동형일 뿐만 아니라, 이 동형사상들이 "자연스럽기"까지 합니다. 이 결과로, 우리는 함자들이 자연스럽게 동형이라는 것을 뜻할 때  $F \cong G$ 라고도 씁니다.

이것이 바로 "자연스러운/표준적인 동형사상이 존재한다"고 말할 때 실제로 의미하는 바입니다. 예를 들어, 저는 앞서(문제 15A\*에서) 표준적인 동형사상  $(V^\vee)^\vee \cong V$ 가 존재한다고 주장하면서 "기저를 선택할 필요가 없다"거나 "하늘이 준 것"이라는 등의 말을 얼버무렸습니다. 놀랍게도 범주론은 이를 형식화할 수 있게 해 줍니다. 이는 단지  $(V^\vee)^\vee \cong \text{id}(V)$ 가  $V \in \text{FDVect}_k$ 에 대해 자연스럽게 성립한다고 말하는 것입니다. 실제로, 우리는 다음과 같은 자연 변환을 가집니다.

$$\begin{array}{ccc}
 & \xrightarrow{\text{id}} & \\
 \text{FDVect}_k & \Downarrow \varepsilon & \text{FDVect}_k \\
 & \xrightarrow{(\bullet^\vee)^\vee} &
 \end{array}$$

여기서 성분  $\varepsilon_V$ 는  $v \mapsto \text{ev}_v$ 로 주어집니다 (앞서 논의했듯이, 이것이 동형사상이라는 사실은  $V$ 와  $(V^\vee)^\vee$ 가 같은 차원을 가지며  $\varepsilon_V$ 가 단사라는 사실로부터 따라옵니다).

또 다른 예는 **비고 71.2.8**에서 찾을 수 있습니다.

## §68.7 (선택) 요네다 보조정리

이제 자연 변환을 다루었으니, 다음을 정의할 수 있습니다:

**정의 68.7.1.** 두 범주  $\mathcal{A}$ 와  $\mathcal{B}$ 의 **함자 범주**는  $[\mathcal{A}, \mathcal{B}]$ 로 표기하며, 다음과 같이 정의됩니다:

- $[\mathcal{A}, \mathcal{B}]$ 의 대상은 (공변) 함자  $F: \mathcal{A} \rightarrow \mathcal{B}$ 이고,
- 사상은 자연 변환  $\alpha: F \rightarrow G$ 입니다.

**질문 68.7.2.** 함자 범주에서 두 대상이 동형사상 관계에 있는 것은 언제입니까?

이로써 처음에 언급했던 마지막 예시를 완성할 수 있습니다:

**연습문제 68.7.3.** 다음 함수들을 구성해 봅시다:

- $A \mapsto H_A$ 로 정의되는  $\mathcal{A} \rightarrow [\mathcal{A}^{\text{op}}, \text{Set}]$ 이며, 이를  $H_\bullet$ 이라 부릅니다.
- $A \mapsto H^A$ 로 정의되는  $\mathcal{A}^{\text{op}} \rightarrow [\mathcal{A}, \text{Set}]$ 이며, 이를  $H^\bullet$ 이라 부릅니다.

어느 쪽이든 반대 범주가 등장한다는 점에 주목하십시오.  $H^A$ 가 공변이라는 점이 마음에 들더라도, 사상  $H^\bullet$ 은 반변입니다. 따라서 앞으로는  $H_\bullet$ 을 사용하는 쪽을 선호하겠습니다.

여기서 핵심 관찰은, 범주  $\mathcal{A}$ 가 주어지면  $H_\bullet$ 이 범주  $\mathcal{A}$ 에 이미 “내장”되어 있는 몇몇 특별한 함수  $\mathcal{A}^{\text{op}} \rightarrow \text{Set}$ 를 제공한다는 것입니다. 이를 바탕으로 다음과 같이 정의합니다:

**정의 68.7.4.** **준층**(presheaf)  $X$ 란 그저 반변 함수  $\mathcal{A}^{\text{op}} \rightarrow \text{Set}$ 일 뿐입니다. 어떤  $A$ 에 대해  $X \cong H_A$ 이면 이를 **표현 가능**(representable)하다고 합니다.

다시 말해, 표현 가능성에 대해 생각할 때 우리가 던지는 질문은 다음과 같습니다:

범주  $\mathcal{A}$ 에 이미 “내장”되어 있는 준층은 어떤 종류입니까?

이 질문에 접근하는 한 가지 방법은 다음과 같습니다: 준층  $X$ 와 특정한  $H_A$ 가 주어지면, 자연 변환  $\alpha: X \Rightarrow H_A$ 의 집합을 살펴보고 여기서 무언가 알아낼 수 있는지 확인할 수 있습니다. 실제로 이 집합은 명시적으로 다음과 같이 쓸 수 있습니다:

**정리 68.7.5 (요네다 보조정리)**

$\mathcal{A}$ 를 범주라 하고,  $A \in \mathcal{A}$ 를 하나 택하며,  $H_A$ 를 반변 요네다 함수라 하겠습니다.  $X: \mathcal{A}^{\text{op}} \rightarrow \text{Set}$ 를 반변 함수라 하겠습니다. 그러면 다음 사상은

$$\left\{ \begin{array}{ccc} \text{자연 변환 } \mathcal{A}^{\text{op}} & \begin{array}{c} \xrightarrow{H_A} \\ \Downarrow \alpha \\ \xrightarrow{X} \end{array} & \text{Set} \end{array} \right\} \rightarrow X(A)$$

$\alpha \mapsto \alpha_A(\text{id}_A) \in X(A)$ 로 정의되며,  $\text{Set}$ 의 동형사상(즉, 전단사)입니다. 더 나아가, 등식의 양변을 함수로 볼 때

$$\mathcal{A}^{\text{op}} \times [\mathcal{A}^{\text{op}}, \text{Set}] \rightarrow \text{Set}$$

이 동형사상은 자연스럽습니다.

이는 처음 보면 놀랍게 느껴질 수 있습니다. 그다지 이상한 일이 아닐 수도 있음을 보여주는, 다소 불완전한 설명을 하나 소개하겠습니다: 범주론에서 흔히 통용되는 경험칙은 “같은 유형의 두 대상이 자연스럽게 구성된다면 아마도 같은 것이다”라는 것입니다. 이 주제는 함수와 자연 변환을 정의할 때, 그리고 단순히 합성을 다룰 때도 볼 수 있었습니다. 이제 자연 변환의 집합을 살펴보기 위해, 우리는 원소  $A \in \mathcal{A}$ 와  $X \in [\mathcal{A}^{\text{op}}, \text{Set}]$  한 쌍을 취해 자연 변환의 집합을 구성했습니다. 이 두 정보로부터 집합을 얻는 다른 방법이 있을까요? 있습니다: 그냥  $X(A)$ 를 보면 됩니다. 요네다 보조정리는 여기서도 우리의 경험칙이 여전히 성립함을 말해주고 있습니다.

요네다 보조정리의 몇 가지 따름정리는 [Le14]에 기록되어 있습니다. 이 장이 이미 다소 길어졌으므로, 여기서는 명제만 적어두고 증명은 [Le14]를 참고하도록 하겠습니다.

1. 앞서 언급했듯이,  $H^\bullet$ 은 다음 함수를 제공합니다

$$\mathcal{A} \rightarrow [\mathcal{A}^{\text{op}}, \text{Set}].$$

흥미롭게도 이 함수는 실제로 완전 충실(fully faithful)합니다. 즉, 이는 그야말로 범주  $\mathcal{A}$ 를 오른쪽의 함수 범주 안에 매립합니다(케일리 정리가 모든 군을 치환군 안에 매립하는 것과 매우 유사합니다).

2.  $X, Y \in \mathcal{A}$ 이면

$$H_X \cong H_Y \iff X \cong Y \iff H^X \cong H^Y.$$

이것이 왜 예상되는지 보기 위해, 구체적으로  $\mathcal{A} = \text{Grp}$ 을 생각해 봅시다.  $A, X, Y$ 가 모든  $A$ 에 대해  $H_X(A) \cong H_Y(A)$ 를 만족하는 군이라고 합시다. 예를 들어,

- $A = \mathbb{Z}$ 이면,  $|X| = |Y|$ 입니다.
- $A = \mathbb{Z}/2\mathbb{Z}$ 이면,  $X$ 와  $Y$ 는 위수 2인 원소의 개수가 같습니다.
- ...

각  $A$ 는  $X$ 와  $Y$ 가 어떻게 유사한지에 대한 정보를 주지만, 전체 자연 동형사상은  $X \cong Y$ 를 함의할 만큼 강력합니다.

3. 공변 망각함자  $U: \text{Grp} \rightarrow \text{Set}$ 을 생각해 봅시다.<sup>3</sup> 이것은 다음과 같은 의미에서  $H^{\mathbb{Z}}$ 로 표현될 수 있습니다.

$$\text{Hom}_{\text{Grp}}(\mathbb{Z}, G) \cong U(G) \quad \text{에 의해} \quad \phi \mapsto \phi(1).$$

즉,  $G$ 의 원소들은  $+1$ 의 상(또는 원한다면  $-1$ 의 상)에 의해 결정되는 사상  $\mathbb{Z} \rightarrow G$ 와 전단사 관계에 있습니다. 따라서  $U$ 의 표현은  $\mathbb{Z}$ 를 살펴보고  $+1 \in U(\mathbb{Z})$ 를 선택함으로써 결정되었습니다.

이것의 일반화는 다음과 같습니다:  $\mathcal{A}$ 를 범주,  $X: \mathcal{A} \rightarrow \text{Set}$ 을 공변함자라고 합시다. 그러면 표현  $H^A \cong X$ 는 대상  $A \in \mathcal{A}$ 와 어떤 조건을 만족하는 원소  $u \in X(A)$ 로 구성됩니다. 정리 68.7.5에서 역사상이 무엇인지 안다면 이 조건<sup>4</sup>을 읽어낼 수 있습니다. 위 상황에서는  $X = U$ ,  $A = \mathbb{Z}$ ,  $u = \pm 1$ 입니다.

## §68.8 생각해 볼 만한 조금 더 어려운 문제

**문제 68A.** 자연 변환의 두 정의(하나는  $\mathcal{A} \times \mathbf{2} \rightarrow \mathcal{B}$ 에 관한 것이고, 다른 하나는 사상  $F(A) \xrightarrow{\alpha_A} G(A)$ 에 관한 것)가 동치임을 보이십시오.

**문제 68B.**  $\mathcal{A}$ 를 사상이 집합들 사이의 전단사인 유한집합들의 범주라고 합시다.  $A \in \mathcal{A}$ 에 대해,  $F(A)$ 를  $A$ 의 순열들의 집합,  $G(A)$ 를  $A$  위의 순서들의 집합이라고 합시다.<sup>5</sup>

- (a)  $F$ 와  $G$ 를 함자  $\mathcal{A} \rightarrow \text{Set}$ 로 확장하십시오.
- (b) 모든  $A$ 에 대해  $F(A) \cong G(A)$ 임을 보이되, 이 동형사상은 자연스럽지 않음을 보이십시오.

**문제 68C** (요네다 보조정리 증명하기). 정리 68.7.5의 맥락에서:

- (a) 기술된 사상이 실제로 전단사임을 증명하십시오. (이를 위해서는 아마 역사상을 명시적으로 써 내려가야 할 것입니다.)
-  (b) 이 전단사가 실제로 자연스러움을 증명하십시오. (이는 장황하지만 어렵지는 않습니다. 처음부터 끝까지 할 수 있는 일은 오직 하나뿐입니다.)

<sup>3</sup>사실은 쌍대 버전을 적용해야 합니다. 정리 68.7.5은 반변함자를 사용합니다.

<sup>4</sup>완전성을 위해, 그 조건은 다음과 같습니다: 모든  $A' \in \mathcal{A}$ 와  $x \in X(A')$ 에 대해,  $(Xf)(u) = x$ 를 만족하는 유일한  $f: A \rightarrow A'$ 가 존재합니다.

<sup>5</sup>순열이란 전단사  $A \rightarrow A$ 이고, 순서란 전단사  $\{1, \dots, n\} \rightarrow A$ 이며, 여기서  $n$ 은  $A$ 의 크기입니다.



# 69 범주에서의 극한 (작성 예정)

범주론 장의 초반부에서 여러 화살표를 그려 곱을 구성하는 훌륭한 방법을 살펴보았습니다. 이 개념은 엄청나게 일반화될 수 있음이 밝혀졌으며, 여기서 그 맛보기를 보여드리고자 합니다.

이 장을 전개하기 위해 [Le14]의 접근법을 따릅니다.

서론을 작성하십시오

## §69.1 등화자

이 절의 대표적인 예:  $f, g: X \rightarrow Y$ 의 등화자는  $f(x) = g(x)$ 를 만족하는 점들의 집합입니다.

두 집합  $X$ 와  $Y$ , 그리고 사상  $X \xrightarrow{f, g} Y$ 가 주어졌을 때, 우리는 이들의 등화자를 다음과 같이 정의합니다

$$\{x \in X \mid f(x) = g(x)\}.$$

우리는 이것을 정의하는 범주론적인 방법도 원합니다.

두 대상  $X$ 와  $Y$ 가 있고, 이들 사이에 두 사상  $f$ 와  $g$ 가 있다고 합시다:

$$X \xrightleftharpoons[f]{f} Y$$

이 도식 위의 원뿔은 대상  $A$ 와  $X, Y$  위의 화살표로 이루어지며, 이는 도식을 가환하게 만듭니다. 다음과 같습니다.

$$\begin{array}{ccc} A & & \\ q \downarrow & \searrow f \circ q = g \circ q & \\ X & \xrightleftharpoons[f]{f} & Y \end{array}$$

[Le14]에 따라, 우리는 이 원뿔을 **포크**라고 부릅니다. 이 이름은  $A \rightarrow X \rightrightarrows Y$ 를 한 줄로 나란히 쓸 때 얻어지는 모양에서 유래합니다. 다만 원뿔로서의 성질을 강조하기 위해, 그림에서는 포크를 구부려 그렸습니다.

사실상,  $Y$  위의 화살표는 단지  $f \circ q = g \circ q$ 를 강제할 뿐입니다. 어쨌든, 등화자란  $f$ 와  $g$ 의 “보편적 포크”입니다: 이는 대상  $E$ 와 사상  $E \xrightarrow{e} X$ 로서, 각  $A \xrightarrow{q} X$ 에 대해 다음 도식이

$$\begin{array}{ccc} A & & \\ q \swarrow & \downarrow \exists! h & \searrow \\ X & \xrightleftharpoons[f]{f} & Y \\ e \swarrow & & \searrow \end{array}$$

유일한  $A \xrightarrow{h} E$ 에 대해 가환이 됩니다. 다시 말해, 위와 같은 임의의 사상  $A \xrightarrow{q} X$ 는  $E$ 를 통해 유일하게 분해되어야 합니다.

여기서도 점선 화살표는 생략할 수 있으며, 앞서와 마찬가지로 등화자는 존재하지 않을 수도 있습니다. 하지만 존재하는 경우에는 다음과 같습니다.

**연습문제 69.1.1.**  $E \xrightarrow{e} X$ 와  $E' \xrightarrow{e'} X$ 가 등화자라면,  $E \cong E'$ 임을 보이십시오.

### 예제 69.1.2 (등화자의 예시)

- (a) Set에서,  $X \xrightarrow{f,g} Y$ 가 주어지면 등화자  $E$ 는  $E = \{x \mid f(x) = g(x)\}$ 로 구현될 수 있으며, 포함사상  $e: E \hookrightarrow X$ 가 그 사상이 됩니다. 관례적으로, 남용하여 흔히  $E$  자체를 등화자라고 부르겠습니다.
- (b) Top, Grp에서도 마찬가지입니다. 적절한 구조가 보존되는지 확인해야 합니다(e.g.  $\{\phi(g) = \psi(g) \mid g \in G\}$ 가 군임을 확인해야 합니다).
- (c) 특히, 준동형사상  $\phi: G \rightarrow H$ 가 주어지면, 포함사상  $\ker \phi \hookrightarrow G$ 는  $\phi: G \rightarrow H$ 와 자명한 준동형사상  $G \rightarrow H$ 에 대한 등화자입니다.

(c)에 따르면 등화자는, Grp에서의 자명한 준동형사상처럼 특별히 지정된 "자명한 사상"이 존재할 경우 핵의 개념에 다가갈 수 있게 해줍니다. 이 개념은 아벨 범주에 관한 장에서 자세히 다루겠습니다.

## §69.2 당겨오기 사각형 (작성 예정)

저에게 편지를 써 주십시오.

좋은 예시:  $(-3, 1)$ 과  $(-1, 3)$  위의 미분가능 함수

### 예제 69.2.1

## §69.3 극한

우리는  $X_i$ 의 이산 집합 위의 원뿔(곱을 얻기 위해)과 화살표 쌍 위의 원뿔(포크를 얻기 위해)을 정의했습니다. 대상과 화살표로 이루어진 임의의 일반적인 **도식** 위에서도 원뿔을 정의할 수 있음이 밝혀졌습니다. 이때 각 대상으로 향하는  $A$ 로부터의 사영을 지정하고,  $A$ 로부터의 사영들이 도식 안의 화살표들과 가환할 것을 요구합니다.

이제 원뿔이 보편적이기를 요구하면, 매우 일반적인 **극한**의 정의를 얻게 됩니다. 언제 나처럼, 이들은 유일한 동형사상까지 유일합니다. 같은 방식으로 쌍대 개념인 **쌍대극한**도 정의할 수 있습니다.

## §69.4 생각해 볼 만한 조금 더 어려운 문제

**문제 69A\*** (등화자는 단사 사상입니다). 임의의 도식  $X \rightrightarrows Y$ 의 등화자가 단사 사상임을 보이십시오.

밀어내기 정사각형은 텐서곱을 줍니다

p진

상대 중국인의 나머지 정리!!

# 70 아벨 범주

이 장에서는 좀 더 친숙한 개념들을 범주론적 언어로 번역하겠습니다. 이를 위해서는 우리의 범주에 대한 몇 가지 추가적인 가정이 필요하며, 그 정점에는 이른바 “아벨 범주”의 정의가 있습니다. 이것이 끝나면, “도식 추적”이라는 것이 무엇에 관한 것인지 말씀드릴 수 있을 것입니다.

이 장 전체에서 “ $\hookrightarrow$ ”는 단사 사상을 나타내는 데, “ $\twoheadrightarrow$ ”는 전사 사상을 나타내는 데 사용됩니다.

## §70.1 영 대상, 핵, 여핵, 그리고 상

**이 절의 대표적인 예:** Grp에서, 자명군과 준동형사상이 영 대상과 영 사상입니다.  $G, H$ 가 아벨 군이면  $\phi: G \rightarrow H$ 의 여핵은  $H/\text{im } \phi$ 입니다.

범주의 **영 대상**은 시작 대상이면서 동시에 끝 대상인 대상  $0$ 이며, 물론 유일한 동형사상까지 유일합니다. 예를 들어, Grp에서 영 대상은 자명군이고, Vect $_k$ 에서는 한 점으로 이루어진 0차원 벡터 공간이며, 그런 식으로 계속됩니다.

**질문 70.1.1.** Set과 Top에는 영대상이 없음을 보이십시오.

이 장의 나머지 부분에서는 모든 범주가 영대상을 갖는다고 하겠습니다.

영대상을 갖는 범주  $\mathcal{A}$ 에서, 임의의 두 대상  $A$ 와  $B$ 는 따라서 특별한 사상을 하나 갖습니다

$$A \rightarrow 0 \rightarrow B$$

이는 **영 사상**이라 불리며 마찬가지로  $0$ 으로 표기됩니다. 예를 들어 Grp에서 이는 자명한 준동형사상입니다.

이제 다음과 같이 정의할 수 있습니다:

**정의 70.1.2.** 사상  $A \xrightarrow{f} B$ 를 생각해봅시다. **핵**은 이 사상과 사상  $A \xrightarrow{0} B$ 의 등화자로 정의됩니다. 따라서 이는 다음을 만족하는 사상  $\text{ker } f: \text{Ker } f \hookrightarrow A$ 입니다.

$$\begin{array}{ccc} \text{Ker } f & & \\ \text{ker } f \downarrow \cap & \searrow 0 & \\ A & \xrightarrow{f} & B \end{array}$$

가 가환하며, 게다가 같은 성질을 갖는 다른 어떤 사상도  $\text{Ker } f$ 를 통해 유일하게 분해됩니다 (즉 이 성질에 대해 보편적입니다). **문제 69A\***에 의해  $\text{ker } f$ 는 단사 사상이며, 이것이 “ $\hookrightarrow$ ”의 사용을 정당화합니다.

우리는 사상을 나타내는 데  $\text{ker } f$ 를, 대상을 나타내는 데  $\text{Ker } f$ 를 사용하고 있음에 주목하십시오. 마찬가지로 쌍대 개념인 여핵을 정의합니다:

**정의 70.1.3.** 사상  $A \xrightarrow{f} B$ 를 생각해 봅시다.  $f$ 의 **여핵**은 다음을 만족하는 사상  $\text{coker } f: B \twoheadrightarrow \text{Coker } f$ 입니다

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ & \searrow 0 & \downarrow \text{coker } f \\ & & \text{Coker } f \end{array}$$

가 가환하며, 게다가 같은 성질을 갖는 다른 어떤 사상도  $\text{Coker } f$ 를 통해 유일하게 분해됩니다(즉 이 성질에 대해 보편적입니다). 따라서 이는 이 사상과 사상  $A \xrightarrow{0} B$ 의 “쌍대등화자”입니다. **문제 69A\***의 쌍대에 의해  $\text{coker } f$ 는 전사 사상이며, 이것이 “ $\rightarrow$ ”의 사용을 정당화합니다.

사상  $A \xrightarrow{f} B$ 의 여핵을 “ $f$ 의 상으로 나눈  $B$ ”라고 생각하십시오.

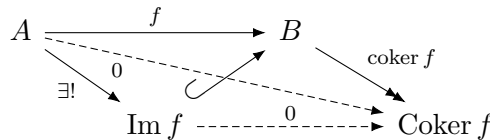
#### 예제 70.1.4 (여핵)

사상  $\mathbb{Z}/6\mathbb{Z} \rightarrow D_{12} = \langle r, s \mid r^6 = s^2 = 1, rs = sr^{-1} \rangle$ 을 생각해 봅시다. 그러면  $\text{Grp}$ 에서 이 사상의 여핵은  $D_{12}/\langle r \rangle \cong \mathbb{Z}/2\mathbb{Z}$ 입니다.

준동형사상의 상이 일반적으로 공역에서 정규가 아닐 수 있으므로, 이는 항상 우리가 원하는 대로 되지는 않습니다. 그럼에도 불구하고 이를 이용하여 다음을 정의할 수 있습니다:

**정의 70.1.5.**  $A \xrightarrow{f} B$ 의 **상**은  $\text{coker } f$ 의 핵입니다. 이를  $\text{Im } f = \text{Ker}(\text{coker } f)$ 로 표기합니다. 이로부터 유일한 사상  $\text{im } f: A \rightarrow \text{Im } f$ 가 주어집니다.

이것이 존재할 때, 이는 우리의 구체적인 “상”의 개념과 일치합니다. 그림으로 나타내면:



$\text{Im } f$ 의 보편성에 의해, 전체 도식을 가환하게 만드는 유일한 사상  $\text{im } f: A \rightarrow \text{Im } f$ 가 존재함을 알 수 있음에 주목하십시오.

## §70.2 가법 범주와 아벨 범주

**이 절의 대표적인 예:**  $\text{Ab}$ ,  $\text{Vect}_k$ , 또는 더 일반적으로  $\text{Mod}_R$ .

이제 가법 범주와 아벨 범주의 개념을 정의할 수 있으며, 이는 이 개념이 가장 유용하게 쓰이는 범주의 유형입니다.

**정의 70.2.1. 가법 범주**  $\mathcal{A}$ 란 다음을 만족하는 것입니다:

- $\mathcal{A}$ 는 영대상을 가지며, 임의의 두 대상은 곱을 가집니다.
- 더 중요한 것은: 모든  $\text{Hom}_{\mathcal{A}}(A, B)$ 가 (가법적으로 표기된) 아벨 군을 이루며, 합성이 덧셈에 대해 분배된다는 것입니다:

$$(g + h) \circ f = g \circ f + h \circ f \quad \text{그리고} \quad f \circ (g + h) = f \circ g + f \circ h.$$

영 사상이 각 군의 항등원 역할을 합니다.

요컨대:

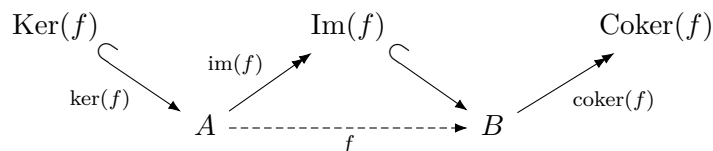
**가법 범주에서는 두 사상을 더할 수 있습니다.**

어차피 이는 원소에 대해 이야기할 수 없는 상황에서 유일하게 말이 되는 정의입니다.

**정의 70.2.2. 아벨 범주**  $\mathcal{A}$ 란 임의의 사상  $A \xrightarrow{f} B$ 에 대해 다음과 같은 추가적인 성질을 갖는 것입니다,

- 핵과 여핵이 존재하고,
- 사상이 상을 통해 인수분해되어  $\text{im}(f)$ 가 전사 사상이 되는 것입니다.

그러면, 이는 다음 도식을 낳습니다



### 예제 70.2.3 (아벨 범주의 예시)

- $\text{Vect}_k$ ,  $\text{Ab}$ 는 아벨 범주이며, 여기서  $f + g$ 는 통상적인 의미를 가집니다.
- 이를 일반화하면,  $R$ -가군의 범주  $\text{Mod}_R$ 은 아벨 범주입니다.
- $\text{Grp}$ 는 가법 범주조차 되지 못하는데, 사상 쌍에 교환 가능한 덧셈을 부여할 방법이 없기 때문입니다.

이제부터는 가법 범주는 기본적으로 잊어도 되며, 우리는 아벨 범주에서 작업하게 될 것입니다.

일반적으로, 어떤 범주가 아벨 범주라고 가정하면, 이러한 핵, 여핵, ... 이 가질 것으로 기대하는 모든 성질이 실제로 성립합니다. 예를 들면,

### 명제 70.2.4 (단사 사상 $\iff$ 자명한 핵)

사상  $A \xrightarrow{f} B$ 가 단사 사상인 것은 그 핵이  $0 \rightarrow A$ 인 것과 동치입니다. 쌍대적으로,  $A \xrightarrow{f} B$ 가 전사 사상인 것은 그 여핵이  $B \rightarrow 0$ 인 것과 동치입니다.

증명. 쉬운 방향은 다음과 같습니다:

**연습문제 70.2.5.**  $A \xrightarrow{f} B$ 가 단사 사상이면  $0 \rightarrow A$ 가 핵임을 보이십시오. (이는 비아벨 범주에서도 성립합니다.)

물론 핵은 동형사상까지 유일하므로, 단사 사상  $\implies 0$  핵입니다. 반대로,  $0 \rightarrow A$ 가  $A \xrightarrow{f} B$ 의 핵이라고 가정합시다. 이를 위해 이제 기저 준동형사상들의 군 구조를 활용할 수 있습니다. 다음 도식을 가정합시다.

$$Z \begin{array}{c} \xrightarrow{g} \\ \xrightarrow{h} \end{array} A \xrightarrow{f} B$$

가환이라고 가정합시다. 그러면  $(g - h) \circ f = g \circ f - h \circ f = 0$ 이 되어, 우리는 가환 도식에 도달하게 됩니다.

$$\begin{array}{ccc} Z & & \\ g-h \downarrow & \searrow 0 & \\ A & \xrightarrow{f} & B \end{array}$$

그러나  $0 \rightarrow A$ 가 핵이므로  $g - h$ 가 0을 통해 인수분해되며, 따라서  $g - h = 0 \implies g = h$ 이고, 이는 곧  $f$ 가 단사 사상임을 뜻합니다.  $\square$

**명제 70.2.6 (동형사상  $\iff$  단사 사상이면서 전사 사상)**

아벨 범주에서, 어떤 사상이 동형사상인 것과 그것이 단사 사상이면서 전사 사상인 것은 동치입니다.

증명. 생략합니다. (뒤에서 제시되는 미첼 매장 정리는 어차피 작은 부분 범주를 살펴봄으로써, 우리가 관심을 갖는 대부분의 상황에 대해 이를 함의합니다.)  $\square$

**§70.3 완전열**

**이 절의 대표적인 예:**  $0 \rightarrow G \rightarrow G \times H \rightarrow H \rightarrow 0$ 은 완전합니다.

완전열은 호몰로지 군에 대해 배우기 전까지는 극도로 동기가 부족해 보일 것인데, 호몰로지 군은 완전열이 등장하는 가장 자연스러운 곳 중 하나입니다. 이를 감안하면, 호몰로지 군에 관한 장을 이 장과 동시에 읽어보는 것이 도움이 될 수 있습니다.

먼저, 일반적인 범주론적 정의의 동기를 제공하기 위해 군에 대한 정의를 서술하겠습니다. 다음과 같은 군의 열은

$$G_0 \xrightarrow{f_1} G_1 \xrightarrow{f_2} G_2 \xrightarrow{f_3} \dots \xrightarrow{f_n} G_n$$

$f_k$ 의 상이  $f_{k+1}$ 의 핵일 때  $G_k$ 에서 완전이라고 합니다. 수열 전체가  $k = 1, \dots, n-1$ 에서 완전이면 그 수열 전체가 완전이라고 합니다.

**예제 70.3.1 (완전열)**

(a) 다음 열은

$$0 \rightarrow \mathbb{Z}/3\mathbb{Z} \xrightarrow{\times 5} \mathbb{Z}/15\mathbb{Z} \rightarrow \mathbb{Z}/5\mathbb{Z} \rightarrow 0$$

완전합니다. 사실,  $0 \rightarrow G \hookrightarrow G \times H \rightarrow H \rightarrow 0$ 은 일반적으로 완전합니다. (여기서 0은 자명군을 나타냅니다.)

(b) 군에 대해, 사상  $0 \rightarrow A \rightarrow B$ 가 완전한 것은  $A \rightarrow B$ 가 단사인 것과 동치입니다.

(c) 군에 대해, 사상  $A \rightarrow B \rightarrow 0$ 이 완전한 것은  $A \rightarrow B$ 가 전사인 것과 동치입니다.

원형적인 예시를 살펴보면, 사실 **짧은 완전열** ( $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  형태의 완전열)은 세상에서 가장 자연스러운 것입니다:

**이는 기본적으로 그저 방정식  $C = B/A$ 일 뿐입니다.**

“짧은 완전열  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ 이 존재한다”는 표현을 볼 때마다, 이를 머릿속으로 “ $C \cong B/A$ ”로 번역할 수 있습니다. 다만 약간의 차이가 있습니다: 군은 숫자보다 더 많은 구조를 가지므로, 이 열은 사상에 대한 정보도 담고 있습니다 —  $A$ 를  $B$ 의 부분군으로 식별하는 사상, 그리고  $C$ 를 몫군  $B/A$ 로 식별하는 사상 말입니다.

**예제 70.3.2 (더 많은 완전열)**

(a) 다음 열은

$$0 \rightarrow \mathbb{Z} \xrightarrow{\times 3} \mathbb{Z} \rightarrow \mathbb{Z}/3\mathbb{Z} \rightarrow 0$$

짧게 완전합니다.

(b) 다음도 마찬가지로입니다

$$0 \rightarrow \mathbb{Z} \xrightarrow{\times 5} \mathbb{Z} \rightarrow \mathbb{Z}/5\mathbb{Z} \rightarrow 0.$$

보시다시피, “ $C \cong B/A$ ”라는 서술된 방정식은 완전히 정확하지는 않으며,  $C$ 가 무엇인지를 결정하는 데에는 사상  $A \rightarrow B$ 도 중요합니다. 이는 흔히 쓰이는 표기법도 설명해줍니다: 사상  $\mathbb{Z} \xrightarrow{\times 3} \mathbb{Z}$ 의 상은 보통  $3\mathbb{Z}$ 로 표기되며, 따라서  $\mathbb{Z}/3\mathbb{Z} = \frac{\mathbb{Z}}{3\mathbb{Z}}$ 입니다.

이제, 이 정의를 일반적인 아벨 범주  $\mathcal{A}$ 에서 모방하고자 합니다. 그러므로,  $A \xrightarrow{f} B \xrightarrow{g} C$ 가 완전할 때에 대한 기준을 적어봅시다. 우선  $g \circ f = 0$ 이어야 하는데, 이는  $\text{im}(f) \subseteq \text{ker}(g)$ 라는 사실을 나타냅니다. 관련된 모든 대상을 추가하면, 아래의 가환 도식을 얻습니다.

$$\begin{array}{ccccc} A & & \xrightarrow{0} & & C \\ & \searrow f & & \nearrow g & \\ & & B & & \\ \text{im } f & \xrightarrow{\iota} & & & \text{Ker } g \\ & \nearrow \exists! & & \searrow & \\ & & \text{Im } f & \xrightarrow{\quad} & \text{Ker } g \end{array}$$

여기서 사상  $A \twoheadrightarrow \text{Im } f$ 는 전사 사상인데,  $\mathcal{A}$ 가 아벨 범주라고 가정하고 있기 때문입니다. 따라서, 다음이 성립합니다

$$0 = (g \circ \iota) \circ \text{im } f = g \circ (\iota \circ \text{im } f) = g \circ f = 0$$

하지만  $\text{im } f$ 가 전사 사상이므로, 이는  $g \circ \iota = 0$ 을 의미합니다. 그러므로 유일한 사상  $\text{Im } f \rightarrow \text{Ker } g$ 가 존재하며, 우리는 이 도식이 가환할 것을 요구합니다. 요컨대,

**정의 70.3.3.**  $\mathcal{A}$ 를 아벨 범주라 합시다. 다음 열은

$$\cdots \rightarrow A_{n-1} \xrightarrow{f_n} A_n \xrightarrow{f_{n+1}} A_{n+1} \rightarrow \cdots$$

$f_{n+1} \circ f_n = 0$ 이고 표준 사상  $\text{Im } f_n \rightarrow \text{Ker } f_{n+1}$ 이 동형사상이면  $A_n$ 에서 **완전**합니다. 전체 열은 각  $A_i$ 에서 완전하면 완전합니다. (유한열의 경우 맨 처음과 맨 마지막 대상에는 조건을 부과하지 않습니다.)

**연습문제 70.3.4.** 이전과 마찬가지로,  $0 \rightarrow A \rightarrow B$ 가 완전열인 것  $\iff A \rightarrow B$ 가 단사 사상인 것임을 보이십시오.

## §70.4 프레이드-미첼 매장 정리

이제 프레이드-미첼 매장 정리를 소개하는데, 이는 본질적으로 임의의 아벨 범주가 구체적인 범주로 실현될 수 있음을 말합니다.

**정의 70.4.1.** 범주는  $\text{obj}(\mathcal{A})$ 가 (클래스가 아니라) 집합일 때, 즉 “ $\mathcal{A}$ 의 모든 대상들의 집합”이 존재할 때 **작다**고 합니다. 예를 들어,  $\text{Set}$ 은 모든 집합들의 집합이 존재하지 않으므로 작지 않습니다.

### 정리 70.4.2 (프레이드-미첼 매장 정리)

$\mathcal{A}$ 를 작은 아벨 범주라 합시다. 그러면 (1을 가지지만 가환이 아닐 수도 있는) 환  $R$ 과, 왼쪽  $R$ -가군의 범주로 가는 충만하고 충실하며 완전한 함자가 존재합니다.

여기서 함자는 완전열을 보존할 때 **완전**하다고 합니다. 이 정리가 좋은 이유는 다음을 의미하기 때문입니다.

**임의의 아벨 범주에서 성립하는 온갖 이상한 정의들을 대체로 잊어버릴 수 있습니다.**

아벨 범주에 관한 명제를 마주할 때는 언제나, 단사/전사/핵/상/완전 등이 여러분의 기존 개념과 일치하는 "구체적인" 범주에 대해서만 증명하면 충분합니다.

**비고 70.4.3** — "작다"는 조건은  $\mathcal{A}$ 의 대상들이 실제로 집합을 이루도록 요구하는 기술적 장애물입니다. 저는 이 구별을 무시하겠는데, 충분한 집합론적 기교를 부리면 이를 거의 항상 우회할 수 있기 때문입니다.

예를 들어, 다음을 증명해 봅시다.

**보조정리 70.4.4 (짧은 다섯 개 보조정리)**

아벨 범주에서 다음의 가환 도식을 생각합시다.

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \xrightarrow{p} & B & \xrightarrow{q} & C \longrightarrow 0 \\ & & \cong \downarrow \alpha & & \downarrow \beta & & \cong \downarrow \gamma \\ 0 & \longrightarrow & A' & \xrightarrow{p'} & B' & \xrightarrow{q'} & C' \longrightarrow 0 \end{array}$$

위쪽과 아래쪽 행이 완전하다고 가정합시다.  $\alpha$ 와  $\gamma$ 가 동형사상이면,  $\beta$ 도 동형사상입니다.

증명. 우리는  $\beta$ 가 전사 사상임을 증명합니다 (단사 사상을 얻는 증명도 비슷합니다). 매장 정리에 의해 이 범주를 어떤  $R$ 에 대한  $R$ -가군으로 취급할 수 있습니다. 이는 우리 범주를  $R$ -가군으로 구체적으로 해석하여 그림 속 원소들을 이리저리 옮기는, 이른바 "도식 추적"을 할 수 있게 해줍니다.

$b'$ 를  $B'$ 의 원소라 합시다. 그러면  $c' := q'(b') \in C'$ 이고,  $\gamma$ 가 전사이므로  $\gamma(c) = c'$ 인  $c$ 가 있으며, 마지막으로  $q(b) = c$ 인  $b \in B$ 가 있습니다. 그림:

$$\begin{array}{ccc} b \in B & \xrightarrow{q} & c \in C \\ \beta \downarrow & & \cong \downarrow \gamma \\ b' \in B' & \xrightarrow{q'} & c' \in C' \end{array}$$

그런데  $\beta(b) = b'$ 가 반드시 성립하는 것은 아닙니다. 하지만 도식이 가환이므로 적어도 다음이 성립합니다.

$$q'(b') = q'(\beta(b))$$

따라서  $b' - \beta(b) \in \text{Ker } q' = \text{Im } p'$ 이고,  $p'(a') = b' - \beta(b)$ 인  $a' \in A'$ 가 존재합니다. 이제  $\alpha$ 를 이용하여 이를  $a \in A$ 로 끌어올립니다. 그림:

$$\begin{array}{ccc} a \in A & & b \in B \\ \downarrow & & \\ a' \in A' & \xrightarrow{\quad} & b' - \beta(b) \in B' \xrightarrow{\quad} 0 \in C \end{array}$$

그러면 다음을 얻습니다.

$$\beta(b + p(a)) = \beta b + \beta p a = \beta b + p' \alpha a = \beta b + (b' - \beta b) = b'$$

따라서  $b' \in \text{Im } \beta$ 이며, 이로써  $\beta$ 가 전사임의 증명이 완성됩니다.  $\square$

일반적으로, (매장 정리를 사용하든 사용하지 않든) 위와 같은 스타일의 증명은 종종 도식 추적이라는 이름으로 불립니다. 이 용어에 정확한 정의가 있는지는 잘 모르겠지만, 다음은 알루피[A109]의 인용문입니다.

범 보조정리 [문제 70C\*]를 증명하는 일은 공개적으로 해서는 안 되는 일이며, 다른 사람들이 읽도록 검증의 세부 사항을 적어 두는 것은 악명 높게도 쓸모없습니다. 그 세부 사항들은 본질적으로 모두 자명하지만, 순식간에 표기법의 수렁으로 빠져들게 됩니다. 이러한 증명들은 통틀어 도식 추적이라는 스포츠로 알려져 있으며, 칠판 위 도식의 서로 다른 부분들을 여러 손가락으로 가리키면서 자신이 다루고 있는 원소들을 소리 내어 말하고 그것들의 운명을 진술하는 방식으로 가장 잘 수행됩니다.

## §70.5 긴 완전열 쪼개기

**이 절의 대표적인 예:** 제1 동형사상 정리.

실제로, 임의의 완전열은 짧은 완전열들로 나뉜다는 것이 밝혀집니다. 이는 다음에 의존합니다:

### 명제 70.5.1 (아벨 범주에서의 "제1 동형사상 정리")

$A \xrightarrow{f} B$ 를 아벨 범주의 사상이라 합시다. 그러면 다음과 같은 완전열이 존재합니다

$$0 \rightarrow \text{Ker } f \xrightarrow{\text{ker } f} A \xrightarrow{\text{im } f} \text{Im } f \rightarrow 0.$$

### 예제 70.5.2

아벨 범주의 두 가지 예시에서 이 정리를 분석해 봅시다:

- (a) 아벨 군의 범주에서, 이는 본질적으로 제1 동형사상 정리입니다.
- (b) 범주  $\text{Vect}_k$ 에서, 이는 계수-퇴화차수 정리, 정리 9.7.7에 해당합니다.

따라서, 임의의 완전열은 다음과 같이 짧은 완전열들로 나뉠 수 있습니다

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \searrow & & \searrow & & \searrow \\
 & & & C_n & & & C_{n+2} \\
 & & \swarrow & & \swarrow & & \swarrow \\
 & & 0 & & 0 & & 0 \\
 \dots & \xrightarrow{\quad} & A_{n-1} & \xrightarrow{f_{n-1}} & A_n & \xrightarrow{f_n} & A_{n+1} & \xrightarrow{f_{n+1}} & \dots \\
 & \searrow & \swarrow & & \searrow & & \swarrow & & \\
 & & C_{n-1} & & C_{n+1} & & & & \\
 & \swarrow & \searrow & & \swarrow & & \searrow & & \\
 & 0 & & 0 & & 0 & & 0 & 
 \end{array}$$

여기서 모든  $k$ 에 대해  $C_k = \text{im } f_{k-1} = \text{ker } f_k$ 입니다.

## §70.6 생각해 볼 만한 조금 더 어려운 문제

**문제 70A** (네 보조정리). 아벨 범주에서, 다음 가환 도식을 고려합시다

$$\begin{array}{ccccccc}
 A & \xrightarrow{p} & B & \xrightarrow{q} & C & \xrightarrow{r} & D \\
 \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow & & \delta \downarrow \\
 A' & \xrightarrow{p'} & B' & \xrightarrow{q'} & C' & \xrightarrow{r'} & D'
 \end{array}$$

여기서 첫 번째와 두 번째 행은 완전합니다.  $\alpha$ 가 전사 사상이고,  $\beta$ 와  $\delta$ 가 단사 사상이면,  $\gamma$ 가 단사 사상임을 증명하십시오.



**문제 70B** (다섯 보조정리). 아벨 범주에서, 다음 가환 도식을 고려하십시오

$$\begin{array}{ccccccccc}
 A & \xrightarrow{p} & B & \xrightarrow{q} & C & \xrightarrow{r} & D & \xrightarrow{s} & E \\
 \alpha \downarrow & & \beta \downarrow & & \gamma \downarrow & & \delta \downarrow & & \varepsilon \downarrow \\
 A' & \xrightarrow{p'} & B' & \xrightarrow{q'} & C' & \xrightarrow{r'} & D' & \xrightarrow{s'} & E'
 \end{array}$$

여기서 두 행은 완전하고,  $\beta$ 와  $\delta$ 는 동형사상이며,  $\alpha$ 는 전사 사상이고,  $\varepsilon$ 는 단사 사상입니다.  $\gamma$ 가 동형사상임을 증명하십시오.



**문제 70C\*** (뱀 보조정리). 아벨 범주에서, 다음 도식을 고려하십시오

$$\begin{array}{ccccccc}
 A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\
 \downarrow a & & \downarrow b & & \downarrow c & & \\
 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C'
 \end{array}$$

여기서 첫 번째와 두 번째 행은 완전열입니다. 다음과 같은 완전열이 존재함을 증명하십시오

$$\text{Ker } a \rightarrow \text{Ker } b \rightarrow \text{Ker } c \rightarrow \text{Coker } a \rightarrow \text{Coker } b \rightarrow \text{Coker } c.$$

**문제 70D** (아벨 범주가 아닌 가법 범주). 다음과 같은 범주를 고려하십시오:

- 대상은  $A$ 가  $B$ 의 부분군인 아벨 군의 쌍  $(B, A)$ 입니다.
- 사상  $(B, A) \rightarrow (B', A')$ 은  $f^{\text{img}}(A) \subseteq A'$ 을 만족하는 사상  $f: B \rightarrow B'$ 입니다.

(이는 [장 73](#)에서 본 PairTop 범주와 유사하다고 생각할 수 있습니다. 여기서는 범주를 가법적으로 만들기 위해 아벨 군을 사용합니다.)

이 범주는 아벨 군의 짧은 완전열  $0 \rightarrow A \rightarrow B \rightarrow B/A \rightarrow 0$ 의 범주로 동등하게 볼 수 있습니다.

사상  $(X, 0) \rightarrow (X, X)$ 가 단사 사상이자 전사 사상이지만 동형사상은 아님을 보이십시오. 이 범주가 아벨 범주가 아니라는 결론을 내리십시오.

# XVIII

대수적 위상수학 II: 호몰로지

## 제XVIII부: 목차

|           |                                |            |
|-----------|--------------------------------|------------|
| <b>71</b> | <b>특이 호몰로지</b>                 | <b>727</b> |
| 71.1      | 단체와 경계 . . . . .               | 727        |
| 71.2      | 특이 호몰로지 군 . . . . .            | 728        |
| 71.3      | 호몰로지 함자와 사슬 복합체 . . . . .      | 733        |
| 71.4      | 사슬 복합체의 더 많은 예시 . . . . .      | 737        |
| 71.5      | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 739        |
| <b>72</b> | <b>긴 완전열</b>                   | <b>741</b> |
| 72.1      | 짧은 완전열과 네 가지 예시 . . . . .      | 741        |
| 72.2      | 호몰로지 군의 긴 완전열 . . . . .        | 743        |
| 72.3      | 마이어-피토리스 완전열 . . . . .         | 745        |
| 72.4      | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 751        |
| <b>73</b> | <b>절제와 상대 호몰로지</b>             | <b>753</b> |
| 73.1      | 동기 . . . . .                   | 753        |
| 73.2      | 긴 완전열 . . . . .                | 754        |
| 73.3      | 쌍의 범주 . . . . .                | 755        |
| 73.4      | 절단 . . . . .                   | 757        |
| 73.5      | 몇 가지 응용 . . . . .              | 758        |
| 73.6      | 차원의 불변성 . . . . .              | 759        |
| 73.7      | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 760        |
| <b>74</b> | <b>보너스: 세포 호몰로지</b>            | <b>761</b> |
| 74.1      | 차수 . . . . .                   | 761        |
| 74.2      | 세포 사슬 복합체 . . . . .            | 762        |
| 74.3      | 여담: 왜 호몰로지 군들이 같은가? . . . . .  | 764        |
| 74.4      | 응용: 베타 수를 통한 오일러 지표 . . . . .  | 766        |
| 74.5      | 세포 경계 공식 . . . . .             | 767        |
| 74.6      | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 770        |
| <b>75</b> | <b>특이 코호몰로지</b>                | <b>773</b> |
| 75.1      | 코사슬 복합체 . . . . .              | 773        |
| 75.2      | 공간의 코호몰로지 . . . . .            | 774        |
| 75.3      | 공간들의 코호몰로지는 함자적입니다 . . . . .   | 775        |
| 75.4      | 보편 계수 정리 . . . . .             | 776        |
| 75.5      | 보편 계수 정리에 대한 설명 . . . . .      | 777        |
| 75.6      | 코호몰로지 군 계산 예시 . . . . .        | 778        |
| 75.7      | 코호몰로지 군의 시각화 . . . . .         | 780        |
| 75.8      | 상대 코호몰로지 군 . . . . .           | 783        |
| 75.9      | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 784        |
| <b>76</b> | <b>코호몰로지의 응용</b>               | <b>785</b> |
| 76.1      | Poincaré 쌍대성 . . . . .         | 785        |
| 76.2      | 드람 코호몰로지 . . . . .             | 785        |
| 76.3      | 등급 환 . . . . .                 | 787        |
| 76.4      | 컵곱 . . . . .                   | 789        |
| 76.5      | 상대 코호몰로지 유사환 . . . . .         | 792        |
| 76.6      | 빼기합 . . . . .                  | 793        |
| 76.7      | 교차곱 . . . . .                  | 795        |
| 76.8      | Künneth 공식 . . . . .           | 799        |
| 76.9      | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 801        |

# 71 특이 호몰로지

이제  $\pi_1(X)$ 를 정의했으므로, 같은 개념을 포착하는 두 번째 방법인  $H_1(X)$ 로 관심을 돌리겠습니다. 그런 다음  $n \geq 2$ 에 대해  $H_n(X)$ 를 정의하겠습니다.  $H_n$  군의 좋은 점은,  $\pi_n$  군과 달리 실제로 계산하기가 훨씬 쉽다는 것입니다. 단점은 그 정의에 상당히 많은 준비가 필요하며, "대수적 위상수학"의 "대수적" 부분이 훨씬 더 기술적이 된다는 것입니다.

## §71.1 단체와 경계

**이 절의 대표적인 예:**  $\partial[v_0, v_1, v_2] = [v_0, v_1] - [v_0, v_2] + [v_1, v_2]$ .

먼저 가장 기본적인 것부터 시작하겠습니다.

**정의 71.1.1.** 표준  $n$ -단체는  $\Delta^n$ 으로 표기하며, 다음과 같이 정의됩니다.

$$\{(x_0, x_1, \dots, x_n) \mid x_i \geq 0, x_0 + \dots + x_n = 1\}.$$

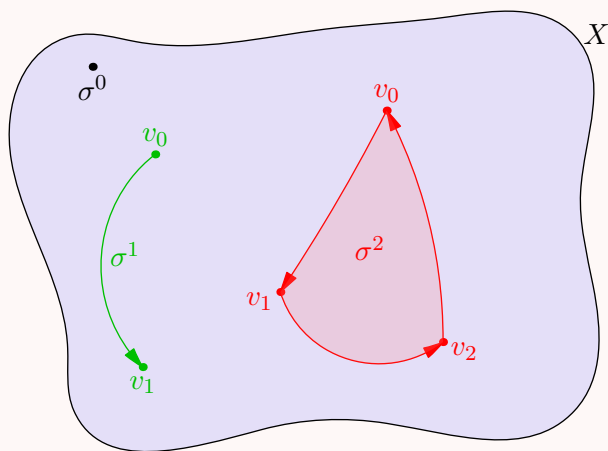
따라서 이것은 몇몇 꼭짓점  $[v_0, \dots, v_n]$ 의 볼록 껍질입니다. 곧 명확해질 이유로 인해 꼭짓점의 순서  $v_0, \dots, v_n$ 를 유지하고 있음에 유의하십시오.

위상 공간  $X$ 가 주어졌을 때, 특이  $n$ -단체는 사상  $\sigma: \Delta^n \rightarrow X$ 입니다.

### 예제 71.1.2 (특이 단체)

- (a)  $\Delta^0 = [v_0]$ 는 단지 하나의 점이므로,  $X$ 의 특이 0-단체는 단지  $X$ 의 한 점입니다.
- (b)  $\Delta^1 = [v_0, v_1]$ 은 하나의 구간이므로,  $X$ 의 특이 1-단체는 단지  $X$ 의 경로입니다.
- (c)  $\Delta^2 = [v_0, v_1, v_2]$ 는 정삼각형이므로,  $X$ 의 특이 2-단체는  $X$  안의 "원판"처럼 보입니다.

다음은 공간  $X$  안에서 세 가지 모두를 나타낸 그림입니다.



화살표가 꼭 필요한 것은 아니지만, 꼭짓점의 "순서"를 추적하는 데 도움이 되도록 포함했습니다. 이는 곧 유용하게 쓰일 것입니다.

이제 스토크스 정리를 논할 때와 매우 비슷한 작업을 하겠습니다. 특이  $n$ -단체에 경계  $\partial$  연산자를 부여하겠습니다. 이를 통해  $n$ -단체의 형식적 선형합  $\sum_k a_k \sigma_k$ 를 얻게 되는데, 이를  $n$ -사슬이라고 부릅니다.

이 경우

**정의 71.1.3.** 꼭짓점이  $[v_0, \dots, v_n]$ 인 특이  $n$ -단체  $\sigma$ 가 주어졌을 때, 모든  $i$ 에 대해  $(n-1)$ -단체  $[v_0, \dots, v_{i-1}, v_{i+1}, \dots, v_n]$ 이 있음에 유의하십시오. **경계 연산자**  $\partial$ 은 다음과 같이 정의됩니다.

$$\partial(\sigma) := \sum_i (-1)^i [v_0, \dots, v_{i-1}, v_{i+1}, \dots, v_n].$$

경계 연산자는 그런 다음  $n$ -사슬로 선형적으로 확장됩니다.

$$\partial\left(\sum_k a_k \sigma_k\right) := \sum_k a_k \partial(\sigma_k).$$

관례상, 0-사슬은 빈 경계를 가집니다.

#### 예제 71.1.4 (경계 연산자)

예제 71.1.2에 나타낸 사슬들을 생각해 봅시다. 그러면

- (a)  $\partial\sigma^0 = 0$ .
- (b)  $\partial(\sigma^1) = [v_1] - [v_0]$ : 이는 점  $v_1$ 에 대응하는 0-사슬과 점  $v_0$ 에 대응하는 0-사슬의 "차"입니다.
- (c)  $\partial(\sigma^2) = [v_0, v_1] - [v_0, v_2] + [v_1, v_2]$ ; 즉, 이는  $\sigma^2$ 의 "변"을 이루는 세 방향 화살표의 합으로 생각할 수 있습니다.
- (d) 다시 경계를 취하면 다음을 얻는다는 점에 주목하십시오.

$$\begin{aligned} \partial(\partial(\sigma^2)) &= \partial([v_0, v_1]) - \partial([v_0, v_2]) + \partial([v_1, v_2]) \\ &= ([v_1] - [v_0]) - ([v_2] - [v_0]) + ([v_2] - [v_1]) \\ &= 0. \end{aligned}$$

$\partial^2 = 0$ 이라는 사실은 물론 우연이 아닙니다.

#### 정리 71.1.5 ( $\partial^2 = 0$ )

임의의 사슬  $c$ 에 대해,  $\partial(\partial(c)) = 0$ 입니다.

증명. 문제 45B와 본질적으로 동일합니다: 이는 그저 여러 개의  $\sum$  기호를 써 내려가는 문제일 뿐입니다. 성실한 독자라면 직접 계산을 시도해 보셔도 좋습니다.  $\square$

**비고 71.1.6** — 미분 형식을 적분하는 데 사용되는 사슬과 호몰로지에서의 사슬 사이의 기묘한 유사성은 우연이 아닙니다. 훨씬 나중에 다룰 드람 코호몰로지가 이 관계를 명시적으로 밝혀 줄 것입니다.

## §71.2 특이 호몰로지 군

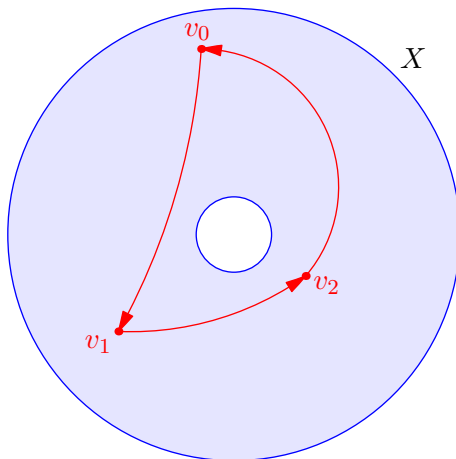
이 절의 대표적인 예: 아마도  $H_n(S^m)$ 일 것이며, 특히  $m = n = 1$ 인 경우일 것입니다.

$X$ 를 위상 공간이라 하고,  $C_n(X)$ 를 앞서 정의한  $X$ 의  $n$ -사슬들의 자유 아벨 군이라 합시다. 위에서 한 작업으로부터 경계 연산자  $\partial$ 을 얻게 되므로, 다음과 같은 사상들의 열을 갖습니다

$$\dots \xrightarrow{\partial} C_3(X) \xrightarrow{\partial} C_2(X) \xrightarrow{\partial} C_1(X) \xrightarrow{\partial} C_0(X) \xrightarrow{\partial} 0$$

(여기서 0은 자명군을 나타내는 데 사용하고 있으며, 이는 아벨 군에 대한 표준 표기법입니다.) 이를 **특이 사슬 복합체**라 부르겠습니다.

이제, 이것이 공간의 구멍을 어떻게 탐지할 수 있게 해 줄까요? 그 이유를 보기 위해, 빨간색으로 그려진 1-사슬  $c$ 를 가진 환형(annulus)을 살펴봅시다:



다음에 주목하십시오

$$\partial c = ([v_1] - [v_0]) - ([v_2] - [v_0]) + ([v_2] - [v_1]) = 0$$

그러므로 이 1-사슬  $c$ 는 자명한 경계를 가지므로 "사이클(cycle)"이라고 말할 수 있습니다. 그러나  $c$  자체는 어떤 2-사슬의 경계도 아닌데, 이는 공간 중심에 구멍이 있기 때문입니다 —  $c$ 의 내부를 "채워 넣는" 것이 불가능합니다! 따라서 우리는 다음과 같은 대수적 사실을 통해 구멍을 탐지한 것입니다

$$c \in \ker(C_1(X) \xrightarrow{\partial} C_0(X)) \quad \text{그러나} \quad c \notin \text{im}(C_2(X) \xrightarrow{\partial} C_1(X)).$$

실제로, 만약 구멍이 존재하지 않았다면 이 명제는 거짓이었을 것입니다.

**비고 71.2.1** — 호모토피와 호몰로지는 "구멍"에 대해 다소 다른 개념을 포착한다는 점에 유의하십시오. 예를 들어,  $T$ 를 토러스라고 합시다. 그러면 모든 사상  $S^2 \rightarrow T$ 는 널호모토픽(nulhomotopic)이므로  $\pi_2(T)$ 는 자명하지만, **명제 72.3.6**에서 보게 되듯이  $H_2(T) \cong \mathbb{Z}$ 입니다.

적어도  $n = 1$ 인 경우에는, **정리 71.2.7**에 따르면 임의의 경로 연결 공간  $X$ 와  $x_0 \in X$ 에 대해  $H_1(X)$ 는  $\pi_1(X, x_0)$ 의 아벨화가 되며, 이는 기대할 수 있는 최선의 결과에 가깝습니다 —  $H_1(X)$ 는 반드시 아벨 군이어야 하는 반면,  $\pi_1(X, x_0)$ 은 아벨 군일 필요가 없습니다. 그럼에도 불구하고,  $\pi_1(X, x_0)$ 이 자명하지 않으면서  $H_1(X)$ 가 자명한 경우도 여전히 가능합니다 — 예시는 <https://math.stackexchange.com/q/1052414>를 참고하십시오.

이 아이디어는 다음과 같이 임의의 차원에서 포착할 수 있습니다.

**정의 71.2.2.** 다음을 봅시다

$$\dots \xrightarrow{\partial} C_2(X) \xrightarrow{\partial} C_1(X) \xrightarrow{\partial} C_0(X) \xrightarrow{\partial} 0$$

위와 같습니다.  $c \in C_n(X)$ 가 다음과 같다고 말합니다:

- $c \in \ker \left( C_n(X) \xrightarrow{\partial} C_{n-1}(X) \right)$ 이면 **사이클(cycle)**이라 하고,
- $c \in \operatorname{im} \left( C_{n+1}(X) \xrightarrow{\partial} C_n(X) \right)$ 이면 **경계(boundary)**라 합니다.

사이클과 경계를 각각  $Z_n(X), B_n(X) \subseteq C_n(X)$ 로 표기합니다.<sup>1</sup>

**질문 71.2.3.** 표기법에 익숙해지기 위해:  $B_n$ 과  $Z_n$ 이 그 자체로 아벨 군이며,  $B_n(X) \subseteq Z_n(X) \subseteq C_n(X)$ 임을 확인해 보십시오.

핵심은 이제 다음을 정의할 수 있다는 것입니다:

**정의 71.2.4.**  $n$ 번째 호몰로지 군  $H_n(X)$ 는 다음과 같이 정의됩니다

$$H_n(X) := Z_n(X)/B_n(X).$$

**예제 71.2.5 (영번째 호몰로지 군)**

위상 공간  $X$ 에 대해  $H_0(X)$ 를 계산해 봅시다.  $C_0(X)$ 를 취하는데, 이는 그저  $X$ 의 점들의 형식적 선형합입니다.

먼저  $\partial: C_0(X) \rightarrow 0$ 의 핵을 생각해 보면,  $\partial$ 의 핵은 공간  $C_0(X)$  전체입니다. 즉, 모든 점이 "순환"입니다.

그렇다면 경계는 무엇일까요? 핵심 아이디어는  $[b] - [a] = 0$ 인 것과  $a$ 에서  $b$ 로 이어지는 1-사슬이 존재하는 것, 즉  $a$ 에서  $b$ 로 가는 경로가 존재하는 것이 동치라는 점입니다. 특히,

$$X \text{가 경로 연결됨} \implies H_0(X) \cong \mathbb{Z}.$$

더 일반적으로, 다음이 성립합니다

**명제 71.2.6 (호몰로지 군은 경로 연결 성분으로 분리됩니다)**

$X = \bigcup_{\alpha} X_{\alpha}$ 가 경로 연결 성분으로의 분해라면,

$$H_n(X) \cong \bigoplus_{\alpha} H_n(X_{\alpha}).$$

가 성립합니다. 특히,  $X$ 가  $r$ 개의 경로 연결 성분을 가진다면,  $H_0(X) \cong \mathbb{Z}^{\oplus r}$ 입니다.

( $\mathbb{Z}^{\oplus r}$ 을 보고 놀랐다면, 아벨 군은  $\mathbb{Z}$ -가군과 같은 것이므로,  $G, H$ 가 아벨 군일 때  $G \times H$  대신  $G \oplus H$ 라는 표기를 관용적으로 사용한다는 점을 기억하십시오.)

이제 첫 번째 호몰로지 군을 살펴봅시다.

**정리 71.2.7 (후레비치 정리)**

$X$ 가 경로 연결이라고 합시다. 그러면  $H_1(X)$ 는  $\pi_1(X, x_0)$ 의 아벨화입니다.

이를 증명하지는 않겠지만, 예시로부터 대략적으로 확인할 수 있습니다. 군  $H_1(X)$ 는  $\pi_1(X, x_0)$ 와 동일한 정보를 담고 있습니다. ( $Z_1(X)$ 에서의) 순환은  $\pi_1(X, x_0)$ 에서 다뤘던 고리와 같은 것에 대응하며, ( $B_1(X)$ 에서의, 즉 우리가 나누는 대상인) 경계는 정확히  $\pi_1(X, x_0)$

<sup>1</sup> $C_n(X)$ 를 사이클을 나타내는 데 쓰지 않는 이유는, 이미 그 표기법이 사용 중이라는 명백한 이유 외에도, 문자  $Z$ 가 독일어 단어 "Zyklus"에서 유래했기 때문입니다.

에서의 널호모토픽 고리에 해당합니다. 차이점은  $H_1(X)$ 에서는 고리들이 교환 가능하지만,  $\pi_1(X, x_0)$ 에서는 그렇지 않다는 것입니다.

**비고 71.2.8 (여담: 범주론적 해석)** — 이로부터, 각  $(X, x_0)$ 에 대해 후레비치 사상  $\pi_1(X, x_0) \xrightarrow{\phi} H_1(X)$ 가 존재한다고 말할 수 있습니다. 하지만 그 이상의 사실이 있습니다. 이 사상은 자연스러운데, 점을 가진 공간 사이의 사상  $h: (X, x_0) \rightarrow (Y, y_0)$ 에 대해 다음이

$$\begin{array}{ccc} \pi_1(X, x_0) & \xrightarrow{h_{\#}} & \pi_1(Y, y_0) \\ \downarrow \phi & & \downarrow \phi \\ H_1(X) & \xrightarrow{h_*} & H_1(Y) \end{array}$$

가환한다는 의미입니다.

범주론의 용어로,  $\phi$ 는  $\pi_1$ 에서  $H_1$ 로 가는 자연 변환이라고 말합니다.

이를 달리 표현하면 다음과 같습니다. 우리는 군들의 모임을 가지고 있고

$$\{\pi_1(X, x_0) \mid (X, x_0) \text{ 점을 가진 공간}\}$$

그리고

$$\{H_1(X) \mid (X, x_0) \text{ 점을 가진 공간}\}$$

이때 자연 변환  $\phi$ 는 준동형사상들의 모임으로 볼 수 있습니다.

$$\{\phi: \pi_1(X, x_0) \rightarrow H_1(X) \mid (X, x_0) \text{ 점을 가진 공간}\}$$

자연성 조건을 만족하는

물론,  $\pi_1$ 이 함자라는 사실은 **정리 65.6.2**에서 설명했듯이  $\{\pi_1(X, x_0) \mid (X, x_0) \text{ 점을 가진 공간}\}$ 가 점을 가진 공간으로 색인된 군들의 모임보다 훨씬 더 많은 것을 의미한다는 것을 뜻합니다.

### 예제 71.2.9 (환면의 첫 번째 호몰로지 군)

구체적인 예를 들기 위해, 위의 환면  $X$ 를 생각해봅시다. 우리는  $X$ 의 구멍을 한 바퀴 감는 사슬  $c$ 를 찾았습니다. 요점은 실제로

$$H_1(X) = \langle c \rangle \cong \mathbb{Z}$$

사슬  $c, 2c, \dots$ 는  $H_1(X)$ 에서 모두 서로 다르지만, 다른 모든 1-사슬은 이들 중 하나와 동치라는 것입니다. 이는  $X$ 가 사실상  $S^1$ 과 같다는 사실을 담아냅니다.

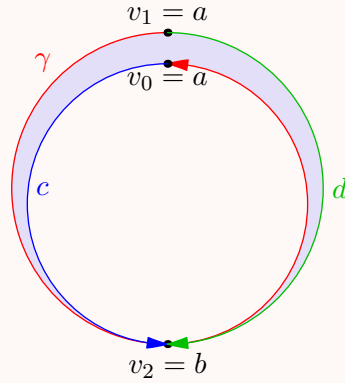
### 예제 71.2.10 ( $S^1$ 에서의 명시적인 경계)

$X = S^1$ 에서,  $a$ 를 가장 위쪽 점,  $b$ 를 가장 아래쪽 점이라고 합시다.  $c$ 를 원의 왼쪽 절반을 따라  $a$ 에서  $b$ 로 가는 단체,  $d$ 를 원의 오른쪽 절반을 따라  $a$ 에서  $b$ 로 가는 단체라고 합시다. 마지막으로,  $\gamma$ 를  $S^1$ 을 반시계 방향으로 한 바퀴 감으며  $a$ 에서 자기 자신으로 가는 고리  $\gamma$ 를 나타내는 단체라고 합시다.  $H_1(S^1)$ 에서 다음이 성립한다고

주장합니다.

$$\gamma = c - d$$

이는 기하학적으로  $c - d$ 가 원을 한 바퀴 감는 것을 나타낸다는 뜻이며, (당연히 우리가 예상하는 바입니다).



실제로 이는 위 그림에서 확인할 수 있는데, 여기서 우리는 경계가 정확히  $\gamma - c + d$ 인 2-단체를 그렸습니다. 이 그림은 다소 비유적입니다. 실제로는  $v_0 = v_1 = a$ 이며, 전체 2-단체는  $S^1$  안에 내장되어 있습니다. 특히 호몰로지라는 이름이 붙은 이유가 바로 이것인데, 단체의 상이 때때로 상당히 “특이하게” 보일 수 있기 때문입니다.

#### 예제 71.2.11 (숫자 8 모양 도형의 첫 번째 호몰로지 군)

$X_8$ 을 생각해봅시다 (예제 65.2.9 참고). 호몰로지와 호모토피 모두  $X_8$  안의 두 고리를 인식하며, 이들을  $a$ 와  $b$ 라고 부릅니다. 차이점은  $\pi_1(X_8, x_0)$ 에서는 이 두 고리가 교환하는 것이 허용되지 않는다는 것입니다.  $\pi_1$ 에서의 군 연산이 “경로를 이어붙이는” 것이기 때문에  $ab \neq ba$ 입니다. 하지만 호몰로지 군  $H_1(X)$ 에서는  $a$ 와  $b$ 를 형식적으로 더해서 1-사슬  $a + b$ 를 얻는 방식으로 더합니다. 따라서

$$H_1(X) \cong \mathbb{Z}^{\oplus 2} \quad \text{한편} \quad \pi_1(X, x_0) = \langle a, b \rangle.$$

입니다.

#### 예제 71.2.12 ( $S^2$ 의 호몰로지 군)

$S^2$ , 즉 이차원 구를 생각해 봅시다. 경로 연결되어 있으므로  $H_0(S^2) = \mathbb{Z}$ 입니다. 또한  $\pi_1(S^2)$ 가 자명한 것과 같은 이유로  $H_1(S^2) = 0$ 입니다. 반면 우리는 다음과 같이 주장합니다.

$$H_2(S^2) \cong \mathbb{Z}.$$

$H_2(S^2)$ 의 원소들은  $S^2$ 를 사면체 모양의 자루로 감싸는 것(또는 두 개의 자루, 세 개의 자루 등)에 대응합니다. 따라서 두 번째 호몰로지 군을 통해  $S^2$ 의 구형 공동을 감지할 수 있습니다.<sup>a</sup>

<sup>a</sup>비교 71.2.1에서 언급했듯이,  $\pi_2$ 와 달리  $H_2$ 는 구형뿐만 아니라 다른 종류의 공동도 감지합니다.

사실 더 일반적으로는 다음이 성립함이 밝혀집니다.

$$H_n(S^m) \cong \begin{cases} \mathbb{Z} & n = m \text{ 또는 } n = 0 \\ 0 & \text{그렇지 않으면.} \end{cases}$$

**예제 71.2.13 (수축 가능한 공간)**

임의의 수축 가능한 공간  $X$ 가 주어지면, 다음이 성립함이 밝혀집니다.

$$H_n(X) \cong \begin{cases} \mathbb{Z} & n = 0 \\ 0 & \text{그렇지 않으면.} \end{cases}$$

그 이유는 호모토피 군과 마찬가지로 호몰로지 군 역시 호모토피 불변량이기 때문임이 밝혀집니다. (이는 다음 절에서 증명하겠습니다.) 따라서 수축 가능한  $X$ 의 호몰로지 군은 한 점 공간의 호몰로지 군과 같으며, 이는 위에서 언급한 것들입니다.

**예제 71.2.14 (원환면의 호몰로지 군)**

당분간은 증명할 수 없겠지만, 다음이 성립함이 밝혀집니다.

$$H_n(S^1 \times S^1) \cong \begin{cases} \mathbb{Z} & n = 0, 2 \\ \mathbb{Z}^{\oplus 2} & n = 1 \\ 0 & \text{그렇지 않으면.} \end{cases}$$

1에서의 호몰로지 군은  $\pi_1(S^1 \times S^1) \cong \mathbb{Z}^2$ 이라는 우리가 아는 사실에 대응하며, 2에서의 호몰로지 군은 원환면의 "공동"을 감지합니다.

이는 아주 멋진 이야기이지만, 실제로 호몰로지 군을 어떻게 계산할 수 있을까요? 이는 다소 긴 이야기가 될 것이며, 실제로 호몰로지 군을 계산할 수 있게 되기까지는 상당한 양의 대수학과 기하학을 다뤄야 합니다. 앞으로는 어떤 것이 순수하게 대수적인지(임의의 사슬 복합체에 대해 성립하는지), 그리고 어떤 부분이 실제로 기하학적으로 참인 사실을 말하고 있는지를 계속 구분해 두는 것이 종종 도움이 될 것입니다.

## §71.3 호몰로지 함자와 사슬 복합체

앞서 언급했듯이 호몰로지 군은 호모토피 불변량입니다. 이는 함자  $\pi_1: \mathbf{hTop}_* \rightarrow \mathbf{Grp}$ 를 만들기 위해 했던 작업과 비슷한 과정이 될 것입니다. 천천히 진행하다가 마지막에 가서야 범주론이라는 커튼을 젖혀 드러내는 대신, 이번에는 시간을 절약하기 위해 처음부터 범주론으로 시작하겠습니다.

**정의 71.3.1.** 범주  $\mathbf{hTop}$ 은 다음과 같이 정의됩니다.

- 대상: 위상 공간.
- 사상: 사상  $X \rightarrow Y$ 의 호모토피 동치류.

특히,  $X$ 와  $Y$ 가 호모토피 동치일 때, 오직 그때만  $\mathbf{hTop}$ 에서 동형입니다.

이는  $\mathbf{hTop}_*$ 와 같지만 기준점이 없다는 점만 다르다는 것을 알 수 있습니다.

**정리 71.3.2** (호몰로지는 함자  $\mathbf{hTop} \rightarrow \mathbf{Ab}$ 입니다)

임의의 특정한  $n$ 에 대해,  $H_n$ 은 함자  $\mathbf{hTop} \rightarrow \mathbf{Ab}$ 입니다. 특히,

- 임의의 사상  $f: X \rightarrow Y$ 가 주어지면, 유도된 사상  $f_*: H_n(X) \rightarrow H_n(Y)$ 를 얻습니다.
- 호모토피 동치인 두 사상  $f, g: X \rightarrow Y$ 에 대해  $f_* = g_*$ 입니다.
- 호모토피 동치인 두 공간  $X$ 와  $Y$ 는 동형인 호몰로지 군을 가집니다. 즉,  $f: X \rightarrow Y$ 가 호모토피 동치이면  $f_*: H_n(X) \rightarrow H_n(Y)$ 는 동형사상입니다.
- (여기에 여러분이 좋아하는 함자에 관한 결과를 넣으십시오.)

이를 위해서는 사상  $f: X \rightarrow Y$ 를 취해 사상  $H_n(f): H_n(X) \rightarrow H_n(Y)$ 를 얻는 방법을 기술해야 합니다. 그런 다음 이 사상이 호모토피의 선택에 의존하지 않음을 보여야 합니다. (이는 앞서  $f_{\#}$ 에 대해 했던 작업과 유사한 것입니다.) 이번에는 이를 증명하는 것이 훨씬 까다로운 것으로 밝혀지며, 처음에 구축한 사슬 복합체  $C_{\bullet}(X)$ 로 다시 돌아가야 합니다.

**§71.3.i 사슬 복합체의 대수학**

대수학부터 시작해 봅시다. 먼저, 복합체를 임의의 아벨 군의 수열로 일반화한 다음과 같은 추상화를 정의하겠습니다. 사실 이는 ( $\mathbf{AbGrp}$ 뿐만 아니라) 임의의 범주에서 성립합니다. 전략은 다음과 같습니다. 필요한 모든 것을 완전히 추상적으로 정의한 다음, 우리가 원하는 기하학적 개념들이 이 설정에 대응함을 보이겠습니다.

**정의 71.3.3.** **사슬 복합체**는 군  $A_n$ 들과 사상들의 수열입니다.

$$\dots \xrightarrow{\partial} A_{n+1} \xrightarrow{\partial} A_n \xrightarrow{\partial} A_{n-1} \xrightarrow{\partial} \dots$$

이때 인접한 두 사상의 합성은 영 사상이 됩니다. 이를 보통  $A_{\bullet}$ 로 표기합니다.

$n$ 번째 호몰로지 군  $H_n(A_{\bullet})$ 은  $\ker(A_n \rightarrow A_{n-1}) / \operatorname{im}(A_{n+1} \rightarrow A_n)$ 으로 정의됩니다. 사이클과 경계는 이전과 같은 방식으로 정의됩니다.

이는 분명히 앞서 살펴본 구조를, 원래의 기하학적 맥락에서 완전히 벗어나 대수적으로 일반화한 것에 지나지 않습니다.

**정의 71.3.4.** **사슬 복합체의 사상**(또는 사슬 사상)  $f: A_{\bullet} \rightarrow B_{\bullet}$ 은 다음 도식이 성립하도록 하는, 모든  $n$ 에 대한 사상  $f_n$ 들의 수열입니다.

$$\begin{array}{ccccccc} \dots & \xrightarrow{\partial_A} & A_{n+1} & \xrightarrow{\partial_A} & A_n & \xrightarrow{\partial_A} & A_{n-1} \xrightarrow{\partial_A} \dots \\ & & \downarrow f_{n+1} & & \downarrow f_n & & \downarrow f_{n-1} \\ \dots & \xrightarrow{\partial_B} & B_{n+1} & \xrightarrow{\partial_B} & B_n & \xrightarrow{\partial_B} & B_{n-1} \xrightarrow{\partial_B} \dots \end{array}$$

가환입니다. 이 정의 아래에서 사슬 복합체들의 모임은 범주가 되며, 이를  $\mathbf{Cmplx}$ 로 표기합니다.

사슬 복합체의 사상  $f: A_{\bullet} \rightarrow B_{\bullet}$ 이 주어지면,  $A_n$ 의 모든 사이클은  $B_n$ 의 사이클로 보내진다는 점에 주목하십시오. 왜냐하면 다음 사각형이

$$\begin{array}{ccc} A_n & \xrightarrow{\partial_A} & A_{n-1} \\ f_n \downarrow & & \downarrow f_{n-1} \\ B_n & \xrightarrow{\partial_B} & B_{n-1} \end{array}$$

가환이기 때문입니다. 마찬가지로,  $A_n$ 의 모든 경계는  $B_n$ 의 경계로 보내집니다. 따라서,

$f: A_\bullet \rightarrow B_\bullet$ 인 모든 사상은 모든  $n$ 에 대해 사상  $f_*: H_n(A) \rightarrow H_n(B)$ 를 줍니다.

**연습문제 71.3.5.**  $H_n$ 을 함자  $\text{Cmplx} \rightarrow \text{Grp}$ 로 해석하십시오.

다음으로, 두 사상  $f$ 와  $g$ 가 호모토픽하다는 것이 무엇을 의미하는지 정의하고자 합니다. 그 답은 다음과 같습니다.

**정의 71.3.6.**  $f, g: A_\bullet \rightarrow B_\bullet$ 이라 합시다. 다음이 성립하도록 하는, 모든  $n$ 에 대한 사상  $P_n: A_n \rightarrow B_{n+1}$ 을 찾을 수 있다고 가정합니다.

$$g_n - f_n = \partial_B \circ P_n + P_{n-1} \circ \partial_A$$

그러면  $P$ 는  $f$ 에서  $g$ 로의 **사슬 호모토피**이며,  $f$ 와  $g$ 는 **사슬 호모토픽**합니다.

이를 그림으로 나타낼 수 있습니다(주의: 대각선의 점선 화살표들은 다른 모든 화살표와 가환하지 않습니다).

$$\begin{array}{ccccccc}
 \cdots & \xrightarrow{\partial_A} & A_{n+1} & \xrightarrow{\partial_A} & A_n & \xrightarrow{\partial_A} & A_{n-1} \xrightarrow{\partial_A} \cdots \\
 & & \downarrow g-f & \nearrow P_n & \downarrow g-f & \nearrow P_{n-1} & \downarrow g-f \\
 \cdots & \xrightarrow{\partial_B} & B_{n+1} & \xrightarrow{\partial_B} & B_n & \xrightarrow{\partial_B} & B_{n-1} \xrightarrow{\partial_B} \cdots
 \end{array}$$

정의는, 각 기울어진 "평행사변형"에서  $g-f$  화살표가 양변을 따르는 두 합성의 합이 된다는 것입니다.

**비고 71.3.7** — 이 방정식은 지금으로서는 그것이 올바른 대수적 작용을 한다는 것을 곧 보이려 한다는 사실을 제외하면 전혀 동기가 없어 보일 것입니다. 이 방정식의 유도는 다음 절까지 미뤄둔 기하학적 맥락에서 비롯되며, 그곳에서 "호모토피"가 자연스럽게 "사슬 호모토피"를 낳게 됩니다.

이제, 이 정의의 요점은 다음과 같습니다

**명제 71.3.8** (사슬 호모토픽 사상은 호몰로지 군에서 동일한 사상을 유도합니다)

$f, g: A_\bullet \rightarrow B_\bullet$ 를 사슬 호모토픽 사상  $A_\bullet \rightarrow B_\bullet$ 라 합시다. 그러면 유도된 사상  $f_*, g_*: H_n(A_\bullet) \rightarrow H_n(B_\bullet)$ 는 각  $n$ 에 대해 일치합니다.

증명. 이는  $g-f$ 가 호몰로지 군 위에서 영 사상을 준다는 것을 보이는 것과 동치입니다. 다시 말해,  $A_n$ 의 모든 사이클이  $g-f$ 에 의해  $B_n$ 의 경계가 됨을 확인해야 합니다.

**질문 71.3.9.** 이것이 참임을 확인하십시오. □

### §71.3.ii 사슬 복합체의 기하학

이제 위 그림의 기하학적 세부 사항을 채워 넣어 봅시다. 먼저:

**보조정리 71.3.10 (공간의 사상  $\implies$  특이 사슬 복합체의 사상)**

각  $f: X \rightarrow Y$ 는 사상  $C_n(X) \rightarrow C_n(Y)$ 를 유도합니다.

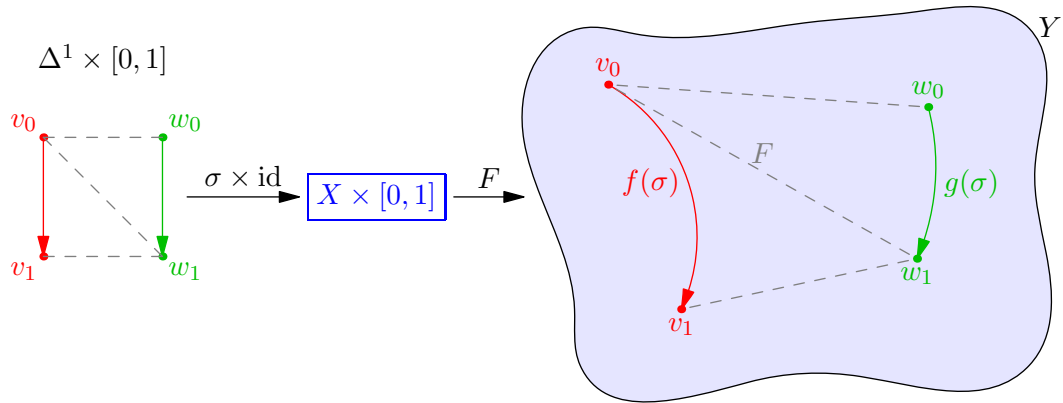
증명. 다음 합성을 생각해봅시다

$$\Delta^n \xrightarrow{\sigma} X \xrightarrow{f} Y.$$

다시 말해,  $X$ 의 경로가  $Y$ 의 경로가 되는 등입니다. ( $\partial$ 이 관여하는 사각형들이 가환함을 확인하는 것은 어렵지 않습니다; 원한다면 직접 확인해 보십시오.)  $\square$

이제 우리가 보여야 할 것은  $f, g: X \rightarrow Y$ 가 호모토픽이면 이들이 사슬 호모토픽이라는 것입니다. 사슬 호모토픽을 만들어내기 위해서는, 모든  $n$ -단체  $X$ 를  $Y$ 에서의  $(n+1)$ -사슬로 보내는 사상, 즉  $P_n$ 을 정의해야 합니다.

어떻게 이를 해낼 수 있을지 생각해봅시다.  $n$ -단체  $\sigma: \Delta^n \rightarrow X$ 를 취하여  $f$ 와  $g$ 를 통과시켜봅시다; 아래 그림은 공간  $Y$ 로 사상된 1-단체  $\sigma$ (즉  $X$ 에서의 경로)를 나타낸 것입니다. 호모토피란  $F(-, 0) = f$ 이고  $F(-, 1) = g$ 를 만족하는 사상  $F: X \times [0, 1] \rightarrow Y$ 가 존재함을 뜻하며, 그 일부를 아래  $Y$ 에 대한 그림에서 회색 화살표로 나타내었습니다.



이 그림은 우리가 어떻게 나아가야 할지를 시사합니다: 우리는 지금까지 그려온 1-사슬들로부터  $Y$  위의 2-사슬을 만들어내고자 합니다. 호모토피  $F$ 는  $Y$  위에 "사각형" 구조, 즉  $v_0, v_1, w_1, w_0$ 로 둘러싸인 사각형을 제공합니다. 우리는 이를 두 개의 삼각형으로 나눕니다; 그것이 바로 우리의 2-사슬입니다.

이를 형식적으로 만들기 위해서는  $\Delta^1 \times [0, 1]$ (이는 실제로 사각형입니다)을 취하여 두 개의 삼각형으로 나누면 됩니다. 그런 다음  $\sigma \times \text{id}$ 를 적용하면  $X \times [0, 1]$ 에서의 2-사슬을 얻게 되고, 마지막으로  $F$ 를 적용하면 모든 것이 우리 공간  $Y$ 로 사상됩니다. 우리 예제에서 최종 상은 두 개의 삼각형으로 이루어진 2-사슬이며, 이는 우리 그림에서  $[v_0, w_0, w_1] - [v_0, v_1, w_1]$ 로 쓸 수 있습니다; 그 경계는 빨강, 초록, 회색으로 주어집니다.

더 일반적으로,  $n$ -단체  $\phi = [x_0, \dots, x_n]$ 에 대해 이른바 프리즘 연산자  $P_n$ 을 다음과 같이 정의합니다. 각  $i$ 에 대해  $v_i = f(x_i)$ 이고  $w_i = g(x_i)$ 로 둡시다. 그러면 다음과 같이 정의합니다

$$P_n(\phi) := \sum_{i=0}^n (-1)^i (F \circ (\phi \times \text{id})) [v_0, \dots, v_i, w_i, \dots, w_n].$$

이는 앞서의 구성을  $n > 1$ 인 차원으로 일반화한 것에 불과합니다; 우리는  $\Delta^n \times [0, 1]$ 을  $n+1$ 개의 단체로 나누고,  $\phi \times \text{id}$ 에 의해  $X$ 로 사상한 다음 전체를  $Y$ 로 밀어넣습니다.  $(-1)^i$ 는 "대각선" 면들이 서로 상쇄되도록 보장합니다.

이제 모든  $\sigma$ 에 대해 다음이 성립함을 주장합니다,

$$\partial_Y(P_n(\sigma)) = g(\sigma) - f(\sigma) - P_{n-1}(\partial_X \sigma).$$

그림에서  $\partial_Y \circ P_n$ 은 프리즘 전체의 경계입니다(그림에서 이는 빨강, 초록, 회색 선이 되며, 상쇄되는 대각선 회색은 포함하지 않습니다).  $g - f$ 는 초록에서 빨강을 뺀 것이고,  $P_{n-1} \circ \partial_X$ 는 프리즘의 회색 모서리들을 나타냅니다( $v_1$ 에서  $w_0$ 로 가는 대각선은 포함하지 않습니다). 실제로 (그저 여러 개의  $\Sigma$  기호를 적어보는 것만으로도) 위 항등식이 성립함을 확인할 수 있습니다.

그림으로 나타내면:

$$g(\sigma) - f(\sigma) = \partial_Y(P_n(\sigma)) + P_{n-1}(\partial_X(\sigma))$$

이로써  $f$ 에서  $g$ 로 가는 사슬 호모토피가 주어지며, 정리 71.3.2의 증명이 완성됩니다.

## §71.4 사슬 복합체의 더 많은 예시

이제 이 장을 마무리하며 사슬 복합체의 몇 가지 예시를 더 제시하고자 하며, 이는 다음 장에서 위상적 호몰로지 군을 마침내 계산하는 데 사용할 것입니다.

### 예제 71.4.1 (축소 호몰로지 군)

$X$ 가 (공집합이 아닌) 위상 공간이라고 합시다. 표준 특이 복합체를 다음과 같이 증대할 수 있습니다: 이전과 같은 방식을 그대로 사용하되, 끝부분에  $\mathbb{Z}$ 를 추가하여 증대시키며, 다음과 같습니다:

$$\cdots \rightarrow C_1(X) \rightarrow C_0(X) \xrightarrow{\varepsilon} \mathbb{Z} \rightarrow 0$$

여기서  $\varepsilon$ 는 점  $p_i \in X$ 에 대해  $\varepsilon(\sum n_i p_i) = \sum n_i$ 로 정의됩니다. (0-사슬은 그저 점들의 형식적 합임을 기억하십시오!) 이를 **증대 특이 사슬 복합체**라 부르고  $\tilde{C}_\bullet(X)$ 로 표기합니다.

이는 무작위적인 일처럼 보일 수 있지만, 우리가 처음 시작했던 정의들을 취하여 "거꾸로 일반화"함으로써 정당화할 수 있습니다.  $n$ -단체는  $n+1$ 개의 꼭짓점  $[v_0, \dots, v_n]$ 으로 주어짐을 기억하십시오. 이는  $(-1)$ -단체가 0개의 꼭짓점, 즉  $\square$ 로 주어짐을 시사합니다!

표준  $n$ -단체의 정의에  $n = -1$ 을 대입해도 같은 결론에 도달합니다.  $\Delta^{-1}$ 은 좌표가 모두 음이 아니며 합이 1인 점들로 이루어진  $\mathbb{R}^0$ 의 부분집합이어야 합니다. 그러한 점은 존재하지 않으므로,  $\Delta^{-1} = \{\}$ 입니다. 따라서 위상 공간  $X$ 가 주어졌을 때,  $X$ 에서의 특이  $(-1)$ -단체는 함수  $\{\} \rightarrow X$ 여야 합니다. 그러한 함수는 하나 존재합니다: 상이 공집합인 공함수입니다.

즉, 모든 위상 공간  $X$ 는 정확히 하나의  $(-1)$ -단체를 가지며, 이를  $\{\}$ 와 동일시합니다. 따라서  $(-1)$ 번째 사슬 군  $C_{-1}(X)$ 는 하나의 원소로 생성된 자유 아벨 군입니다; 즉  $\tilde{C}_{-1}(X) \cong \mathbb{Z}$ 입니다(여기서 이 동형사상은  $\{\}$ 를 1과 동일시합니다).

경계는 어떨까요? 단체  $[v_0, \dots, v_n]$ 의 경계를 취하기 위해서는, 각 꼭짓점을 하나씩 제거하고 교대합을 취합니다. 따라서  $\partial([v]) = \emptyset$ 입니다. 이를 복합체에 선형적으로 확장하면  $\partial(\sum n_i p_i) = \sum n_i \cdot 1$ 을 얻습니다 — 즉  $\varepsilon$ 는 실제로 경계 연산자가  $\tilde{C}_0(X) \xrightarrow{\partial} \tilde{C}_{-1}(X)$ 인 경우로 일반화된 것에 불과합니다.<sup>a</sup>

<sup>a</sup> $n \leq -2$ 인 경우는 어떨까요?  $n$ -단체는 길이가  $(n+1)$ 인 꼭짓점 목록에서 나오므로,  $(-2)$ -단체는 길이가  $(-1)$ 인 꼭짓점 목록을 필요로 할 것입니다 — 하지만 그런 목록은 존재하지 않습니다. 따라서  $(-1)$ -단체는 하나 존재하지만,  $(-2)$ -단체는 0개 존재합니다( $n < -2$ 일 때도 마찬가지입니다). 0개의 원소로 생성된 자유 아벨 군은 자명군이므로,  $\tilde{C}_{-2} \cong 0$ 입니다. 특히,  $\partial(\emptyset) = 0$ 입니다.

**질문 71.4.2.** 위 사슬의  $\mathbb{Z}$ 에서의 호몰로지는 무엇입니까? (힌트:  $X$ 가 공집합이 아니어야 합니다.)

**정의 71.4.3.** 증대 사슬 복합체의 호몰로지 군들을 공간  $X$ 의 **축소 호몰로지 군**  $\tilde{H}_n(X)$ 라 부릅니다.

$n > 0$ 일 때  $\tilde{H}_n(X) \cong H_n(X)$ 임은 명백합니다. 하지만  $n = 0$ 일 때,  $\varepsilon$ 에 의한 사상  $H_0(X) \rightarrow \mathbb{Z}$ 는 핵  $\tilde{H}_0(X)$ 를 가지므로,  $H_0(X) \cong \tilde{H}_0(X) \oplus \mathbb{Z}$ 입니다.

이는 보통 그저 추가적인 편의일 뿐입니다. 예를 들어, 이는  $X$ 가 수축가능이면 그 모든 축소 호몰로지 군이 소멸함을 의미하며, 따라서 특별한  $n = 0$ 인 경우를 계속 신경 쓸 필요가 없게 됩니다.

**질문 71.4.4.** 앞서  $H_n(S^m)$ 에 대해 주장한 내용을 고려할 때,  $\tilde{H}_n(S^m)$ 은 무엇이어야 합니까?

#### 예제 71.4.5 (상대 사슬군)

$X$ 가 위상 공간이고  $A \subseteq X$ 가 부분공간이라고 합시다. 다음과 같이 정의하여  $A$ 로 “뺀”을 취할 수 있습니다

$$C_n(X, A) := C_n(X)/C_n(A)$$

모든  $n$ 에 대해 그렇습니다. 따라서 전적으로  $A$ 에 포함된 사슬은 자명합니다. 그러면  $C_n(X)$  위의 보통  $\partial$ 이 새로운 사슬 복합체를 생성합니다

$$\dots \xrightarrow{\partial} C_{n+1}(X, A) \xrightarrow{\partial} C_n(X, A) \xrightarrow{\partial} C_{n-1}(X, A) \xrightarrow{\partial} \dots$$

이는  $\partial$ 이  $C_n(A)$ 를  $C_{n-1}(A)$ 로 보내기 때문에 잘 정의됩니다.

**정의 71.4.6.** 이 상대 사슬 복합체의 호몰로지 군을 **상대 호몰로지 군**이라 하며  $H_n(X, A)$ 로 표기합니다.

하나의 순진한(naïve) 추측은 이것이  $H_n(X)/H_n(A)$ 와 같을 수도 있다는 것입니다. 이는

사실이 아니며, 일반적으로는 의미조차 통하지 않습니다.  $X$ 를  $\mathbb{R}^2$ 로,  $A = S^1$ 을 그 안의 원으로 잡으면,  $H_1(X) = H_1(\mathbb{R}^2) = 0$ 이고  $H_1(S^1) = \mathbb{Z}$ 입니다.

또 다른 추측은  $H_n(X, A)$ 가 그저  $\tilde{H}_n(X/A)$ 일지도 모른다는 것입니다. 이는 대부분의 합리적인 공간  $X$ 와  $A$ 에 대해 참으로 밝혀질 것이며, **장 73**에서 절제 정리(excision theorem)에 이르렀을 때 논의하겠습니다.

#### 예제 71.4.7 (마이어-비토리스 열)

공간  $X$ 가 두 열린집합  $U$ 와  $V$ 로 덮인다고 합시다.  $C_n(U+V)$ 를 다음과 같이 정의할 수 있습니다: 각 단체의 상이 전적으로  $U$ 에 포함되거나 전적으로  $V$ 에 포함되는 사슬들로 구성됩니다.

물론 그러면  $\partial$ 은 또 다른 사슬 복합체를 정의합니다

$$\dots \xrightarrow{\partial} C_{n+1}(U+V) \xrightarrow{\partial} C_n(U+V) \xrightarrow{\partial} C_{n-1}(U+V) \xrightarrow{\partial} \dots$$

그리하여 다시 한번, 이 복합체에 대한 호몰로지 군을 정의할 수 있으며, 이를  $H_n(U+V)$ 로 표기합니다. 놀랍게도  $H_n(U+V) \cong H_n(X)$ 임이 밝혀질 것입니다.

## §71.5 생각해 볼 만한 조금 더 어려운 문제

**문제 71A.**  $n \geq 1$ 에 대해 다음 합성이

$$S^{m-1} \hookrightarrow D^n \xrightarrow{F} S^{m-1}$$

어떠한 연속함수  $F$ 에 대해서도  $S^{m-1}$  위의 항등사상이 될 수 없습니다.

**문제 71B** (브라우어르 부동점 정리). 앞선 문제를 이용하여 임의의 연속함수  $f: D^n \rightarrow D^n$ 이 부동점을 가짐을 증명하십시오.



# 72 긴 완전열

이 장에서는 임의의 공간의 호몰로지 군을 계산할 수 있게 해주는 사슬 복합체에 관한 핵심 사실, 이른바 "긴 완전열"을 소개합니다.

아벨 범주에 대해 읽어보지 않은 분들을 위해: 아벨 군의 사상들의 열은

$$\cdots \rightarrow G_{n+1} \rightarrow G_n \rightarrow G_{n-1} \rightarrow \cdots$$

임의의 화살표의 상이 다음 화살표의 핵과 같으면 **완전**합니다. 특히,

- 사상  $0 \rightarrow A \rightarrow B$ 는  $A \rightarrow B$ 가 단사일 때 그리고 그때만 완전입니다.
- 사상  $A \rightarrow B \rightarrow 0$ 은  $A \rightarrow B$ 가 전사일 때 그리고 그때만 완전입니다.

(덧붙여서: 호몰로지 군이 모두 자명한 사슬 복합체를 무엇이라고 부르겠습니까?) 짧은 완전열은  $0 \rightarrow A \hookrightarrow B \twoheadrightarrow C \rightarrow 0$  형태의 것입니다.

## §72.1 짧은 완전열과 네 가지 예시

**이 절의 대표적인 예:** 상대 수열과 마이어-비토리스 수열.

$\mathcal{A} = \text{AbGrp}$ 라고 합시다. 이미  $\mathcal{A}$ 에서 사슬 복합체의 사상을 정의했음을 상기하십시오.

**정의 72.1.1.** 사슬 복합체의 사상이 있다고 합시다

$$0 \rightarrow A_\bullet \xrightarrow{f} B_\bullet \xrightarrow{g} C_\bullet \rightarrow 0$$

아래 도식의 각 행이 짧은 완전이면 **짧은 완전**이라고 합니다.

$$\begin{array}{ccccccc}
 & \vdots & & \vdots & & \vdots & \\
 & \downarrow \partial_A & & \downarrow \partial_B & & \downarrow \partial_C & \\
 0 & \longrightarrow & A_{n+1} & \xhookrightarrow{f_{n+1}} & B_{n+1} & \xrightarrow{g_{n+1}} & C_{n+1} \longrightarrow 0 \\
 & & \downarrow \partial_A & & \downarrow \partial_B & & \downarrow \partial_C \\
 0 & \longrightarrow & A_n & \xhookrightarrow{f_n} & B_n & \xrightarrow{g_n} & C_n \longrightarrow 0 \\
 & & \downarrow \partial_A & & \downarrow \partial_B & & \downarrow \partial_C \\
 0 & \longrightarrow & A_{n-1} & \xhookrightarrow{f_{n-1}} & B_{n-1} & \xrightarrow{g_{n-1}} & C_{n-1} \longrightarrow 0 \\
 & & \downarrow \partial_A & & \downarrow \partial_B & & \downarrow \partial_C \\
 & & \vdots & & \vdots & & \vdots
 \end{array}$$

이는 기본적으로 사슬 복합체에 대한 적절한 /의 정의에 대해  $C_\bullet = B_\bullet / A_\bullet$ 임을 의미합니다.

이는 **절 70.3**의 정의와 일치합니다.

**예제 72.1.2** (마이어-비토리스 짧은 완전열과 그 증대)

$X = U \cup V$ 를 열린 덮개라고 합시다. 각  $n$ 에 대해 다음을 고려하십시오

$$\begin{aligned} C_n(U \cap V) &\hookrightarrow C_n(U) \oplus C_n(V) \twoheadrightarrow C_n(U + V) \\ c &\longmapsto (c, -c) \\ (c, d) &\longmapsto c + d \end{aligned}$$

(적절한 기저를 취하면) 후자의 사상의 핵이 정확히 첫 번째 사상의 상임을 쉽게 알 수 있습니다. 이는 짧은 완전열을 생성합니다

$$0 \rightarrow C_\bullet(U \cap V) \hookrightarrow C_\bullet(U) \oplus C_\bullet(V) \twoheadrightarrow C_\bullet(U + V) \rightarrow 0.$$

**예제 72.1.3** (증대된 마이어-비토리스 열)

다음은 덧셈으로써 마이어-비토리스 열의 각 사슬 복합체 또한 증대할 수 있습니다

$$\begin{array}{ccccccc} 0 & \longrightarrow & C_0(U \cap V) & \hookrightarrow & C_0(U) \oplus C_0(V) & \twoheadrightarrow & C_0(U + V) \longrightarrow 0 \\ & & \downarrow \varepsilon & & \downarrow \varepsilon \oplus \varepsilon & & \downarrow \varepsilon \\ 0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z} \oplus \mathbb{Z} & \longrightarrow & \mathbb{Z} \longrightarrow 0 \end{array}$$

도식의 아래쪽에 덧셈으로써 증대할 수 있습니다. 다시 말해 위 내용을 다음과 같이 수정합니다

$$0 \rightarrow \tilde{C}_\bullet(U \cap V) \hookrightarrow \tilde{C}_\bullet(U) \oplus \tilde{C}_\bullet(V) \twoheadrightarrow \tilde{C}_\bullet(U + V) \rightarrow 0$$

여기서  $\tilde{C}_\bullet$ 는 정의 71.4.3에서 정의된 사슬 복합체입니다.

**예제 72.1.4** (상대 사슬 짧은 완전열)

$C_n(X, A) := C_n(X)/C_n(A)$ 이므로, 다음과 같은 짧은 완전열을 얻습니다

$$0 \rightarrow C_\bullet(A) \hookrightarrow C_\bullet(X) \twoheadrightarrow C_\bullet(X, A) \rightarrow 0$$

모든 공간  $X$ 와 부분공간  $A$ 에 대해. 이는 증대될 수 있습니다: 다음을 얻습니다

$$0 \rightarrow \tilde{C}_\bullet(A) \hookrightarrow \tilde{C}_\bullet(X) \twoheadrightarrow C_\bullet(X, A) \rightarrow 0$$

마지막 행을 추가하여

$$\begin{array}{ccccccc} 0 & \longrightarrow & C_0(A) & \hookrightarrow & C_0(X) & \twoheadrightarrow & C_0(X, A) \longrightarrow 0 \\ & & \downarrow \varepsilon & & \downarrow \varepsilon & & \\ 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\text{id}} & \mathbb{Z} & \longrightarrow & 0 \longrightarrow 0. \end{array}$$



$$\begin{array}{ccccc}
 & B_n & \xrightarrow{g_n} & C_n & \\
 & \downarrow \partial_B & & \downarrow \partial_C & \\
 A_{n-1} & \xrightarrow{f_{n-1}} & B_{n-1} & \xrightarrow{g_{n-1}} & C_{n-1}
 \end{array}$$

$C_n$ 의 모든 순환을  $A_{n-1}$ 의 순환으로 보내야 합니다. (그런 다음 수많은 "잘 정의됨" 문제를 확인해야 하지만, 지금은 이를 제쳐 둡시다.)

$c \in C_n$ 이 순환이라고 합시다(즉  $\partial_C(c) = 0$ ). 전사성에 의해,  $g_n(b) = c$ 인  $b \in B_n$ 이 존재하며, 이는 아래로  $\partial_B(b)$ 에 대응됩니다. 이제  $\partial_B(b)$ 의  $g_{n-1}$ 에 의한 상은 정사각형의 가환성에 의해 영이므로,  $f_{n-1}$ 을 통해 당겨올 수 있어  $A_{n-1}$ 의 유일한 원소를 얻습니다( $B_{n-1}$ 에서의 완전성에 의해).

요약하면:  $c$ 에서  $a$ 로 가기 위해 우리는 "왼쪽, 아래, 왼쪽"으로 이동합니다:

$$\begin{array}{ccccc}
 & b & \xrightarrow{g_n} & \boxed{c} & \\
 & \downarrow \partial_B & & \downarrow \partial_C & \\
 \boxed{a} & \xrightarrow{f_{n-1}} & \partial_B(b) & \xrightarrow{g_{n-1}} & 0
 \end{array}$$

**연습문제 72.2.3.** 복원된  $a$ 가 실제로 순환임을, 즉  $\partial_A(a) = 0$ 임을 빠르게 확인해 봅시다. (또 다른 행이 필요하며,  $\partial_B^2 = 0$ 이라는 사실도 필요합니다.)

최종 결론은 다음과 같습니다:

**사슬 복합체의 짧은 완전열은 호몰로지 군의 긴 완전열을 줍니다.**

특히, 앞서 주어진 네 가지 예를 살펴봅시다.

**예제 72.2.4** (마이어-비토리스 긴 완전열, 임시 버전)

마이어-비토리스 열은  $X = U \cup V$ 가 열린 덮개일 때 다음을 줍니다

$$\cdots \rightarrow H_n(U \cap V) \rightarrow H_n(U) \oplus H_n(V) \rightarrow H_n(U + V) \rightarrow H_{n-1}(U \cap V) \rightarrow \cdots$$

그리고 그 축약 버전

$$\cdots \rightarrow \tilde{H}_n(U \cap V) \rightarrow \tilde{H}_n(U) \oplus \tilde{H}_n(V) \rightarrow \tilde{H}_n(U + V) \rightarrow \tilde{H}_{n-1}(U \cap V) \rightarrow \cdots$$

이 버전이 "임시적"인 이유는 다음 절에서  $H_n(U+V)$ 와  $\tilde{H}_n(U+V)$ 를 더 나은 것으로 대체할 것이기 때문입니다. 상대 호몰로지 열에 대해서는 다음과 같습니다:

**정리 72.2.5 (상대 호몰로지에 대한 긴 완전열)**

$X$ 를 공간이라 하고,  $A \subseteq X$ 를 부분공간이라고 합시다. 다음의 긴 완전열이 있습니다

$$\cdots \rightarrow H_n(A) \rightarrow H_n(X) \rightarrow H_n(X, A) \rightarrow H_{n-1}(A) \rightarrow \cdots$$

그리고

$$\cdots \rightarrow \tilde{H}_n(A) \rightarrow \tilde{H}_n(X) \rightarrow H_n(X, A) \rightarrow \tilde{H}_{n-1}(A) \rightarrow \cdots$$

이 수열들의 완전성은  $H_n(U + V)$ 나  $H_n(X, A)$ 가 어떤 모습인지 무언가 알기만 한다면  $H_n(X)$ 에 대해 **엄청난 양의 정보**를 줄 것입니다. 이것이 다음 장의 목적입니다.

**§72.3 마이어-피토리스 완전열**

**이 절의 대표적인 예:**  $S^m$ 을 두 개의 반구로 나누어  $H_n(S^m)$ 을 계산하기

이제 많은 대수학을 다루었으니, 약간의 기하학을 끌어들어야 합니다. Napkin에는 두 가지 주요한 기하학적 결과가 있습니다. 하나는 절제 정리로, 다음 장에서 다룹니다. 다른 하나는 여기서 제시하는 것으로, 마이어-피토리스 완전열을 활용할 수 있게 해줍니다. 증명은 다소 복잡하여 생략하며, 자세한 내용은 [Ha02]를 참고하십시오.

첫 번째 정리는 지금까지 유지해온  $H_n(U + V)$ 라는 표기가 불필요하며, 단순히  $H_n(X)$ 로 대체할 수 있다는 것입니다:

**정리 72.3.1 (열린 덮개 호몰로지 정리)**

포함 사상  $\iota: C_\bullet(U + V) \hookrightarrow C_\bullet(X)$ 를 생각해봅시다. 그러면  $\iota$ 는 동형사상을 유도합니다

$$H_n(U + V) \cong H_n(X).$$

**비고 72.3.2** — 사실 이는 두 개의 덮개  $U \cup V$ 로 이루어진 경우뿐만 아니라, 임의의 (비가산일지라도) 열린 덮개에 대해서도 성립합니다. 하지만 여기서는 **예제 72.1.2**에 필요한 것이므로, 두 개의 열린집합으로 이루어진 특수한 경우만 서술합니다.

따라서 **예제 72.1.2**와 위 정리를 함께 사용하면, 모든  $H_n(U + V)$ 를  $H_n(X)$ 로 대체한 후 다음이 성립함을 알 수 있습니다:

**정리 72.3.3 (마이어-피토리스 긴 완전열)**

$X = U \cup V$ 가 열린 덮개라면, 다음과 같은 긴 완전열이 존재합니다

$$\cdots \rightarrow H_n(U \cap V) \rightarrow H_n(U) \oplus H_n(V) \rightarrow H_n(X) \rightarrow H_{n-1}(U \cap V) \rightarrow \cdots$$

그리고

$$\cdots \rightarrow \tilde{H}_n(U \cap V) \rightarrow \tilde{H}_n(U) \oplus \tilde{H}_n(V) \rightarrow \tilde{H}_n(X) \rightarrow \tilde{H}_{n-1}(U \cap V) \rightarrow \cdots$$

마침내 우리는 구의 호몰로지 군을 계산할 수 있습니다.

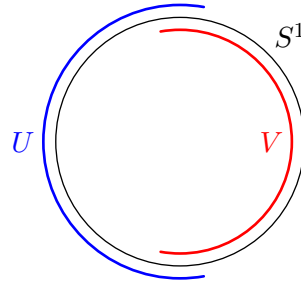
**정리 72.3.4** ( $S^m$ 의 호몰로지 군)

정수  $m$ 과  $n$ 에 대하여,

$$\tilde{H}_n(S^m) \cong \begin{cases} \mathbb{Z} & n = m \\ 0 & \text{그렇지 않으면.} \end{cases}$$

생성원  $\tilde{H}_n(S^n)$ 은  $S^n$ 을 정확히 한 번 덮는  $n$ -세포입니다 (예를 들어,  $\tilde{H}_1(S^1)$ 의 생성원은  $S^1$ 을 한 번 감는 고리입니다).

증명. 이 문제는 재미있으므로,  $m = 1$ 인 경우만 풀이하고 나머지는 여러분에게 맡기겠습니다. 원  $S^1$ 을 그림과 같이 두 개의 호  $U$ 와  $V$ 로 분해합니다:



$U$ 와  $V$ 는 각각 수축 가능하므로, 이들의 축소 호몰로지 군은 모두 소멸합니다. 게다가  $U \cap V$ 는 두 점과 호모토피 동치이므로, 다음이 성립합니다

$$\tilde{H}_n(U \cap V) \cong \begin{cases} \mathbb{Z} & n = 0 \\ 0 & \text{그렇지 않으면.} \end{cases}$$

이제 다시 짧은 완전열의 다음 부분을 생각해봅시다

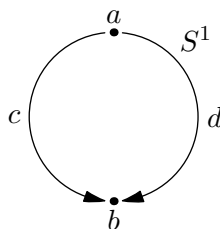
$$\cdots \rightarrow \underbrace{\tilde{H}_n(U) \oplus \tilde{H}_n(V)}_{=0} \rightarrow \tilde{H}_n(S^1) \xrightarrow{\partial} \tilde{H}_{n-1}(U \cap V) \rightarrow \underbrace{\tilde{H}_{n-1}(U) \oplus \tilde{H}_{n-1}(V)}_{=0} \rightarrow \cdots$$

이로부터  $\tilde{H}_n(S^1)$ 은  $n = 1$ 일 때  $\mathbb{Z}$ 이고, 그 외에는 0임을 알 수 있습니다.

이제  $\tilde{H}_1(S^1)$ 의 생성원을 분석하는 일이 남았습니다. 이 동형사상은 연결 준동형사상  $\partial$ 에 의해 주어졌으며, 이는 다음 도식에서 "왼쪽, 아래, 왼쪽" 절차(비고 72.2.2)로 주어짐에 유의하십시오

$$\begin{array}{ccc} C_1(U) \oplus C_1(V) & \longrightarrow & C_1(U + V) \\ \downarrow \partial \oplus \partial & & \\ C_0(U \cap V) & \longrightarrow & C_0(U) \oplus C_0(V) \end{array}$$

$U \cap V$ 의 서로소인 두 경로에 표시된 대로 점  $a$ 와  $b$ 를 표시합니다.



그러면  $a - b$ 는  $H_0(U \cap V)$ 의 생성원을 나타내는 사이클입니다.  $\partial$ 의 원상은 다음과 같이 구할 수 있습니다:  $a$ 와  $b$ 를 잇는 사슬을  $c$ 와  $d$ 라 하고,  $c$ 는  $U$ 에 포함되며  $d$ 는  $V$ 에 포함된다고 하면, 도식은 다음과 같이 완성됩니다

$$\begin{array}{ccc} (c, d) & \longmapsto & c - d \\ \downarrow & & \\ a - b & \longmapsto & (a - b, a - b) \end{array}$$

다시 말해  $\partial(c - d) = a - b$ 이므로,  $c - d$ 는  $\tilde{H}_1(S^1)$ 의 생성원입니다.

따라서 우리는  $c - d$ 가  $((H_1(S^1) \text{에서})) S^1$ 을 반시계 방향으로 한 번 감는 고리  $\gamma$ 와 동치임을 보이고자 합니다. 이는 **예제 71.2.10**에서 예시로 보였습니다.  $\square$

따라서 마이어-피토리스(Mayer-Vietoris)의 핵심 아이디어는 다음과 같습니다.

**마이어-피토리스를 이용하면  $X$ 를 두 개의 열린집합으로 나누어  $H_n(X)$ 를 계산할 수 있습니다.**

몇 가지 예를 더 살펴보겠습니다.

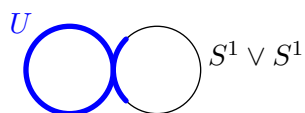
**명제 72.3.5 (8자 도형의 호몰로지 군)**

$X = S^1 \vee S^1$ 을 8자 도형이라고 합시다. 그러면

$$\tilde{H}_n(X) \cong \begin{cases} \mathbb{Z}^{\oplus 2} & n = 1 \\ 0 & \text{그렇지 않으면.} \end{cases}$$

$\tilde{H}_1(X)$ 의 생성원은 8자 모양 도형의 두 고리입니다.

증명. 다시 한번, 간단히 하기 위해 축소 호몰로지 군을 다루겠습니다.  $U$ 를 아래에 보이는 것처럼 8자 모양 도형의 "왼쪽" 절반에 오른쪽 부분을 조금 더한 것이라고 합시다.



집합  $V$ 는 대칭적으로 정의됩니다. 이 경우  $U \cap V$ 는 수축 가능하며,  $U$ 와  $V$ 는 각각  $S^1$ 과 호모토피 동치입니다.

따라서 긴 완전열의 한 구간을 다음과 같이 읽을 수 있습니다.

$$\cdots \rightarrow \underbrace{\tilde{H}_n(U \cap V)}_{=0} \rightarrow \tilde{H}_n(U) \oplus \tilde{H}_n(V) \rightarrow \tilde{H}_n(X) \rightarrow \underbrace{\tilde{H}_{n-1}(U \cap V)}_{=0} \rightarrow \cdots$$

이로써  $\tilde{H}_n(X) \cong \tilde{H}_n(S^1) \oplus \tilde{H}_n(S^1)$ 임을 얻습니다. 생성원에 관한 주장은, 위 동형사상에 따라  $\tilde{H}_n(X)$ 의 생성원이  $\tilde{H}_n(U)$ 와  $\tilde{H}_n(V)$ 의 생성원이라는 사실로부터 따라오며, 이는 앞선 정리에서 기하학적으로 설명한 바 있습니다.  $\square$

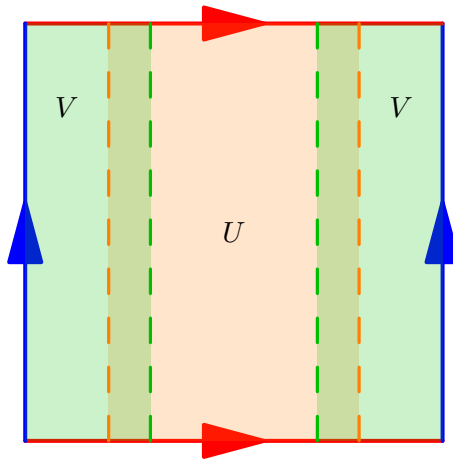
지금까지는 공간의 특정 부분을 항상 수축 가능하게 만들 수 있었다는 점에서 매우 운이 좋았습니다. 이는 항상 성립하는 것은 아니며, 다음 예제에서는 풀이를 완성하기 위해 실제로 문제의 사상들을 이해해야 할 것입니다.

**명제 72.3.6 (원환면의 호몰로지 군)**

$X = S^1 \times S^1$ 을 원환면이라고 합시다. 그러면

$$\tilde{H}_n(X) = \begin{cases} \mathbb{Z}^{\oplus 2} & n = 1 \\ \mathbb{Z} & n = 2 \\ 0 & \text{그렇지 않으면.} \end{cases}$$

증명. 2차원 종이 위에서 도식을 보기 좋게 만들기 위해, 원환면을 변이 식별된 정사각형으로 나타내겠습니다. 다만 3차원적으로 그려도 그림은 마찬가지로 의미가 통합니다. 그림에 나타난  $U$ (연한 주황색으로 칠해짐)와  $V$ (초록색으로 칠해짐)를 생각해 봅시다. (왼쪽과 오른쪽(파란색) 변이 식별되어 있기 때문에, 그림에서는 연결되어 보이지 않더라도  $V$ 는 연결되어 있음에 유의하십시오.)



3차원 그림에서  $U$ 와  $V$ 는 함께 원환면을 이루는 두 개의 원기둥입니다. 이번에는  $U$ 와  $V$ 가 각각  $S^1$ 과 호모토피 동치이며, 교집합  $U \cap V$ 는 두 원의 서로소 합집합입니다. 따라서  $\tilde{H}_1(U \cap V) \cong \mathbb{Z} \oplus \mathbb{Z}$ 이고,  $H_0(U \cap V) \cong \mathbb{Z}^{\oplus 2} \implies \tilde{H}_0(U \cap V) \cong \mathbb{Z}$ 입니다.

$n \geq 3$ 일 때, 다음을 연습합니다.

$$\cdots \rightarrow \underbrace{\tilde{H}_n(U \cap V)}_{=0} \rightarrow \tilde{H}_n(U) \oplus \tilde{H}_n(V) \rightarrow \tilde{H}_n(X) \rightarrow \underbrace{\tilde{H}_{n-1}(U \cap V)}_{=0} \rightarrow \cdots$$

따라서  $n \geq 3$ 에 대해  $H_n(X) \cong 0$ 입니다. 또한  $X$ 가 경로 연결이므로  $H_0(X) \cong \mathbb{Z}$ 입니다. 이제 남은 것은  $H_2(X)$ 와  $H_1(X)$ 를 계산하는 것입니다.

먼저  $H_2(X)$ 를 구해 봅시다. 먼저 다음 구간을 살펴봅시다.

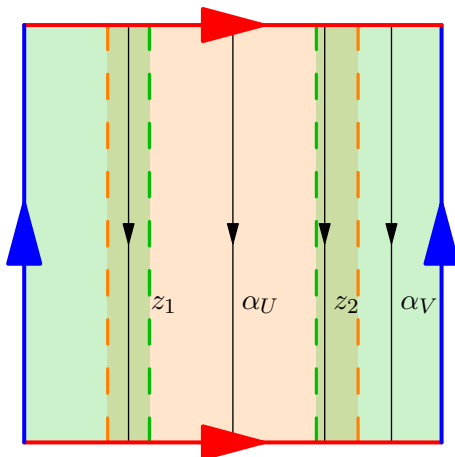
$$\cdots \rightarrow \underbrace{\tilde{H}_2(U) \oplus \tilde{H}_2(V)}_{=0} \rightarrow \tilde{H}_2(X) \xrightarrow{\partial} \underbrace{\tilde{H}_1(U \cap V)}_{\cong \mathbb{Z} \oplus \mathbb{Z}} \xrightarrow{\phi} \underbrace{\tilde{H}_1(U) \oplus \tilde{H}_1(V)}_{\cong \mathbb{Z} \oplus \mathbb{Z}} \rightarrow \cdots$$

안타깝게도 이번에는 왼쪽에 0이 하나밖에 없기 때문에  $\tilde{H}_2(X)$ 가 무엇인지 바로 명확하지 않습니다. 이를 알아내려면 사상  $\partial$ 과  $\phi$ 가 실제로 어떤 모습인지 파악해야 합니다. 앞으로 보게 되겠지만, 두 군이 동형이더라도  $\phi$ 는 동형사상이 아니라는 점에 유의하십시오.

영 항의 존재로 인해 연결 사상  $\partial$ 를 단사로 만들 수 있었습니다. 먼저,  $\tilde{H}_2(X)$ 는  $\partial$ 의 상과 동형이며, 이는 정확히 삽입된 화살표  $\phi$ 의 핵입니다.  $\ker \phi$ 가 무엇인지 알아내려면, 사상  $C_\bullet(U \cap V) \rightarrow C_\bullet(U) \oplus C_\bullet(V)$ 가 어떻게 구성되었는지 다시 떠올려야 합니다: 그것은  $c \mapsto (c, -c)$ 였습니다. 따라서 호몰로지 군의 유도 사상은 실제로 짐작하는 그대로입니다:  $\tilde{H}_1(U \cap V)$ 의 1-사이클  $z$ 는  $\tilde{H}_1(U) \oplus \tilde{H}_1(V)$ 의  $(z, -z)$ 로 보내집니다.

특히,  $\tilde{H}_1(U \cap V) = \mathbb{Z} \oplus \mathbb{Z}$ 의 두 생성원  $z_1$ 과  $z_2$ , 즉  $U \cap V$ 의 각 연결 성분에서 하나씩의 사이클을 생각해 봅시다. (분명히 하자면,  $U \cap V$ 는 두 개의 "손목 밴드"로 이루어져 있으며,  $z_i$ 는  $i$ 번째 것을 한 번 감습니다.) 나아가  $\alpha_U$ 를  $\tilde{H}_1(U) \cong \mathbb{Z}$ 의 생성원으로,  $\alpha_V$ 를  $\tilde{H}_1(V) \cong \mathbb{Z}$ 의 생성원으로 놓겠습니다.

이 원소들은 아래에 그려져 있습니다.



$z_1, z_2, \alpha_U, \alpha_V$ 는 호몰로지 군의 원소이므로, 경로를 다소 옮겨도 무방하다는 점에 유의하십시오 — 예를 들어,  $\tilde{H}_1(U)$ 의 원소로서  $z_1$ 로 그려진 사슬과  $\alpha_U$ 는 같은 원소를 나타냅니다. 그러면 다음을 얻습니다.

$$z_1 \mapsto (\alpha_U, -\alpha_V) \quad \text{그리고} \quad z_2 \mapsto (\alpha_U, -\alpha_V).$$

(부호는 생성원에 대해 어느 방향을 선택하는지에 따라 달라질 수 있습니다.  $\mathbb{Z}$ 에는 가능한 생성원이 두 개 있다는 점에 유의하십시오.) 이를 행렬로도 나타낼 수 있습니다.

$$\phi = \begin{bmatrix} 1 & 1 \\ -1 & -1 \end{bmatrix}.$$

그리고  $\phi(z_1 - z_2) = 0$ 임을 관찰할 수 있는데, 이는 이 사상이 자명하지 않은 핵을 가짐을 의미합니다! 즉,

$$\ker \phi = \langle z_1 - z_2 \rangle \cong \mathbb{Z}.$$

따라서  $\tilde{H}_2(X) \cong \operatorname{im} \partial \cong \ker \phi \cong \mathbb{Z}$ 입니다. 또한  $\operatorname{im} \phi$ 가  $(\alpha_U, -\alpha_V)$ 에 의해 생성되는 집합이라는 점도 유의합니다; (특히  $\operatorname{im} \phi \cong \mathbb{Z}$ 이며  $\operatorname{im} \phi$ 에 의한 몫도  $\mathbb{Z}$ 입니다).

$\tilde{H}_1(X)$ 의 경우도 상황이 비슷한데, 이번에는 다음과 같습니다

$$\dots \xrightarrow{\phi} \underbrace{\tilde{H}_1(U) \oplus \tilde{H}_1(V)}_{\cong \mathbb{Z} \oplus \mathbb{Z}} \xrightarrow{\psi} \tilde{H}_1(X) \xrightarrow{\partial} \underbrace{\tilde{H}_0(U \cap V)}_{\cong \mathbb{Z}} \rightarrow \underbrace{\tilde{H}_0(U) \oplus \tilde{H}_0(V)}_{=0} \rightarrow \dots$$

그리고 이로부터 연결 사상  $\partial$ 이 전사임을 알 수 있으므로,  $\operatorname{im} \partial \cong \mathbb{Z}$ 입니다. 이제 다음도 성립합니다

$$\begin{aligned} \ker \partial &\cong \operatorname{im} \psi \cong (\tilde{H}_1(U) \oplus \tilde{H}_1(V)) / \ker \psi \\ &\cong (\tilde{H}_1(U) \oplus \tilde{H}_1(V)) / \operatorname{im} \phi \cong \mathbb{Z} \end{aligned}$$

이는  $\operatorname{im} \phi$ 에 대해 이미 알고 있던 사실 때문입니다. 마무리를 위해서는 몇 가지 대수적 기교가 필요합니다. 첫 번째는 **명제 70.5.1**로, 이는 다음과 같은 짧은 완전열을 줍니다

$$0 \rightarrow \underbrace{\ker \partial}_{\cong \operatorname{im} \psi \cong \mathbb{Z}} \hookrightarrow \tilde{H}_1(X) \twoheadrightarrow \underbrace{\operatorname{im} \partial}_{\cong \mathbb{Z}} \rightarrow 0.$$

$\tilde{H}_1(X) \cong \mathbb{Z} \oplus \mathbb{Z}$ 가 유일한 가능성임을 스스로 납득해 보시길 바라지만, 이를 보조정리 72.3.8로 엄밀하게 증명하겠습니다.  $\square$

**비고 72.3.7** — 앞서 우리는 (증명 없이)  $\pi_2(X)$ 가 자명하다고 언급했습니다 — 즉, 호모토피는 원환면에서 어떠한 "2차원 구멍"도 찾아내지 못합니다. 그렇다면 어째서  $H_2(X) \cong \mathbb{Z}$ 인 것일까요?

다음 방법을 사용하여 긴 완전열로부터  $H_2(X)$ 의 자명하지 않은 원소를 직접 계산해 보고 싶을 수도 있습니다. 긴 완전열을 살펴봅시다:

$$\begin{array}{ccccccc} \cdots & \longrightarrow & \underbrace{H_2(U) \oplus H_2(V)}_{=0} & \longrightarrow & \underbrace{H_2(X)}_{\cong \mathbb{Z}} & & \\ & & \searrow \partial & & & & \\ \underbrace{H_1(U \cap V)}_{\cong \mathbb{Z} \oplus \mathbb{Z}} & \xrightarrow{\phi} & \underbrace{H_1(U) \oplus H_1(V)}_{\cong \mathbb{Z} \oplus \mathbb{Z}} & \longrightarrow & \cdots & & \end{array}$$

우리는  $H_2(X)$ 의 자명하지 않은 어떤 원소를 찾고자 합니다 — 이를 위해,  $\ker \phi \subseteq H_1(U \cap V)$ 의 한 원소를 취하여  $\partial$ 에 대한 그 원상을 취할 수 있습니다.

이를 위해서는  $z_1 - z_2$ 로 충분할 것입니다.  $\partial$ 에 대한 그 원상을 취하려면,  $\partial$ 이 어떻게 구성되었는지를 상기할 필요가 있습니다 — 그것은 도식에서 "왼쪽, 아래, 왼쪽" 절차였습니다:

$$\begin{array}{ccc} C_2(U) \oplus C_2(V) & \longrightarrow & C_2(X) \\ \downarrow & & \\ C_1(U \cap V) \hookrightarrow & C_1(U) \oplus C_1(V) & \end{array}$$

그리하여, 몫 사상 아래에서  $z_1 - z_2$ 로 사상되는  $C_1(U \cap V)$ 의 (단한) 원소를 찾는 다음, 이를 "오른쪽, 위, 오른쪽"으로 이동시켜  $C_2(X)$ 의 한 원소로 만듭니다.

모든 것을 올바르게 수행하였다면, 그 결과는 원환면 전체이어야 합니다!

이는 다음 요점을 강조합니다:

**호몰로지가 탐지하는 "구멍"이 반드시  $S^n$ 의 내부처럼 생길 필요는 없습니다.**

앞의 예시는 이전 것들과는 다른 성격을 지니고 있음을 주목하시길 바랍니다. 왜냐하면 군을 계산하기 위해서라도 긴 완전열에 나오는 사상들이 실제로 무엇인지 알아내야 했기 때문입니다. 원리적으로는 앞의 증명에 나온 모든 동형사상을 알아내어  $\tilde{H}_1(S^1 \times S^1)$ 의 생성원을 명시적으로 계산할 수도 있겠지만, 세부 사항에 매몰되는 것을 피하기 위해 여기서는 그렇게 하지 않겠습니다.

마지막으로, 마지막 단계를 완전히 정당화하기 위해 다음을 제시합니다:

**보조정리 72.3.8 (분할 보조정리)**

아벨 군의 짧은 완전열  $0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$ 에 대하여, 다음은 서로 동치입니다:

- (a)  $A \xrightarrow{f} B \xrightarrow{p} A$ 가 항등 사상이 되도록 하는  $p: B \rightarrow A$ 가 존재합니다.
- (b)  $C \xrightarrow{s} B \xrightarrow{g} C$ 가 항등 사상이 되도록 하는  $s: C \rightarrow B$ 가 존재합니다.
- (c)  $B$ 에서  $A \oplus C$ 로 가는 동형사상이 존재하여 다음 도식이

$$\begin{array}{ccccccc}
 & & & B & & & \\
 & & f \nearrow & \uparrow & \searrow g & & \\
 0 & \longrightarrow & A & & & C & \longrightarrow 0 \\
 & & \searrow & \downarrow \cong & \nearrow & & \\
 & & & A \oplus C & & & 
 \end{array}$$

가환이 됩니다. ( $A \oplus C$ 에 딸린 사상들은 자명한 것들입니다.)

특히,  $C$ 가 자유 가군일 때는 언제나 (b)가 성립합니다.

이러한 경우 우리는 짧은 완전열이 **분할된다**고 말합니다. 요점은 다음과 같습니다

**분할되는 완전열은  $A$ 와  $C$ 가 주어졌을 때  $B$ 를 얻을 수 있게 해 줍니다.**

특히,  $C = \mathbb{Z}$ 이거나 임의의 자유 아벨 군인 경우, 조건 (b)는 필연적으로 참입니다. 따라서 짧은 완전열  $0 \rightarrow \mathbb{Z} \rightarrow \tilde{H}_1(X) \rightarrow \mathbb{Z} \rightarrow 0$ 을 얻었다면, 증명이 끝났습니다.

**비고 72.3.9** — 안타깝게도, 모든 완전열이 분해되는 것은 아닙니다: 분해되지 않는 짧은 완전열의 예는 다음과 같습니다

$$0 \rightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\times 2} \mathbb{Z}/4\mathbb{Z} \twoheadrightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 0$$

$\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ 가 참이 아니기 때문입니다.

**비고 72.3.10** — 분해 보조정리는 임의의 아벨 범주에서 참입니다. “직합”은 두 대상  $A$ 와  $C$ 의 쌍대극한입니다.

## §72.4 생각해 볼 만한 조금 더 어려운 문제

**문제 72A.** 정리 72.3.4의 증명을 완성하십시오, 즉 모든  $m$ 과  $n$ 에 대해  $H_n(S^m)$ 을 계산하십시오. (먼저  $m = 2$ 인 경우를 시도해 보면, 어떻게 진행해야 할지 알 수 있을 것입니다.)

**문제 72B.**  $p \geq 1$ 개의 점을 제거한  $\mathbb{R}^n$ 의 축소 호몰로지 군을 계산하십시오.

**문제 72C\*.**  $n \geq 1$ 과  $k \geq 0$ 을 정수라 합시다.  $H_k(\mathbb{R}^n, \mathbb{R}^n \setminus \{0\})$ 을 계산하십시오.

**문제 72D** (아홉 보조정리). 다음과 같은 가환 도식을 생각해 봅시다

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & A_1 & \longrightarrow & B_1 & \longrightarrow & C_1 \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & A_2 & \longrightarrow & B_2 & \longrightarrow & C_2 \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & A_3 & \longrightarrow & B_3 & \longrightarrow & C_3 \longrightarrow 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 0 & & 0 & & 0
 \end{array}$$

그리고 모든 행이 완전하고, 두 열이 완전하다고 가정합니다. 세 번째 열도 완전함을 보이십시오.



**문제 72E\*** (클라인 병). 클라인 병  $K$ 의 축소 호몰로지 군이 다음과 같이 주어짐을 보이십시오.

$$\tilde{H}_n(K) = \begin{cases} \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & n = 1 \\ 0 & \text{그렇지 않으면.} \end{cases}$$

**문제 72F\*** (삼중 긴 완전열).  $A \subseteq B \subseteq X$ 를 부분공간이라 합시다. 다음과 같은 긴 완전열이 존재함을 보이십시오

$$\cdots \rightarrow H_n(B, A) \rightarrow H_n(X, A) \rightarrow H_n(X, B) \rightarrow H_{n-1}(B, A) \rightarrow \cdots$$

# 73 절제와 상대 호몰로지

우리는 이미 마이어-비에토리스 완전열을 사용하는 방법을 살펴보았습니다: 우리는 다음과 같은 완전열에서 시작했습니다

$$\cdots \rightarrow H_n(U \cap V) \rightarrow H_n(U) \oplus H_n(V) \rightarrow H_n(U + V) \rightarrow H_{n-1}(U \cap V) \rightarrow \cdots$$

그리고 그 축소 버전에서 시작하여,  $H_n(U + V) \cong H_n(X)$ 라는 기하학적 사실에 의존했습니다. 이는 우리가  $H_n(X)$ 에 대해 대수적으로 계산을 할 수 있게 해주었습니다.

이 장에서는 사슬 복합체와 연관된 긴 완전열로 관심을 돌립니다

$$0 \rightarrow C_n(A) \hookrightarrow C_n(X) \twoheadrightarrow C_n(X, A) \rightarrow 0.$$

이 설정은 앞의 두 장과 매우 비슷해 보이겠지만,  $H_n: \mathbf{hTop} \rightarrow \mathbf{Grp}$ 에 더하여 쌍  $(X, A)$ 를  $H_n(X, A)$ 로 보내는 함자  $H_n: \mathbf{hPairTop} \rightarrow \mathbf{Grp}$ 를 갖게 된다는 점이 다릅니다. 그런 다음, (역시 증명 없이) 핵심적인 기하학적 결과를 서술하고, 이를 이용하여 추론을 이끌어냅니다.

## §73.1 동기

주된 동기는 다음과 같습니다:

**상대 호몰로지는 몫공간의 대수적 유사물입니다.**

그러므로 예를 들어, 쌍의 사상  $f: (X, A) \rightarrow (Y, B)$ 를 볼 때,  $X/A \rightarrow Y/B$ 를 떠올려야 합니다.

이는 공간  $A \subseteq X$ 에 대해  $H_n(X, A) \cong \tilde{H}_n(X/A)$ 가 성립한다는 “합리적인 추측”을 설명해줍니다.

**정리 73.4.3**에 의해, 위의 추측은 대부분의 공간에서 실제로 참입니다. 예를 들면:

**질문 73.1.1.**  $X = [0, 1]$ 이고  $A = \{0, 1\}$ 이라고 합시다.  $H_1(X/A)$ 와  $H_1(X, A)$ 가  $\mathbb{Z}$ 와 동형사상임을 보이십시오. (이 예에서는  $\pi_1(X/A)$ 도 마찬가지입니다.)

그러나 모든 경우에 성립하지는 않습니다. **예제 64.2.6**와 유사하게,  $A$ 가 닫혀 있지 않으면 이상한 일이 일어날 수 있습니다:

**예제 73.1.2** ( $A$ 가  $X$ 에서 열려 있을 때의  $H_n(X, A)$ )

$X = D^2$ 을 닫힌 원판이라고 합시다.

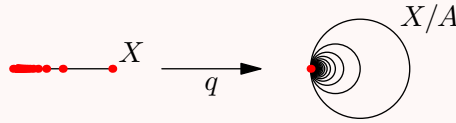
$A$ 가 적당히 좋은 경우, 예를 들어  $A = S^1$ 이  $X$ 의 경계라면,  $H_2(X, A) \cong H_2(X/A) \cong \mathbb{Z}$ 가 성립합니다.

그러나  $0$ 이  $X$ 의 중심일 때  $A = X \setminus \{0\}$ 이라면,  $H_2(X, A)$ 는 여전히  $\mathbb{Z}$ 와 동형사상이지만  $H_2(X/A) \cong 0$ 입니다. (뒤의 동형사상은 보기가 더 어려운데, 주로  $X/A$ 가 이상한 공간이기 때문입니다 — 이는 하우스도르프가 아닙니다.)

$A$ 가  $X$ 에서 닫혀 있을 때조차도, 문제가 여전히 발생할 수 있습니다.

**예제 73.1.3** (축소되는 원들의 켜기합)

$X$ 를 구간  $[0, 1]$ 이라 하고,  $A \subseteq X$ 를  $A = \{\frac{1}{n} \mid n \in \mathbb{Z}^+\} \cup \{0\}$ 라고 합시다. 이 경우, 몫공간  $X/A$ 는 아래에 그려진 것처럼 축소되는 원들의 켜기합과 동형사상일 것입니다.



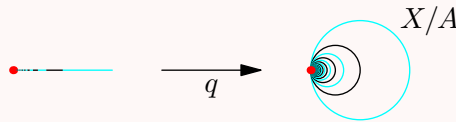
$X/A$ 에서, 빨간 점  $A/A$ 의 임의의 열린 근방은 유한 개를 제외한 모든 원을 포함해야 함에 유의하십시오.

우리는 다음을 주장합니다:

$$H_1(X, A) \not\cong \tilde{H}_1(X/A).$$

무엇이 잘못될 수 있을까요? 일반적으로 말해서, 대수적으로 작업할 때는 모든 것이 유한하지만, 위상수학에서는 무한과 관련된 것들을 고려해야 합니다.

$C(X/A)$ 에서 청록색으로 그려진 다음 1-단체를 생각해봅시다.



$H(X, A)$ 의 모든 원소는  $C(X)$ 에서 1-사이클로 표현되는 대표원을 가지며, 이는 유한히 많은 1-단체로 구성되고, 각 1-단체는 1-경계의 차이를 법으로 하여 선분  $[a, b]$ 와 동치입니다. 따라서 직관적으로,  $H(X, A)$ 의 모든 원소는 오직 “유한히 많은 원”만을 덮을 수 있습니다 (또는 유한히 많은 것을 제외한 나머지 전부).

아직 이 모든 것을 형식화할 만큼 충분한 도구를 갖추지 못했습니다. 형식적으로 말하자면, 몫 사상  $q: X \rightarrow X/A$ 와  $q: A \rightarrow A/A$ 는  $q_*: H_1(X, A) \rightarrow H_1(X/A, A/A)$ 를 유도하며,  $q_*$ 는 단사가 아닙니다.

그럼에도 불구하고,  $H_n(X, A) \cong \tilde{H}_n(X/A)$ 를 만족하는 좋은 공간  $A \subseteq X$ 에 대해서는,  $H_n(A)$ 와  $\tilde{H}_n(X/A)$ 에 기반하여  $H_n(X)$ 를 계산할 수 있을 것입니다 —  $A$ 와  $X/A$ 는 어떤 의미에서  $X$ 보다 더 작고 더 단순하다는 점에 주목하십시오.

**§73.2 긴 완전열**

정리 72.2.5을 상기해 보면, 이는 다음 수열들이

$$\cdots \rightarrow H_n(A) \rightarrow H_n(X) \rightarrow H_n(X, A) \rightarrow H_{n-1}(A) \rightarrow \cdots$$

그리고

$$\cdots \rightarrow \tilde{H}_n(A) \rightarrow \tilde{H}_n(X) \rightarrow H_n(X, A) \rightarrow \tilde{H}_{n-1}(A) \rightarrow \cdots$$

긴 완전열이라는 것을 말해줍니다. 문제 72F\*에 의해 우리는 심지어 다음의 긴 완전열도 얻습니다

$$\cdots \rightarrow H_n(B, A) \rightarrow H_n(X, A) \rightarrow H_n(X, B) \rightarrow H_{n-1}(B, A) \rightarrow \cdots$$

$A \subseteq B \subseteq X$ 에 대해.

이는  $X/B$ 가  $\frac{X/A}{B/A}$ 와 동형이라는 사실의 유사물입니다 — 우리는 “분수에서 공통 인수를 약분”하는 셈입니다.

위의 첫 번째 긴 완전열을 응용하면 다음을 얻습니다:

**보조정리 73.2.1 (축약 가능한 공간에 대한 상대 호몰로지)**

$X$ 를 위상 공간이라 하고,  $A \subseteq X$ 를 축약 가능하다고 합시다. 모든  $n$ 에 대해,

$$H_n(X, A) \cong \tilde{H}_n(X).$$

증명.  $A$ 가 축약 가능하므로, 모든  $n$ 에 대해  $\tilde{H}_n(A) = 0$ 입니다. 각  $n$ 에 대해 긴 완전열의 다음 구간이 주어집니다

$$\cdots \rightarrow \underbrace{\tilde{H}_n(A)}_{=0} \rightarrow \tilde{H}_n(X) \rightarrow H_n(X, A) \rightarrow \underbrace{\tilde{H}_{n-1}(A)}_{=0} \rightarrow \cdots$$

따라서  $0 \rightarrow \tilde{H}_n(X) \rightarrow H_n(X, A) \rightarrow 0$ 이 완전하므로, 이는  $H_n(X, A) \cong \tilde{H}_n(X)$ 임을 의미합니다.  $\square$

특히, 이 정리는  $A$ 가 한 점일 때에도 적용됩니다.  $A = \emptyset$ 인 경우 역시 주목할 만합니다. 이 결과들을 하나의 보조정리로 정리합니다:

**보조정리 73.2.2 (상대 호몰로지는 절대 호몰로지를 일반화한다)**

$X$ 를 임의의 공간이라 하고,  $* \in X$ 를 한 점이라 합시다. 그러면 모든  $n$ 에 대해,

$$H_n(X, \{*\}) \cong \tilde{H}_n(X) \quad \text{그리고} \quad H_n(X, \emptyset) = H_n(X).$$

## §73.3 쌍의 범주

이제 단순히  $H_n(X)$ 가 아니라  $H_n(X, A)$ 를 갖게 되었으므로, 자연스러운 다음 단계는 쌍에 대한 적절한 범주를 만들고 앞서와 같은 함자적 체계를 우리 스스로에게 부여하는 것입니다.

**정의 73.3.1.**  $\emptyset \neq A \subseteq X$ 와  $\emptyset \neq B \subseteq Y$ 를 부분공간이라 하고, 사상  $f: X \rightarrow Y$ 를 생각해 봅시다. 만약  $f^{\text{img}}(A) \subseteq B$ 이면 다음과 같이 씁니다

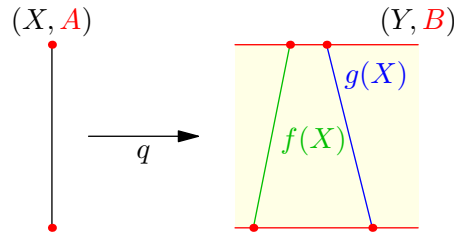
$$f: (X, A) \rightarrow (Y, B).$$

우리는  $f$ 가 쌍  $(X, A)$ 와  $(Y, B)$  사이의 **쌍의 사상**이라고 말합니다.

**정의 73.3.2.** 우리는  $f, g: (X, A) \rightarrow (Y, B)$ 가 “쌍의 사상들을 통해 호모토픽”하다면 **쌍-호모토픽**이라고 말합니다.

더 형식적으로, **쌍-호모토픽**  $f, g: (X, A) \rightarrow (Y, B)$ 는 사상  $F: [0, 1] \times X \rightarrow Y$ 이며, 이를  $F_t(X)$ 로 표기할 것인데,  $F$ 는 사상  $f, g: X \rightarrow Y$ 의 호모토픽이고 각  $F_t$  자체가 쌍의 사상입니다.

쌍-호모토픽인 전형적인  $f, g: (X, A) \rightarrow (Y, B)$ 는 다음과 같이 생겼을 수 있습니다. 모든  $t \in [0, 1]$ 에 대해  $F_t^{\text{img}}(A) \subseteq B$ 이어야 함에 주목하십시오.



따라서 우리는 자연스럽게 두 범주에 도달합니다:

- PairTop, 위상 공간의 쌍들의 범주, 그리고
- hPairTop, 사상이 오직 호모토피까지만 동치인 것을 제외하면 같은 범주입니다.

**정의 73.3.3.** 이전과 마찬가지로, 쌍  $(X, A)$ 와  $(Y, B)$ 가 hPairTop에서 동형이면 이 둘을 **쌍-호모토피 동치**라고 합니다. hPairTop의 동형사상을 **쌍-호모토피 동치사상**이라고 합니다.

**비고 73.3.4** — 쌍의 쌍-호모토피 동치는 정의 65.5.3에서 정의된 공간의 호모토피 동치를 자연스럽게 일반화한 것입니다. 실제로  $A = B = \emptyset$ 이면,  $X$ 가  $Y$ 와 호모토피 동치인 것은  $(X, \emptyset)$ 이  $(Y, \emptyset)$ 과 쌍-호모토피 동치인 것과 동치입니다.

프리즘 연산자를 이용하여 이전과 같은 방식을 반복하면 다음을 얻을 수 있습니다:

#### 보조정리 73.3.5 (상대 호몰로지의 유도 사상)

우리는 함수를 가지고 있습니다

$$H_n: \text{hPairTop} \rightarrow \text{Grp}.$$

즉,  $f: (X, A) \rightarrow (Y, B)$ 이면 유도된 사상을 얻습니다

$$f_*: H_n(X, A) \rightarrow H_n(Y, B).$$

그리고 이러한  $f$ 와  $g$ 가 쌍-호모토피 동치이면  $f_* = g_*$ 입니다.

이제 우리는 쌍에 대해 수축 가능 공간의 유사 개념을 원합니다. 즉,  $H_n(X, A) = 0$ 을 만족하는 공간의 쌍  $(X, A)$ 입니다. 올바른 정의는 다음과 같습니다:

**정의 73.3.6.**  $A \subseteq X$ 라 합시다.  $r: (X, A) \rightarrow (A, A)$ 가 쌍-호모토피 동치인 쌍의 사상이 존재하면,  $A$ 를  $X$ 의 **변형 수축**<sup>1</sup>이라고 합니다.

#### 예제 73.3.7 (변형 수축의 예시)

- 한 점  $p$ 가 공간  $X$ 의 변형 수축이면,  $X$ 는 수축 가능합니다. 왜냐하면 수축  $r: X \rightarrow \{*\}$ 가 (사상  $X \rightarrow X$ 로 볼 때) 항등 사상  $\text{id}_X: X \rightarrow X$ 와 호모토피하기 때문입니다.
- 구멍 뚫린 원판  $D^2 \setminus \{0\}$ 은 그 경계  $S^1$ 으로 변형 수축됩니다.
- 더 일반적으로,  $D^n \setminus \{0\}$ 은 그 경계  $S^{n-1}$ 으로 변형 수축됩니다.
- 마찬가지로,  $\mathbb{R}^n \setminus \{0\}$ 은 구  $S^{n-1}$ 로 변형 수축됩니다.

<sup>1</sup>다른 자료(예: [Ha02])에서는 이를 약한 의미에서의 변형 수축이라고 부를 수도 있습니다

물론 이 상황에서는 다음이 성립합니다

$$H_n(X, A) \cong H_n(A, A) = 0.$$

**연습문제 73.3.8.**  $A \subseteq V \subseteq X$ 이고  $A$ 가  $V$ 의 변형 수축이면, 모든  $n$ 에 대해  $H_n(X, A) \cong H_n(X, V)$ 임을 보이십시오. (문제 72F\*를 이용하십시오. 풀이는 다음 절에 있습니다.)

## §73.4 절단

이제 상대 호몰로지 군에 대한 정리 72.3.1의 유사 결과인, 핵심 기하학적 결과를 살펴보겠습니다.

### 정리 73.4.1 (절단)

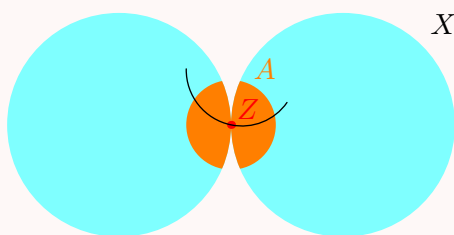
$Z \subseteq A \subseteq X$ 를  $Z$ 의 폐포가  $A$ 의 내부에 포함되는 부분공간이라 합시다. 그러면 포함 사상  $\iota: (X \setminus Z, A \setminus Z) \hookrightarrow (X, A)$ 가 (쌍의 사상으로서 볼 때) 상대 호몰로지 군의 동형사상을 유도합니다

$$H_n(X \setminus Z, A \setminus Z) \cong H_n(X, A).$$

이는 상대 호몰로지 군  $H_n(X, A)$ 를 계산할 때  $A$ 의 부분집합  $Z$ 를 절단(삭제)할 수 있음을 의미합니다. 이는 직관적으로 이해가 됩니다. 우리는 " $A$ 의 점들로 뭉을 취하고" 있으므로, 집합  $A$ 의 내부 구조는 그다지 중요하지 않아야 하기 때문입니다.

### 예제 73.4.2

절단은 사소해 보일 수 있습니다 ( $H_n(X, A)$ 에서 "상대 경계로 나눈 상대 사이클"의 경우,  $A$  내부에 있는 부분을  $Z$ 에 닿지 않을 때까지 조금씩 조정하기만 하면 됩니다). 하지만 이것이 항상 가능하지는 않다는 것을 깨닫기 전까지의 이야기입니다 — 자칫하면 사이클을 잘라 분리해 버릴 수도 있습니다! 예를 들어:



절단의 주요 응용은  $H_n(X, A) \cong \tilde{H}_n(X/A)$ 가 언제 성립하는지를 결정하는 것입니다. 답은:

### 정리 73.4.3 (상대 호몰로지 $\implies$ 몫공간)

$X$ 를 공간이라 하고,  $A$ 를 닫힌 부분공간이라 하되  $A$ 가 어떤 열린집합  $V \subseteq X$ 의 변형 수축이라고 하겠습니다. 그러면 몫사상  $q: X \rightarrow X/A$ 는 다음과 같은 동형사상을 유도합니다

$$H_n(X, A) \cong H_n(X/A, A/A) \cong \tilde{H}_n(X/A).$$

증명의 핵심 아이디어는 다음과 같습니다:  $H(X, A) \cong H(X/A, A/A)$ 가 반드시 성립하는 것은 아니지만(실제로 앞서 두 가지 반례를 살펴보았습니다),  $A$ 를 잘라내면 자명하게

$H(X-A, A-A) \cong H(X/A-A/A, A/A-A/A)$ 가 성립합니다. 안타깝게도 이 군은  $H(X, A)$ 와 동형이 아니므로, 집합  $V$ 를 이용하여 이를 바로잡습니다 — 즉,  $H(X-A, V-A) \cong H(X/A-A/A, V/A-A/A)$ 입니다. 나머지 작업은 절제 정리와 변형 수축을 이용하여 좌변이  $H(X, A)$ 와 동형이고 우변이  $H(X/A)$ 와 동형임을 보이는 것입니다.

증명. 가정에 의해 다음과 같은 쌍의 사상들을 고려할 수 있습니다:

$$\begin{aligned} r &: (V, A) \rightarrow (A, A) \\ q &: (X, A) \rightarrow (X/A, A/A) \\ \hat{q} &: (X-A, V-A) \rightarrow (X/A-A/A, V/A-A/A). \end{aligned}$$

더욱이  $r$ 은 쌍-호모토피 동치입니다. 삼중쌍의 긴 완전열(이는 **문제 72F\***이었습니다)을 고려하면 다음과 같은 도식을 얻습니다

$$\begin{array}{ccccccc} H_n(V, A) & \longrightarrow & H_n(X, A) & \xrightarrow{f} & H_n(X, V) & \longrightarrow & H_{n-1}(V, A) \\ \downarrow \cong r & & & & & & \downarrow \cong r \\ \underbrace{H_n(A, A)}_{=0} & & & & & & \underbrace{H_{n-1}(A, A)}_{=0} \end{array}$$

여기서 동형사상들은  $r$ 이 쌍-호모토피 동치이기 때문에 성립합니다. 따라서  $f$ 는 동형사상입니다. 마찬가지로 사상

$$g: H_n(X/A, A/A) \rightarrow H_n(X/A, V/A)$$

은 동형사상입니다.

이제 다음의 가환 도식을 고려하겠습니다

$$\begin{array}{ccccc} H_n(X, A) & \xrightarrow{f} & H_n(X, V) & \xleftarrow{\text{Excise}} & H_n(X-A, V-A) \\ \downarrow q_* & & & & \downarrow \cong \hat{q}_* \\ H_n(X/A, A/A) & \xrightarrow{g} & H_n(X/A, V/A) & \xleftarrow{\text{Excise}} & H_n(X/A-A/A, V/A-A/A) \end{array}$$

그리고 가장 오른쪽 화살표  $\hat{q}_*$ 가 동형사상임을 관찰합니다. 이는  $A$  바깥에서 사상  $\hat{q}$ 가 항등 사상이기 때문입니다. 우리는  $f$ 와  $g$ 가 동형사상임을 알고 있으며, "절제(Excise)"라고 표시된 두 화살표 역시 (절제에 의해) 동형사상임을 알고 있습니다. 이로부터  $q_*$ 가 동형사상임을 결론지을 수 있습니다. 물론 점에 대한 상대 호몰로지가 단지 상대 호몰로지 군일 뿐이라는 사실은 이미 알고 있습니다(이는 **보조정리 73.2.1**의 중요한 경우입니다).  $\square$

## §73.5 몇 가지 응용

절제의 좋은 응용 중 하나는  $\tilde{H}_n(X \vee Y)$ 를 계산하는 것입니다.

### 정리 73.5.1 (빼기합의 호몰로지)

$X$ 와  $Y$ 를 각각 기준점  $x_0 \in X$ 와  $y_0 \in Y$ 를 가진 공간이라 하고, 각 점이 어떤 열린 근방의 변형 수축이라고 가정하겠습니다. 그러면 모든  $n$ 에 대해 다음이 성립합니다

$$\tilde{H}_n(X \vee Y) = \tilde{H}_n(X) \oplus \tilde{H}_n(Y).$$

증명.  $X \amalg Y$ 의 부분집합  $\{x_0, y_0\}$ 에 대해 정리 73.4.3를 적용하면,

$$\begin{aligned}\tilde{H}_n(X \vee Y) &\cong \tilde{H}_n((X \amalg Y)/\{x_0, y_0\}) \cong H_n(X \amalg Y, \{x_0, y_0\}) \\ &\cong H_n(X, \{x_0\}) \oplus H_n(Y, \{y_0\}) \\ &\cong \tilde{H}_n(X) \oplus \tilde{H}_n(Y).\end{aligned}\quad \square$$

또 다른 응용은  $H_n(S^m)$ 을 계산하는 두 번째 방법을 제공하는 것입니다. 이를 위해 우리는 다음을 증명하겠습니다

$$\tilde{H}_n(S^m) \cong \tilde{H}_{n-1}(S^{m-1})$$

임의의  $n, m > 1$ 에 대해. 하지만,

- $\tilde{H}_0(S^n)$ 은  $n = 0$ 일 때  $\mathbb{Z}$ 이고 그 외에는 0입니다.
- $\tilde{H}_n(S^0)$ 은  $n = 0$ 일 때  $\mathbb{Z}$ 이고 그 외에는 0입니다.

따라서  $\min\{m, n\}$ 에 대한 귀납법으로 우리는 직접

$$\tilde{H}_n(S^m) \cong \begin{cases} \mathbb{Z} & m = n \\ 0 & \text{그렇지 않으면} \end{cases}$$

을 얻는데, 이것이 바로 우리가 원했던 것입니다.

주장을 증명하기 위해, 쌍  $X = D^2$ 와  $A = S^1$ 로 이루어진 완전열을 생각해 봅시다.

**예제 73.5.2**  $((X, A) = (D^2, S^1))$ 에 대한 긴 완전열)

경계가  $S^1$ 인  $D^2$ (이는 수축 가능합니다)를 생각해 봅시다. 분명히  $S^1$ 은  $D^2 \setminus \{0\}$ 의 변형 수축이며, 경계 위의 모든 점을 융합하면  $D^2/S^1 \cong S^2$ 를 얻습니다. 따라서 다음과 같은 긴 완전열을 얻습니다

$$\begin{array}{ccccc}\tilde{H}_2(S^1) & \longrightarrow & \underbrace{\tilde{H}_2(D^2)}_{=0} & \longrightarrow & \tilde{H}_2(S^2) \\ & \searrow & & \nearrow & \\ \tilde{H}_1(S^1) & \longrightarrow & \underbrace{\tilde{H}_1(D^2)}_{=0} & \longrightarrow & \tilde{H}_1(S^2) \\ & \searrow & & \nearrow & \\ \tilde{H}_0(S^1) & \longrightarrow & \underbrace{\tilde{H}_0(D^2)}_{=0} & \longrightarrow & \underbrace{\tilde{H}_0(S^2)}_{=0}\end{array}$$

이 도식으로부터 우리는 다음을 읽어낼 수 있습니다

$$\dots, \quad \tilde{H}_3(S^2) = \tilde{H}_2(S^1), \quad \tilde{H}_2(S^2) = \tilde{H}_1(S^1), \quad \tilde{H}_1(S^2) = \tilde{H}_0(S^1).$$

더 일반적으로, 쌍  $(X, A) = (D^m, S^{m-1})$ 에 대한 완전열은  $\tilde{H}_n(S^m) \cong \tilde{H}_{n-1}(S^{m-1})$ 임을 보여주며, 이는 원하는 결론입니다.

## §73.6 차원의 불변성

여기 절제의 응용에 대한 마지막 예시가 있습니다.

**정의 73.6.1.**  $X$ 를 공간,  $p \in X$ 를 점이라 합시다.  $X$ 에서  $p$ 의  $k$ 번째 **국소 호몰로지 군**은 다음과 같이 정의됩니다

$$H_k(X, X \setminus \{p\}).$$

$p$ 의 임의의 열린 근방  $U$ 에 대해, 절제에 의해 다음이 성립함을 유의하십시오

$$H_k(X, X \setminus \{p\}) \cong H_k(U, U \setminus \{p\}).$$

따라서 이 국소 호몰로지 군은  $p$  근처의 공간에만 의존합니다.

**정리 73.6.2 (차원의 불변성, Brouwer 1910)**

$U \subseteq \mathbb{R}^n$ 과  $V \subseteq \mathbb{R}^m$ 을 공집합이 아닌 열린집합이라 합시다. 만약  $U$ 와  $V$ 가 동형이면,  $m = n$ 입니다.

증명.  $x \in U$ 인 점과 그 국소 호몰로지 군을 생각해 봅시다. 절제에 의해,

$$H_k(\mathbb{R}^n, \mathbb{R}^n \setminus \{x\}) \cong H_k(U, U \setminus \{x\}).$$

하지만  $\mathbb{R}^n \setminus \{x\}$ 가  $S^{n-1}$ 와 호모토피 동치이므로, **정리 72.2.5**의 긴 완전열은 다음을 알려줍니다

$$H_k(\mathbb{R}^n, \mathbb{R}^n \setminus \{x\}) \cong \begin{cases} \mathbb{Z} & k = n \\ 0 & \text{그렇지 않으면.} \end{cases}$$

유사하게,  $y \in V$ 가 주어지면 다음이 성립합니다

$$H_k(\mathbb{R}^m, \mathbb{R}^m \setminus \{y\}) \cong H_k(V, V \setminus \{y\}).$$

$U \cong V$ 이면, 따라서 우리는 다음을 유도합니다

$$H_k(\mathbb{R}^n, \mathbb{R}^n \setminus \{x\}) \cong H_k(\mathbb{R}^m, \mathbb{R}^m \setminus \{y\})$$

모든  $k$ 에 대해서 말입니다. 이는 물론  $m = n$ 일 때만 일어날 수 있습니다. □

## §73.7 생각해 볼 만한 조금 더 어려운 문제

**문제 73A.**  $X = S^1 \times S^1$ ,  $Y = S^1 \vee S^1 \vee S^2$ 라 합시다. 모든 정수  $n$ 에 대해

$$H_n(X) \cong H_n(Y)$$

임을 보이십시오.

**문제 73B** (Hatcher §2.1 연습문제 18).  $\mathbb{Q} \subset \mathbb{R}$ 을 생각해봅시다.  $\tilde{H}_1(\mathbb{R}, \mathbb{Q})$ 를 계산하십시오.

**문제 73C\*.** 위상  $n$ -다양체의 국소 호몰로지 군은 무엇입니까?

**문제 73D.**

$$X = \{(x, y) \mid x \geq 0\} \subseteq \mathbb{R}^2$$

가 반평면을 나타낸다고 합시다.  $X$ 의 점들의 국소 호몰로지 군은 무엇입니까?



**문제 73E** (브라우어-조르당 분리 정리, 조르당 곡선 정리의 일반화).  $X \subseteq \mathbb{R}^n$ 이  $S^{n-1}$ 과 위상동형인 부분집합이라고 합시다.  $\mathbb{R}^n \setminus X$ 가 정확히 두 개의 경로 연결 성분을 가짐을 증명하십시오.

# 74 보너스: 세포 호몰로지

이제 세포 호몰로지를 도입하겠습니다. 이는 본질적으로 우리가 원하는 임의의 CW 복합체의 호몰로지 군을 계산할 수 있게 해줍니다.

## §74.1 차수

이 절의 대표적인 예:  $z \mapsto z^d$ 는 차수  $d$ 를 갖습니다.

임의의  $n > 0$ 과 사상  $f: S^n \rightarrow S^n$ 에 대해, 다음을 고려합시다:

$$f_*: \underbrace{H_n(S^n)}_{\cong \mathbb{Z}} \rightarrow \underbrace{H_n(S^n)}_{\cong \mathbb{Z}}$$

이는 어떤 상수  $d$ 에 의한 곱셈이어야 합니다. 이  $d$ 를  $f$ 의 **차수**라 부르며,  $\deg f$ 로 표기합니다.

**질문 74.1.1.**  $\deg(f \circ g) = \deg(f) \deg(g)$ 임을 보이십시오.

**예제 71.2.12**에서 언급했듯이, 대략적으로 말하면:

$\deg f$ 는  $\text{im } f$ 가  $S^n$ 을 몇 번 감는지를 셉니다.

또는,  $\text{im } f$ 가 몇 개의 “ $S^n$  자루”로 이루어져 있는지를 셉니다.

### 예제 74.1.2 (차수)

- (a)  $n = 1$ 일 때, 사상  $z \mapsto z^k$  ( $S^1 \subseteq \mathbb{C}$ 로 볼 때)는 차수  $k$ 를 갖습니다.
- (b) 반사 사상  $(x_0, x_1, \dots, x_n) \mapsto (-x_0, x_1, \dots, x_n)$ 은 차수  $-1$ 을 갖습니다; 이를 증명하지는 않겠지만, 기하학적으로 이는 명백해야 합니다.
- (c) 대척점 사상  $x \mapsto -x$ 는 위와 같은 반사  $n + 1$ 개의 합성이므로 차수  $(-1)^{n+1}$ 을 갖습니다. 이 사상을  $-\text{id}$ 로 표기합니다.

당연히,  $f$ 와  $g$ 가 호모토픽하다면  $\deg f = \deg g$ 입니다. 실제로 Hopf의 정리에 따르면 이것이 분류 불변량입니다:  $\deg f = \deg g$ 이기만 하면 언제든지  $f$ 와  $g$ 는 호모토픽합니다. 이것의 한 가지 좋은 응용은 다음과 같습니다:

### 정리 74.1.3 (털 난공 정리)

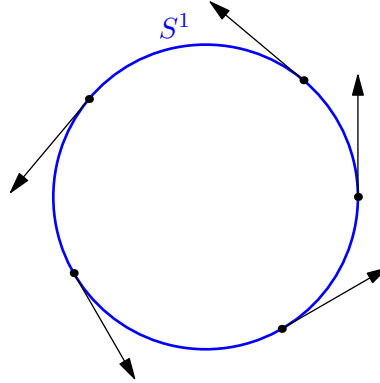
$n > 0$ 이 짝수이면,  $S^n$ 은 연속적인 0이 아닌 접벡터장을 갖지 않습니다.

증명. 벡터들이 0이 아니라면 일반성을 잃지 않고 노름이 1이라고 할 수 있습니다; 즉 모든  $x$ 에 대해 직교하는 단위벡터  $v(x)$ 가 존재합니다. 그러면 다음과 같이 호모토픽 사상  $F: S^n \times [0, 1] \rightarrow S^n$ 을 구성할 수 있습니다:

$$(x, t) \mapsto (\cos \pi t)x + (\sin \pi t)v(x).$$

이는  $\text{id}$ 에서  $-\text{id}$ 로 가는 호모토피를 줍니다. 따라서  $\deg(\text{id}) = \deg(-\text{id})$ 이며, 이는  $1 = (-1)^{n+1}$ 을 의미하므로  $n$ 은 홀수여야 합니다.  $\square$

물론,  $n$ 이 홀수일 때는 언제나 그러한 벡터장을 구성할 수 있습니다. 예를 들어,  $n = 1$ 일 때 그러한 벡터장이 아래에 그려져 있습니다.



## §74.2 세포 사슬 복합체

시작하기 전에, 다음을 기술합니다:

### 보조정리 74.2.1 (CW 호몰로지 군)

$X$ 를 CW 복합체라 합시다. 그러면

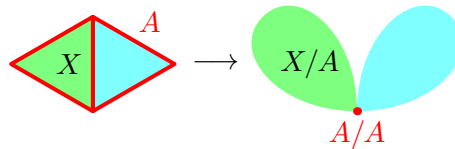
$$H_k(X^n, X^{n-1}) \cong \begin{cases} \mathbb{Z}^{\oplus X \text{의 } \#n\text{-셀}} & k = n \\ 0 & \text{그 외의 경우.} \end{cases}$$

그리고

$$H_k(X^n) \cong \begin{cases} H_k(X) & k \leq n-1 \\ 0 & k \geq n+1. \end{cases}$$

증명. 첫 번째 부분은  $(X^n, X^{n-1})$ 이 정리 73.4.3의 가정을 만족한다는 것을 언급함으로써 즉시 얻어집니다. 따라서  $H_k(X^n, X^{n-1}) \cong \tilde{H}_k(X^n/X^{n-1})$ 이며,  $X^n/X^{n-1}$ 은 여러 개의  $n$ -구의 켜기합입니다.

예를 들어,  $n = 2$ 인 경우 (여기서는 "구"가 풍선 모양의 덩어리로 그려져 있습니다):



두 번째 부분에서는  $k$ 를 고정하고,  $n \leq k-1$  또는  $n \geq k+2$ 인 한

$$\underbrace{H_{k+1}(X^n, X^{n-1})}_{=0} \rightarrow H_k(X^{n-1}) \rightarrow H_k(X^n) \rightarrow \underbrace{H_k(X^n, X^{n-1})}_{=0}.$$

따라서 다음과 같은 동형사상을 얻습니다

$$H_k(X^{k-1}) \cong H_k(X^{k-2}) \cong \dots \cong H_k(X^0) = 0$$

그리고

$$H_k(X^{k+1}) \cong H_k(X^{k+2}) \cong \dots \cong H_k(X). \quad \square$$

따라서 군  $H_k(X^k, X^{k-1})$ 이 매우 좋다는 것을 알 수 있습니다: 이들은  $X$ 의 세포들을 기저로 가지는 자유 아벨 군입니다. 그래서 이들에게 이름을 붙입니다:

**정의 74.2.2.** CW 복합체  $X$ 에 대해, 다음과 같이 정의합니다

$$\text{Cells}_k(X) = H_k(X^k, X^{k-1})$$

여기서 관례상  $\text{Cells}_0(X) = H_0(X^0, \emptyset) = H_0(X^0)$ 입니다. 따라서  $\text{Cells}_k(X)$ 는  $X$ 의  $k$ -세포들을 기저로 가지는 아벨 군입니다.

이제  $\text{Cells}_k = H_k(X^k, X^{k-1})$ 을 사용하여, 우리의 긴 완전열을 이용해 이들 사이의 사상을 엮어 봅시다. 다음 도식을 살펴봅시다.

$$\begin{array}{ccccccc}
 & & \underbrace{H_3(X^2)}_{=0} & & & & \\
 & & \downarrow 0 & & & & \\
 \boxed{\text{Cells}_4(X)} & \xrightarrow{\partial_4} & H_3(X^3) & \longrightarrow & \underbrace{H_3(X^4)}_{\cong H_3(X)} & \xrightarrow{0} & \underbrace{H_3(X^4, X^3)}_{=0} \\
 & \searrow d_4 & \downarrow \hookrightarrow & & & & \\
 & & \boxed{\text{Cells}_3(X)} & & & & \\
 & & \downarrow \partial_3 & \searrow d_3 & & & \\
 \underbrace{H_2(X^1)}_{=0} & \xrightarrow{0} & H_2(X^2) & \hookrightarrow & \boxed{\text{Cells}_2(X)} & \xrightarrow{\partial_2} & H_1(X^1) \longrightarrow \underbrace{H_1(X^2)}_{\cong H_1(X)} \xrightarrow{0} \underbrace{H_1(X^2, X^1)}_{=0} \\
 & & \downarrow & & \searrow d_2 & & \downarrow \hookrightarrow \\
 & & \underbrace{H_2(X^3)}_{\cong H_2(X)} & & & & \boxed{\text{Cells}_1(X)} \\
 & & \downarrow 0 & & & & \downarrow \partial_1 \\
 \underbrace{H_2(X^3, X^2)}_{=0} & & & & \underbrace{H_0(\emptyset)}_{=0} \xrightarrow{0} & H_0(X^0) \hookrightarrow & \boxed{\text{Cells}_0(X)} \xrightarrow{\partial_0} \dots \\
 & & & & & & \downarrow \\
 & & & & & & \underbrace{H_0(X^1)}_{\cong H_0(X)} \\
 & & & & & & \downarrow 0 \\
 & & & & & & \underbrace{H_0(X^1, X^0)}_{=0}
 \end{array}$$

아이디어는, 인접한 스켈레톤들에 의해 생성된 모든 완전열을 취하여, 이를 군  $H_k(X^k)$ 에서 서로 엮은 것으로, 완전열의 절반은 세로로, 나머지 절반은 가로로 배치됩니다.

이 경우, 합성에 의해 그림과 같이  $H_k(X^k, X^{k-1})$  사이의 파란색 사상들의 수열이 생성됩니다.

**질문 74.2.3.** 인접한 두 파란색 화살표의 합성이 영임을 보이십시오.

따라서 위의 도식으로부터, 다음과 같은 화살표들의 수열을 읽어낼 수 있습니다

$$\dots \xrightarrow{d_5} \text{Cells}_4(X) \xrightarrow{d_4} \text{Cells}_3(X) \xrightarrow{d_3} \text{Cells}_2(X) \xrightarrow{d_2} \text{Cells}_1(X) \xrightarrow{d_1} \text{Cells}_0(X) \xrightarrow{d_0} 0.$$

이는 **세포 사슬 복합체**라 불리는 사슬 복합체입니다; 앞서 언급했듯이 모든 호몰로지 군은 자유 군이지만, 이들은 대부분의 합리적인 CW 복합체에 대해 유한 생성이기도 하다는 점에서 특히 좋습니다 (앞서 다루었던 거대한  $C_\bullet(X)$ 와는 다릅니다). 다시 말해,  $H_k(X^k, X^{k-1})$ 은 실제로 다룰 수 있는 특히 좋은 "구체적인" 자유 군입니다.

우리가 이에 관심을 가지는 또 다른 이유는 실제로 다음과 같기 때문입니다:

**정리 74.2.4** (세포 사슬 복합체는  $H_n(X)$ 를 줍니다)

세포 사슬 복합체의  $k$ 번째 호몰로지 군은  $H_k(X)$ 와 동형입니다.

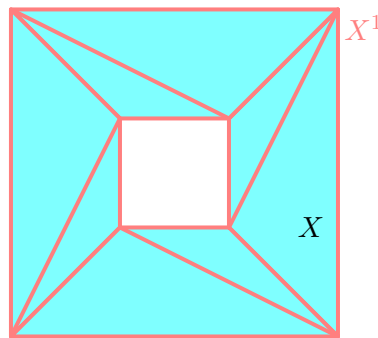
증명. 도식으로부터 따라 나옵니다; **문제 74D**. □

## §74.3 여담: 왜 호몰로지 군들이 같은가?

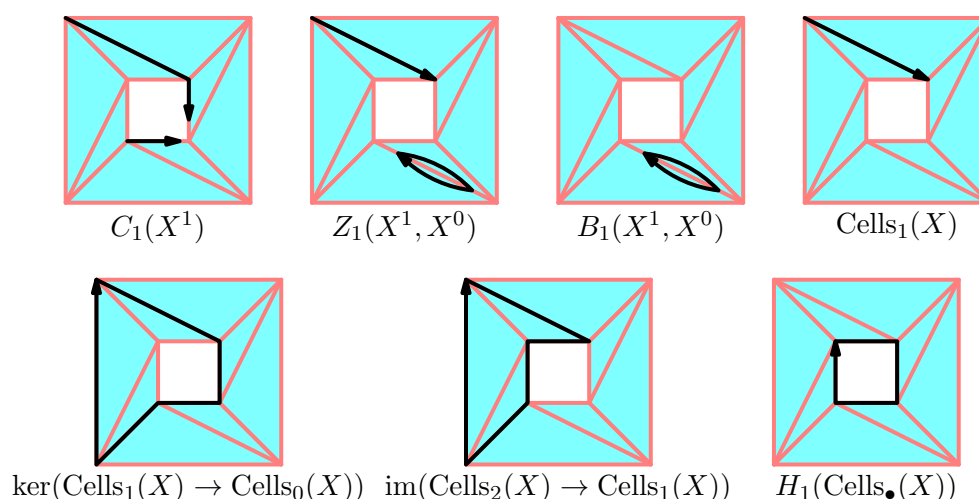
이를 설명하는 또 다른 직관이 있습니다 — 대략적으로 말하면,

$$H_k(\text{Cells}_\bullet(X)) = \frac{\text{정렬된 사이클}}{\text{정렬된 경계}} = \frac{\text{정렬된 사이클} \times \text{잡음}}{\text{정렬된 경계} \times \text{잡음}} = \frac{\text{사이클}}{\text{경계}} = H_k(X).$$

설명해 보겠습니다. 다음과 같이 생긴 CW 복합체  $X$ 를 생각해 봅시다. 여기서  $X^1$ 은 빨간색으로 그려져 있습니다. 각 파란색 영역은 하나의 2-세포에 해당합니다.



그러면, 다음 그림을 살펴봅시다.



많아 보이니, 설명해 보겠습니다.

- 첫 번째 그림은  $C_1(X^1)$ 의 전형적인 원소를 묘사합니다 — 즉,  $X^1$ 에 포함된 1-사슬로서,  $\Delta^1$ 에서  $X^1$ 로 가는 두 사상의 형식적 합이며, 그 상은 검은색 화살표로 그려져 있습니다.

사상들의 상만이 묘사되어 있으며, 단체  $\Delta^1$ 의 어느 점이  $X^1$  내부의 어느 점으로 대응되는지와 같은 정보는 나타나 있지 않다는 점에 유의하십시오 — 비록 서로 다른 연속 사상들은  $C_1(X^1)$ 의 서로 다른 원소를 만들어내지만 말입니다.

- 두 번째 그림은  $Z_1(X^1, X^0)$ 의 전형적인 원소, 즉 상대 사이클을 나타냅니다.

상대 사이클이나 군  $Z_1(X^1, X^0)$ 이 무엇인지 공식적으로 정의한 적은 없지만,  $Z_1(X^1)$ 의 정의로부터 그 정의를 짐작할 수 있습니다 — 이는 경계가 소멸하는  $C_1(X^1, X^0) = C_1(X^1)/C_1(X^0)$ 의 부분군입니다.

아래쪽 고리가 평평하게 그려진 것은 그저 보기 좋게 하기 위함일 뿐이며 — 전체는 빨간색 골격, 즉  $X^1$  안에 포함되어 있습니다.

물론 몫의 원소이므로 대표 원소 하나만 그려져 있습니다 — ”모드로 없앤” 부분은  $X^0$  안에 완전히 포함된 사슬, 즉 몇몇 꼭짓점들입니다.

- 세 번째 그림은  $B_1(X^1, X^0)$ 의 전형적인 원소, 즉 상대 경계를 나타냅니다.

이는  $\text{im}(C_2(X^1, X^0) \xrightarrow{\partial} C_1(X^1, X^0))$ 에 속합니다 — 말로 풀면, 경계가 그려진 원소와 같아지는 어떤 2-사슬이 존재한다는 것입니다.

- 네 번째 그림은  $Cells_1(X)$ 의 전형적인 원소, 즉 ”상대 경계로 나눈 상대 사이클”을 나타냅니다.

이 군이  $X$ 의 각 1-세포로 생성되는 아벨 군과 어떻게 동형인지는 직관적으로 명백하기를 바랍니다.

사실 이러한 원소 각각을, 모든 끝점이 어떤 꼭짓점 안에 놓이는(즉 그 원소의 경계가  $X^0$  안에 있는)  $C_1(X^1)$ 의 ”정렬된 원소”로 생각할 수 있으며, 각 1-세포에 대해 그 세포를 덮는 정준 1-단체가 하나 선택됩니다(같은 상을 갖는 서로 다른 단체들은 직관적으로 속도를 바꾸는 ”재매개변수화”에 대응하며, 단체와 그 재매개변수화의 차이는 사실  $B_1(X^1, X^0)$ 의 원소임에 유의하십시오 — 이를 엄밀하게 만들어 보십시오! 힌트: 프리즘 연산자를 사용하십시오.)

- 다섯 번째 그림은 다음의 전형적인 원소를 나타냅니다

$$\ker(Cells_1(X) \xrightarrow{\partial} Cells_0(X))$$

이는 위에서 설명한 대로 "정렬된" 1-사이클(즉  $Z_1(X)$ 의 원소)인 "세포 사이클"로 생각할 수 있습니다.

- 여섯 번째 그림은 다음의 전형적인 원소를 나타냅니다

$$\text{im} \left( \text{Cells}_2(X) \xrightarrow{\partial} \text{Cells}_1(X) \right)$$

이는 위와 같은 의미에서 "정렬된" 1-경계(즉  $B_1(X)$ <sup>1</sup>의 원소)인 "세포 경계"로 생각할 수 있습니다.

- 마지막으로, 마지막 그림은  $H_1(\text{Cells}_\bullet(X))$ 이며, 이는

$$H_1(\text{Cells}_\bullet(X)) = \frac{\ker \left( \text{Cells}_1(X) \xrightarrow{\partial} \text{Cells}_0(X) \right)}{\text{im} \left( \text{Cells}_2(X) \xrightarrow{\partial} \text{Cells}_1(X) \right)}.$$

또는 대략적으로 말하면,

$$H_1(\text{Cells}_\bullet(X)) = \frac{\text{정렬된 사이클}}{\text{정렬된 경계}}.$$

이것이 바로  $\frac{\text{정렬된 사이클}}{\text{정렬된 경계}} = \frac{\text{사이클}}{\text{경계}}$ 가 의미하는 바입니다. 적절한 형식화와 정준 단체들의 임의의 선택을 통해<sup>2</sup> 위의 논증을 엄밀하게 만들 수 있습니다.

"잡음"이란 무엇을 의미할까요? 이 부분은 명백하기를 바라지만, 요점은 정렬된 사이클이 여전히 사이클(즉  $Z_1(X)$ 의 원소)로 남아 있으면서도(재매개변수화나  $B_1(X^1, X^0)$ 의 원소를 더함으로써) 약간 "이리저리 움직여질" 수 있다는 것입니다. 정렬된 경계에 대해서도 마찬가지입니다.

그러므로 요점은 — 분자와 분모의 공통된 잡음 인자를 "약분"할 수 있으며, 그 결과는 변하지 않는다는 것입니다.

단체 근사에 대한 형식적인 논의는 [Ha02]를 참고하십시오.

## §74.4 응용: 베티 수를 통한 오일러 지표

이것의 좋은 응용으로는 유한 CW 복합체  $X$ 의 **오일러 지표**를 정의하는 것이 있습니다. 물론 우리는 다음과 같이 쓸 수 있습니다

$$\chi(X) = \sum_n (-1)^n \cdot \#(X \text{의 } n\text{-세포})$$

이는 익숙한  $V - E + F$  공식을 일반화합니다. 그러나 이 정의는 CW 복합체의 선택에 의존한다는 점에서 만족스럽지 않은데, 우리는 사실  $\chi(X)$ 가 공간  $X$  자체에만 의존하고 (어떻게 만들어졌는지에 의존하지 않기를) 원하기 때문입니다. 이를 염두에 두고 다음을 증명합니다:

### 정리 74.4.1 (베티 수를 통한 오일러 지표)

임의의 유한 CW 복합체  $X$ 에 대해 다음이 성립합니다

$$\chi(X) = \sum_n (-1)^n \text{rank } H_n(X).$$

<sup>1</sup>이는  $B_1(X^1)$ 의 원소가 아닙니다! 그 이유를 생각해 보십시오.

<sup>2</sup>엄밀히 말하면  $X$  위에 이른바  $\Delta$ -복합체 구조가 필요하지만, 냅킨에서는  $\Delta$ -구조를 정의하지 않습니다. 자세한 내용은 [Ha02]를 참고하십시오.

따라서  $\chi(X)$ 는 CW 분해의 선택에 의존하지 않습니다. 다음의 수들은

$$b_n = \text{rank } H_n(X)$$

$X$ 의 **베티 수**라고 부릅니다. 실제로 이를 이용해 임의의 적당한 공간에 대해  $\chi(X)$ 를 정의할 수 있습니다.  $X$ 가 CW 복합체인 (흔한) 경우 이 정의가 오일러 지표의 일반적인 정의와 일치하므로 우리는 만족스럽습니다.

증명.  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow D \rightarrow 0$ 이 완전열이면  $\text{rank } B + \text{rank } D = \text{rank } A + \text{rank } C$ 라는 사실을 인용합니다. 그러면 예를 들어 다음 행은

$$\underbrace{H_2(X^1)}_{=0} \xrightarrow{0} H_2(X^2) \hookrightarrow H_2(X^2, X^1) \xrightarrow{\partial_2} H_1(X^1) \rightarrow \underbrace{H_1(X^2)}_{\cong H_1(X)} \xrightarrow{0} \underbrace{H_1(X^2, X^1)}_{=0}$$

세포 도식에서 나온 것으로

$$\#(2\text{-세포}) + \text{rank } H_1(X) = \text{rank } H_2(X^2) + \text{rank } H_1(X^1).$$

더 일반적으로,

$$\#(k\text{-셀}) + \text{rank } H_{k-1}(X) = \text{rank } H_k(X^k) + \text{rank } H_{k-1}(X^{k-1})$$

이는  $H_{-1}$  항을 제외하면  $k = 0$ 에 대해서도 성립합니다( $\#0\text{-셀} = \text{rank } H_0(X^0)$ 는 자명하므로). 이를  $(-1)^k$ 로 곱하고  $k \geq 0$ 에 걸쳐 합하면 결론을 얻습니다.  $\square$

#### 예제 74.4.2 (베티 수의 예시)

- (a)  $S^n$ 의 베티 수는  $b_0 = b_n = 1$ 이고 나머지는 0입니다. 오일러 지표는  $1 + (-1)^n$ 입니다.
- (b) 원환면  $S^1 \times S^1$ 의 베티 수는  $b_0 = 1, b_1 = 2, b_2 = 1$ 이고 나머지는 0입니다. 따라서 오일러 지표는 0입니다.
- (c)  $\mathbb{CP}^n$ 의 베티 수는  $b_0 = b_2 = \dots = b_{2n} = 1$ 이고 나머지는 0입니다. 따라서 오일러 지표는  $n + 1$ 입니다.
- (d) 클라인 병의 베티 수는  $b_0 = 1, b_1 = 1$ 이고 나머지는 0입니다. 따라서 오일러 지표는 0으로, 구와 같습니다(이는 이들의 CW 구조가 같은 수의 세포를 사용하기 때문이기도 합니다).

$S^n, S^1 \times S^1, \mathbb{CP}^n$ 과 같은 “좋은” 공간에서는 베티 수에  $b_k = b_{n-k}$ 라는 멋진 대칭성이 있음을 알 수 있습니다. 이는 더 일반적으로도 성립하는 사실입니다. 푸앵카레쌍대성과 **문제 76A†**를 참고하십시오.

## §74.5 세포 경계 공식

실제로 사상  $d_n$ 이 무엇인지 명시적으로 기술할 수 있습니다.  $H_k(X^k, X^{k-1})$ 가  $X$ 의  $k$ -세포를 기저로 가짐을 상기하면, 다음을 얻습니다:

### 정리 74.5.1 ( $k = 1$ 에 대한 세포 경계 공식)

$k = 1$ 일 때,

$$d_1: \text{Cells}_1(X) \rightarrow \text{Cells}_0(X)$$

는 단순히 경계 사상입니다.

**정리 74.5.2** ( $k > 1$ 에 대한 세포 경계)

$k > 1$ 을 양의 정수라 합시다.  $e^k$ 를  $k$ -세포라 하고,  $\{e_\beta^{k-1}\}_\beta$ 가  $X$ 의 모든  $(k-1)$ -세포를 나타낸다고 합시다. 그러면

$$d_k: \text{Cells}_k(X) \rightarrow \text{Cells}_{k-1}(X)$$

는 기저 원소에 대해 다음과 같이 주어집니다

$$d_k(e^k) = \sum_{\beta} d_{\beta} e_{\beta}^{k-1}$$

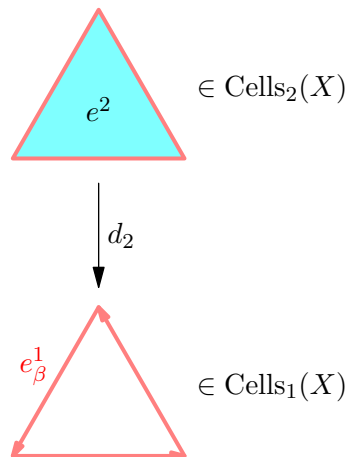
여기서  $d_{\beta}$ 는 다음 합성 사상의 차수입니다

$$S^{k-1} = \partial e^k \xrightarrow{\text{붙이다}} X^{k-1} \rightarrow S_{\beta}^{k-1}.$$

여기서 첫 번째 화살표는  $e^k$ 의 부착 사상이고, 두 번째 화살표는  $X^{k-1} \setminus e_{\beta}^{k-1}$ 를 한 점으로 붕괴시키는 몫사상입니다.

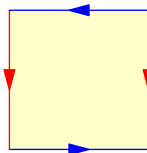
여기서 차수는 무엇을 하고 있는 것일까요? 기저 원소  $e^k \in \text{Cells}_k(X)$ 는 단지 하나의  $k$ -세포이고, 그 경계는 단지 그 경계를 이루는 세포들이어야 함을 기억하십시오.

위와 같은 시각화를 통해 다음과 같은 것을 할 수 있습니다.



하지만 그리 쉽지 않습니다! CW 복합체에서  $k$ -세포의 경계는  $X^{k-1}$  안의 임의의 점들로 융합될 수 있으므로,  $k$ -세포의 "모서리"가 반드시  $(k-1)$ -세포일 필요는 없다는 점에 유의하십시오.

설상가상으로, 때로는 중복된 모서리가 있을 수 있습니다 — 클라인 병에서 그려진 마주 보는 두 모서리 각 쌍은 실제로 방향이 다를 수 있는 같은 모서리입니다.



이러한 경우, 각 모서리의 중복도를 세어야 합니다 — 그리고 이것이 바로 사상의 차수가 세는 것입니다! 잠시 후 클라인 병의 호몰로지 군을 계산하는 명시적인 예를 살펴보겠습니다.

이는 CW 복합체의 호몰로지 군을 계산하는 알고리즘을 제공합니다:

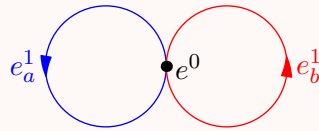
- 세포 사슬 복합체를 구성합니다. 여기서  $\text{Cells}_k(X)$ 는  $\mathbb{Z}^{\oplus \#k\text{-셀}}$ 입니다.

- $d_1: \text{Cells}_1(X) \rightarrow \text{Cells}_0(X)$ 은 그냥 경계 사상입니다 (따라서  $d_1(e^1)$ 은 두 끝점의 차이입니다).
- $k > 1$ 에 대해, 기저 원소 위에서  $d_k: \text{Cells}_k(X) \rightarrow \text{Cells}_{k-1}(X)$ 를 다음과 같이 계산합니다. 각  $k$ -세포  $e^k$ 에 대해 다음을 반복하십시오:
  - 모든  $k-1$  세포  $e_\beta^{k-1}$ 에 대해,  $e^k$ 의 경계를  $e_\beta^{k-1}$ 의 경계에 용접했을 때의 차수를 계산하며, 이를  $d_\beta$ 라 합니다.
  - 그러면  $d_k(e^k) = \sum_\beta d_\beta e_\beta^{k-1}$ 입니다.
- 이제 세포 사슬 복합체의 사상들을 얻었으므로, (핵을 상으로 나눈 몫을 취하여) 호몰로지를 직접 계산할 수 있습니다.

예를 들어 이를 이용하여 토러스의 호몰로지 군을 다시 계산할 수 있으며, 클라인 병 및 다른 공간들에 대해서도 마찬가지입니다.

### 예제 74.5.3 (토러스의 세포 호몰로지)

이전과 같이  $e^0, e_a^1, e_b^1, e^2$ 로 구성된 토러스를 생각해 봅시다. 여기서  $e^2$ 는 단어  $aba^{-1}b^{-1}$ 를 통해 붙여집니다. 예를 들어,  $X^1$ 은 다음과 같습니다



세포 사슬 복합체는 다음과 같습니다

$$0 \longrightarrow \mathbb{Z}e^2 \xrightarrow{d_2} \mathbb{Z}e_a^1 \oplus \mathbb{Z}e_b^1 \xrightarrow{d_1} \mathbb{Z}e^0 \xrightarrow{d_0} 0$$

이제 세포 경계 공식을 적용해 봅시다:

- $d_1$ 이 경계 공식이었음을 상기하십시오.  $d_1(e_a^1) = e_0 - e_0 = 0$ 이고 마찬가지로  $d_1(e_b^1) = 0$ 입니다. 따라서  $d_1 = 0$ 입니다.
- $d_2$ 에 대해서는,  $e^2$ 의 경계가  $e_a^1$ 에 미치는 상을 생각해 봅시다.  $X^1$  주위를 따라, 이는  $e_a^1$ 를 한 번,  $e_b^1$ 를 한 번, 다시  $e_a^1$ 를 (반대 방향으로) 한 번, 그리고 다시  $e_b^1$ 를 한 번 감쌉니다.  $e_b^1$  전체를 한 점으로 붕괴시키면, 이 사상의 차수가 0임을 알 수 있습니다. 따라서  $d_2(e^2)$ 에는  $e_a^1$  계수가 없습니다. 마찬가지로  $e_b^1$  계수도 없으므로,  $d_2 = 0$ 입니다.

따라서

$$d_1 = d_2 = 0.$$

이므로 복합체의 모든 사상에서 사상의 핵은 전체 공간이고 상은  $\{0\}$ 입니다. 따라서 호몰로지 군은  $\mathbb{Z}, \mathbb{Z}^{\oplus 2}, \mathbb{Z}$ 입니다.

### 예제 74.5.4 (클라인 병의 세포 호몰로지)

$X$ 를 클라인 병이라 합시다. 이전과 같이 세포  $e^0, e_a^1, e_b^1, e^2$ 를 생각해 보되, 이번에는  $e^2$ 가 단어  $abab^{-1}$ 를 통해 붙여집니다. 따라서  $d_1$ 은 여전히 영이지만, 이번에는 대신  $d_2(e^2) = 2e_a^1$ 가 됩니다 (왜일까요?). 따라서 우리의 도식은 다음과 같습니다

$$0 \xrightarrow{0} \mathbb{Z}e^2 \xrightarrow{d_2} \mathbb{Z}e_a^1 \oplus \mathbb{Z}e_b^1 \xrightarrow{d_1} \mathbb{Z}e^0 \xrightarrow{d_0} 0$$

$$e^2 \longmapsto 2e_a^1$$

$$e_1^a \longmapsto 0$$

$$e_1^b \longmapsto 0$$

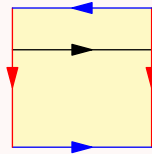
그러므로  $H_0(X) \cong \mathbb{Z}$ 임을 얻지만, 이번에는

$$H_1(X) \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

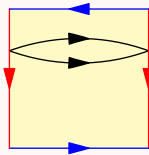
입니다 (이는  $\mathbb{Z}^{\oplus 2}$ 를  $2\mathbb{Z}$ 의 사본으로 나눈 몫입니다). 또한  $\ker d_2 = 0$ 이므로, 이제  $H_2(X) = 0$ 입니다.

이것이 말이 되는지 검산해 봅시다 — 즉, 경계는 아니지만 두 배로 하면 경계가 되는 어떤 사이클이 존재함을 확인해 봅시다.

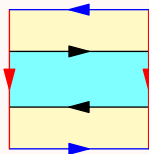
사실, 대부분의 사이클이 성립합니다.



경로를 두 배로 하면, 다음과 같은 것을 얻습니다.



여기서 중요한 부분은 다음과 같습니다: 두 파란색 변이 반대 방향으로 동일시되어 있으므로, 경로 중 하나를 변을 가로질러 당겨서 방향을 뒤집을 수 있습니다... 그런데 이제 이 영역은 실제로 청록색 영역의 경계입니다! 이것으로 끝났습니다.



두 호모토피 동치 경로의 차이가 경계임을 스스로 확인하는 것만 남았습니다.

## §74.6 생각해 볼 만한 조금 더 어려운 문제

문제 74A<sup>†</sup>.  $n$ 을 양의 정수라 합시다. 다음을 보이십시오

$$H_k(\mathbb{CP}^n) \cong \begin{cases} \mathbb{Z} & k = 0, 2, 4, \dots, 2n \\ 0 & \text{그 외의 경우.} \end{cases}$$

문제 74B. 전사가 아닌 사상  $f: S^n \rightarrow S^n$ 의 차수가 영임을 보이십시오.



**문제 74C** (무어 공간).  $G_1, G_2, \dots, G_N$ 을 유한 생성 아벨 군의 수열이라고 합시다. 다음을 만족하는 공간  $X$ 를 구성하십시오.

$$\tilde{H}_n(X) \cong \begin{cases} G_n & 1 \leq n \leq N \\ 0 & \text{그 외의 경우.} \end{cases}$$

**문제 74D.** 정리 74.2.4를 증명하여,  $X$ 의 호몰로지 군이 세포 사슬 복합체의 호몰로지 군과 일치함을 보이십시오.



**문제 74E<sup>†</sup>.**  $n$ 을 양의 정수라고 합시다. 다음을 보이십시오.

$$H_k(\mathbb{RP}^n) \cong \begin{cases} \mathbb{Z} & k = 0 \text{이거나 } k = n \equiv 1 \pmod{2} \text{인 경우} \\ \mathbb{Z}/2\mathbb{Z} & k \text{가 홀수이고 } 0 < k < n \text{인 경우} \\ 0 & \text{그 외의 경우.} \end{cases}$$



# 75 특이 코호몰로지

이 장의 동기를 부여하는 한 가지 방법이 있습니다. 다음이 성립함이 밝혀집니다:

- 모든  $n$ 에 대해  $H_n(\mathbb{CP}^2) \cong H_n(S^2 \vee S^4)$ 입니다.
- 모든  $n$ 에 대해  $H_n(\mathbb{CP}^3) \cong H_n(S^2 \times S^4)$ 입니다.

이는 불행한 일인데, 가능하다면 이 공간들을 구별하고 싶지만(실제로 이들은 호모토피 동치가 아니기 때문입니다), 호몰로지 군으로는 이들의 차이를 구별할 수 없기 때문입니다.

이 장에서는 코호몰로지 군  $H^n(X)$ 과  $H^n(Y)$ 를 정의하겠습니다. 사실  $H^n$ 들은 이른바 보편 계수 정리에 의해  $H_n$ 들로 완전히 결정됩니다. 하지만 모든 코호몰로지 군을 모아 코호몰로지 환  $H^\bullet$ 을 이룰 수 있음이 밝혀집니다.<sup>1</sup> 그러면  $H^\bullet(X) \not\cong H^\bullet(Y)$ 가 환으로서 성립하지 않음을 보게 될 것입니다.

## §75.1 코사슬 복합체

**정의 75.1.1. 코사슬 복합체**  $A^\bullet$ 은 지표가 증가한다는 점을 제외하면 대수적으로 사슬 복합체와 동일합니다. 즉 다음을 만족하는 아벨 군들의 수열입니다

$$\dots \xrightarrow{\delta} A^{n-1} \xrightarrow{\delta} A^n \xrightarrow{\delta} A^{n+1} \xrightarrow{\delta} \dots$$

$\delta^2 = 0$ 을 만족합니다. 표기상으로는 이제 위첨자를 사용하며,  $\partial$  대신  $\delta$ 를 사용합니다. **코호몰로지 군**을 다음과 같이 정의합니다

$$H^n(A^\bullet) = \ker(A^n \xrightarrow{\delta} A^{n+1}) / \operatorname{im}(A^{n-1} \xrightarrow{\delta} A^n).$$

### 예제 75.1.2 (드람 코호몰로지)

우리는 이미 코사슬 복합체의 한 예를 만난 바 있습니다:  $M$ 을 매끄러운 다양체라 하고  $\Omega^k(M)$ 을  $M$  위의  $k$ -형식들의 가법군이라 합시다. 그러면 다음과 같은 코사슬 복합체를 얻습니다

$$0 \xrightarrow{d} \Omega^0(M) \xrightarrow{d} \Omega^1(M) \xrightarrow{d} \Omega^2(M) \xrightarrow{d} \dots$$

그 결과로 얻어지는 코호몰로지를 **드람 코호몰로지**라 부르며, 뒤에서 설명하겠습니다.

드람의 코사슬 복합체 외에, 코사슬 복합체를 얻는 가장 흔한 방법은 사슬 복합체를 쌍대화하는 것입니다. 구체적으로, 아벨 군  $G$ 를 하나 고릅니다;  $\operatorname{Hom}(-, G)$ 가 반변 함자임에 주목하면, 다음의 임의의 사슬 복합체를

$$\dots \xrightarrow{\partial} A_{n+1} \xrightarrow{\partial} A_n \xrightarrow{\partial} A_{n-1} \xrightarrow{\partial} \dots$$

코사슬 복합체로 보냅니다:  $A^n = \operatorname{Hom}(A_n, G)$ 로 두면 다음을 얻습니다

$$\dots \xrightarrow{\delta} A^{n-1} \xrightarrow{\delta} A^n \xrightarrow{\delta} A^{n+1} \xrightarrow{\delta} \dots$$

<sup>1</sup>[Ha02]에는 왜 코호몰로지가 호몰로지보다 더 많은 구조를 갖는지에 대한 설명이 있습니다 — 대략적으로 말하면, 자연스러운 사상  $X \times X \rightarrow X$ 는 그다지 흥미롭지 않은 사영이어야 하지만,  $p \mapsto (p, p)$ 로 주어지는 더 흥미로운 자연스러운 사상  $X \rightarrow X \times X$ 가 존재하기 때문입니다.

여기서  $\delta(A_n \xrightarrow{f} G) = A_{n+1} \xrightarrow{\partial} A_n \xrightarrow{f} G$ 입니다.

이것들이 우리가 대수적 위상수학에서 가장 많이 연구하는 코호몰로지 군이므로, 여기에 특별한 표기를 부여합니다.

**정의 75.1.3.** 아벨 군들의 사슬 복합체  $A_\bullet$ 과 또 다른 군  $G$ 가 주어졌을 때,

$$H^n(A_\bullet; G)$$

를  $\text{Hom}(-, G)$ 를 적용하여 얻은 쌍대 코사슬 복합체  $A^\bullet$ 의 코호몰로지 군으로 나타내기로 합니다. 다시 말해  $H^n(A_\bullet; G) = H^n(A^\bullet)$ 입니다.

## §75.2 공간의 코호몰로지

**이 절의 대표적인 예:**  $C^0(X; G)$ 는 모든 함수  $X \rightarrow G$ 이고,  $H^0(X)$ 는 경로 성분에서 상수인 함수  $X \rightarrow G$ 입니다.

관심 있는 경우는  $C_\bullet(X)$ 를 사용하는 우리의 일반적인 기하학적 상황입니다.

**정의 75.2.1.** 공간  $X$ 와 아벨 군  $G$ 에 대해, 특이 사슬 복합체  $C_\bullet(X)$ 의 쌍대를  $C^\bullet(X; G)$ 로 정의하고, 이를  $X$ 의 **특이 코사슬 복합체**라 부릅니다; 그 원소들을 **코사슬**이라 부릅니다. 그러면 공간  $X$ 의 **코호몰로지 군**을 다음과 같이 정의합니다

$$H^n(X; G) := H^n(C_\bullet(X); G) = H^n(C^\bullet(X; G)).$$

**비고 75.2.2** —  $G$ 가 (예를 들어  $\mathbb{Z}$ 나  $\mathbb{R}$ 처럼) 환이기도 하다면,  $H^n(X; G)$ 는 아벨 군일 뿐만 아니라 실제로  $G$ -가군이 됨에 유의하십시오.

**예제 75.2.3** ( $C^0(X; G)$ ,  $C^1(X; G)$ ,  $H^0(X; G)$ )

$X$ 를 위상 공간이라 하고  $C^\bullet(X)$ 를 생각합시다.

- $C_0(X)$ 는  $X$  위의 자유 아벨 군이며,  $C^0(X) = \text{Hom}(C_0(X), G)$ 입니다. 따라서 0-공사슬은  $X$ 의 모든 점을  $G$ 의 원소로 보내는 함수입니다.
- $C_1(X)$ 는  $X$ 의 1-단체들 위의 자유 아벨 군입니다. 따라서  $C^1(X)$ 는 모든 1-단체를  $G$ 의 원소로 보내야 합니다.

이제  $\delta: C^0(X) \rightarrow C^1(X)$ 를 이해해 봅시다. 0-공사슬  $\phi \in C^0(X)$ , 즉 준동형사상  $\phi: C^0(X) \rightarrow G$ 가 주어졌을 때,  $\delta\phi: C^1(X) \rightarrow G$ 는 무엇입니까? 답:

$$\delta\phi: [v_0, v_1] \mapsto \phi([v_0]) - \phi([v_1]).$$

따라서  $\ker(C^0 \xrightarrow{\delta} C^1) \cong H^0(X; G)$ 의 원소들은 경로 연결 성분 위에서 상수인 공사슬 들입니다.

특히  $H_0(X)$ 와 매우 유사하게,  $X$ 가  $r$ 개의 경로 연결 성분을 가질 때

$$H^0(X) \cong G^{\oplus r}$$

입니다 (여기서  $r$ 은 유한<sup>2</sup>).

<sup>2</sup>  $X$ 가 무한히 많은 경로 연결 성분을 가질 경우 재미있는 일이 일어납니다. 즉 무한 인덱스 집합에 대해  $X = \coprod_\alpha X_\alpha$ 라고 합시다. 이 경우  $H_0(X) = \bigoplus_\alpha G$ 인 반면  $H^0(X) = \prod_\alpha G$ 입니다. 호몰로지에서는

**표기의 남용 75.2.4.** 이 장에서 우리가 다룰 유일한 공사슬 복합체는 위와 같은 쌍대 복합체입니다. 따라서 공사슬 복합체  $A^\bullet$ 을 쓸 때마다 이는  $A_\bullet$ 에  $\text{Hom}(-, G)$ 를 적용하여 암묵적으로 주어지는 것입니다.

더 높은 코호몰로지 군  $H^n(X; G)$  (또는 공사슬 군  $C^n(X; G) = \text{Hom}(C_n(X), G)$ )조차도 는 구체적으로 설명하기가 더 어렵습니다.

### §75.3 공간들의 코호몰로지는 함자적입니다

이제 코호몰로지 군들이 여전히 동일한 좋은 함자적 성질을 보이는지 확인합니다. 먼저 우리가 앞서 얻었던 결과들을 범주화해 봅시다:

**질문 75.3.1.** 공사슬 복합체들의 범주  $\text{CoCmplx}$ 를 정의합니다.

**연습문제 75.3.2.**  $\text{Hom}(-, G)$ 를

$$\text{Hom}(-, G): \text{Cmplx}^{\text{op}} \rightarrow \text{CoCmplx}.$$

로부터의 반변 함자로 해석하십시오. 이는 특히 사슬 사상  $f: A_\bullet \rightarrow B_\bullet$ 가 주어지면, 쌍대 사상  $f^\vee: B^\bullet \rightarrow A^\bullet$ 를 자연스럽게 얻는다는 것을 의미합니다.

**질문 75.3.3.**  $H^n: \text{CoCmplx} \rightarrow \text{Grp}$ 을 함자로 해석합니다. 이들을 합성하여 반변 함자  $H^n(-; G): \text{Cmplx}^{\text{op}} \rightarrow \text{Grp}$ 를 얻습니다.

그러면  $H_n: \text{hTop} \rightarrow \text{Grp}$ 에 대한 우리의 결과와 정확히 유사하게 다음이 성립합니다:

**정리 75.3.4** ( $H^n(-; G): \text{hTop}^{\text{op}} \rightarrow \text{Grp}$ )

모든  $n$ 에 대해,  $H^n(-; G)$ 는  $\text{hTop}^{\text{op}}$ 에서  $\text{Grp}$ 로 가는 반변 함자입니다.

증명. 아이디어는 앞서 각기동 연산자를 구성하며 이미 했던 작업을 활용하는 것입니다. 먼저  $\text{Top}^{\text{op}} \rightarrow \text{Grp}$ 의 함자들로 이루어진 전체 수열을 구성합니다:

$$\text{Top}^{\text{op}} \xrightarrow{C_\bullet} \text{Cmplx}^{\text{op}} \xrightarrow{\text{Hom}(-; G)} \text{CoCmplx} \xrightarrow{H^n} \text{Grp}$$

$$\begin{array}{ccccccc} X & & C_\bullet(X) & & C^\bullet(X; G) & & H^n(X; G) \\ f \downarrow & \xrightarrow{\quad} & f_\# \downarrow & \xrightarrow{\quad} & \uparrow f^\# & \xrightarrow{\quad} & \uparrow f^* \\ Y & & C_\bullet(Y) & & C^\bullet(Y; G) & & H^n(Y; G). \end{array}$$

직합을 얻는 반면 코호몰로지에서는 직접곱을 얻습니다.

이들은 무한 인덱스 집합에서는 실제로 서로 다릅니다. 일반적인 가군의 경우  $\bigoplus_\alpha M_\alpha$ 는 유한 개의 0이 아닌 항만 허용하도록 정의됩니다. (이는 냅킨에서 앞서 전혀 언급된 적이 없는데, 처음  $M \oplus N$ 만을 정의하고 이를 유한 직합으로 확장했을 뿐이기 때문입니다.) 군들의 곱인  $\prod_\alpha G_\alpha$ 에는 이런 제한이 없습니다. 이는  $C_0(X)$ 가  $G$ 의 경로 연결 성분들로부터 나온 0-사슬들의 형식적 선형합(모든 형식적 합이 그렇듯 유한 합)이라는 사실에 대응됩니다. 하지만  $C^0(X)$ 의 공사슬은  $X$ 의 각 경로 연결 성분에서  $G$ 로 가는 함수이며, 여기에는 아무 제한이 없습니다.

여기서  $f^\sharp = (f_\sharp)^\vee$ 이며,  $f^*$ 는 공사슬 복합체의 호몰로지 군 위에 유도된 결과 사상입니다.

그러므로 이전과 마찬가지로 우리가 보여야 할 것은  $f \simeq g$ 이면  $f^* = g^*$ 라는 것뿐입니다. 이제  $f_\sharp - g_\sharp = P\partial + \partial P$ 를 만족하는 각기등 연산자가 있었음을 상기합니다. 전치 함자  $\text{Hom}(-; G)$ 를 적용하면  $f^\sharp - g^\sharp = \delta P^\vee + P^\vee \delta$ 를 얻는데, 여기서  $P^\vee: C^{n+1}(Y; G) \rightarrow C^n(X; G)$ 입니다. 따라서  $f^\sharp$ 와  $g^\sharp$ 는 사슬 호모토픽하므로  $f^* = g^*$ 입니다.  $\square$

## §75.4 보편 계수 정리

이제 우리는 코호몰로지 군들이 호몰로지 군들에 의해 동형사상까지 결정됨을 보이고자 합니다:  $H_n(A_\bullet)$ 가 주어지면,  $H^n(A_\bullet; G)$ 를 추출할 수 있습니다. 이는 보편 계수 정리에 의해 달성됩니다.

### 정리 75.4.1 (보편 계수 정리)

$A_\bullet$ 을 자유 아벨 군들의 사슬 복합체라 하고,  $G$ 를 또 다른 아벨 군이라 합시다. 그러면 다음과 같은 자연스러운 짧은 완전열이 존재합니다

$$0 \rightarrow \text{Ext}(H_{n-1}(A_\bullet), G) \rightarrow H^n(A_\bullet; G) \xrightarrow{h} \text{Hom}(H_n(A_\bullet), G) \rightarrow 0.$$

게다가 이 완전열은 분할되므로, 특히

$$H^n(C_\bullet; G) \cong \text{Ext}(H_{n-1}(A_\bullet), G) \oplus \text{Hom}(H_n(A_\bullet), G).$$

다행히도, 우리가 관심을 갖는 경우인  $A_\bullet$ 는  $C_\bullet(X)$ 이며 이는 정의상 자유입니다. 우리가 설명해야 할 것은 두 가지, 즉 사상  $h$ 가 무엇인지와 사상  $\text{Ext}$ 가 무엇인지입니다.

$$h: H^n(A_\bullet; G) \rightarrow \text{Hom}(H_n(A_\bullet), G)$$

가 어떻게 정의되는지 추측하는 것은 그리 어렵지 않습니다.  $H^n(A_\bullet; G)$ 의 원소는  $A_n$ 의 순환을  $G$ 의 원소로 보내는 함수로 표현됩니다. 이 정리의 내용은  $h$ 가 전사이며 그 핵이  $\text{Ext}(H_{n-1}(A_\bullet), G)$ 임을 보이는 것입니다.

$\text{Ext}$ 는 어떻습니까?  $\text{Ext}(-, G)$ 는 이른바 **Ext 함자**이며, 다음과 같이 정의됩니다.  $H$ 를 아벨 군이라 하고,  $H$ 의 **자유 분해**를 생각합시다. 이는 다음과 같은 완전열을 의미합니다

$$\dots \xrightarrow{f_2} F_1 \xrightarrow{f_1} F_0 \xrightarrow{f_0} H \rightarrow 0$$

여기서 각  $F_i$ 는 자유입니다. 그러면  $\text{Hom}(-, G)$ 를 적용하여 다음과 같은 코사슬 복합체를 얻을 수 있습니다

$$\dots \xleftarrow{f_2^\vee} \text{Hom}(F_1, G) \xleftarrow{f_1^\vee} \text{Hom}(F_0, G) \xleftarrow{f_0^\vee} \text{Hom}(H, G) \leftarrow 0.$$

하지만 이 코사슬 복합체는 완전할 필요가 없습니다 (범주론적 용어로,  $\text{Hom}(-, G)$ 는 완전성을 보존하지 않습니다). 우리는

$$\text{Ext}(H, G) := \ker(f_2^\vee) / \text{im}(f_1^\vee)$$

로 정의하며, 이것이 자유 분해의 선택에 의존하지 않는다는 것이 정리입니다. 여기에는 많은 호몰로지 대수학이 관여하는데, 시간을 들여 논의하지는 않겠습니다. 하지만 제가 포함한 이 작은 부분의 요점은, 원하는 어떤 자유 분해든 골라서 위 계산을 할 수 있기 때문에  $\text{Ext}$  함자는 실제로 계산하기가 매우 쉽다는 것입니다.

**비고 75.4.2** — 여러분은 이미 위장된 형태로 "자유 분해"를 본 적이 있습니다 — **절 18.3**에서, 우리는 임의의 가군  $M$ 을  $R^{\oplus d}/K$ 로 씌으로써 PID 위의 유한생성 가군의 구조 정리를 증명했는데, 이때  $R^{\oplus d}$ 와  $K$  모두 자유입니다. 이는 다음과 같은 자유 분해를 줍니다

$$\cdots \rightarrow 0 \rightarrow K \hookrightarrow R^{\oplus d} \twoheadrightarrow M \rightarrow 0.$$

직관적으로,  $\text{Ext}$  함자를 "있어야 하지만 없는 사상들"을 측정하는 것으로 생각할 수 있습니다 — 몇 가지 예를 본 후에 점차 직관을 얻게 될 것입니다.<sup>a</sup>

<sup>a</sup><https://mathoverflow.net/a/679>에서 가져옴.

### 보조정리 75.4.3 ( $\text{Ext}$ 함자 계산하기)

임의의 아벨 군  $G, H, H'$ 에 대해 다음이 성립합니다

- (a)  $\text{Ext}(H \oplus H', G) = \text{Ext}(H, G) \oplus \text{Ext}(H', G)$ .
- (b)  $H$ 가 자유일 때  $\text{Ext}(H, G) = 0$ 이고, 그리고
- (c)  $\text{Ext}(\mathbb{Z}/n\mathbb{Z}, G) = G/nG$ .

증명. (a)에 대해서는,  $\cdots \rightarrow F_1 \rightarrow F_0 \rightarrow H \rightarrow 0$ 과  $\cdots \rightarrow F'_1 \rightarrow F'_0 \rightarrow H' \rightarrow 0$ 이 자유 분해라면,  $F_1 \oplus F'_1 \rightarrow F_0 \oplus F'_0 \rightarrow H \oplus H' \rightarrow 0$ 도 자유 분해임에 주목하십시오.

(b)에 대해서는,  $0 \rightarrow H \rightarrow H \rightarrow 0$ 이 자유 분해임에 주목하십시오.

(c) 부분은 다음 자유 분해를 취함으로써 따라옵니다

$$0 \rightarrow \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow 0$$

그리고 여기에  $\text{Hom}(-, G)$ 를 적용함으로써 따라옵니다.

**질문 75.4.4.** 여기서부터 (c)의 증명을 마무리하십시오. □

**질문 75.4.5.**  $\text{Ext}$  연습 문제:  $\text{Ext}(\mathbb{Z}^{\oplus 2015}, G)$ 와  $\text{Ext}(\mathbb{Z}/30\mathbb{Z}, \mathbb{Z}/4\mathbb{Z})$ 를 계산하십시오.

## §75.5 보편 계수 정리에 대한 설명

앞 장에는 여러분이 비명을 지르게 만들 수도 있는, 설명되지 않은 수많은 기호와 공식들이 있습니다:

저는 이제  $\mathbb{CP}^2$ 와  $S^2 \vee S^4$ 가 서로 다른지 더 이상 신경 쓰지 않습니다! 도대체 이 공간들은 무엇입니까?

그럼에도 불구하고, 그리 어렵지는 않습니다. 이 정리에서 읽어내야 할 두 가지 핵심 사항이 있습니다:

- $H_n(A_\bullet) = 0$ 이더라도,  $\text{Ext}(H_{n-1}(A_\bullet), G) \neq 0$ 이면 여전히  $H^n(A_\bullet; G) \neq 0$ 일 수 있습니다.  
저차원의 경우에는 실제로 시각화할 수 있습니다 — **절 75.7**에서 클라인 병에 대해 이를 다룹니다.
- $H^n(A_\bullet; G)$ 는  $A_\bullet$ 가 무엇이든 상관없이, 각  $A_n$ 이 자유이기만 하면  $H_n(A_\bullet)$ 와  $G$ 에 의해 유일하게 결정됩니다.

이는 다음을 의미합니다: 원한다면 보편 계수 정리의 공식을 잊어버리고, 세포 사슬 복합체  $\text{Cells}_\bullet(X)$ 를 사용하여 다음과 같이 코호몰로지를 계산할 수 있습니다:

$$H^n(X; G) = \frac{\ker(\text{Hom}(\text{Cells}_n(X), G) \rightarrow \text{Hom}(\text{Cells}_{n+1}(X), G))}{\text{im}(\text{Hom}(\text{Cells}_{n-1}(X), G) \rightarrow \text{Hom}(\text{Cells}_n(X), G))}.$$

결국, 세포 사슬 복합체와 특이 사슬 복합체는 둘 다 자유이며 같은 호몰로지 군을 가지므로, 보편 계수 정리에 의해 이들은 같은 코호몰로지 군을 가져야 합니다.

그럼에도 불구하고, 보편 계수 정리의 공식은 바람직합니다. 왜냐하면 대개 사슬 복합체  $A_\bullet$ 가  $H_\bullet(A_\bullet)$ 보다 더 복잡하기 때문입니다.

### 예제 75.5.1

클라인 병의 세포 사슬 복합체는 다음과 같은 형태를 가집니다:

$$\cdots \rightarrow \mathbb{Z} \xrightarrow{1 \mapsto (0,2)} \mathbb{Z}^2 \xrightarrow{(a,b) \mapsto 0} \mathbb{Z}.$$

호몰로지 군은 다음과 같습니다:

$$H_2 = 0, H_1 = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, H_0 = \mathbb{Z}.$$

실제로 더 단순하지만, 그 차이는 미미합니다 (4개 대신 3개의 생성자가 있고, 사상을 추적할 필요가 없습니다). 세포 호몰로지가 이미 매우 효율적이기 때문입니다.

이 공식은 다시 어디서 나오는 것일까요? 다음과 같이 생각할 수 있습니다. 보편 계수 정리에 따르면  $H^\bullet(A_\bullet; G)$ 는 오직  $H_\bullet(A_\bullet)$ 에만 의존하므로,  $H_\bullet$ 가 주어졌을 때 자유 아벨 군으로 이루어진 임의의 사슬 복합체  $A_\bullet$ 를 구성하여 쌍대화하면 됩니다.

모든 항에 대해  $H_k = 0$ 이고, 오직  $H_{n-1} \neq 0$ 이라고 가정합시다. 그러면 항진적으로  $H^n \cong \text{Ext}(H_{n-1}; G)$ 가 성립합니다 — 자유 분해는 바로 사슬 복합체이기 때문입니다!

**연습문제 75.5.2.** 이를 검증해 보십시오. (힌트: 완전열  $Z_{n-1} \rightarrow H_{n-1} \rightarrow 0$ 에서 시작합니다. 이를  $H_{n-1}$ 의 자유 분해로 확장할 수 있습니까?)

모든 항에 대해  $H_k = 0$ 이고, 오직  $H_n \neq 0$ 이라고 가정합시다. 그러면  $H^n \cong \text{Hom}(H_n, G)$ 임을 알 수 있습니다.

보편 계수 정리는 단순히 자유 분해의 선택이 결과에 영향을 주지 않는다는 것과, 다른 항들이 0이 아닐 수 있다면  $H^n$ 이 위 두 경우의 두 군의 직합이 된다는 것을 말해줍니다.

원한다면 자유 분해의 선택이 중요하지 않다는 사실을 직접 증명해볼 수도 있습니다 — 다소 까다롭지만 그렇게 어렵지는 않습니다. 이는 사슬 복합체 사이의 사상을 구성하는 문제로 귀결되며 (도식이 가환하도록 만드는 것은 어렵지 않은데, 군들이 자유 군이므로 기저를 원하는 곳으로 보낼 수 있기 때문입니다), 두 자유 분해가 사슬 호모토픽함을 보이면 됩니다.

## §75.6 코호몰로지 군 계산 예시

**이 절의 대표적인 예:** 아마도  $H^n(S^m)$ 일 것입니다.

보편 계수 정리는 호몰로지 군을 알고 있다면 임의의 코호몰로지 군을 계산할 수 있는 직접적인 방법을 제공합니다.

**예제 75.6.1** ( $S^m$ 의 코호몰로지 군)

이제  $H^n(S^m)$ 을 계산하는 것은 간단합니다:  $H_n(S^m)$ 이 항상 자유 군이므로 모든 Ext 항이 사라지며, 따라서 다음을 얻습니다

$$H^n(S^m) \cong \text{Hom}(H_n(S^m), G) \cong \begin{cases} G & n = m, n = 0 \\ 0 & \text{그 외의 경우.} \end{cases}$$

**예제 75.6.2** (원환면의 코호몰로지 군)

이 예시 역시 0이 아닌 Ext 항이 없습니다. 이번에는  $H^n(S^1 \times S^1)$ 이 항상 자유 군이기 때문입니다. 따라서 다음을 얻습니다

$$H^n(S^1 \times S^1) \cong \text{Hom}(H_n(S^1 \times S^1), G).$$

$H_n(S^1 \times S^1)$ 이 차원  $n = 0, 1, 2$ 에서 각각  $\mathbb{Z}$ ,  $\mathbb{Z}^{\oplus 2}$ ,  $\mathbb{Z}$ 이므로 다음을 유도할 수 있습니다

$$H^n(S^1 \times S^1) \cong \begin{cases} G & n = 0, 2 \\ G^{\oplus 2} & n = 1. \end{cases}$$

이 예시들로부터 다음을 알아챌 수 있습니다:

**보조정리 75.6.3** (0차와 1차 코호몰로지 군은 단순히 쌍대이다)

$n = 0$ 과  $n = 1$ 인 경우, 다음이 성립합니다

$$H^n(X; G) \cong \text{Hom}(H_n(X), G).$$

증명.  $n = 0$ 인 경우는 이미 보였습니다.  $n = 1$ 인 경우,  $H_0(X)$ 가 자유 군이므로 Ext 항이 사라짐에 주목하십시오.  $\square$

**예제 75.6.4** (클라인 병의 코호몰로지 군)

이 예시에서는 실제로 Ext 항이 존재합니다. **예제 74.5.4**에서 클라인 병  $K$ 의 호몰로지 군이 차원  $n = 0$ 에서  $\mathbb{Z}$ 이고  $n = 1$ 에서  $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ 이며, 그 외에는 0임을 상기하십시오.  $n = 0$ 인 경우, 다시 단순히  $H^0(K; G) \cong \text{Hom}(\mathbb{Z}, G) \cong G$ 를 얻습니다.  $n = 1$ 인 경우, Ext 항은  $\text{Ext}(H_0(K), G) \cong \text{Ext}(\mathbb{Z}, G) = 0$ 이므로

$$H^1(K; G) \cong \text{Hom}(\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, G) \cong G \oplus \text{Hom}(\mathbb{Z}/2\mathbb{Z}, G).$$

여기서  $\text{Hom}(\mathbb{Z}/2\mathbb{Z}, G)$ 는  $G$ 에서 위수가 2인 원소들(그리고  $0 \in G$ )로 이루어진 부분 군입니다.

하지만  $n = 2$ 인 경우, 우리는 첫 번째로 흥미로운 Ext 군을 얻게 됩니다: 완전열은 다음과 같습니다

$$0 \rightarrow \text{Ext}(\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, G) \rightarrow H^2(X; G) \rightarrow \underbrace{H_2(X)}_{=0} \rightarrow 0.$$

따라서 다음을 얻습니다

$$H^2(X; G) \cong (\text{Ext}(\mathbb{Z}, G) \oplus \text{Ext}(\mathbb{Z}/2\mathbb{Z}, G)) \oplus 0 \cong G/2G.$$

그 이상의 모든 군은 사라집니다. 요약하면:

$$H^n(X; G) \cong \begin{cases} G & n = 0 \\ G \oplus \text{Hom}(\mathbb{Z}/2\mathbb{Z}, G) & n = 1 \\ G/2G & n = 2 \\ 0 & n \geq 3. \end{cases}$$

## §75.7 코호몰로지 군의 시각화

더 큰 값의  $n$ 에 대해  $C^n(X; G)$ 와  $H^n(X; G)$ 를 이해해 보도록 하겠습니다.

위에서와 같이,  $C_n(X)$ 는  $X$  위의  $n$ -단체들로 생성된 자유 아벨 군이므로, 원소  $f \in C^n(X; G)$ 는 각  $n$ -단체를  $G$ 의 원소로 보내는 함수입니다 ( $C_n(X)$  전체로 선형적으로 확장됩니다).

이 값의 할당은 어떠한 좋은 성질도 가질 필요가 없습니다 —  $n$ -단체는 단순히 (연속) 사상  $\sigma: \Delta^n \rightarrow X$ 이며,  $\text{im } \sigma_1 = \text{im } \sigma_2$  일지라도 서로 다른 사상  $\sigma_1$ 과  $\sigma_2$ 는 서로 다른 것으로 간주된다는 점을 상기하십시오. 특히,

- $[v_0, v_1, v_2]$ 가 특이 단체라면,  $f([v_0, v_1, v_2]) + f([v_0, v_2, v_1]) = 0$ 이 성립할 필요는 없습니다.
- 상이 한 점에 포함되는 특이  $n$ -단체( $n \geq 1$ )가  $f$ 에 의해 반드시 0으로 보내질 필요는 없습니다.

하지만  $C_n(X)$ 의 원소들이 이렇게 좋지 않다는 것은 중요하지 않습니다! 왜 그러한지는 아래에서 살펴보겠습니다.

호몰로지의 경우(정의 71.2.2)에서 우리는 다음과 같이 정의하였습니다:

$$\begin{aligned} Z_n(X) &:= \ker \left( C_n(X) \xrightarrow{\partial} C_{n-1}(X) \right), \\ B_n(X) &:= \text{im} \left( C_{n+1}(X) \xrightarrow{\partial} C_n(X) \right), \\ H_n(X) &:= Z_n(X) / B_n(X). \end{aligned}$$

$Z_n(X)$ 와  $B_n(X)$ 의 원소들은 각각 사이클과 경계라고 불리며, 명백한 기하학적 해석을 갖습니다.

그러므로,

$$H_n(X) = \frac{n\text{-사이클}}{n\text{-바운더리}}.$$

이번 절에서는 잠시 다음과 같이 정의하겠습니다:

$$\begin{aligned} Z^n(X; G) &:= \ker \left( C^n(X; G) \xrightarrow{\delta} C^{n+1}(X; G) \right), \\ B^n(X; G) &:= \text{im} \left( C^{n-1}(X; G) \xrightarrow{\delta} C^n(X; G) \right), \\ H^n(X; G) &:= Z^n(X; G) / B^n(X; G). \end{aligned}$$

이번 절에서는  $Z^n(X; G)$ 의 원소들을 **코사이클**이라 부르고,  $B^n(X; G)$ 의 원소들을 **코경계**라 부를 것입니다. 다시 한번,

$$H^n(X; G) = \frac{n\text{-코사이클}}{n\text{-코바운더리}}.$$

왜 원소들이 위와 같이 명명되었는지는 기하학적으로 덜 명확하지만, 만약 군  $G$ 가 체라고 가정한다면(여기서 군 연산은 체의 덧셈 연산입니다),<sup>3</sup> 다음이 성립합니다:

- $n$ -코사이클은 모든  $n$ -경계를  $0 \in G$ 로 보내는 사상입니다;
- $n$ -코경계는 모든  $n$ -사이클을  $0 \in G$ 로 보내는 사상입니다.

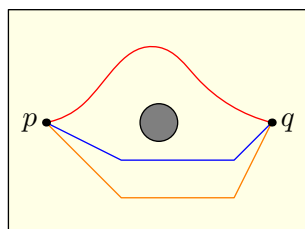
첫 번째 명제는 명백합니다(정의를 따라가면 됩니다). 두 번째 명제는 한 방향으로만 일반적으로 성립합니다(코경계는 모든 사이클을 0으로 보내지만, 모든 사이클을 0으로 보내는 사상이 반드시 코경계일 필요는 없습니다 — 이는 나중에 클라인 병 예제에서 살펴보겠습니다).

$n$ -코사이클이 어떤 모습이어야 하는지 살펴보겠습니다. 먼저,

**경계가 같은 호모토픽한 사슬들은 코사이클에 의해 동일한 값으로 보내집니다.**

두  $k$ -단체가 호모토픽하다는 것이 무엇을 의미하는지는 절 65.4에서 정의하였습니다 — 현재 상황에서는 경계가 항상 고정된다는 조건을 추가로 요구합니다.

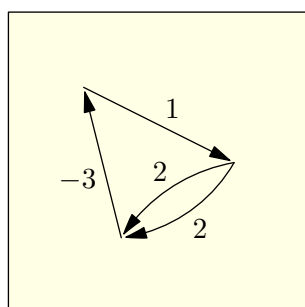
예를 들어, 아래에서 파란색과 주황색 1-단체는 호모토픽하지만, 빨간색 1-단체는 그렇지 않습니다.



증명은 어렵지 않습니다 — 호모토픽한 두  $k$ -단체의 차이가 어떤 것(그들의 내부입니다!)의 경계임을 보이고, 그 내부를 몇 개의  $k+1$ -단체의 합으로 쓰기만 하면 됩니다. (힌트: 가장 쉬운 방법은 사실 내부를 두  $k+1$ -단체의 차이로 쓰는 것이며, 정점 순서 문제에 주의하십시오.)

#### 연습문제 75.7.1. 증명을 완성하십시오.

전형적인 1-코사이클은 아래와 같은 모습일 수 있으며, 각 화살표에는 해당 1-단체에 할당된 값이 표시되어 있습니다. 사이클은 반드시 0으로 보내져야 함을 기억하십시오.

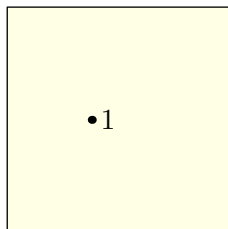


이제 다음 관찰을 살펴보겠습니다:

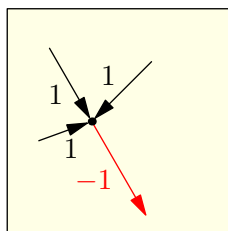
**코경계를 법으로 하여 코사이클만을 고려한다면, 우리는 기본적으로 사이클에 할당된 값에만 관심을 갖게 됩니다.**

<sup>3</sup><https://math.stackexchange.com/q/4712676>를 참조하십시오.

왜 그럴까요?  $k$ -공경계는 어떤  $(k-1)$ -공사슬의  $\delta$ 라는 사실을 기억하십시오. 그러면, 다음과 같은 0-공사슬이 주어졌을 때:



그  $\delta$ 는 대략 다음과 같은 모양일 것입니다:



그러므로, 대략적으로 말하면,

주어진 공사슬에 공경계를 더하거나 빼면, 대부분의 사슬에 할당된 값을 원하는 대로 조정할 수 있습니다.

“대부분의 사슬”이라고 말한 이유는, 만약 그 사슬들이 순환을 이룬다면, 공경계를 더해도 그 값을 바꿀 수 없기 때문입니다.

다행히도,

- 경계인 순환에는 항상 값 0이 할당됩니다.
- 호모토픽한 순환에는 동일한 값이 할당됩니다.

일반화하자면, 사실 호몰로그한 (즉, 사상  $Z_k(X) \rightarrow H_k(X)$  아래에서 같은 값으로 대응되는) 순환에는 같은 값이 할당됩니다.

따라서,

각 “경계를 법으로 한 순환”에 대한 공순환의 값을 안다면, 그 공순환은 공경계를 법으로 거의 결정됩니다.

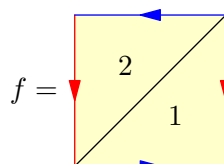
기호로 쓰면:  $H^n(X; G)$ 는  $\text{Hom}(H_n(X), G)$ 와 “거의 동형”입니다.

다시 말해, 공경계를 법으로 한 공순환은 경계를 법으로 한 순환 위에서 “평가”될 수 있습니다.

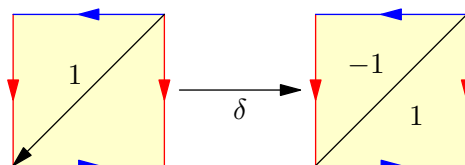
이것이 바로 보편 계수 정리가 말하는 바이지만, 정리는 그보다 더 많은 것을 말합니다: “오차항”은 정확히  $\text{Ext}(H_{n-1}(X), G)$ 입니다.

오차항이 왜 존재할까요? 위에서  $K$ 가 클라인 병일 때  $H^2(K; G)$ 를 계산하는 예를 다뤘습니다. 이제  $G = \mathbb{Z}$ 를 가정하고 기하학적으로 이를 살펴봅시다.

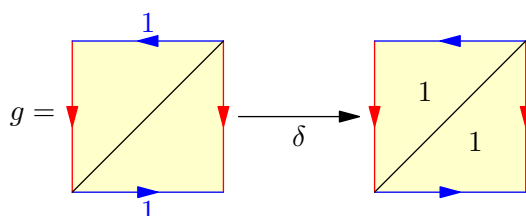
전형적인 2-공사슬  $f \in C^2(K; \mathbb{Z})$ 는 대략 다음과 같은 모양일 수 있습니다. (몇 개의 2-단체에 할당된 값만 표시되어 있는데, 2-단체가 너무 많아 모두 그릴 수 없기 때문입니다.)



공경계는 다음과 같은 모양일 수 있습니다 — 위의 상황과 동일하게, 특정 단체에 할당된 값 자체는 중요하지 않으며, 공경계를 더함으로써 두 단체 사이에서 할당된 값을 “이전”할 수 있습니다.



그러므로, 클라인 병 전체 곡면에 할당된 값은 3이라고 간단히 말할 수 있습니다 — 형식적으로,  $e_K^2 \in C_2(K)$ 를 위의 두 2-단체의 합이라 하면,  $f(e_K^2) = 3$ 이라고 쓸 수 있습니다. 그러나:



클라인 병 전체 곡면에 대응하는 2-사슬의 경계는 파란 변의 2배이므로, 파란 변에서 값 1을 갖는 1-공사슬의  $\delta$ 는  $e_K^2$ 에 값 2를 할당하게 됩니다.

기호로 쓰면:  $e_b^1 \in C_1(K)$ 를 파란 변이라 하고,  $g(e_b^1) = 1$ 을 만족하는  $g \in C^1(K; \mathbb{Z})$ 를 택하면,  $\delta(g)(e_K^2) = 2$ 입니다.  $e_K^2$ 가 순환이 아님에도 불구하고, 우리는 여전히 그 할당된 값을 2를 범으로 신경 써야 합니다! 왜냐하면 공경계  $\delta(g)$ 를 더하거나 빼는 것은 그 값을 오직 2의 배수만큼만 조정할 수 있기 때문입니다.

따라서,

**영역  $e^k \in C_k(X)$ 의 경계  $\partial e^k \in C_{k-1}(X)$ 가  $n$ 으로 나누어떨어진다면, 우리는  $e^k$ 에 할당된 값을  $n$ 을 범으로 신경 써야 합니다.**

이것으로 오차항  $\text{Ext}(H_{n-1}(X), G)$ 이 어디서 비롯되는지 설명됩니다.

**절 76.2**에서 드람 코호몰로지와 또 다른 비교를 살펴봅시다 — 그 경우, 군  $G$ 는 체  $\mathbb{R}$ 이므로,  $\text{Ext}(H_{n-1}(X), G)$ 는 항상 0입니다.

## §75.8 상대 코호몰로지 군

상대 코호몰로지 군 역시 자명한 방식으로 정의할 수 있습니다: 사슬 복합체를 쌍대화하여

$$\dots \xrightarrow{\partial} C_1(X, A) \xrightarrow{\partial} C_0(X, A) \rightarrow 0$$

여쌍대 복합체를 얻습니다

$$\dots \xleftarrow{\delta} C^1(X, A; G) \xleftarrow{\delta} C^0(X, A; G) \leftarrow 0.$$

이것의 코호몰로지 군을 취할 수 있습니다.

**정의 75.8.1.** 이렇게 얻어진 군들을 **상대 코호몰로지 군**이라 하며  $H^n(X, A; G)$ 로 표기합니다.

또한, 축소 코호몰로지 군 역시 정의할 수 있습니다. 이를 수행하는 한 가지 방법은 증대된 특이 사슬 복합체를 취하여

$$\dots \xrightarrow{\partial} C_1(X) \xrightarrow{\partial} C_0(X) \xrightarrow{\varepsilon} \mathbb{Z} \rightarrow 0$$

쌍대화함으로써

$$\dots \xleftarrow{\delta} C^1(X; G) \xleftarrow{\delta} C^0(X; G) \xleftarrow{\varepsilon^\vee} \underbrace{\mathrm{Hom}(\mathbb{Z}, G)}_{\cong G} \leftarrow 0.$$

우리가 추가하는  $\mathbb{Z}$  역시 자유이므로, 보편 계수 정리가 여전히 적용됩니다. 따라서 이는 우리에게 축소 코호몰로지 군을 줄 것입니다.

하지만 우리가 이미 상대 코호몰로지 군을 정의했으므로, 다음과 같이 정의하는 것이 가장 간단합니다:

**정의 75.8.2.** 공집합이 아닌 공간  $X$ 의 **축소 코호몰로지 군**은  $\tilde{H}^n(X; G)$ 로 표기되며, 어떤 점  $*$   $\in X$ 에 대해  $H^n(X, \{*\}; G)$ 로 정의됩니다.

## §75.9 생각해 볼 만한 조금 더 어려운 문제

**문제 75A\*** (빼기곱 코호몰로지). 임의의  $G$ 와  $n$ 에 대해 다음이 성립합니다

$$\tilde{H}^n(X \vee Y; G) \cong \tilde{H}^n(X; G) \oplus \tilde{H}^n(Y; G).$$

**문제 75B<sup>†</sup>.** 표수가 0인 체  $F$ 와 유한 생성 호몰로지 군을 갖는 공간  $X$ 에 대해 다음을 증명하십시오:

$$H^k(X, F) \cong (H_k(X))^{\vee}.$$

따라서 체 위에서 코호몰로지는 호몰로지의 쌍대입니다.

**문제 75C** ( $\mathbb{RP}^n$ 의  $\mathbb{Z}/2\mathbb{Z}$ -코호몰로지). 다음을 증명하십시오

$$H^m(\mathbb{RP}^n, \mathbb{Z}/2\mathbb{Z}) \cong \begin{cases} \mathbb{Z} & m = 0 \text{이거나, } m \text{이 홀수이고 } m = n \text{인 경우} \\ \mathbb{Z}/2\mathbb{Z} & 0 < m < n \text{이고 } m \text{이 홀수인 경우} \\ 0 & \text{그 외의 경우.} \end{cases}$$

# 76 코호몰로지의 응용

위상수학에 관한 이 마지막 장에서는 코호몰로지 군의 몇 가지 좋은 성질을 (대부분 증명 없이) 서술하고, 특히 이른바 컵 곱을 소개하겠습니다. 컵 곱에 대한 실제 논고는 [Ha02] 또는 [Ma13a]을 참고하십시오.

앞 장에서 언급했듯이, 모든 코호몰로지 군  $H^*(X)$ 를 한데 모아 코호몰로지 환을 구성할 수 있으며, 이는 호몰로지의 경우보다 더 많은 구조를 부여합니다 —  $\mathbb{CP}^2$ 와  $S^2 \vee S^4$ 를, 또는  $\mathbb{CP}^3$ 와  $S^2 \times S^4$ 를 구별하기에 충분한 구조입니다.

위의 설명이 전혀 설명적이지 않음에도(그 구조가 무엇에 관한 것인지에 대한 통찰을 주지 않습니다), 실제로 어떤 사람들은 이렇게 말할 것입니다:

호몰로지가 직관적으로 무엇을 측정하는지는 중요하지 않습니다. 그것은 매우 어려운 것(위상수학)을 받아들여 단순한 것(아벨 군)으로 바꾸어 주는 편리한 도구이기 때문입니다.

그럼에도 불구하고, 컵 곱이 실제로 시각화 가능하다는 점은 흥미롭습니다! 적어도 차원이 3을 넘지 않을 때는 그렇습니다.

## §76.1 Poincaré 쌍대성

첫 번째 멋진 결과: 토러스나  $S^n$ 과 같은 "좋은" 공간의 (코)호몰로지 군에서 대칭성을 눈치 채셨을 수도 있습니다. 실제로 이는 다음에 의해 예측됩니다:

### 정리 76.1.1 (Poincaré 쌍대성)

$M$ 이 매끄러운 유향 콤팩트  $n$ -다양체라면, 자연스러운 동형사상이 존재합니다

$$H^k(M; \mathbb{Z}) \cong H_{n-k}(M)$$

모든  $k$ 에 대해 성립합니다. 특히,  $k > n$ 일 때  $H^k(M) = 0$ 입니다.

따라서 매끄럽고 방향이 주어진 콤팩트 다양체의 경우, 코호몰로지 군과 호몰로지 군은 그다지 다르지 않습니다.

이로부터 우리가 베티 수를 처음 정의할 때 언급했던 대칭성이 따라 나옵니다:

### 따름정리 76.1.2 (베티 수의 대칭성)

$M$ 을 매끄럽고 방향이 주어진 콤팩트한  $n$ -다양체라 하고,  $b_k$ 를 그 베티 수라 합시다. 그러면

$$b_k = b_{n-k}.$$

증명. 문제 76A<sup>†</sup>.

□

## §76.2 드람 코호몰로지

이제 미분 형식과 특이 코호몰로지 사이의 연관성을 밝히겠습니다.

$M$ 을 매끄러운 다양체라 합시다. 우리는  $M$ 의 호몰로지 군과 코호몰로지 군에 관심이 있습니다. 실수의 덧셈군인  $G = \mathbb{R}$ 인 경우로 특수화하겠습니다.

**질문 76.2.1.** 유한 생성 아벨 군  $H$ 에 대해  $\text{Ext}(H, \mathbb{R}) = 0$ 임을 확인하십시오.

따라서 실수 계수를 사용하면 보편 계수 정리는 다음을 말해줍니다

$$H^k(M; \mathbb{R}) \cong \text{Hom}(H_k(M), \mathbb{R}) = (H_k(M))^\vee$$

여기서  $H_k(X)$ 를 실수 벡터 공간으로 간주합니다. 그러므로  $H_k(M)$  또는  $H^k(M; \mathbb{R})$  중 하나를 파악하고 싶습니다.

다음 코사슬 복합체를 생각해 봅시다

$$0 \rightarrow \Omega^0(M) \xrightarrow{d} \Omega^1(M) \xrightarrow{d} \Omega^2(M) \xrightarrow{d} \Omega^3(M) \xrightarrow{d} \dots$$

$H_{\text{dR}}^k(M)$ 을 그 코호몰로지 군이라 합시다. 따라서 드람 코호몰로지는 닫힌 형식을 완전 형식으로 나눈 것입니다.

코사슬 : 코사이클 : 코바운더리 =  $k$ -형식 : 닫힌 형식 : 완전 형식.

전체 요점은 다음과 같습니다:

#### 정리 76.2.2 (드람의 정리)

임의의 매끄러운 다양체  $M$ 에 대해, 다음과 같은 자연스러운 동형사상이 존재합니다

$$H^k(M; \mathbb{R}) \cong H_{\text{dR}}^k(M).$$

즉 이 정리는 다양체  $M$ 의 실수 코호몰로지 군이 실제로 미분 형식의 거동만으로 주어진다는 것입니다. 따라서,

**코호몰로지 군의 원소들을 공간 위의  $G$ -값 미분 형식으로 비유적으로 생각할 수 있습니다.**

왜 이런 일이 일어날까요? 사실 우리는 공간의 구멍을 반영하는 미분 형식의 거동을 이미 관찰한 바 있습니다. 예를 들어,  $M = S^1$ 을 원이라 하고 **각도 형식**  $\alpha$ 를 생각해 봅시다(예제 44.7.4 참고). 이 형식  $\alpha$ 는 닫혀 있지만 완전하지는 않은데, 이는  $S^1$ 을 한 바퀴 완전히 돌 수 있기 때문입니다. 따라서  $\alpha$ 가 완전하지 못하다는 사실은  $H_1(S^1) \cong \mathbb{Z}$ 임을 시사합니다.

또 다른 직관으로서 다음을 주목합시다:

- 각  $k$ -미분 형식  $\omega$ 는 각  $k$ -매끄러운 부분다양체  $S \subseteq M$ 을 받아 실수  $\int_S \omega$ 를 반환하는 함수로 해석될 수 있습니다.
- 지금은 모든  $k$ -단체가 매끄럽다고 가정해 봅시다. 그러면 다음을 얻습니다:
  - $k$ -공사슬은 각  $k$ -단체를 실수로 보내는 함수입니다.
  - $k$ -공사이클은 경계를 0으로 보내는  $k$ -공사슬입니다.
  - $k$ -공경계는 사이클을 0으로 보내는  $k$ -공사슬입니다.

한편:

- 미분 형식은 각  $k$ -단체를 실수로 보내면서 특정한 선형성 및 매끄러움 성질을 만족하는 함수입니다 — 예를 들면:

\*  $k \geq 1$ 이고  $k$ -단체의 상이 한 점에 포함되어 있다면, 그것은 0으로 보내져야 합니다.

- \*  $k$ -단체를 재매개변수화하더라도, 부여된 값은 동일해야 합니다.
- \*  $k$ -단체의 두 꼭짓점을 뒤바꾸면, 부여된 값은 부호가 반대가 되어야 합니다.
- \* 두  $k$ -단체를 한 면을 따라 붙여서 하나의  $k$ -단체를 만들 수 있다면, 부여된 값은 그 부분  $k$ -단체들에 부여된 대응 값들의 합이어야 합니다.
- \* 등등.

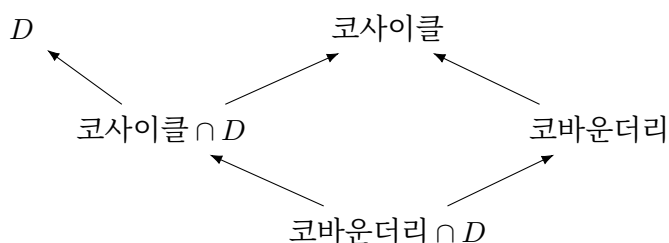
- 닫힌 형식은 경계를 0으로 보내는 미분 형식입니다.
- 완전 형식은 사이클을 0으로 보내는 미분 형식입니다.

우리는 이 대응 관계를 알아차리지 않을 수 없습니다 — 요점은 다음과 같습니다:

$$H^k(M; \mathbb{R}) = \frac{\text{코사이클}}{\text{코바운더리}} \cong \frac{\text{코사이클} \cap \text{미분 형식}}{\text{코바운더리} \cap \text{미분 형식}} = H_{\text{dR}}^k(M).$$

대략적으로 말해, 왼쪽의 분자와 분모가 모두 더 크지만, 이들이 서로 상쇄됩니다. 이를 [절 74.3](#)과 비교해 볼 수 있습니다.

또는, 그림으로 나타내면(지면 관계상 미분 형식의 군은  $D$ 로 표기합니다):



이는 정확히 제2 동형사상 정리의 설정입니다<sup>1</sup>. 그리고 여러분은 이 두 몫이 왜 동형인지 직접 밝혀볼 수 있습니다.

## §76.3 등급 환

**이 절의 대표적인 예:** 다항식 환은 가환 등급 환인 반면,  $\wedge^\bullet(V)$ 는 반가환환입니다.

드람 코호몰로지에서 미분 형식은 또 다른 방식으로 상호작용할 수 있습니다:  $k$ -형식  $\alpha$ 와  $\ell$ -형식  $\beta$ 가 주어지면,  $(k + \ell)$ -형식을 생각할 수 있습니다

$$\alpha \wedge \beta.$$

따라서 형식들의 집합에  $\beta \wedge \alpha = (-1)^{k\ell} \alpha \wedge \beta$ 를 만족하는 “곱”을 부여할 수 있습니다. 이는 더 일반적인 구조의 특수한 경우입니다:

**정의 76.3.1. 등급 유사환**  $R$ 은 아벨 군입니다

$$R = \bigoplus_{d \geq 0} R^d$$

여기서  $R^0, R^1, \dots$ 은 아벨 군이며, 추가로 결합적인 이항 연산  $\times: R \times R \rightarrow R$ 을 가집니다. 우리는  $r \in R^d$ 이고  $s \in R^e$ 이면  $rs \in R^{d+e}$ 이어야 함을 요구합니다.  $R^d$ 의 원소를 **균질 원소**라고 부르며,  $r \in R^d$ 이고  $r \neq 0$ 이면  $|r| = d$ 로 씁니다.

교환법칙을 가정하지 않는다는 점에 유의하십시오. 사실 이러한 “환”은 항등원 1조차 갖지 않을 수도 있습니다. 추가적인 성질이 있는 경우에는 다른 용어를 사용합니다:

<sup>1</sup>절 3.6 참고.

**정의 76.3.2. 등급환**은 1을 가지는 등급 유사환입니다. 이것이 교환적이면 **교환 등급환**이라고 합니다.

**정의 76.3.3.** 등급 (유사)환  $R$ 은, 임의의 균질 원소  $r$ 과  $s$ 에 대해 다음이 성립하면 **반교환적**이라고 합니다

$$rs = (-1)^{|r||s|}sr.$$

**비고 76.3.4** — 왜  $rs = -sr$ 이 아닐까요? 이 정의는 켄기콧이 반교환적이라는 사실에서 영감을 받았습니다.  $f_1, \dots, f_r, g_1, \dots, g_s$ 가 0-형식이라 할 때,  $f = df_1 \wedge df_2 \wedge \dots \wedge df_r$ 을  $r$ -형식으로,  $g = dg_1 \wedge dg_2 \wedge \dots \wedge dg_s$ 을  $s$ -형식으로 두면, 다음 식에서 출발하여

$$f \wedge g = (df_1 \wedge df_2 \wedge \dots \wedge df_r) \wedge (dg_1 \wedge dg_2 \wedge \dots \wedge dg_s)$$

인접한 두 항을 반복적으로 교환하면, 다음 식을 얻기 위해 총  $rs$ 번의 교환이 필요합니다

$$g \wedge f = (dg_1 \wedge dg_2 \wedge \dots \wedge dg_s) \wedge (df_1 \wedge df_2 \wedge \dots \wedge df_r).$$

선형성에 의해, 일반적으로 임의의  $r$ -형식  $f$ 와 임의의  $s$ -형식  $g$ 에 대해  $fg = (-1)^{rs}gf$ 임을 증명할 수 있습니다.

요약하면:

| 등급환의 종류 | 1을 가질 필요가 없음 | 1을 가져야 함 |
|---------|--------------|----------|
| 가정 없음   | 등급 유사환       | 등급환      |
| 반가환     | 반가환 유사환      | 반가환환     |
| 가환      |              | 가환 등급환   |

**예제 76.3.5 (등급환의 예)**

- (a) 환  $R = \mathbb{Z}[x]$ 는 **교환 등급환**이며,  $d$ 번째 성분은  $x^d$ 의 배수들입니다.
- (b) 환  $R = \mathbb{Z}[x, y, z]$ 는 **교환 등급환**이며,  $d$ 번째 성분은 차수  $d$ 인 균질 다항식들(과 0)로 이루어진 아벨 군입니다.
- (c)  $V$ 를 벡터 공간이라 하고, 다음 아벨 군을 고려합시다

$$\dot{\bigwedge}(V) = \bigoplus_{d \geq 0} \bigwedge^d(V).$$

예를 들어,  $e_1 + (e_2 \wedge e_3) \in \dot{\bigwedge}(V)$ 이라고 합시다. 우리는  $\dot{\bigwedge}(V)$ 에 곱  $\wedge$ 를 부여하여 이를 **반교환환**으로 만듭니다.

- (d) 다양체  $M$ 의 미분 형식들의 집합, 즉

$$\Omega^\bullet(M) = \bigoplus_{d \geq 0} \Omega^d(M)$$

에 곱  $\wedge$ 를 부여한 것을 생각해 봅시다. 이것은 **반교환환**입니다.

네 가지 예 모두 곱셈 항등원을 가집니다.

$\Omega^\bullet(M)$ 의 상황으로 돌아가 봅시다. 다시 드람 코호몰로지 군  $H_{\text{dR}}^k(M)$ 을 생각해 보면, 그 원소들은 완전 형식을 법으로 한 닫힌 형식들입니다. 우리는 다음을 주장합니다:

**보조정리 76.3.6** (썰기곱은 드람 코호몰로지를 보존한다)

썰기곱은 다음 사상을 유도합니다

$$\wedge: H_{\text{dR}}^k(M) \times H_{\text{dR}}^\ell(M) \rightarrow H_{\text{dR}}^{k+\ell}(M).$$

증명. 먼저, 연산자  $d$ 가 다음을 만족함을 상기합시다

$$d(\alpha \wedge \beta) = (d\alpha) \wedge \beta + \alpha \wedge (d\beta).$$

이제  $\alpha$ 와  $\beta$ 가 닫힌 형식이라고 합시다. 그러면 위로부터  $\alpha \wedge \beta$ 는 명백히 닫혀 있습니다. 또한  $\alpha$ 가 닫혀 있고  $\beta = d\omega$ 가 완전하면, 다음 항등식으로부터  $\alpha \wedge \beta$ 는 완전합니다

$$d(\alpha \wedge \omega) = d\alpha \wedge \omega + \alpha \wedge d\omega = \alpha \wedge \beta.$$

마찬가지로  $\alpha$ 가 완전하고  $\beta$ 가 닫혀 있으면  $\alpha \wedge \beta$ 는 완전합니다. 따라서 완전 형식을 법으로 곱을 취하는 것이 타당하며, 이로부터 위의 정리가 성립합니다.  $\square$

따라서 우리는 반교환환

$$H_{\text{dR}}^\bullet(M) = \bigoplus_{k \geq 0} H_{\text{dR}}^k(M)$$

을 곱  $\wedge$ 와 항등원  $1 \in \wedge^0(\mathbb{R}) = \mathbb{R}$ 과 함께 얻을 수 있습니다.

**§76.4 컵곱**

이것에서 영감을 받아, 임의의 위상 공간  $X$ 와 환  $R$ (여기서  $R$ 은 항상처럼 1을 갖는 가환환입니다)에 대해  $\bigoplus_{k \geq 0} H^k(X; R)$  위에 유사한 곱을 구성할 수 있는지 살펴보고자 합니다. 이를 수행하는 방법은 컵 곱을 통해서입니다.

그러면 이것은 다음과 같이 두 코사슬을 곱하는 방법을 제공합니다.

**정의 76.4.1.**  $\phi \in C^k(X; R)$ 이고  $\psi \in C^\ell(X; R)$ 이라고 합시다. 그러면 이들의 **컵 곱**  $\phi \smile \psi \in C^{k+\ell}(X; R)$ 을 다음과 같이 정의할 수 있습니다.

$$(\phi \smile \psi)([v_0, \dots, v_{k+\ell}]) = \phi([v_0, \dots, v_k]) \cdot \psi([v_k, \dots, v_{k+\ell}])$$

여기서 곱셈은  $R$ 에서 이루어집니다.

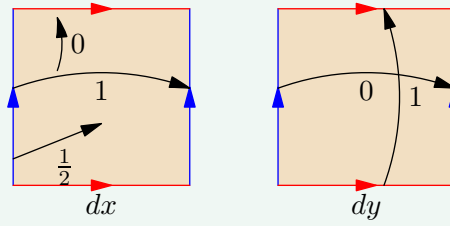
**질문 76.4.2.**  $R$ 이 1을 갖는다고 가정할 때,  $\smile$ 의 항등원이 되는 0-코사슬은 무엇입니까?

**비고 76.4.3 (경고)** —  $n$ -미분 형식을 명백한 방식으로  $n$ -코사슬로 해석할 수는 있지만, 컵 곱은 썰기 곱의 일반화가 아닙니다! 예를 들어,  $X = \mathbb{R}^2$ 라고 하고,  $v_0 = (1, 0)$ ,  $v_1 = (0, 0)$ ,  $v_2 = (0, 1)$ 이며 모든 변이 직선이라고 가정할 때,  $[v_0, v_1, v_2]$ 와  $[v_2, v_1, v_0]$ 에 대해  $dx \smile dy$ 를 계산해 보십시오.

이는 우리가 교대화 연산자를 갖고 있지 않기 때문입니다. 자세한 내용은 **절 44.5**를 참조하십시오. 이 경우 환  $G$ 는 모든 0이 아닌 원소가 역원을 갖지는 않는  $\mathbb{Z}$ 일 수 있으므로, 나눗셈이 문제를 일으킬 것입니다.

그럼에도 불구하고 차이는 깔끔하게 상쇄되며, 코호몰로지 군에서 대응하는 원소는 여전히 썰기 곱  $dx \wedge dy$ 로 해석되는 원소와 같습니다 — 이것이 아래에서 서술할  $H^\bullet(M; \mathbb{R}) \cong H_{\text{dR}}^\bullet(M)$ 이 의미하는 바입니다.

토러스의 익숙한 예와, 1-공사이클 “ $dx$ ”와 “ $dy$ ”를 생각해 봅시다.



썰기 곱에 대해 알고 있는 바로부터,  $T$ 가 토러스 전체일 때 (부호  $\pm$ 까지)  $(dx \wedge dy)(T) = 1$ 이 되기를 원합니다. 실제로 위의 정의를 사용하면 (직접 풀어 보십시오!  $T$ 를 임의로 두 삼각형으로 나누십시오) 이는 성립합니다. 그럼에도 불구하고, 우리는 컵 곱 자체보다는 호몰로지 환 위에 유도되는 컵 곱에 훨씬 더 관심이 있습니다.

먼저, 이전과 유사한 결과를 증명합니다.

#### 보조정리 76.4.4 (컵 곱과 $\delta$ )

$\delta(\phi \smile \psi) = \delta\phi \smile \psi + (-1)^k \phi \smile \delta\psi$ 가 성립합니다.

증명. 직접적인  $\Sigma$  계산입니다. □

따라서 드람 코호몰로지에 사용했던 것과 동일한 절차를 통해, 유도된 사상을 얻습니다.

$$\smile: H^k(X; R) \times H^\ell(X; R) \rightarrow H^{k+\ell}(X; R).$$

그런 다음 원소들이 다음의 유한 합인 **특이 코호몰로지 환**을 정의합니다.

$$H^\bullet(X; R) = \bigoplus_{k \geq 0} H^k(X; R)$$

그리고 곱셈은  $\smile$ 로 주어집니다. 따라서 이는 등급환(항등원은  $1_R \in R$ )이며 실제로 반가환입니다:

#### 명제 76.4.5 (코호몰로지는 반가환입니다)

$H^\bullet(X; R)$ 는 반가환환이며, 이는  $\phi \smile \psi = (-1)^{k\ell} \psi \smile \phi$ 임을 의미합니다.

증명은 [Ha02, 정리 3.11, 210–212쪽]를 참조하십시오. 더욱이, 드람 동형사상이 존재합니다.

#### 정리 76.4.6 (드람은 환 동형사상으로 확장됩니다)

임의의 매끄러운 다양체  $M$ 에 대해, 드람 코호몰로지 군에서 특이 코호몰로지 군으로의 동형사상은 실제로 다음의 동형사상을 제공합니다.

$$H^\bullet(M; \mathbb{R}) \cong H_{\text{dR}}^\bullet(M)$$

반가환환의 동형사상입니다.

따라서 “미분 형식”이 코호몰로지 군의 원소를 시각화하는 방법이라면, 썰기 곱은 컵 곱을 시각화하는 올바른 방법입니다.

이제 몇 가지 흔한 공간들의 코호몰로지 환을 (대부분 증명 없이) 제시합니다.

**예제 76.4.7 (토러스의 코호몰로지)**

토러스의 코호몰로지 환  $H^\bullet(S^1 \times S^1; \mathbb{Z})$ 는 관계식  $\alpha \smile \alpha = \beta \smile \beta = 0$ 과  $\alpha \smile \beta = -\beta \smile \alpha$ 를 만족하는 원소  $|\alpha| = |\beta| = 1$ 에 의해 생성됩니다. (여기에는 항등원 1도 포함됩니다.) 따라서  $\mathbb{Z}$ -가군으로서는

$$H^\bullet(S^1 \times S^1; \mathbb{Z}) \cong \mathbb{Z} \oplus [\alpha\mathbb{Z} \oplus \beta\mathbb{Z}] \oplus (\alpha \smile \beta)\mathbb{Z}.$$

이는 예상된 차원  $1 + 2 + 1 = 4$ 를 줍니다. 이는 반가환적입니다.

여러분은 위 비교에서  $dx$ 와  $dy$ 라고 불리는 원소로서  $\alpha$ 와  $\beta$ 를 이미 본 적이 있습니다.

**예제 76.4.8 ( $S^n$ 의 코호몰로지 환)**

$n \geq 1$ 에 대해  $S^n$ 을 생각해 봅시다. 자명하지 않은 코호몰로지 군은  $H^0(S^n; \mathbb{Z}) \cong H^n(S^n; \mathbb{Z}) \cong \mathbb{Z}$ 로 주어집니다. 따라서 아벨 군으로서는

$$H^\bullet(S^n; \mathbb{Z}) \cong \mathbb{Z} \oplus \alpha\mathbb{Z}$$

여기서  $\alpha$ 는  $H^n(S^n; \mathbb{Z})$ 의 생성원입니다.

이제  $|\alpha \smile \alpha| = 2n$ 임을 관찰합니다. 그러나  $H^{2n}(S^n; \mathbb{Z}) = 0$ 이므로  $\alpha \smile \alpha = 0$ 이어야 합니다. 따라서 더 간결하게는,

$$H^\bullet(S^n; \mathbb{Z}) \cong \mathbb{Z}[\alpha]/(\alpha^2).$$

혼란스럽게도, 이 등급 환은 가환적이면서 동시에 반가환적입니다. 그 이유는  $\alpha \smile \alpha = 0 = -(\alpha \smile \alpha)$ 이기 때문입니다.

**예제 76.4.9 (실사영 공간과 복소사영 공간의 코호몰로지 환)**

다음이 성립함이 밝혀져 있습니다.

$$H^\bullet(\mathbb{RP}^n; \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}[\alpha]/(\alpha^{n+1})$$

$$H^\bullet(\mathbb{CP}^n; \mathbb{Z}) \cong \mathbb{Z}[\beta]/(\beta^{n+1})$$

여기서  $|\alpha| = 1$ 은  $H^1(\mathbb{RP}^n; \mathbb{Z}/2\mathbb{Z})$ 의 생성원이고  $|\beta| = 2$ 는  $H^2(\mathbb{CP}^n; \mathbb{Z})$ 의 생성원입니다.

혼란스럽게도, 두 등급 환 모두 가환적이면서 동시에 반가환적입니다. 첫 번째 경우는  $\mathbb{Z}/2\mathbb{Z}$ 에서 작업하기 때문인데, 여기서는  $1 = -1$ 이므로 반가환성이 실제로 가환성과 동치가 됩니다. 두 번째 경우는 모든 영이 아닌 동차 원소가 차수 2를 갖기 때문입니다.

여기서 이미 곱  $\smile$ 이 켜기 곱  $\wedge$ 와 다른 흥미로운 예를 하나 얻었습니다 —  $n \geq 2$ 이면, 위의 생성원  $\alpha$ 와  $\beta$ 는  $\alpha \smile \alpha \neq 0$ 이고  $\beta \smile \beta \neq 0$ 입니다.

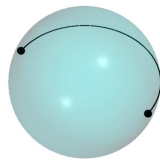
여기서 무슨 일이 일어나는지 살펴봅시다. 위의 공식은 다음을 말해줍니다.

$$H^\bullet(\mathbb{RP}^2; \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}[\alpha]/(\alpha^3)$$

아벨 군으로서,  $H^0(\mathbb{RP}^2; \mathbb{Z}/2\mathbb{Z})$ ,  $H^1(\mathbb{RP}^2; \mathbb{Z}/2\mathbb{Z})$ ,  $H^2(\mathbb{RP}^2; \mathbb{Z}/2\mathbb{Z})$ 에는 각각 영이 아닌 원소가 하나씩 있으며, 나머지 군은 0입니다.

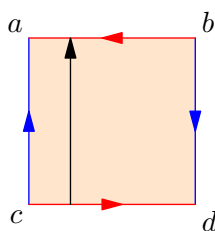
$\mathbb{RP}^2$ 는 시각화하기가 그리 어렵지 않습니다 — 이는 단순히 반대편 꼭짓점을 동일시하는 관계로 뭉을 취한 2-구입니다.

그 위에는 0과 호모토피가 아닌(호몰로지가 아닌) 1-사이클이 존재합니다:



보여기가 그리 쉽지는 않지만, 이러한 모든 1-사이클은 서로 호몰로지가 같으며, 그 사이클의 두 배는 0과 호몰로지가 같습니다.

이에 따라  $H^1(\mathbb{RP}^2; \mathbb{Z}/2\mathbb{Z}) \cong \text{Hom}(H_1(\mathbb{RP}^2), \mathbb{Z}/2\mathbb{Z})$ 이며, 그 유일한 자명하지 않은 원소  $\alpha$ 는 이러한 각 1-사이클을 1로 보냅니다.



$\alpha \smile \alpha$ 를 생각해 봅시다.  $\alpha$ 는  $dx$ 와  $dy$  둘 다처럼 동시에 작용한다는 점에 주목합시다(파란 변과 빨간 변 모두 값 1이 할당되었습니다), 따라서 이는 실사영평면 전체 곡면에 값 1을 할당합니다! 따라서 이는 자명하지 않습니다.

**연습문제 76.4.10.** 이를 확인하기 위해 컵 곱  $\alpha \smile \alpha$ 를 직접 계산해 보십시오. (곡면을 몇 개의 삼각형으로 나누십시오.  $[a, c, d] + [a, d, b] - [c, c, d] + [c, d, c]$ 가 하나의 유효한 선택입니다. 경계가 영이 아니지만 2로 나누어떨어짐을 확인하십시오.)

## §76.5 상대 코호몰로지 유사환

$A \subseteq X$ 에 대해, 상대 컵 곱 또한 정의할 수 있습니다.

$$H^k(X, A; R) \times H^\ell(X, A; R) \rightarrow H^{k+\ell}(X, A; R).$$

결국, 두 코사슬 중 하나가  $A$  안의 사슬에서 사라진다면, 그들의 컵 곱 역시 사라집니다. 이를 통해 **상대 코호몰로지 유사환**과 **축소 코호몰로지 유사환**(단,  $A = \{*\}$ )을 정의할 수 있습니다. 즉,

$$H^\bullet(X, A; R) = \bigoplus_{k \geq 0} H^k(X, A; R)$$

$$\tilde{H}^\bullet(X; R) = \bigoplus_{k \geq 0} \tilde{H}^k(X; R).$$

이들은 모두 **반가환 유사환**입니다. 실제로, 종종  $\tilde{H}^0(X; R) = 0$ 이 성립하여 항등원이 전혀 존재하지 않습니다.

다시 한번 함자성을 확인할 수 있습니다.

**정리 76.5.1 (코호몰로지 (유사)환은 함자적이다)**

환  $R$ (교환환이며 1을 가짐)을 고정합시다. 그러면 다음과 같은 함자를 얻습니다

$$\begin{aligned} H^\bullet(-; R) : \mathbf{hTop}^{\text{op}} &\rightarrow \mathbf{GradedRings} \\ H^\bullet(-, -; R) : \mathbf{hPairTop}^{\text{op}} &\rightarrow \mathbf{GradedPseudoRings}. \end{aligned}$$

안타깝게도, (코)호몰로지 군과는 달리, CW 복합체와 같은 좋은 공간에 대해서조차 컵 곱을 결정하는 것<sup>2</sup>은 자명하지 않은 작업입니다. 따라서 계산 측면에서는 많은 것을 다루지 않을 것입니다. 그러나 약간의 진전은 이를 수 있습니다.

**§76.6 췌기합**

이제 우리의 목표는  $\tilde{H}^\bullet(X \vee Y)$ 를 계산하는 것입니다. 이를 위해서는 두 등급 유사환의 곱을 정의해야 합니다.

**정의 76.6.1.**  $R$ 과  $S$ 를 두 등급 유사환이라 합시다. **곱 유사환**  $R \times S$ 는 그 바탕이 되는 아벨 군을 다음과 같이 취함으로써 정의되는 등급 유사환입니다

$$R \oplus S = \bigoplus_{d \geq 0} (R^d \oplus S^d).$$

곱셈은  $R$ 과  $S$ 로부터 오며, 이어서  $r \in R, s \in S$ 에 대해  $r \cdot s = 0$ 으로 선언합니다.

이는 **예제 4.3.8**에서 정의된 곱 환의 등급 버전일 뿐임에 주목하십시오.

**연습문제 76.6.2.**  $R$ 과  $S$ 가 등급 환(즉  $1_R$ 과  $1_S$ 를 가진다는 뜻)이라면,  $R \times S$  역시 그러함을 보이십시오.

이제, 정리는 다음과 같습니다.

**정리 76.6.3 (췌기합의 코호몰로지 유사환)**

다음이 성립합니다

$$\tilde{H}^\bullet(X \vee Y; R) \cong \tilde{H}^\bullet(X; R) \times \tilde{H}^\bullet(Y; R)$$

등급 유사환으로서 말입니다.

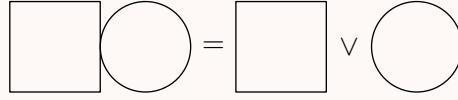
단지 두 환이 동형이라는 사실만 알아서는 큰 도움이 되지 않으며, 그 동형사상이 무엇인지 안다면 훨씬 더 좋을 것입니다 — 그래야 간단한 경우에는 여러분 스스로 두 환이 동형임을 직접 확인할 수 있습니다.

이 동형사상은 가장 자명한 것입니다:  $X \vee Y$  안의 각 사슬  $c$ 에 값  $f(c) \in R$ 를 대응시키는  $f \in C^\bullet(X \vee Y; R)$ 가 주어졌을 때, 이를  $C^\bullet(X)$ 의 원소로 해석할 수 있습니다. 왜냐하면  $X$  안의 각 사슬은 자명하게  $X \vee Y$  안의 사슬이기도 하여  $f$ 에 넣을 수 있기 때문입니다 — 형식적으로는, 매장  $X \hookrightarrow X \vee Y$ 가  $C_\bullet(X) \hookrightarrow C_\bullet(X \vee Y)$ 를 유도합니다. 이 사상은  $\tilde{H}^\bullet(X \vee Y; R) \rightarrow \tilde{H}^\bullet(X; R) \times \tilde{H}^\bullet(Y; R)$ 를 유도하며, 환 곱셈, 즉 컵 곱을 보존합니다.

<sup>2</sup>미분 형식으로 옮겨갔다가 다시 돌아오는 방법을 제외하면 말입니다. 여러분은 이미 위에서 췌기곱을 계산해 본 적이 있습니다.

**예제 76.6.4**

$X$ 와  $Y$ 가 다음 그림과 같이 나타내어져 있다고 합시다.



$f \in \tilde{H}^1(X; \mathbb{Z})$ 가 전체 정사각형에  $f(X) = 2$ 를 대응시키고,  $g \in \tilde{H}^1(Y; \mathbb{Z})$ 가 전체 원에  $g(Y) = 3$ 을 대응시킨다고 합시다. 그러면, 물론  $\tilde{H}^1(X \vee Y)$  안에서  $(f, g)$ 에 대응하는 원소는 전체 공간  $X \vee Y$ 에 대응하는 코사이클에  $2 + 3 = 5$ 를 대응시킬 것입니다.

이를 통해 서두에서 제기된 첫 번째 질문을 해결할 수 있습니다.  $X = \mathbb{CP}^2$ 이고  $Y = S^2 \vee S^4$ 라 합시다. 다음이 성립합니다

$$H^\bullet(\mathbb{CP}^2; \mathbb{Z}) \cong \mathbb{Z}[\alpha]/(\alpha^3).$$

따라서 이는 세 개의 원소로 생성되는 등급 환입니다.

- 차원 0에서의 1.
- 차원 2에서의  $\alpha$ .
- 차원 4에서의  $\alpha^2$ .

다음으로, 축소 코호몰로지 유사환을 생각해 봅시다

$$\tilde{H}^\bullet(S^2 \vee S^4; \mathbb{Z}) \cong \tilde{H}^\bullet(S^2; \mathbb{Z}) \oplus \tilde{H}^\bullet(S^4; \mathbb{Z}).$$

따라서 절대 코호몰로지 환  $H^\bullet(S^2 \vee S^4; \mathbb{Z})$ 는 마찬가지로 세 개의 원소로 생성되는 등급 환입니다.

- 1은 차원 0에 있습니다 (0차원을 다시 더해 넣으면).
- $a_2$ 는 차원 2에 있습니다 ( $H^\bullet(S^2; \mathbb{Z})$ 로부터).
- $a_4$ 는 차원 4에 있습니다 ( $H^\bullet(S^4; \mathbb{Z})$ 로부터).

예상했던 대로 각 등급 성분은 동형입니다. 그러나 전자에서는 차수 2인 두 생성원의 곱이

$$\alpha \cdot \alpha = \alpha^2.$$

후자에서는 차수 2인 두 생성원의 곱이

$$a_2 \cdot a_2 = a_2^2 = 0$$

$a_2 \smile a_2 = 0 \in H^\bullet(S^2; \mathbb{Z})$ 이기 때문입니다.

따라서  $S^2 \vee S^4$ 와  $\mathbb{CP}^2$ 는 호모토피 동치가 아닙니다.

직관적으로, 위 증명이 말하는 바는 다음과 같습니다:

**자명하지 않은 4-공사슬**  $a_4 \in H^4(S^2 \vee S^4; \mathbb{Z})$ 는 2-공사슬  $a_2$ 와 아무 관련이 없는 반면, 4-공사슬  $\alpha^2 \in H^4(\mathbb{CP}^2)$ 는 2-공사슬  $\alpha$ 와 자기 자신의 컵곱  $\alpha \smile \alpha$ 입니다.

아래 연습문제는  $\mathbb{RP}^2$ 가 비배향임을 제외하면 시각화하기 훨씬 쉬울 것입니다 — 사실, 우리는 위에서 왜  $\alpha \in H^1(\mathbb{RP}^2)$ 인 영이 아닌 원소에 대해  $\alpha \smile \alpha \neq 0$ 인지 이미 살펴보았습니다.

**연습문제 76.6.5.** 마찬가지로, 각 등급 성분이 동형임에도 불구하고  $\tilde{H}^\bullet(S^1 \vee S^2; \mathbb{Z}/2\mathbb{Z}) \not\cong \tilde{H}^\bullet(\mathbb{RP}^2; \mathbb{Z}/2\mathbb{Z})$ 임을 보여서  $S^1 \vee S^2$ 와  $\mathbb{RP}^2$ 가 호모토피 동치가 아님을 보이십시오.

## §76.7 교차곱

이 절에서는 교차곱을 정의하겠습니다.

### §76.7.i 동기

대략적으로 말해, 동기는 다음과 같습니다:

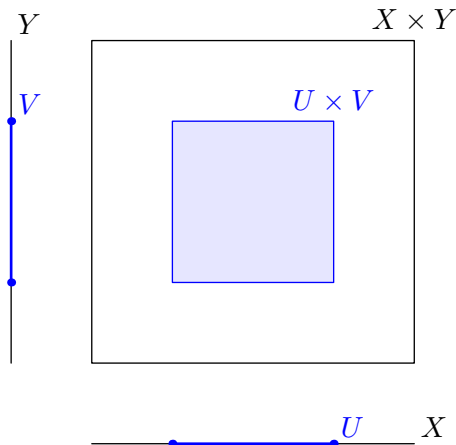
$X$ 가  $m$ 차원 구멍을 가지고  $Y$ 가  $n$ 차원 구멍을 가진다면,  $X \times Y$ 는  $(m+n)$ 차원 구멍을 가집니다.

이는 "구멍"을 적절히 해석했을 때(호몰로지로는 코호몰로지로는) 대부분의 흔한 경우에 참입니다.

우리는 위 명제를 형식화하고 증명할 것입니다.

### §76.7.ii 특이 호몰로지에서의 교차곱

먼저,  $m$ -단체  $f: \Delta^m \rightarrow X$ 와  $n$ -단체  $g: \Delta^n \rightarrow Y$ 를 받아서  $(m+n)$ -사슬  $f \times g \in C_{m+n}(X \times Y)$ 를 반환하는 **교차곱**을 정의합니다.<sup>3</sup> 이것이야말로 여러분이 이를 정의할 가장 자연스러운 방법입니다: 직관적으로,  $X$  안의  $m$ 차원 정육면체와  $Y$  안의  $n$ 차원 정육면체의 곱은  $X \times Y$  안의  $(m+n)$ 차원 정육면체입니다.



단체의 경우,  $\Delta^m \times \Delta^n$ 을 유한히 많은  $\Delta^{m+n}$ 의 복사본들로 세분해야 합니다.

$n = 1$ 인 경우에는 프리즘 연산자를 다룰 때 이미 세분을 살펴본 바 있습니다. 일반적인 경우에 대해서는 [Ha02, page 277]를 참고하십시오 — 그 개수는 빠르게 커지는데, 예를 들어  $\Delta^{15} \times \Delta^{15}$ 를 덮으려면  $\binom{30}{15} = 155117520$ 개의 단체가 필요합니다!

형식적으로, 우리는 사슬의 교차곱을 다음과 같은 함수로 정의할 수 있습니다:

$$C_m(X) \times C_n(Y) \xrightarrow{\times} C_{m+n}(X \times Y).$$

이것이 호몰로지 군 위의 사상을 유도함을 증명할 수 있습니다:

$$H_m(X) \times H_n(Y) \xrightarrow{\times} H_{m+n}(X \times Y).$$

<sup>3</sup>제가 아는 한, 이는 그저 기호  $\times$ 가 십자가 모양이기 때문이며,  $\mathbb{R}^3$ 에서의 벡터 외적과는 아무 관련이 없습니다.

**연습문제 76.7.1.**  $X = Y = S^1$ 이라 하여,  $X \times Y$ 가 토러스가 되도록 합시다.  $\alpha$ 를  $H_1(X)$ 의 생성원,  $\beta$ 를  $H_1(Y)$ 의 생성원이라 합시다.  $\alpha \times \beta$ 가  $H_2(X \times Y)$ 의 생성원임을 보이십시오.

사실, 다음이 성립합니다:

### 정리 76.7.2

$X$ 와  $Y$ 가 CW 복합체이고  $R$ 이 PID이면,  $H_m(X)$ 와  $H_n(Y)$ 의 0이 아닌 두 원소의 교차곱은 0이 아닙니다.

이는 앞서 우리가 가졌던 직관을 공식화합니다 — 적어도, 호몰로지를 "구멍"의 척도로 사용한다면 그렇습니다.

### §76.7.iii 교차곱은 $\mathbb{Z}$ -가군 준동형사상이 아님

이 절에서는,  $a$ 와  $b$ 가 각각  $\mathbb{Z}$ -가군  $C_m(X)$ 와  $C_n(Y)$ 의 원소일 때,  $\times(a, b)$ 를  $a \times b \in C_{m+n}(X \times Y)$ 를 의미하는 것으로 쓰고,  $(a, b)$ 는 곱  $C_m(X) \times C_n(Y)$ 에서 대응하는 원소를 나타내는 것으로 씁니다.

우리가 정리해야 할 작은 기술적 세부사항이 있습니다 — 위에서, 우리는 다음과 같이 씁니다

$$\times: C_m(X) \times C_n(Y) \rightarrow C_{m+n}(X \times Y).$$

하지만 이렇게 쓰면,  $\times$ 는  $\mathbb{Z}$ -가군 준동형사상이 아닙니다!

### 예제 76.7.3

$a$ 와  $b$ 를 각각  $C_m(X)$ 와  $C_n(Y)$ 의 임의의 0이 아닌 원소라 합시다. 그러면,

$$\begin{aligned}\times(a, b) &= a \times b \\ 2 \cdot (a, b) &= (2a, 2b) \\ \times(2 \cdot (a, b)) &= 4(a \times b).\end{aligned}$$

동형사상에 대해 논하거나,  $C_{m+n}(X \times Y)$  또는  $H_{m+n}(X \times Y)$ 의  $\mathbb{Z}$ -가군 구조를 가지고 무언가를 하고자 한다면,  $\mathbb{Z}$ -가군 준동형사상을 갖는 편이 좋습니다.

이는 쉽게 고칠 수 있습니다:  $\times$ 는 쌍선형이므로, 텐서곱을 고려하는 것이 자연스럽습니다:

$$\times: C_m(X) \otimes_{\mathbb{Z}} C_n(Y) \rightarrow C_{m+n}(X \times Y).$$

이 표기법으로,  $\times(a \otimes b) = a \times b$ 입니다. (부수적으로, 이제  $\times(a \otimes b + c \otimes d) = a \times b + c \times d$ 라고도 쓸 수 있습니다.)

그러므로, 정리 76.7.2을 다시 서술해 봅시다:

### 정리 76.7.4

$X$ 와  $Y$ 가 CW 복합체이면,

$$\times: H_m(X) \otimes_{\mathbb{Z}} H_n(Y) \rightarrow H_{m+n}(X \times Y)$$

는 단사  $\mathbb{Z}$ -가군 준동형사상입니다.

### §76.7.iv 세포 호몰로지에서의 교차곱

특이 호몰로지를 이용한 정의는 상당히 번거롭습니다 — 사슬의 구성 요소로 단체를 사용하기 때문에,  $X$ 와  $Y$ 에서 두 단체의 곱은  $X \times Y$ 에서 방대한 단체들의 모임이 됩니다.

이제 세포 호몰로지를 이용해 교차곱을 다시 정의할 것입니다 — 교차곱의 두 정의가 호몰로지 군에서 동일한 결과를 주기 때문에, 안전하게 건너뛰어도 됩니다.

$X$ 와  $Y$ 가 CW 복합체이면, 더 잘할 수 있습니다.  $X \times Y$ 는 자연스러운 CW 복합체 구조를 가짐을 알 수 있습니다:  $X$ 의 각 세포  $e^m$ 과  $Y$ 의 세포  $e^n$ 에 대해, 그 곱은  $X \times Y$ 의 세포  $e^{m+n}$ 을 이룹니다.

#### 예제 76.7.5

$X$ 와  $Y$ 가 둘 다 두 개의 0-세포와 하나의 1-세포로 이루어진 선분이면, 이들의 곱  $X \times Y$ 는 다음을 포함하는 자연스러운 CW 복합체 구조를 갖습니다:

- 4개의 0-세포,
- 4개의 1-세포,
- 1개의 2-cell입니다.

장 74에서 다룬 세포 군  $\text{Cells}_\bullet(X)$ 를 떠올려 보십시오. 각 기저 원소는  $X$ 의 한 세포에 대응합니다. 그러면 기저 원소들에 대해 십자곱을 정의할 수 있습니다:

$$\times : \text{Cells}_m(X) \otimes_{\mathbb{Z}} \text{Cells}_n(Y) \rightarrow \text{Cells}_{m+n}(X \times Y).$$

지독하게 명시적으로 말하자면:  $e^m \in \text{Cells}_m(X)$ ,  $e^n \in \text{Cells}_n(Y)$ 라 할 때, 십자곱은  $e^m \times e^n = e^m \times e^n \in \text{Cells}_{m+n}(X \times Y)$ 로 정의됩니다 — 사용된 표기법조차 자명합니다.

물론 이는 호몰로지 군 사이의 사상을 유도합니다:

$$\times : H_m(X) \otimes_{\mathbb{Z}} H_n(Y) \rightarrow H_{m+n}(X \times Y).$$

이 사상은 앞서 정의한 사상과 동일합니다.

### §76.7.v 세포 코호몰로지에서의 십자곱

위와 같은 방식을 이번에는 코호몰로지에 대해 적용합니다 — 호몰로지와 코호몰로지는 "구멍"을 재는 방식이 미묘하게 다르다는 점을 기억하십시오. 클라인 병  $K$ 의 경우  $H_2(X) = 0$ 이지만  $H^2(X; \mathbb{Z}) \neq 0$ 입니다.

두 세포 코사슬  $f \in \text{Hom}(\text{Cells}_m(X); R)$ 과  $g \in \text{Hom}(\text{Cells}_n(Y); R)$ 이 주어졌을 때, 코사슬  $f \times g \in \text{Hom}(\text{Cells}_{m+n}(X \times Y); R)$ 을 얻고자 합니다.

물론 이는 가장 자연스러운 방식으로 정의됩니다:  $X$ 의 세포  $e^m$ 과  $Y$ 의 세포  $e^n$ 에 대해,  $(f \times g)(e^m \times e^n) = f(e^m) \cdot g(e^n)$ 이 성립합니다.

그렇듯해 보입니까? 아직은 아닙니다 —  $X \times Y$ 의 모든  $(m+n)$ -세포  $e^{m+n}$ 이  $X$ 의  $m$ -세포와  $Y$ 의  $n$ -세포의 곱으로 이루어지는 것은 아니기 때문입니다. 그러한 경우에는 단순히  $(f \times g)(e^{m+n}) = 0$ 이라고 선언합니다.

늘 그렇듯이, 이 사상은 코호몰로지 군 사이의  $R$ -가군 준동형사상을 유도합니다:

$$\times : H^m(X; R) \otimes_R H^n(Y; R) \rightarrow H^{m+n}(X \times Y; R).$$

### §76.7.vi 동기 부여: 미분 형식의 십자곱

위에서 다룬 두 세포 코사슬의 십자곱의 정의는 깔끔하지만, 무미건조하고 동기가 부족해 보일 수 있습니다.

알고 보면 미분 형식에 대해서도 같은 방식을 적용할 수 있습니다. 게다가 이는 켤레곱  $\alpha \wedge \beta$ 를 정의하는 깔끔한 방법을 제공합니다! 실제로 어떻게 작동하는지 살펴봅시다.

정의를 제시하는 대신, 여기 몇 가지 예시를 들어보겠습니다. 동기가 충분한 독자라면 이 개념을 formal하게 정의해 볼 수 있을 것입니다.

#### 예제 76.7.6 (미분 형식의 십자곱 예시)

여기 몇 가지 예시가 있습니다.

- $X$ 와  $Y$ 가 각각 평면의  $x$ 축과  $y$ 축이라면, 십자곱  $dx \times dy$ 는  $2(dx \wedge dy)$ 와 같습니다.

이는 분명 자연스럽습니다 —  $dx$ 는 벡터  $\mathbf{e}_1$ 에 값 1을 부여하고,  $2dy$ 는 벡터  $\mathbf{e}_2$ 에 값 2를 부여하므로,  $dx \times 2dy$ 는  $\mathbf{e}_1$ 과  $\mathbf{e}_2$ 로 생성되는 단위 정사각형 — 즉  $\mathbf{e}_1 \wedge \mathbf{e}_2$  — 에 값  $1 \cdot 2 = 2$ 를 부여해야 함을 알 수 있습니다.

- $X$ 를  $xy$ -평면이라 하고,  $Y$ 를  $z$ 축이라 합시다. 십자곱  $dx \times dz$ 를 생각해 봅시다. 그 결과는 어떤 2-형식이어야 하겠습니까?

분명히  $(dx \times dz)(\mathbf{e}_1 \wedge \mathbf{e}_3) = 1$ 이고  $(dx \times dz)(\mathbf{e}_2 \wedge \mathbf{e}_3) = 0$ 이어야 합니다. 하지만 이것만으로는  $dx \times dz$ 를 유일하게 결정하기에 충분하지 않습니다.

그래서 우리는 다음과 같이 선언합니다:  $(dx \times dz)(\mathbf{e}_1 \wedge \mathbf{e}_2) = 0$ . 이로써  $dx \times dz = dx \wedge dz$ 를 얻습니다.

더 일반적으로,  $X$ 와  $Y$ 에 대한 기저를 선택하고 기저 원소들에 대한  $\alpha \times \beta$ 의 값을 정의함으로써 십자곱을 정의할 수 있습니다.

약속한 대로 — 십자곱을 이용해 켤레곱을 정의할 수 있습니다. 할 수 있는 방법은 오직 하나뿐입니다:

**정의 76.7.7** (켤레곱을 크로스곱을 이용해 정의하기).  $X$ 가  $\mathbb{R}$ -벡터 공간일 때,  $\alpha \in (\wedge^m(X))^\vee$  이고  $\beta \in (\wedge^n(X))^\vee$ 라 하면,  $\alpha \wedge \beta \in (\wedge^{m+n}(X))^\vee$ 는 다음과 같이 정의됩니다

$$\alpha \wedge \beta = \Delta^*(\alpha \times \beta)$$

여기서  $\Delta: X \rightarrow X \times X$ ,  $\Delta(x) = (x, x)$ 는 대각 사상입니다.  $\Delta^*$ 가 당겨오기 연산을 나타낸다는 것을 상기하십시오.

더 간단히 말하면,  $\alpha \wedge \beta$ 를  $X$  안의  $(m+n)$ -켤레에 대해 계산하려면, 대각 사상을 이용해 그것을  $X \times X$ 로 밀어 보낸 다음,  $\alpha \times \beta$ 에 넘겨주면 됩니다.

#### §76.7.vii 코호몰로지 군들을 이어붙이기

위에서 우리가  $R$ -가군 준동형사상을 가지고 있었음을 상기하십시오

$$\times: H^m(X; R) \otimes_R H^n(Y; R) \rightarrow H^{m+n}(X \times Y; R).$$

모든  $H^\bullet(X; R)$ 을 실제로 이어붙여 반가환 등급환, 즉 코호몰로지 환을 만드는 것이 가능하다는 것을 우리는 알고 있습니다. 그래서 우리는 이 사상을  $R$ -대수 준동형사상으로 확장하고자 합니다

$$\times: H^\bullet(X; R) \otimes_R H^\bullet(Y; R) \rightarrow H^\bullet(X \times Y; R).$$

우리는 아직 두 등급환의 텐서곱이 무엇인지 정의하지 않았습니다 — 다음 절에서 이를 formal하게 정의할 것입니다만, 직관적으로는 모든  $H^m(X; R) \otimes_R H^n(Y; R)$ 을 이어붙인 것으로 이루어집니다.

## §76.8 Künneth 공식

이제  $S^2 \times S^4$ 와  $\mathbb{CP}^3$  공간을 구별하고자 합니다. 이를 위해서는  $H^n(X; R)$ 와  $H^n(Y; R)$ 를 이용하여  $H^n(X \times Y; R)$ 를 나타내는 공식이 필요합니다. 이러한 공식을 **Künneth 공식**이라고 부릅니다. 이 절에서는 두 등급환의 텐서곱과 관련된 매우 특수한 경우만 사용하겠습니다.

**정의 76.8.1.**  $A$ 와  $B$ 를  $R$ -가군이기도 한 두 등급환이라 합시다(여기서  $R$ 은 1을 갖는 가환 환입니다). **텐서곱**  $A \otimes_R B$ 를 다음과 같이 정의합니다. 아벨 군으로서는, 그것은

$$A \otimes_R B = \bigoplus_{d \geq 0} \left( \bigoplus_{k=0}^d A^k \otimes_R B^{d-k} \right).$$

곱셈은 기저 원소들에 대해 다음과 같이 주어집니다

$$(a_1 \otimes b_1)(a_2 \otimes b_2) = (a_1 a_2) \otimes (b_1 b_2).$$

물론 곱셈 항등원은  $1_A \otimes 1_B$ 입니다.

이제  $X$ 와  $Y$ 를 위상 공간이라 하고, 그 곱을 취합시다: 우리는 다음 도식을 가집니다

$$\begin{array}{ccc} & X \times Y & \\ \pi_X \swarrow & & \searrow \pi_Y \\ X & & Y \end{array}$$

여기서  $\pi_X$ 와  $\pi_Y$ 는 사영입니다.  $H^k(-; R)$ 이 함자적이므로, 이는 유도된 사상들을 줍니다

$$\begin{aligned} \pi_X^* &: H^k(X \times Y; R) \rightarrow H^k(X; R) \\ \pi_Y^* &: H^k(X \times Y; R) \rightarrow H^k(Y; R) \end{aligned}$$

모든  $k$ 에 대해.

이를 이용하면, 이른바 **크로스곱**을 정의할 수 있습니다.

**정의 76.8.2.**  $R$ 을 환이라 하고,  $X$ 와  $Y$ 를 공간이라 합시다.  $\pi_X$ 와  $\pi_Y$ 를  $X \times Y$ 에서 각각  $X$ 와  $Y$ 로의 사영이라 합시다. 그러면 **크로스곱**은 다음과 같은 사상입니다

$$H^\bullet(X; R) \otimes_R H^\bullet(Y; R) \xrightarrow{\times} H^\bullet(X \times Y; R)$$

이는 다음과 같이 코사이클에 작용합니다:  $\phi \times \psi = \pi_X^*(\phi) \smile \pi_Y^*(\psi)$ .

이는  $X$  위의  $k$ -코사이클과  $Y$  위의  $\ell$ -코사이클을 가지고 곱공간  $X \times Y$  위의  $(k + \ell)$ -코사이클을 만드는 가장 자연스러운 방법일 뿐입니다.

**비고 76.8.3** — 물론, 이 정의는 위에서 세포 코호몰로지를 이용한 정의와 일치합니다만, 증명은 생략합니다.

### 정리 76.8.4 (Künneth 공식)

$X$ 와  $Y$ 를 CW 복합체라 하고, 모든  $k$ 에 대해  $H^k(Y; R)$ 이 유한 생성 자유  $R$ -가군이라 합시다. 그러면 크로스곱은 다음과 같은 반가환환의 동형사상입니다

$$H^\bullet(X; R) \otimes_R H^\bullet(Y; R) \rightarrow H^\bullet(X \times Y; R).$$

즉:

$X$ 와  $Y$ 의 구멍 쌍과  $X \times Y$ 의 구멍 사이에는 일대일 대응이 존재합니다. 더욱이, 이 대응은 컵 곱을 보존합니다.

여기서 "구멍"은 이 경우 "코호몰로지 군의 생성원"으로 이해되어야 합니다.

어쨌든, 이로써 처음에 제기했던 질문을 마침내 해결할 수 있습니다. 우리는 모든  $n$ 에 대해  $H_n(\mathbb{CP}^3) \cong H_n(S^2 \times S^4)$ 임을 보았으므로, 따라서  $H^n(\mathbb{CP}^3; \mathbb{Z}) \cong H^n(S^2 \times S^4; \mathbb{Z})$  역시 성립합니다.

하지만 이제 코호몰로지 환을 살펴봅시다. 먼저, 다음을 얻습니다

$$H^\bullet(\mathbb{CP}^3; \mathbb{Z}) \cong \mathbb{Z}[\alpha]/(\alpha^4) \cong \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \alpha^2\mathbb{Z} \oplus \alpha^3\mathbb{Z}$$

여기서  $|\alpha| = 2$ 이며, 따라서 이는 다음에 의해 생성되는 등급환입니다

- 1, 차수 0.
- $\alpha$ , 차수 2.
- $\alpha^2$ , 차수 4.
- $\alpha^3$ , 차수 6.

이제 다음을 분석해봅시다

$$H^\bullet(S^2 \times S^4; \mathbb{Z}) \cong \mathbb{Z}[\beta]/(\beta^2) \otimes \mathbb{Z}[\gamma]/(\gamma^2).$$

따라서 이는 다음 원소들에 의해 생성됩니다:

- $1 \otimes 1$ , 차수 0.
- $\beta \otimes 1$ , 차수 2.
- $1 \otimes \gamma$ , 차수 4.
- $\beta \otimes \gamma$ , 차수 6.

다시금 각 차원에서 우리는 동일한 아벨 군을 얻습니다. 하지만  $\beta \otimes 1$ 을 제공하면 다음을 얻는다는 점에 주목하십시오

$$(\beta \otimes 1)(\beta \otimes 1) = \beta^2 \otimes 1 = 0.$$

그러나  $H^\bullet(\mathbb{CP}^3; \mathbb{Z})$ 의 차수 2 생성원은 이러한 성질을 갖지 않습니다. 따라서 이 두 등급환은 동형이 아닙니다.

$S^2 \times S^4$ 의 자명하지 않은 4차 코사이클  $1 \otimes \gamma$ 는 2차 코사이클  $\beta \otimes 1$ 과 직교하는 반면,  $\mathbb{CP}^3$ 의 4차 코사이클  $\alpha^2$ 는 2차 코사이클  $\alpha$  자신과의 컵 곱  $\alpha \smile \alpha$ 입니다.

따라서  $\mathbb{CP}^3$ 와  $S^2 \times S^4$ 는 호모토피 동치가 아니라는 결론이 나옵니다.

**연습문제 76.8.5.**  $H^\bullet(\mathbb{RP}^3; \mathbb{Z}/2\mathbb{Z})$ 와  $H^\bullet(S^1 \times S^2; \mathbb{Z}/2\mathbb{Z})$ 에 대해서도 같은 절차를 수행하십시오. ( $S^1 \times S^2$ 를 바깥면과 안쪽면이 붙어 있는 두꺼워진 구로,  $\mathbb{RP}^3$ 를 경계면 위의 대척점들이 붙어 있는 닫힌 3차원 공으로 시각화해 보십시오. 형식적으로 계산하기 전에, 상상력을 발휘하여 호몰로지 군과 코호몰로지 군이 무엇인지 추측해 보십시오.)

## §76.9 생각해 볼 만한 조금 더 어려운 문제

**문제 76A<sup>†</sup>** (푸앵카레쌍대성에 의한 베티 수의 대칭성).  $M$ 을 매끄러운 방향 지어진 콤팩트  $n$ 차원 다양체라 하고,  $b_k$ 를 그 베티 수라 하십시오.  $b_k = b_{n-k}$ 임을 증명하십시오.

**문제 76B.** 짝수  $n$ 에 대해  $\mathbb{R}P^n$ 이 방향 지을 수 없음을 보이십시오.

**문제 76C.**  $\mathbb{R}P^3$ 이  $\mathbb{R}P^2 \vee S^3$ 과 호모토피 동치가 아님을 보이십시오.



**문제 76D.** 모든  $m, n \geq 1$ 에 대해  $S^m \vee S^n$ 이  $S^m \times S^n$ 의 변형 수축이 아님을 보이십시오.



# XIX

대수기하학 I: 고전적 다양체

## 제XIX부: 목차

---

|           |                                                  |            |
|-----------|--------------------------------------------------|------------|
| <b>77</b> | <b>아핀 다양체</b>                                    | <b>805</b> |
| 77.1      | 아핀 다양체 . . . . .                                 | 805        |
| 77.2      | 아이디얼을 통한 아핀 다양체의 명명 . . . . .                    | 806        |
| 77.3      | 근 아이디얼과 힐베르트의 영점 정리 . . . . .                    | 807        |
| 77.4      | $\mathbb{A}^1$ 에서 대수다양체의 그림 . . . . .            | 808        |
| 77.5      | 소 아이디얼은 기약 아핀 다양체에 대응합니다 . . . . .               | 810        |
| 77.6      | $\mathbb{A}^2$ 와 $\mathbb{A}^3$ 에서의 그림 . . . . . | 810        |
| 77.7      | 극대 아이디얼 . . . . .                                | 811        |
| 77.8      | 비근호(non-radical) 아이디얼을 통해 스킴을 동기 부여하기 . . . . .  | 812        |
| 77.9      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                   | 813        |
| <br>      |                                                  |            |
| <b>78</b> | <b>환 달린 공간으로서의 아핀 다양체</b>                        | <b>815</b> |
| 78.1      | 개요 . . . . .                                     | 815        |
| 78.2      | $\mathbb{A}^n$ 위의 자리스키 위상 . . . . .              | 815        |
| 78.3      | 아핀 다양체 위의 자리스키 위상 . . . . .                      | 817        |
| 78.4      | 좌표환 . . . . .                                    | 818        |
| 78.5      | 정칙 함수의 층 . . . . .                               | 819        |
| 78.6      | 특수 열린집합 위의 정칙 함수 . . . . .                       | 821        |
| 78.7      | 베이비 환달린 공간 . . . . .                             | 822        |
| 78.8      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                   | 823        |
| <br>      |                                                  |            |
| <b>79</b> | <b>사영 다양체</b>                                    | <b>825</b> |
| 79.1      | 등급환 . . . . .                                    | 825        |
| 79.2      | 주변 공간 . . . . .                                  | 826        |
| 79.3      | 동차 아이디얼 . . . . .                                | 828        |
| 79.4      | 환달린 공간으로서 . . . . .                              | 829        |
| 79.5      | 정칙함수의 예시 . . . . .                               | 830        |
| 79.6      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                   | 832        |
| <br>      |                                                  |            |
| <b>80</b> | <b>보너스: 베주 정리(Bézout's theorem)</b>              | <b>833</b> |
| 80.1      | 근기가 아닌 아이디얼 . . . . .                            | 833        |
| 80.2      | 유한개 점들의 힐베르트 함수 . . . . .                        | 834        |
| 80.3      | 힐베르트 다항식 . . . . .                               | 836        |
| 80.4      | Bézout의 정리 . . . . .                             | 838        |
| 80.5      | 응용 . . . . .                                     | 839        |
| 80.6      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                   | 840        |
| <br>      |                                                  |            |
| <b>81</b> | <b>대수다양체의 사상</b>                                 | <b>843</b> |
| 81.1      | 초급 유유평간의 사상 정의하기 . . . . .                       | 843        |
| 81.2      | 가장 단순한 예시 분류 . . . . .                           | 844        |
| 81.3      | 몇 가지 추가 응용과 예시 . . . . .                         | 846        |
| 81.4      | 쌍곡선 효과 . . . . .                                 | 847        |
| 81.5      | 생각해 볼 만한 조금 더 어려운 문제 . . . . .                   | 849        |

---

# 77 아핀 다양체

이 장에서는 아핀 다양체를 소개합니다. 좌표의 맥락에서 이를 소개하지만, 다른 장들을 거치면서 이러한 관점에서 점차 벗어나, 다양체를 좌표에 매장된 것으로 보지 않고 “내재적 대상”으로 바라보게 될 것입니다.

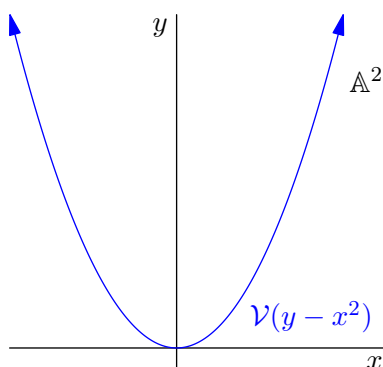
단순화를 위해 대부분의 논의를 복소수체 위에서 진행하지만, 이 논의는 임의의 대수적으로 닫힌 체로 일반화됩니다.

## §77.1 아핀 다양체

**이 절의 대표적인 예:**  $\mathcal{V}(y - x^2)$ 는  $\mathbb{A}^2$  안의 포물선입니다.

**정의 77.1.1.** 다항식들의 집합  $S \subseteq \mathbb{C}[x_1, \dots, x_n]$ 이 주어졌을 때(반드시 유한이거나 심지어 가산일 필요는 없습니다),  $\mathcal{V}(S)$ 가  $S$ 에 속한 모든 다항식 위에서 소멸하는 점들의 집합을 나타내도록 합시다. 이러한 집합을 **아핀 다양체**라고 부릅니다. 이는  $n$ 차원 **아핀 공간**(나중에 사영 공간과 구별하기 위해  $\mathbb{A}^n$ 으로 표기합니다) 안에 존재합니다.

예를 들어, 포물선은 다항식  $y - x^2$ 의 영점 궤적입니다. 그림:



### 예제 77.1.2 (아핀 다양체의 예)

이 예들은 점  $(x, y)$ 의 쌍으로 이루어진 2차원 공간  $\mathbb{A}^2$ 에 있습니다.

- (a) 직선은  $\mathcal{V}(Ax + By + C)$ 로 생각할 수 있습니다.
- (b) 위와 같은 포물선은  $\mathcal{V}(y - x^2)$ 로 그릴 수 있습니다.
- (c) 쌍곡선은  $\mathcal{V}(xy - 1)$ 일 수 있습니다.
- (d) 두 축은  $\mathcal{V}(xy)$ 로 생각할 수 있습니다. 이는  $x = 0$  또는  $y = 0$ 인 점들의 집합입니다.
- (e) 점  $(x_0, y_0)$ 은  $\mathcal{V}(x - x_0, y - y_0)$ 로 생각할 수 있습니다.
- (f) 공간 전체  $\mathbb{A}^2$ 는  $\mathcal{V}(0)$ 으로 생각할 수 있습니다.
- (g) 공집합은 상수 다항식 1의 영점 궤적, 즉  $\mathcal{V}(1)$ 입니다.

## §77.2 아이디얼을 통한 아핀 다양체의 명명

**이 절의 대표적인 예:**  $\mathcal{V}(I)$ 는 포물선이며, 여기서  $I = (y - x^2)$ 입니다.

이미 눈치채셨을 수도 있듯이, 다양체는  $\mathcal{V}(-)$ 를 통해 여러 방식으로 명명될 수 있습니다. 예를 들어, 다음의 해집합은

$$x = 3 \text{ 그리고 } y = 4$$

바로 점  $(3, 4)$ 입니다. 하지만 이는 다음의 해집합이기도 합니다

$$x = 3 \text{ 그리고 } y = x + 1.$$

그러므로, 예를 들어

$$\{(3, 4)\} = \mathcal{V}(x - 3, y - 4) = \mathcal{V}(x - 3, y - x - 1).$$

그것은 조금 성가신 일인데, 이상적인<sup>1</sup> 세계라면 모든 다양체에 대해 하나의 이름만 있어야 하기 때문입니다. 이를 달성할 수 있는지 살펴봅시다.

부분적인 해결책은 작은 집합 대신 아이디얼을 사용하는 것입니다. 즉, 다음의 아이디얼을 생각해봅시다

$$I = (x - 3, y - 4) = \{p(x, y) \cdot (x - 3) + q(x, y) \cdot (y - 4) \mid p, q \in \mathbb{C}[x, y]\}$$

그리고  $\mathcal{V}(I)$ 를 살펴봅시다.

**질문 77.2.1.**  $\mathcal{V}(I) = \{(3, 4)\}$ 임을 스스로 확인해 보십시오.

그러므로  $\mathcal{V}(x - 3, y - 4)$ 라고 쓰는 대신, 이를  $\mathcal{V}(I)$ 로 생각하는 것이 타당합니다. 여기서  $I = (x - 3, y - 4)$ 는 두 다항식  $x - 3$ 과  $y - 4$ 로 생성되는 아이디얼입니다. 이는 다음과 같은 이유로 개선된 표현입니다

**질문 77.2.2.**  $(x - 3, y - x - 1) = (x - 3, y - 4)$ 임을 확인하십시오.

두 말할 필요 없이, 이 패턴은 일반적으로 성립합니다.

**질문 77.2.3.**  $\{f_i\}$ 를 다항식들의 집합이라 하고, 이  $\{f_i\}$ 로 생성되는 아이디얼  $I$ 를 생각하십시오.  $\mathcal{V}(\{f_i\}) = \mathcal{V}(I)$ 임을 보이십시오.

따라서 우리는  $I$ 가 아이디얼일 때에만  $\mathcal{V}(I)$ 를 고려할 것입니다. 물론 우리의 아이디얼은 흔히 하나 또는 두 개의 다항식으로 생성되므로, 다음과 같은 표기법을 얻게 됩니다:

**표기의 남용 77.2.4.** 다항식들의 집합  $f_1, \dots, f_m$ 이 주어졌을 때,  $\mathcal{V}(f_1, \dots, f_m)$ 을  $\mathcal{V}((f_1, \dots, f_m))$ 의 축약형으로 두겠습니다. 다시 말해,  $\mathcal{V}(f_1, \dots, f_m)$ 은  $\mathcal{V}(I)$ 의 축약형이며, 여기서  $I$ 는 아이디얼  $I = (f_1, \dots, f_m)$ 입니다.

바로 이 지점에서 뇌터 조건이 진가를 발휘합니다: 이는 모든 아이디얼  $I \subseteq \mathbb{C}[x_1, \dots, x_n]$ 이 유한 개의 다항식으로 위와 같은 형태로 쓰일 수 있음을 보장하는데, 이는 그 아이디얼이 유한 생성이기 때문입니다. ( $\mathbb{C}[x_1, \dots, x_n]$ 이 뇌터 환이라는 사실은 힐베르트 기저 정리, 즉 **정리 4.9.5**로부터 따라옵니다.) 이는 다행스러운 일인데, 무한 개의 다항식 집합을 다루는 것은 그다지 즐거운 일이 아니기 때문입니다.

<sup>1</sup>말장난을 의도한 것은 아니지만 재미를 위해 남겨둡니다.

### §77.3 근 아이디얼과 힐베르트의 영점 정리

**이 절의 대표적인 예:**  $\mathbb{C}[x]$ 에서  $\sqrt{(x^2)} = (x)$ 이고,  $\mathbb{Z}$ 에서  $\sqrt{(12)} = (6)$ 입니다.

이제 이 이름이 유일한지 궁금할 수 있습니다: 즉,  $\mathcal{V}(I) = \mathcal{V}(J)$ 이면  $I = J$ 가 성립할까요? 안타깝게도 답은 그렇지 않습니다: 반례는 단지  $\mathbb{A}^1$ 에서도 찾을 수 있습니다. 그것은

$$\mathcal{V}(x) = \mathcal{V}(x^2).$$

다시 말해,  $x = 0$ 의 해집합은  $x^2 = 0$ 의 해집합과 같습니다.

흠, 이는 어리석습시다. 우리는 아이디얼  $(x^2)$ 을 받아서 아이디얼  $(x)$ 로 만들어 주는 연산을 원합니다. 이를 수행하는 방법은 아이디얼의 근을 이용하는 것입니다.

**정의 77.3.1.**  $R$ 을 환이라 하십시오. 아이디얼  $I \subseteq R$ 의 **근**은  $\sqrt{I}$ 로 표기하며, 다음과 같이 정의됩니다

$$\sqrt{I} = \{r \in R \mid r^m \in I \text{ 어떤 정수 } m \geq 1 \text{에 대해}\}.$$

$I = \sqrt{I}$ 이면, 아이디얼  $I$  자체가 **근 아이디얼**이라고 말합니다.

예를 들어,  $\sqrt{(x^2)} = (x)$ 입니다.  $\sqrt{I}$ 가 실제로 아이디얼임을 확인해 보는 시간을 가져 보아도 좋습니다.

**비고 77.3.2 (수론적 동기)** — 이는 사실 정수론에서의 "근"이라는 개념과 동일합니다.  $\mathbb{Z}$ 에서 아이디얼  $(n)$ 의 근은 중복된 소인수들을 모두 제거하는 것에 해당하며, 예를 들면

$$\sqrt{(12)} = (6).$$

특히,  $\sqrt{(6)}$ 을 구해 보려 하면, 그냥  $(6)$ 을 다시 얻을 뿐입니다; 새로운 소인수를 짜낼 수는 없습니다.

이는 사실 더 일반적으로 성립하며, 이에 대응하는 멋진 대안적 정의가 있습니다: 임의의 아이디얼  $I$ 에 대해, 다음이 성립합니다

$$\sqrt{I} = \bigcap_{I \subseteq \mathfrak{p} \text{ 소}} \mathfrak{p}.$$

지금 이를 증명할 수도 있겠지만, 이는 나중에 처음 필요할 때 **정리 84.5.2**에서 증명될 것입니다.

알아 두어야 할 즉각적인 성질들은 다음과 같습니다.

#### 명제 77.3.3 (근의 성질)

임의의 환에서:

- $I$ 가 아이디얼이면,  $\sqrt{I}$ 는 항상 근 아이디얼입니다.
- 소 아이디얼은 근기 아이디얼입니다.
- $I \subseteq \mathbb{C}[x_1, \dots, x_n]$ 에 대해  $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$ 가 성립합니다.

증명. 이는 모두 자명합니다.

- $f^m \in \sqrt{I}$ 이면  $f^{mn} \in I$ 이므로,  $f \in \sqrt{I}$ 입니다.
- 소 아이디얼  $\mathfrak{p}$ 에 대해  $f^n \in \mathfrak{p}$ 이면,  $f \in \mathfrak{p}$ 이거나  $f^{n-1} \in \mathfrak{p}$ 이며, 후자의 경우 귀납법으로 계속 진행할 수 있습니다.

- $f(x_1, \dots, x_n) = 0$ 인 것과 어떤 정수  $m$ 에 대해  $f(x_1, \dots, x_n)^m = 0$ 인 것은 동치입니다.  $\square$

마지막 부분은 이치에 맞습니다:  $x = 0$ 을  $x^2 = 0$ 이라고 부르는 일은 결코 없을 것이며, 따라서  $\mathcal{V}(x^2)$ 를 그냥  $\mathcal{V}(x)$ 라고 부르고 싶어질 것입니다. 이로써 힐베르트 영점 정리(Hilbert's Nullstellensatz)라는 정리를 얻게 됩니다.

### 정리 77.3.4 (힐베르트 영점 정리)

아핀 대수다양체  $V = \mathcal{V}(I)$ 가 주어졌을 때,  $V$ 의 모든 점에서 소멸하는 다항식들의 집합은 정확히  $\sqrt{I}$ 입니다. 따라서  $I$ 와  $J$ 가  $\mathbb{C}[x_1, \dots, x_n]$ 의 아이디얼이라면,

$$\mathcal{V}(I) = \mathcal{V}(J)\sqrt{I} = \sqrt{J}\text{일 필요충분조건.}$$

다시 말해

$\mathbb{C}[x_1, \dots, x_n]$ 의 근기 아이디얼들은  $n$ 차원 아핀 대수다양체들과 정확히 대응됩니다.

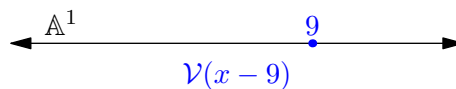
힐베르트 영점 정리의 증명은 [문제 77D](#)에서 다룰 것입니다; 지금으로서는 이 정리가 본질적으로  $\mathbb{C}$ 가 대수적으로 닫혀 있다는 사실에 의존한다는 점을 짚어둘 만합니다. 예를 들어, 이는  $\mathbb{R}[x]$ 에서는 성립하지 않으며,  $(x^2 + 1)$ 이 소멸 집합이 공집합인 극대 아이디얼이 되는 경우가 그렇습니다.

## §77.4 $\mathbb{A}^1$ 에서 대수다양체의 그림

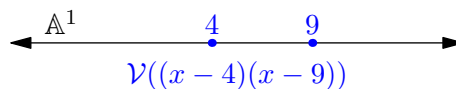
**이 절의 대표적인 예:** 점들의 유한 집합 (사실 이것이 유일한 자명하지 않은 예시입니다).

먼저 몇 가지 그림을 그려봅시다. 이어지는 내용에서는  $\mathbb{C}$ 를 직선으로 그리겠습니다... 죄송합니다.

우선, 복소직선  $\mathbb{A}^1$ 만을 살펴봅시다. 그 위에는 어떤 다양한 대수다양체들이 있을까요? 우선,  $(x - 9)$ 로 생성되는 단일 점  $9 \in \mathbb{C}$ 가 있습니다.



또 다른 예로는 점 4가 있습니다. 그리고 실제로, 원한다면 이 두 점만으로 이루어진 아이디얼을 얻을 수 있습니다;  $\mathcal{V}((x - 4)(x - 9))$ 를 생각해 봅시다.



일반적으로  $\mathbb{A}^1$ 에서는 단지

$$\mathcal{V}((x - a_1)(x - a_2) \dots (x - a_n)).$$

를 취함으로써 유한한 점들의 집합  $\{a_1, \dots, a_n\}$ 을 얻을 수 있습니다. 반면, 집합  $\{0, 1, 2, \dots\}$ 는 아핀 대수다양체로 얻을 수 없습니다. 이 점들 모두에서 소멸하는 유일한 다항식은 영다항식뿐입니다. 실제로, 두 가지 예외를 제외하면 이것들이 유일한 아핀 대수다양체임을 스스로 확인할 수 있습니다.

- 직선 전체  $\mathbb{A}^1$ 은  $\mathcal{V}(0)$ 으로 주어지며,
- 공집합은  $\mathcal{V}(1)$ 으로 주어집니다.

**연습문제 77.4.1.** 이것들이  $\mathbb{A}^1$ 의 유일한 대수다양체임을 보이십시오. ( $\mathcal{V}(I)$ 를 그 대수다양체라 하고  $0 \neq f \in I$ 를 하나 택하십시오.)

짐작하시는 대로, 다음이 성립합니다:

**정리 77.4.2 (대수다양체의 교집합과 합집합)**

(a) 아핀 대수다양체들의 교집합은 (무한히 많더라도) 아핀 대수다양체입니다.

(b) 유한 개의 아핀 다양체의 합집합은 아핀 다양체입니다.

실제로 다음이 성립합니다.

$$\bigcap_{\alpha} \mathcal{V}(I_{\alpha}) = \mathcal{V}\left(\sum_{\alpha} I_{\alpha}\right) \quad \text{그리고} \quad \bigcup_{k=1}^n \mathcal{V}(I_k) = \mathcal{V}\left(\bigcap_{k=1}^n I_k\right).$$

이 쉬운 결과는 여러분이 직접 증명해 보시기 바랍니다.

**비고 77.4.3 —** (a) 부분은 합  $I + J$ 가 근기 아이디얼일 필요가 없다는 점에서 약간 오해의 소지가 있습니다: 예를 들어  $\mathbb{C}[x, y]$ 에서  $I = (y - x^2)$ 이고  $J = (y)$ 인 경우,  $x \in \sqrt{I + J}$ 이지만  $x \notin I + J$ 입니다. 하지만 (b) 부분에서는 근기 아이디얼  $I$ 와  $J$ 에 대해 교집합  $I \cap J$ 가 근기 아이디얼입니다.

아이디얼과 다양체 사이의 관계에 관한 또 다른 쉬운 결과로, 다음이 있습니다.

**명제 77.4.4 ( $\mathcal{V}(-)$ 는 포함관계를 뒤집는다)**

$I \subseteq J$ 이면  $\mathcal{V}(I) \supseteq \mathcal{V}(J)$ 입니다. 따라서  $\mathcal{V}(-)$ 는 포함관계를 뒤집습니다.

**질문 77.4.5.** 이를 확인해 보십시오.

따라서 더 큰 아이디얼은 더 작은 다양체에 대응합니다.

이 결과들은 이 장 전반에 걸쳐 많이 사용될 것이므로,  $\mathcal{V}$ 가 포함관계를 뒤집는 성질에 익숙해지는 것이 유용할 것입니다.

**연습문제 77.4.6.** 개념에 좀 더 익숙해지는 데 도움이 되는 간단한 연습문제입니다.

1.  $I = (y - x^2)$ 이고  $J = (x + 1, y + 2)$ 라 합시다.  $\mathcal{V}(I)$ 와  $\mathcal{V}(J)$ 는 무엇입니까?
2.  $\mathcal{V}(K)$ 가 포물선  $y = x^2$ 과 점  $(-1, -2)$ 의 합집합이 되는 아이디얼  $K$ 는 무엇입니까?
3.  $L = (y - 1)$ 이라 합시다.  $\mathcal{V}(L)$ 은 무엇입니까?
4. 교집합  $\mathcal{V}(I) \cap \mathcal{V}(L)$ 은 두 점  $(1, 1)$ 과  $(-1, 1)$ 로 이루어져 있습니다. 이에 대응하는 아이디얼을  $I$ 와  $L$ 로 나타내면 무엇입니까?
5.  $\mathcal{V}(I \cap L)$ 은 무엇입니까?  $\mathcal{V}(IL)$ 은 어떻습니까?

**질문 77.4.7.** 무한히 많은 아이디얼의 교집합은 여전히 아이디얼이지만, 무한히 많은 아핀 다양체의 합집합은 아핀 다양체가 아닐 수 있음에 유의하십시오.

$\mathbb{C}[x]$ 에서  $I_k = (x - k)$ 를 생각하고, 무한 교집합  $I = \bigcap_{k \in \mathbb{N}} I_k$ 를 취합시다.  $\mathcal{V}(I)$ 와  $\bigcup_{k \in \mathbb{N}} \mathcal{V}(I_k)$ 는 무엇입니까?

## §77.5 소 아이디얼은 기약 아핀 다양체에 대응합니다

**이 절의 대표적인 예:**  $(xy)$ 는  $\mathbb{A}^2$ 에서 두 직선의 합집합에 대응합니다.

$\mathbb{A}^1$ 의 아핀 다양체 대부분은, 예컨대  $\{4, 9\}$ 처럼, 가장 단순한 ”한 점” 아이디얼들의 합집합에 불과함에 유의하십시오. 분류를 쉽게 하기 위해, 기약 다양체의 경우로 관심을 제한할 수 있습니다.

**정의 77.5.1.** 다양체  $V$ 는 두 개의 진부분다양체의 합집합  $V = V_1 \cup V_2$ 로 쓸 수 없을 때 **기약**이라고 합니다.

**표기의 남용 77.5.2.** 주의: 다른 문헌에서는 기약성이 다양체의 정의의 일부입니다.

### 예제 77.5.3 ( $\mathbb{A}^1$ 의 기약 다양체)

$\mathbb{A}^1$ 의 기약 다양체는 다음과 같습니다.

- 공집합  $\mathcal{V}(1)$ ,
- 한 점  $\mathcal{V}(x - a)$ , 그리고
- 전체 직선  $\mathbb{A}^1 = \mathcal{V}(0)$ 입니다.

### 예제 77.5.4 (두 축의 합집합)

$\mathbb{C}[x, y]$ 에서 소 아이디얼이 아닌 것을 하나 생각해 봅시다. 예를 들어  $I = (xy)$ 입니다. 이것의 소멸 집합  $\mathcal{V}(I)$ 는 두 직선  $x = 0$ 과  $y = 0$ 의 합집합입니다. 따라서  $\mathcal{V}(I)$ 는 가약입니다.

일반적으로 다음이 성립합니다.

### 정리 77.5.5 (소 아이디얼 $\iff$ 기약)

$I$ 를 근기 아이디얼이라 하고,  $V = \mathcal{V}(I)$ 를 공집합이 아닌 대수다양체라 합시다. 그러면  $I$ 가 소 아이디얼인 것과  $V$ 가 기약인 것은 동치입니다.

**증명.** 먼저  $V$ 가 기약이라고 가정하고,  $I$ 가 소 아이디얼임을 보이겠습니다.  $f, g \in \mathbb{C}[x_1, \dots, x_n]$ 이고  $fg \in I$ 라고 합시다. 그러면  $V$ 는 합집합  $\mathcal{V}(f) \cup \mathcal{V}(g)$ 의 부분집합입니다. 실제로  $V = (V \cap \mathcal{V}(f)) \cup (V \cap \mathcal{V}(g))$ 입니다.  $V$ 가 기약이므로  $V = V \cap \mathcal{V}(f)$ 라고 가정할 수 있으며, 따라서  $f$ 는  $V$  전체에서 소멸합니다. 그러므로  $f \in I$ 입니다.

역방향도 마찬가지로입니다. □

## §77.6 $\mathbb{A}^2$ 와 $\mathbb{A}^3$ 에서의 그림

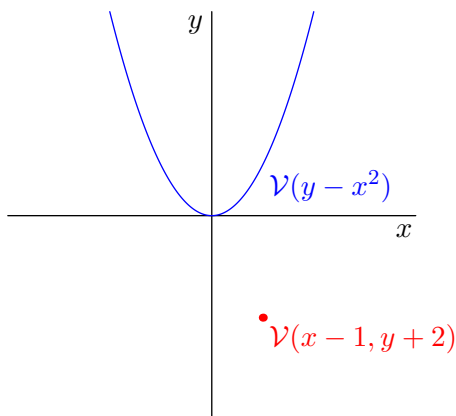
**이 절의 대표적인 예:** 다양한 곡선과 초곡면.

이 개념을 이용하면 이제 ”복소 아핀 평면”  $\mathbb{A}^2$ 에서 그림을 그릴 수 있습니다. 이 안의 기약 아핀 대수다양체는 무엇일까요?

앞선 논의에서 보았듯이,  $\mathbb{A}^2$ 에서 기약 아핀 대수다양체의 이름을 붙이는 것은  $\mathbb{C}[x, y]$ 의 소 아이디얼들의 이름을 붙이는 것과 같습니다. 다음은 몇 가지 예입니다.

- 아이디얼  $(0)$ 은 소 아이디얼입니다.  $\mathcal{V}(0)$ 은 늘 그렇듯이 평면 전체에 대응됩니다.
- 아이디얼  $(x - a, y - b)$ 는 소 아이디얼입니다. 왜냐하면  $\mathbb{C}[x, y]/(x - a, y - b) \cong \mathbb{C}$ 는 정역이기 때문입니다. (사실  $\mathbb{C}$ 가 체이므로, 아이디얼  $(x - a, y - b)$ 는 극대입니다.) 이것의 소멸 집합은  $\mathcal{V}(x - a, y - b) = \{(a, b)\} \in \mathbb{C}^2$ 이며, 따라서 이러한 아이디얼들은 한 점에 대응됩니다.
- $f(x, y)$ 를  $y - x^2$ 와 같은 기약 다항식이라고 합시다. 그러면  $(f)$ 는 소 아이디얼입니다! 여기서  $\mathcal{V}(I)$ 는 "여차원 1의 곡선"입니다.

약간의 다항식 대수학을 이용하면(이번에도 유클리드 호제법으로 직접 확인해 보셔도 좋습니다), 이것들이 사실  $\mathbb{C}[x, y]$ 의 유일한 소 아이디얼들입니다. 다음은 그림입니다.



늘 그렇듯이, 이러한 기약 대수다양체들의 합집합으로 이루어진 대수다양체를 만들 수 있습니다. 예를 들어 포물선  $y = x^2$ 와 점  $(20, 15)$ 로 이루어진 대수다양체를 원한다면 다음과 같이 쓰면 됩니다.

$$\mathcal{V}\left((y - x^2)(x - 20), (y - x^2)(y - 15)\right).$$

$\mathbb{A}^3$ 에서의 그림은 설명하기가 더 어렵습니다. 여기서도 영차원 점  $(a, b, c)$ 에 대응되는 점  $\mathcal{V}(x - a, y - b, z - c)$ 와, 각 기약 다항식  $f$ 에 대한 일차원 곡면  $\mathcal{V}(f)$ 가 있습니다(예를 들어  $x + y + z = 0$ 은 평면입니다). 하지만  $\mathcal{V}(x, y)$ 와 같이 더 많은 소 아이디얼들이 있는데, 이는 평면  $x = 0$ 과  $y = 0$ 의 교집합에 대응됩니다. 즉 일차원  $z$ 축입니다. "일차원" 대수다양체를 분류하는 합리적인 방법은 없다는 것이 밝혀졌습니다. 이들은 "기약 곡선"에 대응됩니다.

따라서 Ravi Vakil [Va17]이 말했듯이,  $\mathbb{C}[x, y, z]$ 의 소 아이디얼을 결정하는 순수하게 대수적인 질문은 근본적으로 기하학적인 답을 가지고 있습니다.

## §77.7 극대 아이디얼

**이 절의 대표적인 예:** 모든 극대 아이디얼은  $(x_1 - a_1, \dots, x_n - a_n)$  형태입니다.

더 큰 아이디얼은 더 작은 대수다양체에 대응된다는 것을 기억하십시오.

위 그림들이 시사했듯이, 가장 작은 대수다양체는 한 점입니다. 게다가 이름에서 짐작할 수 있듯이, 가장 큰 아이디얼은 극대 아이디얼입니다. 예를 들어, 다음과 같은 형태의 모든 아이디얼은

$$(x_1 - a_1, \dots, x_n - a_n)$$

몫이 다음과 같으므로 극대입니다.

$$\mathbb{C}[x_1, \dots, x_n]/(x_1 - a_1, \dots, x_n - a_n) \cong \mathbb{C}$$

체(field)입니다. 문제는: 모든 극대 아이디얼이 이런 형태인가 하는 것입니다.  
답은 그렇다입니다.

### 정리 77.7.1 (약한 영점 정리, 극대 아이디얼로 표현한 버전)

$\mathbb{C}[x_1, \dots, x_n]$ 의 모든 극대 아이디얼은  $(x_1 - a_1, \dots, x_n - a_n)$  형태입니다.

이 증명은 놀랍도록 자명하지 않으므로 아직 여기서는 다루지 않겠습니다. [Va17, §7.4.3]을 참고하십시오. 이 역시  $\mathbb{C}$ 가 대수적으로 닫혀 있다는 사실을 사용합니다. (예를 들어  $(x^2 + 1)$ 은  $\mathbb{R}[x]$ 의 극대 아이디얼입니다.) 따라서:

$\mathbb{C}$  위에서, 극대 아이디얼은 하나의 점에 대응됩니다.

따라서  $\mathbb{C}$  위의 여러 아이디얼들은 다양한 종류의 아핀 다양체에 대응됩니다:

| 대수적 성격   | 기하적 성격   |
|----------|----------|
| 근 아이디얼   | 아핀 대수다양체 |
| 소 아이디얼   | 기약 다양체   |
| 극대 아이디얼  | 한 점      |
| 임의의 아이디얼 | (스킴?)    |

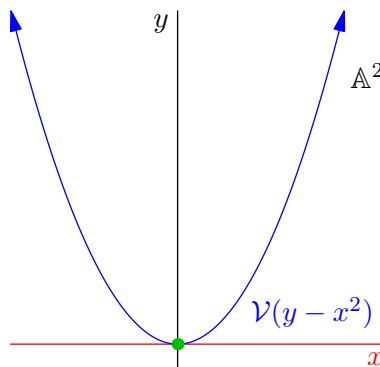
아직 이야기하지 않은 것이 하나 있습니다: 마지막 항목은 무엇일까요?

## §77.8 비근호(non-radical) 아이디얼을 통해 스킴을 동기 부여하기

스킴의 가장 기본적인 동기 중 하나는 중복도(multiplicity)를 셀 수 있도록 스킴을 사용하고자 한다는 것입니다. 즉, 다음 교집합을 생각해 봅시다

$$\mathcal{V}(y - x^2) \cap \mathcal{V}(y) \subseteq \mathbb{A}^2$$

이것은 포물선과 접하는  $x$ 축의 교집합이며, 아래 그림의 초록색 점입니다.



안타깝게도 다양체로서는 그냥 한 점일 뿐입니다! 하지만 우리는 이것을 어떤 의미에서 중복도가 2이므로 "이중점(double point)"으로 생각하고자 합니다. 이는 아이디얼을 살펴보면 확인할 수 있습니다:

$$(y - x^2) + (y) = (x^2, y)$$

그리고 근호를 취하는 것을 대충 무시한다면, 다음을 얻습니다

$$\mathbb{C}[x, y]/(x^2, y) \cong \mathbb{C}[\varepsilon]/(\varepsilon^2).$$

따라서 문제의 아이디얼들은 이중점의 존재를 알아채고 있는 것입니다.

이를 포착하기 위해서는 다양체보다 더 정교한 대상이 필요합니다. 다양체는 결국 그저 점들의 집합일 뿐이며, 위상만으로는 더 많은 정보를 담을 수 없습니다(한 점 위에는 오직 하나의 위상만 존재하기 때문입니다!). 이 정교한 대상이 바로 스킴입니다.

## §77.9 생각해 볼 만한 조금 더 어려운 문제

여기에는 실제 계산을 좀 있으면 좋겠습니다

**문제 77A.** 두 아이디얼  $I$ 와  $J$ 에 대해,  $I \subseteq \sqrt{I}$ 이고  $\sqrt{I} \cap \sqrt{J} = \sqrt{IJ} \subseteq \sqrt{I \cap J}$ 임을 보이십시오.

**문제 77B.** 실(real) 아핀 다양체  $V \subseteq \mathbb{A}_{\mathbb{R}}^n$ 은 항상  $\mathcal{V}(f)$  형태로 쓸 수 있음을 보이십시오.

**문제 77C** (복소 다양체는 공집합일 수 없습니다).  $I$ 가  $\mathbb{C}[x_1, \dots, x_n]$ 의 진 아이디얼이면  $\mathcal{V}(I) \neq \emptyset$ 임을 증명하십시오.



**문제 77D.**  $n$ 차원에서의 힐베르트 영점정리(Hilbert's Nullstellensatz)가 약한 영점정리(Weak Nullstellensatz)로부터 따라 나옴을 보이십시오. (이 풀이는 **라비노비치 트릭**이라고 불립니다.)



# 78 환 달린 공간으로서의 아핀 다양체

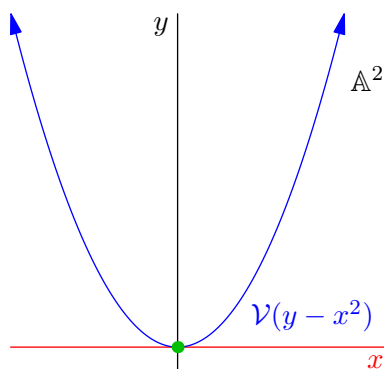
앞 장에서와 마찬가지로, 간단함을 위해  $\mathbb{C}$  위의 아핀 다양체만을 다루겠습니다.

## §78.1 개요

19세기 초 군론은 기이한 존재였습니다. 19세기 동안 군은 문자 그대로  $GL(n)$  또는  $S_n$ 의 부분집합으로 정의되었습니다. 실제로 “군”이라는 단어는 아직 발명되지 않았습니다. 이는 터무니없게 들릴 수 있지만 사실이었습니다 – Sylow는 이 개념 없이 자신의 정리들을 전개했습니다. 훨씬 나중에야 비로소 군의 추상적 정의, 즉  $S_n$ 으로의 어떠한 매장으로부터도 독립적인 추상 집합  $G$ 이자 그 자체로 하나의 대상이라는 정의가 주어졌습니다.

우리는 이제 아핀 다양체에 대해서도 같은 종류의 변화를 이루려고 합니다. 이를 주변 공간  $\mathbb{A}^n$  안에 갇힌 대상으로 생각하는 대신, 우리는 그것을 그 자체로 하나의 대상으로 만들고자 합니다. 구체적으로, 우리에게 아핀 다양체는 각 열린집합마다 함수의 환을 갖춘 위상 공간이 될 것입니다. 이것이 바로 우리가 이를 **환 달린 공간**이라 부르는 이유입니다.

위상 공간에 관한 부분은 그리 과격하지 않습니다. 핵심적인 통찰은 함수의 환을 추가하는 것입니다. 예를 들어, 지난 장의 이중점을 생각해 봅시다.



집합으로서 그것은 하나의 점이며, 따라서 가능한 위상은 오직 하나뿐입니다. 그러나 함수 환을 추가하면 이를 단순한 하나의 점과 구별할 수 있게 해 줍니다.

이 구성은 상당히 복잡하므로, 다음과 같이 진행하겠습니다:  $\mathbb{A}^n$  안의 기존 아핀 다양체 위에 구조를 하나씩 정의해 나가서, 환 달린 공간의 모든 데이터를 갖출 때까지 진행하겠습니다. 이후의 장들에서는 이러한 개념들이 자라나 현대 대수기하학의 핵심, 즉 스킴이 될 것입니다.

## §78.2 $\mathbb{A}^n$ 위의 자리스키 위상

**이 절의 대표적인 예:**  $\mathbb{A}^1$ 에서 닫힌집합은 유한 개의 점들의 모임입니다.  $\mathbb{A}^2$ 에서 공집합이 아닌 열린집합은 전체 공간에서 곡선/점들의 유한 모임을 뺀 것입니다.

먼저 모든 다양체  $V$ 에 위상 구조를 부여하는 것으로 시작합니다. (지금까지는) 아핀 다양체가 모두  $\mathbb{A}^n$  안에 있으므로,  $\mathbb{A}^n$ 에 적절한 위상을 주고 나서  $V$ 를 부분공간으로 보기만 하면 됩니다.

그러나  $\mathbb{A}^n$ 에 표준적인 유클리드 위상을 부여하는 대신, 우리는 훨씬 더 기이한 위상을 부여합니다.

**정의 78.2.1.**  $\mathbb{A}^n$  위의 **자리스키 위상**에서, 닫힌집합은 다음과 같은 형태의 집합들입니다

$$\mathcal{V}(I) \quad \text{여기서 } I \subseteq \mathbb{C}[x_1, \dots, x_n].$$

물론 열린집합은 이러한 집합들의 여집합입니다.

**예제 78.2.2** ( $\mathbb{A}^1$  위의 자리스키 위상)

$\mathbb{A}^1$ 의 열린집합을 결정해 봅시다.  $\mathbb{A}^1$ 은 평소와 같이 ( $\mathbb{C}$ 가 이차원이라는 사실을 무시하고) 직선으로 그려 보겠습니다.

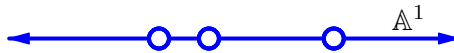
$\mathbb{C}[x]$ 는 주 아이디얼 정역이므로, 모든  $I \subseteq \mathbb{C}[x]$ 에 대해  $\mathcal{V}(I)$ 를 살펴보는 대신, 단 하나의  $f$ 에 대한  $\mathcal{V}(f)$ 만 살펴보면 됩니다. 다항식  $f$ 에는 몇 가지 유형이 있습니다:

- 어디서나 소멸하는 영다항식 0: 이는 전체 공간  $\mathbb{A}^1$ 이 닫힌집합임을 의미합니다.
- 어디서도 소멸하지 않는 상수다항식 1: 이는  $\emptyset$ 이 닫힌집합임을 의미합니다.
- 차수  $n$ 인 다항식  $c(x - t_1)(x - t_2) \dots (x - t_n)$ . 이는  $n$ 개의 근을 가지므로,  $\{t_1, \dots, t_n\}$ 은 닫힌집합입니다.

따라서  $\mathbb{A}^1$ 의 닫힌집합은 정확히  $\mathbb{A}^1$  전체와 점들의 유한 집합들(공집합  $\emptyset$ 을 포함하여)입니다. 결과적으로,  $\mathbb{A}^1$ 의 열린집합은

- $\emptyset$ , 그리고
- 점들의 유한한 모임(공집합일 수도 있음)을 뺀  $\mathbb{A}^1$ 입니다.

따라서,  $\mathbb{A}^1$ 의 “전형적인” 열린집합의 그림은 다음과 같을 수 있습니다



몇 개의 표시된 점들을 제외한 모든 것입니다!

**예제 78.2.3** ( $\mathbb{A}^2$  위의 자리스키 위상)

마찬가지로,  $\mathbb{A}^2$ 에서 흥미로운 닫힌집합은 다음의 유한 합집합(공집합일 수도 있음)으로 이루어집니다.

- $\mathcal{V}(y - x^2)$ (포물선)과 같은 닫힌 곡선, 그리고
- $\mathcal{V}(x - 3, y - 4)$ (점  $(3, 4)$ )와 같은 단일 점.

물론 전체 공간  $\mathbb{A}^2 = \mathcal{V}(0)$ 와 공집합  $\emptyset = \mathcal{V}(1)$ 도 닫힌집합입니다.

따라서  $\mathbb{A}^2$ 에서 공집합이 아닌 열린집합은 유한한 점들의 모임과 일차원 곡선들을 제외한 전체 평면으로 이루어집니다.

**질문 78.2.4.**  $\mathbb{A}^2$ 에서 “전형적인” 열린집합의 그림을 (본인의 그림 실력이 닿는 한) 그려보십시오.

이 모든 것이 말하고자 하는 바는

**공집합이 아닌 자리스키 열린집합은 거대하다는 것입니다.**

이는 여러분이 위상수학에서 익숙해져 있던 것과 중요한 차이점입니다. 아주 명확히 말하자면:

- 과거에 제가 "점  $p$ 의 열린 근방에서 이러저러한 성질을 가진다"와 같은 말을 했다면, 이는 " $p$  주변의 작은 영역에서 참이다"라는 뜻으로 여겨졌을 것입니다.
- 자리스키 위상에서는, "점  $p$ 의 열린 근방에서 이러저러한 성질을 가진다"는 말을 "특정 곡선 위의 점들을 제외한 사실상 모든 점에서 참이다"라는 뜻으로 이해해야 합니다.

실제로 "열린 근방"이라는 표현은 더 이상 정확한 서술이 아닙니다. 그럼에도 불구하고, 앞으로 나올 여러 그림에서는 열린 근방을 원으로 그리는 것이 여전히 도움이 될 것입니다.

이제 제가 서술한 대로 닫힌집합들이 실제로 위상을 이룬다는 것을 확인하는 일이 남아 있습니다. 즉, 다음을 간단히 확인해야 합니다.

- $\emptyset$ 과  $\mathbb{A}^n$ 은 둘 다 닫힌집합입니다.
- 닫힌집합들의 교집합은 (무한 교집합이라도) 여전히 닫힌집합입니다.
- 닫힌집합들의 유한 합집합은 여전히 닫힌집합입니다.

사실 닫힌집합은 아핀 다양체와 같은 것이므로, 우리는 이미 이를 알고 있습니다!

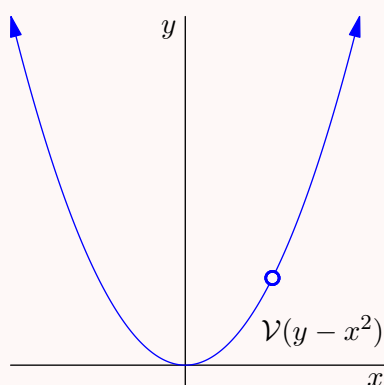
### §78.3 아핀 다양체 위의 자리스키 위상

**이 절의 대표적인 예:**  $V = \mathcal{V}(y - x^2)$ 가 포물선이라면,  $V$ 에서  $(1, 1)$ 을 뺀 것은  $V$ 에서 열려 있습니다. 또한, 평면에서 원점을 뺀 것은  $D(x) \cup D(y)$ 입니다.

앞서 말했듯이, 다양체  $V$ 를  $\mathbb{A}^n$ 의 부분공간으로 간주함으로써  $V$ 는 자리스키 위상을 물려받습니다.  $V$ 의 열린 부분집합은 " $V$ 에서 자리스키 닫힌집합 몇 개를 뺀 것"으로 생각해야 합니다. 예를 들어:

#### 예제 78.3.1 (다양체의 열린집합)

$V = \mathcal{V}(y - x^2) \subseteq \mathbb{A}^2$ 를 포물선이라 하고,  $U = V \setminus \{(1, 1)\}$ 라 합시다. 우리는  $U$ 가  $V$ 에서 열린집합임을 주장합니다.



실제로  $\tilde{U} = \mathbb{A}^2 \setminus \{(1, 1)\}$ 은  $\mathbb{A}^2$ 에서 열린집합이므로(이는 닫힌집합  $\mathcal{V}(x - 1, y - 1)$ 의 여집합이기 때문입니다),  $U = \tilde{U} \cap V$ 는  $V$ 에서 열린집합입니다. 한편 집합  $U$ 는  $\mathbb{A}^2$ 에서는 열린집합이 아님에 유의하십시오.

이제 나중에 매우 유용하게 쓰일 정의를 하나 소개하겠습니다.

**정의 78.3.2.** 아핀 다양체  $V \subseteq \mathbb{A}^n$ 과  $f \in \mathbb{C}[x_1, \dots, x_n]$ 가 주어졌을 때, **판별 열린집합** (distinguished open set)  $D(f)$ 를  $f$ 에서 소멸하지 않는 점들로 이루어진  $V$ 의 열린집합으로 정의합니다:

$$D(f) = \{p \in V \mid f(p) \neq 0\} = V \setminus \mathcal{V}(f).$$

[Va17]에서 Vakil은 표기  $D(f)$ 를 "소멸하지-않는 집합(doesn't-vanish set)"으로 기억할 것을 제안합니다.

**예제 78.3.3 (판별 열린집합의 (합집합) 예시)**

- (a)  $V = \mathbb{A}^1$ 이면  $D(x)$ 는 한 점을 제외한 직선에 대응됩니다.
- (b)  $V = \mathcal{V}(y - x^2) \subseteq \mathbb{A}^2$ 이면,  $D(x - 1)$ 은  $(1, 1)$ 을 제외한 포물선에 대응됩니다.
- (c)  $V = \mathbb{A}^2$ 이면,  $D(x) \cup D(y) = \mathbb{A}^2 \setminus \{(0, 0)\}$ 는 구멍 뚫린 평면입니다. 이 집합이 판별 열린집합이 아님을 보일 수 있습니다.

이 개념을 주 아이디얼(principal ideal)의 유사물로 생각할 수 있습니다: 모든 열린집합은 어떤 아이디얼  $I$ 에 대해  $V \setminus \mathcal{V}(I)$  형태로 쓸 수 있지만,  $I = (f)$ 가 주 아이디얼이라면 그 집합은 판별 열린집합  $D(f)$ 로 쓸 수 있습니다. 마찬가지로, 두 주 아이디얼의 곱(교집합이 아닙니다!)이 주 아이디얼인 것처럼, 두 판별 열린집합의 교집합도 판별 열린집합입니다.

**명제 78.3.4 (판별 열린집합의 성질)**

$\mathcal{V}$ 가 포함관계를 뒤집는다는 점을 상기하면,  $\mathcal{V}$ 의 여집합이라는 점에서  $D$ 는 "포함관계를 보존"할 것으로 기대됩니다. 실제로 그렇습니다:

- $(f) \subseteq (g)$  (즉,  $g \mid f$ )이면,  $D(f) \subseteq D(g)$ 입니다.
- $(fg) \subseteq (f) \cap (g)$ 임을 상기하십시오. 판별 열린집합에 대해서는  $D(fg) = D(f) \cap D(g)$ 가 성립합니다.

$D$ 의 거동에 익숙해지는 것이 유용합니다.

**질문 78.3.5.**  $V = \mathcal{A}^2$ 이면,  $D(x)$ 는  $y$ 축을 제외한 평면이고,  $D(y)$ 는  $x$ 축을 제외한 평면입니다.  $D(xy)$ 는 무엇이겠습니까?

## §78.4 좌표환

**이 절의 대표적인 예:**  $V = \mathcal{V}(y - x^2)$ 이면  $\mathbb{C}[V] = \mathbb{C}[x, y]/(y - x^2)$ 입니다.

다음으로 할 일은  $V$ 에서 기저체  $\mathbb{C}$ 로 가는 함수들을 살펴보는 것입니다. 우리는 다양체  $V$  위의 대수적(다항) 함수로 관심을 제한합니다: 이 함수들은  $V$  위의 모든 점  $(a_1, \dots, a_n)$ 을 어떤 복소수  $P(a_1, \dots, a_n) \in \mathbb{C}$ 로 보내야 합니다. 예를 들어, 3차원 아핀 다양체 위의 유효한 함수로는  $(a, b, c) \mapsto a$ 가 있을 수 있는데, 이 사영을 그냥 " $x$ "라고 부릅니다. 마찬가지로 표준적인 사영  $y$ 와  $z$ 도 있으며, 이들을 조합하여 다항식을 만들 수 있습니다, 예컨대  $x^2y + 2xyz$ 처럼 말입니다.

**정의 78.4.1.** 다양체  $V$ 의 **좌표환**(coordinate ring)  $\mathbb{C}[V]$ 는  $V$  위의 다항 함수들의 환입니다. (표기법은 다음 절에서 설명합니다.)

**비고 78.4.2** ("좌표환"이라는 이름의 의미) — 위의 함수  $x, y, z$ 를 **좌표 함수**(coordinate functions)라고 부르는데, 이는 이들이 다양체  $V$ 의 각 점을 그 좌표로 보내기 때문입니다. 따라서 좌표환  $\mathbb{C}[V]$ 는 단순히  $\mathbb{C}$ 와 좌표 함수들에 의해 생성되는 환입니다.

언뜻 보면 이것이 그냥  $\mathbb{C}[x_1, \dots, x_n]$ 이라고 생각할 수도 있습니다. 하지만 자세히 살펴보면 주어진 다양체 위에서는 이 함수들 중 일부가 서로 같다는 것을 깨닫게 됩니다. 예를 들어,  $\mathbb{A}^2$  안의 포물선  $V = \mathcal{V}(y - x^2)$ 을 생각해 봅시다. 그러면 다음 두 함수는

$$\begin{aligned} V &\rightarrow \mathbb{C} \\ (x, y) &\mapsto x^2 \\ (x, y) &\mapsto y \end{aligned}$$

실제로 같은 함수입니다!  $V$ 를 생성하는 아이디얼  $I$ 로 "나머지 취하기(mod out)"를 해야 합니다. 이는 자연스럽게 다음으로 이어집니다:

**정리 78.4.3** (좌표환은 아이디얼에 대응됩니다)

$I$ 를 근기 아이디얼(radical ideal)이라 하고,  $V = \mathcal{V}(I) \subseteq \mathbb{A}^n$ 이라 합시다. 그러면

$$\mathbb{C}[V] \cong \mathbb{C}[x_1, \dots, x_n]/I.$$

증명. 위와 같이 자연스러운 전사가 존재합니다

$$\mathbb{C}[x_1, \dots, x_n] \twoheadrightarrow \mathbb{C}[V]$$

그리고 핵은  $I$ 입니다. □

따라서 다양체  $V$ 의 성질은 환  $\mathbb{C}[V]$ 의 성질에 대응됩니다.

## §78.5 정칙 함수의 층

**이 절의 대표적인 예:**  $V = \mathbb{A}^1$ ,  $U = V \setminus \{0\}$ 이라고 합시다. 그러면  $1/x \in \mathcal{O}_V(U)$ 는  $U$  위에서 정칙입니다.

$V$ 를 아핀 다양체라 하고  $\mathbb{C}[V]$ 를 그 좌표환이라고 합시다. 이 장의 시작에서 언급했듯이, 우리는 다양체를 오직 그 내재적 성질에 기반하여 정의하고자 하며, 이는 그 위의 대수 함수들의 모임을 연구함으로써 이루어집니다.

[Va17]의 "동기가 되는 예시: 미분 가능 함수의 층" 절에서, 미분 가능 다양체를 그 위의 미분 가능 함수들을 연구함으로써 어떻게 연구할 수 있는지에 대한 비교를 볼 수 있습니다.

$V$  위의 모든 유리 함수의 집합을  $\mathcal{O}_V$ 로 표기합시다(나중에 보게 되겠지만, 여러 표현을 허용해야 하므로 이 용어는 그다지 정확하지 않습니다). 우리는 이를 하나의 집합으로 볼 수 있지만, 이는 유리 함수의 전체 구조를 포착하지는 못합니다:

**질문 78.5.1.**  $\mathbb{C}[V]$ 의 임의의 두 원소  $f$ 와  $g$ 에 대해,  $\frac{f(x)}{g(x)}$ 가 잘 정의되는 집합이 자리스키 위상에서 열린집합임을 보이십시오. (힌트:  $g^{\text{pre}}(0)$ 는 닫혀 있습니다.)

그래서 우리는 임의의 열린집합  $U$ 에 대해  $\mathcal{O}_V(U)$ 라는 개념을 정의하고자 합니다: 임의의 열린 부분집합 위의 "좋은" 함수들입니다. 당연히  $\mathbb{C}[V]$ 의 임의의 함수는  $\mathcal{O}_V(U)$ 의 함수로서 작동할 것입니다. 그러나 구조를 더 많이 포착하기 위해 유리 함수를 허용함으로써 "좋은" 함수의 정의를 약간 느슨하게 하고자 합니다.

주된 예시는  $1/x$ 가  $\mathbb{A}^1 \setminus \{0\}$  위에서 정칙 함수여야 한다는 것입니다. 첫 번째 자연스러운 추측은 다음과 같습니다:

**정의 78.5.2.**  $U \subseteq V$ 를 다양체  $V$ 의 열린집합이라고 합시다.  $U$  위의 **유리 함수**는  $\mathbb{C}[V]$ 의 두 원소  $f$ 와  $g$ 의 몫  $f(x)/g(x)$ 이며, 여기서  $x \in U$ 에 대해  $g(x) \neq 0$ 이기를 요구합니다.

그러나 이 정의는 다소 지나치게 제한적입니다; 우리는 여러 표현을 허용해야 합니다:

**정의 78.5.3.**  $U \subseteq V$ 를 열린집합이라고 합시다. 함수  $\phi: U \rightarrow \mathbb{C}$ 가 **정칙 함수**라 함은, 모든 점  $p \in U$ 에 대해  $p$ 를 포함하는 열린집합  $U_p \subseteq U$ 와  $U_p$  위의 유리 함수  $f_p/g_p$ 를 찾을 수 있어서 다음이 성립함을 말합니다

$$\phi(x) = \frac{f_p(x)}{g_p(x)} \quad \forall x \in U_p.$$

특히, 우리는 집합  $U_p$  위에서  $g_p(x) \neq 0$ 이기를 요구합니다.  $U$  위의 모든 정칙 함수의 집합을  $\mathcal{O}_V(U)$ 로 표기합니다.

따라서,

**$\phi$ 가  $U$  위에서 국소적으로 유리 함수이면  $U$  위에서 정칙입니다.**

이 정의는 오해를 불러일으킬 정도로 복잡하며, 예시들이 이를 상당히 명확하게 밝혀줄 것입니다. 첫째로, 실제로는 대부분의 경우 정칙 함수의 “전역적” 표현을 몫의 형태로 찾을 수 있으므로,  $p$ 들에 대해 신경 쓸 필요가 없을 것입니다. 예를 들어:

**예제 78.5.4 (정칙 함수)**

- (a) 함수  $f \in \mathbb{C}[V]$ 는 분명히 정칙인데, 모든  $p$ 에 대해  $g_p = 1$ ,  $f_p = f$ 로 택할 수 있기 때문입니다. 그러므로 임의의 열린집합  $U$ 에 대해  $\mathbb{C}[V] \subseteq \mathcal{O}_V(U)$ 입니다.
- (b)  $V = \mathbb{A}^1$ ,  $U_0 = V \setminus \{0\}$ 이라고 합시다. 그러면  $1/x \in \mathcal{O}_V(U_0)$ 는  $U_0$  위에서 정칙입니다.
- (c)  $V = \mathbb{A}^1$ ,  $U_{12} = V \setminus \{1, 2\}$ 라고 합시다. 그러면

$$\frac{1}{(x-1)(x-2)} \in \mathcal{O}_V(U_{12})$$

는  $U_{12}$  위에서 정칙입니다.

그렇지만  $p$ 들을 포함하는 “국소적” 조항은 여전히 필요합니다.

**예제 78.5.5 (국소적 표현의 요구)**

다음 다양체를 생각해봅시다

$$V = \mathcal{V}(ab - cd) \subseteq \mathbb{A}^4$$

그리고 열린집합  $U = V \setminus \mathcal{V}(b, d)$ 를 생각해봅시다.  $U$  위에는 다음과 같이 주어지는 정칙 함수가 있습니다

$$(a, b, c, d) \mapsto \begin{cases} a/d & d \neq 0 \\ c/b & b \neq 0. \end{cases}$$

이들이 ( $ab = cd$ 이므로) "같은 함수"임은 명백하지만, 0으로 나누는 문제가 발생하므로 이를 표현하기 위해 " $a/d$ "나 " $c/b$ "라고 쓸 수는 없습니다. 이것이 바로 정칙 함수의 정의에서 여러 표현을 허용해야 하는 이유입니다.

사실, 우리는 나중에 정칙 함수의 정의가 층화라 불리는 더 일반적인 구성의 특수한 경우임을 보게 될 것인데, 이 구성에서는 " $P$ 인 함수들의 준층"이 "국소적으로  $P$ 인 함수들의 층"으로 변환됩니다.

## §78.6 특수 열린집합 위의 정칙 함수

**이 절의 대표적인 예:**  $\mathbb{A}^1 \setminus \{0\}$  위의 정칙 함수는  $P(x)/x^n$ 입니다.

예상할 수 있듯이 0으로 나누는 문제는 본질적으로 공간  $V$  전체에서의 정칙 함수를 금지합니다. 즉,  $\mathcal{O}_V(V)$  안에는 이미  $\mathbb{C}[V]$ 에 있던 것이 아닌 정칙 함수가 존재하지 않습니다. 사실, 우리는 특수 열린집합 위의 정칙 함수를 계산하는 더 일반적인 결과를 가지고 있습니다:

### 정리 78.6.1 (특수 열린집합 위의 정칙 함수)

$V \subseteq \mathbb{A}^n$ 을 아핀 다양체라 하고  $D(g)$ 를 그 특수 열린 부분집합이라 합시다. 그러면

$$\mathcal{O}_V(D(g)) = \left\{ \frac{f}{g^k} \mid f \in \mathbb{C}[V] \text{ 그리고 } k \in \mathbb{Z} \right\}.$$

특히,  $\mathcal{O}_V(V) = \mathcal{O}_V(D(1)) \cong \mathbb{C}[V]$ 입니다.

이 정리의 증명은 영점 정리(Nullstellensatz)를 필요로 하므로,  $\mathbb{C}$ 가 대수적으로 닫혀 있다는 사실에 의존합니다. 실제로  $\mathbb{C}$ 를  $\mathbb{R}$ 로 바꾸면 반례를 쉽게 찾을 수 있습니다:  $\frac{1}{x^2+1}$ 을 생각해봅시오.

증명.  $f/g^n$  형태의 모든 함수가 성립함은 명백하므로, 우리는 그 역방향을 원합니다. 이는 길기 때문에 처음 읽을 때는 생략해도 될 것입니다.

상황은 다음과 같습니다.  $U = D(g)$ 라고 합시다. 우리에게 정칙 함수  $\phi$ 가 주어져 있는데, 이는 모든 점  $p \in D(g)$ 에서  $\phi$ 를  $f_p/g_p$  (단,  $f_p, g_p \in \mathbb{C}[V]$ )로 표현할 수 있는 열린 근방  $U_p$ 가 존재함을 의미합니다. 그러면, 우리는  $\phi = f/g^n$ 이 되도록 하는  $f \in \mathbb{C}[V]$ 와 정수  $n$ 을 구성하고자 합니다.

먼저, 특정한  $U_p$ 와  $f_p/g_p$ 를 살펴봅시다.  $U_p$ 를 특수 열린집합  $D(h_p)$ 로 축소합니다. 그런 다음,  $\tilde{f}_p = f_p h_p$ 이고  $\tilde{g}_p = g_p h_p$ 라 합시다. 그러면 다음을 얻습니다

$$\frac{\tilde{f}_p}{\tilde{g}_p} \text{에서 성립합니다 } D(h_p) \subseteq U \subseteq X.$$

수정된  $f_p$ 와  $g_p$ 를 사용함으로써 얻는 요점은 다음과 같습니다:

$$\tilde{f}_p \tilde{g}_q = \tilde{f}_q \tilde{g}_p \quad \forall p, q \in U.$$

실제로, 이는 정의에 의해  $D(h_p) \cap D(h_q)$  위에서 성립하며, 이 집합 밖에서는 좌변과 우변이 모두 0입니다.

이제,  $D(g) = \bigcup_{p \in U} D(\tilde{g}_p)$ 임을, 즉

$$\mathcal{V}(g) = \bigcap_{p \in U} \mathcal{V}(\tilde{g}_p).$$

그러므로 영점 정리(Nullstellensatz)에 의해 다음을 알 수 있습니다

$$g \in \sqrt{(\tilde{g}_p : p \in U)} \implies \exists n : g^n \in (\tilde{g}_p : p \in U).$$

다시 말해, 어떤  $n$ 과  $k_p \in \mathbb{C}[V]$ 에 대해 다음이 성립합니다

$$g^n = \sum_p k_p \tilde{g}_p$$

여기서 오직 유한개의  $k_p$ 만이 0이 아닙니다. 이제, 우리는 다음을 주장합니다

$$f := \sum_p k_p \tilde{f}_p$$

이 성립함을 주장합니다. 이는 임의의  $q \in U$ 에 대해 다음을 관찰함으로써 알 수 있습니다

$$f \tilde{g}_q - g^n \tilde{f}_q = \sum_p k_p (\tilde{f}_p \tilde{g}_q - \tilde{g}_p \tilde{f}_q) = 0. \quad \square$$

이는 전역 정칙 함수가 좌표환 안의 것들과 정확히 같다는 것을 의미합니다: 국소적으로 뭉이 되도록 허용한다고 해서 새로운 것을 얻지는 못합니다. (특수 열린집합에 대해서도 마찬가지입니다.)

#### 예제 78.6.2 (특수 열린집합 위의 정칙 함수)

(a) 이미 말했듯이,  $g = 1$ 로 두면 임의의 아핀 다양체  $V$ 에 대해  $\mathcal{O}_V(V) \cong \mathbb{C}[V]$ 를 되찾습니다.

(b)  $V = \mathbb{A}^1$ ,  $U_0 = V \setminus \{0\}$ 이라고 합시다. 그러면

$$\mathcal{O}_V(U_0) = \left\{ \frac{P(x)}{x^n} \mid P \in \mathbb{C}[x], \quad n \in \mathbb{Z} \right\}.$$

따라서 더 많은 예시는  $1/x$ 와  $(x+1)/x^3$ 입니다.

**질문 78.6.3.** 정칙 함수에 관한 우리의 정리가 왜 예제 78.5.5에는 적용되지 않습니까?

정칙 함수는 다음 장에서 스킴을 정의하고 나면 매우 중요해질 것입니다.

## §78.7 베이비 환달린 공간

요약하면, 아핀 대수다양체  $V$ 가 주어졌을 때 우리는 다음을 가지고 있습니다:

- 점들의 집합이라는 구조,
- 이 점들 위에 주어진 위상 공간  $V$ 라는 구조, 그리고
- 모든 열린집합  $U \subseteq V$ 에 대해, 환  $\mathcal{O}_V(U)$ . 이 환의 원소들은 함수  $U \rightarrow \mathbb{C}$ 입니다.

다음과 같이 정하기로 합시다:

**정의 78.7.1. 베이비 환달린 공간**이란 모든 열린집합  $U$ 에 대해 환  $\mathcal{O}_X(U)$ 가 주어진 위상 공간  $X$ 를 말합니다. 이때 환  $\mathcal{O}_X(U)$ 의 원소들은 함수  $f: U \rightarrow \mathbb{C}$ 일 것이 요구되며, 이를  $X$ 의  $U$  위에서의 정칙 함수라고 부릅니다.

따라서 아핀 대수다양체는 베이비 환달린 공간입니다.

**비고 78.7.2** — 이것은 표준적인 정의가 아닙니다. 해해.

이것을 "베이비 환달린 공간"이라고 부르는 이유는, 환달린 공간에서는 환  $\mathcal{O}_V(U)$ 가 실제로 임의의 환일 수 있지만, 상당히 기술적인 일련의 조건들을 만족해야 하기 때문입니다. 이런 경우 모든 작업을 수행하는 것은 바로  $\mathcal{O}_V$ 이며, 우리는  $\mathcal{O}_V$ 를 층이라 불리는 일종의 합자로 생각합니다.

다음 몇 장에서는 아핀/사영/준사영 대수다양체만을 다룰 것이므로, 전체 정의를 다룰 필요가 없도록 이들을 그냥 베이비 환달린 공간이라고 부르기로 하겠습니다. 핵심 개념은 이러한 대수다양체를 임베딩과 무관한 내재적 대상으로 생각하고자 한다는 것입니다. 베이비 환달린 공간은 철학적으로 올바른 접근입니다.

어쨌든, 아핀 대수다양체는 베이비 환달린 공간  $(V, \mathcal{O}_V)$ 입니다. 다음 장에서는 사영 및 준사영 대수다양체를 만나게 될 것인데, 이들은 (베이비) 환달린 공간의 더 많은 예시를 제공합니다. 이러한 예시들을 옆두에 두고, 마침내 환달린 공간의 완전한 정의를 세우고 이를 이용하여 스킴을 정의할 것입니다.

## §78.8 생각해 볼 만한 조금 더 어려운 문제

**문제 78A<sup>†</sup>.** 임의의  $n \geq 1$ 에 대해  $\mathbb{A}^n$ 의 자리스키 위상이 하우스도르프 공간이 아님을 보이십시오.

**문제 78B<sup>†</sup>.**  $V$ 를 아핀 대수다양체라 하고, 그 자리스키 위상을 생각합시다.

- (a) 자리스키 위상이 **뇌터적**임을 보이십시오. 즉, 닫힌 부분집합들의 무한 감소열  $Z_1 \supseteq Z_2 \supseteq Z_3 \supseteq \dots$ 이 존재하지 않음을 보이십시오.
- (b) 뇌터 위상 공간이 콤팩트함을 증명하십시오. 따라서 대수다양체는 위상적으로 콤팩트합니다.

**문제 78C<sup>\*</sup>** (구멍 뚫린 평면).  $V = \mathbb{A}^2$ 이고  $X = \mathbb{A}^2 \setminus \{(0, 0)\}$ 을 원점이 제거된 평면( $V$ 의 열린집합입니다)이라고 합시다.  $\mathcal{O}_V(X)$ 를 계산하십시오.



# 79 사영 다양체

$\mathbb{A}^n$ 에서 아핀 다양체를 공부했으니, 이제  $\mathbb{CP}^n$ 을 고려합니다.  $\mathbb{A}^n$ 의 경우와 마찬가지로 이것도 초보적인 환 공간으로 만들겠습니다.

## §79.1 등급환

**이 절의 대표적인 예:**  $\mathbb{C}[x_0, \dots, x_n]$ 은 등급환입니다.

먼저 등급환이 무엇인지 정의하는 데 시간을 들여, 이 용어를 지금과 나중에 사용할 수 있도록 하겠습니다.

이 정의는 **정의 76.3.2**와 동일합니다.

**정의 79.1.1. 등급환**  $R$ 은 다음과 같은 추가적인 구조를 갖는 환입니다: 아벨 군으로서 다음과 같이 분해됩니다

$$R = \bigoplus_{d \geq 0} R^d$$

여기서  $R^0, R^1, \dots$ 는 아벨 군입니다. 환의 곱셈은  $r \in R^d$ 이고  $s \in R^e$ 이면  $rs \in R^{d+e}$ 가 되는 성질을 가집니다.  $R^d$ 의 원소를 **동차 원소**라고 부르며, “ $r \in R^d$ ”를 뜻하기 위해 “ $d = \deg r$ ”라고 씁니다.

0이 아닌 차수의 동차 원소들로 생성되는 아이디얼  $R \setminus R^0$ 을  $R^+$ 로 표기하고, 이를 **비관계 아이디얼**이라고 부릅니다.

**비고 79.1.2** — 전문가를 위해: 우리가 다루는 모든 등급환은 1을 갖는 가환환입니다.

### 예제 79.1.3 (등급환의 예)

- (a) 환  $\mathbb{C}[x]$ 는 차수에 의해 등급화됩니다: 아벨 군으로서  $\mathbb{C}[x] \cong \mathbb{C} \oplus x\mathbb{C} \oplus x^2\mathbb{C} \oplus \dots$ 입니다.
- (b) 더 일반적으로, 다항식환  $\mathbb{C}[x_0, \dots, x_n]$ 은 차수에 의해 등급화됩니다.

**표기의 남용 79.1.4.**  $r = 0$ 인 경우  $\deg r$ 이라는 표기는 남용적입니다; 모든  $d$ 에 대해  $0 \in R^d$ 임에 유의하십시오. 따라서  $r = 0$ 인 경우를 제외하면  $r$ 의 “유일한” 차수에 대해 말하는 것이 타당합니다.

동차 아이디얼을 자주 언급하게 될 것입니다:

**정의 79.1.5.** 아이디얼  $I \subseteq \mathbb{C}[x_0, \dots, x_n]$ 이  $I = (f_1, \dots, f_m)$ 로 쓸 수 있고 각  $f_i$ 가 동차 다항식이면 **동차**라고 합니다.

**비고 79.1.6** —  $I$ 와  $J$ 가 동차이면,  $I + J, IJ, I \cap J, \sqrt{I}$ 도 동차입니다.

**보조정리 79.1.7** (등급 몫도 등급화됩니다)

$I$ 를 등급환  $R$ 의 동차 아이디얼이라고 합시다. 그러면

$$R/I = \bigoplus_{d \geq 0} R^d / (R^d \cap I)$$

$R/I$ 를 등급환으로 실현합니다.

이러한 주장들은 단순히 대수학이므로, 여기서는 증명을 생략합니다.

**비고 79.1.8** — 다른 몇몇 책에서는 동차 아이디얼(또는 **등급 아이디얼**)을 아벨 군으로서  $I = \bigoplus_{d \geq 0} (R^d \cap I)$ 를 만족하는 아이디얼  $I$ 로 동등하게 정의하기도 합니다. 실제로, 등급 아이디얼은 정확히 몫이 자연스럽게 등급화되는 아이디얼임을 확인할 수 있습니다.

**예제 79.1.9** (등급 몫환의 예)

$R = \mathbb{C}[x, y]$ 이고  $I = (x^3, y^2)$ 로 설정합시다.  $S = R/I$ 라고 합시다. 그러면

$$\begin{aligned} S^0 &= \mathbb{C} \\ S^1 &= \mathbb{C}x \oplus \mathbb{C}y \\ S^2 &= \mathbb{C}x^2 \oplus \mathbb{C}xy \\ S^3 &= \mathbb{C}x^2y \\ S^d &= 0 \quad \forall d \geq 4. \end{aligned}$$

그래서 실제로  $S = R/I$ 는 등급화되며, 6차원  $\mathbb{C}$ -벡터 공간입니다.

**§79.2 주변 공간**

**이 절의 대표적인 예:** 아마도  $\mathcal{V}_{pr}(x^2 + y^2 - z^2)$ 일 것입니다.

이번에 우리가 다루기로 선택한 점들의 집합은  $\mathbb{CP}^n$ 이며, 이는 우리에게  $n$ -순서쌍의 집합으로 생각될 수 있습니다

$$(x_0 : x_1 : \cdots : x_n)$$

모두 0은 아니며, 스케일링에 대해 동일시합니다. 동등하게, 이는  $\mathbb{C}^{n+1}$ 에서 원점을 지나는 직선들의 집합입니다. 사영 공간은 **절 64.6**에서 완전히 정의되어 있으므로, 사영 공간에 익숙하지 않다면 그곳을 참조하십시오.

이를 생각하는 올바른 방법은 “무한대에서의 점들을 더한  $\mathbb{A}^n$ ”입니다:

**정의 79.2.1.** 다음과 같은 집합을 정의합니다

$$U_i = \{(x_0 : \cdots : x_n) \mid x_i \neq 0\} \subseteq \mathbb{CP}^n.$$

이들은 **표준 아핀 차트**라고 불립니다.

이 이름은 다음에서 유래합니다:

**연습문제 79.2.2** (필수).  $U_i$ 에서  $\mathbb{A}^n$ 으로의 자연스러운 전단사를 제시하십시오. 이로써  $\mathbb{CP}^n$ 을 아핀 집합  $U_i$ 에 “무한대에서의 점들”을 더한 것으로 생각할 수 있습니다.

**비고 79.2.3** — 실제로 이 차트들  $U_i$ 는 통상적인 위상을 가진  $\mathbb{CP}^n$ 을 정칙 전이 함수를 갖는 복소 다양체로 만듭니다.

**예제 79.2.4** (구어적으로,  $\mathbb{CP}^1 = \mathbb{A}^1 \cup \{\infty\}$ )

공간  $\mathbb{CP}^1$ 은 순서쌍  $(s : t)$ 들로 이루어지며, 이는 복소수  $z/1$ 을 나타내는 것으로 생각할 수 있습니다. 특히  $U_1 = \{(z : 1)\}$ 은 본질적으로  $\mathbb{A}^1$ 의 또 다른 사본입니다. 새로운 점은 오직 하나,  $(1 : 0)$ 뿐입니다.

그러나 이전과 마찬가지로 이 위에 자리스키 위상을 부여하고자 합니다. 구체적으로,  $\mathbb{CP}^2 = \{(x_0 : x_1 : x_2)\}$ 를 살펴봅시다. 아핀 공간에서 그랬던 것처럼  $\mathbb{CP}^2$ 에서의 영점 궤적을 고려하고자 하며, 이를 통해 사영 대수다양체의 개념을 얻고자 합니다.

그런데 이것이 그리 쉽지는 않습니다: 예를 들어, 함수 “ $x_0$ ”은  $\mathbb{CP}^2$ 의 점들 위에서 잘 정의된 함수가 아닌데, 이는  $(x_0 : x_1 : x_2) = (5x_0 : 5x_1 : 5x_2)$ 이기 때문입니다! 그래서 우리는 여전히 영점 궤적을 가지는 이러한 “의사 함수”들을 고려하고 싶습니다. 이들은 바로 동차 다항식  $f$ 인데,  $f$ 가 차수  $d$ 의 동차 다항식인 것은 다음과 동치이기 때문입니다

$$f(\lambda x_0, \dots, \lambda x_n) = \lambda^d f(x_0, \dots, x_n).$$

특히,  $f$ 가 동차 다항식이면 “ $f(x_0, \dots, x_n) = 0$ ”이라는 관계는 잘 정의됩니다. 따라서 다음과 같이 말할 수 있습니다:

**정의 79.2.5.**  $f$ 가 동차 다항식이면, 그 **영점 궤적**을 다음과 같이 정의할 수 있습니다

$$\mathcal{V}_{\text{pr}}(f) = \{(x_0 : \dots : x_n) \mid f(x_0, \dots, x_n) = 0\}.$$

동차 조건은 정말로 필요합니다. 예를 들어, “ $x_0 - 1 = 0$ ”을 요구하는 것은 말이 되지 않는데, 이는 점  $(1 : 1 : 1)$ 과  $(2015 : 2015 : 2015)$ 가 같은 점이기 때문입니다.

동차 다항식이 우리가 원하는 바를 정확히 수행함을 확인하는 것은 자명합니다; 따라서 이제 다음과 같이 정의할 수 있습니다:

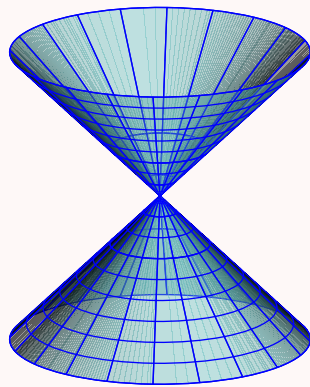
**정의 79.2.6.**  $\mathbb{CP}^n$ 에서의 **사영 대수다양체**는  $n+1$ 개의 변수를 가진 동차 다항식들의 임의의 모임에 대한 공통 영점 궤적입니다.

**예제 79.2.7** ( $\mathbb{CP}^2$ 에서의 원뿔곡선, 또는  $\mathbb{C}^3$ 에서의 원뿔)

다음 대수다양체를 그려봅시다

$$\mathcal{V}_{\text{pr}}(x^2 + y^2 - z^2) \subseteq \mathbb{CP}^2$$

이는  $x^2 + y^2 = z^2$ 을 만족하는 점  $[x : y : z]$ 들로 이루어져 있습니다. 이를  $\mathbb{C}^3$ 의 부분공간으로 본다면(즉,  $\mathbb{CP}^2$ 를 원점을 지나는 직선들의 집합으로 생각함으로써), “원뿔”을 얻게 됩니다:



이제 표준 아핀 차트를 취하면, 다음을 얻습니다:

- $x = 1$ 에서는 쌍곡선  $\mathcal{V}(1 + y^2 - z^2)$ 을 얻습니다.
- $y = 1$ 에서는 쌍곡선  $\mathcal{V}(1 + x^2 - z^2)$ 을 얻습니다.
- $z = 1$ 일 때, 원  $\mathcal{V}(x^2 + y^2 - 1)$ 을 얻습니다.

그렇긴 하지만,  $\mathbb{C}$  위에서는 쌍곡선과 원이 같은 것입니다; 지난 장에서와 마찬가지로  $\mathbb{C}$ 를 1차원으로 그림으로써 약간의 편법을 쓰고 있습니다.

**질문 79.2.8.** 위 원뿔과  $z = 1$  평면의 교집합을 그려보고, 실제로 원이 나오는지 확인하십시오. (이 기하학적 그림은 나중에 중요하게 쓰입니다.)

### §79.3 동차 아이디얼

이제, 다음으로 하고 싶은 것은 아이디얼  $I$ 에 대해  $\mathcal{V}_{\text{pr}}(I)$ 를 정의하는 것입니다. 물론,  $x_0 - 1$ 과 같은 것이 의미가 없다는 문제에 다시 부딪히게 됩니다.

이를 해결하는 방법은 동차 아이디얼만을 사용하는 것입니다.

**정의 79.3.1.**  $I$ 가 동차 아이디얼이면, 다음과 같이 정의합니다

$$\mathcal{V}_{\text{pr}}(I) = \{x \mid f(x) = 0 \forall f \in I\}.$$

**연습문제 79.3.2.** 동차 아이디얼  $I$ 에 대해 " $f(x) = 0 \forall f \in I$ "라는 개념이 잘 정의됨을 보이십시오.

그래서, 우리는 동차 근 아이디얼과 사영 다양체를 전단사로 대응시키는 널스텔렌자츠와 같은 정리를 기대하고 싶습니다. 안타깝게도:

#### 예제 79.3.3 (무관 아이디얼)

몇 가지 꿈과 희망을 짓밟기 위해, 다음 아이디얼을 생각해봅시다

$$I = (x_0, x_1, \dots, x_n).$$

이를 **무관 아이디얼**이라 부릅니다; 이는 동차 근 아이디얼이지만  $\mathcal{V}_{\text{pr}}(I) = \emptyset$ 입니다.

그러나, 무관 아이디얼을 제외하면:

**정리 79.3.4 (동차 널스텔렌자츠)**

$I$ 와  $J$ 를 동차 아이디얼이라 합시다.

(a)  $\mathcal{V}_{\text{pr}}(I) = \mathcal{V}_{\text{pr}}(J) \neq \emptyset$ 이면  $\sqrt{I} = \sqrt{J}$ 입니다.

(b)  $\mathcal{V}_{\text{pr}}(I) = \emptyset$ 이면,  $I = (1)$ 이거나  $\sqrt{I} = (x_0, x_1, \dots, x_n)$ 입니다.

따라서 다음 사이에 자연스러운 전단사가 존재합니다:

- $\mathbb{CP}^n$  안의 사영 다양체들, 그리고
- 무관 아이디얼을 제외한  $\mathbb{C}[x_0, \dots, x_n]$ 의 동차 근 아이디얼들.

증명. 첫 번째 부분을 위해,  $V = \mathcal{V}_{\text{pr}}(I)$ 와  $W = \mathcal{V}_{\text{pr}}(J)$ 를  $\mathbb{CP}^n$  안의 사영 다양체라 합시다.  $\mathbb{CP}^n$ 을  $\mathbb{C}^{n+1}$ 에서 원점을 지나는 직선들로 해석함으로써, 이들을  $\mathbb{A}^{n+1}$  안의 아핀 다양체로 볼 수 있습니다.

대수적으로, 이는 동차 아이디얼  $I, J \subseteq \mathbb{C}[x_0, \dots, x_n]$ 을 취하고, 같은 아이디얼을 사용하여  $\mathbb{A}^{n+1}$  안의 아핀 다양체  $V_{\text{aff}} = \mathcal{V}(I)$ 와  $W_{\text{aff}} = \mathcal{V}(J)$ 를 잘라냄으로써 이루어집니다. 예를 들어, 원뿔  $x^2 + y^2 - z^2 = 0$ 은  $\mathbb{CP}^2$ 에서는 원뿔곡선(1차원 곡선)이지만,  $\mathbb{A}^3$ 에서는 원뿔(2차원 곡면)로도 생각할 수 있습니다.

그러면 (a)에 대해,  $V_{\text{aff}} = W_{\text{aff}}$ 이므로  $\sqrt{I} = \sqrt{J}$ 입니다.

(b)에 대해,  $V_{\text{aff}}$ 는 공집합이거나  $\mathbb{A}^{n+1}$ 의 원점뿐이므로, 널스텔렌자츠에 의해 원하는 대로  $I = (1)$ 이거나  $\sqrt{I} = (x_0, \dots, x_n)$ 입니다.  $\square$

다양체의 교집합과 합집합에 관한 정리 77.4.2의 사영적 유사물은 사영 다양체에 대해서도 그대로 성립합니다.

## §79.4 환달린 공간으로서

**이 절의 대표적인 예:**  $\mathbb{CP}^1$ 에서 한 점을 제외한 부분의 정규 함수는 정확히  $P(s/t)$ .

형태의 함수입니다. 이제 모든 사영 다양체  $V$ 를 초보적인 환달린 공간으로 만들어 봅시다. 우리는 이미 점들의 집합, 즉  $\mathbb{CP}^n$ 의 부분집합을 가지고 있습니다.

위상은 다음과 같이 정의됩니다.

**정의 79.4.1.**  $I$ 가 동차 아이디얼일 때  $\mathcal{V}_{\text{pr}}(I)$  꼴의 집합들을 닫힌집합으로 선언함으로써  $\mathbb{CP}^n$ 에 **자리스키 위상**을 부여합니다.

그러면 모든 사영 다양체  $V$ 는 그 부모인  $\mathbb{CP}^n$ 으로부터 자리스키 위상을 물려받습니다.

**특별 열린집합**  $D(f)$ 는  $V \setminus \mathcal{V}_{\text{pr}}(f)$ 입니다.

따라서 이제 모든 사영 다양체  $V$ 는 위상 공간이 됩니다. 남은 것은 정칙함수의 층  $\mathcal{O}_V$ 를 부여하는 일입니다. 이를 위해서는 조금 조심할 필요가 있습니다. 아핀의 경우에는 분자와 분모를 제공하는 데 사용할 수 있는 함수들의 좋은 작은 환, 즉 좌표환  $\mathbb{C}[x_0, \dots, x_n]/I$ 가 있었습니다. 그러므로 다음과 같이 정의하는 것이 자연스러워 보입니다.

**정의 79.4.2.**  $I$ 가 동차 근기 아이디얼일 때, 사영 다양체  $V = \mathcal{V}_{\text{pr}}(I) \subseteq \mathbb{CP}^n$ 의 **동차 좌표 환**은 다음 환으로 정의됩니다

$$\mathbb{C}[V] = \mathbb{C}[x_0, \dots, x_n]/I.$$

**비고 79.4.3** — 비고 78.4.2의 경우와 달리,  $\mathbb{C}[V]$ 의 원소는 더 이상  $V$ 에서  $\mathbb{C}$ 로 가는 함수에 대응하지 않습니다. 그럼에도 불구하고, 이는  $\mathcal{V}(I) \subseteq \mathbb{A}^{n+1}$ 에서  $\mathbb{C}$ 로 가는 함수입니다.

그러나 유리함수를 정의할 때는 분자와 분모가 같은 차수여야 한다는 새로운 요구 사항을 부과해야 합니다.

**정의 79.4.4.**  $U \subseteq V$ 를 사영 다양체  $V$ 의 열린집합이라 합시다. 사영 다양체  $V$  위의 **유리함수**  $\phi$ 는 몫  $f/g$ 로서, 여기서  $f, g \in \mathbb{C}[V]$ 이고,  $f$ 와  $g$ 는 같은 차수의 동차이며,  $\mathcal{V}_{\text{pr}}(g) \cap U = \emptyset$ 입니다. 이렇게 하여 함수  $\phi: U \rightarrow \mathbb{C}$ 를 얻습니다.

**예제 79.4.5** (유리함수의 예시)

$V = \mathbb{CP}^1$ 이 좌표  $(s : t)$ 를 갖는다고 합시다.

(a)  $U = V$ 이면, 상수함수  $c/1$ 이  $U$  위의 유일한 유리함수입니다.

(b) 이제  $U_1 = V \setminus \{(1 : 0)\}$ 이라 합시다. 그러면 정칙함수의 한 예시는 다음과 같습니다

$$\frac{s^2 + 9t^2}{t^2} = \left(\frac{s}{t}\right)^2 + 9.$$

$U_1$ 을  $\mathbb{C}$ 로 생각하면(즉, 무한대 점을 뺀  $\mathbb{CP}^1$ 이므로  $\mathbb{A}^1$ 과 같습니다) 이는 정말로 그저 함수  $x^2 + 9$ 일 뿐입니다.

그러면 이전과 같은 정의를 반복할 수 있습니다.

**정의 79.4.6.**  $U \subseteq V$ 를 사영 다양체  $V$ 의 열린집합이라 합시다. 모든 점  $p$ 에 대해,  $p$ 를 포함하는 열린집합  $U_p$ 와  $U_p$  위의 유리함수  $f_p/g_p$ 를 찾아 다음을 만족시킬 수 있으면, 함수  $\phi: U \rightarrow \mathbb{C}$ 를 **정칙함수**라고 합니다

$$\phi(x) = \frac{f_p(x)}{g_p(x)} \quad \forall x \in U_p.$$

특히,  $U_p \cap \mathcal{V}_{\text{pr}}(g_p) = \emptyset$ 을 요구합니다.  $U$  위의 모든 정칙함수의 집합을  $\mathcal{O}_V(U)$ 로 나타냅니다.

물론, 앞선 예시의 유리함수들도 정칙함수의 예시입니다. 이로써 베이비 환 공간으로서의 사영 다양체  $V$ 의 정의가 완성됩니다.

## §79.5 정칙함수의 예시

당연히, 특별 열린집합 위의 정칙함수가 무엇인지 말씀드려야 하는데, 이는 지난번의 정리 78.6.1에 대응됩니다.

**정리 79.5.1** (사영 다양체에 대한 특별 열린집합 위의 정칙함수)

$V$ 를 사영 다양체라 하고,  $g \in \mathbb{C}[V]$ 가 양의 차수의 동차라고 합시다(따라서  $g$ 는 상수가 아닙니다). 그러면

$$\mathcal{O}_V(D(g)) = \left\{ \frac{f}{g^r} \mid f \in \mathbb{C}[V] \text{ 차수 } r \deg g \text{의 동차} \right\}.$$

$g = 1$ 인 경우는 어떨까요? 비슷한 결과가 성립하지만,  $V$ 가 기약이라는 가정이 필요합니다.

**정의 79.5.2.** 사영 다양체  $V$ 는 두 개의 진(사영) 부분다양체의 합집합으로 쓸 수 없으면 기약입니다.

**정리 79.5.3** (사영 공간 위의 상수 정칙함수만 존재)

$V$ 를 기약 사영 다양체라고 합시다. 그러면  $V$  위의 정칙함수는 오직 상수뿐이며, 따라서

$$\mathcal{O}_V(V) \cong \mathbb{C}.$$

이는  $\mathbb{C}$ 가 대수적으로 닫혀 있다는 사실에 의존합니다.

이에 대한 증명은 지금은 생략합니다.

**예제 79.5.4** (위에서 기약성이 필요한 이유)

$V$ 가 기약이어야 하는 이유는, 그렇지 않으면 예를 들어  $V$ 를 두 점의 합집합으로 취할 수 있기 때문입니다. 이 경우  $\mathcal{O}_V(V) \cong \mathbb{C}^{\oplus 2}$ 입니다.

**비고 79.5.5** —  $g = 1$ 일 때  $\mathcal{O}_V(D(g))$ 가 그토록 다르게 동작하는 것이 이상하게 보일 수 있습니다. 한 가지 모호한 설명은, 사영 다양체에서  $\deg g > 0$ 이면 특정 열린집합  $D(g)$ 가 아핀 다양체와 매우 비슷해 보인다는 것입니다. 예를 들어  $\mathbb{CP}^1$ 에서  $\mathbb{CP}^1 \setminus \{0\} \cong \mathbb{A}^1$ 입니다(여기서  $\cong$ 는 제가 정확히 규정하지 않은 의미로 사용됩니다). 따라서 이 주장은 대응하는 아핀의 결과와 관련되게 됩니다. 하지만  $\deg g = 0$ 이고  $g \neq 0$ 이면  $D(g)$ 는 사영 다양체 전체가 되며, 이는 아핀처럼 보이지 않으므로 이러한 유비가 성립하지 않습니다.

**예제 79.5.6** ( $\mathbb{CP}^1$  위의 정칙 함수)

$V = \mathbb{CP}^1$ 이라 하고, 좌표를  $(s : t)$ 라 합시다.

- (a) 정리 79.5.1에 의해,  $U_1$ 이 점  $(1 : 0)$ 을 제외한 표준 아핀 차트라면,  $\mathcal{O}_V(U_1) = \left\{ \frac{f}{t^n} \mid \deg f = n \right\}$ 입니다. 이는 다음과 같이 쓸 수 있습니다

$$\mathcal{O}_V(U_1) \cong \{P(s/t) \mid P \in \mathbb{C}[x]\} \cong \mathcal{O}_{\mathbb{A}^1}(\mathbb{A}^1).$$

이는  $U_1$ 이 “ $\mathbb{A}^1$ 과 매우 비슷해 보인다”는 우리의 지식과 부합합니다.

- (b)  $V$ 가 기약이므로,  $\mathcal{O}_V(V) = \mathbb{C}$ 입니다: 즉  $\mathbb{CP}^1$  위에는 상수가 아닌 함수가 존재하지 않습니다.

**예제 79.5.7** ( $\mathbb{CP}^2$  위의 정칙 함수)

$\mathbb{CP}^2$ 의 좌표를  $(x : y : z)$ 라 하고,  $U_0 = \{(x : y : 1) \in \mathbb{CP}^2\}$ 를 특정 열린집합  $D(z)$ 라 합시다. 그러면 같은 맥락에서,

$$\mathcal{O}_{\mathbb{CP}^2}(U_0) = \left\{ \frac{P(x, y)}{z^n} \mid \deg P = n \right\} \cong \{P(x/z, y/z) \mid P \in \mathbb{C}[x, y]\}.$$

## §79.6 생각해 볼 만한 조금 더 어려운 문제

문제:

# 80 보너스: 베주 정리(Bézout's theorem)

이 장에서는 Bézout 정리를 다룹니다. 이는 차수가  $d$ 와  $e$ 인 두 곡선이  $\mathbb{CP}^2$ 에서 “정확히”  $de$ 개의 점에서 교차해야 한다는 개념을 정확하게 만듭니다. (사영 공간에서 다루므로, 예를 들어 임의의 두 직선은 교차합니다.)

## §80.1 근기가 아닌 아이디얼

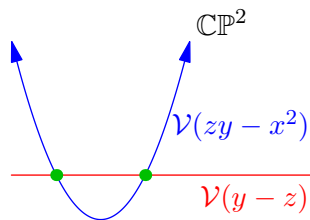
이 절의 대표적인 예: 포물선의 접선.

우리는 중복도를 고려해야 합니다. 그래서 가능할 때마다 다양체  $V$  대신 동차 아이디얼  $I$ 를 다룰 것인데, 이는  $I$ 가 근기 아이디얼이 아닐 가능성을 허용하고자 하기 때문입니다. 어떻게 그렇게 할 수 있는지 살펴봅시다.

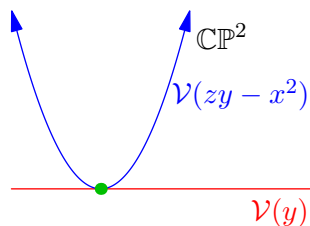
첫 번째 예로,  $y = x^2$ 와 직선  $y = 1$ 을 교차시킨다고 합시다. 더 정확히는,  $\mathbb{CP}^2$ 의 사영 좌표에서 포물선  $zy = x^2$ 와  $y = z$ 를 교차시킵니다. 교집합의 아이디얼은

$$(zy - x^2, y - z) = (x^2 - z^2, y - z) \subseteq \mathbb{C}[x, y, z].$$

따라서 이는 두 개의 점을 갖는 것에 해당하며, 이는 두 교차점을 줍니다:  $(1 : 1 : 1)$ 과  $(-1 : 1 : 1)$ . 다음은 아핀  $z = 1$  차트에서 두 다양체의 그림입니다:



그것은 괜찮지만, 이제  $zy = x^2$ 를 직선  $y = 0$ 과 교차시킨다고 합시다. 그러면 대신 “이중 점”을 얻습니다:



이번에는 대응하는 아이디얼이

$$(zy - x^2, y) = (x^2, y) \subseteq \mathbb{C}[x, y, z].$$

이 아이디얼은 근기 아이디얼이 아니며,  $\sqrt{(x^2, y)} = (x, y)$ 를 취하면  $\mathbb{CP}^2$ 의 단일 사영점  $(0 : 0 : 1)$ 에 대응하는 아이디얼을 얻습니다. 이것이 우리가 다양체 대신 아이디얼을 다루는 이유입니다:  $(x^2, y)$ 와  $(x, y)$ 의 차이를 구분해야 합니다.

## §80.2 유한개 점들의 힐베르트 함수

**이 절의 대표적인 예:** 이중점  $(x^2, y)$ 에 부여된 힐베르트 함수는 결국 상수 2가 됩니다.

**정의 80.2.1.** 공집합이 아닌 사영 다양체  $V$ 가 주어지면,  $V = \mathcal{V}_{\text{pr}}(I)$ 를 만족하는 유일한 근기 아이디얼  $I$ 가 존재합니다. 이 장에서는 이를  $\mathcal{I}_{\text{rad}}(V)$ 로 표기합니다. 공집합인 다양체에 대해서는 무언가 아이디얼을 선택하는 대신  $\mathcal{I}_{\text{rad}}(\emptyset) = (1)$ 로 둡니다.

**정의 80.2.2.**  $I \subseteq \mathbb{C}[x_0, \dots, x_n]$ 이 동차라고 합시다.  $I$ 의 **힐베르트 함수**를  $h_I: \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$ 로 표기하며 다음과 같이 정의합니다

$$h_I(d) = \dim_{\mathbb{C}} (\mathbb{C}[x_0, \dots, x_n]/I)^d$$

즉,  $h_I(d)$ 는  $\mathbb{C}[x_0, \dots, x_n]/I$ 의  $d$ 번째 등급 부분의 차원입니다.

**정의 80.2.3.**  $V$ 가 사영 다양체라면,  $h_V = h_{\mathcal{I}_{\text{rad}}(V)}$ 로 설정하는데, 여기서  $I = \mathcal{I}_{\text{rad}}(V)$ 는 위에서 정의한 대로  $V = \mathcal{V}_{\text{pr}}(I)$ 를 만족하는 근기 아이디얼입니다.

이 경우,  $\mathbb{C}[x_0, \dots, x_n]/I$ 는 그냥  $\mathbb{C}[V]$ 입니다.

### 예제 80.2.4 (0차원에서의 힐베르트 함수의 예)

구체성을 위해  $\mathbb{CP}^2$ 를 사용합시다.

(a)  $V$ 가 아이디얼  $\mathcal{I}_{\text{rad}}(V) = (x, y)$ 를 갖는 단일 점  $(0 : 0 : 1)$ 이라면,

$$\mathbb{C}[V] = \mathbb{C}[x, y, z]/(x, y) \cong \mathbb{C}[z] \cong \mathbb{C} \oplus z\mathbb{C} \oplus z^2\mathbb{C} \oplus z^3\mathbb{C} \dots$$

이는 모든 차수에서 차원이 1입니다. 따라서 다음을 얻습니다:

$$h_I(d) \equiv 1.$$

(b) 이제 “이중점” 아이디얼  $I = (x^2, y)$ 를 사용한다고 합시다. 이번에는 다음을 얻습니다

$$\begin{aligned} \mathbb{C}[x, y, z]/(x^2, y) &\cong \mathbb{C}[z] \oplus x\mathbb{C}[z] \\ &\cong \mathbb{C} \oplus (x\mathbb{C} \oplus z\mathbb{C}) \oplus (xz\mathbb{C} \oplus z^2\mathbb{C}) \oplus (xz^2\mathbb{C} \oplus z^3\mathbb{C}) \oplus \dots \end{aligned}$$

이로부터 다음을 추론합니다

$$h_I(d) = \begin{cases} 2 & d = 1, 2, 3, \dots \\ 1 & d = 0. \end{cases}$$

(c) 이제 두 점으로 이루어진 다양체  $V = \{(1 : 1 : 1), (-1 : 1 : 1)\}$ 을 취해봅시다. 여기서  $\mathcal{I}_{\text{rad}}(V) = (x^2 - z^2, y - z)$ 입니다. 그러면

$$\begin{aligned} \mathbb{C}[x, y, z]/(x^2 - z^2, y - z) &\cong \mathbb{C}[x, z]/(x^2 - z^2) \\ &\cong \mathbb{C}[z] \oplus x\mathbb{C}[z]. \end{aligned}$$

이 예제는 앞의 예제와 같은 힐베르트 함수를 가집니다.

**표기의 남용 80.2.5.** 저는 동형사상 기호  $\mathbb{C}[z] \cong \mathbb{C} \oplus z\mathbb{C} \oplus z^2\mathbb{C}$ 를 남용하고 있으며, 다른 예제들에서도 마찬가지입니다. 이것은  $\mathbb{C}$ -벡터 공간 수준에서만 동형사상입니다. 그러나 다른 예제들의 힐베르트 함수를 계산할 때도 이러한 표기법의 남용을 계속 사용하겠습니다.

**예제 80.2.6** (공집합 다양체에 대한 힐베르트 함수)

$I \subsetneq \mathbb{C}[x_0, \dots, x_n]$  가 아이디얼이고, 근기가 아닐 수도 있지만

$$\mathcal{V}_{\text{pr}}(I) = \emptyset$$

을 만족한다고 합시다. 따라서  $\sqrt{I} = (x_0, \dots, x_n)$  은 무관 아이디얼입니다. 그러므로 모든  $i$ 에 대해  $x_i^{d_i} \in I$  를 만족하는 정수  $d_i$  (단,  $i = 0, \dots, n$ )가 존재합니다. 그 결과,  $d > d_0 + \dots + d_n$  인 임의의  $d$ 에 대해  $h_I(d) = 0$  입니다. 이를 요약하여 다음과 같이 말합니다

$$h_I(d) = 0 \text{ 모든 } d \gg 0 \text{에 대해.}$$

여기서 표기법  $d \gg 0$  은 "충분히 큰 모든  $d$ "를 의미합니다.

이 예제들로부터  $I$ 가 아이디얼이면 힐베르트 함수는 결국 상수가 되는 것으로 보이며, 원하는 상수는  $\mathcal{V}_{\text{pr}}(I)$ 의 크기와 같되,  $I$ 가 근기가 아닌 경우에는 "중복도를 고려하여" 같다는 것을 알 수 있습니다.

이를 증명해 봅시다. 진행하기 전에 짧은 완전열에 대해 독자에게 간단히 상기시키겠습니다: 사상들의 수열  $0 \rightarrow V \hookrightarrow W \twoheadrightarrow X \rightarrow 0$  은  $\text{im}(V \hookrightarrow W) = \ker(W \twoheadrightarrow X)$  를 만족하는 것입니다 (물론 사상  $V \hookrightarrow W$  와  $W \twoheadrightarrow X$  는 각각 단사이고 전사입니다).  $V, W, X$  가  $\mathbb{C}$  위의 유한 차원 벡터 공간이면 이는  $\dim W = \dim V + \dim X$  를 함의합니다.

**명제 80.2.7** ( $I \cap J$  와  $I + J$  의 힐베르트 함수)

$I$  와  $J$  를  $\mathbb{C}[x_0, \dots, x_n]$  의 동차 아이디얼이라 합시다. 그러면

$$h_{I \cap J} + h_{I+J} = h_I + h_J.$$

증명. 임의의  $d \geq 0$  을 생각합시다. 간단히 하기 위해  $S = \mathbb{C}[x_0, \dots, x_n]$  이라 합시다. 그러면

$$0 \longrightarrow [S/(I \cap J)]^d \hookrightarrow [S/I]^d \oplus [S/J]^d \twoheadrightarrow [S/(I + J)]^d \longrightarrow 0$$

$$f \longmapsto (f, f)$$

$$(f, g) \longmapsto f - g$$

은 벡터 공간의 짧은 완전열입니다. 따라서 모든  $d \geq 0$  에 대해 다음이 성립합니다

$$\dim [S/I]^d \oplus [S/J]^d = \dim [S/(I \cap J)]^d + \dim [S/(I + J)]^d$$

이로부터 결론이 도출됩니다. □

**예제 80.2.8** ( $\mathbb{CP}^1$  에서 두 점의 힐베르트 함수)

좌표환  $\mathbb{C}[s, t]$  를 가진  $\mathbb{CP}^1$  에서, 점  $(0 : 1)$  에 대응하는 아이디얼  $I = (s)$  와 점  $(1 : 0)$  에 대응하는 아이디얼  $J = (t)$  를 생각합시다. 그러면  $I \cap J = (st)$  는 이 두 점의 서로소 합집합에 대응하는 아이디얼이며,  $I + J = (s, t)$  는 무관 아이디얼입니다. 그 결과  $d \gg 0$  에 대해  $h_{I+J}(d) = 0$  입니다. 따라서 다음을 얻습니다

$$h_{I \cap J}(d) = h_I(d) + h_J(d) \quad d \gg 0 \text{에 대해}$$

그러므로 두 점으로 이루어진 사영 다양체의 힐베르트 함수는  $d \gg 0$  에 대해 상수 2 입니다.

이 예제는 주요 결과의 내용을 잘 보여줍니다:

### 정리 80.2.9 (0차원 다양체의 힐베르트 함수)

$V$  를  $m$  개의 점으로 이루어진 사영 다양체라 합시다 (단,  $m \geq 0$  은 정수). 그러면

$$h_V(d) = md \gg 0 \text{에 대해.}$$

증명.  $m = 0$  인 경우는 이미 다루었으므로,  $m \geq 1$  이라 가정합시다.  $I = \mathcal{I}_{\text{rad}}(V)$  라 하고,  $k = 1, \dots, m$  에 대해  $I_k = \mathcal{I}_{\text{rad}}(V \text{의 } k\text{번째 점})$  라 합시다.

**연습문제 80.2.10.** 모든  $d$  에 대해  $h_{I_k}(d) = 1$  임을 보이십시오. (예제 80.2.4(a)를 수정하십시오.)

따라서  $m \geq 2$  에 대한 귀납법으로 진행할 수 있으며, 기저 사례  $m = 1$  은 위에서 이미 다루었습니다. 귀납 단계에서는 정리 77.4.2 의 사영적 유사물을 사용합니다.  $d \gg 0$  에 대해  $h_{I_1 \cap \dots \cap I_{m-1}}(d) = m-1$  임을 알고 있습니다 (이는 처음  $m-1$  개의 점입니다;  $I_1 \cap \dots \cap I_{m-1}$  이 근기임에 유의하십시오).  $m$  번째 점을 추가하기 위해 다음을 주목합시다

$$h_{I_1 \cap \dots \cap I_m}(d) = h_{I_1 \cap \dots \cap I_{m-1}}(d) + h_{I_m}(d) - h_J(d)$$

여기서  $J = (I_1 \cap \dots \cap I_{m-1}) + I_m$  입니다. 아이디얼  $J$  는 근기가 아닐 수도 있지만, 앞선 예제에 의해  $\mathcal{V}_{\text{pr}}(J) = \emptyset$  을 만족하므로  $d \gg 0$  에 대해  $h_J = 0$  입니다. 이로써 증명이 완료됩니다.  $\square$

정확히 같은 방식으로 다음을 증명할 수 있습니다:

### 따름정리 80.2.11 ( $\dim \mathcal{V}_{\text{pr}}(I) = 0$ 일 때 $h_I$ 는 결국 상수가 됩니다)

$I$  를 반드시 근기일 필요는 없는 아이디얼이라 하고,  $\mathcal{V}_{\text{pr}}(I)$  가 유한히 많은 점으로 이루어져 있다고 합시다. 그러면 힐베르트 함수  $h_I$  는 결국 상수가 됩니다.

증명. 점의 개수  $m \geq 1$  에 대한 귀납법입니다. 기저 사례  $m = 1$  은 예제 80.2.4(b) 와 연습문제 80.2.10 에서 본질적으로 다루었습니다. 귀납 단계는 근기 아이디얼에 대한 신경을 쓰지 않는다는 점을 제외하면 위 증명과 문자 그대로 동일합니다.  $\square$

## §80.3 힐베르트 다항식

지금까지는 0차원 다양체의 힐베르트 함수에 대해서만 이야기했고, 이 함수가 결국 상수가 됨을 보였습니다. 이제 몇 가지 예를 더 살펴봅시다.

### 예제 80.3.1 ( $\mathbb{CP}^n$ 의 힐베르트 함수)

$\mathbb{CP}^n$ 의 힐베르트 함수는

$$h_{\mathbb{CP}^n}(d) = \binom{d+n}{n} = \frac{1}{n!}(d+n)(d+n-1)\dots(d+1)$$

”공과 항아리” 논법에 의해 다음과 같습니다. 이는 차수가  $n$ 인 다항식입니다.

**예제 80.3.2 (포물선의 힐베르트 함수)**

좌표  $\mathbb{C}[x, y, z]$ 를 갖는  $\mathbb{CP}^2$  안의 포물선  $zy - x^2$ 를 생각합시다. 그러면

$$\mathbb{C}[x, y, z]/(zy - x^2) \cong \mathbb{C}[y, z] \oplus x\mathbb{C}[y, z].$$

조합적인 계산을 하면 다음을 얻습니다.

$$\begin{aligned} h_{(zy-x^2)}(0) &= 1 && \text{기저 } 1 \\ h_{(zy-x^2)}(1) &= 3 && \text{기저 } x, y, z \\ h_{(zy-x^2)}(2) &= 5 && \text{기저 } xy, xz, y^2, yz, z^2. \end{aligned}$$

이로써 실제로  $h_{(zy-x^2)}(d) = 2d + 1$ 임을 알 수 있습니다.

사실, 이러한 ”결국 다항식이 되는” 성질은 항상 성립합니다.

**정리 80.3.3 (힐베르트 다항식)**

$I \subseteq \mathbb{C}[x_0, \dots, x_n]$ 을 (반드시 근기 아이디얼일 필요는 없는) 동차 아이디얼이라 합시다. 그러면

- (a) 모든  $d \gg 0$ 에 대해  $h_I(d) = \chi_I(d)$ 를 만족하는 다항식  $\chi_I$ 가 존재합니다.
- (b)  $\deg \chi_I = \dim \mathcal{V}_{\text{pr}}(I)$ 입니다 (만약  $\mathcal{V}_{\text{pr}}(I) = \emptyset$ 이면  $\chi_I = 0$ 입니다).
- (c) 다항식  $m! \cdot \chi_I$ 는 정수 계수를 갖습니다.

증명. 기저 사례는 앞 절에서 다루었습니다.

귀납 단계에서는 차원  $m$ 인  $\mathcal{V}_{\text{pr}}(I)$ 를 고려합니다.  $\mathcal{V}_{\text{pr}}(I)$ 의 어떤 기약 성분도  $H$  안에 포함되지 않는 초평면  $H$ 를 생각합시다 (이 사실은 기하학적으로 자명하므로 증명 없이 인용하지만, 지난번에 증명을 써보려다 망쳤습니다). 간단히 하기 위해, 일반성을 잃지 않고  $H = \mathcal{V}_{\text{pr}}(x_0)$ 라고 가정합니다.

다시  $S = \mathbb{C}[x_0, \dots, x_n]$ 이라 둡시다. 이제 다음의 짧은 완전열을 생각합시다.

$$0 \longrightarrow [S/I]^{d-1} \hookrightarrow [S/I]^d \longrightarrow [S/(I + (x_0))]^d \longrightarrow 0$$

$$f \longmapsto f \cdot x_0$$

$$f \longmapsto f.$$

(첫 번째 사상의 단사성은  $\mathcal{V}_{\text{pr}}(I)$ 의 기약 성분에 대한 가정으로부터 따라 나옵니다.) 이제 완전성으로부터 다음이 성립합니다.

$$h_I(d) - h_I(d-1) = h_{I+(x_0)}(d).$$

마지막 항은 기하학적으로  $\mathcal{V}_{\text{pr}}(I) \cap H$ 에 대응하며, 그 차원은  $m-1$ 이므로 귀납 가정에 의해

다음은 알 수 있습니다.

$$h_I(d) - h_I(d-1) = \frac{c_0 d^{m-1} + c_1 d^{m-2} + \cdots + c_{m-1}}{(m-1)!} \quad d \gg 0$$

여기서  $c_0, \dots, c_{m-1}$ 은 어떤 정수입니다. 그러면 다항식의 **유한 차분** 이론에 의해 증명이 끝납니다.  $\square$

## §80.4 Bézout의 정리

**정의 80.4.1.**  $\chi_I$ 를  $I$ 의 **힐베르트 다항식**이라 부릅니다. 만약  $\chi_I$ 가 영이 아니면,  $m! \chi_I$ 의 최고차항 계수를  $I$ 의 **차수**라 부르며, 이는 정수이고  $\deg I$ 로 표기합니다.

물론 사영 다양체  $V$ 에 대해서는  $h_V = h_{\mathcal{I}_{\text{rad}}(V)}$ 로,  $\deg V = \deg \mathcal{I}_{\text{rad}}(V)$ 로 둡니다.

**비고 80.4.2** — 아이디얼의 차수  $\deg I$ 는  $\deg h_I$ 와 같지 않다는 점에 유의하십시오!

차수의 몇 가지 성질을 보이겠습니다. 이를 통해 임의의 사영 다양체의 차수를 그 기약 성분들로부터 계산할 수 있게 됩니다.

### 명제 80.4.3 (차수의 성질)

두 다양체  $V$ 와  $W$ 에 대해, 다음이 성립합니다:

- $V$ 와  $W$ 가 서로소이고 차원이 같다면,  $\deg(V \cup W) = \deg V + \deg W$ 입니다.
- $\dim V < \dim W$ 이면,  $\deg(V \cup W) = \deg W$ 입니다.

따라서,

**차수는 성분들에 대해 가법적이며, 가장 높은 차원의 성분의 "차수"를 측정합니다.**

증명. 정리 80.3.3과 명제 80.2.7에서의 힐베르트 다항식의 성질들과, 최고차항 계수가 가장 큰 차수를 갖는 항에만 의존한다는 사실로부터 따라옵니다.  $\square$

### 예제 80.4.4 (차수의 예시)

- $V$ 가  $n \geq 1$ 개의 점으로 이루어진 유한 집합이면, 차수는  $n$ 입니다.
- $I$ 가 중복점에 대응한다면, 차수는 2입니다.
- $\mathbb{CP}^n$ 의 차수는 1입니다.
- 임의의 직선이나 평면은 각각  $\mathbb{CP}^1$ 과  $\mathbb{CP}^2$ 와 "동형"이므로, 차수가 1입니다.
- 포물선의 차수는 2입니다. (대수다양체로서 포물선은 직선과 동형임에 유의하십시오!)
- 포물선과 한 점의 합집합의 차수는 2입니다.

이제,  $f$ 가 동차 이차 다항식이면 주 아이디얼  $(f)$ 의 차수가 2일 것이라고, 그리고 이런 식으로 계속될 것이라고 짐작할 수 있습니다. (예를 들어 우리는 원이 차수 2를 가질 것이라고 기대합니다.) 이는 사실입니다:

**정리 80.4.5 (Bézout의 정리)**

$I$ 가  $\mathbb{C}[x_0, \dots, x_n]$ 의 동차 아이디얼이고  $\dim \mathcal{V}_{\text{pr}}(I) \geq 1$ 이라 하십시오.  $f \in \mathbb{C}[x_0, \dots, x_n]$ 가  $\mathcal{V}_{\text{pr}}(I)$ 의 어떤 기약 성분에서도 소멸하지 않는 차수  $k$ 의 동차 다항식이라 하십시오. 그러면

$$\deg(I + (f)) = k \deg I.$$

기하학적으로,

$V$ 가 임의의 사영 다양체이고,  $\mathcal{V}(f)$ 가 차수  $k$ 의 초곡면이라면, 그 교집합  $V \cap \mathcal{V}(f)$ 는 차수  $k \deg V$ 를 가집니다 — 단,  $V$ 의 어떤 기약 성분이  $\mathcal{V}(f)$  안에 포함되지 않는 경우에 한합니다.

이것이 바로 이 장의 서두에서 언급했던 것입니다.

아이디얼  $I$ 가 근기 아이디얼이 아닐 수 있기 때문에, 이 기하학적 해석 진술은 가능한 가장 일반적인 형태는 아닙니다 — 이 문제는 나중에 스킴으로의 일반화를 통해 바로잡힐 것입니다.

증명. 다시  $S = \mathbb{C}[x_0, \dots, x_n]$ 이라고 합시다. 이번에는 완전열이 다음과 같습니다

$$0 \longrightarrow [S/I]^{d-k} \hookrightarrow [S/I]^d \longrightarrow [S/(I + (f))]^d \longrightarrow 0.$$

이 올림피아드풍의 연습문제는 **문제 80A**로 남겨둡니다. □

**§80.5 응용**

먼저, 차수의 개념이 우리가 기대하던 바와 같다는 것을 보이겠습니다.

**따름정리 80.5.1 (초곡면: 차수가 그 이름값을 하는 이유)**

$V$ 를 초곡면, 즉  $\mathcal{I}_{\text{rad}}(V) = (f)$ 이고  $f$ 는 차수  $k$ 의 동차 다항식이라고 합시다. 그러면  $\deg V = k$ 입니다.

증명.  $\deg(0) = \deg \mathbb{CP}^n = 1$ 임을 기억하십시오. Bézout의 정리에서  $I = (0)$ 으로 놓으십시오. □

$\mathbb{CP}^2$ 에서 혼한 특수한 경우는 다음과 같습니다:

**따름정리 80.5.2 (곡선에 대한 베주 정리(Bézout's theorem))**

$\mathbb{CP}^2$ 에서 공통 기약 성분을 갖지 않는 임의의 두 곡선  $X$ 와  $Y$ 에 대해,

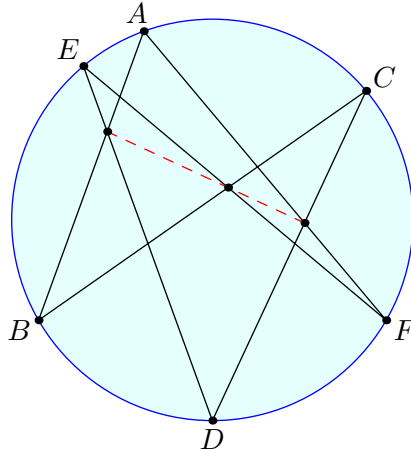
$$|X \cap Y| \leq \deg X \cdot \deg Y.$$

이제 이를 사용하여 파스칼 정리를 증명합니다.

**정리 80.5.3 (파스칼 정리)**

$A, B, C, D, E, F$ 를  $\mathbb{CP}^2$ 에서 원뿔곡선  $\mathcal{C}$  위에 놓인 서로 다른 여섯 점이라 합시다. 그러면 점  $AB \cap DE$ ,  $BC \cap EF$ ,  $CD \cap FA$ 는 한 직선 위에 있습니다.

증명.  $X$ 를 세 직선  $AB, CD, EF$ 의 합집합과 같은 대수다양체라 합시다. 그러면  $X = \mathcal{V}_{\text{pr}}(f)$ 가 되는 어떤 삼차 다항식  $f$ 가 존재합니다(이는 세 개의 일차식의 곱입니다). 마찬가지로,  $Y = \mathcal{V}_{\text{pr}}(g)$ 를 세 직선  $BC, DE, FA$ 의 합집합과 같은 대수다양체라 합시다.



이제  $P$ 를 원뿔곡선  $\mathcal{C}$  위의 임의의 점으로, 여섯 점  $A, B, C, D, E, F$ 와는 다른 점이라 합시다. 다음의 사영 대수다양체를 생각합시다

$$V = \mathcal{V}_{\text{pr}}(\alpha f + \beta g)$$

여기서 상수  $\alpha$ 와  $\beta$ 는  $P \in V$ 가 되도록 선택됩니다.

**질문 80.5.4.**  $\alpha$ 와  $\beta$ 를 어떻게 선택하든 상관없이,  $V$ 가 여섯 점  $A, B, C, D, E, F$ 뿐만 아니라 세 점  $AB \cap DE, BC \cap EF, CD \cap FA$ 도 포함함을 보이십시오.

이제  $|V \cap \mathcal{C}| \geq 7$ 임에 주목하십시오. 그러나  $\deg V = 3$ 이고  $\deg \mathcal{C} = 2$ 입니다. 이는  $V$ 와  $\mathcal{C}$ 가 기약 성분을 공유하지 않는 한 베주 정리(Bézout's theorem)에 모순됩니다. 이는 차수의 이유로  $V$ 가 직선과 원뿔곡선의 합집합인 경우에만 일어날 수 있습니다. 즉 다음이 성립해야 합니다

$$V = \mathcal{C} \cup \text{직선}.$$

마지막으로, 세 교점  $AB \cap DE, BC \cap EF, CD \cap FA$ 는  $\mathcal{C}$  위에 있지 않으므로, 반드시 이 직선 위에 있어야 함에 주목하십시오.  $\square$

파스칼 정리는 사실 케일리-바카라흐 정리의 특수한 경우일 뿐이며, 이 정리는 타원 곡선 위의 덧셈 연산이 결합적임을 증명하는 데 사용될 수 있다는 점을 언급하고자 합니다. 관심 있는 독자는 같은 기법을 이용하여 케일리-바카라흐 정리를 증명해 보기를 시도해 볼 수 있습니다.

**§80.6 생각해 볼 만한 조금 더 어려운 문제**

**문제 80A.** 앞서 나온 베주 정리(Bézout's theorem)의 증명을 완성하십시오.



**문제 80B** (USA TST 2016/6).  $ABC$ 를 예각 부등변삼각형이라 하고  $P$ 를 그 내부의 점이라 하십시오.  $A_1, B_1, C_1$ 을 각각 삼각형의 변  $BC, CA, AB$  위로의  $P$ 의 사영이라 하겠습니다.  $AA_1, BB_1, CC_1$ 이 한 점에서 만나고  $\angle PAB + \angle PBC + \angle PCA = 90^\circ$ 가 성립하는 점  $P$ 의 자취를 구하십시오.



# 81 대수다양체의 사상

스킴에 대한 작업을 준비하면서, 아핀 및 사영 대수다양체 사이의 사상에 대해 이야기하는 것으로 이 부분을 마무리하겠습니다. 이는 우리가 그것들을 정의하는 데 시간을 들였기 때문입니다.

아이디어: 아핀 및 사영 대수다양체가 모두 초급 유유평간(baby ringed space)의 특수한 경우임을 알고 있으므로, 사실 우리는 임의의 두 초급 유유평간 사이의 사상을 정의하기만 하면 됩니다.

## §81.1 초급 유유평간의 사상 정의하기

이 절의 대표적인 예: 다음 절을 보십시오.

$(X, \mathcal{O}_X)$ 와  $(Y, \mathcal{O}_Y)$ 를 초급 유유평간이라 하고, 이들 사이의 사상을 어떻게 정의할지 생각해 봅시다.

대수학에서의 지도 원리는 사상이 기저 구조에 대한 함수이면서도, 그 위에 덧붙여진 풍부화된 추가 데이터를 존중하기를 원한다는 것입니다. 아주 초기의 몇 가지 예를 들어 보겠습니다:

### 예제 81.1.1 (사상을 정의하는 방법)

- 군을 생각해 봅시다. 군  $G$ 는 (원소들의) 기저 집합을 가지며, 이를 곱셈 연산으로 풍부화합니다. 따라서 준동형사상은 기저 집합 사이의 사상이면서, 동시에 군의 곱셈을 존중해야 합니다.
- $R$ -가군을 생각해 봅시다. 각  $R$ -가군은 기저 아벨 군을 가지며, 이를 스칼라 곱셈으로 풍부화합니다. 따라서 선형 사상은 아벨 군의 준동형사상이어야 할 뿐만 아니라, 스칼라 곱셈 또한 존중해야 함을 요구합니다.
- 위상 공간을 생각해 봅시다. 공간  $X$ 는 (점들의) 기저 집합을 가지며, 이를 열린 집합들의 위상으로 풍부화합니다. 따라서 우리는 점들의 집합에 대한 사상 중, 위상을 존중하는 것(열린집합의 원상이 열린집합인 것)을 고려합니다.

이번 경우, 유유평간  $(X, \mathcal{O}_X)$ 는 기저 위상 공간을 가지며, 이를 구조층으로 풍부화했습니다. 따라서 우리는 이러한 위상 공간들 사이의 연속 사상  $f: X \rightarrow Y$ 를 원하며, 이는 정칙 함수의 층을 존중해야 합니다.

이를 어떻게 할 수 있을까요? 만약  $\psi: Y \rightarrow \mathbb{C}$ 를 정칙 함수라 하면, 합성을 통해  $X \rightarrow Y \rightarrow \mathbb{C}$ 라는 사상을 자연스럽게 쓸 수 있습니다. 그러면 우리는 이것 또한 정칙 함수이기를 요구하고자 합니다.

더 일반적으로,  $Y$  위의 임의의 정칙 함수를 가져와  $X$  위의 어떤 함수를 얻을 수 있는데, 이를 당겨오기라 부릅니다. 그런 다음 우리는 모든 당겨오기가  $X$  위에서 정칙이기를 요구합니다.

**정의 81.1.2.**  $(X, \mathcal{O}_X)$ 와  $(Y, \mathcal{O}_Y)$ 를 초급 유유평간이라 합시다. 사상  $f: X \rightarrow Y$ 와 정칙 함수  $\phi \in \mathcal{O}_Y(U)$ 가 주어졌을 때,  $\phi$ 의 **당겨오기**를  $f^*\phi$ 로 표기하며, 다음의 합성 함수로 정의합니다

$$f^{\text{pre}}(U) \xrightarrow{f} U \xrightarrow{\phi} \mathbb{C}.$$

”당겨오기”라는 용어의 사용은 미분 형식을 공부할 때와 동일합니다.

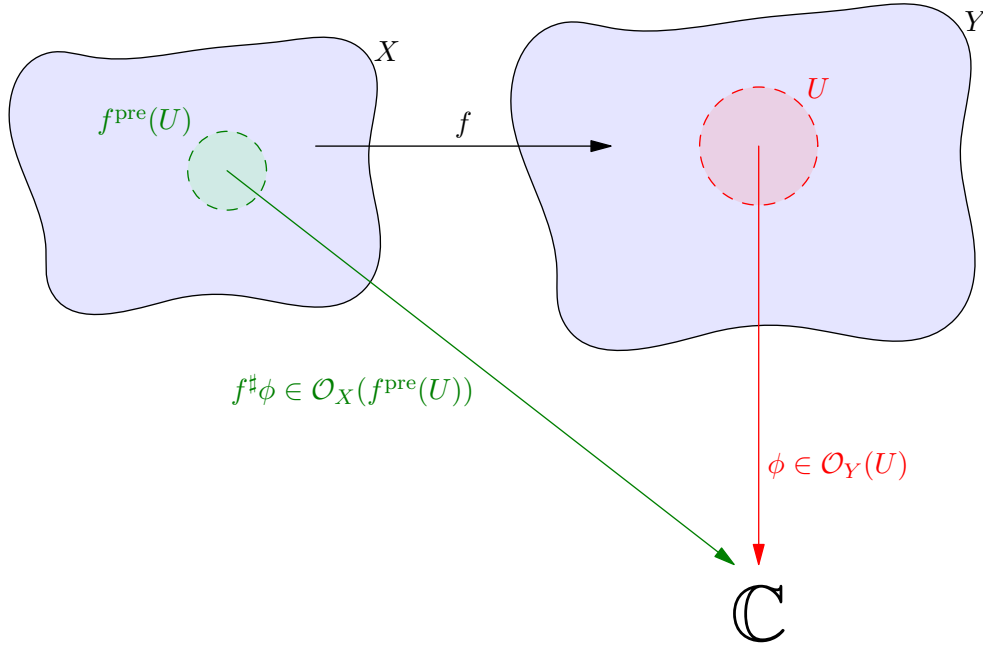
**정의 81.1.3.**  $(X, \mathcal{O}_X)$ 와  $(Y, \mathcal{O}_Y)$ 를 초급 유유평간이라 합시다. 위상 공간 사이의 연속 사상  $f: X \rightarrow Y$ 는,  $Y$  위의 정칙 함수의 모든 당겨오기가  $X$  위에서 정칙 함수일 때 **사상**이라 합니다.

두 초급 유유평간은 그들 사이에 서로 역인 사상들이 존재할 때 **동형**이라 하며, 이때 이 사상들을 **동형사상**이라 부릅니다.

특히, 당겨오기는 모든  $U$ 에 대해 (방향이 뒤집힌) 환 준동형사상

$$f^\sharp: \mathcal{O}_Y(U) \rightarrow \mathcal{O}_X(f^{\text{pre}}(U))$$

을 제공합니다. 따라서 우리의 사상은 많은 정보를 담고 있습니다. 다음은 사상  $f$ 와,  $\phi: U \rightarrow \mathbb{C}$  (여기서  $U \subseteq Y$ )의 당겨오기를 나타낸 그림입니다.



**예제 81.1.4** ( $t \mapsto t^2$  아래에서의  $\frac{1}{y-25}$ 의 당겨오기)

사상

$$f: X = \mathbb{A}^1 \rightarrow Y = \mathbb{A}^1 \quad \text{에 의해} \quad t \mapsto t^2$$

은 대수다양체의 사상입니다. 예를 들어, 열린집합  $Y \setminus \{25\} \subseteq Y$  위의 정칙 함수  $\varphi = \frac{1}{y-25}$ 를 생각해 봅시다.  $f$ 의 역상은  $X \setminus \{\pm 5\}$ 입니다. 따라서 당겨오기는

$$f^\sharp \varphi: X \setminus \{\pm 5\} \rightarrow \mathbb{C}$$

$$\text{에 의해} \quad x \mapsto \frac{1}{x^2 - 25}$$

이며, 이는  $X \setminus \{\pm 5\}$  위에서 정칙입니다.

## §81.2 가장 단순한 예시 분류

**이 절의 대표적인 예:** 정리 81.2.2; 그것들은 그저 다항식일 뿐입니다.

철학적인 관점에서, 우리는 앞선 정의를 선호하는데, 이는 우리의 다양체를 매장된 대상이 아니라 내재적인 대상으로 다룬다는 우리의 철학에 부합하기 때문입니다. 그러나 이를 실제로 검증하는 것은 다소 성가신 일입니다.

그러므로 이 절에서 우리는 다음을 할 것입니다.

- $\mathbb{A}^m \rightarrow \mathbb{A}^n$ 로부터의 모든 사상을 분류하고,
- $\mathbb{CP}^m \rightarrow \mathbb{CP}^n$ 로부터의 모든 사상을 분류합니다.

이어지는 내용에서 어떤 것이 사상임을 주장할 때 많은 부분을 대충 얼버무릴 것인데, 이는 그렇게 하는 것이 대부분 세부 사항을 확인하는 작업이기 때문입니다. 이어지는 정리들은 우리에게 좌표에 더 기반을 두고 실제 계산에 사용하기 더 쉬운, 사상에 대한 대안적인 정의를 제공할 것입니다.

### §81.2.i 아핀 분류

앞서 우리는  $t \mapsto t^2$ 가 어떻게 사상을 주는지 보았습니다. 더 일반적으로, 임의의 다항식  $P(t)$ 가 주어졌을 때, 사상  $t \mapsto P(t)$ 도 성립합니다. 그리고 사실, 이것이 전부입니다:

**연습문제 81.2.1.**  $X = \mathbb{A}^1, Y = \mathbb{A}^1$ 이라 합시다.  $\text{id} \in \mathcal{O}_Y(Y)$ 를 고려함으로써, 다른 정칙 함수는 존재하지 않음을 보이십시오.

사실, 앞선 연습문제를 일반화해봅시다:

#### 정리 81.2.2 (아핀 다양체의 정칙 사상은 전역적으로 다항식이다)

$X \subseteq \mathbb{A}^m$ 과  $Y \subseteq \mathbb{A}^n$ 이 아핀 다양체라 합시다. 다양체의 모든 사상  $f: X \rightarrow Y$ 는 다음과 같이 주어집니다

$$x = (x_1, \dots, x_m) \xrightarrow{f} (P_1(x), \dots, P_n(x))$$

여기서  $P_1, \dots, P_n$ 은 다항식입니다.

증명. 그러한 모든 함수가 성립함을 확인하는 것은 그리 어렵지 않으므로, 반대 방향으로 가봅시다.  $f: X \rightarrow Y$ 가 사상이라 합시다.

먼저,  $f^{\text{pre}}(Y) = X$ 임을 주목하십시오. 이제 사영  $(y_1, \dots, y_n) \mapsto y_1$ 로 주어지는 정칙 함수  $\pi_1 \in \mathcal{O}_Y(Y)$ 를 고려합시다. 따라서 우리는  $\pi_1 \circ f$ 가  $X$  위에서 정칙이어야 함이 필요합니다.

하지만 아핀 다양체의 경우  $\mathcal{O}_X(X)$ 는 단순히 좌표환  $\mathbb{C}[X]$ 이므로,  $\pi_1 \circ f = P_1$ 이 되는 다항식  $P_1$ 이 존재함을 알 수 있습니다. 다른 좌표들에 대해서도 마찬가지입니다.  $\square$

### §81.2.ii 사영 분류

안타깝게도, 사영적인 설정에서는 상황이 다소 더 기묘합니다.  $X \subseteq \mathbb{CP}^m$ 과  $Y \subseteq \mathbb{CP}^n$ 이 사영 다양체라면, 모든 함수

$$x = (x_0 : x_1 : \dots : x_m) \mapsto (P_0(x) : P_1(x) : \dots : P_n(x))$$

$P_i$ 들이 같은 차수의 동차식이고 동시에 모두 소멸하지 않는 한 유효한 사상입니다. 하지만 아핀 다양체에 대한 증명을 반복하려 하면 문제에 부딪힙니다:  $\pi_1$  사상이 존재하지 않습니다. ((1:1) = (2:2)를 1로 보낼까요, 아니면 2로 보낼까요?)

그리고 안타깝게도, 이를 고칠 방법은 없습니다. 반례:

**예제 81.2.3** (전역적으로 다항식이 아닌 사영 사상)

$V = \mathcal{V}_{\text{pr}}(xy - z^2) \subseteq \mathbb{CP}^2$ 라 합시다. 그러면 사상

$$V \rightarrow \mathbb{CP}^1 \quad \text{에 의해} \quad (x : y : z) \mapsto \begin{cases} (x : z) & x \neq 0 \\ (z : y) & y \neq 0 \end{cases}$$

은 사영 다양체의 사상임이 밝혀집니다. 이는  $x, y \neq 0$ 이면  $(x : z) = (z : y)$ 이기 때문에 잘 정의되는 것이며, 정칙 함수의 정의를 연상시켜야 합니다.

좋은 소식은 “국소적인” 문제만이 유일한 제약 요인이라는 것입니다.

**정리 81.2.4** (사영 다양체의 정칙 사상은 국소적으로 다항식이다)

$X \subseteq \mathbb{CP}^m$ 과  $Y \subseteq \mathbb{CP}^n$ 이 사영 다양체이고  $f: X \rightarrow Y$ 가 사상이라 합시다. 그러면 모든 점  $p \in X$ 에서 열린 근방  $U_p \ni p$ 와 (그  $U$ 에 의존하는) 다항식  $P_0, P_1, \dots, P_n$ 이 존재하여 다음이 성립합니다

$$f(x) = (P_0(x) : P_1(x) : \dots : P_n(x)) \quad \forall x = (x_0 : \dots : x_n) \in U_p.$$

물론 다항식  $P_i$ 는 같은 차수의 동차식이어야 하며  $U_p$ 의 어떤 점에서도 동시에 소멸할 수 없습니다.

**예제 81.2.5** (동형사상의 예)

사실, 사상  $V = \mathcal{V}_{\text{pr}}(xy - z^2) \rightarrow \mathbb{CP}^1$ 은 동형사상입니다. 역사상  $\mathbb{CP}^1 \rightarrow V$ 는 다음과 같이 주어집니다

$$(s : t) \mapsto (s^2 : t^2 : st).$$

따라서 실제로  $V \cong \mathbb{CP}^1$ 입니다.

**§81.3 몇 가지 추가 응용과 예시**

**이 절의 대표적인 예:**  $\mathbb{A}^1 \hookrightarrow \mathbb{CP}^1$ 은 좋은 예입니다.

이전 절에서는 아핀 다양체를 아핀 다양체로, 사영 다양체를 사영 다양체로 완전히 정리했습니다. 그러나 이 장의 시작에서 제시한 정의는 임의의 베이비 환 달린 공간에 대해서도 성립하므로, 탐구할 여지가 여전히 많이 남아 있습니다.

예를 들어, **아핀 공간과 사영 공간이 서로 대화하게 만들 수 있습니다.** 안 될 이유가 있겠습니까? 당겨오기 기반 정의의 힘은, 서로 다른 곳에 존재하더라도 임의의 베이비 환 달린 공간들이 소통할 수 있게 해준다는 데 있습니다.

**예제 81.3.1** ( $\mathbb{A}^1 \hookrightarrow \mathbb{CP}^1$ 의 매장)

다음 사상을 생각해 봅시다

$$f: \mathbb{A}^1 \hookrightarrow \mathbb{CP}^1 \quad \text{에 의해} \quad t \mapsto (t : 1).$$

이것 역시 다양체의 사상입니다. (당겨오기가 어떤 모습일지 보이십니까?) 이는  $\mathbb{CP}^1$ 이 “ $\mathbb{A}^1$ 에 무한원점 하나를 더한 것”이라는 사실을 반영합니다.

더 많은 베이비 환 달린 공간을 만들어내는 또 다른 방법이 여기 있습니다. 임의의 사영 다양체가 주어지면, 그것의 열린 부분집합을 취할 수 있고, 그것 자체가 베이비 환 달린 공간이 됩니다. 여기에 이름을 붙여 보겠습니다.

**정의 81.3.2. 준사영 다양체**란 사영 다양체  $V$ 의 열린집합  $X$ 를 말합니다. 임의의 열린집합  $U \subseteq X$ 에 대해 단순히  $\mathcal{O}_X(U) = \mathcal{O}_V(U)$ 로 정의하기 때문에, 이것 역시 베이비 환 달린 공간  $(X, \mathcal{O}_X)$ 입니다.

사영 다양체의 열린 부분집합을 취하기로 한 이유는, 이것이 아핀 다양체까지도 포섭하기 때문입니다. 예를 들면:

**예제 81.3.3 (포물선은 준사영 다양체이다)**

포물선  $V = \mathcal{V}(y - x^2) \subset \mathbb{A}^2$ 을 생각해 봅시다. 사영 다양체  $W = \mathcal{V}_{\text{pr}}(zy - x^2)$ 을 취하고, 표준 아핀 조각  $D(z)$ 를 살펴봅시다. 그러면 다음과 같은 동형사상이 존재합니다

$$\begin{aligned} V &\rightarrow D(z) \subseteq W \\ (x, y) &\mapsto (x : y : 1) \\ (x/z, y/z) &\leftarrow (x : y : z). \end{aligned}$$

결과적으로  $V$ 는  $W$ 의 열린 부분집합과 동형이므로, 이를 준사영으로 간주합니다.



일반적으로 이 증명은 쉽게 적용할 수 있습니다.

**명제 81.3.4 (아핀  $\subseteq$  준사영)**

모든 아핀 다양체는 준사영 다양체와 동형입니다 (즉, 모든 아핀 다양체는 어떤 사영 다양체의 열린 부분집합입니다).

따라서 준사영 다양체는 지금까지 살펴본 두 종류의 다양체를 모두 일반화합니다.

## §81.4 쌍곡선 효과

**이 절의 대표적인 예:**  $\mathbb{A}^1 \setminus \{0\}$ 은 심지어 아핀이다

그렇다면 자연스러운 질문이 생깁니다: 아핀도 사영도 아닌 준사영 다양체가 존재하는가? 답은 그렇다이지만, 서술의 흐름을 위해 일부러 모르는 척하며 반례를 찾아보겠습니다. 실제 예시는 연습문제에서 제시됩니다.

우리의 첫 번째 추측은 가장 단순한 사영 다양체, 이를테면  $\mathbb{CP}^1$ 을 취해서 점 하나를 제거하는 것(열린집합을 얻기 위해)일 수 있습니다. 이는 준사영이지만  $\mathbb{A}^1$ 과 동형입니다. 그래서 대신 가장 단순한 아핀 다양체, 이를테면  $\mathbb{A}^1$ 에서 시작해서 점 하나를 제거해 보겠습니다.

놀랍게도 이것은 통하지 않습니다.

**예제 81.4.1** (핵심 예시: 구멍 뚫린 직선은 쌍곡선과 동형이다)

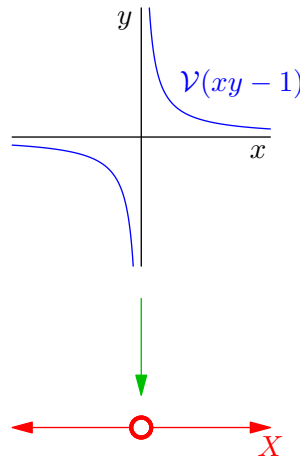
$X = \mathbb{A}^1 \setminus \{0\}$ 을 준사영 다양체라고 합시다. 우리는 실제로 다음과 같은 동형사상이 성립함을 주장합니다

$$X \cong V = \mathcal{V}(xy - 1) \subseteq \mathbb{A}^2$$

이는  $X$ 가 여전히 어떤 아핀 다양체와 동형임을 보여줍니다. 사상들은 다음과 같습니다

$$\begin{aligned} X &\leftrightarrow V \\ t &\mapsto (t, 1/t) \\ x &\mapsto (x, y). \end{aligned}$$

직관적으로,  $\mathbb{A}^2$  안의 "쌍곡선  $y = 1/x$ "는  $x$ 축 위로 사영할 수 있습니다. 관련 그림은 다음과 같습니다.



사실,  $\mathbb{A}^1$ 에서 임의의 개수의 점을 제거하는 방법은 실패합니다.  $\{1, 2, 3\}$ 을 제거하면, 그 결과로 얻어지는 열린집합은 baby ringed space로서  $\mathcal{V}(y(x-1)(x-2)(x-3) - 1)$ 과 동형이며, 이는 통속적으로  $y = \frac{1}{(x-1)(x-2)(x-3)}$ 이라고 부를 수 있습니다.

진실은 더 일반적입니다.

**아핀 다양체의 특별열린집합은 아핀입니다.**

정확한 동형사상은 다음과 같습니다.

**정리 81.4.2** (아핀의 특별열린 부분집합은 아핀이다)

$X = D(f) \subseteq V = \mathcal{V}(f_1, \dots, f_m) \subseteq \mathbb{A}^n$ 을 생각하십시오. 여기서  $V$ 는 아핀 다양체이고, 특별열린집합  $X$ 는 준사영 다양체로 여겨집니다. 다음과 같이 정의하십시오

$$W = \mathcal{V}(f_1, \dots, f_m, y \cdot f - 1) \subseteq \mathbb{A}^{n+1}$$

여기서  $y$ 는  $\mathbb{A}^{n+1}$ 의  $(n+1)$ 번째 좌표입니다. 그러면  $X \cong W$ 입니다.

더 나은 이름이 없어서, 저는 이것을 **쌍곡선 효과**라고 부르겠으며, 이는 나중에 중요한 역할을 하게 될 것입니다.

따라서 아핀이 아닌 준사영 다양체의 예를 찾고자 한다면, 좋은 후보 하나는 특별열린집합이 아닌 아핀 공간의 열린집합일 것입니다. 지금 야심이 있다면, 구멍 뚫린 평면(즉,  $\mathbb{A}^2$ 에서 원점을 뺀 것)이 그러한 예임을 증명해 볼 수 있습니다. 이 예는 다음 장에서 다시 보게 될 것이므로, 다시 시도할 기회가 한 번 더 있을 것입니다.

## §81.5 생각해 볼 만한 조금 더 어려운 문제

**문제 81A.** 다음 사상을 생각하십시오

$$\mathbb{A}^1 \rightarrow \mathcal{V}(y^2 - x^3) \subseteq \mathbb{A}^2 \quad \text{에 의해} \quad t \mapsto (t^2, t^3).$$

이것이 다양체의 사상이지만 동형사상은 아님을 보이십시오.

**문제 81B<sup>†</sup>.** 모든 사영 다양체는 아핀 다양체와 동형인 열린 근방을 가짐을 보이십시오. 이런 의미에서 "사영 다양체는 국소적으로 아핀"입니다.

**문제 81C.**  $V$ 를 아핀 다양체라 하고  $W$ 를 기약 사영 다양체라 하십시오.  $V \cong W$ 인 것과  $V$ 와  $W$ 가 단일 점인 것이 동치임을 증명하십시오.



**문제 81D** (구멍 뚫린 평면은 아핀이 아니다).  $X = \mathbb{A}^2 \setminus \{(0, 0)\}$ 을  $\mathbb{A}^2$ 의 열린집합이라 하십시오.  $V$ 를 임의의 아핀 다양체라 하고  $f: X \rightarrow V$ 를 사상이라 하십시오.  $f$ 가 동형사상이 아님을 보이십시오.



XX

대수기하학 II: 아핀 스킴

## 제XX부: 목차

|           |                                                                    |            |
|-----------|--------------------------------------------------------------------|------------|
| <b>82</b> | <b>층과 한 달린 공간</b>                                                  | <b>855</b> |
| 82.1      | 동기와 주의사항                                                           | 855        |
| 82.2      | 준층                                                                 | 855        |
| 82.3      | 줄기와 짝                                                              | 857        |
| 82.4      | 층                                                                  | 861        |
| 82.5      | 층에서 단면은 짝의 수열"입니다"                                                 | 862        |
| 82.6      | 층화(선택)                                                             | 864        |
| 82.7      | 생각해 볼 만한 조금 더 어려운 문제                                               | 865        |
| <b>83</b> | <b>국소화</b>                                                         | <b>867</b> |
| 83.1      | 스포일러                                                               | 867        |
| 83.2      | 정의                                                                 | 868        |
| 83.3      | 원소를 제외한 국소화                                                        | 869        |
| 83.4      | 소 아이디얼에서의 국소화                                                      | 870        |
| 83.5      | 국소화의 소 아이디얼                                                        | 872        |
| 83.6      | 몫환의 소 아이디얼                                                         | 873        |
| 83.7      | 국소화는 몫과 교환됩니다                                                      | 874        |
| 83.8      | 생각해 볼 만한 조금 더 어려운 문제                                               | 876        |
| <b>84</b> | <b>아핀 스킴: 자리스키 위상</b>                                              | <b>877</b> |
| 84.1      | 조금 더 예고하자면                                                         | 877        |
| 84.2      | 점들의 집합                                                             | 878        |
| 84.3      | 스펙트럼 위의 자리스키 위상                                                    | 879        |
| 84.4      | 크룰 차원                                                              | 882        |
| 84.5      | 근기에 관하여                                                            | 883        |
| 84.6      | 생각해 볼 만한 조금 더 어려운 문제                                               | 885        |
| <b>85</b> | <b>아핀 스킴: 층</b>                                                    | <b>887</b> |
| 85.1      | 구조층의 쓸모없는 정의                                                       | 887        |
| 85.2      | 특별 열린집합의 가치 (또는: 실제로 절편을 계산하는 방법)                                  | 888        |
| 85.3      | 구조층의 줄기                                                            | 890        |
| 85.4      | 국소환과 잉여체: 짝과 값을 잇는 다리                                              | 891        |
| 85.5      | 요약                                                                 | 894        |
| 85.6      | 함수는 값이 아니라 짝에 의해 결정됩니다                                             | 894        |
| 85.7      | 생각해 볼 만한 조금 더 어려운 문제                                               | 895        |
| <b>86</b> | <b>막간: 아핀 스킴의 열여덟 가지 예시</b>                                        | <b>897</b> |
| 86.1      | 예시: $\text{Spec } k$ , 하나의 점                                       | 897        |
| 86.2      | $\text{Spec } \mathbb{C}[x]$ , 일차원 직선                              | 897        |
| 86.3      | $\text{Spec } \mathbb{R}[x]$ , 복소 켈레가 붙은 일차원 직선(영점 정리를 두려워하지 마십시오) | 898        |
| 86.4      | $\text{Spec } k[x]$ , 임의의 바탕체 위에서                                  | 899        |
| 86.5      | $\text{Spec } \mathbb{Z}$ , 1차원 스킴                                 | 899        |
| 86.6      | $\text{Spec } k[x]/(x^2 - 7x + 12)$ , 두 점                          | 900        |
| 86.7      | $\text{Spec } k[x]/(x^2)$ , 이중점                                    | 900        |
| 86.8      | $\text{Spec } k[x]/(x^3 - 5x^2)$ , 이중점과 단일점                        | 901        |
| 86.9      | $\text{Spec } \mathbb{Z}/60\mathbb{Z}$ , 세 점을 가진 스킴                | 901        |
| 86.10     | $\text{Spec } k[x, y]$ , 즉 이차원 평면                                  | 902        |
| 86.11     | $\text{Spec } \mathbb{Z}[x]$ , 이차원 스킴, 그리고 멤퍼드의 그림                 | 903        |
| 86.12     | $\text{Spec } k[x, y]/(y - x^2)$ , 포물선                             | 904        |
| 86.13     | $\text{Spec } \mathbb{Z}[i]$ , 가우스 정수 (일차원)                        | 905        |
| 86.14     | 긴 예제: $\text{Spec } k[x, y]/(xy)$ , 두 축                            | 906        |
| 86.15     | $\text{Spec } k[x, x^{-1}]$ , 구멍 뚫린 직선(또는 쌍곡선)                     | 908        |
| 86.16     | $\text{Spec } k[x]_{(x)}$ , 직선의 원점을 확대한 모습                         | 909        |
| 86.17     | $\text{Spec } k[x, y]_{(x, y)}$ , 평면의 원점을 확대한 모습                   | 910        |
| 86.18     | $\text{Spec } k[x, y]_{(0)} = \text{Spec } k(x, y)$ , 일반점 위의 줄기    | 910        |
| 86.19     | 생각해 볼 만한 조금 더 어려운 문제                                               | 910        |

|           |                                |            |
|-----------|--------------------------------|------------|
| <b>87</b> | <b>국소 환 달린 공간의 사상</b>          | <b>911</b> |
| 87.1      | 단면을 통한 환 달린 공간의 사상 . . . . .   | 911        |
| 87.2      | 줄기를 통한 환 달린 공간의 사상 . . . . .   | 912        |
| 87.3      | 국소 환 달린 공간의 사상 . . . . .       | 913        |
| 87.4      | 아핀 스킴 사이의 사상의 몇 가지 예 . . . . . | 914        |
| 87.5      | 큰 정리 . . . . .                 | 917        |
| 87.6      | 스킴 사상의 추가 예시 . . . . .         | 919        |
| 87.7      | 비아핀 스킴에 관하여 조금 . . . . .       | 920        |
| 87.8      | 여기서 어디로 갈 것인가 . . . . .        | 922        |
| 87.9      | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 922        |



# 82 층과 환 달린 공간

앞서 다룬 아핀 대수다양체  $V$ 의 복잡성 대부분은  $\mathcal{O}_V$ 에서 비롯됩니다. 이것은 "층"이라 불리는 유형의 대상입니다. 이 장의 목적은 이 층이 정확히 무엇이며, 무슨 역할을 하는지를 완전히 정의하는 것입니다.

## §82.1 동기와 주의사항

염두에 둘 전형적인 예시는 위상 공간  $X$  위의 "성질  $P$ 를 갖는 함수들"의 층입니다: 모든 열린집합  $U$ 에 대해,  $\mathcal{F}(U)$ 는  $X$  위의 함수들의 환을 우리에게 줍니다. 하지만 우리는 매우 추상적으로 작업할 것이며,  $\mathcal{F}(U)$ 가 "함수"로서의 해석 없이 단지 환이라고만 가정할 것입니다.

이 장 전체에 걸쳐, 저는 대수기하학 예시들뿐만 아니라  $X$ 가 위상 공간이고  $\mathcal{F}$ 가 미분 가능/해석적/기타 함수들의 층인 경우도 사용할 것입니다. 층의 좋은 점 중 하나는 동일한 추상화가 잘 작동한다는 것이며, 따라서 대수적 예시와 해석적 예시 양쪽으로 직관을 훈련할 수 있습니다. 특히, 자리스키 위상에서는 실제로 그렇게 생기지 않았음에도 불구하고, 열린집합  $U$ 를 계속 타원 모양으로 그릴 수 있습니다.

이 추상화의 보상은 [장 84](#)에서 임의의 스킴을 정의할 수 있게 해준다는 것입니다. 대수다양체는 "함수들의 환"으로  $\mathbb{C}[x_1, x_2, \dots, x_n]/I$ 를 사용하는데, 완전히 일반적인 층을 사용함으로써 우리는 이를 임의의 가환환으로 대체합니다. 특히,  $\mathbb{C}[x]/(x^2)$ 를 선택할 수 있으며, 이는 우리가 줄곧 추구해 온 "중복도" 거동을 제공할 것입니다.

## §82.2 준층

**이 절의 대표적인 예:** 정칙(또는 정규, 연속, 미분가능, 상수, 무엇이든) 함수의 층.

$\mathcal{O}_V$ 의 올바른 일반화는 이른바 환의 층입니다.  $\mathcal{O}_V$ 가  $V$ 의 열린집합을 환으로 보냈으며,  $\mathcal{O}_V(U)$ 가 "함수의 환"이라는 해석을 가졌음을 상기하십시오.

[절 78.5](#)에서  $\mathcal{O}_V$ 가 집합으로서 단순히 대수적 함수들로 이루어져 있음을 상기하십시오. 하지만  $\mathcal{O}_V$ 를 순전히 집합으로만 본다면, 함수들의 구조는 본질적으로 버려지게 됩니다.

$\mathcal{O}_V$  안의 함수들이 서로 어떻게 관련되어 있는지 살펴봅시다:

- $\mathcal{O}_V$ 의 각 함수는 열린집합  $U \subseteq V$  위에서 정의됩니다.
- 두 함수가 같은 열린집합 위에서 정의되어 있다면, 이들을 더하고 곱할 수 있습니다. 다시 말해,  $\mathcal{O}_V(U)$ 는 환입니다.
- 함수  $f \in \mathcal{O}_V(U)$ 가 주어지면, 이를 더 작은 열린 부분집합  $W \subseteq U$ 로 제한할 수 있습니다.

이것들이 우리가 전층에 부과할 연산들입니다.

### §82.2.i 통상적인 정의

그럼 여기 전층의 공식적인 정의가 있습니다. 우리는 환의 전층만을 정의할 것이지만, 집합의 전층, 아벨 군의 전층 등을 정의하는 것도 가능합니다.

**정의 82.2.1.** 위상 공간  $X$ 에 대해,  $\text{OpenSets}(X)$ 가  $X$ 의 열린집합들을 나타낸다고 합시다.

**정의 82.2.2.** 공간  $X$  위의 환의 **전층**은 다음과 같은 함수입니다

$$\mathcal{F}: \text{OpenSets}(X) \rightarrow \text{Rings}$$

즉 각 열린집합에 환  $\mathcal{F}(U)$ 가 대응된다는 뜻입니다.  $\mathcal{F}(U)$ 의 각 원소는 **단면**이라 불립니다. 또한 임의의  $U_1 \subseteq U_2$ 에 대해 **제한 사상**이 갖추어져 있는데, 이는 다음과 같은 사상입니다

$$\text{res}_{U_1, U_2}: \mathcal{F}(U_2) \rightarrow \mathcal{F}(U_1).$$

이 사상은 두 공리를 만족합니다:

- 사상  $\text{res}_{U, U}$ 는 항등사상이며, 그리고
- 다음과 같이 중첩된 부분집합들이 있을 때마다

$$U_{\text{작은}} \subseteq U_{\text{중간}} \subseteq U_{\text{큰}}$$

도식이

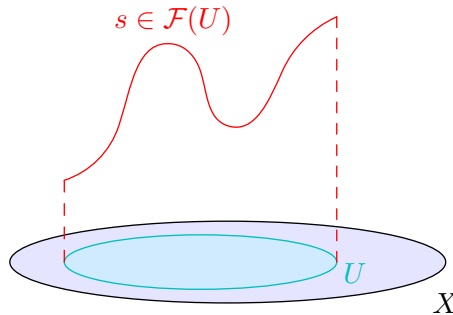
$$\begin{array}{ccc} \mathcal{F}(U_{\text{큰}}) & \xrightarrow{\text{res}} & \mathcal{F}(U_{\text{중간}}) \\ & \searrow \text{res} & \downarrow \text{res} \\ & & \mathcal{F}(U_{\text{작은}}) \end{array}$$

가환입니다.

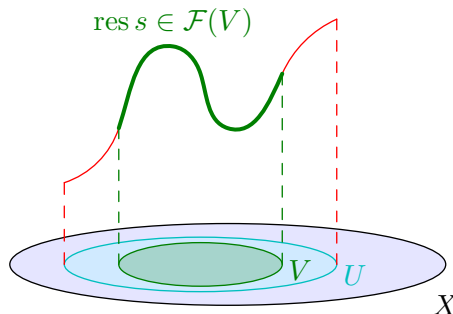
**정의 82.2.3.**  $\mathcal{F}(X)$ 의 원소를 **전역 절단(global section)**이라고 부릅니다.

**표기의 남용 82.2.4.**  $s \in \mathcal{F}(U_2)$ 가 어떤 절단이고  $U_1 \subseteq U_2$ 일 때,  $\text{res}_{U_1, U_2}(s)$ 라고 쓰는 대신  $s|_{U_1}$ 이라고 쓰겠습니다: " $U_1$ 으로 제한된  $s$ ". 이는 표기의 남용인데, 절단  $s$ 는 그저 어떤 환의 원소일 뿐이며, 가장 추상적인 경우에는 함수로서의 자연스러운 해석을 갖지 않을 수도 있기 때문입니다.

절단을 그려볼 수 있는 한 가지 방법이 있습니다. 우리가 흔히 다루는 모든 예시에서, 층은 열린집합  $U$ 에 대해 함수를 반환합니다. 그래서 우리는 공간  $X$ 와 열린집합  $U$ 를 그린 다음, 절단  $s$ 를 나타내기 위해 " $U$  위의 함수"를 그리고자 합니다. 조잡하게나마, 우리가 초등학교에서 함수를 그리도록 배운 방식대로, 곡선의  $xy$ -그래프를 그려서  $s$ 를 나타내겠습니다.



그러면 제한은, 말하자면, 절단의 일부만을 취하는 것에 해당합니다.



이 모든 것은 아직 꿈에 불과한데, 실제로  $s$ 는 어떤 환의 원소이기 때문입니다. 하지만 이 장이 끝날 무렵에는 우리의 꿈을 현실로 만들 수 있게 될 것입니다.

### 예제 82.2.5 (준층의 예시)

- (a) 아핀 대수다양체  $V$ 에 대해,  $\mathcal{O}_V$ 는 물론 층이며,  $\mathcal{O}_V(U)$ 는  $U$  위의 정칙 함수들의 환입니다. 제한 사상은 단지  $U_1 \subseteq U_2$ 일 때 함수  $s \in \mathcal{O}_V(U_2)$ 가 함수  $s|_{U_1} \in \mathcal{O}_V(U_1)$ 로도 생각될 수 있다는 것을 말할 뿐이며, 이 때문에 "제한(restriction)"이라는 이름이 붙었습니다. 그러면 도식의 가환성이 뒤따릅니다.
- (b)  $X \subseteq \mathbb{R}^n$ 을 열린집합이라 합시다. 그러면  $X$  위의 매끄러운/미분가능한/등등의 함수로 이루어진 층이 존재합니다. 사실, 임의의 다양체  $M$ 에 대해서도 같은 구성을 할 수 있습니다.
- (c) 마찬가지로,  $X \subseteq \mathbb{C}$ 가 열린집합이면,  $X$  위의 정칙 함수로 이루어진 층을 구성할 수 있습니다.

이 모든 예시에서, 절단  $s \in \mathcal{F}(U)$ 는 실제로 공간 위의 함수이지만, 일반적으로는 반드시 그럴 필요는 없습니다.

실제로는, 제한 사상에 대해 생각하는 것이 도움이 되기보다 오히려 더 헷갈릴 수 있습니다. 다음과 같이 말하는 편이 낫습니다:

준층은 "성질  $P$ 를 갖는 함수들의 환을 반환하는 것"으로 생각해야 합니다.

### §82.2.ii 범주론적 정의

범주론을 정말 좋아하신다면, 우리는 동치이면서 더 짧은 두 번째 정의를 줄 수 있습니다. 저 자신도 범주를 사랑하는 사람이지만, 저는 이 정의가 덜 직관적이라고 생각합니다. 그러나 그 간결함은 첫 번째 정의를 기억하는 데 도움이 됩니다.

**표기의 남용 82.2.6.** 표기의 남용으로,  $\text{OpenSets}(X)$  역시 포함관계에 의한 순서 범주로 생각될 것입니다. 따라서  $\emptyset$ 은 시작 대상이고 전체 공간  $X$ 는 끝 대상입니다.

**정의 82.2.7.**  $X$  위의 환의 **준층(pre-sheaf)**은 반변 함자

$$\mathcal{F}: \text{OpenSets}(X)^{\text{op}} \rightarrow \text{Rings}.$$

**연습문제 82.2.8.** 이 정의들이 동치임을 확인하십시오.

특히,  $\text{Rings}$ 를 우리가 원하는 어떤 범주로든 대체하는 것이 가능합니다. 우리는 당분간 그렇게 할 필요는 없겠지만, 언급할 가치는 있습니다.

## §82.3 줄기와 싹

**이 절의 대표적인 예:** 싹매끄러운 함수의 싹은 도함수를 알려주지만, 정칙 함수의 싹은 함수 전체를 결정합니다.

앞서 언급했듯이, 이전 절의 유용한 그림들은 여전히 비유에 불과한데, "값"이라는 개념이 없기 때문입니다. "줄기"와 "싹"이라는 단어를 추가함으로써, 우리는 실제로 이를 바꿀 수 있습니다.

**정의 82.3.1.**  $\mathcal{F}$ 를 (환의) 준층이라 합시다. 각 점  $p$ 에 대해, 우리는 **줄기(stalk)**  $\mathcal{F}_p$ 를 다음 집합으로 정의합니다

$$\{(s, U) \mid s \in \mathcal{F}(U), p \in U\}$$

다음을 만족시키는 동치관계  $\sim$ 을 법으로 하여

$$(s_1, U_1) \sim (s_2, U_2) \quad \text{만약} \quad s_1|_V = s_2|_V$$

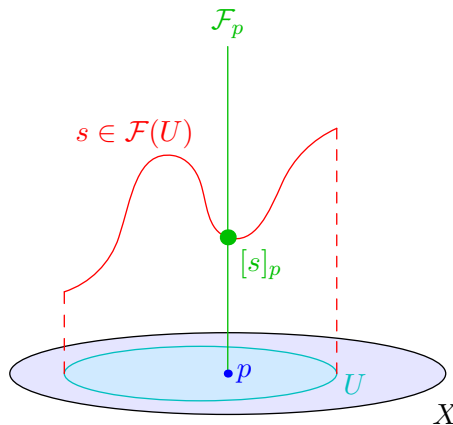
$V \ni p$ 이고  $V \subseteq U_1 \cap U_2$ 인 어떤 열린집합  $V$ 에 대해 그러합니다. 이 동치류 자체를 **씩**이라고 부릅니다.

**정의 82.3.2.** 점  $p$ 에서 주어진  $s \in \mathcal{F}(U)$ 의 **씩**은  $(s, U) \in \mathcal{F}_p$ 에 대한 동치류입니다. 이를  $[s]_p$ 로 표기합니다.

씩을 순서쌍으로 생각하는 것은 거의 쓸모가 없는데, 집합  $U$ 가 임의로 작아질 수 있기 때문입니다. 대신 **씩**을  $p$  근처에 있는 어떤 단면의 "조각"으로 생각해야 합니다. 올바른 사고방식을 위한 좋은 요약은 다음과 같을 것입니다:

**씩은 "풍부해진 값"이며, 줄기는 가능한씩들의 집합입니다.**

이것을 이전의 그림에 추가해 봅시다. 만약 우리가 단면을 계속  $xy$ -도표로 그리기를 고집한다면, 각 점  $p$  위에서 좋은 비유는  $p$ 에서 뺀어 나가는 수직선일 것입니다. 그러면 **씩**은 " $p$ 에서의  $s$ 의 풍부해진 값"이 될 것입니다. 우리는 이를 도표에서 그저 큰 점으로 그립니다. 주된 차이점은 **씩**이 문자 그대로 점  $p$  자체만이 아니라  $p$  주변의 작은 영역에서도 정보를 담고 있다는 의미에서 풍부해져 있다는 것입니다. 따라서 우리는  $p$ 에서 작은 점을 그리는 대신  $[s]_p$ 에 대해 큰 점을 그립니다.



계속하기 전에, 줄기가 그저 집합이 아니라 그 자체로 환이라는 점을 언급해도 좋을 것입니다: 우리는 분명히 풍부해진 값들을 더하거나 뺄 수 있습니다.

**정의 82.3.3.** 줄기  $\mathcal{F}_p$ 는 그 자체로 환으로 간주될 수 있습니다: 예를 들어, 덧셈은 다음과 같이 이루어집니다

$$(s_1, U_1) + (s_2, U_2) = (s_1|_{U_1 \cap U_2} + s_2|_{U_1 \cap U_2}, U_1 \cap U_2).$$

**예제 82.3.4** (실수 매끄러운 함수의 **씩**)

$X = \mathbb{R}$ 이라 하고,  $\mathcal{F}$ 를  $X$  위의 매끄러운 함수들의 준층이라 합시다 (즉  $\mathcal{F}(U)$ 는  $U$  위의 매끄러운 실숫값 함수들의 집합입니다).

전역 단면  $s: \mathbb{R} \rightarrow \mathbb{R}$  (따라서  $s \in \mathcal{F}(X)$ )와 0에서의 그 짝을 생각해 봅시다.

- (a) 당연히, 짝으로부터  $s(0)$ 을 읽어낼 수 있습니다.
- (b) 또한  $s'(0)$ 도 구할 수 있는데, 짝이 극한  $\lim_{h \rightarrow 0} \frac{1}{h}[s(h) - s(0)]$ 을 계산하기에 충분한 정보를 담고 있기 때문입니다.
- (c) 마찬가지로 이계도함수 등도 계산할 수 있습니다.
- (d) 그러나 짝으로부터 예를 들어  $s(3)$ 을 읽어낼 수는 없습니다. 예를 들어, **예제 29.4.4**의 함수를 생각해 봅시다,

$$s(x) = \begin{cases} e^{-\frac{1}{x-1}} & x > 1 \\ 0 & x \leq 1. \end{cases}$$

$s(3) = e^{-\frac{1}{2}}$ 이지만  $[\text{영함수}]_0 = [s]_0$ 임에 유의하십시오. 따라서 짝은 영함수와  $s$ 를 구별할 수 없습니다.

### 예제 82.3.5 (정칙함수의 짝)

정칙함수는 이 점에서 놀랍습니다.  $\mathbb{C}$  위의 정칙 함수들의 층  $\mathcal{F}$ 를 생각해 봅시다. 전역 단면  $s: \mathbb{C} \rightarrow \mathbb{C}$ 를 취합시다. 0에서  $s$ 의 짝이 주어지면,  $s(0)$ ,  $s'(0)$  등을 읽어낼 수 있습니다. 복소해석학의 기적은 영점에서  $s$ 의 도함수들을 아는 것만으로  $s$  전체를 재구성하기에 충분하다는 것입니다: 이제 우리는  $s$ 의 테일러 급수를 계산할 수 있습니다. 따라서 정칙함수의 짝은 함수 전체를 결정합니다; 이는 실함수의 경우보다 "더 많은 정보를 담고" 있습니다.

특히, 우리는 전층의 줄기를 구체적으로 기술할 수 있습니다:

$$\mathcal{F}_p = \left\{ \sum_{k \geq 0} c_k(z-p)^k \mid p \text{ 근방에서 수렴하는} \right\}.$$

예를 들어, 이는  $p$  자체에 극이 없는 한 유리형 함수의 짝을 포함합니다.

그리고 물론, 우리의 대수기하학 예시가 있습니다. 이 예시는 나중에 많이 중요해질 것이므로 지금 신중하게 다루겠습니다.

**표기의 남용 82.3.6.**  $(\mathcal{O}_X)_p$ 라고 쓰는 대신  $\mathcal{O}_{X,p}$ 라고 쓰겠습니다.

### 정리 82.3.7 ( $\mathcal{O}_V$ 의 줄기)

$V \subseteq \mathbb{A}^n$ 이 다양체이고  $p \in V$ 가 한 점이라고 합시다. 그러면

$$\mathcal{O}_{V,p} \cong \left\{ \frac{f}{g} \mid f, g \in \mathbb{C}[V], g(p) \neq 0 \right\}.$$

증명.  $U \subseteq V$  위의 정칙함수  $\varphi$ 는  $\mathbb{C}[V]$ 의 두 함수의 몫이 "국소적으로" 되는  $U$  위의 함수여야 합니다. 그러나 우리는  $p$  근처의 줄기를 살펴보고 있으므로, 짝은  $p$ 에서의 표현 선택까지만 신경을 쓰며, 따라서 우리는 다음과 같이 써도 됩니다

$$\mathcal{O}_{V,p} = \left\{ \left( \frac{f}{g}, U \right) \mid U \ni p, f, g \in \mathbb{C}[V], U \text{에서 } g \neq 0 \right\}$$

같은 관계를 법으로 합니다.

이제 다음 사상이

$$\mathcal{O}_{V,p} \rightarrow \text{원하는 우변} \quad \text{에 의해} \quad \left(\frac{f}{g}, U\right) \mapsto \frac{f}{g}$$

동형사상임을 주장합니다.

- 단사성: 우리는 복소 다항식을 다루고 있으므로, 유리함수는  $p$ 의 임의의 열린 근방에서의 거동에 의해 결정된다는 것을 알고 있습니다; 따라서 두 쌍의 대표원  $(\frac{f_1}{g_1}, U_1)$ 과  $(\frac{f_2}{g_2}, U_2)$ 가  $U_1 \cap U_2$ 에서 일치하는 것은 그것들이 실제로 같은 몫일 때, 그리고 그때만입니다.
- 전사성:  $U = D(g)$ 로 두십시오. □

### 예제 82.3.8 (원점에서 여러분이 좋아하는 다양체들의 줄기)

(a)  $V = \mathbb{A}^1$ 이라고 합시다; 그러면 각 점  $p \in V$ 에서  $\mathcal{O}_V$ 의 줄기는

$$\mathcal{O}_{V,p} = \left\{ \frac{f(x)}{g(x)} \mid g(p) \neq 0 \right\}.$$

원소의 예로는  $x^2 + 5$ ,  $p \neq 1$ 일 때  $\frac{1}{x-1}$ ,  $p \neq \pm 3$ 일 때  $\frac{x+7}{x^2-9}$  등이 있습니다.

(b)  $V = \mathbb{A}^2$ 이라고 합시다; 그러면 원점에서  $\mathcal{O}_V$ 의 줄기는

$$\mathcal{O}_{V,(0,0)} = \left\{ \frac{f(x,y)}{g(x,y)} \mid g(0,0) \neq 0 \right\}.$$

원소의 예로는  $x^2 + y^2$ ,  $\frac{x^3}{xy+1}$ ,  $\frac{13x+37y}{x^2+8y+2}$ 가 있습니다.

(c)  $V = \mathcal{V}(y - x^2) \subseteq \mathbb{A}^2$ 라고 합시다; 그러면 원점에서  $\mathcal{O}_V$ 의 줄기는

$$\mathcal{O}_{V,(0,0)} = \left\{ \frac{f(x,y)}{g(x,y)} \mid f, g \in \mathbb{C}[x,y]/(y - x^2), g(0,0) \neq 0 \right\}.$$

예를 들어,  $\frac{y}{1+x} = \frac{x^2}{1+x}$ 는 줄기 안에서 같은 원소를 나타냅니다. 사실,  $y$ 를 모든 곳에서  $x^2$ 로 치환하여 대표원의 표준적인 선택을 줄 수도 있으므로, 다음과 같이 써도 마찬가지로 옳습니다

$$\mathcal{O}_{V,(0,0)} = \left\{ \frac{f(x)}{g(x)} \mid g(0) \neq 0 \right\}$$

이것은 첫 번째 예와 같습니다.

**비고 82.3.9 (범주를 사랑하는 이들을 위한 여담)** — 여러분은  $\mathcal{F}_p$ 가 마치 " $p \in U$ 인 모든  $\mathcal{F}(U)$ 가 함께 모인 것"처럼 보인다는 것을 눈치챌 수도 있습니다. 그리고 실제로,  $\mathcal{F}_p$ 는  $p \in U$ 인 모든  $\mathcal{F}(U)$ 로 이루어진 도식의 범주론적 쌍대극한입니다. 이것은 흔히 다음과 같이 씁니다

$$\mathcal{F}_p = \varinjlim_{U \ni p} \mathcal{F}(U)$$

따라서 쌍대극한을 갖는 임의의 범주에서 줄기를 정의할 수 있습니다. 다만 쌍에 대해

이야기하려면 그 범주가 구체적이어야 합니다.

## §82.4 층

**이 절의 대표적인 예:** 상수함수는 층이 아니지만, 국소적으로 상수인 함수는 층입니다.

우리는 국소적 거동을 연구하는 줄기에 매우 관심이 많으므로, 우리의 전층에 추가적인 국소적 조건을 부과할 것입니다. 이를 생각하는 한 가지 방법은 다음과 같습니다:

**층이란  $P$ 가 국소적 성질인 전층입니다.**

형식적 정의는 예시만큼 이를 명확히 밝혀주지는 않지만, 안타깝게도 예시가 의미를 갖기 위해서는 먼저 정의를 제시해야 합니다.

**정의 82.4.1.** 위상 공간  $X$  위의 **층**  $\mathcal{F}$ 란 다음 두 가지 추가 공리를 만족하는 전층입니다:  $U$ 가  $X$ 의 열린집합이고,  $U$ 가 열린집합  $U_\alpha \subseteq U$ 들로 덮여 있다고 합시다. 그러면:

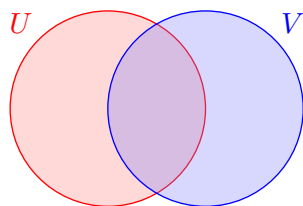
1. (동일성)  $s, t \in \mathcal{F}(U)$ 가 단면이고, 모든  $\alpha$ 에 대해  $s|_{U_\alpha} = t|_{U_\alpha}$ 이면,  $s = t$ 입니다.
2. (접합) 각  $\alpha$ 에 대해 단면  $s_\alpha \in \mathcal{F}(U_\alpha)$ 를 생각합시다. 다음이 성립한다고 합시다

$$s_\alpha|_{U_\alpha \cap U_\beta} = s_\beta|_{U_\alpha \cap U_\beta}$$

각  $U_\alpha$ 와  $U_\beta$ 에 대해. 그러면  $s|_{U_\alpha} = s_\alpha$ 를 만족하는  $s \in \mathcal{F}(U)$ 를 찾을 수 있습니다.

**비고 82.4.2 (공집합을 챙기는 이들을 위하여)** — 위의 공리들은  $\mathcal{F}$ 가 환들의 층일 때  $\mathcal{F}(\emptyset) = 0$  (영환)임을 함의합니다. 이는 실제로 필요해지기 전까지는 걱정할 가치가 없으므로, 방금 한 말은 잊어도 좋습니다.

이는 두 개의 열린집합만 있는 경우로 그림을 그려 보면 가장 잘 이해됩니다: 두 열린집합  $U$ 와  $V$ 를 생각해 봅시다. 그러면 층의 공리들은  $\mathcal{F}(U \cup V)$ ,  $\mathcal{F}(U \cap V)$ ,  $\mathcal{F}(U)$ ,  $\mathcal{F}(V)$ 에 관한 어떤 것을 말하고 있습니다.



그러면 함수들의 층에 대해, 그 공리들은 다음을 말하고 있습니다:

- $s$ 와  $t$ 가  $U \cup V$  위에서 (성질  $P$ 를 갖는) 함수이고  $s|_U = t|_U$ ,  $s|_V = t|_V$ 이면, 전체 합집합 위에서  $s = t$ 입니다. 이는 명백합니다.
- $s_1$ 이  $U$  위에서 성질  $P$ 를 갖는 함수이고  $s_2$ 가  $V$  위에서 성질  $P$ 를 갖는 함수이며, 두 함수가 겹치는 부분에서 일치한다면, 이들을 붙여 전체 공간 위의 함수  $s$ 를 얻을 수 있습니다: 이는 당연하지만, **함정은 이렇게 짜맞춘 함수도 성질  $P$ 를 가져야 한다는 것입니다** (즉  $\mathcal{F}(U \cup V)$ 의 원소여야 합니다). 바로 이 때문에  $P$ 가 국소적인지가 중요합니다.

그러므로 이 둘을 다음과 같이 요약할 수 있습니다: 겹치는 부분에서 일치하는  $U$ 와  $V$  위의 임의의 두 함수는  $U \cup V$  위의 유일한 함수로 붙여집니다. 범주론을 좋아한다면, 이를 **예제 69.2.1**에서 넌지시 언급했음을 기억할지도 모릅니다.

**연습문제 82.4.3** (범주론적 성향을 가진 이들을 위하여). 다음 도식이

$$\begin{array}{ccc} \mathcal{F}(U \cup V) & \longrightarrow & \mathcal{F}(U) \\ \downarrow & & \downarrow \\ \mathcal{F}(V) & \longrightarrow & \mathcal{F}(U \cap V) \end{array}$$

당겨오기 사각형임을 보이십시오.

이제 예시들을 살펴봅시다.

#### 예제 82.4.4 (층의 예시와 반례)

앞 절에서 계산한 줄기의 예시들은 모두 층의 예시였음에 주목하십시오. 더 자세한 내용은 다음과 같습니다:

- (a) 임의의 / 연속인 / 미분 가능한 / 매끄러운 / 정칙 함수들의 전층은 여전히 층입니다. 이는 어떤 함수가 연속임을 확인하려면 작은 열린 근방들만 한 번에 살펴보면 되기 때문입니다.
- (b)  $X = \mathbb{R}$ 이라 하고, 환들의 전층  $\mathcal{F}$ 를 다음과 같이 정의합시다:  

$$\mathcal{F}(U) = \{f: U \rightarrow \mathbb{R} \mid g|_U = f \text{를 만족하는 연속함수 } g: \mathbb{R} \rightarrow \mathbb{R} \text{가 존재합니다}\}.$$
 그러면  $\mathcal{F}$ 는 층이 아닙니다. 실제로  $\mathcal{F}((-1, 0))$ 에서의  $s_1(x) = 0$ 과  $\mathcal{F}((0, 1))$ 에서의  $s_2(x) = 1$ 은 (공집합인) 겹치는 부분에서 일치하지만, 이들은  $\mathcal{F}((-1, 0) \cup (0, 1))$ 의 원소로 붙여질 수 없습니다.
- (c) 복소 다양체  $V$ 에 대해,  $\mathcal{O}_V$ 는 층인데, 이는 정확히 우리의 정의가 국소적으로 다항식들의 몫이었기 때문입니다.
- (d) 공간  $X$  위의 상수 실함수들의 전층은 일반적으로 층이 아닌데, 이는 붙임 공리를 만족하지 못하기 때문입니다. 즉,  $U_1 \cap U_2 = \emptyset$ 인  $X$ 의 서로소인 열린집합들을 가정합시다. 그러면  $s_1$ 이  $U_1$  위의 상수 함수 1이고  $s_2$ 가  $U_2$  위의 상수 함수 2라면, 이들을  $U_1 \cup U_2$  위의 상수 함수로 붙일 수 없습니다.
- (e) 반면, 국소 상수 함수들은 실제로 층을 만들어 냅니다. (함수가 국소 상수라는 것은 모든 점에 대해 어떤 열린 근방 위에서 상수라는 뜻입니다.)

사실  $\mathbf{e}$ 의 층은 상수 함수 전층의 소위 층화라고 불리는 것인데, 이는 곧 정의하겠습니다.

## §82.5 층에서 단면은 싹의 수열"입니다"

**이 절의 대표적인 예:**  $U$  위의 실함수는 각  $p \in U$ 에 대해 어떤 국소 조건을 만족하는 실수  $f(p)$ 의 수열입니다. 유사하게, 단면  $s \in \mathcal{F}(U)$ 는 어떤 국소 호환 조건을 만족하는 싹의 수열입니다.

층 공리를 부과하면, 우리의 비유적 그림은 실제로 거의 완전해집니다. 함수가 각 점에서 값의 선택이어야 했던 것처럼, 단면은 각 줄기에서 싹의 선택이 될 것입니다.

**예제 82.5.1 (실함수 대 줄기(원소))**

$X$ 를 공간이라 하고  $\mathcal{F}$ 를 매끄러운 함수들의 층이라 합시다. 단면  $f \in \mathcal{F}(U)$ 를 취합시다.

- 함수로서  $f$ 는 국소적인 "매끄러움" 조건을 따르는, 모든 점  $p$ 에서의 값  $f(p) \in \mathbb{R}$ 의 선택일 뿐입니다.
- 이제  $f$ 를 줄기(원소)들의 수열로 생각해 봅시다. 모든 점  $p$ 에서 줄기  $[f]_p \in \mathcal{F}_p$ 는 위에서 설명한 값  $f(p)$ 를 우리에게 줍니다. 줄기는 이보다 훨씬 더 많은 데이터를 담고 있습니다: 예를 들어 줄기  $[f]_p$ 만으로도  $f'(p)$ 를 계산할 수 있습니다. 그럼에도 불구하고 우리는 이 비유를 확장하여  $f$ 를 각 점  $p$ 에서 줄기  $[f]_p \in \mathcal{F}_p$ 의 선택으로 생각합니다.

따라서 값  $f(p)$ 라는 개념을 썩  $[f]_p$ 로 대체할 수 있습니다. 이는 일반적인 층  $\mathcal{F}$ 에서  $s(p)$ 라는 개념은 정의되지 않지만  $[s]_p$ 라는 개념은 정의되기 때문에 유용합니다.

위 예시로부터 각 썩  $[s]_p$ 를 안다면 이것으로 전체 단면  $s$ 를 재구성할 수 있어야 함이 명백합니다. 층 공리로부터 이를 확인해봅시다:

**연습문제 82.5.2** (단면은 줄기에 의해 결정된다).  $\mathcal{F}$ 를 층이라 합시다. 다음 자연스러운 사상을 생각합시다

$$\mathcal{F}(U) \rightarrow \prod_{p \in U} \mathcal{F}_p$$

위에서 설명한 것입니다. 이 사상이 단사임을 보이십시오. 즉, 모든  $p \in U$ 에서  $s$ 의 썩들이 단면  $s$ 를 결정함을 보이십시오. ("항등" 층 공리가 필요하지만, "접합"은 필요하지 않습니다.)

그러나 이 사상은 명백히 전사가 아닙니다! 그럼에도 우리는 상(image)을 서술할 수 있습니다: 썩들의 수열  $(g_p)_{p \in U}$ 를 원하는데, 이때 모든 썩  $g_p$  근처에서 썩  $g_q$ 가  $g_p$ 와 "양립 가능"해야 합니다. 이를 정확히 서술하면 다음과 같습니다:

**정의 82.5.3.**  $\mathcal{F}$ 를 전층이라 하고  $U$ 를 열린집합이라 합시다. 썩들의 수열  $(g_p)_{p \in U}$  (각  $p$ 에 대해  $g_p \in \mathcal{F}_p$ )가 "국소적으로 짜맞출" 수 있다면 **양립 가능하다**고 합니다:

임의의  $p \in U$ 에 대해, 열린 근방  $U_p \ni p$ 와 그 위의 단면  $s \in \mathcal{F}(U_p)$ 가 존재하여 각  $q \in U_p$ 에 대해  $[s]_q = g_q$ 를 만족합니다.

직관적으로, 썩들은 각 개별 점  $q$  근처에서 어떤 단면으로 "짜맞춰져야" 합니다 (다만  $U$  전체에 대한 단면일 필요는 없습니다).

이 정의가 우리가 원하는 것임을 독자가 직접 확인해보도록 남겨두겠습니다:

**연습문제 82.5.4.**  $U$  위의 임의의 양립 가능한 썩들의 선택이  $U$ 의 한 단면으로 짜맞춰짐을 증명하십시오. (이때 "접합" 층 공리가 필요하지만 "동일성"은 필요하지 않습니다.)

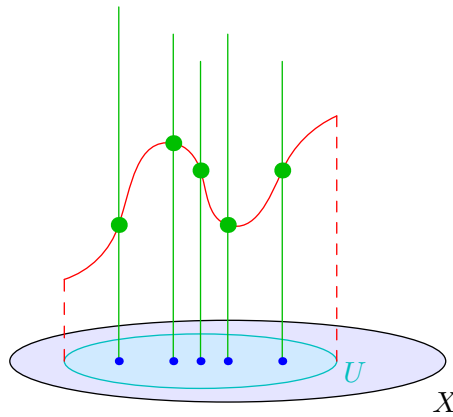
앞의 두 연습문제를 종합하면 다음을 얻습니다:

**정리 82.5.5 ("단면"은 그저 양립 가능한 쌍이다)**

$\mathcal{F}$ 를 층이라 합시다. 다음 사이에는 자연스러운 전단사가 존재합니다

- $\mathcal{F}(U)$ 의 단면들, 그리고
- $U$  위의 양립 가능한 쌍들의 수열들.

아래에서는 이를 그림으로 그려 보이는데, 줄기 하나만이 아니라 여러 개의 줄기를 그리고 그 위에 쌍들을 그립니다. 서로 다른 점에서의 줄기들은 서로 관련이 있을 필요가 없으므로, 이를 나타내기 위해 줄기들의 높이를 서로 다르게 그렸습니다. 그리고 유의할 점은, 쌍들이 충분히 커서 "서로 가까운" 쌍들끼리는 "양립 가능"해야 한다는 것입니다.



이는 예를 들어  $U$  위의 매끄러운 실숫값 함수가 국소 매끄러움 조건을 만족시키면서 각 점  $p \in U$ 에서 실수  $f(p) \in \mathbb{R}$ 를 선택하는 것과 정확히 유사합니다.

따라서 줄기라는 개념은 단면을 "함수"로 보는 관점을 되찾을 수 있게 해줍니다. 그러므로 이론적인 목적에서는,

**층 공리에 의하면, 단면은 양립 가능한 쌍들의 수열입니다.**

특히 이는 제한 사상을 다루기 쉽게 만들어 줍니다: 그저 쌍들의 수열을 절단하면 됩니다!

**§82.6 총화(선택)**

**이 절의 대표적인 예:** 상수 함수의 준층은 국소적으로 상수인 함수의 층이 됩니다.

아이디어는,  $\mathcal{F}$ 가 "성질  $P$ 를 갖는 함수"의 준층이라면, "국소적으로  $P$ 인 함수"의 층  $\mathcal{F}^{\text{sh}}$ 를 대응시켜 이들을 층으로 만들고자 한다는 것입니다. 우리는 이미 이에 대한 두 가지 예를 보았습니다:

**예제 82.6.1 (총화)**

- $X$ 가 위상 공간이고,  $\mathcal{F}$ 가  $X$ 의 열린집합들 위의 상수 함수들의 준층이라면,  $\mathcal{F}^{\text{sh}}$ 는 국소 상수 함수들의 층입니다.
- $V$ 가 아핀 다양체이고,  $\mathcal{F}$ 가 유리 함수들의 준층이라면,  $\mathcal{F}^{\text{sh}}$ 는 정칙 함수들의 층입니다(이는 국소적으로 유리적입니다).

이 절차는 줄기와 짝에 기반합니다. 층의 경우 절편이 호환되는 짝들의 수열에 대응함을 보았습니다. 준층의 경우에도 여전히 줄기와 짝을 정의할 수 있지만, 그 성질은 덜 좋을 것입니다. 하지만 초기 준층  $\mathcal{F}$ 가 주어지면, 우리는  $\mathcal{F}^{\text{sh}}$ 의 절편을 호환되는  $\mathcal{F}$ -짝들의 수열로 정의합니다.

**정의 82.6.2.** 준층  $\mathcal{F}$ 의 **층화**  $\mathcal{F}^{\text{sh}}$ 는 다음과 같이 정의됩니다

$$\mathcal{F}^{\text{sh}}(U) = \{\text{호환되는 } \mathcal{F}\text{-짝 } (g_p)_{p \in U} \text{의 수열}\}.$$

**질문 82.6.3.**  $\mathcal{F}^{\text{sh}}$ 의 제한 사상을 서술하여 정의를 완성하십시오.

**표기의 남용 82.6.4.** 앞으로도 저는 보통 마찬가지로 대충 다룰 것입니다: 층  $\mathcal{F}$ 를 정의할 때,  $\mathcal{F}(U)$ 가 무엇인지만 말할 것이며, 제한 사상  $\mathcal{F}(U_2) \rightarrow \mathcal{F}(U_1)$ 은 암묵적으로 두겠습니다.

이 구성은 절편  $(g_p)_{p \in U} \in \mathcal{F}^{\text{sh}}(U)$ 이 주어졌을 때 점  $p$ 에서의 짝이  $g_p$ 가 되도록 고안되었습니다:

**보조정리 82.6.5 (층화에 의해 보존되는 줄기)**

$\mathcal{F}$ 를 준층이라 하고  $\mathcal{F}^{\text{sh}}$ 를 그 층화라 합시다. 그러면 임의의 점  $q$ 에 대해 다음과 같은 동형사상이 존재합니다

$$(\mathcal{F}^{\text{sh}})_q \cong \mathcal{F}_q.$$

증명.  $(\mathcal{F}^{\text{sh}})_q$ 의 짝은  $((g_p)_{p \in U}, U)$ 의 꼴이며, 여기서  $g_p = (s_p, U_p)$  자체가  $\mathcal{F}_p$ 의 짝이고,  $q \in U$ 입니다. 그러면 그 동형사상은 다음과 같이 주어집니다

$$((g_p)_{p \in U}, U) \mapsto g_q \in \mathcal{F}_q.$$

역사상은 각  $g = (s, U) \in \mathcal{F}_q$ 에 대해 다음과 같이 주어집니다

$$g \mapsto ((g)_{p \in U}, U) \in (\mathcal{F}^{\text{sh}})_q$$

즉 짝들의 수열이 상수 수열입니다. □

앞으로 우리는 층을 경제적으로 구성하기 위해 층화를 사용할 것입니다. 그러나 실제로는 구성의 세부 사항이 중요하지 않은 경우가 많을 것입니다.

## §82.7 생각해 볼 만한 조금 더 어려운 문제

**문제 82A.**  $\mathcal{F}$ 가 이미 층이라면, 모든 열린집합  $U$ 에 대해  $\mathcal{F}(U) \cong \mathcal{F}^{\text{sh}}(U)$ 임을 증명하십시오.

**문제 82B.**  $X$ 를 두 점  $\{p, q\}$ 를 갖는 공간이라 하고  $\mathcal{F}$ 를 그 위의 층이라 합시다.  $\mathcal{F}_p = \mathbb{Z}/5\mathbb{Z}$ 이고  $\mathcal{F}_q = \mathbb{Z}$ 라 가정합시다.  $X$ 의 각 열린집합  $U$ 에 대해  $\mathcal{F}(U)$ 를 서술하십시오. 여기서

(a)  $X$ 에는 이산 위상이 주어져 있습니다.

(b)  $X$ 에는  $\emptyset, \{p\}, \{p, q\}$ 만이 열린집합으로 주어져 있습니다.

**문제 82C (초고층 층).**  $Y$ 를 위상 공간이라 합시다. 점  $p \in Y$ 와 환  $R$ 을 고정합시다. **초고층 층**은 다음과 같이 정의됩니다

$$\mathcal{F}(U) = \begin{cases} R & p \in U \\ 0 & \text{그렇지 않으면} \end{cases}$$

제한 사상은 자명한 방식으로 주어집니다.  $\mathcal{F}$ 의 모든 줄기를 계산하십시오.

(가능한 제안: 먼저  $Y$ 가 하우스도르프인 경우를 다루면, 직관이 올바른 답을 줄 것입니다. 그다음  $Y$ 의 모든 열린집합이  $p$ 를 포함하는 병적인 경우를 다루십시오. 그런 다음 일반적인 답을 구해보십시오.)

**문제 82D.**  $X$  위의 환의 층  $\mathcal{F}$ 가 있고  $s \in \mathcal{F}(X)$ 가 대역 절단면이라 하십시오.  $s$ 의 **지지집합**(support)을 다음과 같이 정의합니다

$$Z = \{p \in X \mid [s]_p \neq 0 \in \mathcal{F}_p\}.$$

$Z$ 가  $X$ 의 닫힌집합임을 보이십시오.

# 83 국소화

아핀 스킴을 정의하는 단계로 나아가기 전에, 국소화라는 또 하나의 대수적 구성을 제대로 다루는 데 시간을 들이겠습니다. 이는 필수적인데, 스킴을 정의할 때 모든 단면과 줄기가 실제로 이 구성을 이용해 얻어진다는 것을 알게 되기 때문입니다.

다소 우스운 슬로건을 하나 들자면 다음과 같습니다:

**국소화는 분모를 추가하는 기술입니다.**

아핀 다양체를 다룰 때  $\left\{ \frac{f}{g} \mid g(p) \neq 0 \right\}$ 와 같은 형태의 식이 끊임없이 등장했던 것을 기억하십시오. 요점은 우리가 많은 분모들을 도입했다는 것입니다. 국소화는 이를 일반적으로 수행하는 간결한 방법을 제공해 줍니다.

이는 또한 왜 이 연산이 "국소화"라고 불리는지를 설명해 줍니다: 우리는 "전역적인" 함수들의 집합에서 시작하여, "더 작은" 열린집합 위에서, 또는 점  $p$ 의 열린 근방에서 잘 정의되는 (더 큰) 함수들의 집합을 얻습니다.

물론 이것은 자리스키 위상이므로, "작다"는 것은 "특정 곡선들을 제외한 모든 곳"을 의미합니다.

표기법에 관한 참고: 앞으로는 환을  $R, S, \dots$ 가 아니라  $A, B, \dots$ 로 표기하는 것을 선호하겠습니다.

## §83.1 스포일러

앞으로 다룰 내용들을 미리 살펴보고, 무엇을 기대해야 할지 알 수 있도록 하겠습니다. 여기서 이해가 되지 않는 부분이 있어도 괜찮은데, 이는 단지 앞으로의 내용을 미리 암시하는 것일 뿐이기 때문입니다.

$V \subseteq \mathbb{A}^n$ 이라 하고, 간단히 하기 위해  $R = \mathbb{C}[V]$ 를 그 좌표환이라 합시다. 이전 절들에서 점  $p \in V$ 에 대해  $\mathcal{O}_V(D(g))$ 와  $\mathcal{O}_{V,p}$ 를 계산하는 방법을 살펴본 바 있습니다. 예를 들어,  $\mathbb{A}^1$ 을 택하고 점  $p$ 를 생각하면,  $\mathcal{O}_{\mathbb{A}^1}(D(x-p)) = \left\{ \frac{f(x)}{(x-p)^n} \right\}$ 이고  $\mathcal{O}_{\mathbb{A}^1,p} = \left\{ \frac{f(x)}{g(x)} \mid g(p) \neq 0 \right\}$ 입니다. 더 일반적으로는, 다음을 얻었습니다

$$\begin{aligned} \mathcal{O}_V(D(g)) &= \left\{ \frac{f}{g^n} \mid f \in R \right\} && \text{정리 78.6.1에 의해} \\ \mathcal{O}_{V,p} &= \left\{ \frac{f}{g} \mid f, g \in R, g(p) \neq 0 \right\} && \text{정리 82.3.7에 의해.} \end{aligned}$$

곧 국소화라 불리는 것을 정의할 텐데, 이는 위의 내용을 표현하는 좋은 방법을 제공해 줄 것입니다:  $R = \mathbb{C}[V]$ 가 좌표환이라면, 위의 것은 다음과 같이 축약될 것입니다

$$\begin{aligned} \mathcal{O}_V(D(g)) &= R[g^{-1}] \\ \mathcal{O}_{V,p} &= R_{\mathfrak{m}} \quad \text{여기서 } \{p\} = \mathcal{V}(\mathfrak{m}). \end{aligned}$$

앞의 것은 " $R$ 을  $g$ 에서 떨어뜨려 국소화한 것"이라 읽고, 뒤의 것은 " $R$ 을  $\mathfrak{m}$ 에서 국소화한 것"이라 읽을 것입니다.

더 일반적으로, 다음 장에서는 좌표환  $R$ 을 완전히 버리고 이를 일반적인 가환환  $A$ (여전히 함수들로 간주되는)로 대체할 것입니다. 우리는  $X = \text{Spec } A$ 라 불리는 환달린 공간을 구성할 것인데, 그 원소들은  $A$ 의 소 아이디얼이며, 이 공간에는 자리스키 위상과 층  $\mathcal{O}_X$ 가

갖추어져 있습니다. 층  $\mathcal{O}_X$ 를 정의하는 올바른 방법은 국소화를 사용하는 것임이 밝혀질 것입니다,

$$\begin{aligned}\mathcal{O}_X(D(f)) &= A[f^{-1}] \\ \mathcal{O}_{X,p} &= A_p\end{aligned}$$

임의의 원소  $f \in A$ 와 소 아이디얼  $\mathfrak{p} \in \operatorname{Spec} A$ 에 대해서 말입니다. 따라서 복소 아핀 다양체의 경우와 마찬가지로, 국소화는 층  $\mathcal{O}_X$ 를 거의 완전히 기술하는 방법을 제공해 줄 것입니다. 다시 말해,

국소화는 "전역적인" 정칙 함수들의 환으로부터 더 작은 열린집합 위의 정칙 함수들의 환을 정의하는, 순수하게 대수적인 방법입니다.

## §83.2 정의

**정의 83.2.1.** 부분집합  $S \subseteq A$ 가  $1 \in S$ 이고  $S$ 가 곱셈에 대해 닫혀 있으면 **곱셈적 집합**이라 합니다.

**정의 83.2.2.**  $A$ 를 환이라 하고  $S \subset A$ 를 곱셈적 집합이라 합시다. 그러면  $S^{-1}A$ 로 표기되는  $S$ 에서의  $A$ 의 **국소화**는 다음과 같은 분수들의 집합으로 정의됩니다

$$\{a/s \mid a \in A, s \in S\}$$

여기서 두 분수  $a_1/s_1 = a_2/s_2$ 가 같다고 선언하는 것은, 어떤  $s \in S$ 에 대해  $s(a_1s_2 - a_2s_1) = 0$  일 때입니다. 이 환에서의 덧셈과 곱셈은 자명한 방식으로 정의됩니다.

특히,  $0 \in S$ 이면  $S^{-1}A$ 는 영환입니다. 그러므로 우리는 보통  $0 \notin S$ 인 상황만을 다룹니다. 이제 아핀 스킴의 구성에 동기를 부여하게 될 두 가지 예를 간략히 제시하겠습니다.

### 예제 83.2.3 ( $\mathbb{C}[x]$ 의 국소화들)

$A = \mathbb{C}[x]$ 라 합시다.

(a)  $x$ 의 거듭제곱들의 집합  $S = \{1, x, x^2, x^3, \dots\}$ 을 생각해 봅시다. 그러면

$$S^{-1}A = \left\{ \frac{f(x)}{x^n} \mid f \in \mathbb{C}[x], n \in \mathbb{Z}_{\geq 0} \right\}.$$

다시 말해,  $x$ 에 대한 로랑 다항식을 얻습니다.

이것을 다음과 같이 알아볼 수 있습니다

$$\mathcal{O}_V(U) \text{ 여기서 } V = \mathbb{A}^1, U = V \setminus \{0\}.$$

즉 구멍 뚫린 직선의 절단들입니다. "쌍곡선 효과"에 따라, 이는 또한  $\mathbb{C}[x, y]/(xy - 1)$ 로도 표현할 수 있습니다.

(b)  $p \in \mathbb{C}$ 라 합시다.  $S = \{g(x) \mid g(p) \neq 0\}$ 이라 하면, 즉  $g(p) \neq 0$ 인 모든 분모를 허용한다고 합시다. 그러면

$$S^{-1}A = \left\{ \frac{f(x)}{g(x)} \mid f, g \in \mathbb{C}[x], g(p) \neq 0 \right\}.$$

이것을 줄기  $\mathcal{O}_{\mathbb{A}^1, p}$ 로 알아볼 수 있습니다. 이는 나중에 중요하게 쓰입니다.

**비고 83.2.4 (왜  $s$ 가 추가로 필요한가?)** — 더 단순한  $a_1 s_2 - a_2 s_1 = 0$ 을 사용할 수는 없는데, 그렇지 않으면 동치 관계가 추이적이지 않을 수 있기 때문입니다. 다음은 반례입니다: 다음을 취해 봅시다

$$A = \mathbb{Z}/12\mathbb{Z} \quad S = \{2, 4, 8\}.$$

그러면 예를 들어  $\frac{0}{1} = \frac{0}{2} = \frac{12}{2} = \frac{6}{1}$ 이 성립합니다. 따라서  $\frac{0}{1} = \frac{6}{1}$ 이 성립해야 하는데, 이는 첫 번째 정의에서만 참입니다. 물론  $A$ 가 정역이라면 (그리고  $0 \notin S$ 라면) 이는 무의미한 문제입니다.

대안으로, 이 더 단순한 관계에서 시작하여 추이적 폐포를 취할 수도 있는데, 이는 동치인 정의를 내놓습니다.

### 예제 83.2.5 (분수체)

$A$ 를 정역이라 하고  $S = A \setminus \{0\}$ 이라 합시다. 그러면  $S^{-1}A = \text{Frac}(A)$ 입니다.

## §83.3 원소를 제외한 국소화

**이 절의 대표적인 예:** 6을 제외하고 국소화한  $\mathbb{Z}$ 는  $\frac{m}{2^x 3^y}$  꼴의 분수를 갖습니다.

이제 우리가 가장 많이 필요로 할 국소화의 두 가지 특수한 경우에 초점을 맞춥니다; 하나는 이 절에서, 다른 하나는 다음 절에서 다룹니다.

**정의 83.3.1.**  $f \in A$ 에 대해,  $f$ 를 제외한  $A$ 의 국소화를  $A[1/f]$  또는  $A[f^{-1}]$ 로 표기하며, 이를  $\{1, f, f^2, f^3, \dots\}^{-1}A$ 로 정의합니다. ( $\{1, f, f^2, \dots\}$ 가 곱셈적임에 유의하십시오.)

**비고 83.3.2** — 문헌에서는  $A[1/f]$  대신  $A_f$ 라는 표기를 더 흔히 볼 수 있습니다. 이는 혼란스러운데, 다음 절에서 정의할  $A_p$ 가 거의 정반대의 것이기 때문입니다. 그래서 저는 이 더 시사적인 (하지만 더 긴) 표기를 선호합니다.

### 예제 83.3.3 (국소화의 몇 가지 산술적 예시)

(a) 6을 제외하고  $\mathbb{Z}$ 를 국소화합니다:

$$\mathbb{Z}[1/6] = \left\{ \frac{m}{6^n} \mid m \in \mathbb{Z}, n \in \mathbb{Z}_{\geq 0} \right\}.$$

따라서  $A[1/6]$ 은 분모가 오직 2와 3의 거듭제곱만으로 이루어진 유리수들로 구성됩니다. 예를 들어, 여기에는  $\frac{5}{12} = \frac{15}{36}$ 이 포함됩니다.

(b) 더 헛갈리는 예시가 있습니다: 원소 5를 제외하고  $\mathbb{Z}/60\mathbb{Z}$ 을 국소화하면,  $(\mathbb{Z}/60\mathbb{Z})[1/5] \cong \mathbb{Z}/12\mathbb{Z}$ 를 얻습니다. 왜 이렇게 되는지 생각해 보시기 바랍니다. 나중에 절 86.9에서 "기하학적" 이유를 살펴보겠습니다.

### 예제 83.3.4 (원소에서의 국소화, 대수기하학적 풍미)

우리는  $A$ 가 대수다양체의 좌표환이면,  $A[1/g]$ 가 기하학적으로  $\mathcal{O}_V(D(g))$ 로 해석됨을 보았습니다. 다음은 몇 가지 특수한 경우입니다:

(a) 앞서 보았듯이,  $A = \mathbb{C}[x]$ 이면,  $A[1/x] = \left\{ \frac{f(x)}{x^n} \right\}$ 은 로랑 다항식들로 구성됩니다.

(b)  $A = \mathbb{C}[x, y, z]$ 라 합시다. 그러면

$$A[1/x] = \left\{ \frac{f(x, y, z)}{x^n} \mid f \in \mathbb{C}[x, y, z], n \geq 0 \right\}$$

은 분모가  $x$ 의 거듭제곱인 유리 함수들입니다.

(c)  $A = \mathbb{C}[x, y]$ 라 합시다.  $y - x^2$ 를 제외하고 국소화하면 다음을 얻습니다

$$A[(y - x^2)^{-1}] = \left\{ \frac{f(x, y)}{(y - x^2)^n} \mid f \in \mathbb{C}[x, y], n \geq 0 \right\}$$

이제는 이것을  $\mathcal{O}_{\mathbb{A}^2}(D(y - x^2))$ 로 알아볼 수 있어야 합니다.

### 예제 83.3.5 (영인자가 있는 예시)

$A = \mathbb{C}[x, y]/(xy)$ 라고 합시다 (직관적으로 두 축의 좌표환입니다).  $x$ 에서 국소화한다고 가정합시다: 즉,  $x$ 를 분모로 허용하는 것입니다.  $A$ 에서  $xy = 0$ 이므로, 이제  $0 = x^{-1}(xy) = y$ 가 되어,  $A$ 에서  $y = 0$ 이 되고, 따라서  $y$ 는 완전히 사라집니다. 이로 부터 다음과 같은 환 동형사상을 얻습니다

$$A[1/x] \cong \mathbb{C}[x, 1/x].$$

나중에 아핀 스킴을 정의하고 나면, [절 86.14](#)에서 기하학적 직관을 이용해 이를 "볼" 수 있을 것입니다.

## §83.4 소 아이디얼에서의 국소화

**이 절의 대표적인 예:**  $\mathbb{Z}$ 를 (5)에서 국소화하면  $5 \nmid n$ 인 분수  $\frac{m}{n}$ 을 갖습니다.

**정의 83.4.1.**  $A$ 가 환이고  $\mathfrak{p}$ 가 소 아이디얼이면, 다음과 같이 정의합니다

$$A_{\mathfrak{p}} := (A \setminus \mathfrak{p})^{-1} A.$$

이를  **$\mathfrak{p}$ 에서의 국소화**라고 부릅니다.

**질문 83.4.2.** 위 정의에서  $S = A \setminus \mathfrak{p}$ 가 왜 곱셈적입니까?

이 특수한 경우가 중요한 이유는, 스킴의 줄기가 모두 이런 형태임을 보게 될 것이기 때문입니다. 사실, 아핀 대수다양체에 대해서도 마찬가지였습니다.

### 예제 83.4.3 (아핀 대수다양체와의 관계)

$V \subseteq \mathbb{A}^n$ 이라 하고,  $A = \mathbb{C}[V]$ 라 하고,  $p = (a_1, \dots, a_n)$ 을 한 점이라 합시다. 다음 극대 (따라서 소) 아이디얼을 생각해봅시다

$$\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n).$$

함수  $f \in A$ 가  $p$ 에서 영이 되는 것은  $f \pmod{\mathfrak{m}} = 0$ 인 것과 동치이며, 이는 다시  $f \in \mathfrak{m}$ 인 것과 동치임을 관찰하십시오. 따라서 [정리 82.3.7](#)에 의해 다음과 같이 쓸 수

있습니다

$$\begin{aligned}\mathcal{O}_{V,p} &= \left\{ \frac{f}{g} \mid f, g \in A, g(p) \neq 0 \right\} \\ &= \left\{ \frac{f}{g} \mid f \in A, g \in A \setminus \mathfrak{m} \right\} \\ &= (A \setminus \mathfrak{m})^{-1} A = A_{\mathfrak{m}}.\end{aligned}$$

따라서,  $\mathcal{O}_{V,p}$ 를 국소화로 간결하게 표현할 수도 있습니다.

이에 따라, 이런 맥락의 예시를 몇 가지 제시합니다.

**예제 83.4.4** (소에서의 국소화의 기하학적 예시)

(a)  $\mathfrak{m}$ 을  $A = \mathbb{C}[x]$ 의 극대 아이디얼  $(x)$ 라 합시다. 그러면

$$A_{\mathfrak{m}} = \left\{ \frac{f(x)}{g(x)} \mid g(0) \neq 0 \right\}$$

는 원점에서 극이 없는 유리함수들로 이루어집니다.

(b)  $\mathfrak{m}$ 을  $A = \mathbb{C}[x, y]$ 의 극대 아이디얼  $(x, y)$ 라 합시다. 그러면

$$A_{\mathfrak{m}} = \left\{ \frac{f(x, y)}{g(x, y)} \mid g(0, 0) \neq 0 \right\}.$$

(c)  $\mathfrak{p}$ 를  $A = \mathbb{C}[x, y]$ 의 소 아이디얼  $(y - x^2)$ 라 합시다. 그러면

$$A_{\mathfrak{p}} = \left\{ \frac{f(x, y)}{g(x, y)} \mid g \notin (y - x^2) \right\}.$$

이는 지금까지 봐온 것과 다소 다릅니다: 분모의 다항식은 포물선 위의 모든 점에서 영이 되지 않는 한,  $(1, 1)$ 과 같은 점에서 영이 되는 것이 허용됩니다. 이는 지금 우리가 익숙한 어떤 줄기에도 대응되지 않지만, 나중에는 대응될 것입니다 (그것은 "포물선의 일반점에서의 줄기"가 될 것입니다).

(d)  $A = \mathbb{C}[x]$ 라 하고 소 아이디얼  $(0)$ 에서 국소화합시다. 이는

$$A_{(0)} = \left\{ \frac{f(x)}{g(x)} \mid g(x) \neq 0 \right\}.$$

를 줍니다. 이는 그냥 모든 유리함수입니다.

**비고 83.4.5** (표기법의 철학) 다시 말하자면:

- 한 원소로부터 벗어나 국소화할 때는, 함수가 그 원소의 (영집합에서) 발산하는 것을 허용합니다;
- 소에서 국소화할 때는, 함수가 그 소의 (전체 영집합을) 제외한 모든 곳에서 발산하는 것을 허용합니다.

따라서 왜 이 두 표기법을 서로 반대라고 말하는지 알 수 있습니다.  
 "전체 영집합에서 발산하지 않을 수도 있는" 함수를 생각하는 것은 혼란스러울 수 있으므로, 소에서의 국소화를 생각하는 (바라건대) 더 직관적인 또 다른 방법은 함수가 그 소 아이디얼에 대응하는 점에서 발산하지 않아야 한다는 것입니다. 예를 들어,  $\mathfrak{p}$ 가  $A = \mathbb{C}[x, y]$ 에서 아이디얼  $(y - x^2)$ 이면,  $A_{\mathfrak{p}}$ 는 포물선 위의 일반점에서 발산하지 않는 함수들의 집합입니다.

#### 예제 83.4.6 (산술적 예시)

$\mathbb{Z}$ 를 몇 가지 다른 소에서 국소화합니다.

(a)  $\mathbb{Z}$ 를  $(0)$ 에서 국소화하면:

$$\mathbb{Z}_{(0)} = \left\{ \frac{m}{n} \mid n \neq 0 \right\} \cong \mathbb{Q}.$$

(b)  $\mathbb{Z}$ 를  $(3)$ 에서 국소화하면, 다음을 얻습니다

$$\mathbb{Z}_{(3)} = \left\{ \frac{m}{n} \mid \gcd(n, 3) = 1 \right\}$$

이는 분모가 3과 서로소인 유리수들의 환입니다.

#### 예제 83.4.7 (분수체)

$A$ 가 정역이면, 국소화  $A_{(0)}$ 는  $A$ 의 분수체입니다.

## §83.5 국소화의 소 아이디얼

이 절의 대표적인 예:  $A = \mathbb{Z}$ 인 경우의 예시.

이제 국소화된 환의 소 아이디얼을 어떻게 생각할 수 있는지 짚어보겠습니다.

#### 명제 83.5.1 ( $S^{-1}A$ 의 소 아이디얼)

$A$ 를 환이라 하고  $S \subseteq A$ 를 곱셈적 집합이라 합시다. 그러면 다음 사이에는 포함 관계를 보존하는 자연스러운 전단사가 존재합니다:

- $S^{-1}A$ 의 소 아이디얼들의 집합, 그리고
- $S$ 와 교차하지 않는  $A$ 의 소 아이디얼들의 집합.

증명. 준동형사상  $\iota: A \rightarrow S^{-1}A$ 를 생각해봅시다.  $S^{-1}A$ 의 임의의 소 아이디얼  $\mathfrak{q} \subseteq S^{-1}A$ 에 대해, 그 원상  $\iota^{\text{pre}}(\mathfrak{q})$ 는  $A$ 의 소 아이디얼입니다(문제 5C\*에 의함). 역으로,  $S$ 와 만나지 않는  $A$ 의 임의의 소 아이디얼  $\mathfrak{p} \subseteq A$ 에 대해,  $S^{-1}\mathfrak{p} = \left\{ \frac{a}{s} \mid a \in \mathfrak{p}, s \in S \right\}$ 는  $S^{-1}A$ 의 소 아이디얼입니다. 번거로운 확인을 통해 이것이 필요한 전단사를 만들어냄을 알 수 있습니다.  $\square$

실제로는 우리가 앞서 자세히 논의한 두 가지 특수한 경우 중 하나가  $S$ 인 따름정리를 거의 항상 사용하게 될 것입니다:

**따름정리 83.5.2 (국소화의 스펙트럼)**

$A$ 를 환이라 합시다.

- (a)  $f$ 가  $A$ 의 원소이면,  $A[1/f]$ 의 소 아이디얼들은  $f$ 를 원소로 포함하지 않는  $A$ 의 소 아이디얼들과 자연스럽게 전단사 관계에 있습니다.
- (b)  $\mathfrak{p}$ 가  $A$ 의 소 아이디얼이면,  $A_{\mathfrak{p}}$ 의 소 아이디얼들은  $\mathfrak{p}$ 의 부분집합인  $A$ 의 소 아이디얼들과 자연스럽게 전단사 관계에 있습니다.

증명. (b) 부분은 자명합니다. 소 아이디얼이  $A \setminus \mathfrak{p}$ 와 만나지 않는 것은 정확히 그것이  $\mathfrak{p}$ 에 포함될 때입니다. (a) 부분에서는  $f$ 의 어떤 거듭제곱도 포함하지 않는  $A$ 의 소 아이디얼을 원합니다. 그런데 만약 그 아이디얼이 소 아이디얼이고  $f^n$ 을 포함한다면,  $f$  또는  $f^{n-1}$  중 하나를 포함해야 하므로, 적어도 소 아이디얼에 대해서는 이 두 조건이 동치입니다.  $\square$

표기법이 다시 한번 다소 성가시다는 점에 유의하십시오. 어쨌든 그림을 확실히 하기 위해 몇 가지 예시를 들어보겠습니다.

**예제 83.5.3 ( $\mathbb{Z}[1/6]$ 의 소 아이디얼)**

$\mathbb{Z}$ 를 원소 6에서 벗어나 국소화한다고, 즉  $\mathbb{Z}[1/6]$ 을 생각해봅시다. 앞서 살펴본 것처럼,

$$\mathbb{Z}[1/6] = \left\{ \frac{n}{2^x 3^y} \mid n \in \mathbb{Z}, x, y \in \mathbb{Z}_{\geq 0} \right\}.$$

분모가 오직 2와 3의 거듭제곱만을 갖는 유리수들로 이루어져 있습니다.  $(5) \subset \mathbb{Z}[1/6]$ 이 소 아이디얼임에 주목하십시오: 즉  $\mathbb{Z}[1/6]$ 의 원소 중 분자가 5로 나누어떨어지는 것들입니다. 마찬가지로 (7), (11), (13), ... 그리고 심지어 (0)도  $\mathbb{Z}[1/6]$ 의 소 아이디얼을 이룹니다.

하지만 (2)와 (3)은 더 이상 소 아이디얼에 대응하지 않습니다. 실제로  $\mathbb{Z}[1/6]$ 에서는  $(2) = (3) = (1)$ , 즉 환 전체가 됩니다.

**예제 83.5.4 ( $\mathbb{Z}_{(5)}$ 의 소 아이디얼)**

$\mathbb{Z}$ 를 소수 (5)에서 국소화한다고 합시다. 앞서 살펴본 것처럼,

$$\mathbb{Z}_{(5)} = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z}, 5 \nmid n \right\}.$$

분모가 5로 나누어떨어지지 않는 유리수들로 이루어져 있습니다. 이는 정역이므로, (0)은 여전히 소 아이디얼입니다. 소 아이디얼이 하나 더 있습니다: (5), 즉 분자가 5로 나누어떨어지는 원소들입니다.

다른 소 아이디얼은 없습니다: 만약  $p \neq 5$ 인 유리 소수라면, 다시  $(p) = (1)$ , 즉 환 전체가 됩니다.

**§83.6 몫환의 소 아이디얼**

여기까지 온 김에, 몫  $A/I$ 의 소 아이디얼은 (국소화에 대한 이전 절에서와 마찬가지로)  $A$ 의 소 아이디얼로 해석할 수 있다는 점을 언급하겠습니다. 만약 그 문제를 풀어봤다면 오래전 **문제 4D\***에서 이를 기억하실 수도 있겠지만, 우리의 목적상 실제로 관심 있는 것은 소 아이디얼뿐입니다.

**명제 83.6.1** ( $A/I$ 의 소 아이디얼)

$A$ 가 환이고  $I$ 가 (반드시 소 아이디얼일 필요는 없는) 임의의 아이디얼이라면,  $A/I$ 의 소 (또는 극대) 아이디얼은  $I$ 의 초집합인  $A$ 의 소 (또는 극대) 아이디얼과 전단사 관계에 있습니다. 이 전단사는 포함 관계를 보존합니다.

증명. 몫 준동형사상  $\psi: A \rightarrow A/I$ 를 생각해봅시다. 임의의 소 아이디얼  $\mathfrak{q} \subseteq A/I$ 에 대해, 그 원상  $\psi^{\text{pre}}(\mathfrak{q})$ 는 소 아이디얼입니다 (문제 5C\*에 의함). 역으로,  $I \subseteq \mathfrak{p} \subseteq A$ 인 임의의 소 아이디얼  $\mathfrak{p}$ 에 대해,  $\mathfrak{p} \pmod{I}$ 를 살펴보면  $A/I$ 의 소 아이디얼을 얻습니다. 성가신 확인 과정을 거치면 이것이 원하는 전단사를 만들어냄을 알 수 있습니다. 이 또한 포함 관계를 보존하며 — 이로부터 극대 아이디얼에 대해서도 같은 명제가 성립합니다.  $\square$

**예제 83.6.2** ( $\mathbb{Z}/60\mathbb{Z}$ 의 소 아이디얼)

환  $\mathbb{Z}/60\mathbb{Z}$ 은 세 개의 소 아이디얼을 갖습니다:

$$\begin{aligned}(2) &= \{0, 2, 4, \dots, 58\} \\ (3) &= \{0, 3, 6, \dots, 57\} \\ (5) &= \{0, 5, 10, \dots, 55\}.\end{aligned}$$

$\mathbb{Z}$ 로 돌아가보면, 이들은  $60\mathbb{Z} = \{\dots, -60, 0, 60, 120, \dots\}$ 의 초집합인 세 개의 소 아이디얼에 대응됩니다.

**§83.7 국소화는 몫과 교환됩니다**

**이 절의 대표적인 예:**  $(\mathbb{C}[x, y]/(xy))[1/x] \cong \mathbb{C}[x, x^{-1}]$ .

여기까지 온 김에, 몫환에서의 국소화를 계산할 수 있게 해주는 가환대수학의 유용한 결과 하나를 언급하겠습니다. 이는 놀라울 정도로 직관적이지 않습니다. 절 85.4.ii에 도달하기 전까지는 이것에 신경 쓸 이유가 없을 것이며, 따라서 이는 우리가 순수하게 대수적인 사실을 (그리고 실제로) 이렇게 일찍 진술할 수 있다는 점을 강조하기 위해서만 미리 배치된 것입니다. 물론 당장은 이것이 필요하지 않겠지만 말입니다.

다음과 같은 몫환이 있다고 합시다

$$A/I = \mathbb{C}[x, y]/(xy)$$

그리고 이 환을 원소  $x$ 에서 벗어나 국소화하려고 한다고 합시다. (엄밀히 말하자면, 실제로는 몫환의 원소인  $x \pmod{xy}$ 에서 벗어나 국소화하는 것이지만, 그냥 이를  $x$ 라고 부르겠습니다.) 표기법조차 금세 어색해진다는 것을 알게 될 것입니다:

$$(\mathbb{C}[x, y]/(xy))[1/x] \tag{83.1}$$

이는 생각하기 어려운데, 여기 등장하는 원소들이 몫의 일부이기 때문입니다: 예를 들어

$$\frac{1 \pmod{xy}}{x \pmod{xy}}$$

이것을 어떻게 생각해야 할까요? 여기 관여하는 영인자들만으로도 이미 불편함을 느끼실 수 있습니다.

하지만 사실 국소화를 먼저 해도 된다는 것이 밝혀지는데, 이 경우 답은 다음과 같습니다

$$\mathbb{C}[x, y, 1/x]/(xy) \tag{83.2}$$

그리고 이는  $\mathbb{C}[x, x^{-1}, y]/(y) \cong \mathbb{C}[x, x^{-1}]$ 가 됩니다.

이는 자명해 보일 수 있지만, 여러분이 예상하는 것만큼 명백하지는 않습니다. 여기에는 표기법상의 눈속임이 존재합니다:

- (83.1)에서, 표기  $(xy)$ 는  $\mathbb{C}[x, y]$ 의 아이디얼을 나타냅니다 — 즉, 집합  $xy\mathbb{C}[x, y]$ 입니다.
- (83.2)에서 표기  $(xy)$ 는 이제  $\mathbb{C}[x, x^{-1}, y]$ 의 아이디얼을 나타냅니다 — 즉, 집합  $xy\mathbb{C}[x, x^{-1}, y]$ 입니다.

그러니 정리의 진술을 적는 것조차 형편없어 보일 수밖에 없습니다.

일반적으로, 우리가 말하고자 하는 것은 만약 아이디얼  $I$ 를 갖는 환  $A$ 가 있고  $S$ 가  $A$ 의 어떤 곱셈적 부분집합이라면,

$$\text{통속적으로 말하면: } S^{-1}(A/I) = (S^{-1}A)/I''.$$

라는 것입니다. 하지만 여기에는 두 가지 잘못된 점이 있습니다:

- 주된 문제는 위에서 보았듯이  $I$ 가  $S^{-1}A$ 의 아이디얼이 아니라는 것입니다. 이는 대신  $S^{-1}I$ 를 사용함으로써 해결되는데, 이는  $x \in I$ 이고  $s \in S$ 인 원소  $\frac{x}{s}$ 들로 이루어져 있습니다. 앞서 보았듯이 실제로는 이러한 구별이 보통 감춰지는데, 대개  $I = (a_1, \dots, a_n) \subseteq A$ 라고 쓰기 때문이며, 이 경우 새로운 아이디얼  $S^{-1}I \subseteq A$ 는 정확히 같은 방식으로  $(a_1, \dots, a_n)$ 이라고 표기할 수 있습니다. 다만 이제는  $S^{-1}A$ 의 부분집합으로 간주될 뿐입니다.
- 두 번째 문제는 엄밀히 말하면  $S$  역시  $A/I$ 의 부분집합이 아니라는 것입니다. 하지만 이는 몫 사상  $A \twoheadrightarrow A/I$  아래에서의  $S$ 의 상을 대신 사용함으로써 쉽게 해결됩니다. 사실 이는 앞선 예시에서 이미 본 바 있습니다:  $\mathbb{C}[x, y]/(xy)$ 를 국소화하려고 했을 때, 실제로는 원소  $x \pmod{xy}$ 에서 국소화하고 있었지만, (언제나처럼) 그냥 이를  $x$ 라고 표기했습니다.

그리하여 이 모든 말, 말, 말 끝에, 우리는 다음의 훌륭한 결과를 얻습니다:

#### 정리 83.7.1 (국소화는 몫과 교환됩니다)

$S$ 를 환  $A$ 의 곱셈 집합이라 하고,  $I$ 를  $A$ 의 아이디얼이라 합시다.  $\bar{S}$ 를 사영 사상  $A \twoheadrightarrow A/I$  아래에서의  $S$ 의 상이라 합시다. 그러면

$$\bar{S}^{-1}(A/I) \cong S^{-1}A/S^{-1}I$$

여기서  $S^{-1}I = \{\frac{x}{s} \mid x \in I, s \in S\}$ 입니다.

증명. 생략합니다; 정말로 궁금하다면 Atiyah-Macdonald가 이런 종류의 내용에 대한 적절한 참고문헌입니다.  $\square$

표기법이 매우 지저분합니다. 하지만 실제로 계산을 할 때는, 대신 다음과 같이 씁니다

$$\left(\mathbb{C}[x, y, z]/(x^2 + y^2 - z^2)\right)[1/x] \cong \mathbb{C}[x, y, z, 1/x]/(x^2 + y^2 - z^2)$$

또는 (소 아이디얼에서 국소화하는 예시로는)

$$\left(\mathbb{Z}[x, y, z]/(x^2 + yz)\right)_{(x, y)} \cong \mathbb{Z}[x, y, z]_{(x, y)}/(x^2 + yz)$$

등등입니다 — 세부 사항을 일부 숨기는 우리의 “실생활” 표기법의 실용성은 실제로 우리의 직관을 오도하기보다는 오히려 이끌어 줍니다. 그러니 아마도 이 절의 교훈은, 몫환의 국소화를 계산할 때마다 잠시 의심을 접어 둔다면 대개 올바른 답을 얻을 수 있다는 것일지도 모릅니다.

이러한 사실들의 기하학적 해석은 나중에  $\text{Spec } A/I$ 를 다룰 때 살펴볼 것이며, 그때가 되면 더 자연스럽게 느껴질 것입니다.

## §83.8 생각해 볼 만한 조금 더 어려운 문제

**문제 83A.**  $A = \mathbb{Z}/2016\mathbb{Z}$ 이라 하고, 원소  $60 \in A$ 를 생각합시다.  $A[1/60]$ , 즉 60을 제외한  $A$ 의 국소화를 계산하십시오.

**문제 83B** (국소화의 단사성).  $A$ 를 환이라 하고,  $S \subseteq A$ 를 곱셈 집합이라 합시다. 사상  $A \rightarrow S^{-1}A$ 가 단사가 되기 위한 필요충분조건을 구하십시오.

**문제 83C\*** (국소환에 대한 암시).  $A$ 를 환이라 하고,  $\mathfrak{p}$ 를 소 아이디얼이라 합시다.  $A_{\mathfrak{p}}$ 는 극대 아이디얼을 몇 개 가집니까?

**문제 83D.**  $A$ 가 영이 아닌 환이고,  $A$ 의 모든 소 아이디얼  $\mathfrak{p}$ 에 대해  $A_{\mathfrak{p}}$ 가 정역이라고 하겠습니까.  $A$ 는 반드시 정역이어야 합니까?

# 84 아핀 스킴: 자리스키 위상

이제 층에 대해 잘 이해했으므로, 아핀 스킴을 정의할 수 있습니다. 이는 환달린 공간 (ringed space)이 될 것이므로, 다음을 정의해야 합니다.

- 점들의 집합,
- 그 위의 위상, 그리고
- 그 위의 구조층.

이 장에서는 처음 두 부분을 다루며, [장 85](#)에서 마지막 부분을 다룹니다.

간단한 참고 사항: [장 86](#)에는 아핀 스킴의 예시가 길게 나열되어 있습니다. 따라서 이 장에서 서술된 내용이 이해되지 않는다면, [장 86](#)를 훑어보며 그곳의 예시들이 더 도움이 되는지 살펴보는 것도 시도해 볼 만합니다.

## §84.1 조금 더 예고하자면

$\text{Spec } A$ 의 구성이 무엇을 할 것인지 설명해 보겠습니다.

$\mathbb{A}^n$ 의 경우, 점들의 집합으로  $\mathbb{C}^n$ 을, 함수의 환으로  $\mathbb{C}[x_1, \dots, x_n]$ 을 사용했으며, 그 후  $\mathbb{C}^n$ 의 점들의 집합이  $\mathbb{C}[x_1, \dots, x_n]$ 의 극대 아이디얼과 대응한다는 것을 언급했습니다. 아핀 스킴에서는 임의의 환  $A$ 를 취하여,  $A$  자체만으로부터 전체 구조를 생성할 것입니다. 그 최종 결과를  $\text{Spec } A$ , 즉  $A$ 의 **스펙트럼**이라 부릅니다. 앞서 만났던 아핀 대수다양체  $\mathcal{V}(I)$ 는 그저  $\text{Spec } \mathbb{C}[\mathcal{V}(I)] = \text{Spec } \mathbb{C}[x_1, \dots, x_n]/I$ 가 될 것이지만, 이제는 어떤 아이디얼  $I$ 도 취할 수 있게 되어, 마침내 "아핀 대수다양체" 장 끝의 표를 완성하게 됩니다.

이 점을 강조하자면:

**아핀 대수다양체  $V$ 에 대해, 좌표환  $\mathbb{C}[V]$ 의 스펙트럼은  $V$ 입니다.**

따라서  $\text{Spec}$ 을 대역 절단의 환을 취하는 연산의 반대 연산으로 생각할 수도 있는데, 이는 순전히 대수적으로 정의되어 아핀 대수다양체 자체의 내재적 성질(환  $\mathcal{O}_V$ )에만 의존하고 embedding에는 의존하지 않도록 되어 있습니다.

이러한 방식으로 아핀 스킴을 구성하면 세 가지 큰 일반화가 이루어질 것입니다:

1. 더 이상 대수적으로 닫힌 체  $\mathbb{C}$  위에서 작업할 필요가 없으며, 심지어 체 위에서 작업할 필요조차 없습니다. 이는 가장 무난한 일반화가 될 것입니다: 이를 위해 현재의 그림을 크게 조정할 필요는 없을 것입니다.
2. 우리는 근기(radical)가 아닌 아이디얼도 허용합니다:  $\text{Spec } \mathbb{C}[x]/(x^2)$ 는 우리가 그토록 오래 찾아왔던 이중점이 될 것입니다. 이는 "두꺼운" 혹은 "흐릿한" 점이라는 개념을 형식화할 수 있게 해 줄 것입니다.
3. 우리의 아핀 스킴에는 이른바 비닫힌점이 존재할 것입니다: 이는 공간 어딘가에 떠 다니고 있지만 어느 특정한 곳에도 있지 않은 것으로 시각화할 수 있는 점들입니다. (이들은 극대가 아닌 소 아이디얼에 대응할 것입니다.) 이것들은 익숙해지는 데 가장 오랜 시간이 걸리겠지만, 나아가면서 이러한 비닫힌점들이 실제로는 그 모습을 파악하고 나면 삶을 더 쉽게 만들어 준다는 것을 알게 될 것입니다.

## §84.2 점들의 집합

이 절의 대표적인 예:  $\text{Spec } \mathbb{C}[x_1, \dots, x_n]/I$ .

환  $A$ 에 대한 첫 번째 놀라움:

**정의 84.2.1.** 집합  $\text{Spec } A$ 는  $A$ 의 소 아이디얼들의 집합으로 정의됩니다.

이는 다소 놀랍게 느껴질 수 있는데,  $\text{Spec } A$ 에는 그저 극대 아이디얼만 있어야 한다고 추측했을 수도 있기 때문입니다. 그렇다면 나머지 아이디얼들은 무엇에 대응할까요? 답은, 이들이 이른바 비닫힌점 또는 생성점이 되어 공간 "어딘가에" 있지만 어느 특정한 곳에도 있지 않다는 것입니다. ("비닫힌"이라는 이름은 다음 장에서 설명됩니다.)

**비고 84.2.2** — 어느 때와 마찬가지로  $A$  자체는 소 아이디얼이 아니지만,  $(0)$ 은  $A$ 가 정역일 때만, 그리고 그럴 때에만 소 아이디얼입니다.

### 예제 84.2.3 (스펙트럼의 예시)

- (a)  $\text{Spec } \mathbb{C}[x]$ 는 모든  $a \in \mathbb{C}$ 에 대해 점  $(x - a)$ 를 포함하며, 이들은 우리가 기하학적으로  $\mathbb{A}^1$ 로 생각하는 것에 대응합니다. 여기에 더하여 점  $(0)$ 도 포함되는데, 이는 어느 특정한 곳에도 있지 않은 "비닫힌점"으로 생각됩니다.
- (b)  $\text{Spec } \mathbb{C}[x, y]$ 는 점  $(x - a, y - b)$ (극대 아이디얼들)뿐만 아니라 다시  $(0)$ 도 포함하는데, 이는 " $\mathbb{C}^2$ 의 어딘가에 있지만 특정할 수 없는 곳"으로 여겨지는 닫혀 있지 않은 점입니다. 또한 기약다항식  $f(x, y)$ 에 대응하는 닫혀 있지 않은 점들도 포함하는데, 예를 들어  $(y - x^2)$ 는 "포물선 위의 일반점"입니다.
- (c)  $k$ 가 체라면,  $\text{Spec } k$ 는 하나의 점으로 이루어지는데, 이는  $k$ 의 유일한 극대 아이디얼이  $(0)$ 이기 때문입니다.

### 예제 84.2.4 (복소 아핀 대수다양체)

$I \subseteq \mathbb{C}[x_1, \dots, x_n]$ 를 아이디얼이라고 합시다. **명제 83.6.1**에 의해, 집합

$$\text{Spec } \mathbb{C}[x_1, \dots, x_n]/I$$

은  $I$ 를 포함하는  $\mathbb{C}[x_1, \dots, x_n]$ 의 소 아이디얼들로 이루어집니다: 다시 말해,  $\mathcal{V}(I)$ 의 모든 닫힌 기약 부분다양체마다 하나의 점을 가집니다. 따라서 (극대 아이디얼  $(x_1 - a_1, \dots, x_n - a_n)$ 에 대응하는) "기하적인 점"들 외에도, 각 대수다양체를 따라 닫혀 있지 않은 점들이 있습니다.

닫혀 있지 않은 점들은 여러분에게 익숙하지 않은 것들입니다: 극대가 아닌 소 아이디얼마다 하나씩 존재합니다("기약 부분다양체"로 시각화됩니다). 저는 이들을 머릿속에서 파리처럼 시각화하기를 좋아합니다: 파리 소리를 들을 수 있으므로 방 안 어딘가에 떠 있다는 것은 알지만, 항상 움직이고 있기 때문에 정확히 어디에 있는지는 결코 알 수 없습니다. 그래서 소 아이디얼  $(0)$ 에 대응하는  $\text{Spec } \mathbb{C}[x, y]$ 의 일반점은 평면 전체에 떠 있고, 아이디얼  $(y - x^2)$ 에 대응하는 점은 포물선을 따라 떠 있는 식입니다.



[Wa]에서 가져온 이미지입니다.

**비고 84.2.5** (소 극대 아이디얼이 아닌 아이디얼들이 왜 포물선 전체에 대응하지 않을까요?) — 이에 대한 기하학적인 이유는 앞서 [절 83.4](#)에서 이미 살펴보았습니다: 환을 극대 아이디얼이 아닌 소 아이디얼에서 국소화하면 포물선의 어딘가에서 발산할 수 있지만 일반적으로는 그렇지 않은 함수들을 얻게 됩니다.

**예제 84.2.6** (스펙트럼의 추가 예시)

- (a)  $\text{Spec } \mathbb{Z}$ 는 모든 소수  $p$ 마다 하나의 점을 가지며, 여기에 더해 어딘가에 있지만 특정할 수 없는 일반점 하나를 가집니다.
- (b)  $\text{Spec } \mathbb{C}[x]/(x^2)$ 는  $(x)$ 만을 소 아이디얼로 가집니다.  $0 = x \cdot x$ 이므로 아이디얼  $(0)$ 은 소 아이디얼이 아닙니다. 따라서 위상 공간으로서,  $\text{Spec } \mathbb{C}[x]/(x^2)$ 는 한 점으로 이루어집니다.
- (c)  $\text{Spec } \mathbb{Z}/60\mathbb{Z}$ 는 세 개의 점으로 이루어집니다. 그것들은 무엇입니까?

## §84.3 스펙트럼 위의 자리스키 위상

**이 절의 대표적인 예:** 여전히  $\text{Spec } \mathbb{C}[x_1, \dots, x_n]/I$ 입니다.

이제  $\text{Spec } A$  위에 위상을 부여합니다.  $\text{Spec } A$  위의 점들이 소 아이디얼이므로, 점  $f$ 를  $\text{Spec } A$  위의 함수로 여기는 유비를 계속 이어갑니다. 즉:

**정의 84.3.1.**  $f \in A$ 이고  $\mathfrak{p} \in \text{Spec } A$ 라고 합시다. 그러면  $\mathfrak{p}$ 에서  $f$ 의 **값**은  $f \pmod{\mathfrak{p}}$ 로 정의되며, 이는  $A/\mathfrak{p}$ 의 한 원소입니다. 이를  $f(\mathfrak{p})$ 로 표기합니다.

**예제 84.3.2** ( $\mathbb{A}^n$ 에서의 소멸 궤적)

$A = \mathbb{C}[x_1, \dots, x_n]$ 이고,  $\mathfrak{m} = (x_1 - a_1, x_2 - a_2, \dots, x_n - a_n)$ 이  $A$ 의 극대 아이디얼이라고 합시다. 그러면 다항식  $f \in A$ 에 대하여,

$$f \pmod{\mathfrak{m}} = f(a_1, \dots, a_n)$$

$A/\mathfrak{m} \cong \mathbb{C}$ 라는 동일시와 함께.

**예제 84.3.3** ( $\text{Spec } \mathbb{Z}$  위의 함수)

$A = \mathbb{Z}$ 를 생각합시다. 그러면 2019는  $\text{Spec } A$  위의 함수입니다. 점 (5)에서의 값은  $4 \pmod{5}$ 이고; 점 (7)에서의 값은  $3 \pmod{7}$ 입니다.

실제로 이후에 나오는 모든 내용에서  $A$ 를  $\mathbb{C}[x_1, \dots, x_n]$ 으로,  $\text{Spec } A$ 를  $\mathbb{A}^n$ 으로 바꾸면, 모든 것이 상당히 익숙해질 것입니다.

**정의 84.3.4.**  $f \in A$ 라고 합시다.  $f$ 의 **소멸 궤적**을 다음과 같이 정의합니다:

$$\mathcal{V}(f) = \{\mathfrak{p} \in \text{Spec } A \mid f(\mathfrak{p}) = 0\} = \{\mathfrak{p} \in \text{Spec } A \mid f \in \mathfrak{p}\}.$$

더 일반적으로, 아핀의 경우와 마찬가지로, 아이디얼  $I$ 에 대한 소멸 궤적을 다음과 같이 정의합니다:

$$\begin{aligned} \mathcal{V}(I) &= \{\mathfrak{p} \in \text{Spec } A \mid f(\mathfrak{p}) = 0 \ \forall f \in I\} \\ &= \{\mathfrak{p} \in \text{Spec } A \mid f \in \mathfrak{p} \ \forall f \in I\} \\ &= \{\mathfrak{p} \in \text{Spec } A \mid I \subseteq \mathfrak{p}\}. \end{aligned}$$

마지막으로,  $\mathcal{V}(I)$  꼴의 집합들을 닫힌 집합으로 선언함으로써  $\text{Spec } A$  위의 **자리스키 위상**을 정의합니다.

이제 유용한 위상적 개념 몇 가지를 정의합니다:

**정의 84.3.5.**  $X$ 를 위상 공간이라고 합시다. 점  $p \in X$ 가 **닫힌 점**이라는 것은 집합  $\{p\}$ 가 닫혀 있다는 것입니다.

**질문 84.3.6** (필수). 점(즉 소 아이디얼)  $\mathfrak{m} \in \text{Spec } A$ 가 닫힌 점인 것과  $\mathfrak{m}$ 이 극대 아이디얼인 것이 동치임을 보이십시오.

**정의 7.2.4**에서 집합  $S$ 의 폐포(즉,  $S$ 를 포함하는 가장 작은 닫힌 집합)를  $\overline{S}$ 로 표기했음을 기억하십시오. 그러므로 닫힌 점  $p$ 는 그 폐포가 단지  $\{p\}$ 인 점으로도 생각할 수 있습니다. 따라서 자리스키 위상은 우리가 예전의 "기하학적" 점들을 단지 닫힌 점들로 다시 언급할 수 있게 해줍니다.

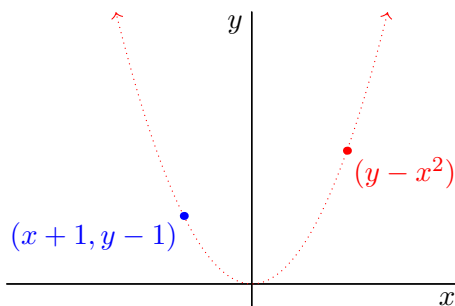
#### 예제 84.3.7 (비닫힌 점, 계속)

$A = \mathbb{C}[x, y]$ 라 하고  $\mathfrak{p} = (y - x^2) \in \text{Spec } A$ 라 합시다. 이는 포물선 위의 "일반점"입니다. 이 점은 닫혀 있지 않지만, 우리는 그 폐포를 계산할 수 있습니다:

$$\overline{\{\mathfrak{p}\}} = \mathcal{V}(\mathfrak{p}) = \{\mathfrak{q} \in \text{Spec } A \mid \mathfrak{q} \supseteq \mathfrak{p}\}.$$

이 폐포는 점  $\mathfrak{p}$ 뿐만 아니라  $(x - 2, y - 4)$ 와  $(x - 3, y - 9)$  같은 여러 극대 아이디얼  $\mathfrak{q}$ 도 포함합니다. 다시 말해, 포물선의 "일반점"의 폐포는 문자 그대로 실제로 포물선 위에 있는 모든 점들의 집합입니다(일반점도 포함).

이는  $\mathfrak{p}$ 를 포물선 "위 어딘가"에 떠 있지만 특별히 어디도 아닌 점으로 그려볼 수 있다는 것을 의미합니다. 그렇다면 폐포를 취했을 때 포물선 전체를 얻는다는 것이 이치에 맞습니다. 왜냐하면  $\mathfrak{p}$ 는 그 점들 중 "어느 것이든 될 수 있었기" 때문입니다.



**예제 84.3.8** ( $y$ 축의 일반점은  $x$ 축 위에 있지 않다)

다시  $A = \mathbb{C}[x, y]$ 라 합시다.  $\text{Spec } A$ 의  $x$ 축인  $\mathcal{V}(y)$ 를 생각해봅시다. 그다음  $y$ 축 위의 일반점인  $\mathfrak{p} = (x)$ 를 생각해봅시다. 다음을 관찰하십시오

$$\mathfrak{p} \notin \mathcal{V}(y).$$

이를 기하학적으로 말하면,  $y$ 축 위의 일반점은  $x$ 축 위에 놓여 있지 않다는 것입니다.

이제 우리는 단어 하나를 더 도입합니다:

**정의 84.3.9.** 위상 공간  $X$ 는 다음 두 조건 중 어느 하나라도 성립하면 **기약**이라 합니다:

- 공간  $X$ 는 두 개의 진 닫힌 부분집합의 합집합으로 쓸 수 없습니다.
- $X$ 의 임의의 두 공집합이 아닌 열린집합은 교차합니다.

$X$ 의 부분집합  $Z$ (보통 닫힌 것)는 부분공간으로서 기약일 때 기약이라 합니다.

**연습문제 84.3.10.** 위의 두 조건이 실제로 동치임을 보이십시오. 또한, 한 점의 폐포는 항상 기약임을 보이십시오.

이는 우리가 아핀 다양체에 대해 정의했던 "기약"의 유사 개념이지만, 이제는 위상적 정의입니다. 다만 실제로 이 정의는 자리스키 위상을 가진 공간에서만 유용합니다. 실제로 임의의 두 공집합이 아닌 열린집합이 교차한다면(그리고 점이 하나보다 많다면), 그 공간은 분명 하우스도르프가 아닙니다! 우리의 예전 아핀 다양체에서와 마찬가지로, 직관적으로는  $\mathcal{V}(xy)$ (두 직선의 합집합)는 기약이어서는 안 됩니다.

**예제 84.3.11** (가약 공간과 기약 공간)

(a) 닫힌집합  $\mathcal{V}(xy) = \mathcal{V}(x) \cup \mathcal{V}(y)$ 는 가약입니다.

(b) 평면 전체  $\text{Spec } \mathbb{C}[x, y]$ 는 기약입니다. 사실 이것이 참인 이유는 (일반점에 막 익숙해지는 중이라면 반직관적이지만) 단순합니다: 일반점  $(0)$ 이 모든 열린집합에 속하므로, 임의의 두 열린집합은 교차합니다.

그래서 실제로 일반점은 우리가 다음 부분을 일종의 편법으로 통과하게 해줍니다:

**명제 84.3.12** (정역의 스펙트럼은 기약이다)

$A$ 가 정역이면,  $\text{Spec } A$ 는 기약입니다.

증명. 그저  $(0)$ 이 소 아이디얼이고, 모든 열린집합에 속한다는 점만 주목하십시오.  $\square$

이는  $\mathbb{C}[x_1, \dots, x_n]/I$ 가 아핀 다양체로서 기약인 것은 정확히  $I$ 가 소 아이디얼일 때였던 예전의 고전적 결과와 비교해봐야 합니다. 이번에는 일반점이 실제로 우리를 위해 그 일을 대신 처리해줍니다: 일반점이 평면 어디에나 떠 있는 것이 허용된다는 사실이 추가적인 노력을 전혀 들이지 않고도  $\mathbb{A}^2$ 가 기약이어야 한다는 발상을 포착하게 해줍니다.

**비고 84.3.13** — 놀랍게도, 이 명제의 역은 거짓입니다: 우리는  $\text{Spec } \mathbb{C}[x]/(x^2)$ 가 오직 한 점만을 가짐을 보았으므로, 이는 분명 기약입니다. 하지만  $A = \mathbb{C}[x]/(x^2)$ 는

정역이 아닙니다. 따라서 이는 "비근기" 행태를 허용함으로써 생기는 기이함 중 하나입니다.

이 시점에서 여러분은 무언가를 눈치챘을지도 모릅니다:

**정리 84.3.14 (점들은 기약 닫힌집합과 전단사 관계에 있다)**

$X = \operatorname{Spec} A$ 를 생각해봅시다. 모든 기약 닫힌집합  $Z$ 에 대해,  $Z = \overline{\{p\}}$ 가 되는 점  $p$ 가 정확히 하나 존재합니다. (특히  $X$ 의 점들은  $X$ 의 닫힌 부분집합과 전단사 관계에 있습니다.)

증명의 아이디어. 점  $p$ 는 닫힌집합  $\mathcal{V}(p)$ 에 대응하며, 이것이 기약임을 보일 수 있습니다.  $\square$

이는 닫혀 있지 않은 점을 그리는 더 나은 방법을 제공합니다: 이러한 점들은 (한 점 이상으로 이루어진) 임의의 기약 닫힌집합을 따라 놓인 일반점들입니다.

이 지점에서,<sup>1</sup> 일반점의 진짜 정의를 드려도 좋을 것 같습니다.

**정의 84.3.15.** 위상 공간  $X$ 가 주어졌을 때, **일반점**  $\eta$ 는 그 폐포가 전체 공간  $X$ 인 점입니다.

따라서 우리에게,  $A$ 가 정역일 때  $\operatorname{Spec} A$ 는 일반점  $(0)$ 을 가집니다.

**표기의 남용 84.3.16.** 매우 주의 깊은 독자라면 제가  $\operatorname{Spec} \mathbb{C}[x, y]$ 에서  $(y - x^2)$ 를 “포물선을 따라가는 일반점”이라고 부르는 데 있어 약간 부주의하다는 것을 알아챘을지도 모릅니다. 실제로 일어나는 일은,  $\mathcal{V}(y - x^2)$ 가 닫힌집합이고, 위상 부분공간으로서 일반점  $(y - x^2)$ 를 가진다는 것입니다.

## §84.4 크룰 차원

놀랍게도, 위상만으로도 차원을 부여하기에 충분합니다. 아핀 스킴의 경우:

**정의 84.4.1.**  $A$ 를 가환환이라 합시다. 소 아이디얼의 사슬  $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subseteq A$ 를 생각합시다. 여기서  $n$ 을 길이라고 부릅니다. 가능한 모든  $n$ 의 상한을  $A$ 의 **크룰 차원**이라고 부릅니다.

크룰 차원은  $A$ 가 영환인 경우를 제외하면 항상 음이 아니며, 영환인 경우에는 관습적으로  $-1$  또는  $-\infty$ 가 사용됩니다.

이 정의는 여러분의 직관과 일치할 것입니다.

**예제 84.4.2 (크룰 차원의 예시)**

(a)  $\mathbb{C}[x_1, \dots, x_n]$ 은 크룰 차원  $n$ 을 가지며, 다음의 사슬이

$$(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \dots, x_n)$$

길이  $n$ 을 가집니다. 이는  $\operatorname{Spec} \mathbb{C}[x_1, \dots, x_n]$ 이  $\mathbb{A}^n$ 에 대응한다는 우리의 기대와 일치합니다.

(b)  $\mathbb{C}[x, y]/(y - x^2)$ 은 크룰 차원 1을 가지며, 다음의 사슬이

$$(y - x^2) \subsetneq (x, y)$$

<sup>1</sup>말장난은 의도한 것이 아닙니다

길이 1을 가집니다. 기하학적으로, 우리는  $(x, y)$ 를 원점으로,  $(y - x^2)$ 를 포물선 자체로 생각합니다.

(c)  $\mathbb{Z}$ 는 크룰 차원 1을 가집니다.

(d)  $\mathbb{Z}/(60)$ 은 크룰 차원 0을 가집니다; 이는 그저 세 점일 뿐입니다.

이는 위상 공간  $X$ 에 대해 더 일반적으로 할 수 있습니다: 공간의 크룰 차원은 기약 닫힌 부분공간의 사슬  $Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n$ 의 상한입니다. 이 정의는  $X$ 가 자리스키 위상을 가지는 상황에서만 사용하고 싶을 것입니다: 특히  $X = \text{Spec } A$ 인 경우, 이는 그저 환  $A$  자체의 크룰 차원일 뿐입니다.

## §84.5 근기에 관하여

$\mathbb{C}^n$ 에서 고전적 대수기하학을 공부했을 때, 우리는 힐베르트 영점정리(정리 77.3.4)가 근기 아이디얼과 아핀 다양체 사이의 전단사를 제공하기 위해 등장하는 것을 보았습니다; 증명이 자명하지 않았기 때문에 우리는 이를 생략했습니다.

그러나 점이  $(\mathbb{C}^n$ 의 튜플이 아니라) 소 아이디얼인 스킴의 경우, 대응되는 결과는 실제로 쉬워집니다:  $A = \mathbb{C}[x_1, \dots, x_n]$ 인 경우에도, (극대 아이디얼뿐만 아니라) 소 아이디얼을 추가하는 것이 오히려 증명을 단순화하는데, 이는 근기(radical)가 소 아이디얼과 잘 어울리기 때문입니다.

우리는 여전히 다음 결과를 가집니다.

**명제 84.5.1** ( $\mathcal{V}(\sqrt{I}) = \mathcal{V}(I)$ )

환  $A$ 의 임의의 아이디얼  $I$ 에 대해  $\mathcal{V}(\sqrt{I}) = \mathcal{V}(I)$ 가 성립합니다.

증명. 우리는  $\sqrt{I} \supseteq I$ 를 가집니다. 따라서 자동으로  $\mathcal{V}(\sqrt{I}) \subseteq \mathcal{V}(I)$ 가 성립합니다.

반대로,  $\mathfrak{p} \in \mathcal{V}(I)$ 이면  $I \subseteq \mathfrak{p}$ 이므로,  $\sqrt{I} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p}$ 입니다 (명제 77.3.3에 의해).  $\square$

앞선 소견에서 핵심 결과를 암시했으며, 이제 이를 증명합니다.

**정리 84.5.2** (근기는 소 아이디얼들의 교집합)

$I$ 를 환  $A$ 의 아이디얼이라 합시다. 그러면

$$\sqrt{I} = \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p}.$$

증명. 이는 가환대수학에서 유명한 명제이며, 여기서는 완결성을 위해서만 증명합니다. 이 증명이 “대부분의 작업을 수행”합니다.

$I \subseteq \mathfrak{p}$ 이면  $\sqrt{I} \subseteq \sqrt{\mathfrak{p}} = \mathfrak{p}$ 임에 유의하십시오. 따라서  $\sqrt{I} \subseteq \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p}$ 입니다.

반대로,  $x \notin \sqrt{I}$ 라고 가정합시다. 이는  $1, x, x^2, x^3, \dots \notin I$ 임을 의미합니다. 그러면 국소화  $(A/I)[1/x]$ 를 고려하는데, 이는 영환이 아닙니다. 다른 모든 환과 마찬가지로 이는 어떤 극대 아이디얼을 가집니다(크룰 정리). 이는  $(A/I)[1/x]$ 의 소 아이디얼들,  $A/I$ 의 소 아이디얼들, 그리고  $A$ 의 소 아이디얼들 사이의 통상적인 전단사에 의해,  $I$ 를 포함하지만  $x$ 는 포함하지 않는  $A$ 의 어떤 소 아이디얼  $\mathfrak{p}$ 가 존재함을 의미합니다. 따라서 원하는 대로  $x \notin \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p}$ 입니다.

여기서 핵심 아이디어는,  $x \in A$ 에 대해, 어떤 양의 유한 정수  $n$ 에 대해  $x^n = 0$ 인 것과  $A[1/x] = 0$ 인 것이 동치라는 것입니다.  
즉, 다시 말해서,

$$\begin{aligned} x \in \sqrt{(0)} &\iff \text{어떤 양의 정수 } n \text{에 대해 } x^n = 0 \\ &\iff A[1/x] = 0 \\ &\iff \text{모든 소 아이디얼 } \mathfrak{p} \text{에 대해 } x \in \mathfrak{p} \text{입니다} \\ &\iff x \in \bigcap_{\mathfrak{p}} \mathfrak{p}. \end{aligned}$$

$I$ 가  $(0)$ 이 아닐 때는, 대신 환  $A/I$ 를 고려하십시오. □

기하학적으로 말하면, 이 정리는 다음을 말합니다:

$\text{Spec } A/I$  위의 정칙 함수  $f$ 에 대해, 그러면

어떤 양의 정수  $n$ 에 대해  $f^n = 0$ 입니다  $\iff f$ 는  $\text{Spec } A/I$ 의 모든 점에서 소멸합니다.

이에 대해, 위의 증명은 다음과 같이 읽힙니다:

$$\begin{aligned} f \in \sqrt{(I)} &\iff \text{어떤 양의 정수 } n \text{에 대해 } f^n \in I \text{입니다} \\ &\iff (A/I)[1/f] = 0 \\ &\iff \text{Spec}(A/I)[1/f] \text{는 공집합입니다} \\ &\iff \text{모든 } \mathfrak{p} \in \text{Spec } A/I \text{에 대해, } f \text{는 } \mathfrak{p} \text{에서 소멸합니다} \\ &\iff f \in \bigcap_{\mathfrak{p} \in \text{Spec } A/I} \mathfrak{p}. \end{aligned}$$

**절 86.7**에서  $A = k[x]$ ,  $I = (x^2)$ ,  $f = x$ 인 예시로 증명을 직접 따라가 보는 것도 좋을 것입니다. 이때  $\text{Spec } A/I$ 의 상을 “흐릿한” 점으로,  $f$ 를 모든 점에서 값이 영인 영이 아닌 함수로 염두에 두십시오.

**비고 84.5.3 (크룰 정리의 한 변형)** — 이 증명에서 더 긴 방향은 본질적으로 임의의  $x \in A$ 에 대해,  $x$ 를 포함하지 않는  $A$ 의 극대 아이디얼이 존재한다는 것을 말하고 있습니다. ”짧은” 증명은 위에서처럼  $(A/I)[1/x]$ 에 크룰 정리를 적용하는 것이지만, (원래 크룰 정리의 증명을 그대로 따라 하여) 초른 보조정리를 사용해 직접 증명할 수도 있습니다.

**예제 84.5.4** ( $\mathbb{Z}$ 에서  $\sqrt{(2016)} = (42)$ )

환  $\mathbb{Z}$ 에서,  $(2016)$ 을 포함하는 서로 다른 소수들이  $(2)$ ,  $(3)$ ,  $(7)$ 이므로  $\sqrt{(2016)} = (42)$ 임을 알 수 있습니다.

기하학적으로, 이는  $\sqrt{I}$ 를 설명하는 좋은 방법을 제공합니다: 이는  $\mathcal{V}(I)$  전체에서 소멸하는 모든 함수들의 집합입니다. 실제로 다음과 같이 쓸 수 있습니다

$$\sqrt{I} = \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \mathcal{V}(I)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \mathcal{V}(I)} \{f \in A \mid f(\mathfrak{p}) = 0\}.$$

이제 다음을 서술할 수 있습니다:

**정리 84.5.5** (근기 아이디얼은 닫힌집합에 대응함)

$I$ 와  $J$ 를  $A$ 의 아이디얼이라 하고, 공간  $\text{Spec } A$ 를 고려합시다. 그러면

$$\mathcal{V}(I) = \mathcal{V}(J) \iff \sqrt{I} = \sqrt{J}.$$

특히, 근기 아이디얼은 정확히  $\text{Spec } A$ 의 닫힌 부분집합들에 대응합니다.

증명.  $\mathcal{V}(I) = \mathcal{V}(J)$ 이면,  $\sqrt{I} = \bigcap_{\mathfrak{p} \in \mathcal{V}(I)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \mathcal{V}(J)} \mathfrak{p} = \sqrt{J}$ 이므로 원하는 대로입니다.

반대로,  $\sqrt{I} = \sqrt{J}$ 라고 가정합시다. 그러면  $\mathcal{V}(I) = \mathcal{V}(\sqrt{I}) = \mathcal{V}(\sqrt{J}) = \mathcal{V}(J)$ 입니다.  $\square$

이를 앞서 다루었던, 기약 닫힌 부분집합이 소 아이디얼에 대응한다는 정리와 비교해 보십시오!

## §84.6 생각해 볼 만한 조금 더 어려운 문제

장 86는 직관을 기르기 위한 아핀 스킴의 많은 예시를 담고 있으므로, 아직 이해되지 않는 부분이 있더라도 이 문제들을 시도하기 전에 미리 읽어보는 것이 도움이 될 수 있습니다.

**문제 84A** ( $\text{Spec } \mathbb{Q}[x]$ ).  $\text{Spec } \mathbb{Q}[x]$ 의 점과 위상을 서술하십시오.

**문제 84B** (곱 환).  $\text{Spec } A \times B$ 의 점과 위상을  $\text{Spec } A$ 와  $\text{Spec } B$ 를 이용하여 서술하십시오.

**문제 84C\*** (아르틴 환을 실제로 생각하는 방법).  $A$ 를 뇌터 환이라 합시다. 다음이 모두 동치임을 증명하십시오:

- (i)  $A$ 는 아르틴 환입니다, 즉 (문제 4H에서 정의된 바와 같이) 내림 사슬 조건을 만족합니다.
- (ii)  $A$ 는 크룰 차원이 0이거나  $A$ 는 영환입니다.
- (iii)  $\text{Spec } A$ 는 유한하고 이산적입니다.
- (iv)  $\text{Spec } A$ 는 유한합니다.



# 85 아핀 스킴: 총

이제  $X = \text{Spec } A$  위에 층  $\mathcal{O}_X$ 를 정의하여 이를 환 달린 공간으로 만듦으로써 정의를 완성합니다. 이는 첫 번째 절에서 신속하게 다룹니다.

이전과 마찬가지로, 우리의 목표는 다음과 같습니다:

층  $\mathcal{O}_X$ 는 아핀 다양체 위의 정칙 함수들의 층과 일치하므로,  $A$ 가 임의의 환일 때에도  $\text{Spec } A$ 에 우리의 기하학적 직관을 적용할 수 있습니다.

하지만 이어지는 여러 장에 걸쳐, 우리가 내린 정의를 실제로는 잊어버리도록 독자를 설득하는 데 시간을 쏟을 것입니다. 이는 실용적으로 볼 때, 층의 절편들이 정의를 직접 사용해서가 아니라 다른 결과들을 사용해서 가장 잘 계산되기 때문입니다.

그 과정에서 관련된 이론도 조금 전개할 것입니다: 줄기를 계산하면서 국소환의 정의를 알게 될 것이고, 절편을 계산하면서 특별 열린집합에 대해 알게 될 것입니다.

다시 한번 상기시켜 드립니다: 장 86에는 더 많은 구체적인 예시가 있습니다. 이 장의 어떤 부분에서 막힌다면 그곳을 살펴보는 것도 나쁘지 않은 방법입니다.

## §85.1 구조층의 쓸모없는 정의

**이 절의 대표적인 예:** 여전히  $\mathbb{C}[x_1, \dots, x_n]/I$ 입니다.

이제  $\text{Spec } A$ 에 자리스키 위상을 부여하였으므로, 남은 일은 그 위에 층  $\mathcal{O}_{\text{Spec } A}$ 를 놓는 것뿐입니다. 이를 위해 이전과 마찬가지로 "정칙 함수"라는 개념이 필요합니다.

이미 국소화를 갖추고 있으므로 이는 쉽게 할 수 있습니다.

**정의 85.1.1.** 먼저,  $\mathcal{F}$ 를 "전역적으로 유리적인" 함수들의 전층이라고 합시다: 즉,  $\mathcal{F}(U)$ 를 다음의 국소화로 정의합니다

$$\mathcal{F}(U) = \left\{ \frac{f}{g} \mid f, g \in A \text{ 그리고 } g(\mathfrak{p}) \neq 0 \ \forall \mathfrak{p} \in U \right\} = \left( A \setminus \bigcup_{\mathfrak{p} \in U} \mathfrak{p} \right)^{-1} A.$$

이제  $\text{Spec } A$  위의 구조층을 정의합니다. 그것은

$$\mathcal{O}_{\text{Spec } A} = \mathcal{F}^{\text{sh}}$$

즉, 방금 정의한  $\mathcal{F}$ 의 층화입니다.

**연습문제 85.1.2.** 이를  $V$ 가 복소 다양체일 때의  $\mathcal{O}_V$ 에 대한 정의와 비교하여, 이들이 본질적으로 일치함을 확인하십시오.

그리하여 우리는 아핀 스킴의 완전한 정의와 함께 성인기로의 여행을 완수하였습니다.

정말로 호환 가능한 배아(germ)를 좋아한다면, 정의를 다음과 같이 풀어 쓸 수 있습니다:

**정의 85.1.3.**  $A$ 를 환이라 합시다. 그러면  $\text{Spec } A$ 는 다음과 같이 설정함으로써 환 달린 공간이 됩니다

$$\mathcal{O}_{\text{Spec } A}(U) = \{(f_{\mathfrak{p}} \in A_{\mathfrak{p}})_{\mathfrak{p} \in U} \text{ 국소적으로 뭉친}\}.$$

즉, 이는 수열  $(f_{\mathfrak{p}})_{\mathfrak{p} \in U}$ 로 이루어지며, 각  $f_{\mathfrak{p}} \in A_{\mathfrak{p}}$ 이고, 모든 점  $\mathfrak{p}$ 에 대해 열린 근방  $U_{\mathfrak{p}}$ 와  $f, g \in A$ 가 존재하여 모든  $\mathfrak{q} \in U_{\mathfrak{p}}$ 에 대해  $f_{\mathfrak{q}} = \frac{f}{g} \in A_{\mathfrak{q}}$ 가 성립합니다.

이제 우리는 이 정의를 기본적으로 잊어버릴 것입니다, 왜냐하면 실제로는 이를 결코 사용하지 않을 것이기 때문입니다. 다음 두 절에서 다음을 보여드리겠습니다:

- 줄기  $\mathcal{O}_{\text{Spec } A, \mathfrak{p}}$ 가 단지  $A_{\mathfrak{p}}$ 일 뿐이라는 것과,
- 임의의 열린집합  $U$ 에 대해 절편  $\mathcal{O}_{\text{Spec } A}(U)$ 는  $U = D(f)$ 가 특별 열린집합인 특수한 경우에만 초점을 맞추으로써 계산될 수 있다는 것입니다.

이 두 결과는 우리의 모든 목적에 충분할 것이므로, 이 정의를 사용하지 않아도 될 것입니다. (그래서 이 절에는 예시가 없습니다.)

## §85.2 특별 열린집합의 가치 (또는: 실제로 절편을 계산하는 방법)

**이 절의 대표적인 예:**  $\text{Spec } \mathbb{C}[x]$ 에서  $D(x)$ 는 구멍 뚫린 직선입니다.

이제 특별 열린집합의 중요성을 정말로 강조해보겠습니다. 정의는 이전과 유사합니다:

**정의 85.2.1.**  $f \in A$ 라 합시다. 그러면  $D(f)$ 는  $f(\mathfrak{p}) \neq 0$ 인  $\mathfrak{p}$ 들의 집합으로, **특별 열린집합**입니다.

특별 열린집합은 서로 이어지는 세 가지 절대적으로 중요한 성질을 가지고 있습니다.

### §85.2.i 자리스키 위상의 기저

첫 번째는 위상적 관찰입니다:

**정리 85.2.2 (특별 열린집합은 기저를 이룹니다)**

특별 열린집합  $D(f)$ 는 자리스키 위상의 기저를 이룹니다: 임의의 열린집합  $U$ 는 특별 열린집합들의 합집합입니다.

증명.  $U$ 를 열린집합이라 하고, 닫힌집합  $V(I)$ 의 여집합이라고 합시다. 그러면 다음을 확인해보십시오.

$$U = \bigcup_{f \in I} D(f). \quad \square$$

### §85.2.ii 절단은 계산 가능합니다

두 번째 결정적인 사실은 특별 열린집합 위의 절단을 명시적으로 계산할 수 있다는 것입니다.

**정리 85.2.3 ( $D(f)$ 의 절단은  $f$ 를 제외한 국소화입니다)**

$A$ 를 환이라 하고  $f \in A$ 라 합시다. 그러면

$$\mathcal{O}_{\text{Spec } A}(D(f)) \cong A[1/f].$$

증명. 생략하지만, 정리 78.6.1과 유사합니다. □

**예제 85.2.4 (구멍 뚫린 직선은 쌍곡선과 동형입니다)**

”쌍곡선 효과”가 다시 나타납니다:

$$\mathcal{O}_{\text{Spec } \mathbb{C}[x]}(D(x)) = \mathbb{C}[x, x^{-1}] \cong \mathbb{C}[x, y]/(xy - 1).$$

여담으로,  $\text{Spec } A = D(1)$  자체가 특별 열린집합이므로 전역 절단을 복원할 수 있다는 점도 어딘가에 짚어두는 편이 좋겠습니다.

### 따름정리 85.2.5 ( $A$ 는 전역 절단의 환입니다)

$\text{Spec } A$ 의 전역 절단의 환은  $A$ 입니다.

증명. 앞선 정리에 의해,  $\mathcal{O}_{\text{Spec } A}(\text{Spec } A) = \mathcal{O}_{\text{Spec } A}(D(1)) = A[1/1] = A$ 입니다.  $\square$

### §85.2.iii 그것들은 아핀입니다

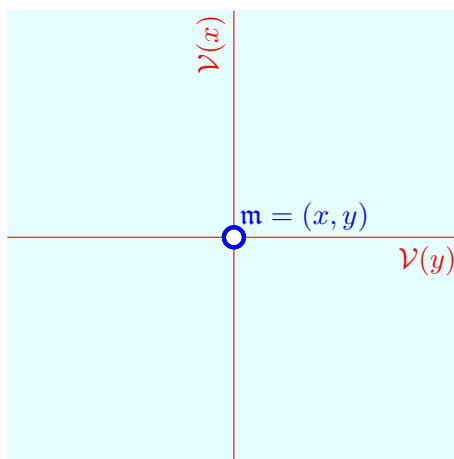
$\mathcal{O}_X(D(f)) = A[1/f]$ 임을 알고 있습니다. 실제로  $\text{Spec } A[1/f]$ 를 그려보면,  $D(f)$ 와 정확히 똑같이 생겼음을 발견하게 됩니다. 따라서 세 번째이자 마지막 중요한 사실은,  $D(f)$ 가 실제로  $\text{Spec } A[1/f]$ 와 동형이라는 것입니다(원점을 제외한 직선이 쌍곡선과 동형인 것과 마찬가지로). 아직 스킴의 사상을 다루지 않았으므로 이를 엄밀하게 만들 수는 없지만, (당장은 아니어도) 나중에 유용하게 쓰일 것입니다.

### §85.2.iv 고전적인 예시: 구멍 뚫린 평면

이제 층화를 한 번도 좋아하지 않았던 분들이 어떻게 층화를 잊어버릴 수 있는지 보여주는 고전적인 계산 예시를 들겠습니다.<sup>1</sup> 그 발상은 다음과 같습니다:

특별 열린집합과 층 공리를 이용하면 실제로 임의의 절단  $\mathcal{O}_X(U)$ 를 계산할 수 있습니다.

$X = \text{Spec } \mathbb{C}[x, y]$ 라 하고, 원점, 즉 점  $\mathfrak{m} = (x, y)$ 를 생각해봅시다. 이 아이디얼은 극대 아이디얼이므로 닫힌점에 대응하며,  $\mathfrak{m}$ 을 제외한 모든 점들로 이루어진 열린집합  $U$ 를 생각할 수 있습니다. 우리는  $\mathcal{O}_X(U)$ 를 계산하고자 합니다.



안타깝게도  $U$ 는 특별 열린집합이 아닙니다. 하지만  $U = D(x) \cup D(y)$ 로 씌으로써 어쨌든 계산할 수 있습니다: 편리하게도  $D(x) \cap D(y) = D(xy)$ 입니다. 층 공리에 의해, 다음과 같은 당겨오기 정사각형을 얻습니다

<sup>1</sup>이러한 관점이 매우 유용하다 보니, Vakil [Va17, §4.1]과 같은 일부 문헌에서는 우리가 했던 것처럼 층화를 사용하는 대신,  $\mathcal{O}_{\text{Spec } A}(D(f)) = A[1/f]$ 를 요구함으로써  $\mathcal{O}_{\text{Spec } A}$ 를 정의합니다.

$$\begin{array}{ccc}
 \mathcal{O}_X(U) & \longrightarrow & \mathcal{O}_X(D(x)) = \mathbb{C}[x, y, x^{-1}] \\
 \downarrow & & \downarrow \\
 \mathcal{O}_X(D(y)) = \mathbb{C}[x, y, y^{-1}] & \longrightarrow & \mathcal{O}_X(D(xy)) = \mathbb{C}[x, y, x^{-1}, y^{-1}].
 \end{array}$$

다시 말해,  $\mathcal{O}_X(U)$ 는 다음과 같은 쌍들로 이루어집니다

$$\begin{aligned}
 f &\in \mathbb{C}[x, y, x^{-1}] \\
 g &\in \mathbb{C}[x, y, y^{-1}]
 \end{aligned}$$

겹치는 부분에서 일치하는 것들입니다:  $D(x) \cap D(y)$ 에서  $f = g$ . 그런데  $f$ 는 분모에  $x$ 가 몇 개 있는 다항식으로,  $g$ 는 분모에  $y$ 가 몇 개 있는 다항식으로 표현할 수 있습니다. 이 둘이 일치한다면, 분모는 사실상 상수가 됩니다. 대략적으로 말하면,

$$\mathbb{C}[x, y, x^{-1}] \cap \mathbb{C}[x, y, y^{-1}] = \mathbb{C}[x, y].$$

결론적으로,

$$\mathcal{O}_X(U) = \mathbb{C}[x, y].$$

즉, 추가적인 함수는 얻지 못합니다.

### §85.3 구조층의 줄기

**이 절의 대표적인 예:**  $\text{Spec } \mathbb{C}[x, y]$ 의  $\mathfrak{m} = (x, y)$ 에서의 줄기는 원점에서 정의된 유리함수입니다.

걱정하지 마십시오, 이번 것은 지난 절보다 쉽습니다.

#### §85.3.i 이들은 국소화입니다

**정리 85.3.1** ( $\text{Spec } A$ 의 줄기는  $A_{\mathfrak{p}}$ 입니다)

$A$ 를 환이라 하고  $\mathfrak{p} \in \text{Spec } A$ 라 합시다. 그러면

$$\mathcal{O}_{\text{Spec } A, \mathfrak{p}} \cong A_{\mathfrak{p}}.$$

특히  $\text{Spec } A$ 는 국소 환달린 공간입니다.

증명. 층화 과정이 줄기를 보존하므로, 우리의 정의에서 전역 유리함수들의 전층인  $\mathcal{F}$ 에 대해서만 확인하면 충분합니다. 증명은 **정리 82.3.7**과 기본적으로 동일합니다: 다음과 같이 배아(germ)들에 대한 자명한 사상  $\mathcal{F}_{\mathfrak{p}} \rightarrow A_{\mathfrak{p}}$ 가 존재합니다

$$(U, f/g \in \mathcal{F}(U)) \mapsto f/g \in A_{\mathfrak{p}}.$$

(왼쪽의  $f/g$ 는  $\mathcal{F}(U)$ 에 속하지만 오른쪽의 것은  $A_{\mathfrak{p}}$ 에 속함에 유의하십시오). 단사성과 전사성을 보이겠습니다:

- 단사:  $(U_1, f_1/g_1)$ 과  $(U_2, f_2/g_2)$ 가  $f_1/g_1 = f_2/g_2 \in A_{\mathfrak{p}}$ 를 만족하는 두 배아라고 합시다. 이는  $A$ 에서 어떤  $h \notin \mathfrak{p}$ 에 대해  $h(f_1g_2 - f_2g_1) = 0$ 임을 뜻합니다. 그러면 두 배아 모두 배아  $(U_1 \cap U_2 \cap D(h), f_1/g_1)$ 과 동일시됩니다.
- 전사:  $U = D(g)$ 라 합시다. □

**예제 85.3.2** ( $x$ 로 나누어떨어지지 않는 분모들)

이 예시는 이미 여러 번 보았으므로, 새로운 표기법으로만 적고 더 이상의 설명은 하지 않겠습니다:  $X = \operatorname{Spec} \mathbb{C}[x]$ 라면

$$\mathcal{O}_{X,(x)} = \mathbb{C}[x]_{(x)} = \left\{ \frac{f}{g} \mid g(0) \neq 0 \right\}.$$

**예제 85.3.3** ( $x$ 나  $y$ 로 나누어떨어지지 않는 분모들)

$X = \operatorname{Spec} \mathbb{C}[x, y]$ 라 하고  $\mathfrak{m} = (x, y)$ 를 원점이라 합시다. 그러면

$$\mathbb{C}[x, y]_{(x, y)} = \left\{ \frac{f(x, y)}{g(x, y)} \mid g(0, 0) \neq 0 \right\}.$$

더 많은 예시를 원한다면, 절 83.4에 있는 것들 중 아무거나 가져와서 그것들이 기하학적으로 무엇을 의미하는지 생각해 보십시오.

**§85.3.ii 국소환의 동기: 배아는 값들을 담아내야 합니다**

우리에게 익숙한 예시  $X = \operatorname{Spec} \mathbb{C}[x, y]$ 로 돌아가서  $\mathfrak{m} = (x, y)$ 를 원점이라고 합시다. 줄기는

$$\mathcal{O}_{X, \mathfrak{m}} = \mathbb{C}[x, y]_{(x, y)} = \left\{ \frac{f(x, y)}{g(x, y)} \mid g(0, 0) \neq 0 \right\}.$$

이제  $f = \frac{1}{xy+4}$ 와 같은 어떤 절편을 살펴봅시다. 이는  $U = D(xy+4)$ 의 절편입니다(또는 더 작은 열린집합의 절편일 수도 있지만, 편의를 위해 이것만 사용하겠습니다). 또한  $U \ni \mathfrak{m}$ 이므로,  $f$ 는  $\mathfrak{m}$ 에서의 배아를 줍니다.

한편,  $f$ 는  $\mathfrak{m}$ 에서 값도 갖습니다: 이는  $f \pmod{\mathfrak{m}} = \frac{1}{4}$ 입니다. 그리고 일반적으로, 원점  $\mathfrak{m}$ 에서 절편이 가질 수 있는 값들의 환은  $\mathbb{C}[x, y]/\mathfrak{m} \cong \mathbb{C}$ 입니다.

이제, 배아를 "풍부화된 값"으로 생각할 수 있다는 관점을 제가 강조했던 것을 기억하실 것입니다. 그렇다면 점  $\mathfrak{m}$ 에서의 절편  $f$ 의 배아를 안다면 — 즉 "풍부화된 값"을 안다면 — 그 값 또한 계산할 수 있어야 한다는 것이 이치에 맞습니다. 이것이 의미하는 바는, 우리가 다음과 같은 사상을 가져야 한다는 것입니다

$$A_{\mathfrak{m}} \rightarrow A/\mathfrak{m}$$

배아를 그에 대응하는 값으로 보내는 사상입니다.

실제로 가능하며, 이는 우리를 다음으로 이끕니다...

**§85.4 국소환과 잉여체: 싹과 값을 잇는 다리**

이 절의 대표적인 예:  $\operatorname{Spec} \mathbb{C}[x, y]$ 의  $\mathfrak{m} = (x, y)$ 에서의 잉여체는  $\mathbb{C}$ 입니다.

**§85.4.i 국소화는 국소환을 줍니다**

이 표기법은 이제 정말 끔찍해질 참이지만, 조금만 참아주십시오.

**정리 85.4.1 (줄기는 국소환입니다)**

$A$ 를 환이라 하고  $\mathfrak{p}$ 를 임의의 소 아이디얼이라 합시다. 그러면 국소화  $A_{\mathfrak{p}}$ 는 정확히 하나의 극대 아이디얼을 가지며, 이는 다음과 같이 명시적으로 주어집니다

$$\mathfrak{p}A_{\mathfrak{p}} = \left\{ \frac{f}{g} \mid f \in \mathfrak{p}, g \notin \mathfrak{p} \right\}.$$

따라서 아이디얼  $\mathfrak{p}A_{\mathfrak{p}}$ 는 “ $\mathfrak{p}$ 에서 소멸하는 짝”이라는 개념을 포착합니다.<sup>2</sup>

증명은 잠시 후에 하겠습니다. 지금은 우리의 예시를 적절한 언어로 제시할 수 있도록 몇 가지 용어를 도입해봅시다.

**정의 85.4.2.** 정확히 하나의 극대 아이디얼  $\mathfrak{m}$ 을 가지는 환  $R$ 을 **국소환**이라 부릅니다. **잉여체**는 몫  $R/\mathfrak{m}$ 입니다.

**질문 85.4.3.** 체는 국소환입니까?

따라서 우리가 발견하는 것은 다음과 같습니다:

**줄기는 가능한 강화된 값들(짝)로 이루어져 있습니다; 잉여체는 (강화되지 않은) 값들의 집합입니다.**

**예제 85.4.4 ( $\text{Spec } \mathbb{C}[x, y]$ 의 원점에서의 줄기)**

다시  $A = \mathbb{C}[x, y]$ ,  $X = \text{Spec } A$ ,  $\mathfrak{p} = (x, y)$ 로 설정하여  $\mathcal{O}_{X, \mathfrak{p}} = A_{\mathfrak{p}}$ 가 되도록 합시다. (국소환  $A_{\mathfrak{p}}$ 의 극대 아이디얼  $\mathfrak{p}A_{\mathfrak{p}}$ 와의 혼동을 피하기 위해, 원점을 나타내는 데  $\mathfrak{p}$ 로 표기를 바꾸었습니다.) 이미 여러 번 말했듯이,  $A_{\mathfrak{p}}$ 는 원점에서 소멸하지 않는 유리함수들로 이루어져 있으며, 예를 들면  $f = \frac{1}{xy+4}$ 와 같습니다.

유일한 극대 아이디얼  $\mathfrak{p}A_{\mathfrak{p}}$ 는 무엇입니까? 답: 이는 원점에서 소멸하는 유리함수들로 이루어져 있습니다: 예를 들어  $\frac{x}{x^2+3y}$ , 또는  $\frac{3x+5y}{2}$ , 또는  $\frac{-xy}{4(xy+4)}$ 입니다. 이런 함수들로 나머지를 취하는 것을 허용하면, 잉여체  $\mathbb{C}$ 를 얻으며,  $f$ 는 값  $\frac{1}{4}$ 를 가지게 됩니다. 그 이유는

$$\frac{1}{xy+4} - \underbrace{\frac{-xy}{4(xy+4)}}_{\text{원점에서 소멸합니다}} = \frac{1}{4}.$$

더 일반적으로,  $f$ 가  $\mathfrak{p}$ 를 포함하는 어떤 열린집합의 임의의 절단이라고 합시다.  $c \in \mathbb{C}$ 를 값  $f(\mathfrak{p})$ , 즉  $f \pmod{\mathfrak{p}}$ 라 합시다. 그러면  $f - c$ 는 원점  $\mathfrak{p}$ 에서 소멸하는 또 다른 절단이 될 것이므로, 약속했던 대로  $f \equiv c \pmod{\mathfrak{p}A_{\mathfrak{p}}}$ 입니다.

좋습니다, 이제 정리의 증명을 적어봅시다.

**정리 85.4.1의 증명.** 집합  $I = \mathfrak{p}A_{\mathfrak{p}}$ 가  $A_{\mathfrak{p}}$ 의 아이디얼임을 확인할 수 있습니다. 더욱이,  $1 \notin I$ 이므로  $I$ 는 진 아이디얼입니다.

이것이 극대이며 유일함을 증명하려면,  $f \notin I$ 인 임의의  $f \in A_{\mathfrak{p}}$ 가  $A_{\mathfrak{p}}$ 의 단원임을 증명하면 충분합니다. 이는  $I$ 가 극대임을 함의합니다: 더 이상 추가할 비단원이 없기 때문입니다.

<sup>2</sup>표기법  $\mathfrak{p}A_{\mathfrak{p}}$ 는 실제로  $f \in \mathfrak{p}$  (여기서  $f \mapsto \frac{f}{1}$ 에 의해  $A_{\mathfrak{p}}$ 의 부분집합으로 간주됩니다)이고  $h \in A_{\mathfrak{p}}$ 인  $f \cdot h$ 의 집합을 뜻합니다. 저 개인적으로는 이것이 도움이 되기보다 혼란스럽다고 느껴서, 각주로 처리합니다.

또한 이는  $I$ 가 유일한 극대 아이디얼임을 함의합니다: 어떤 진 아이디얼도 단원을 포함할 수 없으므로,  $I$ 에 포함되기 때문입니다.

이는 사실 쉽습니다.  $I$ 에 속하지 않는  $A_{\mathfrak{p}}$ 의 원소는  $f, g \in A$ 이고  $f, g \notin \mathfrak{p}$ 인  $x = \frac{f}{g}$ 의 형태여야 합니다. 이러한 원소에 대해,  $x^{-1} = \frac{g}{f} \notin \mathfrak{p}$  또한 성립합니다. 따라서  $x$ 는 단원입니다. 증명 끝.  $\square$

더욱 일반적으로:

층  $\mathcal{F}$ 가 “체 값을 가지는 함수”들로 이루어져 있다면, 줄기  $\mathcal{F}_p$ 는 아마도  $p$ 에서 소멸하는 쌍들로 이루어진 극대 아이디얼을 가질 것입니다.

#### 예제 85.4.5 (비대수기하학적 층에서의 국소환)

$X = \mathbb{R}$ 이고  $\mathcal{F}(U)$ 가 매끄러운 함수들인 예시로 돌아가서,  $p \in X$ 일 때 줄기  $\mathcal{F}_p$ 를 생각해봅시다. 아이디얼  $\mathfrak{m}_p$ 를  $s(p) = 0$ 을 만족하는 쌍  $(s, U)$ 들의 집합으로 정의합니다. 그러면  $\mathfrak{m}_p$ 는 극대입니다: 다음과 같은 완전열이 있습니다

$$0 \rightarrow \mathfrak{m}_p \rightarrow \mathcal{F}_p \xrightarrow{(s, U) \mapsto s(p)} \mathbb{R} \rightarrow 0$$

따라서  $\mathcal{F}_p/\mathfrak{m}_p \cong \mathbb{R}$ 이며, 이는 체입니다.

0이 아닌 극대 아이디얼이 없음을 확인하는 일이 남아 있습니다. 이제  $s \notin \mathfrak{m}_p$ 이면  $s$ 는  $p$ 의 어떤 열린 근방에서 0이 아니며, 그 위에서 함수  $1/s$ 를 구성할 수 있다는 점에 주목하십시오. 따라서  $\mathcal{F}_p \setminus \mathfrak{m}_p$ 의 모든 원소는 단원입니다. 그리고 다시 한번  $\mathfrak{m}_p$ 가 실제로 유일한 극대 아이디얼임을 알 수 있습니다!

따라서 다음 각 유형의 층의 줄기들 역시 국소환입니다.

- 위상 공간 위의 연속 실/복소 함수 층
- 임의의 다양체 위의 매끄러운 함수 층
- 기타 등등

### §85.4.ii 값 계산하기: 편리한 사각형

매우 꼼꼼한 독자라면  $A = \mathbb{C}[x, y]$ 이고 원점인  $\mathfrak{p} = (x, y)$ 인  $\text{Spec } A$ 를 다룬 확장된 예제에서 다소 불편한 점을 눈치챌 수 있습니다.  $f = \frac{1}{xy+4}$ 를 생각해 봅시다. 값이  $\frac{1}{4}$ 이어야 한다”고 판단하기 위해 원래 환  $A$ 에서  $f \pmod{x, y}$ 를 취했습니다. 하지만 사실 우리의 모든 계산은 환  $A$ 에서가 아니라 환  $A_{\mathfrak{p}}$ 에서 이루어졌습니다. 이것이 문제를 일으킬까요?

다행히도, 일반적인 환  $A$ 에서도 아무 문제가 없습니다.

**정의 85.4.6.** 몫  $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ , 즉  $\mathfrak{p}$ 에서의  $\text{Spec } A$ 의 줄기의 잉여체를  $\kappa(\mathfrak{p})$ 로 표기하겠습니다.

그러면 다음은 정리 83.7.1(국소화는 몫과 교환됩니다)의 특수한 경우입니다:

**정리 85.4.7 (배아-값 사각형)**

$A$ 를 환이라 하고  $\mathfrak{p}$ 를 소 아이디얼이라 합시다. 다음 도식은 가환합니다:

$$\begin{array}{ccc} A & \xrightarrow{\text{localize}} & A_{\mathfrak{p}} \\ \text{mod } \mathfrak{p} \downarrow & & \downarrow \text{mod } \mathfrak{p} \\ A/\mathfrak{p} & \xrightarrow{\text{Frac}(-)} & \kappa(\mathfrak{p}) \end{array}$$

특히,  $\kappa(\mathfrak{p})$ 는  $\text{Frac}(A/\mathfrak{p})$ 로도 나타낼 수 있습니다.

그래서 예를 들어  $A = \mathbb{C}[x, y]$ 이고  $\mathfrak{p} = (x, y)$ 이면,  $A/\mathfrak{p} = \mathbb{C}$ 이고  $\text{Frac}(A/\mathfrak{p}) = \text{Frac}(\mathbb{C}) = \mathbb{C}$ 이며, 이는 우리가 예상한 바입니다. 실제로는 어떤 소 아이디얼  $\mathfrak{p}$ 에 대해서도  $\text{Frac}(A/\mathfrak{p})$ 가  $\kappa(\mathfrak{p})$ 를 계산하는 더 쉬운 방법일 것입니다.

**§85.5 요약**

지난 두 장을 요약하기 위해,  $A$ 를 환이라고 합시다.

- $X = \text{Spec } A$ 를  $A$ 의 소 아이디얼들의 집합으로 정의합니다.
  - 극대 아이디얼은 우리에게 익숙한 "닫힌점"이지만, 소 아이디얼은 "일반점"입니다.
- 아이디얼  $I \subseteq A$ 에 대해  $\mathcal{V}(I)$ 를 닫힌집합으로 선언함으로써  $\text{Spec } A$ 에 자리스키 위상을 부여합니다.
  - 특별 열린집합  $D(f)$ 들은 위상 기저를 이룹니다.
  - 기약 닫힌집합은 정확히 점들의 폐포입니다.
- 마지막으로, 층  $\mathcal{O}_X$ 를 정의했습니다. 정의를 다음과 같이 설정했습니다.
  - $\mathcal{O}_X(D(f)) = A[1/f]$ : 특별 열린집합  $D(f)$ 에서도 국소화를 얻습니다.
  - $\mathcal{O}_{X, \mathfrak{p}} = A_{\mathfrak{p}}$ : 줄기는 소 아이디얼에서의 국소화입니다.

$D(f)$ 가 기저이므로, 이 두 성질을 이용하면 임의의 열린집합  $U$ 에 대해  $\mathcal{O}_X(U)$ 를 명시적으로 계산할 수 있으며, 따라서 층화(sheafification)를 이용한 정의에 의존할 필요가 없습니다.

**§85.6 함수는 값이 아니라 싹에 의해 결정됩니다**

**이 절의 대표적인 예:**  $\text{Spec } \mathbb{C}[x]/(x^2)$  위의 함수 0과  $x$ .

이 장을 마치며 한 가지 경고의 말을 덧붙입니다. 임의의 환 달린 공간에서 단면은 그 싹에 의해 결정됩니다. 따라서  $\text{Spec } A$  위에서 함수  $f \in A$ 는 각 줄기  $A_{\mathfrak{p}}$ 에서의 싹에 의해 결정됩니다. 그러나 이제  $f \in A$ 가 각 점에서의 값  $f(\mathfrak{p}) = f \pmod{\mathfrak{p}}$ 에 의해 결정되는 것은 아닙니다.

유명한 예는 다음과 같습니다:

**예제 85.6.1 (이중점에서,  $x$ 의 모든 배수는 모든 점에서 영이 됨)**

공간  $\text{Spec } \mathbb{C}[x]/(x^2)$ 는 점을 오직 하나, 즉  $(x)$ 만 가집니다. 함수 0과  $x$ (그리고 이에 관해서라면  $2x, 3x, \dots$ )는 모두 이 점에서 영이 됩니다. 이는 일반적으로 함수가

값에 의해 유일하게 결정되지는 않음을 보여줍니다.

다행히도, 이러한 종류의 “나쁜” 현상이 언제 일어나는지 명시적으로 특징지을 수 있습니다. 실제로, 우리는 모든  $\mathfrak{p}$ 에 대해  $f(\mathfrak{p}) = g(\mathfrak{p})$ 인 경우, 즉 동등하게  $h = f - g$ 가 모든 소 아이디얼  $\mathfrak{p}$ 에서 영이 되는 경우가 언제인지 알고자 합니다. 이는 다음을 가지는 것과 동등합니다

$$h \in \bigcap_{\mathfrak{p}} \mathfrak{p} = \sqrt{(0)}$$

영 아이디얼의 근기. 따라서 원형적인 예에서, 그 실패는 어떤 큰  $n$ 에 대해  $x^n = 0$ 이라는 사실에 의해 일어난 것입니다.

**정의 85.6.2.** 환  $A$ 에 대해, 영 아이디얼의 근기인  $\sqrt{(0)}$ 을  $A$ 의 **먹영근기**라고 부릅니다. 먹영근기의 원소를 **먹영원**이라고 부릅니다. 0이 유일한 먹영원일 때, 즉  $\sqrt{(0)} = (0)$ 일 때,  $A$ 를 **축소환**이라고 말합니다.

**질문 85.6.3.** 정역은 축소환입니까?

그렇다면 위의 논의로부터 다음을 얻습니다:

**정리 85.6.4 (먹영원만이 문제가 됨)**

두 함수  $f$ 와  $g$ 가  $\text{Spec } A$ 의 모든 점에서 같은 값을 가지는 것은  $f - g$ 가 먹영원인 것과 동치입니다.

특히,  $A$ 가 축소환일 때는,  $\mathfrak{p} \in \text{Spec } A$ 에서의 값  $f(\mathfrak{p})$ 만으로도  $f \in A$ 를 결정하기에 충분합니다.

## §85.7 생각해 볼 만한 조금 더 어려운 문제

장 86에는 직관을 기르기 위한 아핀 스킴의 예시가 많이 담겨 있으므로, 이 문제들을 시도하기 전에 미리 읽어보는 것이 도움이 될 것입니다.



**문제 85A<sup>†</sup>** (스펙트럼은 준콤팩트입니다). 임의의 환  $A$ 에 대해  $\text{Spec } A$ 가 준콤팩트임을 보이십시오.

**문제 85B** (구멍 뚫린 자이로톱, Aaron Pixton 전달). 자이로톱은 스킴  $X = \text{Spec } \mathbb{C}[x, y, z]/(xz, yz)$ 입니다. 닫힌점  $\mathfrak{m} = (x, y, z)$ 를 제거하여 얻은 열린집합을  $U$ 라 합니다.  $\mathcal{O}_X(U)$ 를 계산하십시오.

**문제 85C.** 환  $R$ 이 국소환인 것과 다음 성질이 성립하는 것이 동치임을 보이십시오: 임의의  $x \in R$ 에 대해,  $x$  또는  $1 - x$ 가 단원입니다.

**문제 85D.**  $R$ 을 국소환이라 하고,  $\mathfrak{m}$ 을 그 극대 아이디얼이라 합니다.  $R_{\mathfrak{m}}$ 을 서술하십시오.

**문제 85E.**  $A$ 를 환이라 하고,  $\mathfrak{m}$ 을 극대 아이디얼이라 하십시오.  $\mathfrak{m}$ 을  $\text{Spec } A$ 의 점으로 생각하십시오.  $\kappa(\mathfrak{m}) \cong A/\mathfrak{m}$ 임을 보이십시오.



# 86 막간: 아핀 스킴의 열여덟 가지 예시

앞의 두 장에서 다진 내용을 굳히기 위해, 이제 방대한 예시 목록을 제시합니다. 각 예시는 페이지 단위의 주황색 상자를 갖는 대신 자신만의 절을 갖습니다.

예시를 헤쳐 나가면서 발견하게 될 공통된 주제 하나는, 여러분의 기하학적 직관이 대수적 직관보다 더 나을 수 있다는 것입니다. 예를 들어  $k[x, y]/(xy)$ 를 공부하다 보면 "기하학적으로는 이리이러한 것이 저러저러한 것처럼 보일 것으로 예상한다"고 말하게 되지만, 막상 대수적 표현을 적어보면 서로 같아 보이지 않는 두 표현을 발견하게 됩니다. 하지만 그 후 계산을 좀 해보면 결국 그것들이 동형사상이었음을 알게 됩니다. 그런 의미에서 이 장에서 여러분은 대수적 진술의 그림을 그리기 시작하는 법을 배우게 될 것입니다 — 정말 멋진 일입니다!

또 다른 예시로, 국소화에 대한 연구에서 나왔던 소 아이디얼에 관한 모든 보조정리가 이제 구체적인 형태를 띠기 시작할 것입니다: 다음과 같은 많은 예시를 보게 될 것입니다

- $\text{Spec } A/I$ 는  $\text{Spec } A$ 의  $\mathcal{V}(I)$ 처럼 보입니다,
- $\text{Spec } A[1/f]$ 는  $\text{Spec } A$ 의  $D(f)$ 처럼 보입니다,
- $\text{Spec } A_{\mathfrak{p}}$ 는  $\text{Spec } A$ 의  $\mathcal{O}_{\text{Spec } A, \mathfrak{p}}$ 처럼 보입니다.

이어지는 모든 내용에서  $k$ 는 임의의 체입니다. 또한 다음과 같은 색상 규약을 사용하겠습니다:

- 스킴의 닫힌점은 파란색으로 그림니다.
- 닫히지 않은 점은 빨간색으로 그리며, 그 "자취"는 빨간색 점선으로 그림니다.
- 줄기는 나타날 경우 초록색으로 그림니다.

## §86.1 예시: $\text{Spec } k$ , 하나의 점

이것은 쉽습니다: 임의의 체  $k$ 에 대해,  $X = \text{Spec } k$ 는 유일한 진 아이디얼  $(0)$ 에 대응하는 하나의 점을 가집니다. 여기에 위상을 부여하는 방법은 오직 하나뿐입니다.

층에 관해서는,

$$\mathcal{O}_X(X) = \mathcal{O}_{X, (0)} = k.$$

이렇게 공간은 자신이 어느 체 위에 있고 싶은지를 기억하고 있습니다. 우리가 복소해석 학자라면 한 점 위의 함수 집합은  $\mathbb{C}$ 이고, 정수론자라면 한 점 위의 함수 집합은  $\mathbb{Q}$ 일 수도 있습니다.

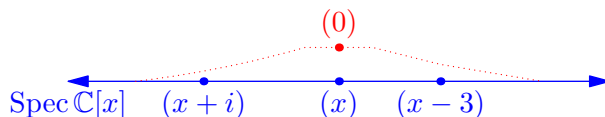
## §86.2 $\text{Spec } \mathbb{C}[x]$ , 일차원 직선

스킴  $X = \text{Spec } \mathbb{C}[x]$ 는 우리가 사랑하는 일차원 직선입니다. 이것은 두 종류의 점으로 이루어집니다:

- 각 복소수  $a \in \mathbb{C}$ 에 대응하는 닫힌점  $(x - a)$ , 그리고
- 일반점  $(0)$ .

자리스키 위상에 관해서는, 모든 열린집합이  $(0)$ 을 포함하는데, 이는 그것이 어디에나 가깝다는 관념을 포착합니다: 여러분이 어디에 서 있든, 파리의 웅웅거리는 소리를 여전히 들을 수 있습니다! 이 공간의 기약성에 걸맞게 열린집합들은 거대합니다: 진 닫힌집합들은 유한개의 닫힌점으로 이루어집니다.

여기 그림이 있습니다: 마땅히 더 나은 자리가 없어서, 점  $(0)$ 은 직선 바로 위에 빨간색으로 떠다니고 있습니다.



“ $\mathfrak{p}$ 에서의 값”이라는 개념은 예상대로 작동합니다. 예를 들어  $f = x^2 + 5$ 는  $\mathbb{C}[x]$ 의 전역 절단입니다. 이것을  $\mathfrak{p} = x - 3$ 에서 평가하면,  $f(\mathfrak{p}) = f \pmod{\mathfrak{p}} = x^2 + 5 \pmod{x-3} = 14 \pmod{x-3}$ 을 얻습니다. 실제로

$$\kappa(\mathfrak{p}) \cong \mathbb{C}$$

이며, 이는 모든 줄기가 잉여체  $\mathbb{C}$ 를 가짐을 의미합니다.

$$\mathbb{C}[x]/\mathfrak{p} \cong \mathbb{C} \quad x \mapsto 3 \text{에 의해}$$

이므로, 우리가 단지  $x = 3$ 을 대입하고 있는 것임을 알 수 있습니다.

물론,  $(x - 3)$ 에서의 줄기는 더 많은 정보를 담고 있습니다. 이 경우 그것은  $\mathbb{C}[x]_{(x-3)}$ 입니다. 이는 점  $(x - 3)$  근처에서 있다면, 분모에  $x - 3$ 이 나타나지 않는 한 유리 함수는 모두 문제없다는 것을 의미합니다. 그래서  $\frac{x^2+8}{(x-1)(x-5)}$ 는  $x = 3$  근처의 싹의 좋은 예시입니다.

일반점  $\eta = (0)$ 을 고려하면 상황은 더 흥미로워집니다.

줄기  $\mathcal{O}_{X,\eta}$ 는 무엇일까요? 그것은  $\mathbb{C}[x]_{(0)} = \mathbb{C}(x)$ 가 되어야 하는데, 이는 다시 유리 함수들의 집합입니다. 그리고 이것이 바로 예상하신 바입니다. 예를 들어,  $\frac{x^2+8}{(x-1)(x-5)}$ 는 확실히 “대부분의” 복소수에서 유리 함수를 나타냅니다.

전역 단면  $f = x^2 + 5$ 를  $\eta$ 에서 계산하면 무슨 일이 일어날까요? 그저  $f(\eta) = x^2 + 5$ 를 얻을 뿐입니다 — 0으로 나눈 나머지를 취하는 것은 별다른 효과가 없습니다. 잘 들어맞게도, 이는 다항식  $f$ 를 일반적인 복소수에서 계산할 수 있으려면 실제로 다항식(또는 유리 함수) 전체가 필요하다는 것을 의미합니다. 이를 잉여체가  $\mathbb{C}(x)$ 라는 관점에서 생각할 수 있습니다:

$$\kappa((0)) = \text{Frac}(\mathbb{C}[x]/(0)) \cong \text{Frac} \mathbb{C}[x] = \mathbb{C}(x).$$

### §86.3 $\text{Spec} \mathbb{R}[x]$ , 복소 켈레가 붙은 일차원 직선(영점 정리를 두려워하지 마십시오)

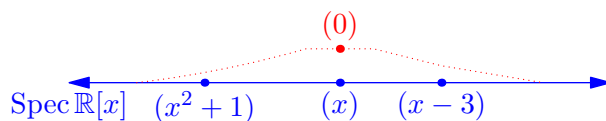
겉모습과는 달리, 이는 실제로 예상보다 훨씬 더  $\text{Spec} \mathbb{C}[x]$ 와 거의 똑같이 보입니다. 명심해야 할 핵심은 이제  $(x^2 + 1)$ 이 하나의 점이며, 이를 대략  $\pm i$ 로 생각할 수 있다는 것입니다. 그러므로  $\mathbb{R}$ 이 대수적으로 닫혀 있지 않다는 사실은 거의 문제가 되지 않습니다 — 어쨌든  $\mathbb{C}$ 가 그 속을 비쳐 보이기 때문입니다. 하지만 이번에는 실수 계수 다항식만을 고려하므로, “켈레”인  $+i$ 와  $-i$ 를 구별하지 않습니다. 달리 말하면,  $a + bi$ 와  $a - bi$ 를 하나의 점으로 접어 넣은 것입니다:  $(x + i)$ 와  $(x - i)$ 가 합쳐져  $x^2 + 1$ 을 이룹니다.

명확히 하자면, 점에는 세 가지 종류가 있습니다:

- 각 실수  $a$ 에 대한  $(x - a)$
- $a^2 < 4b$ 일 때의  $(x^2 - ax + b)$ , 그리고
- 다시, 생성점  $(0)$ .

아이디얼  $(x-a)$ 와  $(x^2-ax+b)$ 는 각각 닫힌 점입니다:  $\mathbb{R}[x]$ 와의 몫은 둘 다 체입니다 (각각  $\mathbb{R}$ 와  $\mathbb{C}$ ).

우리는  $\text{Spec } \mathbb{C}[x]$ 를 1차원 직선으로 그려왔으므로,  $\text{Spec } \mathbb{R}[x]$ 도 같은 방식으로 그려질 것입니다.



이것의 좋은 점 하나는 영점 정리가 고전적인 다양체에서보다 덜 무섭다는 것입니다. 간단히 말하면, 함수  $x^2+1$ 은  $\text{Spec } \mathbb{R}[x]$ 의 한 점, 바로  $(x^2+1)$  자체에서 소멸합니다! (그래서 어떤 의미에서는 우리가 자동으로 대수적 폐포를 다루고 있는 셈입니다.)

오래전에 우리가 약한 영점 정리에 대해 큰 소동을 벌였던 것을 기억하실지 모르겠습니다. 예를 들어 **문제 77C**에서였습니다: 만약  $I$ 가  $\mathbb{C}[x_1, \dots, x_n]$ 의 진 아이디얼이었다면, 모든  $f \in I$ 에 대해  $f(a_1, \dots, a_n) = 0$ 이 되는 어떤 점  $(a_1, \dots, a_n) \in \mathbb{C}^n$ 이 존재했습니다. 스킴을 사용하면 이는 더 이상 문제가 되지 않습니다: 만약  $I$ 가 환  $A$ 의 진 아이디얼이라면, 어떤 극대 아이디얼이 그것을 포함하며, 따라서  $\mathcal{V}(I)$ 는  $\text{Spec } A$ 에서 공집합이 아닙니다.

이번에는 줄기가 예상과 다르게 생겼다는 점을 언급하는 것이 좋겠습니다. 몇 가지 예시가 여기 있습니다:

$$\begin{aligned}\kappa((x^2+1)) &\cong \mathbb{R}[x]/(x^2+1) \cong \mathbb{C} \\ \kappa((x-3)) &\cong \mathbb{R}[x]/(x-3) \cong \mathbb{R} \\ \kappa((0)) &\cong \text{Frac}(\mathbb{R}[x]/(0)) \cong \mathbb{R}(x)\end{aligned}$$

“복소” 점들 위의 잉여체가 더 크다는 것에 주목하십시오: 그 점들 위의 함수는  $\mathbb{C}$ 에서 값을 취합니다.

## §86.4 $\text{Spec } k[x]$ , 임의의 바탕체 위에서

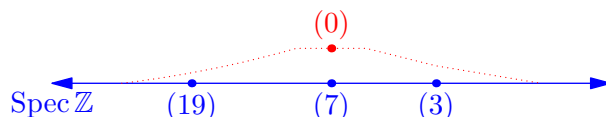
일반적으로,  $\bar{k}$ 가  $k$ 의 대수적 폐포라면,  $\text{Spec } k[x]$ 는 모든 갈루아 켈레들이 함께 붙여진  $\text{Spec } \bar{k}[x]$ 처럼 보입니다. 그러므로 우리는 이제 거의 “대수적으로 닫혀있다”는 가정이 필요하지 않을 것입니다: 우리는 다항식 아이디얼을 다루고 있으므로, 어쨌든 모든 원소가 암묵적으로 그 안에 존재하기 때문입니다.

## §86.5 $\text{Spec } \mathbb{Z}$ , 1차원 스킴

$\text{Spec } \mathbb{Z}$ 의 좋은 점은 이것 역시 1차원 스킴이라는 점에서 기본적으로  $\text{Spec } k[x]$ 처럼 생겼다는 것입니다. 이는 두 종류의 소 아이디얼을 갖습니다:

- 모든 유리 소수  $p$ 에 대한  $(p)$ ,
- 그리고 생성점  $(0)$ .

그러므로 그림은 거의 변하지 않습니다.



이번에는  $\eta = (0)$ 이 줄기  $\mathbb{Z}_{(0)} = \mathbb{Q}$ 를 가지므로, “유리 함수”는 문자 그대로 유리수입니다! 따라서  $\frac{20}{19}$ 는 (2)에서 이중근을, (5)에서 근을, (19)에서 단순극을 가지는 함수입니다. 만약 이를  $\mathfrak{p} = (7)$ 에서 계산하면,  $4 \pmod{7}$ 을 얻습니다. 일반적으로, 잉여체는 여러분이 짐작하는 대로입니다:

$$\kappa((p)) = \mathbb{Z}/(p) \cong \mathbb{F}_p$$

각 소수  $p$ 에 대해, 그리고  $\kappa((0)) \cong \mathbb{Q}$ .

줄기는 닫힌 점에서의 잉여체보다 더 큼니다: 예를 들어

$$\mathcal{O}_{\text{Spec } \mathbb{Z}, (3)} \cong \left\{ \frac{m}{n} \mid 3 \nmid n \right\}$$

3에서 극점이 없는 유리수들로 구성됩니다. 일반점에서의 줄기는  $\mathbb{Z}_{(0)} \cong \text{Frac } \mathbb{Z} = \mathbb{Q}$ 입니다.

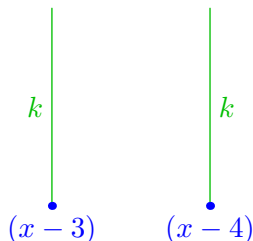
## §86.6 $\text{Spec } k[x]/(x^2 - 7x + 12)$ , 두 점

만약 우리가 아핀 다양체를 다루고 있었다면, 답이 무엇인지 이미 알고 있었을 것입니다:  $x^2 - 7x + 12 = 0$ 은  $x = 3$ 과  $x = 4$ 라는 해를 가지므로, 이것은 두 점을 가진 스킴이어야 합니다.

이것이 실제로 성립함을 확인하기 위해, **명제 83.6.1**를 사용합니다:  $\text{Spec } k[x]/(x^2 - 7x + 12)$ 의 점들은  $(x^2 - 7x + 12)$ 를 포함하는  $k[x]$ 의 소 아이디얼에 대응해야 합니다.  $k[x]$ 가 PID 이므로,  $(x - 3)$ 과  $(x - 4)$  단 두 개만 존재합니다. 이들 각각은  $k[x]$ 와의 몫이 체(구체적으로  $k$ )이므로 극대 아이디얼이며, 따라서 약속했던 대로  $\text{Spec } k[x]/(x^2 - 7x + 12)$ 는 정확히 두 개의 닫힌점을 가집니다.

각 점 위의 줄기는  $k$ 와 동형입니다. 전체 공간  $X$  위의 단면은 단지  $(x - 3)$ 에서의 값과  $(x - 4)$ 에서의 값, 이렇게 두 값을 선택하는 것일 뿐입니다.

$$\text{Spec } k[x]/(x^2 - 7x + 12)$$



그러므로 사실 이것은 다음과 같은 환론적 사실을 기하학적으로 사고하는 방식입니다

$$k[x]/(x^2 - 7x + 12) \cong k \times k \quad \text{에 의해 } f \mapsto (f(3), f(4)).$$

또한 이것은 이 장에서 나오는 첫 번째 기약이 아닌 공간의 예시입니다: 실제로  $X$ 는 심지어 비연결입니다. 이에 따라 떠도는 일반점이 존재하지 않습니다: 공간이 이산적이므로, 모든 점이 닫힌점입니다.

## §86.7 $\text{Spec } k[x]/(x^2)$ , 이중점

이제 “이중점” 스킴에 대해 더 자세히 설명할 수 있습니다

$$X_2 = \text{Spec } k[x]/(x^2)$$

이것이 매우 중요한 동기 부여 예시이기 때문입니다. 이것은 “한 점” 스킴  $X_1 = \text{Spec } k[x]/(x) = \text{Spec } k$ 와 어떻게 다릅니까?  $X_2$ 와  $X_1$ 은 둘 다 정확히 한 점을 가지므로, 당연히 위상도 동일합니다.

차이점은 줄기(점이 하나뿐이므로 단면과 동등함)가 더 크다는 것입니다:

$$\mathcal{O}_{X_2, (x)} = \mathcal{O}_{X_2}(X_2) = k[x]/(x^2).$$

따라서 이중점 위에서 함수를 명시하려면, 하나가 아니라 두 개의 매개변수를 명시해야 합니다: 다항식을 취하면

$$f = a_0 + a_1x + \cdots \in k[x]$$

이를 이중점에서 평가하면  $a_0$ 과 소위 “일계도함수” 둘 다를 기억하게 됩니다.

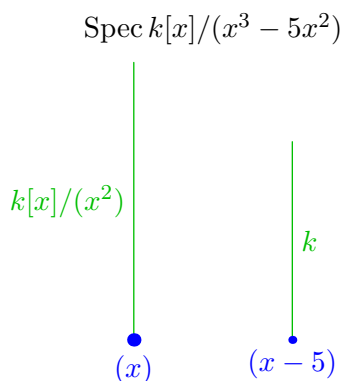
잉여체까지 완전히 내려가면 이중점과 단일점을 더 이상 구별할 수 없다는 점을 언급해야겠습니다. 왜냐하면  $(x)$ 에서의  $\text{Spec } k[x]/(x^2)$ 의 잉여체는

$$\text{Frac}(A/(x)) = \text{Frac } k = k.$$

따라서 값들의 집합은 여전히 그저  $k$ 일 뿐입니다(이는 지난 장 끝에서 나온 “떡영원” 논의로 이어집니다); 그러나 “풍부해진” 값을 가진 줄기는 그 차이를 구별할 수 있습니다.

## §86.8 $\text{Spec } k[x]/(x^3 - 5x^2)$ , 이중점과 단일점

앞의 두 예시를 나란히 놓아도 아무 문제가 없습니다: 스킴  $X = \text{Spec } k[x]/(x^3 - 5x^2)$ 은 단일점 옆에 이중점이 있는 것으로 구성됩니다. 줄기들이 서로 다르다는 점에 주목하십시오: 이중점 위의 줄기가 더 큽니다.



이번에는 암묵적으로 다음과 같은 환 동형사상을 가집니다

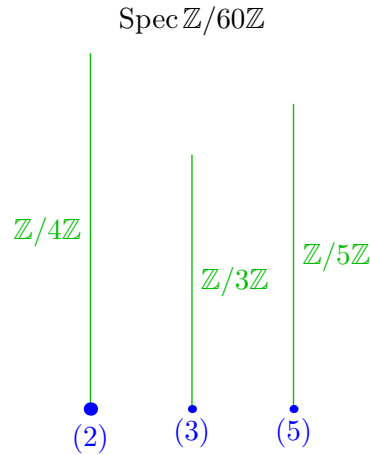
$$k[x]/(x^3 - 5x^2) \cong k[x]/(x^2) \times k$$

$f \mapsto (f(0) + f'(0)x, f(5))$ 에 의한 것입니다. 여기서 도함수는 형식적인 의미로 사용됩니다!

## §86.9 $\text{Spec } \mathbb{Z}/60\mathbb{Z}$ , 세 점을 가진 스킴

환의 곱에 대한 기하학적 예시들이 계속 나타나는 것을 보아왔지만, 사실 정수에서 익숙한 중국인의 나머지 정리도 다르지 않습니다. (이 예시  $X = \text{Spec } \mathbb{Z}/60\mathbb{Z}$ 은 [Val17, §4.4.11]에서 가져온 것입니다.)

**명제 83.6.1**에 의해,  $\mathbb{Z}/60\mathbb{Z}$ 의 소 아이디얼은  $(2)$ ,  $(3)$ ,  $(5)$ 입니다. 하지만 이것을  $\text{Spec } \mathbb{Z}$ 로부터 나온 것으로도 생각할 수 있습니다: 60은  $(2)$ 에서 이중근을 가지고,  $(3)$ 과  $(5)$ 에서는 단일근을 가지는 함수였기 때문입니다.



사실, 제가 지금까지 환 동형사상을 주장해왔지만, 층이야말로 실제로 완전한 증명을 제공해줍니다. 이를 전역 단면의 관점에서 표현해 보겠습니다:

$$\begin{aligned}
 \mathbb{Z}/60\mathbb{Z} &= \mathcal{O}_X(X) \\
 &= \mathcal{O}_X(\{(2)\}) \times \mathcal{O}_X(\{(3)\}) \times \mathcal{O}_X(\{(5)\}) \\
 &= \mathcal{O}_{X,(2)} \times \mathcal{O}_{X,(3)} \times \mathcal{O}_{X,(5)} \\
 &= \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.
 \end{aligned}$$

따라서  $X = \operatorname{Spec} A$ 에 대해  $\mathcal{O}_X(X) = A$ 라는 정리가 여기서 “핵심 작업”을 하고 있습니다; 층의 공리들이 여기서부터 중국인의 나머지 정리를 이끌어냅니다.

이와 관련하여, 이는 앞서 든 예를 생각하는 한 가지 방법을 제공합니다

$$(\mathbb{Z}/60\mathbb{Z})[1/5] \cong \mathbb{Z}/12\mathbb{Z}.$$

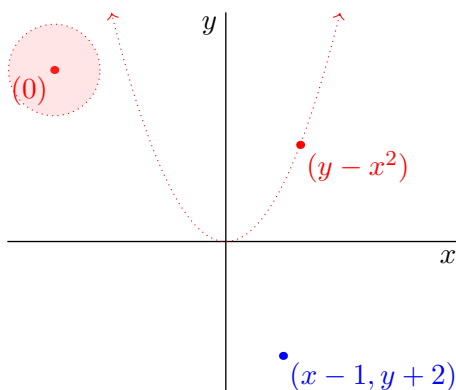
실제로  $\operatorname{Spec} \mathbb{Z}/60\mathbb{Z}[1/5]$ 는 특별열린집합  $D(5)$ 처럼 보여야 합니다: 이는 위 그림에서 점 (5)를 삭제한다는 것을 의미합니다. 그러면  $\mathbb{Z}/12\mathbb{Z}$ 가 남습니다.

## §86.10 $\operatorname{Spec} k[x, y]$ , 즉 이차원 평면

이 스킴은 이미 살펴본 적이 있습니다: 이는 평면으로 시각화됩니다. 세 가지 유형의 점이 있습니다:

- 닫힌점  $(x - a, y - b)$ 는 평면의 개별 점들로 이루어져 있습니다.
- 임의의 기약다항식  $f$ 에 대한 비닫힌점  $(f(x, y))$ 는 어떤 기약곡선을 따라 떠다닙니다. 이를 점이 떠다니는 점선 곡선을 그려서 나타냅니다.
- 생성점 (0)은 평면 전체를 따라 떠다닙니다. 그림에서 이를 어디에 두어야 좋을지 알지 못하므로, 그냥 어딘가에 두고 점선 원을 그려 표시하겠습니다.

다음은 세 가지 유형의 점을 모두 나타낸 그림입니다.



또한 각 점 위의 줄기도 계산해 보겠습니다.

- $(x - 1, y + 2)$  위의 줄기는  $g(1, -2) \neq 0$ 을 만족하는 유리함수  $\frac{f(x, y)}{g(x, y)}$ 들의 집합입니다.
- 비달린점  $(y - x^2)$  위의 줄기는  $g(t, t^2) \neq 0$ 을 만족하는 유리함수  $\frac{f(x, y)}{g(x, y)}$ 들의 집합입니다. 예를 들어 함수  $\frac{xy}{x+y-2}$ 는 여전히 문제가 없습니다; 분모가 포물선 위의 점  $(1, 1)$ 과  $(-2, 4)$ 에서 영이 되기는 하지만, 이는 포물선의 "생성점"(대략적으로 말하면 "대부분의 점")에서의 함수이기 때문입니다.
- $(0)$  위의 줄기는 유리함수의 분수체  $k(x, y)$  전체입니다.

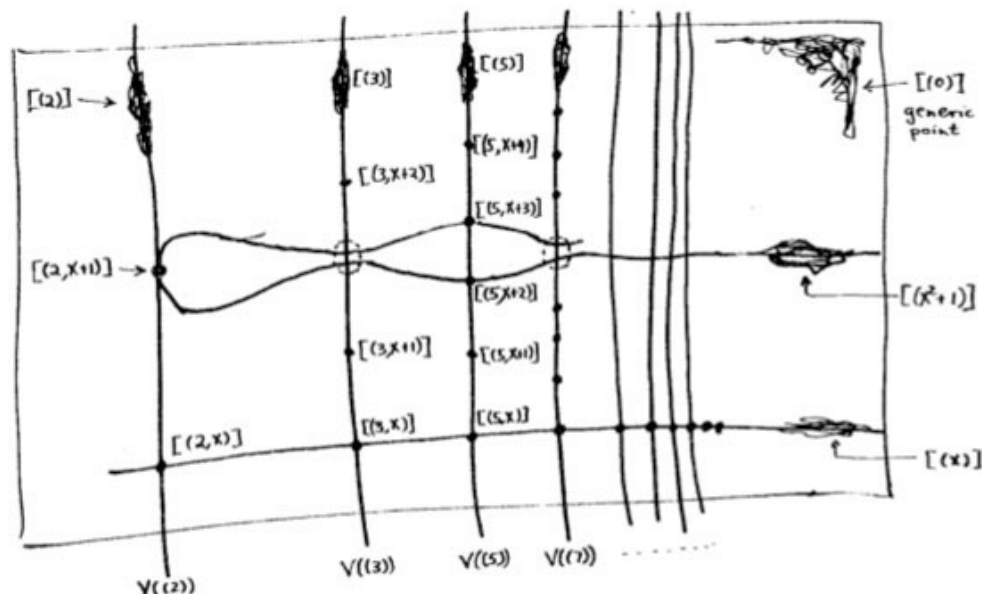
전역 절단  $f = x^2 + y^2$ 을 생각하고, 위의 각 점에서 그 값도 구해 보겠습니다.

- $f \pmod{x - 1, y + 2} = 5$ 이므로,  $f$ 는  $(x - 1, y + 2)$ 에서 값 5를 가집니다.
- 새로운 점은 포물선을 따라서도  $f$ 를 계산할 수 있다는 것입니다 — 이는 몫  $k[x, y]/(y - x^2)$ 에서 특정한 값을 부여받습니다. 예를 들어 이를  $f = x^2 + y^2 \equiv x^2 + x^4 \pmod{y - x^2}$ 로 생각할 수 있습니다. 포물선의 생성점에서  $f$ 의 값을 안다면, 그로부터 포물선 위의 임의의 닫힌점에서의 값도 계산할 수 있음을 주목하십시오.
- 생성점  $(0)$ 에서는  $f \pmod{0} = f$ 입니다. 따라서 다른 어떤 스킴에서와 마찬가지로 "생성점에서 계산하기"는 아무런 변화도 주지 않습니다.

## §86.11 $\text{Spec } \mathbb{Z}[x]$ , 이차원 스킴, 그리고 멤퍼드의 그림

우리는  $\text{Spec } \mathbb{Z}$ 가  $\text{Spec } k[x]$ 와 매우 비슷해 보인다는 것을 보았으며, 이제  $\text{Spec } \mathbb{Z}[x]$ 가  $\text{Spec } k[x, y]$ 와 매우 비슷해 보인다는 것을 확인하겠습니다.

이 스킴을 나타낸 유명한 그림이 멤퍼드의 "붉은 책"에 실려 있는데, 앞서 우리가 그린 그림들과 다소 차이가 있기는 하지만 문화 보존의 취지로 여기에 실어 보겠습니다.



멈퍼드는 점  $p$ 를 나타내는 데  $[p]$ 를 사용하는데, 우리는 그렇게 하지 않으므로 곳곳에 나타나는 대괄호는 무시해도 됩니다. 비닫힌점들은 솜뭉치 형태로 나타나 있습니다.

앞서와 마찬가지로 소 아이디얼에는 세 가지 유형이 있지만, 이번에는 모습이 다소 더 다르게 보일 것입니다:

- 닫힌점은 이제 순서쌍  $(p, f(x))$ 이며, 여기서  $p$ 는 소수이고  $f$ 는  $p$ 를 법으로 하는 기약 다항식입니다. 실제로 이들이 극대 아이디얼입니다: 몫  $\mathbb{Z}[x]/(p, f)$ 는  $\mathbb{F}_p$ 의 어떤 유한 확장이 됩니다.
- 이제 서로 다른 두 가지 "일차원" 비닫힌점이 있습니다:
  - 각 유리 소수는 점  $(p)$ 를 주고, 그리고
  - 각 기약 다항식  $f$ 는 점  $(f)$ 를 줍니다.

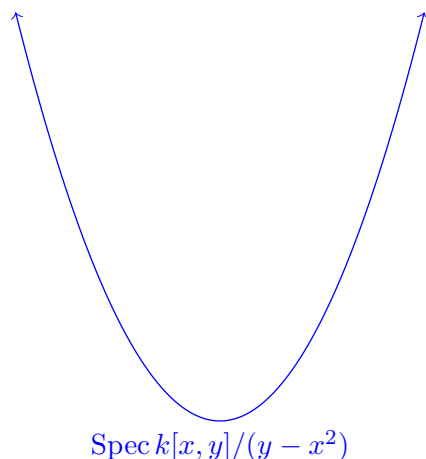
실제로,  $\mathbb{Z}[x]$ 를 각각으로 나눈 몫이 정역임에 주목하십시오.

- $\mathbb{Z}[x]$ 는 정역이므로, 언제나 그렇듯  $(0)$ 이 전체 공간에 대한 우리의 일반점입니다.

제가 다르게 하고 싶었던 부분이 하나 있는데,  $V(3)$ 과  $V(7)$ 에는 점  $(3, x^2 + 1)$ 이 있어야 하는데, 이는 그림에서 닫힌 점으로 그려지지 않고 오히려 점선 타원으로 그려져 있습니다. 이는 위상적인 의미에서는 옳지 않습니다:  $\mathfrak{m} = (3, x^2 + 1)$ 이 극대 아이디얼이므로, 이는 실제로 스킴 내의 하나의 닫힌 점이기 때문입니다. 하지만 이것이 "두 개"인 것처럼 여겨질 수 있는 이유는,  $\mathfrak{m}$ 에서의 잉여체인  $\mathbb{Z}[x]/(3, x^2 + 1)$ 이 이차원  $\mathbb{F}_3$  벡터 공간이기 때문입니다.

## §86.12 $\text{Spec } k[x, y]/(y - x^2)$ , 포물선

**명제 83.6.1**에 의해,  $k[x, y]/(y - x^2)$ 의 소 아이디얼들은  $(y - x^2)$ 의 상위집합인  $k[x, y]$ 의 소 아이디얼들에 대응하며, 이는 곧 닫힌집합  $V(y - x^2)$  안에 포함된  $\text{Spec } k[x, y]$ 의 점들에 대응합니다. 게다가,  $V(y - x^2)$  위의 부분공간 위상은  $\text{Spec } k[x, y]/(y - x^2)$  위의 위상과 일치합니다.



이는 훨씬 더 일반적으로 성립합니다:

**연습문제 86.12.1** (지루한 확인).  $I$ 가 환  $A$ 의 아이디얼이라면,  $\text{Spec } A/I$ 가 위상 공간으로서  $\text{Spec } A$ 의 닫힌 부분집합  $\mathcal{V}(I)$ 와 위상동형임을 보이십시오.

그래서 이것이 "닫힌 매장"이라는 개념입니다:  $\text{Spec } k[x, y]$ 의 닫힌 부분집합이었던 포물선 자체가 하나의 스킴입니다. 사상이라는 개념을 실제로 정의하고 나면, 이에 대해 더 많은 것을 말할 수 있을 것입니다.

다만 이 스킴 위의 층은 포물선 위의 함수들만을 기억할 뿐입니다: 즉 줄기들이 말하자면 "물려받아야지" 않습니다. 이를 확인하기 위해, 원점에서의 줄기를 계산해 봅시다: **정리 83.7.1**에 따르면 그것은

$$k[x, y]_{(x, y)}/(y - x^2) \cong k[x, x^2]_{(x, x^2)} \cong k[x]_{(x)}$$

원점에서의 아핀 직선  $\text{Spec } k[x]$ 의 줄기와 같습니다. 직관적으로 놀랍지 않은데, 원점 근처의 포물선 위 어떤 점을 보더라도 그것은 본질적으로 직선처럼 보이며, 그 위의 함수들도 마찬가지이기 때문입니다.

일반점 위의 줄기는  $\text{Frac}(k[x, y]/(y - x^2))$ 입니다: 즉  $y = x^2$ 이라는 동일시를 갖는 유리 함수들입니다. 이 역시 놀랍지 않습니다.

마지막으로,  $y \mapsto x^2$ 을 보내는 동형사상  $k[x, y]/(y - x^2) \cong k[x]$ 가 존재하므로, 포물선이 실제로  $\text{Spec } k[x]$ 와 동형일 것이라 예상됩니다. 그림으로 보면, 이는 포물선을 "퍼는" 것처럼 보입니다. 일반적으로, 두 환  $A$ 와  $B$ 가 동형일 때  $\text{Spec } A$ 와  $\text{Spec } B$ 가 "같아야" 한다고 기대하고 싶은데 (그렇지 않다면 우리는 경악할 것입니다), 이후에 실제로 그러함을 보게 될 것입니다.

## §86.13 $\text{Spec } \mathbb{Z}[i]$ , 가우스 정수 (일차원)

정수의 경우에서 이 발상을 좀 더 가지고 돌아볼 수 있습니다.

$$\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2 + 1)$$

임에 주목하십시오. 이는 이것이  $\text{Spec } \mathbb{Z}[x]$  안의 "일차원" 닫힌집합임을 의미합니다. 이러한 방식으로, 원소들이 가우스 소수인 스킴을 얻게 됩니다.

어떤 닫힌 점이 다른 것보다 "더 큼"은 잉여체를 봄으로써 알 수 있습니다. 예를 들어 점  $(2 + i)$ 의 잉여체는

$$\kappa((2 + i)) = \mathbb{Z}[i]/(2 + i) \cong \mathbb{F}_5$$

하지만 점 (3)의 잉여체는

$$\kappa((3)) \cong \mathbb{Z}[i]/(3) \cong \mathbb{F}_9$$

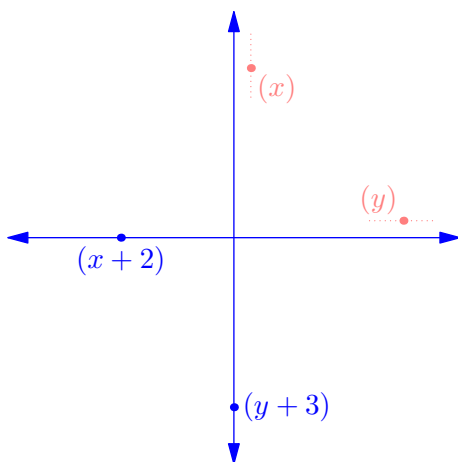
이는 이차  $\mathbb{F}_3$ -확대입니다.

## §86.14 긴 예제: $\text{Spec } k[x, y]/(xy)$ , 두 축

이것은 기약이 아닌 스킴의 첫 번째 예가 될 것입니다.

### §86.14.i 그림

이전과 마찬가지로, 위상적으로 이는  $\text{Spec } k[x, y]$ 의 닫힌집합  $\mathcal{V}(xy)$ 처럼 보입니다. 그림은 다음과 같습니다:



상황이 잘 맞는지 확인하기 위해:

**질문 86.14.1** (건전성 확인).  $(y+3)$ 이 실제로  $\mathcal{V}(x)$  안에 놓인  $\text{Spec } k[x, y]/(xy)$ 의 극대 아이디얼임을 확인하십시오.

아이디얼 (0)은 더 이상 소 아이디얼이 아니므로, 이 공간의 점이 아닙니다. 오히려 이번에는 두 개의 비폐점, 즉 아이디얼  $(x)$ 와  $(y)$ 가 있으며, 이들은 두 축 각각을 감싸며 떠다니는 모습으로 시각화할 수 있습니다. 이 공간은 두 개의 진부분 닫힌집합의 합집합  $\mathcal{V}(x) \cup \mathcal{V}(y)$ 로 쓸 수 있으므로 가약(reducible)입니다. (위상 공간으로서는 여전히 연결되어 있습니다.)

### §86.14.ii $y$ -축 버리기

특수 열린집합  $U = D(x)$ 를 생각해 봅시다. 이는  $\mathcal{V}(x)$ , 즉  $y$ -축을 삭제하는 것에 해당합니다. 따라서  $D(x)$ 는 원점을 삭제한  $\text{Spec } k[x]$ 와 “같아야” 하며, 특히 절단면으로  $k[x, x^{-1}]$ 를 얻어야 한다고 예상합니다. 실제로,

$$\begin{aligned} \mathcal{O}_{\text{Spec } k[x, y]/(xy)}(D(x)) &\cong (k[x, y]/(xy))[1/x] \\ &\cong k[x, x^{-1}, y]/(xy) \cong k[x, x^{-1}, y]/(y) \cong k[x, x^{-1}]. \end{aligned}$$

여기서  $(xy) = (y)$ 는  $x$ 가 단원(unit)이라는 사실로부터 따라 나옵니다. 모든 것이 계획대로입니다.

### §86.14.iii 몇몇 점 위의 줄기

점  $\mathfrak{m} = (x+2)$  위의 줄기를 계산해 봅시다. 이 점은  $x$ -축 위의 점  $(-2, 0)$ 으로 생각할 수 있습니다. (좀 더 편하게 느끼고 싶다면,  $\mathfrak{m} \ni y(x+2) = 2y$ 이므로  $y \in \mathfrak{m}$ 이고, 따라서  $\mathfrak{m} = (x+2, y)$ 로도 쓸 수 있음에 주목하십시오.) 줄기는 다음과 같습니다.

$$\mathcal{O}_{\text{Spec } k[x,y]/(xy), \mathfrak{m}} = (k[x, y]/(xy))_{(x+2)}.$$

하지만 저는 이 국소화에서  $y$ 가 영원(zero element)이 된다고 주장합니다. 실제로  $\frac{y}{1} = \frac{0}{x} = 0$ 입니다. 따라서 전체가 다음으로 붕괴됩니다.

$$\mathcal{O}_{\text{Spec } k[x,y]/(xy), \mathfrak{m}} = k[x]_{(x+2)}$$

이는 어차피  $\text{Spec } k[x]$ 에서  $(x+2)$ 의 줄기입니다. 이는 예상된 결과입니다. 두 직선으로 이루어진 공간이 있지만 원점에서 떨어진 곳에서 있다면, 줄기는 그 멀리 떨어진 점에서의 이상한 거동을 포착하지 못합니다. 그것은 오직  $\mathfrak{m}$  근처에서 일어나는 일에만 관심이 있으므로, 그곳에서는 그냥 아핀 직선처럼 보입니다.

**비고 86.14.2** —  $(k[x, y]/(xy))_{(x+2)}$ 는  $k[x, y]_{(x+2)}/(xy)$ 와 같지 않다는 점에 주목하십시오. 여기서는 순서가 중요합니다. 실제로 후자는 영환(zero ring)인데,  $x$ 와  $y$ 가 모두, 따라서  $xy$ 도 단원이기 때문입니다.

( $x$ -축을 감싸며 떠다니는) 일반점 ( $y$ )도 비슷한 이야기를 들려줄 것입니다. 그 위의 줄기를 살펴보면, “거의 모든” 점들이  $y$ -축의 존재를 인식하지 못하는 것과 마찬가지로, 이 줄기 역시 그것을 인식하지 못한다는 것을 알게 될 것입니다. 실제로 줄기를 계산해 보면:

$$\mathcal{O}_{\text{Spec } k[x,y]/(xy), (y)} = (k[x, y]/(xy))_{(y)}.$$

다시  $\frac{y}{1} = \frac{0}{x} = 0$ 이므로, 이는 그냥

$$\mathcal{O}_{\text{Spec } k[x,y]/(xy), (y)} \cong k[x]_{(0)} \cong k(x).$$

이는 우리가 예상했던 바입니다 (이는  $\text{Spec } k[x]$ 에서  $(0)$  위의 줄기와 동일합니다).

### §86.14.iv 원점 위의 줄기 (까다로운 경우)

원점  $(x, y)$  위의 줄기는 흥미로우며, 가군의 국소화를 이야기하지 않고는 완전히 탐구할 수 없는 개념들을 담고 있습니다. 국소화는 다음과 같이 주어집니다.

$$(k[x, y]/(xy))_{(x,y)}$$

따라서 원소들은 다음과 같아야 합니다.

$$\frac{c + (a_1x + a_2x^2 + \dots) + (b_1y + b_2y^2 + \dots)}{c' + (a'_1x + a'_2x^2 + \dots) + (b'_1y + b'_2y^2 + \dots)}$$

여기서  $c' \neq 0$ 입니다.

이 특성화가 만족스럽지 않게 느껴질 수도 있습니다. 다음은 기하학적 직관입니다. 전역 절단면 환은 다음과 같이 쓸 수 있습니다.

$$k[x, y]/(xy) = c + (a_1x + a_2x^2 + \dots) + (b_1y + b_2y^2 + \dots)$$

이는 모든 전역 절단면이  $x$ -다항식과  $y$ -다항식의 합이라는 뜻입니다. 하지만 이는 단순한 환의 곱  $k[x] \times k[y]$ 는 아닙니다. 상수항이 공유되기 때문입니다. 그러므로 이는  $k[x]$ 와  $k[y]$ 에서 상수항이 일치하는 다항식 쌍으로 생각하는 것이 더 낫습니다.

범주론을 좋아하신다면, 이는 결국 다음과 같은 올곱(fibered product)입니다.

$$k[x, y]/(xy) \cong k[x] \times_k k[y]$$

사상은  $x$ 와  $y$ 를 0으로 보내는  $k[x] \rightarrow k$ 와  $k[y] \rightarrow k$ 입니다. 이런 식으로  $k[x, y]/(xy)$ 를 대체로 두 성분으로 분해할 수 있습니다.

우리는 줄기에 대해서도 정말로 똑같이 할 수 있어야 합니다. 우리는 다음과 같이 말하고 싶습니다.

$$\mathcal{O}_{\text{Spec } k[x, y]/(xy), (x, y)} \cong k[x]_{(x)} \times_k k[y]_{(y)}.$$

한국어로 번역하면: “전형적인” 배아는  $\frac{3+x}{x^2+7} + \frac{4+y^3}{y^2+y+7}$ 처럼 생겨야 하며,  $x$  부분과  $y$  부분이 서로 분리되어 있어야 합니다. 동등하게, 줄기는 원점에서 일치하는  $x$ -배아와  $y$ -배아의 쌍들로 이루어져야 합니다.

실제로 이는 참입니다! 놀랍게 느껴질 수도 있지만, 우리가 왜 이것을 예상하는지 살펴봅시다. 다음 배아를 생각해 봅시다.

$$\frac{1}{1 - (x + y)}.$$

숨을 참고 보면, 이를 기하급수  $1 + (x + y) + (x + y)^2 + \dots$ 로 전개할 수 있다고 상상해볼 수 있습니다.  $xy = 0$ 이므로, 이는 그저  $1 + x + x^2 + x^3 + \dots + y + y^2 + y^3 + \dots$ 가 됩니다. 이는 (쓰인 그대로는) 말이 되지 않지만, 그럼에도 다음의 추측을 시사합니다

$$\frac{1}{1 - (x + y)} = \frac{1}{1 - x} + \frac{1}{1 - y} - 1$$

실제로 참임을 검증할 수 있는 것입니다.

**질문 86.14.3.** 이 항등식이 성립하는지 확인하십시오.

물론 이는 단 하나의 간단한 예시를 위한 계산치고는 상당히 많습니다. 이를 일반화할 방법이 있을까요? 있습니다: 핵심 주장은 “국소화는 극한과 교환한다”는 것입니다. 원한다면 지금 그 명제를 직접 유도해 볼 수 있지만, 여기서는 그렇게 하지 않겠습니다.

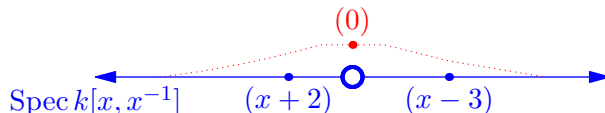
## §86.15 $\text{Spec } k[x, x^{-1}]$ , 구멍 뚫린 직선(또는 쌍곡선)

이는  $\text{Spec } k[x]$ 의  $D(x)$ 처럼, 즉 원점이 제거된 직선처럼 보여야 합니다. 대안적으로는 다음과 같이 쓸 수도 있습니다

$$k[x, x^{-1}] \cong k[x, y]/(xy - 1)$$

그래서 이 스킴은 쌍곡선으로도 그려질 수 있습니다.

먼저, 1차원 그림은 다음과 같습니다.

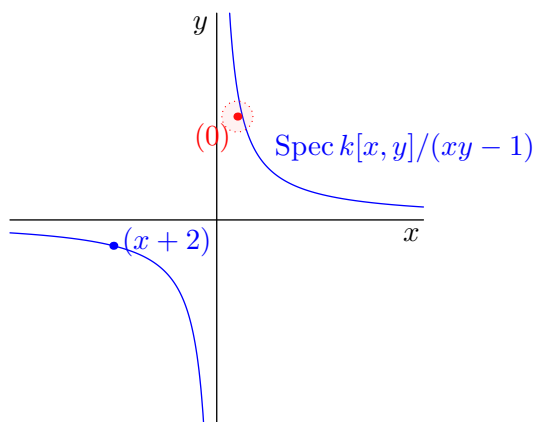


사실 이 스킴은  $\text{Spec } k[x, y]/(xy)$ 를 다루면서  $D(y)$ 를 살펴보았을 때 이미 본 적이 있습니다. 어쨌든, 이제  $(x - 3)$ 에서의 줄기를 계산해 봅시다; 그것은

$$\mathcal{O}_{\text{Spec } k[x, x^{-1}], (x-3)} \cong k[x, x^{-1}]_{(x-3)} \cong k[x]_{(x-3)}$$

$x^{-1}$ 는 어차피  $k[x]_{(x-3)}$  안에 있기 때문입니다. 그러므로 다시 한 번, 원점을 제거하는 것이 더 멀리 떨어진 점  $(x - 3)$ 에서의 줄기에는 영향을 미치지 않음을 알 수 있습니다.

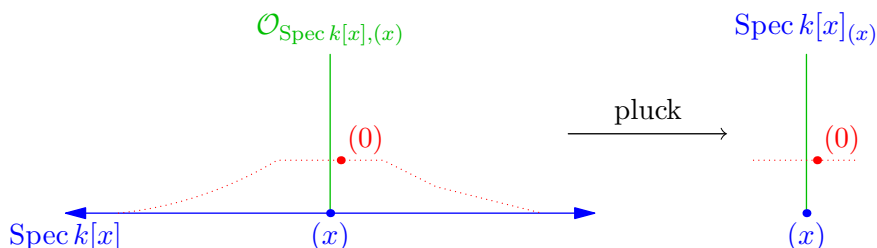
앞서 언급했듯이,  $k[x, x^{-1}]$ 는  $k[x, y]/(xy - 1)$ 와 동형이므로, 같은 곡선을 시각화하는 또 다른 방법은 쌍곡선을 그리는 것입니다(이것이 납작해지면 구멍 뚫린 직선이 된다고 상상할 수 있습니다).  $k[x, y]/(xy - 1)$ 가 실제로 정역이기 때문에 생성점 (0)이 하나 존재하며, 이와 더불어  $(x + 2, y + 1/2) = (x + 2) = (y + 1/2)$ 와 같은 점들도 존재합니다.



### §86.16 $\text{Spec } k[x]_{(x)}$ , 직선의 원점을 확대한 모습

우리는 이미  $\mathcal{O}_{\text{Spec } A_p} \cong A_p$ 임을 알고 있습니다: 따라서  $A_p$ 는  $p$ 에서의 줄기여야 합니다. 이 예시에서는  $\text{Spec } A_p$  또한 이 줄기와 비슷하게 그려져야 함을 보게 될 것입니다.

앞서 우리는  $\text{Spec } k[x]$ 의 그림을 그리는 방법을 살펴보았습니다. 여러분은 원점  $(x)$  위의 줄기(stalk) 그림도 그릴 수 있는데, 농업을 좋아한다면  $(x)$  위에 자라나는 풀이나 다른 식물로 상상해 볼 수도 있습니다. 이 경우,  $\text{Spec } k[x]_{(x)}$ 는 아핀 직선에서 그 줄기를 뽑아냈을 때 나타나는 모습처럼 보일 수 있습니다.



$k[x]_{(x)}$ 는 국소환이므로(소 아이디얼의 국소화이므로), 이 공간에는 닫힌 점이 하나뿐입니다: 극대 아이디얼  $(x)$ 입니다. 그러나 놀랍게도, 점이 하나 더 있습니다: “생성” 점 (0)입니다. 따라서  $\text{Spec } k[x]_{(x)}$ 는 두 점으로 이루어진 공간이지만, 이산 위상을 갖지는 않습니다:  $(x)$ 는 닫힌 점이지만 (0)은 그렇지 않습니다. (이 때문에 이 공간은 다양한 종류의 연습문제에 좋은 반례가 됩니다.)

그러므로 위상적으로 일어나는 일은,  $(x)$ 로 확대해 들어갈 때 “모든 점에 가까웠던” 생성점 (0)이 점  $(x)$  위에 떠 있는 채로 그대로 남는다는 것입니다.

유일한 닫힌 점  $(x)$  위의 줄기는 이전과 동일하다는 점에 주목하십시오:

$$(k[x]_{(x)})_{(x)} \cong k[x]_{(x)}.$$

실제로, 일반적으로  $R$ 이 극대 아이디얼  $\mathfrak{m}$ 을 갖는 국소환이면  $R_{\mathfrak{m}} \cong R$ 입니다. 어차피  $\mathfrak{m}$ 에 속하지 않는 모든 원소  $x \notin \mathfrak{m}$ 는 가역원이었기 때문입니다. 따라서 그림에서 줄기는 동일하게 그려집니다.

마찬가지로, (0) 위의 줄기도 뽑아내기 전과 동일합니다:

$$(k[x]_{(x)})_{(0)} = \text{Frac } k[x]_{(x)} = k(x).$$

더 일반적으로:

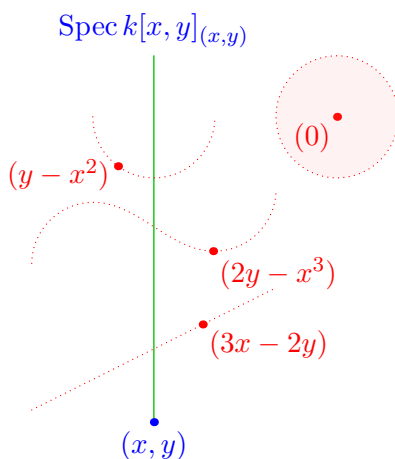
**연습문제 86.16.1.**  $A$ 를 하나의 환이라 하고,  $\mathfrak{q} \subseteq \mathfrak{p}$ 를 소 아이디얼이라 합시다.  $\mathfrak{q}$ 를  $A_{\mathfrak{p}}$ 의 소 아이디얼로 볼 때,  $A_{\mathfrak{q}} \cong (A_{\mathfrak{p}})_{\mathfrak{q}}$ 임을 확인하십시오.

그러므로 이렇게 확대해 들어갈 때, 닫힌 점이 아닌 점들 위에서도 모든 줄기는 그대로 유지됩니다.

### §86.17 $\text{Spec } k[x, y]_{(x, y)}$ , 평면의 원점을 확대한 모습

$\text{Spec } k[x, y]$ , 즉 2차원 평면의 원점 위에 있는 줄기를 뽑아내면 상황이 더욱 놀라워집니다.  $\text{Spec } k[x, y]_{(x, y)}$ 의 점들은  $(x, y)$ 에 포함되는  $k[x, y]$ 의 소 아이디얼들이어야 합니다; 기하학적으로 이들은  $(x, y)$  자체와 원점을 지나는 생성점들입니다. 예를 들어,  $k[x, y]_{(x, y)}$ 에는 포물선  $(y - x^2)$ 에 대응하는 생성점이 존재하고, 직선에 대응하는 또 다른 생성점  $(y - x)$ 도 존재하는 식입니다.

그리하여 우리는 맨 아래에 놓인 유일한 닫힌 점  $(x, y)$ 와, 그 위에 떠 있는 온갖 “1차원” 생성점들 — 직선, 포물선, 그 밖에 무엇이든 — 을 갖게 됩니다. 마지막으로, 2차원 상에 떠 있는 생성점  $(0)$ 이 있는데, 이 점의 폐포는 공간 전체와 같습니다.



### §86.18 $\text{Spec } k[x, y]_{(0)} = \text{Spec } k(x, y)$ , 일반점 위의 줄기

평면의 일반점은 줄기로 그저  $\text{Spec } k(x, y)$ 를 가집니다: 이는 체의 스펙트럼이므로 단일 점입니다. 이 줄기는  $\text{Spec } k[x, y]$ 에 심어졌을 때와 비교하여 그대로 유지됩니다; 함수들은 정확히  $x$ 와  $y$ 의 유리 함수들입니다.

### §86.19 생각해 볼 만한 조금 더 어려운 문제

**문제 86A.**  $\text{Spec } \mathbb{Z}[1/55]$ 의 그림을 그리고, 위상을 서술하며, 각 점에서의 줄기를 계산하십시오.

**문제 86B.**  $\text{Spec } \mathbb{Z}_{(5)}$ 의 그림을 그리고, 위상을 서술하며, 각 점에서의 줄기를 계산하십시오.

**문제 86C.**  $A = (k[x, y]/(xy))[(x + y)^{-1}]$ 라 합시다.  $\text{Spec } A$ 의 그림을 그리십시오. 이것이 위상 공간으로서 연결되어 있지 않음을 보이십시오.

**문제 86D.**  $A = k[x, y]_{(y - x^2)}$ 라 합시다.  $\text{Spec } A$ 의 그림을 그리십시오.

# 87 국소 환 달린 공간의 사상

국소 환 달린 공간의 정의를 설정했으니, 이제 이들 사이의 사상을 정의할 준비가 거의 되었습니다. 이 장 전체에서, 여러분의 환 달린 공간을 우리가 그토록 공들여 정의한 아핀 스킴이라고 상상하십시오. 하지만 임의의 국소 환 달린 공간이라는 일반적인 설정에서 작업해도 달라지는 것은 없습니다.

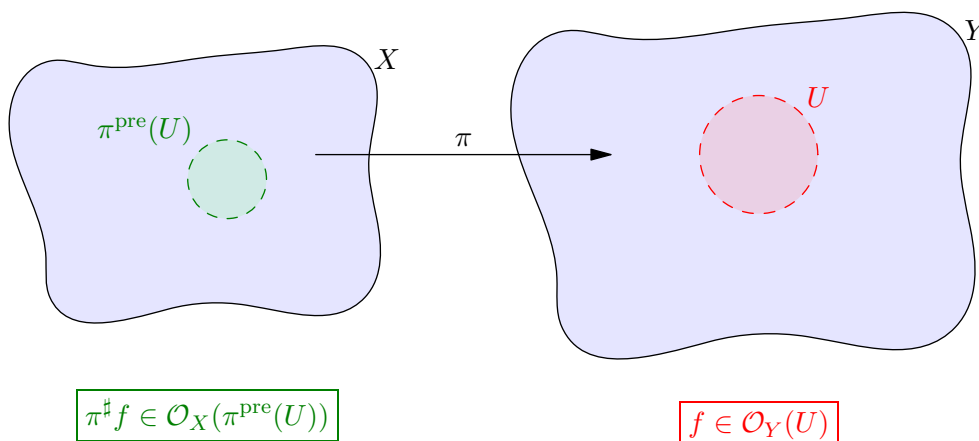
## §87.1 단면을 통한 환 달린 공간의 사상

$(X, \mathcal{O}_X)$ 와  $(Y, \mathcal{O}_Y)$ 를 환 달린 공간이라 합시다. 이들 사이에 함수  $\pi: X \rightarrow Y$ 가 있다는 것이 무엇을 의미하는지 정의하고자 합니다.<sup>1</sup> 먼저 이 사상이 연속이어야 한다는 조건을 요구하지만, 이것만으로는 충분하지 않습니다. 그 위에는 층이 있기 때문입니다!

자, 여러분은 우리가 초급 환 달린 공간에 대해 했던 것을 기억할지도 모릅니다.  $U \subseteq Y$ 의 열린집합 위에 함수가 있을 때마다, 우리는  $\pi^{\text{pre}}(U) \subseteq X$  위에도 이에 대응하는 함수가 있기를 원했습니다. 초급 환 달린 공간의 경우, 이는 합성을 통해 이루어졌는데, 층의 원소들이 실제로 복소수 값을 갖는 함수였기 때문입니다:

$$\pi^\# \phi \text{ 다음과 같이 정의되었습니다 } \phi \circ \pi.$$

그 결과, 모든 열린집합  $U$ 에 대해 사상  $\mathcal{O}_Y(U) \rightarrow \mathcal{O}_X(\pi^{\text{pre}}(U))$ 를 얻었습니다.



이제 일반적인 국소 환 달린 공간의 경우, 단면은 그저 임의의 환일 뿐이며, 그다지 잘 다루지지 않을 수도 있습니다. 그래서 해결책은  $\pi^\#$ 의 데이터를 사상의 정의의 일부로 포함시키는 것입니다.

**비고 87.1.1** — **예제 87.4.2**에서 보게 되듯이, 대수적 다양체의 경우 사상이 위상 공간의 사상에 의해 유일하게 결정되는 상황과는 달리, 여기서는  $\pi^\#$ 가 사상  $\pi$ 에 의해 반드시 유일하게 결정되는 것은 아닙니다. 따라서  $\pi^\#$ 를 포함시키는 것이 필요합니다.

**정의 87.1.2.**  $(X, \mathcal{O}_X) \rightarrow (Y, \mathcal{O}_Y)$ 의 **환 달린 공간의 사상**은 쌍  $(\pi, \pi^\#)$ 로 구성되는데, 여기서  $\pi: X \rightarrow Y$ 는 (위상 공간의) 연속 사상이고,  $\pi^\#$ 는 환 준동형사상의 선택으로 구성됩니다

$$\pi_U^\#: \mathcal{O}_Y(U) \rightarrow \mathcal{O}_X(\pi^{\text{pre}}(U))$$

<sup>1</sup>표기상의 함의: 환 달린 공간의 경우,  $f$ 가 흔히 단면을 나타내는 데 쓰이므로  $\pi$ 는 사상을 나타내는 데 사용될 것입니다.

모든 열린집합  $U \subseteq Y$ 에 대해, 제한 도식이

$$\begin{array}{ccc} \mathcal{O}_Y(U) & \longrightarrow & \mathcal{O}_X(\pi^{\text{pre}}(U)) \\ \downarrow & & \downarrow \\ \mathcal{O}_Y(V) & \longrightarrow & \mathcal{O}_X(\pi^{\text{pre}}(V)) \end{array}$$

$V \subseteq U$ 에 대해 가환하도록 합니다.

**표기의 남용 87.1.3.**  $(\pi, \pi^\sharp): (X, \mathcal{O}_X) \rightarrow (Y, \mathcal{O}_Y)$ 를 그냥  $\pi: X \rightarrow Y$ 로 줄여 쓰겠습니다. 비록 이 표기가 위상 공간에 대한 표기와 정확히 동일하다는 사실에도 불구하고 말입니다.

명백한 항등 사상이 존재하며, 따라서 우리는 동형사상 등도 범주론적인 방식으로 정의할 수 있습니다.

## §87.2 줄기를 통한 환 달린 공간의 사상

놀랍지 않게도, 우리가 국소화를 사랑하게 된 지금, 단면은 줄기보다 다루기 더 번거롭습니다. 그러므로 모든 열린집합  $U$ 에서  $\pi^\sharp_U$ 를 명시하는 대신, 줄기를 통해 그렇게 할 수 있다면 더 나을 것 같습니다(줄기는 열린집합보다 수가 적으므로, 이렇게 하면 많은 수고를 덜 수 있습니다!).

먼저 우리가 실제로 줄기의 사상을 얻는다는 것을 관찰하는 것부터 시작합시다.

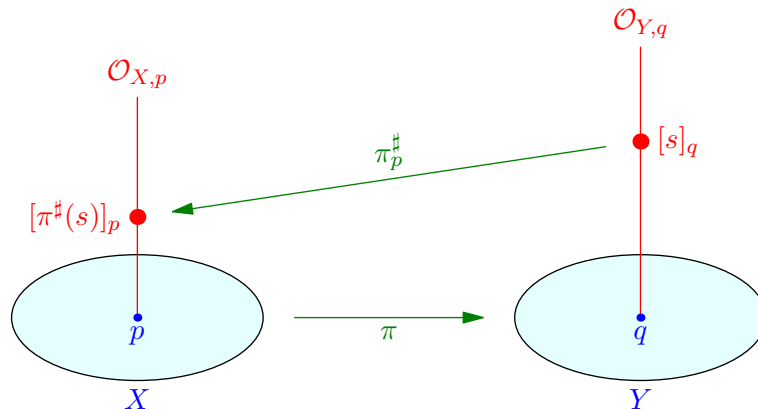
### 명제 87.2.1 (유도된 줄기 사상)

$\pi: X \rightarrow Y$ 가  $\pi(p) = q$ 를 보내는 환 달린 공간의 사상이라면, 우리는 사상을 얻습니다

$$\pi^\sharp_p: \mathcal{O}_{Y,q} \rightarrow \mathcal{O}_{X,p}$$

$\pi(p) = q$ 일 때마다 그러합니다.

이는 국소 환 달린 공간의 사상을, 위상 공간 위의 연속 사상에 더해,  $\pi(p) = q$ 인 각 경우마다  $q$ 에서의 각 짝을  $p$ 에서의 짝으로 대응시키는 배정으로 그릴 수 있음을 의미합니다.



다시, 이를 당겨오기 그림과 비교해 봅시다. 이는 대략, 함수  $f$ 가  $q$ 에서 어떤 풍부한 값을 가진다면,  $\pi^\sharp(f)$ 는  $p$ 에서 그에 대응하는 풍부한 값을 배정받아야 한다는 것을 말하고 있습니다.  $q$ 와  $p$ 에서의 줄기가 일반적으로 서로 다른 환일 수 있으므로 이 유비가 완벽하지는 않지만, 적어도 환 준동형사상(그 배정)은 있어야 합니다.

**증명.**  $(s, U)$ 가  $q$ 에서의 짝이라면,  $(\pi^\sharp(s), \pi^{\text{pre}}(U))$ 는  $p$ 에서의 짝이며, 이는 제한과의 호환성 덕분에 잘 정의된 사상입니다.  $\square$

우리는 이미 다음과 같은 의미에서 유일성을 명백히 가지고 있습니다.

**명제 87.2.2 (줄기를 통한 사상의 유일성)**

환 달린 공간의 사상  $(\pi, \pi^\sharp): (X, \mathcal{O}_X) \rightarrow (Y, \mathcal{O}_Y)$ 와 그에 대응하는 줄기의 사상  $\pi_p^\sharp$ 를 생각합시다. 그러면  $\pi^\sharp$ 는  $\pi_p^\sharp$ 에 의해 유일하게 결정됩니다.

증명. 단면  $s \in \mathcal{O}_Y(U)$ 가 주어졌을 때, 다음과 같이 놓습니다

$$t = \pi_U^\sharp(s) \in \mathcal{O}_X(\pi^{\text{pre}}(U))$$

$\pi^\sharp$  아래에서의 상을 나타냅니다.

각  $p \in \pi^{\text{pre}}(U)$ 에 대해  $t_p$ 를 알고 있는데, 이는 정의에 의해  $\pi_p^\sharp(t)$ 와 같기 때문입니다. 즉,  $t$ 의 모든 싹을 알고 있습니다. 따라서  $t$ 를 알고 있습니다.  $\square$

그러나 모든 줄기 사상의 선택이  $\pi_U^\sharp$ 로 이어지는 것은 아님이 분명해 보입니다: 일종의 “연속성” 또는 “호환성”이 필요합니다. 실제로 명시적인 진술을 적어볼 수 있습니다:  $U$  위의 호환 가능한 싹들의 수열은 각각  $\pi^{\text{pre}}(U)$  위의 호환 가능한 싹들의 수열로 대응되어야 합니다. 지금은 이에 대한 형식적인 진술을 제시하지 않는데, 그 진술이 다루기 번거롭고, 곧 실제 사례에서 (더 이해가 잘 되는 형태로) 보게 될 것이기 때문입니다.

**비고 87.2.3 (동형사상은 줄기에 의해 결정됩니다)** — 증명하지는 않겠지만 알아두면 좋은 사실이 하나 있습니다: 환 달린 공간의 사상  $(\pi, \pi^\sharp): (X, \mathcal{O}_X) \rightarrow (Y, \mathcal{O}_Y)$ 가 동형 사상인 것은  $\pi$ 가 위상동형사상이고, 게다가 각  $p \in X$ 에 대해  $\pi_p^\sharp$ 가 동형사상인 것과 동치입니다.

## §87.3 국소 환 달린 공간의 사상

한편, 우리의 줄기들이 국소환이라는 사실을 보았는데, 이는 실제로 값에 대해 이야기할 수 있게 해줍니다. 그래서 우리는 값의 개념이 보존되도록 보장하기 위해 호환성 조건을 하나 더 추가하고자 합니다. 이제 앞의 그림에서  $p$ 와  $q$ 에서의 줄기는 서로 다를 수 있으므로,  $\kappa(p)$ 와  $\kappa(q)$ 는 서로 다른 체일 수도 있습니다.

**정의 87.3.1. 국소 환 달린 공간의 사상**이란 다음과 같은 추가 성질을 만족하는 환 달린 공간의 사상  $\pi: X \rightarrow Y$ 를 말합니다:  $\pi(p) = q$ 일 때마다, 줄기에서의 사상 또한 잘 정의된 환 준동형사상을 유도합니다.

$$\pi_p^\sharp: \kappa(q) \rightarrow \kappa(p).$$

그래서 우리는  $\pi_p^\sharp$ 가 잉여체에서 체 준동형사상을 유도할 것을 요구합니다<sup>2</sup>. 특히,  $\pi^\sharp(0) = 0$ 이므로, 이는 매우 중요한 무언가를 의미합니다:

**국소 환 달린 공간의 사상에서, 어떤 싹이  $q$ 에서 소멸하는 것은 대응하는 싹이  $p$ 에서 소멸하는 것과 동치입니다.**

**연습문제 87.3.2** (이른바 “국소환 준동형사상”). 이것이 다음을 요구하는 것과 동치임을 보이십시오

$$(\pi_p^\sharp)^{\text{img}}(\mathfrak{m}_{Y,q}) \subseteq \mathfrak{m}_{X,p}$$

<sup>2</sup>이는 문제 5B에 의해 자동으로 단사임을 의미합니다.

즉 쉽게 말하면,  $q$ 에서의 싹의 값이 영인 것은  $p$ 에서 대응하는 싹의 값이 영인 것과 동치입니다.

저는  $(\pi^\#)^{\text{img}}(\mathfrak{m}_{Y,q}) \subseteq \mathfrak{m}_{X,p}$ 라는 이 표현을 그다지 좋아하지 않는데, 많은 기호들 뒤에 기하학적 직관—즉 “한 점에서의 값”이라는 개념이 어떤 식으로든 보존되기를 원한다는 것—을 숨기기 때문입니다.

이 시점에서 우리는 스킴의 정의를 서술할 수 있으며, 앞으로 몇 개의 절 동안은 실제로 사용하지 않겠지만 여기서 그것을 제시하겠습니다.

**정의 87.3.3.** **스킴**이란 모든 점이 아핀 스킴과 동형인 열린 근방을 갖는 국소 환 달린 공간을 말합니다. 스킴의 사상이란 그저 국소 환 달린 공간의 사상입니다.

특히,  $\text{Spec } A$ 는 스킴입니다 (열린 근방이 공간 전체가 되는 경우입니다!). 그러니 이제 그것들부터 살펴보도록 합시다.

## §87.4 아핀 스킴 사이의 사상의 몇 가지 예

좋습니다, 지난 몇 절 동안 예시가 부족했던 점에 대해 사과드립니다. 이제 만회해 보도록 하겠습니다. 여기서는 모든 움직이는 부분들이 실제로 작동하는 모습을 볼 수 있습니다.

### §87.4.i 한 점 스킴

**예제 87.4.1** ( $\text{Spec } \mathbb{R}$ 은 잘 작동합니다)

$X = \text{Spec } \mathbb{R} \rightarrow \text{Spec } \mathbb{R} = Y$ 인 사상은 오직 하나뿐입니다. 실제로 이들은 점이 하나인 공간이며, 사상  $\mathbb{R} = \mathcal{O}_Y(Y) \rightarrow \mathcal{O}_X(X) = \mathbb{R}$ 를 명시하는 방법은 오직 하나뿐인데,  $\mathbb{R}$ 의 체 자기동형사상은 (항등사상) 하나밖에 없기 때문입니다.

**예제 87.4.2** ( $\text{Spec } \mathbb{C}$ 의 공포담)

놀랍게도  $X = \text{Spec } \mathbb{C} \rightarrow \text{Spec } \mathbb{C} = Y$ 인 사상은 여러 개 존재합니다! 실제로 이들은 점이 하나인 공간이므로, 다시금 우리는 사상  $\mathbb{C} = \mathcal{O}_Y(Y) \rightarrow \mathcal{O}_X(X) = \mathbb{C}$ 를 명시하는 것으로 귀착됩니다. 그러나 항등사상 외에도 복소켈레 또한 성립하며, 이른바  $\mathbb{C}$ 의 “야생 자기동형사상” 몇 가지 역시 성립합니다.

이러한 동작은 명백히 끔찍하므로, 예시를 위해 일부 예시들은 방금 본 공포담을 피하기 위해  $\mathbb{C}$  대신  $\mathbb{R}$ 을 사용합니다. 그러나 나중에 환 준동형사상이  $\mathbb{C}$ 를 고정하도록 강제하는 “ $\mathbb{C}$  위의 스킴”을 이용한 간단한 해결책이 있습니다.

**예제 87.4.3** ( $\text{Spec } k$ 와  $\text{Spec } k'$ )

일반적으로,  $k$ 와  $k'$ 이 체라면, 사상  $\text{Spec } k \rightarrow \text{Spec } k'$ 은 체 준동형사상  $k' \rightarrow k$ 와 전단사 대응됨을 알 수 있는데, 명시해야 할 것이 그것밖에 남지 않기 때문입니다.

### §87.4.ii 상수 사상의 예

**예제 87.4.4** ( $((y - 3)$ 로 가는 상수 사상)

우리는 스킴 사상을 분석합니다

$$X = \operatorname{Spec} \mathbb{R}[x] \xrightarrow{\pi} \operatorname{Spec} \mathbb{R}[y] = Y$$

이는  $X$ 의 모든 점을  $\mathfrak{m} = (y-3) \in Y$ 로 보냅니다. 상수 사상은 위상이 아무리 이상하더라도 항상 연속이므로, 이 덕분에 우리는 그저 단면에만 주의를 집중할 수 있습니다. 이 예시는 충분히 간단해서, 저는 줄기가 더 간단하다고 생각함에도 불구하고 단면으로도 처리할 수 있습니다.  $U$ 를  $Y$ 의 임의의 열린집합이라 하면, 우리는 다음과 같은 사상을 명시해야 합니다

$$\pi_U^\sharp: \mathcal{O}_Y(U) \rightarrow \mathcal{O}_X(\pi^{\text{pre}}(U)).$$

$U$ 가  $(y-3)$ 을 포함하지 않으면,  $\pi^{\text{pre}}(U) = \emptyset$ 이므로  $\mathcal{O}_X(\emptyset) = 0$ 은 영환이고 아무것도 할 필요가 없습니다.

반대로  $U$ 가  $(y-3)$ 을 포함한다면  $\pi^{\text{pre}}(U) = X$ 이므로, 이번에는 다음과 같은 사상을 명시하고자 합니다

$$\pi_U^\sharp: \mathcal{O}_Y(U) \rightarrow \mathcal{O}_X(X) = \mathbb{R}[x]$$

이는 제한 사상을 만족합니다. 임의의  $U$ 에 대해, 원소  $y$ 는  $\mathbb{R}[x]$ 의 단원으로 보내져야 함에 주목하십시오.  $(y)$ 를 포함하지 않는  $U$ 의 부분집합에 대해서는  $1/y$  역시 단면이기 때문입니다. 좀 더 자세히 설명하면,  $W = U \cap D(y)$ 라 두어  $(y) \notin W$ 가 되도록 하면, 다음과 같습니다

$$\pi_W^\sharp(y) = \pi_U^\sharp(y) \quad \text{그리고} \quad \pi_W^\sharp(y)\pi_W^\sharp(1/y) = 1.$$

사실 임의의 실수  $c \neq 3$ 에 대해,  $y - c$ 는  $\mathbb{R}[x]$ 의 단원으로 사상되어야 합니다. 이는  $y \mapsto 3 \in \mathbb{R}[x]$ 인 경우에만 가능합니다.

우리는  $y \mapsto 3$ 을 통해  $\mathbb{R}[y] \mapsto \mathbb{R}[x]$ 를 명시했으므로, 그것이 우리가 필요로 했던 모든 환 준동형사상을 결정합니다.

하지만 우리는 줄기를 사용할 수도 있었습니다. 우리는 다음과 같은 사상을 명시하고자 했습니다

$$\mathbb{R}[y]_{(y-3)} = \mathcal{O}_{Y, (y-3)} \rightarrow \mathcal{O}_{X, \mathfrak{p}}$$

모든 소 아이디얼  $\mathfrak{p}$ 에 대해, 호환되는 짝을 호환되는 짝으로 보내는 것입니다...그런데 잠깐,  $(y-3)$ 은 모든 짝을 쏘아내고 있습니다. 따라서  $\mathcal{O}_{\operatorname{Spec} Y, (y-3)}$ 의 모든 개별 짝은  $\operatorname{Spec} X$ 의 모든 점 위에서 (호환되는) 짝을 산출해야 하며, 이는 전역 단면 전체의 데이터에 해당합니다. 그러므로 우리는 실제로는 다음을 명시하려는 것입니다

$$\mathbb{R}[y]_{(y-3)} = \mathcal{O}_{Y, (y-3)} \rightarrow \mathcal{O}_X(X) = \mathbb{R}[x].$$

앞서 보았듯이 이는  $y \mapsto 3$ 을 요구하는데, 임의의  $c \neq 3$ 에 대해  $y - c$ 가  $\mathbb{R}[x]$ 의 단원이기 때문입니다.

#### 예제 87.4.5 ( $(y^2 + 1)$ 로 가는 상수 사상은 존재하지 않음)

모든 것을  $(y^2 + 1)$ 로 보내는 상수 사상  $X = \operatorname{Spec} \mathbb{R}[x] \rightarrow \operatorname{Spec} \mathbb{R}[y] = Y$ 가 존재하는지 살펴봅시다. 앞선 예시를 그대로 따라 하면, 우리가 원하는 것은 다음과 같습니다

$$\mathcal{O}_Y(U) \rightarrow \mathcal{O}_X(X) = \mathbb{R}[x].$$

우리는  $y$ 와  $1/y$ 가 갈 곳이 없음을 알게 됩니다. 지난번과 같은 논증에 의해  $y - c$ 는  $\mathbb{R}[x]$ 의 단원이어야 하는데, 이번에는 임의의 실수  $c$ 에 대해서 그러합니다.

이번에도 줄기는, 심지어 잉여체만으로도, 이를 보여줍니다. 예를 들어 우리는 다음과 같은 체 준동형사상이 필요할 것입니다

$$\mathbb{C} = \kappa((y^2 + 1)) \rightarrow \kappa((x)) = \mathbb{R}$$

그러나 그런 것은 존재하지 않습니다.

여러분은 이미 다음을 눈치챘을지도 모릅니다

**예제 87.4.6 (일반점은 더 작은 점을 밀어낸다)**

이야기를 바꾸어, 사상  $\text{Spec } \mathbb{C}[x] \rightarrow \text{Spec } \mathbb{C}[y]$ 를 생각해 봅시다. 우리는  $\mathfrak{m}$ 이  $\mathbb{C}[x]$ 의 극대 아이디얼(닫힌점)이라면, 이것이 결코  $\mathbb{C}[y]$ 의 일반점 (0)으로 보내질 수 없다고 주장합니다.

그렇지 않다면, 우리는 국소 환 준동형사상을 얻게 될 것입니다

$$\mathbb{C}(y) \cong \mathcal{O}_{\text{Spec } \mathbb{C}[y], (0)} \rightarrow \mathcal{O}_{\text{Spec } \mathbb{C}[x], \mathfrak{m}} \cong \mathbb{C}[x]_{\mathfrak{m}}$$

이는 특히 우리가 잉여체 사이의 사상을 갖는다는 것을 의미합니다

$$\mathbb{C}(y) \rightarrow \mathbb{C}[x]/\mathfrak{m} \cong \mathbb{C}$$

그런데 이는 불가능합니다. 그러한 체 준동형사상은 전혀 존재하지 않기 때문입니다 (왜 그럴까요?).

마지막 예시는 일반적으로 좋은 직관을 줍니다. "더 일반적인" 점은 "덜 일반적인" 점보다 더 큰 줄기를 갖는 경향이 있으며, 따라서 그런 점들을 밀어냅니다.

**§87.4.iii 사상  $t \mapsto t^2$**

이제 우리는  $t \mapsto t^2$ 라는 사상으로 생각할 만한 것을 살펴봅시다.

**예제 87.4.7 (사상  $t \mapsto t^2$ )**

우리는 다음과 같은 사상을 살펴봅시다

$$\pi: X = \text{Spec } \mathbb{C}[x] \rightarrow \text{Spec } \mathbb{C}[y] = Y$$

점에서 다음과 같이 정의됩니다:

$$\begin{aligned} \pi((0)) &= (0) \\ \pi((x - a)) &= (y - a^2). \end{aligned}$$

원하신다면 이 사상이 연속인지 확인해 보실 수 있습니다. 저는 놀랍게도 점에서의 이러한 행동만으로도 실제로  $\pi^\sharp$ 를 읽어낼 수 있다고 주장합니다. 그 이유는 우리가 다음과 같은 요구 사항을 부과했기 때문입니다: 절단  $s$ 가  $\mathfrak{q} \in Y$ 에서 소멸하는 것은  $\pi_X^\sharp(s)$ 가  $\mathfrak{p} \in X$ 에서 소멸하는 것과 동치이며, 여기서  $\pi(\mathfrak{p}) = \mathfrak{q}$ 입니다. 그러면 이제:

- 절단  $y \in \mathcal{O}_Y(Y)$ 를 생각해 봅시다. 이는 오직  $(y) \in \text{Spec } \mathbb{C}[y]$ 에서만 소멸합니다. 그러면 그 상  $\pi_Y^\sharp(y) \in \mathcal{O}_X(X)$ 는 정확히  $(x) \in \text{Spec } \mathbb{C}[x]$ 에서 소멸해야 하므로, 어떤 정수  $n \geq 1$ 에 대해  $\pi_Y^\sharp(y) = x^n$ 입니다.

- 절단  $y - 4 \in \mathcal{O}_Y(Y)$ 를 생각해 봅시다. 이는 오직  $(y - 4) \in \text{Spec } \mathbb{C}[y]$ 에서만 소멸합니다. 그러면 그 상  $\pi_Y^\#(y - 4) \in \mathcal{O}_X(X)$ 는 정확히  $(x - 2) \in \text{Spec } \mathbb{C}[x]$ 와  $(x + 2) \in \text{Spec } \mathbb{C}[x]$ 에서 소멸해야 합니다. 따라서  $\pi_Y^\#(y - 4)$ 는 어떤  $a \geq 1$ 과  $b \geq 1$ 에 대해  $(x - 2)^a(x + 2)^b$ 로 나누어떨어집니다.

따라서 절단들의 최상위 사상  $\pi_Y^\#$ 에서  $y \mapsto x^2$ 이며, 그러므로 모든 절단의 사상에서도 (또한 모든 줄기에서도) 마찬가지로입니다.

위의 예는  $t^2$ 을 어떤 다항식  $f(t)$ 로 바꾸어도 마찬가지로 성립하며, 그러면  $(x - a)$ 는  $(y - f(a))$ 로 사상됩니다.  $y$ 의 상은 다항식  $g(x)$ 여야 하며, 이는 임의의  $c \in \mathbb{C}$ 에 대해  $g(x) - c$ 가  $f(x) - c$ 와 같은 근을 가진다는 성질을 만족해야 합니다. 다시 말하면,  $f$ 와  $g$ 는 같은 값을 가지므로,  $f = g$ 입니다.

**비고 87.4.8 (일반점 줄기의 압도적 위력)** — 또한 지적하고 싶은 점은, 일반점에서의 줄기만으로도 다항식을 읽어낼 수 있다는 것입니다: 예를 들어, 앞선 예에서는

$$\mathbb{C}(y) \cong \mathcal{O}_{\text{Spec } \mathbb{C}[y], (0)} \rightarrow \mathcal{O}_{\text{Spec } \mathbb{C}[x], (0)} \cong \mathbb{C}(x) \quad y \mapsto x^2.$$

이것이 일반점이 그토록 강력한 이유의 일부입니다. 우리는 다항식의 경우, “일반적인” 점에서 무슨 일이 일어나는지 알면 전체 사상을 알아낼 수 있으리라 기대합니다. 이 직관은 참입니다: 일반점에서의 각 배아가 어디로 가는지 아는 것만으로 전체 사상을 알기에 충분합니다.

## §87.4.iv 산술적 예

### 예제 87.4.9 ( $\text{Spec } \mathbb{Z}[i] \rightarrow \text{Spec } \mathbb{Z}$ )

이제 스킴의 사상  $\pi: \text{Spec } \mathbb{Z}[i] \rightarrow \text{Spec } \mathbb{Z}$ 를 구성하겠습니다. 점 위에서는 다음과 같이 작동합니다

$$\begin{aligned} \pi((0)) &= (0) \\ \pi((p)) &= (p) \\ \pi((a + bi)) &= (a^2 + b^2) \end{aligned}$$

여기서  $a + bi$ 는 가우스 소수입니다: 예를 들어  $\pi((2 + i)) = (5)$ 이고  $\pi((1 + i)) = (2)$ 입니다. 앞서와 마찬가지로 지금 줄기에서 유도되는 사상을 알아낼 수도 있겠지만, 잠시 후 그 수고를 덜어 줄 큰 정리를 다루겠습니다.

## §87.5 큰 정리

우리는 국소환 공간의 사상에 대한 전체 데이터를 명시하면서  $\text{Spec } A \rightarrow \text{Spec } B$ 의 몇 가지 예를 손으로 다루어 보았습니다. 사실 그렇게 많은 데이터를 명시할 필요가 없었으며, 그 과정의 상당 부분을 자동화할 수 있다는 것이 밝혀집니다:

**명제 87.5.1 (아핀 재구성)**

$\pi: \text{Spec } A \rightarrow \text{Spec } B$ 를 스킴의 사상이라 합시다.  $\psi: B \rightarrow A$ 를 전역 절단을 취하여 얻어지는 환 준동형사상이라 합시다, 즉

$$\psi = \pi_B^\sharp: \mathcal{O}_{\text{Spec } B}(\text{Spec } B) \rightarrow \mathcal{O}_{\text{Spec } A}(\text{Spec } A).$$

그러면 우리는  $\psi$ 만 가지고  $\pi$ 를 복원할 수 있습니다; 실제로  $\pi$ 는 다음과 같이 명시적으로 주어집니다

$$\pi(\mathfrak{p}) = \psi^{\text{pre}}(\mathfrak{p})$$

그리고

$$\pi_{\mathfrak{p}}^\sharp: \mathcal{O}_{Y, \pi(\mathfrak{p})} \rightarrow \mathcal{O}_{X, \mathfrak{p}} \quad \text{에 의해} \quad f/g \mapsto \psi(f)/\psi(g).$$

이것이 아핀 스킴의 큰 기적입니다. 그 정의에 담긴 엄청난 양의 데이터에도 불구하고, 우리는 아핀 스킴 사이의 사상을 최상위 수준의 단 하나의 환 준동형사상으로 압축할 수 있습니다.

증명. 이는 두 부분을 필요로 합니다.

- 우리는 사상들이 점에서 일치하는지 확인해야 합니다; 놀랍게도 이것이 더 어려운 절반입니다. 이것이 어떻게 작동하는지 보기 위해,  $\mathfrak{q} = \pi(\mathfrak{p})$ 라 합시다. 핵심 사실은 함수  $f \in B$ 가  $\mathfrak{q}$ 에서 소멸하는 것은  $\pi_B^\sharp(f)$ 가  $\mathfrak{p}$ 에서 소멸하는 것과 동치라는 것입니다 (왜냐하면  $\pi_B^\sharp$ 는 국소 환의 준동형사상이어야 하기 때문입니다). 따라서,

$$\begin{aligned} \pi(\mathfrak{p}) = \mathfrak{q} &= \{f \in B \mid f \in \mathfrak{q}\} \\ &= \{f \in B \mid f \text{에서 소멸합니다}\mathfrak{q}\} \\ &= \{f \in B \mid \pi_B^\sharp(f) \text{에서 소멸합니다}\mathfrak{p}\} \\ &= \{f \in B \mid \pi_B^\sharp(f) \in \mathfrak{p}\} = \{f \in B \mid \psi(f) \in \mathfrak{p}\} \\ &= \psi^{\text{pre}}(\mathfrak{p}). \end{aligned}$$

- 우리는 또한 줄기에서의 사상이 같은지도 확인하고 싶습니다.  $\mathfrak{p} \in \text{Spec } A$ ,  $\mathfrak{q} \in \text{Spec } B$ 이고, (위의 두 경우 모두에서)  $\mathfrak{p} \mapsto \mathfrak{q}$ 라 합시다.

우리의 원래  $\pi$ 에서, 사상  $\pi_{\mathfrak{p}}^\sharp: B_{\mathfrak{q}} \rightarrow A_{\mathfrak{p}}$ 를 생각해 봅시다. 우리는 이것이 각  $f \in B$ 를  $\psi(f) \in A$ 로 보낸다는 것을 압니다. 이는  $\mathfrak{q}$ 에서 각 전역 절단  $f \in B$ 의 배아를 취함으로써 얻어집니다. 따라서 이것은 필요한 대로  $f/g$ 를  $\psi(f)/\psi(g)$ 로 보내야 합니다, 왜냐하면 환 준동형사상이기 때문입니다.  $\square$

이 모든 것은 하나의 훌륭한 발상을 시사합니다: 만약  $\psi: B \rightarrow A$ 가 임의의 환 준동형사상이라면, 우리는 방금 발견한 증명의 조각들을 이용하여 스킴의 사상을 구성할 수 있어야 합니다. 우리가 해야 할 유일한 추가 작업은 자리스키 위상에서 연속인 사상을 얻는지, 그리고 적절한  $\pi^\sharp$ 를 얻을 수 있는지 확인하는 것입니다.

이렇게 하여 우리는 아핀 스킴에 관한 거대하고 중요한 정리를 얻습니다.

**정리 87.5.2 ( $\text{Spec } A \rightarrow \text{Spec } B$ 는 그저  $B \rightarrow A$ 입니다)**

이 두 구성은 환 준동형사상  $B \rightarrow A$ 와  $\text{Spec } A \rightarrow \text{Spec } B$  사이의 전단사를 줍니다.

증명. 각  $\pi: \text{Spec } A \rightarrow \text{Spec } B$ 를 취해 환 준동형사상  $\psi$ 를 얻는 방법을 살펴보았습니다.

**명제 87.5.1**은 이 사상이 단사임을 보여줍니다. 따라서 이것이 전사임을, 즉 모든  $\psi$ 가 어떤  $\pi$ 로부터 나온다는 것을 확인하기만 하면 됩니다.

$\psi: B \rightarrow A$ 가 주어지면, **명제 87.5.1**을 그대로 따라 하고 모든 것이 잘 정의됨을 확인함으로써  $(\pi, \pi^\#): \text{Spec } A \rightarrow \text{Spec } B$ 를 정의합니다. 세부 사항은 다음과 같습니다:

- 각 소 아이디얼  $\mathfrak{p} \in \text{Spec } A$ 에 대해,  $\pi(\mathfrak{p}) = \psi^{\text{pre}}(\mathfrak{p}) \in \text{Spec } B$ 로 둡니다 (이는 **문제 5C\***에 의해 역시 소 아이디얼입니다).

**연습문제 87.5.3.** 결과로 얻어지는 사상  $\pi$ 가 자리스키 위상에서 연속임을 보이십시오.

- 이제 줄기 위에서도 사상을 정의하고자 하므로, 각  $\pi(\mathfrak{p}) = \mathfrak{q}$ 에 대해 다음과 같이 둡니다

$$B_{\mathfrak{q}} \ni \frac{f}{g} \mapsto \frac{\psi(f)}{\psi(g)} \in A_{\mathfrak{p}}.$$

이는  $g \notin \mathfrak{q} \implies \psi(g) \notin \mathfrak{p}$ 이므로 성립합니다. 또한  $f \in \mathfrak{q} \implies \psi(f) \in \mathfrak{p}$ 이므로, 이것이 실제로 국소환 준동형사상임을 알 수 있습니다 ( $B_{\mathfrak{q}}$ 의 극대 아이디얼을  $A_{\mathfrak{p}}$ 의 극대 아이디얼로 보냅니다).

$f/g$ 가 열린집합  $U \subseteq B$  위의 절단이라면(즉  $g$ 가  $U$ 의 소 아이디얼들에서 소멸하지 않는다면),  $\psi(f)/\psi(g)$ 는  $\pi^{\text{pre}}(U)$  위의 절단임을 관찰하십시오(즉  $\psi(g)$ 가  $\pi^{\text{pre}}(U)$ 의 소 아이디얼들에서 소멸하지 않습니다). 따라서  $B$  위의 양립 가능한 싹들은 필요하도록  $A$  위의 양립 가능한 싹들로 보내집니다.

마지막으로, 결과로 얻어지는  $\pi$ 는 전역 절단에서  $\pi^\#_B = \psi$ 를 만족하며, 이로써 증명이 완성됩니다.  $\square$

이것은 범주론을 이용해 간결하게 요약될 수 있습니다:

#### 따름정리 87.5.4 (범주론적 해석)

환의 반대 범주  $\text{CRing}^{\text{op}}$ 는 아핀 스킴의 범주  $\text{AffSch}$ 와 “동치”이며,  $\text{Spec}$ 이 함자 역할을 합니다.

이는 예를 들어  $A \cong B$ 일 때마다 자연스럽게  $\text{Spec } A \cong \text{Spec } B$ 임을 의미합니다.

이 정리가 중요하다는 것을 확실히 인식할 수 있도록, 대수기하학 참고문헌에 대해 읽던 중 MathOverflow에서 발견한 재미있는 댓글을 소개합니다<sup>3</sup>:

그 [Hartshorne]는 아핀 스킴의 범주가 환의 범주와 쌍대라는 것을 제가 보기에 전혀 언급하지 않습니다. 저는 스킴의 정의 근처에 큰 글씨로 그것이 쓰여 있기를 기대했습니다. 어떻게 그것을 빠뜨릴 수 있습니까?

## §87.6 스킴 사상의 추가 예시

이제 큰 망치를 손에 넣었으니, 몇 절 전에 했던 것보다 훨씬 더 간략하게 예시들을 논할 수 있습니다. 여러 가지를 마구 던지기 전에,  $\mathbb{C} \rightarrow \mathbb{C}$ 가 자명하지 않은 체 자기동형사상을 갖는다는 앞서 본 이상한 현상을 없애줄 또 다른 정의를 하나 소개하고자 합니다:

**정의 87.6.1.**  $S$ 를 스킴이라고 합시다.  $S$  위의 스킴(scheme over  $S$ ) 또는  $S$ -스킴은 스킴  $X$ 와 사상  $X \rightarrow S$ 의 짝입니다.  $S$ -스킴의 사상은 스킴 사상  $X \rightarrow Y$ 로서 다음 도식이

$$\begin{array}{ccc} X & \longrightarrow & Y \\ & \searrow & \downarrow \\ & & S \end{array}$$

이 가환하도록 하는 스킴 사상  $X \rightarrow Y$ 를 말합니다. 종종  $S = \text{Spec } k$ 인 경우,

$X$ 를 간단히  $k$  위의 스킴 또는  $k$ -스킴이라 부르겠습니다.

<sup>3</sup>From <https://mathoverflow.net/q/2446/70654>.

**예제 87.6.2** ( $\text{Spec } k[\dots]$ )

어떤 아이디얼  $I$ 에 대해  $X = \text{Spec } k[x_1, \dots, x_n]/I$ 이면,  $X$ 는 자연스럽게  $k$ -스킴이 됩니다; 명백한 준동형사상  $k \hookrightarrow k[x_1, \dots, x_n]/I$ 가 있으므로 이것이 사상  $X \rightarrow \text{Spec } k$ 를 줍니다.

**예제 87.6.3** ( $\text{Spec } \mathbb{C}[x] \rightarrow \text{Spec } \mathbb{C}[y]$ )

$\mathbb{C}$ -스킴으로서, 사상  $\text{Spec } \mathbb{C}[x] \rightarrow \text{Spec } \mathbb{C}[y]$ 는 다음 도식이 가환하는 준동형사상  $\psi: \mathbb{C}[y] \rightarrow \mathbb{C}[x]$ 와 일치합니다.

$$\begin{array}{ccc} \mathbb{C}[x] & \xleftarrow{\psi} & \mathbb{C}[y] \\ & \searrow & \uparrow \\ & & \mathbb{C} \end{array}$$

이 가환하도록 하는 환 준동형사상  $\psi: \mathbb{C}[y] \rightarrow \mathbb{C}[x]$ 와 일치합니다. “ $\mathbb{C}$  위”라는 조건이 이전의 병리적 현상을 없애줌을 알 수 있습니다:  $\psi$ 는  $\mathbb{C}$ 를 보존하도록 요구됩니다. 따라서 이 사상은  $y$ 의 상, 즉  $\mathbb{C}[x]$  안의 다항식의 선택에 의해 결정됩니다. 예를 들어  $\psi(y) = x^2$ 이면 우리가 처음 본 예시를 다시 얻습니다. 이는 이러한 사상들이 다항식에 대응해야 한다는 직관과 일치합니다.

**예제 87.6.4** ( $\text{Spec } \mathcal{O}_K$ )

이는 앞서 나온  $\text{Spec } \mathbb{Z}[i]$ 를 일반화한 것입니다.  $K$ 가 수체이고  $\mathcal{O}_K$ 가 정수환이라면, (유일한) 환 준동형사상  $\mathbb{Z} \hookrightarrow \mathcal{O}_K$ 로부터 자연스러운 사상  $\text{Spec } \mathcal{O}_K \rightarrow \text{Spec } \mathbb{Z}$ 가 존재합니다. 각 유리 소수  $(p) \in \mathbb{Z}$  위에서,  $p$ 가 분해되는 소 아이디얼들을 얻게 됩니다. (아쉽게도 아직 분기를 포착할 방법은 없습니다.)

## §87.7 비아핀 스킴에 관하여 조금

마침내 우리가 오랫동안 원했던 동형사상을 (절 85.2.iii에서 처음 언급된) 서술할 수 있습니다:

**정리 87.7.1** (특수 열린집합은 아핀 스킴과 동형입니다)

$A$ 를 환이라 하고  $f$ 를 그 원소라 합시다. 그러면

$$\text{Spec } A[1/f] \cong D(f) \subseteq \text{Spec } A.$$

증명. 성가신 확인이지만 아직 포함되지 않았습니다. (점의 수준에서 소 아이디얼의 전단사는 이미 살펴보았습니다.)  $\square$

**따름정리 87.7.2** (열린 부분집합은 스킴입니다)

- (a) 아핀 스킴의 공집합이 아닌 열린 부분집합은 그 자체로 스킴입니다.
- (b) (아핀이든 아니든) 임의의 스킴의 공집합이 아닌 열린 부분집합은 그 자체로 스킴입니다.

증명. (a) 부분은 본질적으로 이미 완료되었습니다.

**질문 87.7.3.** 정리 85.2.2를 앞선 명제와 결합하여 (a)를 이끌어내십시오.

그러면 (b) 부분은,  $U$ 가 열린집합이고  $p$ 가  $U$ 의 한 점일 때,  $p$ 에서 아핀 열린 근방  $\text{Spec } A$ 를 취한 다음, (a)에서와 같이  $U \cap \text{Spec } A$ 를  $\text{Spec } A$ 의 특수 열린 부분집합들로 덮음으로써 따라 나옵니다.  $\square$

이제 절 85.2.iv을 다시 살펴봅시다 ( $C$ 가  $k$ 로 대체된다는 점만 다릅니다). 그것이  $\text{Spec } k[x, y]$ 의 열린 부분집합  $U$ 임을 이미 살펴보았으므로, 이는 스킴입니다.

**질문 87.7.4.** 실제로  $U$ 가 둘 다 아핀인 두 열린집합으로 덮일 수 있음을 보이십시오.

하지만 이제 정말로 두 개의 특수 열린집합이 필요하다는 것을 보이겠습니다.

**명제 87.7.5 (유명한 예시: 구멍 뚫린 평면은 아핀이 아닙니다)**

$\text{Spec } k[x, y]$ 에서  $(x, y)$ 를 제거하여 얻은 구멍 뚫린 평면  $U = (U, \mathcal{O}_U)$ 는 어떤 아핀 스킴  $\text{Spec } B$ 와도 동형이 아닙니다.

직관적으로 말하면,  $\mathcal{O}_U(U) = k[x, y]$ 이지만  $U$ 는 평면이 아니기 때문입니다.

증명. 우리는 이미  $\mathcal{O}_U(U) = k[x, y]$ 임을 알고 있으며 이를 잘 다룰 수 있습니다. 예를 들어,  $y \in \mathcal{O}_U(U)$ 는 마치  $x$ 축처럼 보이는 곳에서 소멸하는 전역 절단입니다. 마찬가지로,  $x \in \mathcal{O}_U(U)$ 는 마치  $y$ 축처럼 보이는 곳에서 소멸하는 전역 절단입니다. 특히,  $U$ 의 어떤 점도 둘 다에서 소멸하지 않습니다.

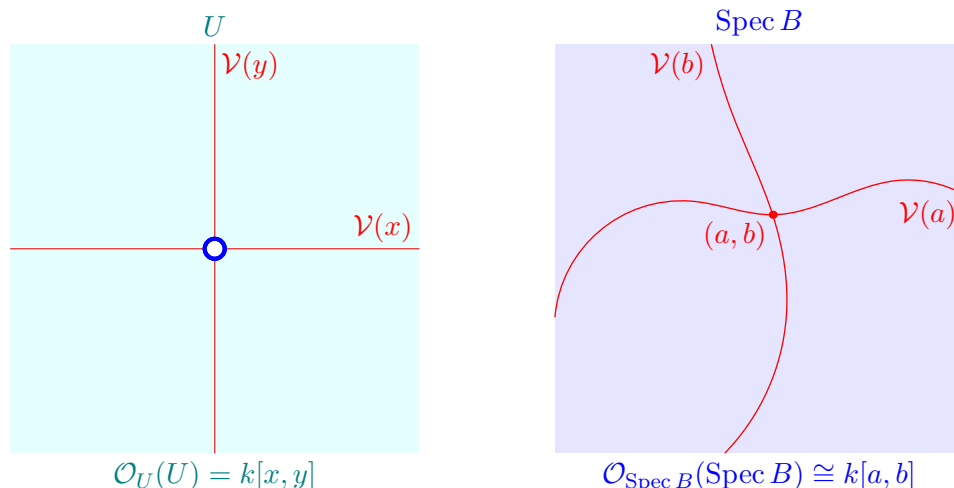
이제 모순을 이끌어내기 위해 동형사상이 존재한다고 가정합니다

$$\psi: \text{Spec } B \rightarrow U.$$

전역 절단에 대한 사상을 취함으로써 (정의의 일부),

$$k[x, y] = \mathcal{O}_U(U) \xrightarrow{\psi^\#} \mathcal{O}_{\text{Spec } B}(\text{Spec } B) \cong B.$$

그러면  $\mathcal{O}_U(U)$ 의 전역 절단  $x$ 와  $y$ 는  $B$ 에서 상  $a$ 와  $b$ 를 가져야 하며; 이로부터 환 동형사상  $B \cong k[a, b]$ 가 존재함이 따라 나옵니다.



이제  $\text{Spec } B$ 에서,  $\mathcal{V}(a) \cap \mathcal{V}(b)$ 는 단 하나의 점, 즉 극대 아이디얼  $\mathfrak{m} = (a, b)$ 를 포함하는 닫힌집합입니다. 따라서  $\text{Spec } B$ 에는  $a$ 와  $b$  모두에서 소멸하는 점이 정확히 하나 존재합니다. 스킴의 사상이 값을 보존하도록 요구했기 때문에 (국소 환달린 공간에 대한 큰 소동이 바로 그 때문입니다), 이는  $U$ 에도  $x$ 와  $y$  모두에서 소멸하는 점이 하나 있어야 함을 의미합니다. 하지만 그런 점은 없습니다 — 우리가 삭제한 것이 바로 원점이었습니다.  $\square$

## §87.8 여기서 어디로 갈 것인가

이 장으로 스킴의 정의를 위한 긴 준비 과정이 마무리됩니다. 지금으로서는 안타깝게도 이것이 제가 시간을 낼 수 있는 한계입니다. 그러므로, 스킴이 실제로 “현실 세계”에서 어떻게 사용되는지 직접 보고 싶다면, 다른 곳을 찾아보아야 합니다.

제가 기꺼이 추천하는 좋은 참고문헌은 [Ga03]이며; 더 어려운 (그리고 유명한) 것으로는 [Va17]이 있습니다. 더 자세한 언급은 [장 A](#)를 참고하십시오.

## §87.9 생각해 볼 만한 조금 더 어려운 문제

**문제 87A.** 아핀 스킴  $X = \text{Spec } R$ 이 주어졌을 때, 스킴의 사상  $X \rightarrow \text{Spec } \mathbb{Z}$ 가 유일하게 존재함을 보이고, 이것이  $X$ 의 점들을 어디로 보내는지 설명하십시오.

**문제 87B.**  $\text{Spec } \mathbb{Z}[x]$ 에서 점  $\mathfrak{m} = (2, x)$ 를 제거하여 얻은 열린 부분집합은 어떤 아핀 스킴과 동형입니까?

# XXI

집합론 I: ZFC, 순서수, 그리고 기수

## 제XXI부: 목차

---

|           |                                 |            |
|-----------|---------------------------------|------------|
| <b>88</b> | <b>막간: 코시의 함수 방정식과 초른의 보조정리</b> | <b>925</b> |
| 88.1      | 괴물을 하나 만들어 봅시다                  | 925        |
| 88.2      | 유한 귀납법 복습                       | 926        |
| 88.3      | 초한 귀납법                          | 926        |
| 88.4      | 함수 방정식 마무리하기                    | 928        |
| 88.5      | 초른의 보조정리                        | 929        |
| 88.6      | 생각해 볼 만한 조금 더 어려운 문제            | 931        |
| <b>89</b> | <b>선택공리를 포함한 체르멜로-프렝켈</b>       | <b>933</b> |
| 89.1      | 공극의 함수방정식                       | 933        |
| 89.2      | 칸토어의 역설                         | 933        |
| 89.3      | 집합론의 언어                         | 934        |
| 89.4      | ZFC의 공리들                        | 935        |
| 89.5      | 부호화                             | 937        |
| 89.6      | 선택과 정렬순서                        | 938        |
| 89.7      | 집합 대 클래스                        | 938        |
| 89.8      | 생각해 볼 만한 조금 더 어려운 문제            | 939        |
| <b>90</b> | <b>순서수</b>                      | <b>941</b> |
| 90.1      | 미취학 아동을 위한 세기                   | 941        |
| 90.2      | 집합론자를 위한 세기                     | 941        |
| 90.3      | 순서수의 정의                         | 944        |
| 90.4      | 순서수는 “높습니다”                     | 945        |
| 90.5      | 초한 귀납법과 초한 재귀법                  | 946        |
| 90.6      | 순서수 산술                          | 947        |
| 90.7      | 집합의 계층                          | 949        |
| 90.8      | 생각해 볼 만한 조금 더 어려운 문제            | 951        |
| <b>91</b> | <b>기수</b>                       | <b>953</b> |
| 91.1      | 등수인 집합과 기수                      | 953        |
| 91.2      | 기수성                             | 954        |
| 91.3      | 알레프 수                           | 954        |
| 91.4      | 기수 산술                           | 955        |
| 91.5      | 기수 지수 연산                        | 957        |
| 91.6      | 공종성                             | 957        |
| 91.7      | 비가측 기수                          | 959        |
| 91.8      | 생각해 볼 만한 조금 더 어려운 문제            | 960        |

---

# 88

## 막간: 코시의 함수 방정식과 초론의 보조정리

이것은 초론의 보조정리에 관한 비공식적인 장으로, *Napkin*의 마지막 부분들에서 다룰 내용에 대한 개요를 제공합니다. 흐름의 연속성을 잃지 않고 건너뛸 수 있습니다.

올림피아드 수학의 세계에는 다음과 같은 유명한 함수 방정식이 있습니다:

$$f: \mathbb{R} \rightarrow \mathbb{R} \quad f(x+y) = f(x) + f(y).$$

그 해가 무엇인지는 다들 알고 있습니다! 명백한 해의 족으로  $f(x) = cx$ 가 있습니다. 그리고 또한 어... 음... 불연속인 해들의 족도 있습니다 (웅얼웅얼) 병적인 (중얼중얼) 선택공리 (웅얼).

초론의 보조정리라 불리는 것도 있습니다. 이것은 선택공리와 동치이기 때문에 무섭게 들리는데, 선택공리 역시 그냥 무섭습니다.

이 글에서는 이것들이 들리는 것만큼 그렇게 무섭지 않다는 것을 보이면서 그 무서움을 걷어내 보려고 합니다.

### §88.1 괴물을 하나 만들어 봅시다

”나쁜”  $f$ 를 한번 구성할 수 있는지 보고 무슨 일이 일어나는지 살펴봅시다.

척도 조정을 통해, 일반성을 잃지 않고  $f(1) = 1$ 이라고 가정합시다. 그러면 모든 정수  $n$ 에 대해  $f(n) = n$ 이며, 여기서부터 다음을 쉽게 보일 수 있습니다

$$f\left(\frac{m}{n}\right) = \frac{m}{n}.$$

따라서  $f$ 는 모든 유리수에 대해 결정됩니다. 그리고 그 다음엔 막히게 됩니다.

이 중 어느 것도, 예컨대  $f(\sqrt{2})$ 를 결정하는 데는 쓸모가 없습니다. 유리수들을 하루 종일 더하고 빼봐야, 이를테면  $\sqrt{2}$ 는 전혀 등장하지 않을 것입니다.

뭐, 어차피 판을 뒤엎어 보려는 것이니, 다음과 같이 놓아 봅시다

$$f(\sqrt{2}) = 2015$$

안 될 이유가 뭐 있겠습니까? 같은 귀납법에 의해  $f(n\sqrt{2}) = 2015n$ 을 얻고, 그러면

$$f(a + b\sqrt{2}) = a + 2015b.$$

여기서  $a$ 와  $b$ 는 유리수입니다. 자, 지금까지는 좋습니다 – 지금 쓰여진 대로라면 이것은 완벽하게 좋은 해입니다. 다만 우리가  $f$ 를 실수 전체 중 아주 작은 부분에 대해서만 정의했다는 점만 빼면 말입니다.

뭐, 이런 일은 하루 종일 계속할 수 있습니다:

$$f(a + b\sqrt{2} + c\sqrt{3} + d\pi) = a + 2015b + 1337c - 999d.$$

완벽하게 모순 없이 성립합니다.

이제 어떻게 계속해 나가야 할지 대략 감이 잡힐 것입니다. 그저 이전의 몇몇과 ”독립적인” 새로운 실수들을 계속 집어넣으면서, 우리가 원하는 아무 값에나 대응시키면 됩니다. 이것이 충분히 작동할 것처럼 느껴집니다. . .

잠시 후 ”독립적”이라는 것이 무엇을 뜻하는지 설명하겠습니다(이미 짐작하셨을 수도 있습니다), 지금 당장은 더 큰 문제가 있습니다: 아무리 많은 수를 집어넣어도, 결코 끝나지 않을 것처럼 보인다는 점입니다. 먼저 두 번째 문제부터 다뤄봅시다.

## §88.2 유한 귀납법 복습

귀납법을 사용할 때는 1, 2, 3, ... 이런 식으로 세어 나갈 수 있습니다. 예를 들어 다음과 같은 "문제"가 있다고 합시다:

$n$ 개의 열린 구간의 교집합이  $\emptyset$ 이거나 열린 구간임을 증명하십시오.

이는 귀납법으로 쉽게 증명할 수 있습니다:  $n = 2$ 일 때 성립하고, 더 큰 경우에도 마찬가지로 쉽습니다.

하지만 이로부터 무한히 많은 열린 구간이 어떤 열린 구간에서 교차한다고 결론지을 수는 없습니다. 실제로 이것은 거짓입니다: 다음 구간들을 생각해 봅시다

$$(-1, 1), \quad \left(-\frac{1}{2}, \frac{1}{2}\right), \quad \left(-\frac{1}{3}, \frac{1}{3}\right), \quad \left(-\frac{1}{4}, \frac{1}{4}\right), \quad \dots$$

이 무한 구간 집합은 단 한 점  $\{0\}$ 에서 교차합니다!

이 이야기의 교훈은 귀납법으로는 무한에 도달할 수 없다는 것입니다. 아쉬운 일인데, 왜냐하면 우리는 괴물을 만드는 데 귀납법을 사용하고 싶었기 때문입니다. 결국 우리가 하고 있는 일이 바로 하나씩 더해 나가는 것이기 때문입니다.

## §88.3 초한 귀납법

그런데 알고 보면 가능합니다만, 새로운 수의 개념, 이른바 순서수가 필요합니다. 저는 이를 [장 90](#)의 첫 두 절에서 완전한 형태로 정의합니다(궁금한 독자는 그 두 절로 바로 건너뛰어도 좋습니다), 하지만 이 장에서는 아직 그 완전한 정의가 필요하지 않습니다.

제가 하고 싶은 말은 이것입니다: 모든 자연수 다음에

$$0, 1, \dots,$$

저는  $\omega$ 라는 새로운 수를 놓겠습니다. 이는 모든 자연수보다 큰 첫 번째 순서수입니다. 그 뒤에는 다음과 같이 불리는 수들이 더 있습니다

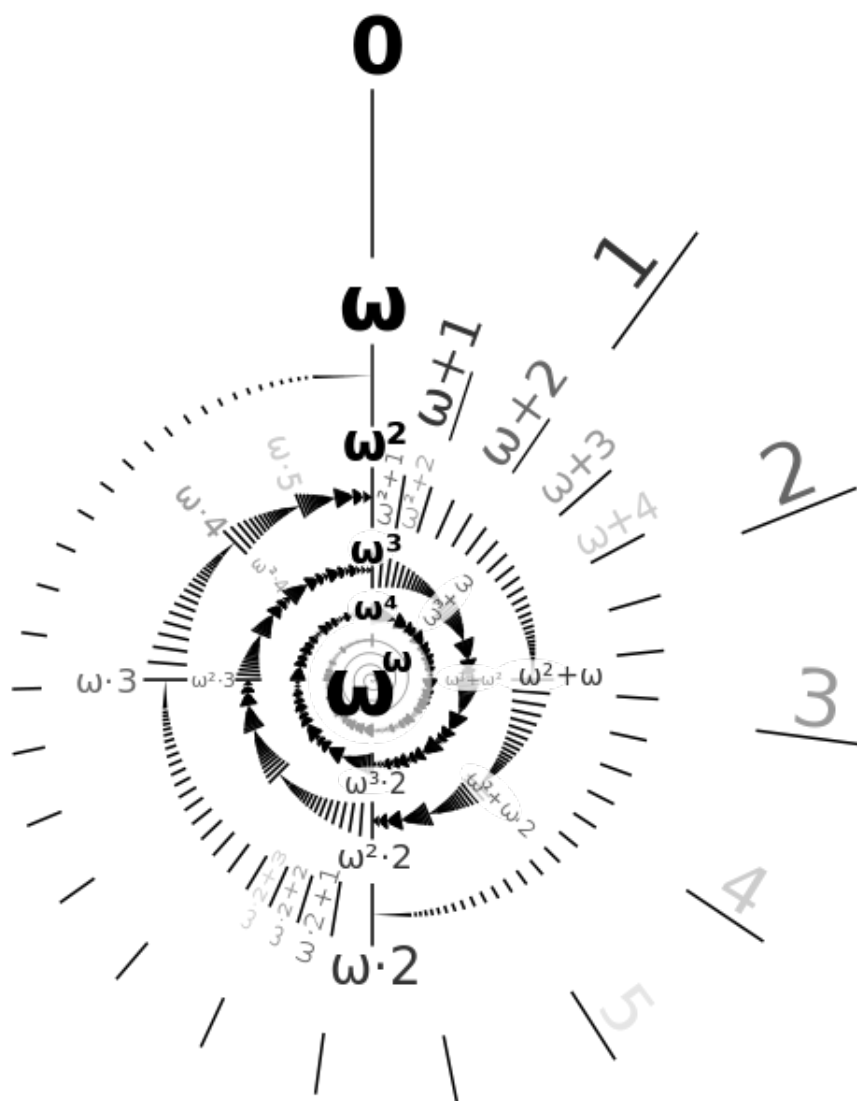
$$\omega + 1, \omega + 2, \dots$$

그리고 마침내  $\omega \cdot 2$ 라는 수가 나옵니다.

목록은 계속됩니다:

$$\begin{aligned} &0, 1, 2, 3, \dots, \omega \\ &\omega + 1, \omega + 2, \dots, \omega + \omega \\ &\omega \cdot 2 + 1, \omega \cdot 2 + 2, \dots, \omega \cdot 3 \\ &\vdots \\ &\omega^2 + 1, \omega^2 + 2, \dots \\ &\vdots \\ &\omega^3, \dots, \omega^4, \dots, \omega^\omega, \dots, \omega^{\omega^\omega} \dots \end{aligned}$$

그림으로 표현하면 대략 이렇게 보입니다:



이미지 출처 [ca]

(이 도식은 초기 구간만 보여줄 뿐이며,  $\omega^\omega + 1000$ 과 같이 더 큰 순서수들이 여전히 존재한다는 점에 유의하십시오).

아무튼, 자연수가 모든 유한 집합을 "지배하는" 것과 같은 방식으로, 순서수는 다음과 같은 의미에서 모든 집합을 지배합니다. 본질적으로 선택 공리를 가정하면, 모든 집합  $S$ 에 대해  $S$ 보다 큰 어떤 순서수  $\alpha$ 가 존재한다는 결론이 따라 나옵니다(이 "크다"는 의미는 이후 장에서야 정확히 다루겠습니다).

그런데 알고 보면(그리고 직관적으로도 알 수 있듯이) 순서수가 아무리 커지더라도 무한 하강 사슬은 존재하지 않습니다. 즉, 어떤 순서수(예를 들어  $2\omega + 4$ )에서 시작해서 아래로 내려가면, 0에 도달하기까지 유한한 횟수의 도약만 할 수 있습니다. (이를 확인하려면  $2\omega + 4$ 에서 시작하는 사슬을 직접 적어 보십시오.) 따라서 귀납법과 재귀법은 여전히 그대로 작동합니다:

**정리 88.3.1 (초한 귀납법)**

명제  $P(-)$ 가 주어졌을 때, 다음을 가정합시다

- $P(0)$ 이 참이고, 그리고
- 모든  $\alpha < \beta$ 에 대해  $P(\alpha)$ 가 참이면,  $P(\beta)$ 도 참입니다.

그러면  $P(\beta)$ 는 참입니다.

마찬가지로, 모든  $\alpha < \beta$ 에 대해  $x_\alpha$ 의 값을 알고 있다면  $x_\beta$ 를 정의하는 재귀를 수행할 수 있습니다.

일반적인 귀납법이나 재귀법과의 차이점은, 우리가 종종 " $x_{n+1} = \dots$ 를 정의한다"와 같은 방식만을 사용한다는 것입니다. 하지만 이것으로는 모든  $\alpha$ 에 대해  $x_\alpha$ 를 정의하기에 충분하지 않습니다. 이를 확인하려면, 우리의 일반적인 귀납법을 사용해서 사다리를 얼마나 높이 오를 수 있는지 시도해 보십시오.

답:  $\omega$ 에는 도달할 수 없습니다! 이는 어떤 자연수  $n$ 에 대해서도  $n+1$ 의 형태가 아니기 때문입니다 – 우리의 유한 귀납법은  $\omega$ 보다 작은 순서수까지만 도달하게 해줍니다. 마찬가지로, 단순한  $+1$ 은 이미 모든  $n$ 에 대해  $\omega + n$ 을 가지고 있더라도 순서수  $\omega \cdot 2$ 에 도달하게 해주지 않습니다. 이러한 순서수들을 **극한 순서수**라고 부릅니다.  $\alpha + 1$ 의 형태인 순서수는 **후행자 순서수**라고 부릅니다.

그래서 초한 귀납법이나 재귀법은 매우 흔히 세 가지 경우로 나뉩니다. 귀납법의 표현으로는 다음과 같은 모습입니다

- (영 사례) 먼저,  $P(0)$ 을 해결합니다.
- (후행자 사례)  $P(\alpha)$ 로부터  $P(\alpha + 1)$ 을 얻을 수 있음을 보입니다.
- (극한 사례)  $\lambda$ 가 극한 순서수일 때, 모든  $\alpha < \lambda$ 에 대해  $P(\alpha)$ 가 주어지면  $P(\lambda)$ 가 성립함을 보입니다.

마찬가지로, 초한 재귀도 종종 경우들로 나뉩니다.

- (기저 경우) 먼저,  $x_0$ 을 정의합니다.
- (후행자 경우)  $x_\alpha$ 로부터  $x_{\alpha+1}$ 을 정의합니다.
- (극한 경우) 모든  $\alpha < \lambda$ 에 대해  $x_\alpha$ 로부터  $x_\lambda$ 를 정의합니다. 여기서  $\lambda$ 는 극한 순서수입니다.

두 상황 모두에서, 유한 귀납법은 처음 두 경우만 다루지만, 세 번째 경우를 다룰 수 있다면 우리는 장벽  $\omega$ 를 훌쩍 넘어설 수 있습니다.

**§88.4 함수 방정식 마무리하기**

우리 문제를 푸는 것으로 돌아갑시다.

$S_n$ 을  $n$ 번째 단계에서 우리가 가진 "기저" 숫자들의 집합이라 합시다. 우리 예시에서는 다음과 같을 수 있습니다

$$S_1 = \{1\}, \quad S_2 = \{1, \sqrt{2}\}, \quad S_3 = \{1, \sqrt{2}, \sqrt{3}\}, \quad S_4 = \{1, \sqrt{2}, \sqrt{3}, \pi\}, \quad \dots$$

그리고 모든 실수를 표현할 수 있을 때까지  $S_i$ 를 계속 쌓아나가고 싶습니다. 완전성을 위해,  $S_0 = \emptyset$ 이라고 선언하겠습니다.

먼저, "독립적"이라는 것을 더 정확히 할 필요가 있습니다. 직관적으로, 이 구성이 작동하는 이유는

$$a + b\sqrt{2} + c\sqrt{3} + d\pi$$

유리수  $a, b, c, d$ (모두 0인 경우를 제외하고)에 대해 절대로 0이 되지 않기 때문입니다. 일반적으로, 숫자들의 집합  $X$ 는 다음 조합이

$$c_1x_1 + c_2x_2 + \cdots + c_mx_m = 0$$

$c_1 = c_2 = \cdots = c_m = 0$ 이 아닌 한 유리수  $\mathbb{Q}$ 에 대해 절대 발생하지 않을 때 "독립적"이라고 합니다. 여기서  $x_i \in X$ 는 서로 다릅니다.  $X$ 가 무한집합이더라도 저는 오직 유한합만을 취할 수 있음에 주의하십시오! (이 개념에는 이름이 있습니다:  $X$ 가  $\mathbb{Q}$  위에서 **선형독립**이기를 원하는 것입니다. 이에 대한 자세한 내용은 벡터 공간 장을 참고하십시오!)

언제 멈춰야 할까요? 우리는 모든 실수가 독립적인 숫자들을 이용해 표현될 수 있을 만큼 큰 집합  $S_{\text{어떤 것}}$ 을 가졌을 때 멈추고 싶습니다. (이 개념에도 이름이 있습니다:  $\mathbb{Q}$ -기저라고 불립니다.) 그러한 집합을 **생성한다**고 부릅니다. 생성하는 집합에 도달하면 멈춥니다.

여전히 귀납할 수 있다는 발상은 괜찮아 보입니다:  $S_\alpha$ 가 생성하지 않는다고 가정합시다. 그러면  $S_\alpha$ 와 독립적인 어떤 숫자, 이를테면  $\sqrt{2015}\pi$  같은 것이 존재합니다. 그러면 그것을 추가하여  $S_{\alpha+1}$ 을 얻습니다. 그리고 계속해 나갑니다.

안타깝게도, 앞서 말했듯이  $S_\alpha$ 에서  $S_{\alpha+1}$ 로 갈 수 있는 것(후행자 경우)만으로는 충분하지 않습니다. 극한 경우도 다뤄야 합니다. 하지만 우리가 쓸 수 있는 트릭이 있는 것으로 밝혀졌습니다. 양의 정수  $n$ 마다 하나씩, 모든 집합  $S_0, S_1, S_2, \dots$ 를 모두 구성했다고 가정하고, 그중 어느 것도 생성하지 않는다고 합시다. 다음으로 구성하고 싶은 것은  $S_\omega$ 입니다. 어떻게든 "도약"해야 합니다. 이를 위해, 이제 다음과 같은 무한합집합을 취합니다

$$S_\omega \stackrel{\text{정의}}{=} S_0 \cup S_1 \cup S_2 \cup \dots$$

이 집합의 원소들 역시 독립적입니다(왜 그럴까요?).

짜잔! "존재하는 모든 집합의 합집합을 취한다"는 단순한 트릭으로, 우리는 첫 번째 극한 순서수  $\omega$ 까지의 장애물을 방금 뛰어넘었습니다. 그런 다음 다시 한번 원소들을 계속 집어넣기만 하면  $S_{\omega+1}, S_{\omega+2}, \dots$ 를 구성할 수 있습니다. 그러다 다음 장애물인  $S_{2\omega}$ 를 뛰어넘어야 할 때가 되면, 이전의 모든 집합들을 "합집합하는" 같은 트릭을 다시 사용하면 됩니다.

따라서 우리는 이 과정을 다음과 같이 공식화할 수 있습니다:

1.  $S_0 = \emptyset$ 이라 합시다.
2. 후행자 단계  $S_{\alpha+1}$ 에서는,  $S_\alpha$ 에 임의의 원소를 추가하여  $S_{\alpha+1}$ 을 얻습니다.
3. 극한 단계  $S_\lambda$ 에서는, 합집합  $\bigcup_{\gamma < \lambda} S_\gamma$ 를 취합니다.

우리가 결국 멈추게 될 것임을 어떻게 알 수 있을까요? 사실 이 과정은 실수들을 많이 소모합니다. 특히, (선택공리를 가정하면) 순서수들은  $\mathbb{R}$ 의 크기보다 커집니다. 따라서 멈추지 않는다면 우리는 말 그대로 모든 단 하나의 실수를 다 써버린 지점에 도달하게 됩니다. 그때가 되면 원소들이 결코 독립적일 수 없으므로, 이는 명백히 불가능합니다!

따라서 초한 재귀에 의해, 우리는 결국 생성하는 어떤  $S_\gamma$ 에 도달합니다: 원소들은 모두 독립적이지만, 모든 실수가 이를 이용해 표현될 수 있습니다. 끝!

## §88.5 초론의 보조정리

이제 초론의 보조정리가 무엇인지 말씀드릴 수 있습니다: 이는 우리가 어떤 부분순서집합에서든 같은 일을 할 수 있게 해줍니다.

위의 예시를 다음과 같이 생각할 수 있습니다: 독립인 원소들의 모든 집합을 고려해 봅시다. 이들은 포함관계에 의해 부분순서집합을 이루며, 우리가 한 일은 말 그대로 사슬을 타고 올라간 것입니다

$$S_0 \subsetneq S_1 \subsetneq S_2 \subsetneq \dots$$

한 번에 한 단계씩만 나아간 것이 아니므로 이는 완전한 등반이라고는 할 수 없습니다:  $S_\omega$  까지 올라가기 위해서는 "도약"을 해야 했고 그 후 다시 등반을 이어갔습니다. 하지만 핵심 아이디어는 부분순서집합의 맨 꼭대기에 이를 때까지 올라가는 것입니다; 앞선 경우에는 생성집합에 도달했을 때가 그에 해당합니다.

같은 방법이 임의의 **부분순서집합**  $\mathbb{P}$ 에 대해서도 그대로 적용됩니다. 용어를 몇 가지 정의해 봅시다. 전체 부분순서집합  $\mathbb{P}$ 의 **국소 최댓값**이란 자신보다 진정으로 큰 다른 원소가 존재하지 않는 원소입니다. (대부분의 저자들은 이를 "극대 원소"라고 부르지만, 저는 "국소 최댓값"이 더 정확한 용어라고 생각합니다.)

이제 **길이  $\gamma$ 인 사슬**이란  $\alpha < \gamma$ 인 모든  $\alpha$ 에 대해  $p_0 < p_1 < p_2 < \dots$ 를 만족하는 원소  $p_\alpha$ 들의 집합입니다. (사슬이 마지막 원소를 갖는 것은  $\gamma$ 가  $\omega + 3$ 과 같은 후속 순서수인 경우, 오직 그 경우에 한함을 관찰하십시오.) 사슬의 **상계**란 사슬의 모든 원소보다 크거나 같은 원소  $\bar{p}$ 입니다; 특히  $\gamma$ 가 후속 순서수라면 사슬의 마지막 원소를 취하는 것만으로 충분합니다.

이러한 언어로 표현하면, 초른의 보조정리는 다음과 같이 서술됩니다

#### 정리 88.5.1 (초른의 보조정리)

$\mathbb{P}$ 를 공집합이 아닌 부분순서집합이라 하십시오. 모든 사슬이 상계를 가진다면,  $\mathbb{P}$ 는 국소 최댓값을 가집니다.

길이가 후속 순서수와 같은 사슬은 항상 상계를 가지지만, 극한의 경우에는 이것이 성립하지 않습니다. 따라서 초른의 보조정리의 가정은 정확히 우리가  $p_\omega$  및 다른 극한 순서수들을 정의하기 위해 "도약"할 수 있게 해주는 것입니다. 그리고 초른의 보조정리의 증명은 간단합니다: 후속 단계에서는 부분순서집합을 계속 타고 올라가고, 극한 단계에서는 초른의 조건을 이용해 도약하여, 이렇게 정말로 긴 사슬을 만들어 나갑니다. 하지만 결국 멈춰야 합니다, 그렇지 않으면 말 그대로  $\mathbb{P}$ 의 원소가 바닥납니다. 그리고 유일하게 가능한 멈춤 지점은 국소 최댓값입니다.

앞서의 풀이를 초른의 보조정리의 언어로 표현하고자 한다면, 다음과 같이 말할 수 있습니다:

증명. 독립인 실수들의 집합을 원소로 갖는 부분순서집합을 살펴봅시다. 모든 사슬  $S_0 \subsetneq S_1 \subsetneq \dots$ 는 상계  $\bigcup S_\alpha$ 를 가집니다 (이것이 실제로 그 부분순서집합의 원소임을 확인해야 합니다). 따라서 초른의 보조정리에 의해, 국소 최댓값  $S$ 가 존재합니다. 그러면  $S$ 는 반드시 생성집합이어야 합니다, 그렇지 않다면 여기에 원소를 하나 더 추가할 수 있을 것이기 때문입니다.  $\square$

그러니 사실상 초른의 보조정리는 제가 앞서 설명한 등반 작업 전체를 부호화하고 있는 것입니다. 이는 모든 상투적인 절차를 담아내는 깔끔한 작은 패키지이며, 무엇을 확인해야 하는지 정확히 알려줍니다.



이미지 출처: [Go09]

마지막으로 여러분이 궁금해할 만한 것 하나: 선택공리는 어디에 쓰이는 것일까요? 아이 디어는 이렇습니다, 어떤 사슬에 대해서든  $\hat{p}$ 가 여러 개 있을 수 있고, 그중 하나를 골라야 합니다. 무한히 많은 횟수에 걸쳐 임의의 선택을 하고 있으므로, 선택공리가 필요합니다. (사실, 정리 88.3.1에서처럼 기수를 논하기 위해서도 선택공리가 필요합니다.) 하지만 정말로 특별할 것은 없습니다.

## §88.6 생각해 볼 만한 조금 더 어려운 문제

문제 88A.  $f: (0, \infty) \rightarrow \mathbb{R}$ 가  $f(1) = 1$ ,  $f(\pi) = \frac{22}{7}$ , 그리고

$$f(x+y) = f(x) + f(y)$$

모든  $x, y > 0$ 에 대해 (다음 식)을 만족한다고 합시다.  $\pi \approx 3.14159265358979$ 임이 주어졌을 때,  $0 < r < 1$ 이고  $f(r) > 9000$ 인 실수  $r$ 의 예를, 계산기 없이 증명과 함께 구하십시오.

문제 88B.  $f: (0, \infty) \rightarrow \mathbb{R}$ 가 다음을 만족한다고 합시다

$$f(x+y) = f(x) + f(y)$$

모든  $x, y > 0$ 에 대해. 다음 각 진술이 참인지 거짓인지 표시하십시오.

1. 함수  $f$ 는 코시 함수 방정식을 계속 만족하면서 항상  $f: \mathbb{R} \rightarrow \mathbb{R}$ 로 확장될 수 있습니다.
2. 만약  $f$ 가 앞선 진술에서처럼 확장된다면,  $f$ 는 반드시 홀함수여야 합니다.
3. 모든  $x > 0$ 에 대해  $f(x) \geq 0$ 이면,  $f$ 는 선형입니다.
4.  $f$ 가 강증가함수이면,  $f$ 는 선형입니다.
5. 함수  $f$ 는  $(0, \infty)$ 에서  $\mathbb{R}$ 로 가는 전단사가 아닙니다.
6.  $f$ 가 단사이지만 선형이 아닐 수 있습니다.
7.  $f$ 가 전사이지만 선형이 아닐 수 있습니다.
8.  $f$ 가 상수가 아니면서 모든  $x \in \mathbb{R}$ 에 대해  $f(x) \in \mathbb{Q}$ 일 수 있습니다.
9.  $f$ 가 상수가 아니면서 모든 0이 아닌  $x \in \mathbb{R}$ 에 대해  $f(x) \notin \mathbb{Q}$ 일 수 있습니다.

**문제 88C** (투키의 보조정리).  $\mathcal{F}$ 를 공집합이 아닌 집합족이라 합시다. 임의의 집합  $A$ 에 대해, 집합  $A$ 가  $\mathcal{F}$ 에 속하는 것과  $A$ 의 모든 유한 부분집합이  $\mathcal{F}$ 에 속하는 것이 동치라고 가정합시다.

극대 집합  $Y \in \mathcal{F}$ 가 존재함을 증명하십시오 (즉,  $Y$ 가  $\mathcal{F}$ 의 다른 어떤 집합에도 포함되지 않음을 의미합니다).

# 89 선택공리를 포함한 체르멜로-프렝켈

[Le14]의 3.1절에 이에 대한 좋은 설명이 있습니다.

## §89.1 궁극의 함수방정식

추상수학에서는 구조를 가져야 할 성질로 정의하는 경우가 많습니다. 예를 들어 군은 이러한 공리를 만족하는 집합과 이항연산이고, 거리 공간은 이러한 공리를 만족하는 집합과 거리 함수입니다.

그러나 이러한 정의들은 이전의 정의에 의존합니다. [Le14]의 생생한 예시를 보면:

- 벡터 공간은 다음을 만족하는 아벨 군입니다...
- 아벨 군은 다음을 만족하는 이항연산을 가집니다...
- 집합 위의 이항연산은...
- 집합은 ...

등등입니다.

어딘가에서는 멈춰야 하는데, 무한한 정의의 목록은 좋지 않기 때문입니다. 멈추는 지점은 결국 성질로 "정의된" 집합이 됩니다. 여기서 요령은 집합이 무엇인지 실제로 정의하지 않으면서도, 이러한 집합들이 특정 성질을 만족한다고 가정한다는 점입니다. 이것이 바로 ZFC 공리입니다. 대략적으로 ZFC는 궁극의 함수방정식으로 생각할 수 있습니다.

이 공리들이 무엇인지 말하기 전에, 주의할 점들을 먼저 이야기해야 합니다.

## §89.2 칸토어의 역설

직관적으로 집합은 순서 없는 원소들의 모임입니다. 두 집합은 같은 원소를 공유하면 같습니다:

$$\{x \mid x \text{ 깃털 없는 두 발 동물입니다}\} = \{x \mid x \text{ 사람입니다}\}$$

(공룡에 관한 문제는 잠시 접어두겠습니다).

또 다른 예로, 아무 대상도 포함하지 않는 공집합  $\emptyset$ 이 있습니다. 집합  $\{1, 2, 3\}$ 을 가질 수도 있고, 자연수의 집합  $\mathbb{N} = \{0, 1, 2, \dots\}$ 을 가질 수도 있습니다. (집합론의 목적상 0은 보통 자연수로 간주됩니다.) 집합은 심지어  $\{\mathbb{Z}, \mathbb{Q}, \mathbb{N}\}$ 처럼 다른 집합을 포함할 수도 있습니다. 다 괜찮아 보이지 않습니까?

문제는 이 정의가 사실 충분히 좋지 않다는 것인데, 그 이유는 다음과 같습니다. "집합은 대상들의 임의의 모임이다"라고만 말한다면, 모든 집합의 집합인 정말로 큰 집합  $V$ 를 생각할 수 있습니다. 여기까지는 문제가 없지 않습니까?  $V \in V$ 라는 기이한 상황이 생기겠지만, 뭐 별일 아닙니다.

불행하게도 이  $V$ 의 존재는 즉시 역설로 이어집니다. 고전적인 것은 러셀의 역설입니다. 저는 대신 다소 더 간단한 것을 제시하겠습니다:  $V$ 가 자기 자신을 포함할 뿐만 아니라, 모든 부분집합  $S \subseteq V$ 가 그 자체로  $V$ 의 원소입니다(즉  $S \in V$ ).  $\mathcal{P}(V)$ 가  $V$ 의 **역집합**(즉  $V$ 의 모든 부분집합)을 나타낸다고 하면, 다음과 같은 포함관계를 얻습니다

$$\mathcal{P}(V) \hookrightarrow V.$$

이는 좋지 않은데, 그 이유는:

**보조정리 89.2.1** (칸토어의 대각선 논법)

임의의 집합  $X$ 에 대해, 단사 사상  $\iota: \mathcal{P}(X) \hookrightarrow X$ 를 구성하는 것은 불가능합니다.

증명. 모순을 이끌어내기 위해  $\iota$ 가 존재한다고 가정하십시오.

**연습문제 89.2.2.**  $\iota$ 가 존재하면 전사 사상  $j: X \twoheadrightarrow \mathcal{P}(X)$ 가 존재함을 보이십시오. (이는 보기보다 쉬운데, 그냥  $\iota$ 를 뒤집으면 됩니다.)

이제  $j$ 가 존재할 수 없다고 주장합니다.

먼저 아이디어를 전달하기 위해  $j$ 에 대한 그림을 그려 보겠습니다:

|          |                   | $x_1$    | $x_2$    | $x_3$    | $x_4$    | $x_5$    | $\dots$  |
|----------|-------------------|----------|----------|----------|----------|----------|----------|
| $x_1$    | $\xrightarrow{j}$ | <b>0</b> | 1        | 1        | 0        | 1        | $\dots$  |
| $x_2$    | $\xrightarrow{j}$ | 1        | <b>1</b> | 0        | 1        | 1        | $\dots$  |
| $x_3$    | $\xrightarrow{j}$ | 0        | 1        | <b>0</b> | 0        | 1        | $\dots$  |
| $x_4$    | $\xrightarrow{j}$ | 1        | 0        | 0        | <b>1</b> | 0        | $\dots$  |
| $x_5$    | $\xrightarrow{j}$ | 0        | 1        | 1        | 1        | <b>1</b> | $\dots$  |
| $\vdots$ |                   | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\ddots$ |

여기서, 각  $j(x) \subseteq X$ 에 대해, 해당 원소가  $j(x)$  안에 있다는 것을 뜻하기 위해 “1”이라고 쓰고, 그렇지 않으면 “0”이라고 쓰겠습니다. 따라서  $j(x_1) = \{x_2, x_3, x_5, \dots\}$ 입니다. ( $X$ 가 비가산일 수 있으므로 여기서 첨자는 정수가 아니라 순서수입니다. 전문가라면 제가  $X$ 의 정렬을 암묵적으로 가정했음을 눈치챌 수 있겠지만, 이 그림은 어디까지나 동기 부여를 위한 것이므로 이 점에 대해서는 깊이 다루지 않겠습니다.) 그런 다음 대각선을 읽어내어 새로운 집합을 얻을 수 있습니다. 우리 예시에서, 대각선은 집합  $A = \{x_2, x_4, x_5, \dots\}$ 를 지정합니다. 그런 다음 이것을 “뒤집어” 집합  $B = \{x_1, x_3, \dots\}$ 를 얻습니다.

형식적 증명으로 돌아갑시다. 위에서 동기를 부여했듯이, 우리는 다음과 같이 정의합니다

$$B = \{x \mid x \notin j(x)\}.$$

구성에 의해,  $B \subseteq X$ 는  $j$ 의 상(image)에 속하지 않으며, 이는  $j$ 가 전사라고 가정했던 것과 모순됩니다.  $\square$

이제 여러분이 집합론자가 아니라면, 아마도 “뭐, 특정 집합들은 볼 수 없나 보다”라고 하며 그냥 넘어갈 수 있을 것입니다. 하지만 여러분이 집합론자라면, 이는 여러분을 걱정스럽게 만듭니다. 왜냐하면 이것이 집합을 그저 “대상들의 모임”으로 정의할 수 없다는 것을 의미한다는 것을 깨닫게 되기 때문입니다. 그렇게 하면 모든 것이 폭발해 버립니다. 무언가 더 필요합니다.

## §89.3 집합론의 언어

우리는 “대상들의 모임”이라는 비형식적 서술 외에 집합을 지칭할 방법이 필요합니다.

그래서 우리가 할 일은 다음과 같습니다. 우리는 논리 진술을 작성하는 방법인 형식적 집합론의 언어를 정의하는 것으로 시작하겠습니다. 먼저 우리가 흔히 쓰는 논리 연산자들을 도입할 수 있습니다:

- $\forall$ 는 “모든  $x$ 에 대해”를 의미합니다
- $\exists$ 는 “존재한다”를 의미합니다

- $=$ 는 “같다”를 의미합니다
- $X \implies Y$ 는 “ $X$ 이면  $Y$ 이다”를 의미합니다
- $A \wedge B$ 는 “ $A$ 이고  $B$ ”를 의미합니다
- $A \vee B$ 는 “ $A$ 이거나  $B$ ”를 의미합니다
- $\neg A$ 는 “ $A$ 가 아니다”를 의미합니다.

우리는 집합론을 다루고 있으므로, 추가할 연산자는 단 하나, 즉 포함 관계  $\in$ 뿐입니다. 그리고 (당분간은) 이것이 우리가 사용할 전부입니다.

그렇다면 “집합  $\{1, 2\}$ ”와 같은 것을 어떻게 표현할까요? 요령은 우리가 실제로 어떤 집합을 “구성”하지 않고, 대신 다음과 같이 간접적으로 지칭한다는 것입니다:

$$\exists S : x \in S \iff ((x = 1) \vee (x = 2)).$$

이는 다음과 같이 읽습니다: “ $x = 1$  또는  $x = 2$ 일 때, 그리고 그때에만  $x$ 가  $S$  안에 있는 그러한  $S$ 가 존재한다”. 우리는 더 이상 집합 그 자체를 대상으로 지칭할 필요가 없습니다 — 이제 우리에게는 집합이 정확히 무엇을 포함하는지에 대한 공식을 씌으로써 집합을 “생성”하는 방법이 생겼습니다. 이는 기계가 파싱할 수 있는 것입니다.

그렇다면 집합이 아닌 1과 2 같은 것들은 어떻게 해야 할까요? 답은 다음과 같습니다:

**집합의 원소들은 그 자체로 집합입니다.**

우리는 모든 것을 집합으로 만들 것입니다. 자연수는 집합이 될 것입니다. 순서쌍도 집합이 될 것입니다. 함수도 집합이 될 것입니다. 나중에 1과 같은 것을 어떻게 집합으로 부호화하는지 정확히 알려드리겠습니다. 지금은 집합이 단지 대상만을 담는 것이 아니라 다른 집합들도 담는다는 것만 알아두시면 됩니다.

이제 어떤 것이 집합인지 아닌지에 대해 이야기하는 것이 말이 됩니다:  $\exists x$ 는 “ $x$ 는 집합이다”를 의미하고,  $\nexists x$ 는 “ $x$ 는 집합이 아니다”를 의미합니다. 다시 말해, 우리는 어떤 것이 집합인지 판별하는 문제를 그것이 존재하는지의 문제로 바꾸어 말한 것이며, 이는 우리의 형식적 언어에서 다루기 더 쉽게 만들어 줍니다. 이는 우리의 공리 체계가 다음을 증명할 수 있게 허용하지 않으면서도, 많은 것들이 존재함을 보일 수 있는 방법을 반드시 찾아야 함을 의미합니다

$$\exists S \forall x : x \in S.$$

왜냐하면 만약 우리가 이 논리식을 증명한다면, 처음에 우리를 이 토끼굴로 빠뜨린 원인이었던 그 “나쁜” 집합을 갖게 되기 때문입니다.

## §89.4 ZFC의 공리들

이 공리들에 대해 특별히 자세히 다루고 싶지는 않습니다; 관심이 있다면 다음을 읽으십시오:

- <https://blog.evanchen.cc/zfc1/>
- <https://blog.evanchen.cc/zfc2/>

다음은 공리들에 대한 훨씬 더 간결한 설명으로, 집합론 언어로 된 대응 문장도 함께 포함합니다.  $\forall$ ,  $\exists$  등을 해석하는 연습을 해볼 가치가 있으며, 형식적 문장을 공리의 자연어 서술과 비교함으로써 그렇게 할 수 있습니다.

먼저, 가장 쉬운 두 공리입니다:

- Extensionality는  $\forall x \forall y ((\forall a (a \in x \iff a \in y)) \implies x = y)$ 라는 문장이며, 이는 두 집합  $x$ 와  $y$ 가 같은 원소를 가지면  $x = y$ 임을 말합니다.

- EmptySet은  $\exists a : \forall x \neg(x \in a)$ 라는 문장입니다; 이는 원소가 없는 집합이 존재함을 말합니다. Extensionality에 의해 이 집합은 유일하므로, 이를  $\emptyset$ 으로 표기합니다.

다음 두 공리는 새로운 집합을 만드는 기본적인 방법을 제공합니다.

- 두 원소  $x$ 와  $y$ 가 주어지면, 그 두 원소만을 포함하는 집합  $a$ 가 존재합니다. 기계 코드로 표현하면, 이는 Pairing이라는 문장이며 다음과 같이 씁니다

$$\forall x \forall y \exists a \quad \forall z, z \in a \iff ((z = x) \vee (z = y)).$$

Extensionality에 의해 이 집합  $a$ 는 유일하므로,  $a = \{x, y\}$ 로 씁니다.

- 집합  $a$ 가 주어지면,  $a$ 의 원소들의 합집합을 만들 수 있습니다. 예를 들어,  $a = \{\{1, 2\}, \{3, 4\}\}$ 이면,  $U = \{1, 2, 3, 4\}$ 는 하나의 집합입니다. 형식적으로, 이는 Union이라는 문장입니다:

$$\forall a \exists U \quad \forall x [(x \in U) \iff (\exists y : x \in y \in a)].$$

$U$ 는 Extensionality에 의해 유일하므로, 이를  $\cup a$ 로 표기합니다.

- 우리는 **멱집합**  $\mathcal{P}(x)$ 를 구성할 수 있습니다. 형식적으로, PowerSet 문장은 다음을 말합니다

$$\forall x \exists P \forall y (y \in P \iff y \subseteq x)$$

여기서  $y \subseteq x$ 는  $\forall z (z \in y \implies z \in x)$ 의 축약입니다. Extensionality가  $P$ 의 유일성을 보장하므로, 이를  $\mathcal{P}(x)$ 로 표기합니다.

- Foundation은 무한히 하강하는 연쇄가 존재하지 않음을 말합니다

$$x_0 \ni x_1 \ni x_2 \ni \dots$$

이는 우리가 귀납을 사용할 수 있게 해주므로 중요합니다. 특히, **어떤 집합도 자기 자신을 포함하지 않습니다.**

- Infinity는  $\omega = \{0, 1, \dots\}$ 가 하나의 집합임을 함의합니다.

이것들은 모두 여러분이 이미 익숙한 것들이므로, 그 직관을 유지하십시오. 다음 것은 덜 직관적입니다:

- **제한된 분리 스키마**는 다음을 말합니다: 집합  $X$ 가 주어지고, 어떤 논리식  $\phi(x)$ 가 있다면,  $X$ 의 원소들을 걸러내어 다음과 같은 부분집합을 얻을 수 있습니다

$$Y = \{x \in X \mid \phi(x)\}.$$

형식적으로, 논리식  $\phi$ 가 주어지면:

$$\forall X \quad \exists Y \quad \forall y (y \in Y \iff y \in X \wedge \phi(y)).$$

이러한 걸러내기는 오직 이미 주어진 집합에 대해서만 할 수 있음에 유의하십시오. 따라서  $\{x \mid x \text{ 집합입니다}\}$ 를 만드는 것은 유효하지 않습니다. 우리는 이 점에 감사해야 하는데, 이것이 칸토어의 역설을 피할 수 있게 해주기 때문입니다.

**표기의 남용 89.4.1.** 엄밀히 말하면, 가능한 모든 논리식  $\phi$ 에 대해 하나씩 존재하는 무한히 많은 문장  $\text{Comprehension}_\phi$ 가 있음에 유의하십시오. 표기를 남용하여, 모든  $\phi$ 에 대한 무한히 많은 공리  $\text{Comprehension}_\phi$ 를  $\text{Comprehension}$ 으로 줄여 표기하겠습니다.

$\text{Replacement}_\phi$ 라 불리는 마지막 스키마가 하나 있습니다.  $X$ 가 집합이고  $\phi(x, y)$ 가 어떤 논리식이어서, 모든  $x \in X$ 에 대해  $\phi(x, y)$ 가 참이 되는 유일한  $y$ 가 전체 영역 안에 존재한다고 합시다: 예를 들어 “ $y = x \cup \{x\}$ ”는 이를 만족합니다. (사실상,  $\phi$ 는  $X$  위에서 함수  $f$ 를 정의하는 셈입니다.) 그러면 정확히 이러한 상들로 이루어진 집합  $Y$ 가 존재합니다: (즉  $f^{\text{img}}(X)$ 는 하나의 집합입니다).

**표기의 남용 89.4.2.** 표기를 남용하여, 모든  $\phi$ 에 대한 무한히 많은 공리  $\text{Replacement}_\phi$ 를  $\text{Replacement}$ 로 줄여 표기하겠습니다.

**비고 89.4.3** — 여기서 “모든  $x \in X$ 에 대해,  $\phi(x, y)$ 가 참이 되는 유일한  $y$ 가 전체 영역 안에 존재한다”는 것은 무엇을 의미할까요? 논리식  $\phi$ 가 주어졌을 때,  $\text{Replacement}_\phi$ 가 공리가 되기 위해 그 진술이 참인지를 우리는 어떻게 판단할 수 있을까요? 일반적으로는 판단할 수 없다는 것이 밝혀집니다. 하지만 우리는 그것이 필요하지 않습니다! 이 문제를 우회하기 위해, 모든  $\phi(x, y)$ 에 대해, 공리  $\text{Replacement}_\phi$ 는 다음을 말합니다

$$“\phi \text{가 함수를 정의한다}” \implies \forall X \quad \exists Y \quad “Y = f^{\text{img}}(X)”.$$

다시 말해,  $\phi$ 가 함수라는 가정은 공리  $\text{Replacement}_\phi$  자체에 “접혀 들어가” 있습니다. 이는 지금 당장은 그다지 중요하지 않겠지만, 나중에 모형 이론에서 중요해질 것인데, 그때 우리는 보조정리 92.5.1에서 모형  $M$ 이  $\text{Replacement}$ 를 만족한다는 것이 무엇을 의미하는지 서술할 것입니다.

우리는 선택 공리에 대한 논의를 잠시 미룹니다.

## §89.5 부호화

이제 이 허술한 집합의 우주를 갖추었으니, 수학을 다시 세우기 시작할 수 있습니다. 이는 다음 장인 순서수에 관한 장에서 더 자세히 보게 될 것입니다.

**정의 89.5.1. 순서쌍**  $(x, y)$ 는 다음과 같은 형태의 집합입니다

$$(x, y) := \{\{x\}, \{x, y\}\}.$$

$(x, y) = (a, b)$ 인 것은  $x = a$ 이고  $y = b$ 인 것과 동치임에 유의하십시오. 순서  $k$ -튜플은 재귀적으로 정의될 수 있습니다: 세 자리 튜플  $(a, b, c)$ 는  $(a, (b, c))$ 를 의미합니다.

**정의 89.5.2. 함수**  $f: X \rightarrow Y$ 는 다음을 만족하는 순서쌍들의 모임으로 정의됩니다

- $(x, y) \in f$ 이면,  $x \in X$ 이고  $y \in Y$ 입니다.
- 모든  $x \in X$ 에 대해,  $(x, y) \in f$ 인  $y \in Y$ 가 유일하게 존재합니다. 이  $y$ 를  $f(x)$ 로 표기합니다.

**정의 89.5.3. 자연수**는 다음과 같이 귀납적으로 정의됩니다

$$\begin{aligned} 0 &= \emptyset \\ 1 &= \{0\} \\ 2 &= \{0, 1\} \\ 3 &= \{0, 1, 2\} \\ &\vdots \end{aligned}$$

모든 자연수의 집합은  $\omega$ 로 표기됩니다.

**표기의 남용 89.5.4.** 네, 죄송합니다만, 집합론에서 0은 자연수로 간주됩니다. 이러한 이유로 저는  $\mathbb{N}$ 이 아니라  $\omega$ 를 사용하고 있는데, 이 책의 다른 모든 부분에서는 명시적으로  $0 \notin \mathbb{N}$ 으로 두고 있기 때문입니다.

등등,等等.

## §89.6 선택과 정렬순서

선택 공리는, 공집합이 아닌 집합들의 모임  $Y$ 가 주어졌을 때,  $Y$ 의 각 원소로부터 하나의 원소를 “고르는” 함수  $g: Y \rightarrow \cup Y$ 가 존재한다는 것을 말합니다. 이는 모든  $y \in Y$ 에 대해  $g(y) \in y$ 임을 의미합니다. (전형적인 예시로는,  $Y$ 가 무한히 많은 서랍을 포함하고, 각 서랍(즉  $y$ )에 양말이 하나씩 들어 있다는 것입니다.)

형식적으로는, 다음 문장입니다

$$\forall Y (\emptyset \notin Y \implies \exists g: Y \rightarrow \cup Y \text{ 인 } \forall y \in Y (g(y) \in y) .)$$

까다로운 부분은 그러한 함수  $g$ 를 우리가 상상할 수 있다는 것이 아니라, 실제로 이 함수  $g$ 가 실제로 하나의 집합이라는 것입니다.

자주 유용하게 쓰이는 동치인 서술 방식이 있습니다.

**정의 89.6.1.**  $X$ 의 **정렬순서**  $<$ 란,  $X$  위의 무한 하강 사슬이 없는 강한 전순서입니다.

집합 위의 정렬순서는 매우 유용한데, 최소 원소를 고를 수 있기 때문입니다: 예를 들어 이는 귀납법을 수행할 수 있게 해줍니다.

### 예제 89.6.2 (정렬순서의 예시와 반례)

- (a) 자연수  $\omega = \{0, 1, 2, \dots\}$ 는  $<$ 에 의해 정렬순서를 이룹니다.
- (b) 정수  $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ 는  $<$ 에 의해 정렬순서를 이루지 않는데, 무한 하강 사슬이 존재하기 때문입니다 ( $-1 > -2 > -3 > \dots$ 를 생각해 보십시오).
- (c) 양의 실수는  $<$ 에 의해 정렬되지 않는데, 이는 다시 감소하는 사슬  $\frac{1}{1} > \frac{1}{2} > \frac{1}{3} > \dots$  때문입니다.
- (d) 양의 정수는 나눗셈 연산  $|$ 에 의해 정렬되지 않습니다. 감소하는 사슬은 없지만, 비교할 수 없는 원소들이 존재합니다 (예를 들어  $3 \nmid 5$ ,  $5 \nmid 3$ 이고  $3 \neq 5$ ).

### 정리 89.6.3 (정렬 정리)

선택공리를 가정하면, 모든 집합에 대해 어떤 정렬 순서를 놓을 수 있습니다.

사실, 정렬 정리는 실제로 선택공리와 동치입니다.

## §89.7 집합 대 클래스

**이 절의 대표적인 예:** 모든 집합의 집합은 진클래스의 표준적인 예시입니다.

”클래스”를 언급하면서 ZFC에 대한 논의를 마무리합니다.

대략적으로 말하면, 일어난 ”나쁜 일”이란 우리가 어떤 집합  $S$ , 즉 ”모든 집합의 집합”을 고려했는데, 그것이 너무 컸다는 것입니다. 즉,

$$\{x \mid x \text{ 집합입니다}\}$$

는 좋지 않습니다. 마찬가지로, 우리는 다음과 같은 집합을 구성할 수 없습니다

$$\{x \mid x \text{순서쌍입니다}\}.$$

칸토어 역설의 교훈은 우리가 원하는 아무 집합이나 만들 수는 없다는 것입니다. 우리는 그보다 더 조심해야 합니다.

그럼에도 불구하고, 어떤 집합이 주어지면 우리는 여전히 그것이 순서쌍인지 아닌지를 알 수 있습니다. 그러므로 편의상, 우리는 **클래스**를 "모든 순서쌍의 클래스"와 같은 하나의 "개념"으로 정의하겠습니다. 형식적으로, 클래스는 어떤 논리식  $\phi$ 에 의해 정의됩니다: 그것은 그 논리식을 만족하는 집합들로 이루어집니다.

특히:

**정의 89.7.1.** 모든 집합의 클래스는  $V$ 로 표기되며,  $V = \{x \mid x = x\}$ 로 정의됩니다. 이는 **폰 노이만 전체**라고 불립니다.

클래스가 집합이 아닐 때 이를 **진클래스**라고 하며, 예를 들면 다음과 같습니다:

**정리 89.7.2** (모든 집합의 집합은 존재하지 않습니다)

$V$ 는 진클래스입니다.

증명. 그렇지 않다고 가정하면,  $V$ 는 집합입니다. 그러면  $V \in V$ 인데, 이는 Foundation을 위반합니다. (사실, 앞서 보았듯이 Foundation이 없더라도  $V$ 는 집합일 수 없습니다).  $\square$

**표기의 남용 89.7.3.** 클래스  $C$ 가 주어지면,  $x$ 가  $C$ 의 정의 성질을 가진다는 것을 나타내기 위해  $x \in C$ 라고 쓰겠습니다. 예를 들어,  $x \in V$ 는 " $x$ 는 집합이다"를 의미합니다.

이는  $x$ 가  $V$ 의 원소라는 것을 의미하지 않습니다 –  $V$ 는 집합이 아니므로 이는 말이 되지 않습니다.

## §89.8 생각해 볼 만한 조금 더 어려운 문제

**문제 89A.**  $A$ 와  $B$ 를 집합이라 합시다.  $A \cap B$ 와  $A \times B$ 가 집합임을 보이십시오.

**문제 89B.** 모든 군의 클래스가 진클래스임을 보이십시오. (군의 정의를 순서쌍  $(G, \cdot)$ 로 취할 수 있으며, 여기서  $\cdot$ 는 함수  $G \times G \rightarrow G$ 입니다.)

**문제 89C.** 정렬 정리로부터 선택공리가 따라 나옴을 보이십시오.

**문제 89D<sup>†</sup>.** 사실 Replacement  $\implies$  Comprehension임을 증명하십시오.

**문제 89E** (대만 IMO 훈련 캠프에서). 각각 빨간색, 초록색, 파란색 중 하나인 모자를 쓴 무한히 많은 사람들을 생각해 봅시다. 각 사람은 자신을 제외한 모든 사람의 모자 색깔을 볼 수 있습니다. 동시에 각 사람은 자신의 모자 색깔을 추측합니다. 이들이 기껏해야 유한히 많은 사람만 자신의 색깔을 잘못 추측하도록 하는 전략을 세울 수 있음을 보이십시오.



# 90 순서수

## §90.1 미취학 아동을 위한 세기

미취학 시절, 우리는 다음과 같이 세는 법을 배웠습니다. 우리는 기호 1, 2, 3, 4, ...의 집합을 정의했습니다. 그러면 선생님이 사과 세 개를 들고 이렇게 말하곤 했습니다:

“하나 . . . 둘 . . . 셋! 사과가 세 개 있습니다.”



이미지 출처 [Ho]

여기서 암묵적인 정의는, 말한 마지막 숫자가 최종 답이라는 것입니다. 이는 무한 집합을 세려고 할 때 몇 가지 명백한 문제를 일으키지만, 유한한 세계에서조차도 이 세는 방법은 가장 단순한 집합에 대해 실패합니다: 다음 그림에는 사과가 몇 개 있습니까?



이미지 출처 [Kr]

답: 0. 아무것도 말할 것이 없으며, 우리의 세는 방법은 가장 단순한 집합인 공집합에 대해 실패했습니다.

## §90.2 집합론자를 위한 세기

이 절의 대표적인 예:  $\omega + 1 = \{0, 1, 2, \dots, \omega\}$  로 하면 될 것 같습니다.

나열된 숫자 중 마지막 것을 사용하는 대신, 저는 기호  $0, 1, 2, \dots$  목록으로 시작하여, 말해지지 않은 첫 번째 숫자를 최종 답으로 삼는 방법을 제안합니다. 그리하여 사과 세 개를 세려면, 우리는 다음과 같이 말할 것입니다

“영 . . . 일 . . . 이! 사과가 세 개 있습니다.”

우리는 이러한 숫자를 순서수라고 부를 것입니다(엄밀한 정의는 나중에 다룹니다). 특히, 우리는 각 순서수를 우리가 말한 것들의 집합으로 정의할 것입니다:

$$\begin{aligned} 0 &= \emptyset \\ 1 &= \{0\} \\ 2 &= \{0, 1\} \\ 3 &= \{0, 1, 2\} \\ &\vdots \end{aligned}$$

이런 방식으로 자연수를 써 내려갈 수 있습니다. 다음과 같은 것을 말해보며 재미를 느낄 수도 있습니다

$$4 := \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}, \{\{\}, \{\{\}\}, \{\{\}, \{\{\}\}\}\}.$$

이런 방식으로, 우리는 곧 모든 자연수를 써 내려가게 됩니다. 다음 순서수인  $\omega$ <sup>1</sup>는 다음과 같이 정의됩니다

$$\omega = \{0, 1, 2, \dots\}$$

다음으로

$$\begin{aligned} \omega + 1 &= \{0, 1, 2, \dots, \omega\} \\ \omega + 2 &= \{0, 1, 2, \dots, \omega, \omega + 1\} \\ \omega + 3 &= \{0, 1, 2, \dots, \omega, \omega + 1, \omega + 2\} \\ &\vdots \end{aligned}$$

그리고 이런 방식으로  $\omega + n$ 을 정의하며, 결국에는 도달합니다

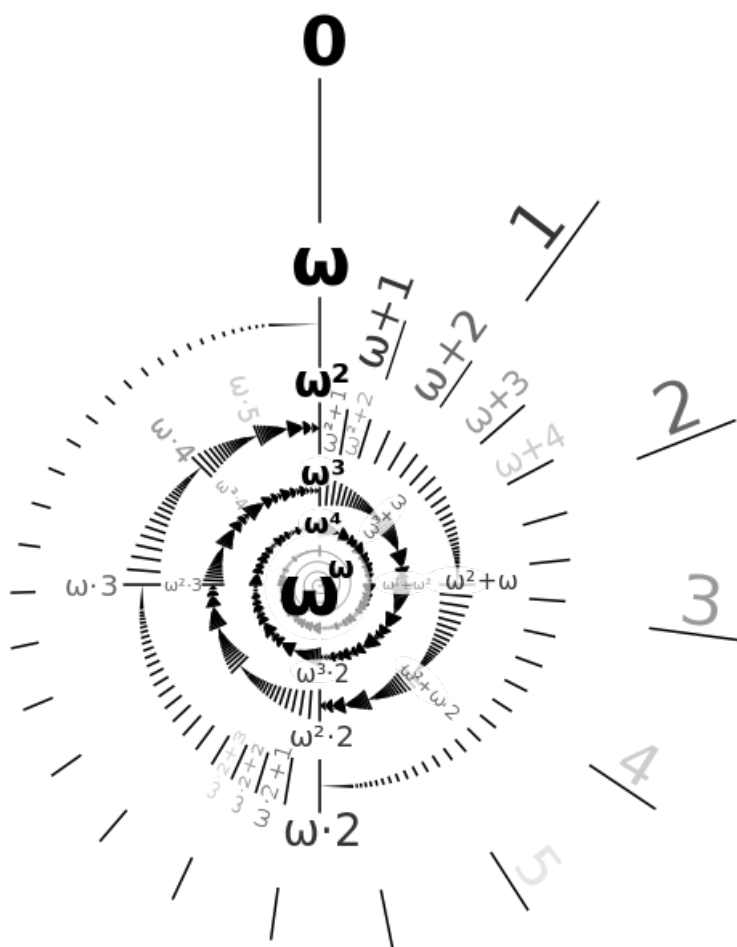
$$\begin{aligned} \omega \cdot 2 &= \omega + \omega = \{0, 1, 2, \dots, \omega, \omega + 1, \omega + 2, \dots\} \\ \omega \cdot 2 + 1 &= \{0, 1, 2, \dots, \omega, \omega + 1, \omega + 2, \dots, \omega \cdot 2\}. \end{aligned}$$

이런 방식으로 우리는 다음을 얻습니다

$$\begin{aligned} &0, 1, 2, 3, \dots, \omega \\ &\omega + 1, \omega + 2, \dots, \omega + \omega \\ &\omega \cdot 2 + 1, \omega \cdot 2 + 2, \dots, \omega \cdot 3, \\ &\vdots \\ &\omega^2 + 1, \omega^2 + 2, \dots \\ &\vdots \\ &\omega^3, \dots, \omega^4, \dots, \omega^\omega \\ &\vdots \\ &\omega^{\omega^{\omega^{\dots}}} \end{aligned}$$

<sup>1</sup>지난 장에서 언급했듯이,  $\omega$ 가 집합이라는 것은 자명하지 않으며, 그 존재성은 일반적으로 Infinity 공리에 의해 상정됩니다.

처음 몇 개의 순서수는 멋진 나선형으로 나타낼 수 있습니다.



**비고 90.2.1** — 이렇게 생각하실 수도 있습니다. 그렇다면 대신 순서수를 다음과 같이 정의하면 어떨까요? 확실히 더 짧고 간단해 보입니다!

$$\begin{aligned}
 0 &= \emptyset \\
 1 &= \{0\} \\
 2 &= \{1\} \\
 3 &= \{2\} \\
 &\vdots \\
 \omega &= \{0, 1, 2, \dots\} \\
 \omega + 1 &= \{\omega\} \\
 &\vdots
 \end{aligned}$$

일반적인 정의가 더 나은 이유는 몇 가지가 있습니다.

- 위의 “대안적 정의”는 균일하지 않습니다 —  $\alpha + 1$  형태의 순서수는 원소가 하나뿐인 집합으로 정의되는 반면, 다른 순서수들은 그것에 이르는 집합으로 정의됩니다.
- 비교가 더 간단해집니다: 두 순서수  $\alpha$ 와  $\beta$ 에 대해,  $\alpha < \beta$ 인 것과  $\alpha \in \beta$ 인 것은 동치입니다.

- 기수는 더 간단해질 것입니다: 집합 5의 크기는 정확히 5입니다.

**비고 90.2.2 (여담)** — 숫자  $\omega^{\omega^{\omega^{\dots}}}$ 에는  $\varepsilon_0$ 라는 이름이 있습니다; 이는  $\omega^{\varepsilon_0} = \varepsilon_0$ 라는 성질을 가집니다. (보통 작은 값을 나타내는 데 쓰이는) “ $\varepsilon$ ”를 사용하는 이유는, 이것이 아무리 거대해 보여도 실제로는 가산 집합이기 때문입니다. 이에 대해서는 나중에 더 다루겠습니다.

## §90.3 순서수의 정의

순서수에 대한 우리의 비형식적 설명은 하나의 사슬을 제공합니다

$$0 \in 1 \in 2 \in \dots \in \omega \in \omega + 1 \in \dots$$

순서수의 실제 정의를 제시하기 위해서는, 먼저 두 개의 보조 용어를 정의할 필요가 있습니다.

**정의 90.3.1.** 집합  $x$ 가 **추이적**(추이적)이라는 것은  $z \in y \in x$ 일 때마다  $z \in x$ 도 성립함을 의미합니다.

**예제 90.3.2** (7은 추이적입니다)

집합 7은 추이적입니다: 예를 들어,  $2 \in 5 \in 7 \implies 2 \in 7$ 입니다.

**질문 90.3.3.** 이것이 다음과 동치임을 보이십시오:  $y \in x$ 일 때마다  $y \subseteq x$ 입니다.

또한, “정렬순서”의 정의를 상기해 봅시다: 무한 하강 사슬이 없는 강한 선형 순서입니다.

**예제 90.3.4** ( $\in$ 은  $\omega \cdot 3$  위에서의 정렬순서입니다)

$\omega \cdot 3$ 에서, 우리는 다음과 같은 순서를 가집니다

$$0 \in 1 \in 2 \in \dots \in \omega \in \omega + 1 \in \dots \in \omega \cdot 2 \in \omega \cdot 2 + 1 \in \dots$$

이 순서는 무한 하강 사슬을 갖지 않습니다. 실제로, 전형적인 하강 사슬은 다음과 같이 보일 수 있습니다

$$\omega \cdot 2 + 6 \ni \omega \cdot 2 \ni \omega + 2015 \ni \omega + 3 \ni \omega \ni 1000 \ni 256 \ni 42 \ni 7 \ni 0.$$

원소가 무한히 많음에도 불구하고, 무한 하강 사슬을 만들 방법은 없습니다.

**연습문제 90.3.5.** (중요) Foundation 공리를 사용하지 않고서도, 순서수의 무한 하강 사슬이 전혀 존재하지 않음을 스스로 확인해 보십시오.

**정의 90.3.6.** **순서수**(순서수)은  $\in$ 에 의해 정렬순서화된 추이적 집합입니다. 모든 순서수의 모임은  $\text{On}$ 으로 표기합니다.

**질문 90.3.7.** 이 정의가 잘 작동함을 스스로 확인해 보십시오.

**예제 90.3.8**

- 위에서 정의된  $0, 1, 2, \dots, \omega, \omega + 1, \dots$  는 모두 순서수입니다.
- $\{3\}$ 은 순서수가 아닙니다 —  $2 \in 3$ 이지만  $2 \notin \{3\}$ 이므로 추이적이지 않습니다.
- $\{0, 1, 2, \{0, 2\}\}$ 은 순서수가 아닙니다 — 두 원소 1과  $\{0, 2\}$ 는 비교 가능하지 않습니다.

순서수를 나타낼 때 우리는 보통 그리스 문자  $\alpha, \beta$  등을 사용합니다.

**정의 90.3.9.** 우리는 다음과 같이 씁니다

- $\alpha < \beta$ 는  $\alpha \in \beta$ 를 의미하고,  $\alpha > \beta$ 는  $\alpha \ni \beta$ 를 의미합니다.
- $\alpha \leq \beta$ 는  $\alpha \in \beta$  또는  $\alpha = \beta$ 를 의미하고,  $\alpha \geq \beta$ 는  $\alpha \ni \beta$  또는  $\alpha = \beta$ 를 의미합니다,

**정리 90.3.10 (순서수는 엄격하게 순서화됩니다)**

임의의 두 순서수  $\alpha$ 와  $\beta$ 가 주어지면,  $\alpha < \beta$ ,  $\alpha = \beta$ , 또는  $\alpha > \beta$  중 하나가 성립합니다.

증명. 놀랍도록 성가시므로 생략합니다. 핵심 아이디어는  $\min(\alpha, \beta) = \alpha \cap \beta$ 로 정의한 다음, 이것이 반드시  $\alpha$  또는  $\beta$ 와 같아야 함을 증명하는 것입니다.  $\square$

**정리 90.3.11 (순서수는 모든 순서 유형을 나타냅니다)**

$<$ 가 집합  $X$  위에서 정렬순서라고 합시다. 그러면 순서를 보존하는 전단사  $\alpha \rightarrow X$ 가 존재하는 유일한 순서수  $\alpha$ 가 존재합니다.

따라서 순서수는 순서형의 가능한 동치류를 나타냅니다. 정렬 집합이 주어질 때마다 그것은 유일한 순서수와 동형입니다.

이제 우리가 하던 “+1” 연산을 형식화합니다:

**정의 90.3.12.** 순서수  $\alpha$ 가 주어지면,  $\alpha + 1 = \alpha \cup \{\alpha\}$ 로 둡니다.  $\alpha + 1$  꼴의 순서수를 **후속 순서수**라고 부릅니다.

**정의 90.3.13.**  $\lambda$ 가 영도 아니고 후속 순서수도 아닌 순서수라면,  $\lambda$ 를 **극한 순서수**라고 부릅니다.

**예제 90.3.14 (후속 순서수와 극한 순서수)**

$7, \omega + 3, \omega \cdot 2 + 2015$ 는 후속 순서수이지만,  $\omega$ 와  $\omega \cdot 2$ 는 극한 순서수입니다.

**§90.4 순서수는 “높습니다”**

먼저, 다음을 주목합니다:

**정리 90.4.1 (모든 순서수의 집합은 존재하지 않습니다)**

$\mathcal{O}_n$ 은 고유 모임입니다.

증명. 모순을 가정하여 그렇지 않다고 합시다. 그러면  $O_n$ 은  $\in$ 에 의해 정렬되고 추이적이므로,  $O_n$ 은 순서수, 즉  $O_n \in O_n$ 이 되는데, 이는 Foundation을 위반합니다.  $\square$

**연습문제 90.4.2** (중요하지 않음).  $O_{n+1}$ 을 고려하여 Foundation 없이 증명을 제시하십시오.

이로부터 다음을 유도합니다:

**정리 90.4.3** (순서수 집합은 유계입니다)

$A \subseteq O_n$ 이라 합시다. 그러면  $A \subseteq \alpha$ 가 되는 어떤 순서수  $\alpha$ 가 존재합니다 (즉,  $A$ 는 유계여야 합니다).

증명. 그렇지 않다면,  $\bigcup A$ 를 살펴봅시다. 이것은 집합입니다. 그러나  $A$ 가 비유계라면 그것은  $O_n$ 과 같아야 하는데, 이는 모순입니다.  $\square$

이를 고려하여, 모든 순서수 집합은 최소 상계인 **상한**을 가집니다. 이것을  $\sup A$ 로 나타냅니다.

**질문 90.4.4.** 다음을 보이십시오

- (a) 임의의 순서수  $\alpha$ 에 대해  $\sup(\alpha + 1) = \alpha$ 입니다.
- (b) 임의의 극한 순서수  $\lambda$ 에 대해  $\sup \lambda = \lambda$ 입니다.

그림에서의 “높음”은 몇 절 뒤에 설명될 것입니다.

## §90.5 초한 귀납법과 초한 재귀법

$\in$ 에 무한 하강 사슬이 없다는 사실은 귀납법과 재귀법이 그대로 성립함을 의미합니다.

**정리 90.5.1** (초한 귀납법)

명제  $P(-)$ 가 주어졌을 때, 다음을 가정합시다

- $P(0)$ 이 참이고,
- 모든  $\alpha < \beta$ 에 대해  $P(\alpha)$ 가 참이면,  $P(\beta)$ 가 참입니다.

그러면  $P(\alpha)$ 는 모든 순서수  $\alpha$ 에 대해 참입니다.

**정리 90.5.2** (초한 재귀법)

모든 순서수  $\alpha$ 에 대해 수열  $x_\alpha$ 를 정의하려면, 다음으로 충분합니다.

- $x_0$ 을 정의하고, 그다음
- 임의의  $\beta$ 에 대해,  $\alpha < \beta$ 인 임의의  $\alpha$ 에 대한  $x_\alpha$ 만을 사용하여  $x_\beta$ 를 정의합니다.

이것이 일반적인 귀납법과 다른 점은 극한 순서수에 있습니다. 실생활에서는 그저 “ $x_{n+1} = \dots$ 을 정의한다”와 같은 일만 할 수도 있습니다. 하지만 이것만으로는 모든  $\alpha$ 에 대해  $x_\alpha$ 를 정의하기에 충분하지 않은데, 왜냐하면 이런 방식으로는  $\omega$ 에 도달할 수 없기 때문입니다. 마찬가지로, 단순히  $+1$ 을 하는 것으로는 모든  $n$ 에 대한  $\omega + n$ 을 이미 가지고 있더라도

순서수  $\omega \cdot 2$ 에 도달할 수 없습니다. 다시 말해, 단순히 1씩 증가시키는 것으로는 극한 단계를 넘어설 수 없지만, 초한 귀납법을 사용하여 위로 도약하면 이 문제를 우회할 수 있습니다.

그래서 초한 귀납법은 흔히 세 가지 경우로 나뉩니다. 귀납법 형식으로는 다음과 같습니다.

- (영 단계) 먼저,  $P(0)$ 을 해결합니다.
- (후속자 단계)  $P(\alpha)$ 로부터  $P(\alpha + 1)$ 을 얻을 수 있음을 보입니다.
- (극한 단계) 극한 순서수  $\lambda$ 에 대해, 모든  $\alpha < \lambda$ 에 대한  $P(\alpha)$ 가 주어졌을 때  $P(\lambda)$ 가 성립함을 보입니다.

마찬가지로, 초한 재귀법 또한 흔히 경우로 나뉩니다.

- (영 단계) 먼저,  $x_0$ 을 정의합니다.
- (후속자 단계)  $x_\alpha$ 로부터  $x_{\alpha+1}$ 을 정의합니다.
- (극한 단계)  $\lambda$ 가 극한 순서수일 때, 모든  $\alpha < \lambda$ 에 대한  $x_\alpha$ 로부터  $x_\lambda$ 를 정의합니다.

두 상황 모두에서, 유한 귀납법은 처음 두 경우만 다루지만, 세 번째 경우를 다룰 수 있다면 장벽  $\omega$  너머로 올라갈 수 있습니다.

## §90.6 순서수 산술

**이 절의 대표적인 예:**  $1 + \omega = \omega \neq \omega + 1$ .

초한 재귀법의 예를 들기 위해, 순서수의 덧셈을 정의해 봅시다. 우리가  $\alpha + 1 = \alpha \cup \{\alpha\}$ 로 정의했음을 상기하십시오. 초한 재귀법에 의해, 다음과 같이 둡니다.

$$\begin{aligned}\alpha + 0 &= \alpha \\ \alpha + (\beta + 1) &= (\alpha + \beta) + 1 \\ \alpha + \lambda &= \bigcup_{\beta < \lambda} (\alpha + \beta).\end{aligned}$$

여기서  $\lambda \neq 0$ 입니다.

우리는 이것을 명시적으로도 할 수 있습니다. 그림으로는 그저  $\alpha$ 를  $\beta$  앞에 나란히 놓는 것입니다. 즉, 다음 집합을 고려할 수 있습니다.

$$X = (\{0\} \times \alpha) \cup (\{1\} \times \beta)$$

(즉,  $\alpha$ 의 각 원소에는 0을 표시하고,  $\beta$ 의 각 원소에는 1을 표시합니다.) 그런 다음 사전식 순서  $<_{\text{lex}}$ (첫 번째 성분으로 정렬한 뒤, 두 번째 성분으로 정렬)에 의해  $X$ 에 정렬 순서를 부여합니다. 이 정렬 순서는 유일한 순서수와 동형입니다.

### 예제 90.6.1 ( $2 + 3 = 5$ )

$\alpha = 2$ 이고  $\beta = 3$ 일 때의 명시적 구성 아래에서, 우리는 다음 집합을 얻습니다.

$$X = \{(0, 0) < (0, 1) < (1, 0) < (1, 1) < (1, 2)\}$$

이는 5와 동형입니다.

**예제 90.6.2** (순서수 산술은 교환법칙이 성립하지 않습니다)

$1 + \omega = \omega$ 임에 주목하십시오! 실제로, 초한적 정의 아래에서 우리는 다음을 얻습니다.

$$1 + \omega = \bigcup_n (1 + n) = 1 \cup 2 \cup 3 \cup \dots = \omega.$$

명시적 구성으로는, 우리는 다음을 얻습니다.

$$X = \{(0, 0) < (1, 0) < (1, 1) < (1, 2) < \dots\}$$

$\omega$ 와 동형인 것입니다.

**연습문제 90.6.3.** 모든  $n \in \omega$ 에 대해  $n + \omega = \omega$ 임을 보이십시오.

**비고 90.6.4** — 순서수 덧셈은 교환적이지 않습니다. 그러나 명시적 구성으로부터 적어도 결합적이라는 것을 알 수 있습니다.

더 나아가, 충분히 작은  $\alpha \neq 0$ 에 대해서는  $\alpha + \beta = \beta$ 가 성립할 수 있음을 알 수 있습니다. 그러나 반대쪽에서는 이런 일이 일어나지 않습니다 —  $\beta < \gamma$ 이면  $\alpha + \beta < \alpha + \gamma$ 입니다.

마찬가지로, 곱셈도 두 가지 방식으로 정의할 수 있습니다. 초한 귀납법으로는:

$$\begin{aligned}\alpha \cdot 0 &= 0 \\ \alpha \cdot (\beta + 1) &= (\alpha \cdot \beta) + \alpha \\ \alpha \cdot \lambda &= \bigcup_{\beta < \lambda} \alpha \cdot \beta.\end{aligned}$$

명시적 구성도 할 수 있습니다: 이번에는  $\beta$ 개의 사본을 나란히 늘어놓되, 각 사본이  $\alpha$ 개의 항목을 담는 그림입니다. 즉,  $\alpha \cdot \beta$ 는 다음의 순서형입니다

$$<_{\text{lex}} \text{에 적용된 } \beta \times \alpha.$$

**예제 90.6.5** (순서수 곱셈은 교환적이지 않습니다)

$\omega \cdot 2 = \omega + \omega$ 이지만,  $2 \cdot \omega = \omega$ 입니다.

**연습문제 90.6.6.** 이를 증명하십시오.

**연습문제 90.6.7.** 순서수 곱셈이 (덧셈과 마찬가지로) 결합적이지만 교환적이지 않음을 확인하십시오. ( $\gamma \times \beta \times \alpha$ 를 살펴보세요.)

순서수 덧셈과 마찬가지로,  $\alpha \cdot (\beta + 1) = (\alpha \cdot \beta) + \alpha$ 로 정의하면  $\beta < \gamma$ 일 때  $\alpha \cdot \beta < \alpha \cdot \gamma$ 가 성립함이 보장됩니다 —  $\alpha > 0$ .

거듭제곱도 이와 같이 정의할 수 있지만, 명시적 구성은 덜 자연스럽습니다 — 이 책의 나머지 부분에서는 이 정의를 사용하지 않으므로 무시하셔도 됩니다.

$\alpha = 0$ 에 대해서는  $0^0 = 1$ 로, 모든  $\beta > 0$ 에 대해  $0^\beta = 0$ 으로 정의합니다. 그 외의 경우

에는:

$$\begin{aligned}\alpha^0 &= 1 \\ \alpha^{\beta+1} &= \alpha^\beta \cdot \alpha \\ \alpha^\lambda &= \bigcup_{\beta < \lambda} \alpha^\beta.\end{aligned}$$

**연습문제 90.6.8.**  $2^\omega = \omega$ 임을 확인하십시오.

## §90.7 집합의 계층

이제 초한 재귀법으로 **폰 노이만 계층**을 정의합니다.

**정의 90.7.1.** 초한 재귀법에 의해, 다음과 같이 설정합니다

$$\begin{aligned}V_0 &= \emptyset \\ V_{\alpha+1} &= \mathcal{P}(V_\alpha) \\ V_\lambda &= \bigcup_{\alpha < \lambda} V_\alpha\end{aligned}$$

초한 귀납법에 의해,  $V_\alpha$ 가 추이적이며 모든  $\alpha < \beta$ 에 대해  $V_\alpha \subseteq V_\beta$ 임을 알 수 있습니다.

**예제 90.7.2** ( $\alpha \leq 3$ 일 때의  $V_\alpha$ )

이 계층의 처음 몇 단계는 다음과 같습니다

$$\begin{aligned}V_0 &= \emptyset \\ V_1 &= \{0\} \\ V_2 &= \{0, 1\} \\ V_3 &= \{0, 1, 2, \{1\}\}.\end{aligned}$$

각  $n$ 에 대해  $V_n$ 은 오직 유한 집합들로만 이루어져 있으며, 각  $n$ 은  $V_{n+1}$ 에서 처음으로 나타난다는 것에 주목하십시오. 다음을 관찰하십시오

$$V_\omega = \bigcup_{n \in \omega} V_n$$

오직 유한 집합들로만 이루어져 있습니다; 따라서  $\omega$ 는  $V_{\omega+1}$ 에서 처음으로 나타납니다.

**질문 90.7.3.**  $V_5$ 에는 몇 개의 집합이 있습니까?

**정의 90.7.4.** 집합  $y$ 의 **계수**(rank)는  $\text{rank}(y)$ 로 표기하며,  $y \in V_{\alpha+1}$ 을 만족하는 가장 작은 순서수  $\alpha$ 입니다.

**예제 90.7.5**

$\text{rank}(2) = 2$ 이며, 실제로 임의의 순서수  $\alpha$ 에 대해  $\text{rank}(\alpha) = \alpha$ 입니다(문제는 나중에). 이것이 여러분의 “+1”이 붙는 이유입니다.

**질문 90.7.6.**  $\text{rank}(y)$ 가  $y \subseteq V_\alpha$ 를 만족하는 가장 작은 순서수  $\alpha$ 임을 보이십시오.

집합의 계수가 실제로 존재하는지는 아직 명확하지 않으므로, 이를 증명합니다:

**정리 90.7.7 (폰 노이만 계층은 완전합니다)**

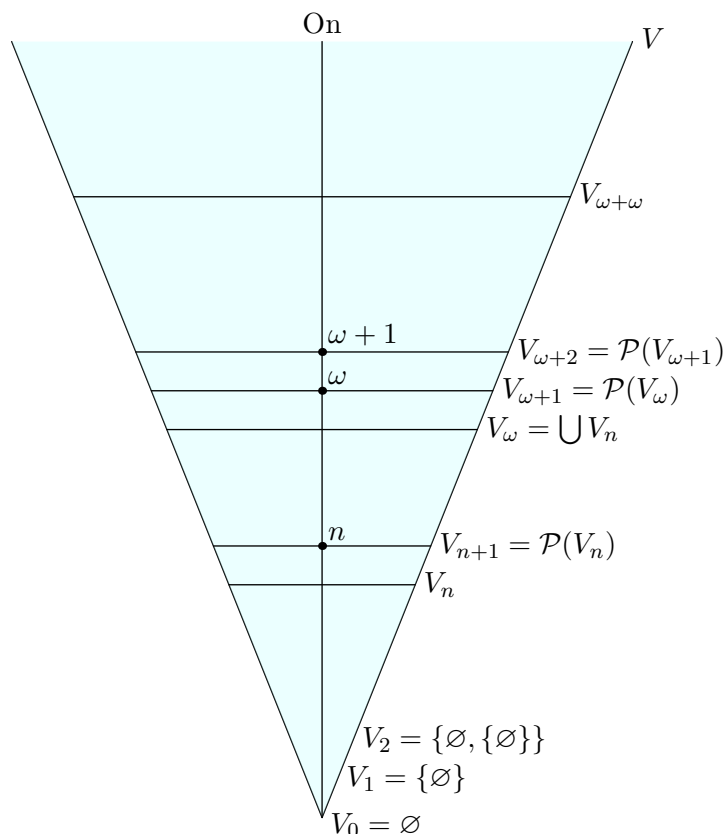
클래스  $V$ 는  $\bigcup_{\alpha \in \text{On}} V_\alpha$ 와 같습니다. 다시 말해, 모든 집합은 어떤  $V_\alpha$ 에 나타납니다.

증명. 귀류법으로 이것이 거짓이라고 가정합니다. 핵심은  $\in$ 가 Foundation을 만족하므로,  $\in$ -극소 반례  $x$ 를 취할 수 있다는 것입니다. 따라서  $\text{rank}(y)$ 는 모든  $y \in x$ 에 대해 정의되며, (Replacement에 의해) 다음 집합을 생각할 수 있습니다

$$\{\text{rank}(y) \mid y \in x\}.$$

이것은 순서수들의 집합이므로 유계입니다. 따라서 모든  $y \in x$ 에 대해  $y \in V_\alpha$ 가 되는 어떤 큰 순서수  $\alpha$ 가 존재하며, 즉  $x \subseteq V_\alpha$ 이므로  $x \in V_{\alpha+1}$ 입니다.  $\square$

이는 우주  $V$ 에 대한 다음과 같은 그림으로 우리를 이끕니다:



우주  $V$ 를,  $V_0 \subsetneq V_1 \subsetneq V_2 \subsetneq \dots$ 와 같이 여러 단계 또는 층으로 이루어진 삼각형으로 상상할 수 있습니다. 이 우주는 꼭대기가 없지만, 각  $V_i$ 는 꼭대기를 가집니다. 그러나 이 우주는 매우 명확한 바닥을 가집니다. 각 단계는 이전 단계보다 상당히 넓습니다.

이 우주의 중심에는 순서수들이 있습니다: 모든 후행자  $V_{\alpha+1}$ 마다 정확히 하나의 새로운 순서수, 즉  $\alpha$ 가 나타납니다. 따라서 순서수의 클래스를 우주의 전체 높이에 걸쳐 뻗어 있는 얇은 선으로 그릴 수 있습니다. 어떤 집합이 순서수  $\alpha$ 와 같은 단계에 나타나면 그 집합은 계수  $\alpha$ 를 가집니다.

정수의 연구인 정수론 전체는  $V_\omega$  안에 존재합니다. 실수의 연구인 실해석학은  $V_{\omega+1}$  안에 존재하는데, 이는 실수가 (이진 전개를 통해)  $\mathbb{N}$ 의 부분집합으로 부호화될 수 있기 때문입니다. 함수해석학은 그보다 한 단계 더 나아간  $V_{\omega+2}$ 에 존재합니다. 실질적으로 대부분의 수학은  $V_{\omega+\omega}$ 를 넘어서지 않습니다. 이는 우주 전체의 진정한 규모에 비하면 보잘것없습니다.

## §90.8 생각해 볼 만한 조금 더 어려운 문제

**문제 90A.** 초한 귀납법을 사용하여 임의의  $\alpha$ 에 대해  $\text{rank}(\alpha) = \alpha$ 임을 증명하십시오.

**문제 90B** (Online Math Open).  $V_5$ 에 있는 추이적 집합의 개수를 세십시오.

**문제 90C** (Goodstein).  $a_2$ 를 임의의 양의 정수라 합시다. 다음과 같이 무한 수열  $a_2, a_3, \dots$ 을 재귀적으로 정의합니다. 만약  $a_n = 0$ 이면,  $a_{n+1} = 0$ 입니다. 그렇지 않으면,  $a_n$ 을 밑  $n$ 으로 쓰고, 모든 지수도 밑  $n$ 으로 쓰며, 식에 있는 모든 수가  $n$  이하가 될 때까지 이 과정을 계속합니다. 그런 다음  $n$ 을(지수를 포함하여!) 모두  $n+1$ 로 바꾸고, 1을 빼서 그 결과를  $a_{n+1}$ 로 둡니다. 예를 들어  $a_2 = 11$ 이면 다음과 같습니다

$$a_2 = 2^3 + 2 + 1 = 2^{2+1} + 2 + 1$$

$$a_3 = 3^{3+1} + 3 + 1 - 1 = 3^{3+1} + 3$$

$$a_4 = 4^{4+1} + 4 - 1 = 4^{4+1} + 3$$

$$a_5 = 5^{5+1} + 3 - 1 = 5^{5+1} + 2$$

등등입니다. 어떤 정수  $N > 2$ 에 대해  $a_N = 0$ 임을 증명하십시오.



# 91 기수

순서수는 전순서를 측정합니다. 그러나 크기를 측정하는 데는 그다지 훌륭한 역할을 하지 못합니다. 예를 들어,  $\omega$ 와  $\omega + 1$ 의 원소들 사이에는 전단사가 존재합니다:

$$\begin{aligned}\omega + 1 &= \{ \omega \ 0 \ 1 \ 2 \ \dots \} \\ \omega &= \{ \ 0 \ 1 \ 2 \ 3 \ \dots \}.\end{aligned}$$

실제로, 여러분이 아마 이미 알고 있듯이,  $\omega$ 와  $\omega^2$  사이에도 전단사가 존재합니다:

| +                | 0  | 1   | 2   | 3   | 4   | ... |
|------------------|----|-----|-----|-----|-----|-----|
| 0                | 0  | 1   | 3   | 6   | 10  | ... |
| $\omega$         | 2  | 4   | 7   | 11  | ... |     |
| $\omega \cdot 2$ | 5  | 8   | 12  | ... |     |     |
| $\omega \cdot 3$ | 9  | 13  | ... |     |     |     |
| $\omega \cdot 4$ | 14 | ... |     |     |     |     |

따라서 순서수는 크기를 추적하는 데 좋은 역할을 하지 못합니다. 이를 위해 기수라는 개념으로 눈을 돌립니다.

## §91.1 등수인 집합과 기수

**정의 91.1.1.** 두 집합  $A$ 와  $B$ 가 그 사이에 전단사가 존재하면 **등수**라고 하며,  $A \approx B$ 로 표기합니다.

**정의 91.1.2.** **기수**란  $\alpha < \kappa$ 인 어떤  $\alpha$ 에 대해서도  $\alpha \approx \kappa$ 가 성립하지 않는 순서수  $\kappa$ 입니다.

### 예제 91.1.3 (기수의 예)

모든 유한한 수는 기수입니다. 또한,  $\omega$ 도 기수입니다. 그러나  $\omega + 1$ ,  $\omega^2$ ,  $\omega^{2015}$ 는 가산이므로 기수가 아닙니다.

### 예제 91.1.4 ( $\omega^\omega$ 는 가산입니다)

$\omega^\omega$ 조차도 가산 합집합이므로 기수가 아닙니다

$$\omega^\omega = \bigcup_n \omega^n$$

그리고 각  $\omega^n$ 은 가산입니다.

**질문 91.1.5.** 왜 무한 기수는 극한 순서수여야 하는가?

**비고 91.1.6** — 기수의 정의에는 미심쩍은 부분이 있습니다: 이는 외부 함수  $f$ 에 의존한다는 점입니다. 즉,  $\kappa$ 가 기수임을 확인하려면  $\kappa$  자체만 보아서 안 되며,  $\alpha < \kappa$ 인  $\alpha$ 에 대해 전단사  $f: \kappa \rightarrow \alpha$ 가 존재하지 않음을 확인하기 위해 전체 우주  $V$ 를 살펴

보아야 합니다. 지금은 이것이 문제가 되지 않지만, 나중에 모형 이론에서 이는 매우 직관에 반하는 현상으로 이어질 것입니다.

## §91.2 기수성

이제 기수를 정의했으므로, 집합을 기수와 연결지어 그 크기를 논할 수 있습니다.

**정의 91.2.1.** 집합  $X$ 의 **기수성**이란  $X \approx \kappa$ 가 성립하는 가장 작은 순서수  $\kappa$ 입니다. 이를  $|X|$ 로 표기합니다.

**질문 91.2.2.** 왜  $|X|$ 는 기수여야 하는가?

**비고 91.2.3** — 그러한 순서수  $\kappa$ 가 실제로 존재함을 확립하려면 정렬 정리(동치적으로, 선택 공리)가 필요합니다.

기수는 순서수이므로,  $\kappa_1 \leq \kappa_2$ 인지 묻는 것이 타당합니다. 여기서는 우리의 일반적인 직관이 잘 작동합니다.

### 명제 91.2.4 (농도 성질의 재서술)

$X$ 와  $Y$ 를 집합이라 합시다.

- (i)  $X \approx Y$ 인 것은  $|X| = |Y|$ 인 것과 동치이며, 이는  $X$ 에서  $Y$ 로의 전단사가 존재하는 것과 동치입니다.
- (ii)  $|X| \leq |Y|$ 인 것은 단사 사상  $X \hookrightarrow Y$ 가 존재하는 것과 동치입니다.

부지런한 독자들은 이를 직접 증명해 보시기 바랍니다.

## §91.3 알레프 수

**이 절의 대표적인 예:**  $\aleph_0 = \omega$ 이며,  $\aleph_1$ 은 첫 번째 비가산 순서수입니다.

먼저, 기수가 임의로 커질 수 있음을 확인해 봅시다:

### 명제 91.3.1

모든 집합  $X$ 에 대해  $|X| < |\mathcal{P}(X)|$ 입니다.

증명. 단사 사상  $X \hookrightarrow \mathcal{P}(X)$ 는 존재하지만, **보조정리 89.2.1**에 의해 단사 사상  $\mathcal{P}(X) \hookrightarrow X$ 는 존재하지 않습니다.  $\square$

따라서 다음과 같이 정의할 수 있습니다:

**정의 91.3.2.** 기수  $\kappa$ 에 대해,  $\kappa^+$ 를  $\kappa$ 보다 큰 가장 작은 기수로 정의하며, 이를 **후속 기수**라 부릅니다.

이  $\kappa^+$ 는 존재하며  $\kappa^+ \leq |\mathcal{P}(\kappa)|$ 를 만족합니다.

다음으로, 다음을 주장합니다:

**연습문제 91.3.3.**  $A$ 가 기수들의 집합이면  $\cup A$ 가 기수임을 보이십시오.

따라서 초한 귀납법에 의해 다음을 연습니다:

**정의 91.3.4.** 임의의  $\alpha \in \text{On}$ 에 대해, **알레프 수**를 다음과 같이 정의합니다

$$\begin{aligned}\aleph_0 &= \omega \\ \aleph_{\alpha+1} &= (\aleph_\alpha)^+ \\ \aleph_\lambda &= \bigcup_{\alpha < \lambda} \aleph_\alpha.\end{aligned}$$

따라서 다음과 같은 기수들의 수열을 연습니다

$$0 < 1 < 2 < \dots < \aleph_0 < \aleph_1 < \dots < \aleph_\omega < \aleph_{\omega+1} < \dots$$

정의에 의해,  $\aleph_0$ 은 자연수의 기수이고,  $\aleph_1$ 은 첫 번째 비가산 순서수이며, ...입니다. 알레프 수가 모든 기수를 이룬다는 것을 주장합니다:

**보조정리 91.3.5** (알레프 수는 모든 무한 기수를 이룹니다)

$\kappa$ 가 기수이면,  $\kappa$ 는 유한(즉,  $\kappa \in \omega$ )이거나, 어떤  $\alpha \in \text{On}$ 에 대해  $\kappa = \aleph_\alpha$ 입니다.

증명.  $\kappa$ 가 무한이라 가정하고,  $\aleph_\alpha \geq \kappa$ 를 만족하는 최소의  $\alpha$ 를 취합니다. 모순을 이끌기 위해  $\aleph_\alpha > \kappa$ 라고 가정합니다.  $\alpha = 0$ 인 경우는 자명하므로,  $\alpha > 0$ 이라 가정할 수 있습니다.  $\alpha = \bar{\alpha} + 1$ 이 후속 순서수이면, 다음이 성립합니다

$$\aleph_{\bar{\alpha}} < \kappa < \aleph_\alpha = (\aleph_{\bar{\alpha}})^+$$

이는 후속 기수의 정의에 모순됩니다.

$\alpha = \lambda$ 가 극한 순서수이면,  $\aleph_\lambda$ 는 상한  $\bigcup_{\gamma < \lambda} \aleph_\gamma$ 입니다. 따라서  $\aleph_\gamma > \kappa$ 를 만족하는 어떤  $\gamma < \lambda$ 가 존재해야 하며, 이는  $\alpha$ 의 최소성에 모순됩니다.  $\square$

**정의 91.3.6.** 후속 기수가 아닌 무한 기수를 **극한 기수**라 부릅니다. 이는 정확히  $\lambda$ 가 극한 순서수일 때  $\aleph_\lambda$  형태의 기수들과  $\aleph_0$ 입니다.

## §91.4 기수 산술

**이 절의 대표적인 예:**  $\aleph_0 \cdot \aleph_0 = \aleph_0 + \aleph_0 = \aleph_0$

순서수 산술을 설정했던 방식을 떠올려 봅시다. 특히  $\omega + \omega > \omega$ 이고  $\omega^2 > \omega$ 임에 유의하십시오. 기수는 크기를 세는 것이므로 이러한 성질은 바람직하지 않으며, 우리는 다음이 성립하기를 원합니다

$$\begin{aligned}\aleph_0 + \aleph_0 &= \aleph_0 \\ \aleph_0 \cdot \aleph_0 &= \aleph_0\end{aligned}$$

$\omega + \omega$ 와  $\omega \cdot \omega$ 는 가산이기 때문입니다. 기수의 경우, 우리는 단순히 “순서를 무시합니다”. 기수 산술의 정의는 예상대로입니다:

**정의 91.4.1** (기수 산술). 기수  $\kappa$ 와  $\mu$ 가 주어졌을 때, 다음과 같이 정의합니다

$$\kappa + \mu := |(\{0\} \times \kappa) \cup (\{1\} \times \mu)|$$

그리고

$$\kappa \cdot \mu := |\mu \times \kappa|.$$

**질문 91.4.2.** 이것이 유한 기수에 대해 여러분이 유치원에서 배운 것과 일치하는지 확인하십시오.

**표기의 남용 91.4.3.** 우리가 서수 산술과 같은 기호를 사용하고 있지만 결과는 다르기 때문에( $\omega \cdot \omega = \omega^2$ 이지만  $\aleph_0 \cdot \aleph_0 = \aleph_0$ 입니다) 이는 표기법의 약간의 남용입니다. 일반적으로, 제가 기수 산술에 대해 이야기하는지 서수 산술에 대해 이야기하는지 확실히 밝히도록 하겠습니다.

이러한 혼동을 막기 위해, 우리는 서수와 기수에 대해 서로 다른 기호를 사용합니다. 구체적으로,  $\omega$ 는 항상 서수로 간주된  $\{0, 1, \dots\}$ 를 가리키며,  $\aleph_0$ 는 항상 기수로 간주된 같은 집합을 가리킵니다. 더 일반적으로,

**정의 91.4.4.**  $\omega_\alpha = \aleph_\alpha$ 를 순서수로 본 것이라 합시다.

하지만 우리가 이미 본 바와 같이  $\aleph_0 \cdot \aleph_0 = \aleph_0$ 입니다. 사실, 이는 훨씬 더 일반적으로 성립합니다:

**정리 91.4.5 (무한 기수의 제곱)**

$\kappa$ 를 무한 기수라고 합시다. 그러면  $\kappa \cdot \kappa = \kappa$ 입니다.

**증명.** 명백히  $\kappa \cdot \kappa \geq \kappa$ 이므로, 우리는  $\kappa \cdot \kappa \leq \kappa$ 임을 보이려고 합니다.

아이디어는  $\aleph_0 \cdot \aleph_0 = \aleph_0$ 에 대해 우리가 가졌던 것과 같은 증명을 반복해 보는 것이므로, 여기서 다시 언급합니다. 우리는  $\aleph_0$ 의 원소들의 “제곱”을 취한 다음, 대각선에 따라 재정렬했습니다:

|   | 0  | 1   | 2   | 3   | 4   | ... |
|---|----|-----|-----|-----|-----|-----|
| 0 | 0  | 1   | 3   | 6   | 10  | ... |
| 1 | 2  | 4   | 7   | 11  | ... |     |
| 2 | 5  | 8   | 12  | ... |     |     |
| 3 | 9  | 13  | ... |     |     |     |
| 4 | 14 | ... |     |     |     |     |

일반적인  $\kappa$ 에 대해서도 이 아이디어를 그대로 사용하고 싶습니다. 그러나 무한 서수에 대해서는 덧셈이 잘 작동하지 않으므로  $\alpha + \beta$  대신  $\max\{\alpha, \beta\}$ 를 사용하는 것이 더 편리할 것입니다. 구체적으로, 우리는  $\kappa \times \kappa$  위에 다음과 같이 순서 <최대값>를 둡니다:  $\kappa \times \kappa$ 의  $(\alpha_1, \beta_1)$ 과  $(\alpha_2, \beta_2)$ 에 대해, 다음이 성립하면  $(\alpha_1, \beta_1) <_{\text{최대값}} (\alpha_2, \beta_2)$ 라고 선언합니다

- $\max\{\alpha_1, \beta_1\} < \max\{\alpha_2, \beta_2\}$ 이거나
- $\max\{\alpha_1, \beta_1\} = \max\{\alpha_2, \beta_2\}$ 이고  $(\alpha_1, \beta_1)$ 이 사전식으로  $(\alpha_2, \beta_2)$ 보다 앞섭니다.

이 대체 순서(의도적으로 덧셈을 언급하지 않는)는 다음과 같은 모습입니다:

|   | 0  | 1  | 2  | 3  | 4  | ... |
|---|----|----|----|----|----|-----|
| 0 | 0  | 1  | 4  | 9  | 16 | ... |
| 1 | 2  | 3  | 5  | 10 | 17 | ... |
| 2 | 6  | 7  | 8  | 11 | 18 | ... |
| 3 | 12 | 13 | 14 | 15 | 19 | ... |
| 4 | 20 | 21 | 22 | 23 | 24 | ... |
| ⋮ | ⋮  | ⋮  | ⋮  | ⋮  | ⋮  | ⋮   |

이제 우리는  $\kappa$ 에 대한 초한 귀납법으로 진행합니다. 기저 경우는  $\kappa = \aleph_0$ 이며, 위에서 완료했습니다. 이제,  $<_{\text{최대값}}$ 는  $\kappa \times \kappa$ 의 정렬 순서이므로, 이것이 어떤 서수  $\gamma$ 와 순서를 보

존하는 전단사 관계에 있음을 알 수 있습니다. 우리의 목표는  $|\gamma| \leq \kappa$ 임을 보이는 것입니다. 이를 위해서는, 임의의  $\bar{\gamma} \in \gamma$ 에 대해  $|\bar{\gamma}| < \kappa$ 임을 증명하는 것으로 충분합니다.

이 전단사 관계 아래에서  $\bar{\gamma}$ 가 점  $(\alpha, \beta) \in \kappa \times \kappa$ 에 대응한다고 합시다.  $\alpha$ 와  $\beta$ 가 둘 다 유한하면 확실히  $\bar{\gamma}$ 도 유한합니다. 그렇지 않으면,  $\bar{\kappa} = \max\{\alpha, \beta\} < \kappa$ 라고 합시다. 그러면  $\bar{\gamma}$  아래에 있는 점들의 개수는 최대

$$|\alpha| \cdot |\beta| \leq \bar{\kappa} \cdot \bar{\kappa} = \bar{\kappa}$$

귀납 가설에 의해 다음과 같습니다. 따라서 원하는 대로  $|\bar{\gamma}| \leq \bar{\kappa} < \kappa$ 입니다.  $\square$

이로부터 기수의 덧셈과 곱셈이 정말로 지루하다는 것이 따라 나옵니다:

#### 정리 91.4.6 (무한 기수 산술은 자명합니다)

기수  $\kappa$ 와  $\mu$ 가 주어졌고 그중 하나가 무한하다면, 우리는 다음을 얻습니다

$$\kappa \cdot \mu = \kappa + \mu = \max\{\kappa, \mu\}.$$

증명. 요점은 이 두 값이 모두 최댓값의 제곱보다 작다는 것입니다. 세부 사항을 적어보면:

$$\begin{aligned} \max\{\kappa, \mu\} &\leq \kappa + \mu \\ &\leq \kappa \cdot \mu \\ &\leq \max\{\kappa, \mu\} \cdot \max\{\kappa, \mu\} \\ &= \max\{\kappa, \mu\}. \end{aligned} \quad \square$$

## §91.5 기수 지수 연산

이 절의 대표적인 예:  $2^\kappa = |\mathcal{P}(\kappa)|$ .

정의 91.5.1.  $\kappa$ 와  $\lambda$ 가 기수라고 합시다. 그러면

$$\kappa^\lambda := |\mathcal{F}(\lambda, \kappa)|.$$

여기서  $\mathcal{F}(A, B)$ 는  $A$ 에서  $B$ 로 가는 함수들의 집합입니다.

표기의 남용 91.5.2. 앞서와 마찬가지로, 기수 연산과 순서수 연산 모두에 같은 표기법을 사용하고 있습니다. 죄송합니다!

특히  $2^\kappa = |\mathcal{P}(\kappa)| > \kappa$ 이므로, 이제부터는 표기법  $2^\kappa$ 를 자유롭게 사용할 수 있습니다. (이는 순서수 연산과는 완전히 다르다는 점에 유의하십시오. 순서수 연산에서는  $2^\omega = \bigcup_{n \in \omega} 2^n = \omega$ 였습니다. 기수 연산에서는  $2^{\aleph_0} > \aleph_0$ 입니다.)

안타깝게도  $2^{\aleph_0}$ 이 무엇과 같은지는 아직 말씀드리지 않았습니다. 자연스러운 추측은  $2^{\aleph_0} = \aleph_1$ 이라는 것이며, 이를 **연속체 가설**이라고 부릅니다. 이는 결정 불가능한 것으로 밝혀졌습니다 – 즉 ZFC 공리로부터 이를 증명하거나 반증하는 것이 불가능합니다.

## §91.6 공종성

이 절의 대표적인 예:  $\aleph_0, \aleph_1, \dots$  은 모두 정칙적이지만,  $\aleph_\omega$ 는 공종성이  $\omega$ 입니다.

정의 91.6.1.  $\lambda$ 를 순서수(보통 극한 순서수)라 하고,  $\alpha$ 를 또 다른 순서수라 합시다. 순서수 사이의 사상  $f: \alpha \rightarrow \lambda$ 가 모든  $\bar{\alpha} < \alpha$ 에 대해  $f(\bar{\alpha}) \leq \bar{\alpha}$ 를 만족하는 어떤  $\bar{\alpha} \in \alpha$ 가 존재할 때, 이를 **공종**이라고 부릅니다. 다시 말해, 이 사상은  $\lambda$  안에서 임의로 높이 도달합니다.

**예제 91.6.2** (공종 사상의 예)

- (a)  $n \mapsto \omega^n$ 으로 정의되는 사상  $\omega \rightarrow \omega^\omega$ 는 공종적입니다.
- (b) 임의의 순서수  $\alpha$ 에 대해, 항등 사상  $\alpha \rightarrow \alpha$ 는 공종적입니다.

**정의 91.6.3.**  $\lambda$ 를 극한 순서수라 합시다.  $\lambda$ 의 **공종성**은  $\text{cof}(\lambda)$ 로 표기하며, 공종 사상  $\alpha \rightarrow \lambda$ 가 존재하는 가장 작은 순서수  $\alpha$ 입니다.

**질문 91.6.4.** 왜  $\alpha$ 는 반드시 무한 기수여야 합니까?

보통 우리는 기수  $\kappa$ 의 공종성을 구하는 데 관심이 있습니다.

그림으로 표현하자면, 우주의 밑바닥에 서서 순서수의 사슬을 따라  $\kappa$ 까지 올라다본다고 상상할 수 있습니다. 여러분에게는 기관총이 있고 위쪽으로 총알을 쏘고 있으며, 임의로 높이 도달하되  $\kappa$ 보다는 작게 도달하고자 합니다. 공종성은 바로 이를 위해 필요한 총알의 개수입니다.

이제 "대부분"의 경우 기수의 공종성은 자기 자신임을 관찰합니다.<sup>1</sup> 이러한 기수를 **정칙**이라고 부릅니다.

**예제 91.6.5** ( $\aleph_0$ 은 정칙적입니다)

$\text{cof}(\aleph_0) = \aleph_0$ 인데, 이는  $\aleph_0 = \omega$ 의 어떤 유한 부분집합도 임의로 높이 도달할 수 없기 때문입니다.

**예제 91.6.6** ( $\aleph_1$ 은 정칙적입니다)

$\text{cof}(\aleph_1) = \aleph_1$ 입니다. 실제로 어떤 가산 순서수 집합  $A = \{\alpha_0, \alpha_1, \dots\} \subseteq \aleph_1$ 이  $\aleph_1$  내부에서 임의로 높이 도달한다고 가정하고 모순을 이끌어내 봅시다. 그러면  $\Lambda = \cup A$ 는 가산 순서수인데, 이는 가산 개의 가산 순서수들의 합집합이기 때문입니다. 다시 말해  $\Lambda \in \aleph_1$ 입니다. 그러나  $\Lambda$ 는  $A$ 의 상계이므로, 모순입니다.

반면, 정칙적이지 않은 기수도 존재합니다. 이들은 "드문" 경우이므로 **특이**라고 부릅니다.

**예제 91.6.7** ( $\aleph_\omega$ 는 정칙적이지 않습니다)

$\aleph_0 < \aleph_1 < \aleph_2 < \dots$ 가  $\aleph_0$ 개의 항만 가지고 있음에도 불구하고  $\aleph_\omega$  안에서 임의로 높은 곳까지 도달함을 주목하십시오. 따라서  $\text{cof}(\aleph_\omega) = \aleph_0$ 이 성립합니다.

이제 여러분이 품고 있었을지 모를 의심을 확인해 보겠습니다:

**정리 91.6.8** (후속 기수는 정칙이다)

$\kappa = \kappa^+$ 가 후속 기수이면, 이는 정칙입니다.

**증명.**  $\aleph_1$ 이 정칙임을 보인 증명을 그대로 따라 하겠습니다.

어떤  $\mu \leq \kappa$ 에 대해, 기수로서  $\kappa$  안에서 임의로 높은 곳까지 도달하는  $\mu$ 개의 집합이 존재

<sup>1</sup>주의하십시오 — 순서수의 공종성은 보통 자기 자신보다 엄밀하게 작습니다. 실제로 어떤 순서수의 공종성이 자기 자신이라면, 그 순서수는 반드시 기수여야 합니다.

한다고 가정하고 모순을 이끌어내겠습니다. 이 집합들 각각은 농도가 많아야  $\bar{\kappa}$ 여야 함을 주목하십시오. 이  $\mu$ 개 집합 전체의 합집합을 취하면, 상한 역할을 하는 순서수  $\Lambda$ 를 얻습니다. 이 합집합의 원소의 개수는 많아야

$$\# \text{집합} \cdot \# \text{원소} \leq \mu \cdot \bar{\kappa} = \bar{\kappa}$$

따라서  $|\Lambda| \leq \bar{\kappa} < \kappa$ 입니다. □

## §91.7 비가측 기수

그렇다면 극한 기수는 어떻습니까? 이들 대부분은 특이 기수인 것으로 보입니다: 만약  $\aleph_\lambda \neq \aleph_0$ 가 극한 기수라면(즉  $\lambda$ 가 극한 순서수라면), 길이가  $\lambda$ 인 수열  $\{\aleph_\alpha\}_{\alpha \in \lambda}$ 는 분명히 공종적입니다.

### 예제 91.7.1 (알레프 부동점)

다음의 거대한 기수를 생각해 봅시다

$$\kappa = \aleph_{\aleph_{\aleph_{\ddots}}}$$

$\kappa = \aleph_\kappa$ 이므로 이는 무섭도록 거대해 보일 수 있지만, 다음 수열의 극한이므로 그 공종도는  $\omega$ 입니다

$$\aleph_0, \aleph_{\aleph_0}, \aleph_{\aleph_{\aleph_0}}, \dots$$

더 일반적으로, 실제로 다음을 증명할 수 있습니다

$$\text{cof}(\aleph_\lambda) = \text{cof}(\lambda).$$

하지만  $\lambda$ 가 너무나 커서  $\lambda = \aleph_\lambda$ 가 되는 것도 실제로 가능합니다.

$\aleph_0$ 이 아닌 정칙 극한 기수에는 특별한 이름이 있습니다: 이를 **약비가측**이라 합니다. 이러한 기수는 너무나 거대하여 ZFC 안에서 그 존재성을 증명하거나 반증하는 것이 불가능합니다. 이것이 이른바 "큰 기수"라 불리는 것들 중 최초의 예입니다.

무한 기수  $\kappa$ 가 다음을 만족하면 이를 **강극한 기수**라 합니다

$$\forall \bar{\kappa} < \kappa \quad 2^{\bar{\kappa}} < \kappa$$

임의의 기수  $\bar{\kappa}$ 에 대해. 예를 들어,  $\aleph_0$ 은 강극한 기수입니다.

**질문 91.7.2.** 강극한 기수가 실제로 극한 기수여야 하는 이유는 무엇입니까? (이는 알미울 정도로 쉽습니다.)

**비고 91.7.3** — 극한 기수는 다음을 만족하는 영이 아닌 기수  $\kappa$ 로 동치하게 정의할 수 있습니다

$$\forall \bar{\kappa} < \kappa \quad (\bar{\kappa})^+ < \kappa.$$

이를 강극한 기수의 정의와 비교해 보면 그 유사성을 알 수 있습니다. (이 언급은 앞선 질문에 대한 답도 함께 제공합니다.)

$\aleph_0$ 이 아닌 정칙 강극한 기수를 **강비가측**이라 합니다.

## §91.8 생각해 볼 만한 조금 더 어려운 문제

문제 91A.  $|V_\omega|$ 를 계산하십시오.

문제 91B. 임의의 극한 순서수  $\alpha$ 에 대해  $\text{cof}(\alpha)$ 가 정칙 기수임을 증명하십시오.

문제 91C\* (강접근불가능 기수). 임의의 강접근불가능 기수  $\kappa$ 에 대해  $|V_\kappa| = \kappa$ 임을 보이십시오.

문제 91D (콰니히의 정리). 모든 무한 기수  $\kappa$ 에 대해

$$\kappa^{\text{cof}(\kappa)} > \kappa$$

임을 보이십시오.

# XXII

## 집합론 II: 모형 이론과 강제법

## 제XXII부: 목차

---

|           |                                |            |
|-----------|--------------------------------|------------|
| <b>92</b> | <b>내부 모형 이론</b>                | <b>963</b> |
| 92.1      | 모형 . . . . .                   | 963        |
| 92.2      | 문장과 만족 . . . . .               | 964        |
| 92.3      | 레비 계층 . . . . .                | 966        |
| 92.4      | 부분구조와 타르스키-보트 정리 . . . . .     | 967        |
| 92.5      | ZFC의 공리 얻기 . . . . .           | 968        |
| 92.6      | Mostowski 붕괴 . . . . .         | 969        |
| 92.7      | 비가측 기수 추가하기 . . . . .          | 970        |
| 92.8      | 가산 모형에 관한 자주 묻는 질문 . . . . .   | 972        |
| 92.9      | 내부 모형 그려 보기 . . . . .          | 972        |
| 92.10     | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 974        |
| <br>      |                                |            |
| <b>93</b> | <b>강제법(Forcing)</b>            | <b>975</b> |
| 93.1      | 순서집합 설정하기 . . . . .            | 976        |
| 93.2      | 부분 순서 집합의 추가 성질 . . . . .      | 978        |
| 93.3      | 이름과 제네릭 확장 . . . . .           | 979        |
| 93.4      | 강제법의 기본 정리 . . . . .           | 982        |
| 93.5      | (선택적) 관계 정의하기 . . . . .        | 982        |
| 93.6      | 나머지 공리들 . . . . .              | 984        |
| 93.7      | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 985        |
| <br>      |                                |            |
| <b>94</b> | <b>연속체 가설 깨뜨리기</b>             | <b>987</b> |
| 94.1      | 실수 추가하기 . . . . .              | 987        |
| 94.2      | 가산 사슬 조건 . . . . .             | 988        |
| 94.3      | 기수의 보존 . . . . .               | 989        |
| 94.4      | 무한 조합론 . . . . .               | 990        |
| 94.5      | 생각해 볼 만한 조금 더 어려운 문제 . . . . . | 991        |

---

# 92 내부 모형 이론

모형 이론은 정말로 메타적이므로, 여기서는 주의를 기울여야 합니다.

대략적으로, “ZFC의 모형”이란 군이 군 공리를 만족하는 이항 연산을 가진 집합인 것과 마찬가지로, ZFC 공리를 만족하는 이항 관계를 가진 집합입니다. 안타깝게도, 군과는 달리, 모형의 흥미로운 예시를 제시하기는 매우 어려운데, 그 이유는 단순히 우리가 문자 그대로 전체 우주를 모형화하려 하고 있기 때문입니다.

## §92.1 모형

**이 절의 대표적인 예:**  $(\omega, \in)$ 는 PowerSet을 만족하며,  $V_\kappa$ 는  $\kappa$ 가 도달 불가능할 때의 모형입니다(나중에 다룹니다).

**정의 92.1.1. 모형**  $\mathcal{M}$ 은 집합  $M$ 과 이항 관계  $E \subseteq M \times M$ 으로 구성됩니다. ( $E$  관계는 모형에서의 “ $\in$ ”입니다.)

**비고 92.1.2 —** 여기서는  $M$ 이 집합인 집합 크기 모형만을 다루고 있습니다. 전문가라면 실제로  $M$ 이 클래스인 경우도 다룰 수 있음을 알고 있겠지만, 그러려면 지금은 지나치게 신중을 기해야 할 것입니다.

모형이 주어지면, “EmptySet을 만족하는가?”와 같이 그것에 대해 특정한 질문을 던질 수 있습니다. 무슨 뜻인지 예시를 하나 보여드린 후 엄밀하게 만들어 보겠습니다.

### 예제 92.1.3 (어리석은 모형)

$\mathcal{M} = (M, E) = (\omega, \in)$ 로 놓아 봅시다. 이는 그다지 좋은 ZFC의 모형이 아니지만, 처음 몇 개의 공리 중 일부를 이해할 수 있는지 살펴봅시다.

(a)  $\mathcal{M}$ 은 Extensionality를 만족하는데, 이는 다음 문장입니다

$$\forall x \forall y \forall a : (a \in x \iff a \in y) \implies x = y.$$

이는 단지  $E$ 가 실제로  $\in$ 이라는 사실로부터 따라옵니다.

(b)  $\mathcal{M}$ 은 EmptySet을 만족하는데, 이는 다음 문장입니다

$$\exists a : \forall x \neg(x \in a).$$

즉,  $a = \emptyset \in \omega$ 로 잡으면 됩니다.

(c)  $\mathcal{M}$ 은 Pairing을 만족하지 않는데,  $1, 3 \in \omega$ 이지만  $\{1, 3\}$ 은  $\omega$ 에 속하지 않기 때문입니다.

(d) 놀랍게도,  $\mathcal{M}$ 은 Union을 만족하는데, 임의의  $n \in \omega$ 에 대해  $\cup n$ 이  $n - 1$ 이기 때문입니다( $n = 0$ 인 경우는 제외). 합집합 공리는 다음을 명시합니다

$$\forall a \exists U \quad \forall x [(x \in U) \iff (\exists y : x \in y \in a)].$$

여기서 주목할 중요한 점은, “ $\forall a$ ”가 오직 모형인 우주  $\mathcal{M}$  안의 집합들에 대해서만 범위를 갖는다는 것입니다.

**예제 92.1.4 (중요: 이 어리석은 모형은 PowerSet을 만족합니다)**

무엇보다도 가장 놀라운 점은,  $\mathcal{M} = (\omega, \in)$ 이 PowerSet을 만족한다는 것입니다. 이는 정말 중요한 예시입니다.

이것이 터무니없다고 생각할 수도 있습니다.  $2 = \{0, 1\}$ 을 보십시오. 이것의 멍집합은  $\{0, 1, 2, \{1\}\}$ 인데, 이는 모형 안에 있지 않지 않습니까?

자, PowerSet을 좀 더 자세히 살펴봅시다. 이는 다음을 명시합니다:

$$\forall x \exists a \forall y (y \in a \iff y \subseteq x).$$

$x = 2 = \{0, 1\}$ 로 놓으면 어떻게 될까요? 사실,  $a = 3 = \{0, 1, 2\}$ 가 작동한다고 주장할 수 있습니다. 핵심은 “모든  $y$ 에 대해”인데 – 이는 오직  $\mathcal{M}$  안의 대상들에 대해서만 범위를 갖습니다.  $\mathcal{M}$ 에서, 2의 부분집합은 오직  $0 = \emptyset$ ,  $1 = \{0\}$ ,  $2 = \{0, 1\}$ 뿐입니다. “실제 세계”(즉  $V$ )에서의 “집합”  $\{1\}$ 은 모형  $\mathcal{M}$ 에서는 집합이 아닙니다.

특히, 이 낯선 새로운 세계에서는  $2^n = n+1$ 이라고 말할 수 있는데,  $n = \{0, 1, \dots, n-1\}$ 이 실제로 오직  $n+1$ 개의 부분집합만을 가지기 때문입니다.

**예제 92.1.5 (매개변수가 있는 문장)**

모형에 던지는 문장에는 “매개변수”가 포함될 수도 있습니다. 예를 들어, 앞서와 같이  $\mathcal{M} = (\omega, \in)$ 이라면  $\mathcal{M}$ 은 다음 문장을 만족합니다

$$\forall x \in 3 (x \in 5).$$

**§92.2 문장과 만족**

이 직관적인 개념을 바탕으로, 모형이 어떤 문장을 만족한다는 것이 무엇을 의미하는지 정의할 수 있습니다.

**정의 92.2.1.** 임의의 문장  $\phi$ 는 다음 다섯 가지 형태 중 하나로 쓸 수 있음에 유의하십시오:

- $x \in y$
- $x = y$
- 어떤 더 짧은 문장  $\psi$ 에 대해  $\neg\psi$  (“ $\psi$ 가 아니다”)
- 어떤 더 짧은 문장  $\psi_1, \psi_2$ 에 대해  $\psi_1 \vee \psi_2$  (“ $\psi_1$  또는  $\psi_2$ ”)
- 어떤 더 짧은 문장  $\psi$ 에 대해  $\exists x \psi$  (“ $x$ 가 존재한다”)

**질문 92.2.2.**  $\wedge$ (그리고)와  $\forall$ (모든 것에 대해)는 어떻게 된 것입니까? (힌트:  $\neg$ 를 사용하십시오.)

흔히 (사실상 거의 항상) 우리는 이른바 “논리식 복잡도에 대한 귀납법”을 통해 진행하게 될 것인데, 이는 이것을 이용하여 귀납적으로 무언가를 정의하거나 증명한다는 뜻입니다. 우리는 모든 논리식이 유한할 것을 요구함에 유의하십시오.

이제  $a = b$ 나  $\exists a \forall x \neg(x \in a)$ 와 같은 문장  $\phi$ 와, 모형  $\mathcal{M} = (M, E)$ 가 있다고 합시다. 우리는  $\mathcal{M}$ 이  $\phi$ 를 만족하는지 묻고자 합니다.

이것에 의미를 부여하려면, 특정 변수들을 **매개변수**로 지정해야 합니다. 예를 들어, 제가 여러분에게

“ $a = b$ 인가?”

라고 물었다면, 여러분이 가장 먼저 던질 질문은  $a$ 와  $b$ 가 무엇이나는 것일 것입니다. 따라서  $a$ ,  $b$ 는 매개변수가 될 것입니다: 이 문장이 의미를 가지려면 저는 이들에 값을 부여해야 합니다.

반면, 제가 여러분에게

“ $\exists a \forall x \neg (x \in a)$ 인가?”

라고 물었다면, 여러분은 그냥 “그렇다”라고 대답할 것입니다. 이 경우  $x$ 와  $a$ 는 매개변수가 아닙니다. 일반적으로 매개변수란 그 의미가 어떤  $\forall$ 나  $\exists$ 에 의해 주어지지 않는 변수들을 말합니다.

앞으로 우리는  $\phi(x_1, \dots, x_n)$ 이 매개변수  $x_1, \dots, x_n$ 을 가지는 논리식  $\phi$ 를 나타내는 것으로 하겠습니다. 여기서  $n = 0$ 일 수도 있음에 유의하십시오. 예를 들어 모든 ZFC 공리는 매개변수를 갖지 않습니다.

**질문 92.2.3.** 아래에서 만족의 정의를 읽기 전에 미리 추측해 보십시오. (그다지 어렵지 않게 추측할 수 있습니다!)

**정의 92.2.4.**  $\mathcal{M} = (M, E)$ 를 모형이라 합시다.  $\phi(x_1, \dots, x_n)$ 을 문장이라 하고,  $b_1, \dots, b_n \in M$ 이라 합시다. 우리는 다음과 같은 관계를 정의할 것입니다

$$\mathcal{M} \models \phi[b_1, \dots, b_n]$$

그리고  $\mathcal{M}$ 이 매개변수  $b_1, \dots, b_n$ 을 가지고 문장  $\phi$ 를 **만족한다**고 말합니다.

이 관계는 논리식 복잡도에 대한 귀납법으로 다음과 같이 정의됩니다:

- $\phi$ 가 “ $x_1 = x_2$ ”이면  $\mathcal{M} \models \phi[b_1, b_2] \iff b_1 = b_2$ 입니다.
- $\phi$ 가 “ $x_1 \in x_2$ ”이면  $\mathcal{M} \models \phi[b_1, b_2] \iff b_1 E b_2$ 입니다.  
(이것이 “ $E$ 가  $\in$ 을 해석한다”라는 말의 의미입니다.)
- $\phi$ 가 “ $\neg \psi$ ”이면  $\mathcal{M} \models \phi[b_1, \dots, b_n] \iff \mathcal{M} \not\models \psi[b_1, \dots, b_n]$ 입니다.
- $\phi$ 가 “ $\psi_1 \vee \psi_2$ ”이면  $\mathcal{M} \models \phi[b_1, \dots, b_n]$ 은 어떤  $i = 1, 2$ 에 대해  $\mathcal{M} \models \psi_i[b_1, \dots, b_n]$ 임을 뜻합니다.
- 가장 중요한 경우:  $\phi$ 가  $\exists x \psi(x, x_1, \dots, x_n)$ 이라고 합시다. 그러면  $\mathcal{M} \models \phi[b_1, \dots, b_n]$ 인 것은 다음과 동치입니다

$$\exists b \in M \text{ 인 그러한 } \mathcal{M} \models \psi[b, b_1, \dots, b_n].$$

$\psi$ 는 매개변수가 하나 더 있음에 유의하십시오.

모델의 정보가 실제로 어디에서 사용되는지 주목하십시오.  $x_1 \in x_2$ 를 해석할 때는 오직  $E$ 만을 사용하는데, 이는 놀랍지 않습니다. 그러나 집합  $M$ 을 사용하는 것은 오직  $\exists$  (그리고 따라서  $\forall$ ) 위를 훑을 때뿐입니다. 이는 명심할 만한 가치가 있습니다:

**모델의 행동은 본질적으로 전체 모델  $M$ 을 훑는  $\exists$ 와  $\forall$ 에서 비롯됩니다.**

그리고 마지막으로,

**정의 92.2.5.** **ZFC의 모델**이란 모든 ZFC 공리를 만족하는 모델  $\mathcal{M} = (M, E)$ 입니다.

우리는 특히  $M$ 이 추이적인 집합인,  $(M, \in)$  형태의 모델에 관심이 있습니다. (우리는 우주가 추이적이기를 원하는데, 그렇지 않으면 우주 자체에 속하지 않는 집합의 원소가 존재하게 되며, 이는 매우 이상한 일입니다.) 이러한 모델을 **추이적 모델**이라 부릅니다.

**표기의 남용 92.2.6.**  $M$ 이 추이적 집합이면, 모델  $(M, \in)$ 은 간단히  $M$ 으로 줄여 씁니다.

**정의 92.2.7.** ZFC의 **내부 모델**이란 ZFC를 만족하는 추이적 모델입니다.

**비고 92.2.8** — ZFC의 모델에 대한 정의는  $\varphi$ 에 매개변수가 없는 경우의  $M \models \varphi$ 만을 사용합니다. 그럼에도 불구하고,  $\varphi$ 가 매개변수를 가질 때  $M \models \varphi$ 가 무엇을 뜻하는지도 우리가 정의하고 있음을 알 수 있는데, 이는  $M \models \exists x \psi(x)$ 의 정의에서 그것이 사용되기 때문입니다.

확장  $\varphi(x_1, \dots, x_n)$ 은 둥근 괄호로 표기되지만,  $M \models \varphi[b_1, \dots, b_n]$ 은 대괄호로 표기됩니다 — 이는 매개변수  $b_1, \dots, b_n$ 을  $\varphi$ 에 "형식적으로 대입"한 것으로 생각할 수 있는데, 만약  $b_1, \dots, b_n$ 을  $\varphi$ 에 "실제로" 대입한다면  $\varphi(b_1, \dots, b_n)$ 은 그저 하나의 불리언 값일 뿐이기 때문입니다.

## §92.3 레비 계층

**이 절의 대표적인 예:**  $\text{isSubset}(x, y)$ 는 절대적입니다. 공리  $\text{EmptySet}$ 은  $\Sigma_1$ 이고,  $\text{isPowerSetOf}(X, x)$ 는  $\Pi_1$ 입니다.

기억해야 할 핵심은 모델의 동작이 대체로  $\exists$ 와  $\forall$ 에 의해 결정된다는 것입니다. 사실 이보다 더 많은 것을 말할 수 있습니다.

다음과 같은 논리식을 생각해봅시다

$$\text{isEmpty}(x) : \neg \exists a (a \in x)$$

이는 주어진 집합  $x$ 가 그 안에 원소를 가지는지 확인합니다. 기술적으로 이 안에는 " $\exists$ "가 들어 있습니다. 하지만 어쨌든 이  $\exists$ 는 실제로 전체 모델을 훑지는 않는데, 이는 그것이  $x$  안에서 찾도록 유계되어 있기 때문입니다. 즉, 우리는 이를 비공식적으로 다음과 같이 다시 쓸 수 있습니다

$$\neg(\exists a \in x)$$

이는 엄밀한 형식에 들어맞지는 않지만, 우리가 오직  $a \in x$  위만을 살펴보고 있다는 점을 짚어 줍니다. 우리는 이러한 한정사를 **유계 한정사**라 부릅니다.

우리는 유계 한정사를 가진 문장을 선호하는데, 이는 그것들이 추이적 모델에 대해 **절대적**인 성질을 나타내기 때문입니다. 여러분을 둘러싼 모델  $M$ 이 아무리 이상하더라도 상관 없습니다.  $M$ 이 추이적이기만 하다면,

$$M \models \text{isEmpty}(\emptyset)$$

항상 성립할 것입니다. 마찬가지로, 문장

$$\text{isSubset}(x, y) : x \subseteq y \text{ i.e. } \forall a \in x (a \in y)$$

은 절대적입니다. 이러한 성질을 가진 문장을  $\Sigma_0$  또는  $\Pi_0$ 이라 부릅니다.

다음과 같은 문장에서는 상황이 다릅니다

$$\text{isPowerSetOf}(y, x) : \forall z (z \subseteq x \iff z \in y)$$

이는 영어로 " $y$ 는  $x$ 의 멱집합이다", 즉 그냥  $y = \mathcal{P}(x)$ 를 뜻합니다. 여기서  $\forall z$ 는 유계가 아닙니다. 이러한 기이함이 다음과 같은 것들을 가능하게 합니다

$$\omega \models \text{"}\{0, 1, 2\} \text{는 } \{0, 1\} \text{의 멱집합이다"}$$

그리고 따라서

$$\omega \models \text{PowerSet}$$

이는 앞서 든 우리의 어리석은 예시였습니다. 문장  $\text{isPowerSetOf}$ 는 비유계  $\forall$  뒤에 절대적 문장이 오는 형태로 이루어져 있으므로, 우리는 이를  $\Pi_1$ 이라고 말합니다.

더 일반적으로, **레비 계층**은 우리의 한정사가 얼마나 유계인지를 추적합니다. 구체적으로,

- 유계 한정사만을 가진 논리식은  $\Delta_0 = \Sigma_0 = \Pi_0$ 입니다.
- $\psi$ 가  $\Pi_n$ 인 경우,  $\exists x_1 \dots \exists x_k \psi$  형태의 논리식은  $\Sigma_{n+1}$ 로 간주됩니다.
- $\psi$ 가  $\Sigma_n$ 인  $\forall x_1 \dots \forall x_k \psi$  형태의 논리식은  $\Pi_{n+1}$ 로 간주됩니다.

( $\Sigma_n$ 이면서 동시에  $\Pi_n$ 인 논리식을  $\Delta_n$ 이라고 부르지만,  $n = 0$ 인 경우를 제외하고는 이를 사용하지 않겠습니다.)

### 예제 92.3.1 ( $\Delta_0$ 문장의 예시)

- 위에서 논의한  $\text{isEmpty}(x)$ ,  $x \subseteq y$  문장들입니다.
- “ $x$ 는 추이적이다”라는 논리식은  $\Delta_0$  문장으로 전개될 수 있습니다.
- “ $x$ 는 순서수이다”라는 논리식은  $\Delta_0$  문장으로 전개될 수 있습니다.

**연습문제 92.3.2.** “ $x$ 는 추이적이다”와 “ $x$ 는 순서수이다”의 전개를  $\Delta_0$  형태로 작성하십시오.

### 예제 92.3.3 (더 복잡한 논리식)

- 공리  $\text{EmptySet}$ 은  $\Sigma_1$ 이며, 이는  $\exists a(\text{isEmpty}(a))$ 이고,  $\text{isEmpty}(a)$ 는  $\Delta_0$ 입니다.
- 위에서 논의했듯이 “ $y = \mathcal{P}(x)$ ”라는 논리식은  $\Pi_1$ 입니다.
- “ $x$ 는 가산이다”라는 논리식은  $\Sigma_1$ 입니다. 이를 표현하는 한 가지 방법은 “ $\exists f$ 가  $x \hookrightarrow \omega$ 인 단사 사상이다”인데, 이는 필연적으로 비유계인 “ $\exists f$ ”를 갖습니다.
- 공리  $\text{PowerSet}$ 은  $\Pi_3$ 입니다:

$$\forall y \exists P \forall x (x \subseteq y \iff x \in P).$$

**비고 92.3.4 (왜 교대하는 무한정 한정사 개수만 고려하는가?)** — 공식  $\exists a \exists b \psi(a, b)$ 는  $\exists c (c \text{는 순서쌍 } (a, b) \text{이다} \wedge \psi(a, b))$ 로도 쓸 수 있음에 주목하십시오. 이는 왜 공식  $\exists a \exists b \psi(a, b)$ 만을  $\Sigma_1$ 으로 간주하고자 하는지를 설명해 줍니다.

## §92.4 부분구조와 타르스키-보트 정리

$\mathcal{M}_1 = (M_1, E_1)$ 과  $\mathcal{M}_2 = (M_2, E_2)$ 를 모델이라고 합시다.

**정의 92.4.1.**  $M_1 \subseteq M_2$ 이고  $E_1$ 이  $E_2$ 와 일치하면  $\mathcal{M}_1 \subseteq \mathcal{M}_2$ 라고 말하며, 이때  $\mathcal{M}_1$ 을  $\mathcal{M}_2$ 의 **부분구조**라고 부릅니다.

그건 지루한 이야기입니다. 흥미로운 부분은 다음과 같습니다:

**정의 92.4.2.**  $\mathcal{M}_1 \subseteq \mathcal{M}_2$ 이고 모든 문장  $\phi(x_1, \dots, x_n)$ 과 매개변수  $b_1, \dots, b_n \in M_1$ 에 대해 다음이 성립하면,  $\mathcal{M}_1 \prec \mathcal{M}_2$ 이다, 또는  $\mathcal{M}_1$ 이  $\mathcal{M}_2$ 의 **초등 부분구조**이다라고 말하며, 이때 다음이 성립합니다

$$\mathcal{M}_1 \models \phi[b_1, \dots, b_n] \iff \mathcal{M}_2 \models \phi[b_1, \dots, b_n].$$

다시 말해,  $\mathcal{M}_1$ 과  $\mathcal{M}_2$ 는 가능한 모든 문장에 대해 일치합니다.  $b_i$ 는 반드시  $\mathcal{M}_1$ 에서 와야 함에 유의하십시오. 만약  $b_i$ 가  $\mathcal{M}_2$ 에서 왔다면  $\mathcal{M}_1$ 에 무언가를 묻는 것은 말이 되지 않을 것입니다.

이제 물어봅시다:  $\mathcal{M}_1 \prec \mathcal{M}_2$ 는 어떻게 성립하지 않을 수 있을까요? 가능한 문장들을 살펴보면, 원자 논리식이나 “ $\wedge$ ”, “ $\neg$ ” 중 어느 것도 문제를 일으키지 않을 것입니다.

지금쯤 여러분이 갖게 될 직관은, 문제가 발생하는 것은  $\forall$ 과  $\exists$ 에 도달했을 때라는 것입니다. 유계 한정사에 대해서는 문제가 생기지 않습니다. 그러나 비유계 한정사는 모델 전체를 탐색하며, 바로 그 지점에서 문제가 발생합니다.

“구체적인 예”를 들자면:  $\mathcal{M}_1$ 을 MIT,  $\mathcal{M}_2$ 를 매사추세츠 주라고 상상해봅시다.  $\mathcal{M}_1$ 이 MIT에 해커가 존재한다고 생각한다면, 확실히 매사추세츠 주에도 해커가 존재합니다. 문제가 생기는 경우는 다음과 같은 것입니다:

$$\mathcal{M}_2 \models \text{“}\exists x : x \text{는 번호가 } > 50 \text{인 강의이다”}.$$

이는  $\mathcal{M}_2$ 에서는 참인데, 예컨대 목격자로  $x = \text{Math 55}$ 를 취할 수 있기 때문입니다. 하지만  $\mathcal{M}_1$ 에서는 거짓인데, MIT에서는 모든 과목이 18.701과 같은 식으로 번호가 매겨지기 때문입니다.

**문제는  $\mathcal{M}_2$ 에서의 명제들에 대한 목격자가 반드시  $\mathcal{M}_1$ 에 대한 목격자로 전파되지는 않는다는 점입니다.**

Tarski-Vaught 판정법은 이것이 유일한 장애물임을 말해줍니다:  $\mathcal{M}_2$ 의 모든 증인을  $\mathcal{M}_1$ 의 증인으로 대체할 수 있다면  $\mathcal{M}_1 \prec \mathcal{M}_2$ 입니다.

#### 보조정리 92.4.3 (Tarski-Vaught)

$\mathcal{M}_1 \subseteq \mathcal{M}_2$ 라고 합시다. 그러면  $\mathcal{M}_1 \prec \mathcal{M}_2$ 인 것은 다음과 동치입니다: 모든 문장  $\phi(x, x_1, \dots, x_n)$ 와 매개변수  $b_1, \dots, b_n \in M_1$ 에 대해,  $\mathcal{M}_2 \models \phi(\tilde{b}, b_1, \dots, b_n)$ 에 대한 증인  $\tilde{b} \in M_2$ 가 존재하면  $\mathcal{M}_1 \models \phi(b, b_1, \dots, b_n)$ 에 대한 증인  $b \in M_1$ 이 존재합니다.

증명. 위의 논의 이후에는 쉽습니다. 이를 형식화하려면 논리식의 복잡도에 대한 귀납법을 사용하십시오.  $\square$

## §92.5 ZFC의 공리 얻기

이제  $M$ 이 ZFC 공리를 만족하기 위한 조건을 적어보고자 합니다. 그 발상은, ZFC 공리들의 거의 전부가 어떤 원하는 집합에 대한 단순한  $\Sigma_1$  주장이며, 따라서 어떤 공리를 검증하는 것은 그 공리의 증인이 실제로 모델 안에 있는지를 확인하는 적절한 “단힘” 조건을 확인하는 것으로 귀결된다는 것입니다.

예를 들어, EmptySet 공리는 “ $\exists a(\text{isEmpty}(a))$ ”이며, 따라서  $\emptyset \in M$ 이기만 하면 만족되는데, 이는 물론 공집합이 아닌 임의의 추이적 집합  $M$ 에 대해 참입니다.

**보조정리 92.5.1** (ZFC를 물려받는 추이적 집합)

$M$ 을 공집합이 아닌 추이적 집합이라고 합시다. 그러면

- (i)  $M$ 은 Extensionality, Foundation, EmptySet을 만족합니다.
- (ii)  $x, y \in M \implies \{x, y\} \in M$ 이면  $M \models \text{Pairing}$ 입니다.
- (iii)  $x \in M \implies \cup x \in M$ 이면  $M \models \text{Union}$ 입니다.
- (iv)  $x \in M \implies \mathcal{P}(x) \cap M \in M$ 이면  $M \models \text{PowerSet}$ 입니다.
- (v) 모든  $x \in M$ 과 매개변수를 사용해  $M$ -정의가능한 모든 함수  $F: x \rightarrow M$ 에 대해  $F^{\text{img}}(x) \in M$ 이 성립하면  $M \models \text{Replacement}$ 입니다.
- (vi)  $\omega \in M$ 이기만 하면  $M \models \text{Infinity}$ 입니다.

여기서, 집합  $X \subseteq M$ 이 다음과 같이 실현될 수 있으면 이를 **매개변수를 사용해  $M$ -정의가능**하다고 합니다

$$X = \{x \in M \mid \phi[x, b_1, \dots, b_n]\}$$

어떤 (고정된) 매개변수  $b_1, \dots, b_n \in M$ 의 선택에 대해서 말입니다.  $n = 0$ 도 허용하며, 이 경우  $X$ 를 **매개변수 없이  $M$ -정의가능**하다고 합니다.  $X$  자체가  $M$ 에 속할 필요는 없다는 점에 유의하십시오! 사소한 예로,  $X = M$ 은 매개변수 없이  $M$ -정의가능하며(그저  $\phi[x]$ 가 항상 참이 되도록 잡으면 됩니다), 이때 당연히  $X \in M$ 은 성립하지 않습니다.

**연습문제 92.5.2.** 위의 (i)-(iv)를 확인하십시오.

**비고 92.5.3** — 보조정리 92.5.1의 명제들에 대한 역은 (vi)를 제외한 모든 주장에서 참입니다.

## §92.6 Mostowski 붕괴

지금까지는 생각하기 더 쉬웠기 때문에 추이적 모델에 대해서만 이야기해 왔습니다. 여기 우리가 추이적 모델에만 관심을 가져도 되는 두 번째, 더 나은 이유가 있습니다.

**보조정리 92.6.1** (Mostowski 붕괴 정리)

$X = (X, \in)$ 을 Extensionality를 만족하는 모델이라 하고,  $X$ 는 (추이적이 아닐 수도 있는) 집합이라고 합시다. 그러면 추이적 모델  $M = (M, \in)$ 에 대해 동형사상  $\pi: X \rightarrow M$ 이 존재합니다.

이는 추이적 붕괴라고도 불립니다. 실제로  $\pi$ 와  $M$ 은 모두 유일합니다.

증명. 증명의 발상은 매우 간단합니다.  $\in$ 이 정초적이고 외연적이므로(각각 Foundation과 Extensionality를 만족하므로),  $\in$ 에 대해  $X$ 의  $\in$ -극소 원소  $x_\emptyset$ 을 살펴볼 수 있습니다. 명백히, 우리는 그것을  $0 = \emptyset$ 으로 보내고자 합니다.

그다음  $\in$  하에서 그다음으로 작은 집합을 취해  $1 = \{\emptyset\}$ 으로 보냅니다. 이를 "계속 반복"하는데, 이것이 정확히 우리가 원하는 바를 수행함을 확인하기는 어렵지 않습니다.

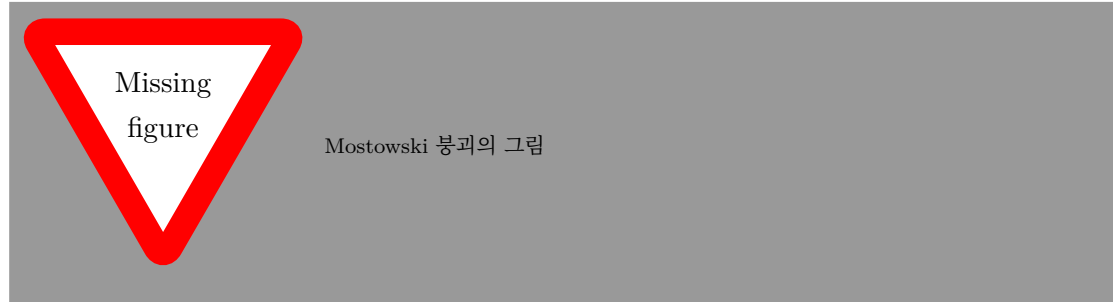
형식화하기 위해,  $\pi$ 를 초한 재귀법으로 정의합니다:

$$\pi(x) := \{\pi(y) \mid y \in x\}.$$

이렇게 구성된 이  $\pi$ 는 그 역할을 해냅니다. □

**비고 92.6.2 (전문가를 위한 여담)** — Napkin의 초기 버전에서는 이것이  $\mathcal{X} \models \text{Foundation} + \text{Extensionality}$ 를 만족하는 일반적인 모델  $\mathcal{X} = (X, E)$ 에 대해서도 참이라고 주장했습니다. 이는 거짓입니다. 이는  $E$ 가 정초적임을 함의하지도 않는데,  $X$  자체에는 속하지 않는  $X$ 의 부분집합들의 무한 하강 사슬이 존재할 수 있기 때문입니다. 또 다른 문제는  $E$ 가 집합류(set-like)가 아닐 수도 있다는 것입니다.

이에 대한 그림은  $M$ 의 원소들을  $V$ 의 바닥으로 "붕괴시키는" 것이며, 이름도 여기서 유래합니다.



## §92.7 비가측 기수 추가하기

이 절의 대표적인 예:  $V_\kappa$

이쯤에서 이렇게 물으실 수 있습니다. 그런데 제 ZFC의 모델은 어디 있습니까?

유감스럽지만 이제 인정해야 합니다: ZFC는 ZFC의 모델이 존재한다는 것을 결코 증명할 수 없습니다(단, ZFC가 모순적인 경우는 예외이지만, 그것은 더 나쁜 상황일 것입니다). 이것은 괴델의 불완전성 정리라고 불리는 결과입니다.

그럼에도 불구하고, 매우 소박한 가정 몇 가지를 추가하면 실제로 모델이 존재함을 보일 수 있습니다: 예를 들어, 강비가측 기수  $\kappa$ 가 존재한다고 가정하면 그 역할을 하기에 충분하며,  $V_\kappa$ 가 그러한 모델이 될 것입니다 (문제 92D\*). 직관적으로 왜 그런지 알 수 있습니다:  $\kappa$ 는 너무 커서 그보다 낮은 계수를 가진 어떤 집합도, 심지어 그것의 멍집합을 취하거나, Replacement 공리를 사용하거나, ZFC가 허용하는 다른 어떤 방법을 쓰더라도 그것을 벗어날 수 없습니다.

더 비관적으로 말하면, 이는 그러한  $\kappa$ 가 존재한다는 것을 ZFC에서 증명하는 것이 불가능함을 보여줍니다. 그럼에도 불구하고, 편의를 위해 이제부터는  $ZFC^+$  하에서 논의를 진행하는데, 이는 그러한  $\kappa$ 의 존재를 마지막 공리로 추가한 것입니다. 이제 우리는 가지고 놀 수 있는 모델  $V_\kappa$ 를 갖게 되었습니다. 기쁩니다!

좋습니다. 이제 정말로 미친 짓을 해보겠습니다.

### 정리 92.7.1 (가산 추이적 모델)

$ZFC^+$ 를 가정합니다. 그러면  $X$ 가 가산 집합인, ZFC의 추이적 모델  $X$ 가 존재합니다.

증명. 안전벨트를 매십시오.

먼저, 우리는  $ZFC^+$ 를 가정했으므로,  $V_\kappa = (V_\kappa, \in)$ 를 우리의 ZFC 모델로 취할 수 있습니다. 집합  $X_0 = \emptyset$ 에서 시작합니다. 그런 다음 모든 정수  $n$ 에 대해,  $X_{n+1}$ 을 얻기 위해 다음을 수행합니다.

- $X_n$ 의 모든 원소를 포함하는  $X_{n+1}$ 에서 시작합니다.

- $X_n$ 에 속한 논리식  $\phi(x, x_1, \dots, x_n)$ 과  $b_1, \dots, b_n$ 을 생각합니다.  $V_\kappa$ 가 다음을 만족하는  $b \in V_\kappa$ 가 존재한다고 생각한다고 가정합니다.

$$V_\kappa \models \phi[b, b_1, \dots, b_n].$$

그런 다음 원소  $b$ 를  $X_{n+1}$ 에 추가합니다.

- 우리는 이를 집합론 언어에서 가능한 모든 논리식에 대해 수행합니다. 또한 이전 집합  $X_n$ 으로부터 나온 가능한 모든 매개변수 집합을 넣어야 합니다.

매 단계마다  $X_n$ 은 가산입니다. 이유:  $X_n$ 에는 가능한 유한 매개변수 집합이 가산 개 있고, 가능한 논리식도 가산 개 있으므로, 각 단계에서 우리가 추가하는 것은 전체적으로 가산 개뿐입니다. 이는 가산 집합들의 무한 중첩 수열을 보여줍니다

$$X_0 \subseteq X_1 \subseteq X_2 \subseteq \dots$$

이들 중 어느 것도  $V_\kappa$ 의 초등 부분구조가 아닌데, 각  $X_n$ 이  $X_{n+1}$  안의 증인들에 의존하기 때문입니다. 그래서 우리는 대신 합집합을 취합니다:

$$X = \bigcup_n X_n.$$

이는 Tarski-Vaught 판정법을 만족하며, 가산입니다.

한 가지 사소한 주의사항이 있습니다:  $X$ 는 추이적이지 않을 수도 있습니다. 우리는 신경 쓰지 않는데, 그저 그것의 Mostowski 붕괴를 취하면 되기 때문입니다.  $\square$

잠시 시간을 내어 이것이 얼마나 미친 것인지 감상해 보십시오. 이는 우리가 적을 수 있는 문장이 가산 개라는 사실에 돌이킬 수 없이 의존합니다.

**비고 92.7.2** — 이 증명은 원소  $b$ 를  $X_{n+1}$ 에 추가할 때 선택 공리에 크게 의존합니다. 선택 공리 없이는 이러한 결정들을 한꺼번에 내릴 방법이 없습니다.

보통 선택 공리 사용을 형식화하는 올바른 방법은, 모든 논리식  $\phi(x, x_1, \dots, x_n)$ 에 대해 (아주 처음부터) 함수  $f_\phi(x_1, \dots, x_n)$ 를 미리 정해 놓아서, 임의의  $b_1, \dots, b_n$ 이 주어졌을 때  $f_\phi(b_1, \dots, b_n)$ 이 (존재한다면)  $b$ 의 적절한 값을 내놓도록 하는 것입니다. 개인적으로는 이것이 증명의 정신을 감추고 있다고 생각하지만, 선택 공리가 정확히 어떻게 사용되는지는 명확하게 보여줍니다.

이  $f_\phi$ 들에는 이름이 있는데, **스콜렘 함수**라고 합니다.

증명에서 사용한 트릭은 더 일반적인 상황에서도 성립합니다.

### 정리 92.7.3 (하향 Löwenheim-Skolem 정리)

$\mathcal{M} = (M, E)$ 가 모델이고,  $A \subseteq M$ 이라고 합시다. 그러면  $A \subseteq B \subseteq M$ 이며  $(B, E) \prec \mathcal{M}$ 인 집합  $B$ ( $A$ 의 **스콜렘 꺾질**이라 불림)가 존재하며,

$$|B| = \max \{\omega, |A|\}.$$

우리의 경우, 우리가 한 것은 단순히  $A$ 를 공집합으로 잡은 것입니다.

**질문 92.7.4.** 이를 증명하십시오. (이전과 정확히 같은 증명입니다.)

## §92.8 가산 모형에 관한 자주 묻는 질문

가장 흔한 질문은 "이게 어떻게 가능한가?"이며, 근소한 차로 뒤를 잇는 것은 "방금 무슨 일이 일어난 것인가?"입니다.

첫 번째 질문에 최선을 다해 답해 보겠습니다. 서로 부딪히는 두 가지가 있는 것처럼 보입니다.

(1)  $M$ 은 ZFC의 추이적 모형이지만, 그 전체 집합은 가산입니다.

(2) ZFC는 비가산 집합이 존재한다고 우리에게 말해 줍니다!

(이는 매우 많은 사람들을 혼란스럽게 했기에 이름이 있는데, **스콜렘의 역설**이라고 합니다.)

이것이 성립하는 이유는 사실 앞서 지적했습니다. 가산성은 절대적이지 않으며, 이는  $\Sigma_1$  개념입니다.

집합  $x$ 가 가산이라는 것은 단사 사상  $x \hookrightarrow \omega$ 가 존재한다는 것임을 상기하십시오. 첫 번째 진술은 단지 우주  $V$  안에서 단사 사상  $F: M \hookrightarrow \omega$ 가 존재한다는 것을 말할 뿐입니다. 특히 임의의  $x \in M$ 에 대해 ( $M$ 이 추이적이므로  $x \subseteq M$ 이기도 합니다),  $x$ 는  $V$  안에서 가산입니다. 이것이 첫 번째 진술의 내용입니다.

그러나  $M$ 이 ZFC의 모형이 되려면,  $M$ 은 ZFC의 진술들이 참이라고 여기기만 하면 됩니다. 더 정확히 말하면, ZFC가 비가산 집합이 존재한다고 말한다는 사실은 다음을 의미합니다

$$M \models \exists x \text{ 비가산.}$$

다시 말해,

$$M \models \exists x \forall f (f: x \rightarrow \omega \text{ 이면 } f \text{는 단사가 아닙니다.})$$

핵심은  $\forall f$ 가 오직 우리의 작은 모형  $M$  안에 있는 함수들만 찾는다는 것입니다. "실제 세계"  $V$ 에서는 단사 함수  $f: x \rightarrow \omega$ 가 존재한다는 것이 참입니다.<sup>1</sup> 그러나  $M$ 은 그것들이 존재한다는 사실을 전혀 모릅니다! 이는 통 속의 뇌와 같습니다.  $M$ 은 자신 바깥의 어떤 정보에도 무지합니다.

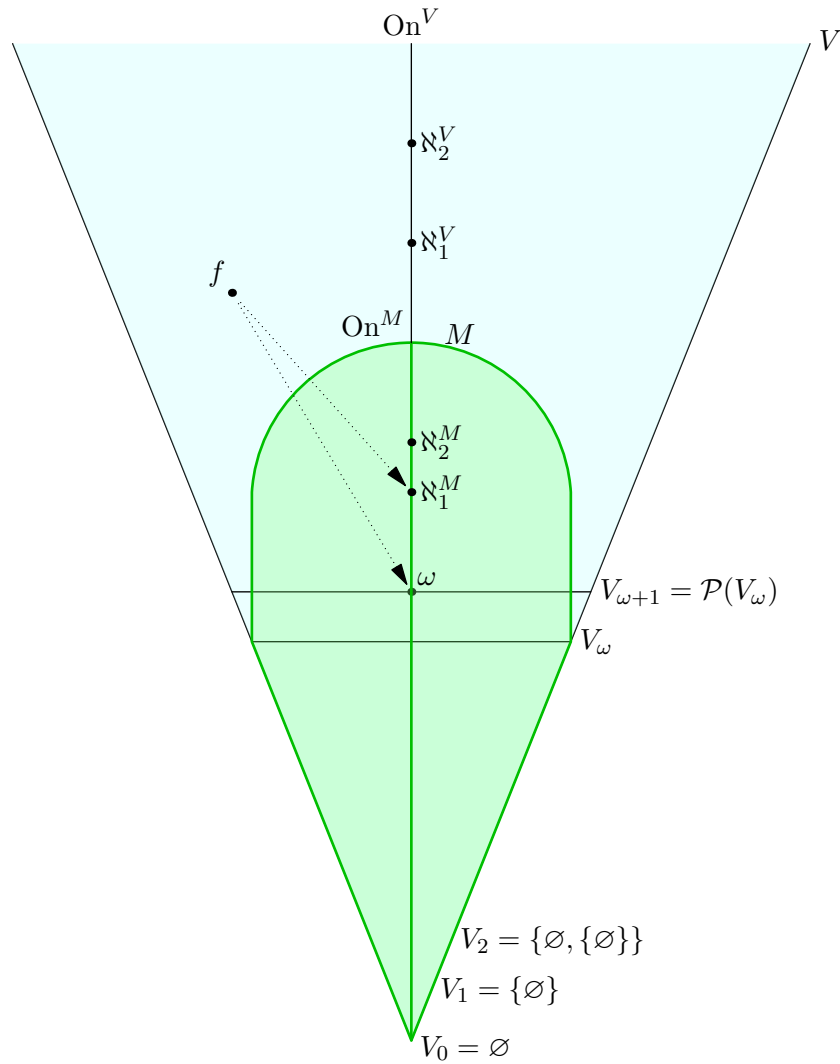
그래서 실제로  $M$ 에 나타나는 모든 순서수는 실제 세계에서는 가산입니다. 다만  $M$  안에서서는 가산이 아닐 뿐입니다.  $M \models \text{ZFC}$ 이므로,  $M$ 은 가장 작은 비가산 기수, 이를테면  $\aleph_1^M$ 이 존재한다고 여길 것입니다. 이는 모형  $M$  안에서  $\aleph_1^M$ 과  $\omega$  사이에 전단사가 없다는 성질을 가진  $M$  안의 가장 작은 (무한) 순서수가 될 것입니다. 그러나 우리는 그러한 전단사가 실제 세계  $V$ 에서는 반드시 존재한다는 것을 알고 있습니다.

다른 방식으로 말하면,  $M$ 에서의 농도는 실제 세계에서의 농도와 매우 다르게 보일 수 있는데, 이는 농도가 전단사로 측정되기 때문이며, 이는 아마도 불가피한 일이지만 혼란을 초래합니다.

## §92.9 내부 모형 그려 보기

다음은 가산 추이적 모형  $M$ 의 그림입니다.

<sup>1</sup>  $M$ 이 추이적이고 가산이므로, 임의의  $x \in M$ 에 대해  $x$  자체도 많아야 가산 개의 원소만을 가질 수 있습니다.  $M$ 이 추이적이지 않다면 이는 반드시 성립하지는 않습니다.



$M$ 과  $V$ 는 유한 집합에 대해서는 반드시 일치해야 하는데, 모든 유한 집합은 이를 표현할 수 있는 논리식을 가지기 때문입니다. 그러나  $V_\omega$ 를 지나면 모형과 실제 우주는 갈라지기 시작합니다.

전체 모형  $M$ 은 가산이므로, 첫 번째 비가산 기수  $\aleph_1^V$  (위 첨자는 "실제 우주  $V$ 의"를 의미합니다) 아래로 우주의 작은 부분만을 차지합니다.  $M$  안의 순서수는 정확히  $V$ 의 순서수 중 우연히 모형 안에 속하는 것들인데, " $\alpha$ 는 순서수이다"라는 문장이 절대적이기 때문입니다. 반면,  $M$ 은 오직 하찮은 집합, 그것도 가산 집합에 불과하므로, 이러한 순서수들의 일부만을 가집니다.  $M$ 의 순서수를 나타내기 위해 우리는  $\text{On}^M$ 이라고 쓰며, 위 첨자는 " $M$ 에서 계산된 순서수"를 의미합니다. 마찬가지로,  $\text{On}^V$ 는 이제 "실제 순서수의 집합"을 나타낼 것입니다.

그럼에도 불구하고, 모델  $M$ 은 자신만의 버전의 첫 번째 비가산 기수  $\aleph_1^M$ 을 가지고 있습니다. 참된 우주에서  $\aleph_1^M$ 은 가산입니다( $\aleph_1^V$ 보다 작습니다), 하지만 이를 증언하는 필요한 전단사가  $M$  내부에 존재하지 않을 수 있습니다. 이것이 바로  $\aleph_1^M$ 이 원래 우주에서는 가산 기수임에도,  $M$ 이 그것을 비가산이라고 생각할 수 있는 이유입니다.

그러므로 우리의 모델  $M$ 은 통 속의 뇌입니다.  $M$ 은 우연히 ZFC의 모든 공리를 믿게 되며, 따라서  $M$ 에서 참인 모든 명제는  $V$ 에서도 참일 수 있습니다. 하지만  $M$ 은 자신을 둘러싼 우주를 볼 수 없습니다.  $M$ 은 자신이 비가산이라고 믿는  $\aleph_1^M$ 이 사실은 그저 평범한 가산 순서수에 불과하다는 것을 전혀 알지 못합니다.

## §92.10 생각해 볼 만한 조금 더 어려운 문제

**문제 92A\***. 임의의 추이적 모델  $M$ 에 대해,  $M$  안의 순서수들의 집합 자체가 하나의 순서수임을 보이십시오.

**문제 92B<sup>†</sup>**.  $\mathcal{M}_1 \subseteq \mathcal{M}_2$ 라고 가정합시다. 다음을 보이십시오.

(a)  $\phi$ 가  $\Delta_0$ 이면,  $\mathcal{M}_1 \models \phi[b_1, \dots, b_n] \iff \mathcal{M}_2 \models \phi[b_1, \dots, b_n]$ 입니다.

(b)  $\phi$ 가  $\Sigma_1$ 이면,  $\mathcal{M}_1 \models \phi[b_1, \dots, b_n] \implies \mathcal{M}_2 \models \phi[b_1, \dots, b_n]$ 입니다.

(c)  $\phi$ 가  $\Pi_1$ 이면,  $\mathcal{M}_2 \models \phi[b_1, \dots, b_n] \implies \mathcal{M}_1 \models \phi[b_1, \dots, b_n]$ 입니다.

(이 장을 이해했다면 쉬울 것입니다.)



**문제 92C<sup>†</sup>** (반영).  $\kappa$ 를 비가산 기수라고 하고, 모든  $\alpha < \kappa$ 에 대해  $|V_\alpha| < \kappa$ 라고 합시다. 임의의  $\delta < \kappa$ 에 대해  $\delta < \alpha < \kappa$ 이면서  $V_\alpha \prec V_\kappa$ 인  $\alpha$ 가 존재함을 증명하십시오. 다시 말해,  $V_\alpha \prec V_\kappa$ 인  $\alpha$ 들의 집합이  $\kappa$ 에서 비유계임을 증명하십시오. 이는  $V_\kappa$ 의 성질들이  $V_\alpha$ 의 성질로 반영됨을 의미합니다.



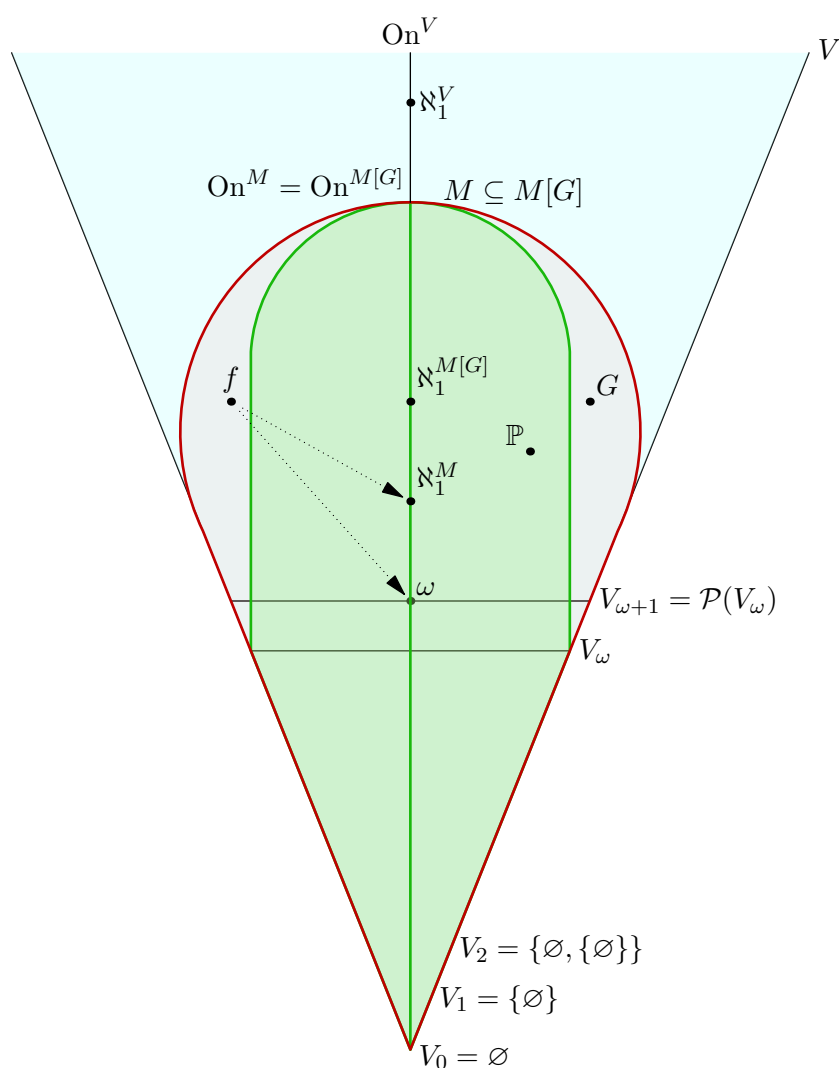
**문제 92D\*** (강비가산 기수는 모델을 만들어 냅니다).  $\kappa$ 를 강비가산 기수라고 합시다.  $V_\kappa$ 가 ZFC의 모델임을 증명하십시오.

# 93 강제법(Forcing)

이제 폴 코언(Paul Cohen)의 **강제법(forcing)** 기법을 소개하며, 이를 이용해 연속체 가설을 무너뜨릴 것입니다.

작동 방식은 다음과 같습니다. 추이적 모델  $M$ 과 그 안에 있는 순서집합  $\mathbb{P}$ 가 주어졌을 때, "제네릭(generic)" 부분집합  $G \subseteq \mathbb{P}$ 를 생각할 수 있으며, 이때  $G$ 는  $M$  안에 있지 않습니다. 그런 다음  $M$ 과  $G$ 를 모두 포함하는 더 큰 우주  $M[G]$ 를 구성할 것입니다. (이 표기법은 의도적으로 예를 들어  $\mathbb{Z}[\sqrt{2}]$ 와 같은 표기법입니다 - 대수학의 경우,  $\mathbb{Z}$ 를 취해 새로운 원소  $\sqrt{2}$ 와 그로부터 생성될 수 있는 모든 것을 추가하는 것입니다.)  $\mathbb{P}$ 를 잘 선택함으로써  $M[G]$ 가 바람직한 성질을 갖도록 만들 수 있습니다.

그림:



모델  $M$ 은 초록색으로 그려져 있으며, 그 확장인  $M[G]$ 는 빨간색으로 그려져 있습니다.

모델  $M$ 과  $M[G]$ 는 같은 순서수를 공유하며, 이는 여기서  $M$ 이  $M[G]$ 보다 높지 않은 것으로 표현되어 있습니다. 그러나 이와 관련된 한 가지 문제는, 강제법이 원래는 존재하지 않았던  $M$ 의 기수들 사이의 새로운 전단사 함수를 도입할 수 있다는 것입니다. 이는 **기수 붕괴(cardinal collapse)**라 불리는 현상으로 이어집니다: 말 그대로,  $M$ 에서의 기수가  $M[G]$

에서는 더 이상 기수가 아니라 그저 하나의 순서수가 되어버립니다. 이는  $G$ 를 첨가하는 과정에서 이전 우주에는 없었던 전단사 함수를 우연히 얻게 될 수 있기 때문입니다. 그려진 도식에서, 이것이 바로  $\omega$ 를  $\aleph_1^M$ 으로 대응시키는 함수  $f$ 입니다. 본질적으로, 이 어려움은 " $\kappa$ 가 기수이다"라는 명제가  $\Pi_1$  명제라는 데 있습니다.

연속체 가설의 경우, 임의의 제네릭 부분집합  $G$ 가  $\aleph_2^M$ 개의 실수를 "인코딩"하게 되는  $\mathbb{P}$ 를 도입할 것입니다. 그런 다음 기수 붕괴가 일어나지 않는다는 것, 즉  $\aleph_2^{M[G]} = \aleph_2^M$ 임을 보일 것입니다. 따라서  $M[G]$ 는 원하는 대로  $\aleph_2^{M[G]}$ 개의 실수를 갖게 될 것입니다.

### §93.1 순서집합 설정하기

**이 절의 대표적인 예:** 무한 이진 트리

$M$ 을 ZFC의 추이적 모델이라 합시다.  $\mathbb{P} = (\mathbb{P}, \leq) \in M$ 을 모델  $M$  안에 존재하며 최대 원소  $1_{\mathbb{P}}$ 를 갖는 순서집합이라 합시다.  $\mathbb{P}$ 의 원소들은 **조건(conditions)**이라 불리는데, 이는 그것들이  $M[G]$ 에서 참이 되도록 강제하기 때문입니다.

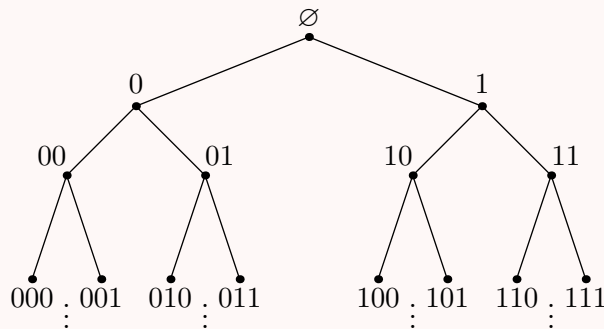
**정의 93.1.1.** 부분집합  $D \subseteq \mathbb{P}$ 가 **조밀(dense)**하다는 것은, 모든  $p \in \mathbb{P}$ 에 대해  $q \leq p$ 인  $q \in D$ 가 존재함을 의미합니다.

조밀 부분집합의 예로는  $\mathbb{P}$  전체뿐 아니라 아래쪽에서의 임의의 "조각(slice)"도 있습니다.

**정의 93.1.2.**  $p, q \in \mathbb{P}$ 에 대해,  $r \leq p$ 이고  $r \leq q$ 인  $r \in \mathbb{P}$ 가 존재하면 " $p$ 는  $q$ 와 **양립 가능(compatible)**하다"고 하며  $p \parallel q$ 라고 씁니다. 그렇지 않으면  $p$ 와  $q$ 는 **양립 불가능(incompatible)**하다고 하며  $p \perp q$ 라고 씁니다.

#### 예제 93.1.3 (무한 이진 트리)

$\mathbb{P} = 2^{<\omega}$ 를 아래에 나타낸, 자명한 방식으로 무한히 확장된 **무한 이진 트리(infinite binary tree)**라 합시다:



- (a) 최대 원소  $1_{\mathbb{P}}$ 는 빈 문자열  $\emptyset$ 입니다.
- (b)  $D = \{001\text{로 끝나는 모든 문자열}\}$ 은 조밀 집합의 예시입니다.
- (c)  $\mathbb{P}$ 의 두 원소는 비교 가능하지 않는 한 양립가능하지 않습니다.

#### 예제 93.1.4 (무한 사슬)

$\mathbb{P} = (\mathbb{N}, \geq)$ 라 합시다. 이는 "무한 일진 트리(infinite unary tree)"로 볼 수 있습니다.

- 최대 원소  $1_{\mathbb{P}}$ 는 1입니다.
- 어떤 집합이 조밀하다는 것은 그것이 무한히 많은 원소를 가짐과 동치입니다.

예를 들어, 모든 양의 짝수의 집합과 모든 소수의 집합은 조밀합니다.

이제 "제네릭(generic)"하다는 것이 무엇을 의미하는지 구체적으로 명시할 수 있습니다.

**정의 93.1.5.** 공집합이 아닌 집합  $G \subseteq \mathbb{P}$ 가 **필터(filter)**라는 것은 다음을 만족함을 의미합니다

(a) 집합  $G$ 는 위로 닫혀 있습니다:  $\forall p \in G(\forall q \geq p)(q \in G)$ .

(b)  $G$ 의 임의의 두 원소 쌍은 서로 양립가능합니다.

모델  $M$  안에 있는 모든  $D$ 에 대해,  $D$ 가 조밀하면  $G \cap D \neq \emptyset$ 일 때,  $G$ 를  **$M$ -제네릭**이라고 합니다.

**질문 93.1.6.**  $G$ 가 필터이면  $1_{\mathbb{P}} \in G$ 임을 보이십시오.

$D \in M$ 이라는 조건이 중요하다는 점에 유의하십시오. 그 이유는 다음과 같습니다:

**질문 93.1.7.** 무한 이진 트리에서 다음을 보이십시오:

- 모든 필터  $G$ 에 대해,  $G \cap D = \emptyset$ 을 만족하는 (반드시  $M$ 에 속할 필요는 없는) 조밀한 부분집합  $D$ 가 존재합니다.
- 구체적으로,  $G \in M$ 이면 그러한 집합  $D$ 를  $D \in M$ 이 되도록 선택할 수 있습니다 — 특히 이 경우  $G$ 는  $M$ -제네릭이 아닙니다.

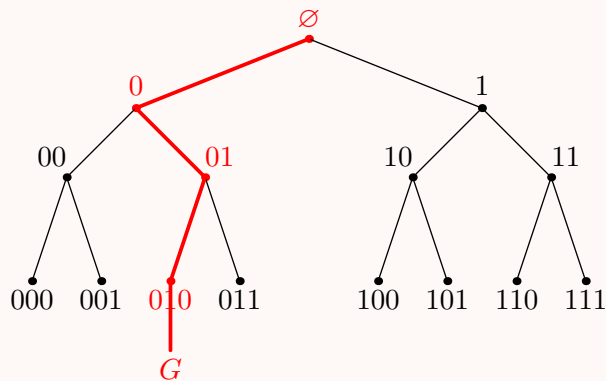
이는 보조정리 93.2.5에서 나중에 형식화하겠습니다.

**예제 93.1.8** (무한 이진 트리 위의 제네릭 필터)

$\mathbb{P} = 2^{<\omega}$ 라고 합시다.  $\mathbb{P}$  위의 제네릭 필터는 다음과 같은 형태의 집합입니다

$$\{0, b_1, b_1b_2, b_1b_2b_3, \dots\}.$$

따라서  $\mathbb{P}$  위의 모든 제네릭 필터는 이진수  $b = 0.b_1b_2b_3\dots$ 에 대응합니다.<sup>a</sup> 어떤 실수가 제네릭 필터에 대응하는지를 설명하기는 더 어렵지만, 그러한 실수는 정말로 "무작위처럼 보여야" 합니다. 예를 들어, 011로 끝나는 문자열들의 집합은 조밀하므로,  $b$  안에 "011"이 나타나리라 기대할 수 있고, 더 일반적으로는  $b$ 가 모든 이진 문자열을 포함하리라 기대할 수 있습니다. 따라서  $\pi - 3$ 의 이진 전개는 제네릭에 대응할 것이라 기대할 수 있지만, 0.010101... 같은 것은 그렇지 않을 것입니다. 이것이 바로 이들을 "제네릭"이라고 부르는 이유입니다.



<sup>a</sup>서로 다른 두 필터가  $0.1000\dots$  과  $0.0111\dots$  처럼 같은 실수에 대응하는 경우가 있을 수 있지만, 그러한 필터는 반드시 제네릭이 아니라는 점에 유의하십시오.

### 예제 93.1.9 (무한 사슬 위의 제네릭 필터)

$\mathbb{P} = (\mathbb{N}, \geq)$  위에는 오직 하나의 제네릭 필터가 있습니다: 바로  $\mathbb{N}$  자체입니다. 이는 실제로 제네릭입니다 — 모든 조밀한 집합과 교차합니다. 이는 어떤 기준으로 보아도 “무작위처럼 보이지” 않는다고 말할 수도 있습니다 — 하지만 생각해 보면, 뿌리  $1_{\mathbb{P}} = 1$ 에서 시작하여 매 단계마다 무작위로 아래로 내려간다고 해도, 갈 수 있는 곳은 오직 한 곳뿐입니다!

**연습문제 93.1.10.** 모든 제네릭 필터  $2^{<\omega}$ 가 위와 같은 형태를 가짐을 확인하십시오. 반대로, 이진수가 필터를 준다는 것을 보이되, 그것이 반드시 제네릭일 필요는 없음을 보이십시오.

$p \geq q$ 이면, 문장  $q \in G$ 는 문장  $p \in G$ 보다 더 많은 정보를 알려준다는 점에 주목하십시오. 그런 의미에서  $q$ 는 더 강한 조건입니다. 또 다른 의미에서  $1_{\mathbb{P}}$ 는 가능한 가장 약한 조건인데, 이는  $G$ 에 대해 아무것도 알려주지 않기 때문입니다;  $G$ 가 위로 닫혀 있으므로 우리는 항상  $1_{\mathbb{P}} \in G$ 를 가집니다.

## §93.2 부분 순서 집합의 추가 성질

제네릭 필터가 존재함을 반드시 확인해야 합니다.

### 예제 93.2.1

$\mathbb{P}$ 가 무한 이진 트리이고  $M$ 이  $\mathbb{P}$ 의 모든 부분집합을 포함한다면, 제네릭 필터는 존재하지 않습니다 — 모든 필터  $G \subseteq \mathbb{P}$ 에 대해,  $\mathbb{P} \setminus G$ 는 조밀한 집합  $D \in M$ 이고,  $G \cap D = \emptyset$ 이기 때문입니다.

사실 이는 다소 까다롭지만, 가산 모델에 대해서는 성립합니다:

### 보조정리 93.2.2 (Rasiowa-Sikorski 보조정리)

$M$ 이 ZFC의 가산 추이적 모델이고  $\mathbb{P}$ 가 부분 순서 집합이라고 합시다. 그러면  $M$ -제네릭 필터  $G$ 가 존재합니다.

증명. 본질적으로, 하나씩 처리하십시오. **문제 93B.** □

다행히도, CH를 깨뜨리기 위해서는 어차피  $M$ 이 가산이기를 원할 것입니다.

우리가 올바른 길을 가고 있는지 확인하기 위해 해야 할 또 다른 일은 제네릭 집합  $G$ 가 실제로  $M$ 에 속하지 않음을 보장하는 것입니다. (비유:  $\mathbb{Z}[3]$ 은 정말로 어리석은 확장입니다.) 이를 보장하는 조건은 다음과 같습니다:

**정의 93.2.3.** 부분순서  $\mathbb{P}$ 가 모든  $p \in \mathbb{P}$ 에 대해  $q \perp r$ 인  $q, r \leq p$ 가 존재할 때 **분할**이라고 합니다.

**예제 93.2.4** (무한 이진 나무는 (매우) 분할적입니다)

무한 이진 나무는 분할적일 수 있는 만큼 최대로 분할적입니다.  $p \in 2^{<\omega}$ 가 주어지면, 그 바로 아래에 있는 두 원소를 생각하면 됩니다.

**보조정리 93.2.5** (분할 부분순서는 제네릭 집합을 배제합니다)

$\mathbb{P}$ 가 분할적이라고 합시다. 그러면  $F \subseteq \mathbb{P}$ 가  $F \in M$ 인 필터이면,  $\mathbb{P} \setminus F$ 는 조밀합니다. 특히,  $G \subseteq \mathbb{P}$ 가 제네릭이면,  $G \not\subseteq F$ 입니다.

증명.  $p \notin \mathbb{P} \setminus F \iff p \in F$ 을 생각해봅시다.  $\mathbb{P}$ 가 분할적이므로, 서로 호환되지 않는  $q, r \leq p$ 가 존재합니다.  $F$ 는 필터이므로 둘 다 포함할 수 없으며, 그중 하나는  $F$  밖에 있어야 합니다. 이를  $q$ 라고 합시다. 따라서  $p \in \mathbb{P} \setminus (\mathbb{P} \setminus F)$ 의 모든 원소는  $\mathbb{P} \setminus F$ 에 속하는 원소  $q \leq p$ 를 갖습니다. 이것으로  $\mathbb{P} \setminus F$ 가 조밀함을 증명하기에 충분합니다.

**질문 93.2.6.** 제네릭  $G$ 에 관한 보조정리의 마지막 주장을 유도하십시오. □

## §93.3 이름과 제네릭 확장

이제 부분순서  $\mathbb{P}$ 와 연관된 이름을 정의하겠습니다.

**정의 93.3.1.**  $M$ 이 ZFC의 추이적 모형이고,  $\mathbb{P} = (\mathbb{P}, \leq) \in M$ 이 부분순서라고 합시다.  **$\mathbb{P}$ -이름**의 계층을 다음과 같이 재귀적으로 정의합니다

$$\begin{aligned} \text{Name}_0 &= \emptyset \\ \text{Name}_{\alpha+1} &= \mathcal{P}(\text{Name}_\alpha \times \mathbb{P}) \\ \text{Name}_\lambda &= \bigcup_{\alpha < \lambda} \text{Name}_\alpha. \end{aligned}$$

마지막으로,  $\text{Name} = \bigcup_\alpha \text{Name}_\alpha$ 는 모든  $\mathbb{P}$ -이름의 클래스를 나타냅니다.

(이  $\text{Name}_\alpha$ 들은  $V_\alpha$ 들의 유사물입니다: 각  $\text{Name}_\alpha$ 는 그저 랭크가  $\leq \alpha$ 인 모든 이름들의 집합입니다.)

**정의 93.3.2.** 필터  $G$ 에 대해,  $\tau^G$ 로 표기되는  $\tau$ 의  $G$ 에 의한 **해석**을 다음의 초한 재귀법을 사용하여 정의합니다

$$\tau^G = \left\{ \sigma^G \mid \langle \sigma, p \rangle \in \tau \text{ 그리고 } p \in G \right\}.$$

그런 다음 모형을 다음과 같이 정의합니다

$$M[G] = \left\{ \tau^G \mid \tau \in \text{Name}^M \right\}$$

여기서  $\text{Name}^M$ 은 클래스  $\text{Name}$ 의 원소 중  $M$ 에 속하는 것들입니다. 따라서  $M[G]$ 는 집합입니다. 말로 표현하면,  $M[G]$ 는 ( $M$ 에 의해 계산된) 가능한 모든  $\mathbb{P}$ -이름들의 해석입니다.

$\mathbb{P}$ -이름을 “퍼지 집합”이라고 생각하면 됩니다. 아이디어는 이렇습니다. 보통의 집합은 보통의 집합들의 모임이므로, 퍼지 집합은 퍼지 집합들의 모임이어야 합니다. 이 퍼지 집합들은 아직 오지 않은 크리스마스의 유령들과 같다고 생각할 수 있습니다: 그것들은 확실한 것이 아니라 있을 수 있는 것을 나타냅니다. 다시 말해, 그것들은 다양한  $G$ 의 선택에 대한  $M[G]$ 의 가능한 미래들을 나타냅니다.

모든 퍼지 집합에는 원소  $p \in \mathbb{P}$ 가 고정되어 있습니다. 심판의 때가 오면, 우리는 제네릭  $G$ 를 선택하여  $\mathbb{P}$ -이름들의 우주를 걸러냅니다.  $G$ 의 원소가 붙어 있는 퍼지 집합들은 실제 세계로 구현되고,  $G$  밖의 원소가 붙어 있는 퍼지 집합들은 존재에서 사라집니다. 그 결과가  $M[G]$ 입니다.

### 예제 93.3.3 (이름 계층의 처음 몇 단계)

계산해 봅시다

$$\begin{aligned}\text{Name}_0 &= \emptyset \\ \text{Name}_1 &= \mathcal{P}(\emptyset \times \mathbb{P}) \\ &= \{\emptyset\} \\ \text{Name}_2 &= \mathcal{P}(\{\emptyset\} \times \mathbb{P}) \\ &= \mathcal{P}(\{\langle \emptyset, p \rangle \mid p \in \mathbb{P}\}).\end{aligned}$$

이에 대응하는 폰 노이만 우주와 비교해 보십시오.

$$V_0 = \emptyset, V_1 = \{\emptyset\}, V_2 = \{\emptyset, \{\emptyset\}\}.$$

### 예제 93.3.4 (해석의 예시)

앞서 언급했듯이,  $\text{Name}_1 = \{\emptyset\}$ 입니다. 이제 다음을 가정합니다

$$\tau = \{\langle \emptyset, p_1 \rangle, \langle \emptyset, p_2 \rangle, \dots, \langle \emptyset, p_n \rangle\} \in \text{Name}_2.$$

그러면

$$\tau^G = \{\emptyset \mid \langle \emptyset, p \rangle \in \tau \text{ 그리고 } p \in G\} = \begin{cases} \{\emptyset\} & \text{만약 어떤 } p_i \in G \\ \emptyset & \text{그렇지 않으면.} \end{cases}$$

특히,  $1_{\mathbb{P}} \in G$ 이므로, 다음이 성립합니다:

- $n = 0$ 일 때,  $\tau = \emptyset$ 이므로,  $\tau^G = \emptyset$ 입니다.
- $n = 1$ 이고  $p_1 = 1_{\mathbb{P}}$ 일 때,  $\tau = \{\langle \emptyset, 1_{\mathbb{P}} \rangle\}$ 이므로,  $\tau^G = \{\emptyset\}$ 입니다.

따라서,

$$\{\tau^G \mid \tau \in \text{Name}_2\} = V_2.$$

사실, 이는 2뿐만 아니라 임의의 자연수  $n$ 에 대해서도 성립합니다.

따라서,  $M[G]$ 와  $M$ 은 유한 집합에 대해 일치합니다.

이제,  $M[G]$ 가  $M$ 의 원소들을 포함하는지 확인하고자 합니다. 위의  $\{\tau^G \mid \tau \in \text{Name}_2\} = V_2$ 의 증명은 쉽게 응용할 수 있습니다:  $1_{\mathbb{P}}$ 가 반드시  $G$ 에 속해야 하므로, 모든  $x \in M$ 에 대해 다음 집합을 정의합니다

$$\check{x} = \{\langle \check{y}, 1_{\mathbb{P}} \rangle \mid y \in x\}$$

초한 재귀법으로 정의합니다. 기본적으로,  $\check{x}$ 는 모든 중첩 단계에서 모든 원소에  $1_{\mathbb{P}}$ 를 태그로 붙인  $x$ 의 복사본일 뿐입니다.

**예제 93.3.5**

$\check{0} = 0$ 과  $\check{1} = \{\langle \check{0}, 1_{\mathbb{P}} \rangle\}$ 을 계산해 보십시오. 따라서

$$(\check{0})^G = 0 \quad \text{그리고} \quad (\check{1})^G = 1.$$

입니다.

**질문 93.3.6.** 일반적으로  $(\check{x})^G = x$ 임을 보이십시오. (계수 귀납법.)

그러나, 우리는  $G$  또한  $M[G]$ 에 속하도록 만들고 싶습니다. 사실, 그 이름을 정확히 적어 낼 수 있습니다: 다음과 같이 정의합니다

$$\dot{\mathbb{P}} := \{\langle \check{p}, p \rangle \mid p \in \mathbb{P}\}.$$

**질문 93.3.7.**  $(\dot{\mathbb{P}}) \in \text{Name}^M$ 이고,  $(\dot{\mathbb{P}})^G = G$ 임을 보이십시오.

**질문 93.3.8.**  $M[G]$ 가 추이적임을 확인하십시오: 즉,  $\sigma^G \in \tau^G \in M[G]$ 이면,  $\sigma^G \in M[G]$ 임을 보이십시오. (이는 어처구니없을 정도로 쉽습니다.)

요약하면,

**$M[G]$ 는  $M$ 을 확장하는 추이적 모델입니다 ( $G$ 를 포함합니다).**

게다가,  $G$ 가 단지 필터일 뿐이라 해도 이는 상당히 잘 작동합니다. 당장 얻을 수 있는 것이 무엇인지 살펴봅시다.

**보조정리 93.3.9 (필터로부터 얻어지는 성질들)**

$M$ 을 ZFC의 추이적 모델이라 합시다.  $G$ 가 필터이면,  $M[G]$ 는 추이적이며 Extensionality, Foundation, EmptySet, Infinity, Pairing, Union을 만족합니다.

이제 PowerSet, Replacement, 그리고 선택공리가 남습니다.

증명. Extensionality와 Foundation은 거저 얻어집니다. 그러면 Infinity와 EmptySet은  $M \subseteq M[G]$ 로부터 따라옵니다.

Pairing에 대해서는,  $\sigma_1^G, \sigma_2^G \in M[G]$ 라고 가정합시다. 그러면

$$\sigma = \{\langle \sigma_1, 1_{\mathbb{P}} \rangle, \langle \sigma_2, 1_{\mathbb{P}} \rangle\}$$

$\sigma^G = \{\sigma_1^G, \sigma_2^G\}$ 를 만족합니다. ( $M \models \text{Pairing}$ 을 사용했음에 유의하십시오.) Union은 문제로 남겨두니, 지금 바로 시도해 보시기를 권합니다.  $\square$

여기까지는  $M[G]$ 에서 어떤 문장이 언제 참인지에 대해 전혀 알 필요가 없었습니다. 우리가 원하는 사실들을 얻기 위해서는  $\check{x}$ 나  $\{\langle \sigma_1, 1_{\mathbb{P}} \rangle, \langle \sigma_2, 1_{\mathbb{P}} \rangle\}$ 와 같은 이름들을 고안하기만 하면 되었습니다. 하지만 나머지 공리들에 대해서는, 이러한 추가적인 힘이 정말로 필요합니다. 이를 위해 강제법의 기본 정리를 도입해야 합니다.

### §93.4 강제법의 기본 정리

모델  $M$ 은 안타깝게도  $G$ 가 무엇일지 전혀 알지 못하며, 다만 그것이 어떤 제네릭 필터라는 것만 알 뿐입니다.<sup>1</sup> 그럼에도 불구하고, 우리는 강제법 관계라 불리는 관계  $\Vdash$ 를 정의하려 합니다. 대략적으로, 우리는 다음과 같이 쓰려고 합니다

$$p \Vdash \varphi(\sigma_1, \dots, \sigma_n)$$

여기서  $p \in \mathbb{P}$ ,  $\sigma_1, \dots, \sigma_n \in M[G]$ 이며, 이는 다음과 동치입니다:

임의의 제네릭  $G$ 에 대해, 만약  $p \in G$ 이면,  $M[G] \models \varphi[\sigma_1^G, \dots, \sigma_n^G]$ 입니다.

$\Vdash$ 는  $G$ 를 참조하지 않고 정의된다는 점에 주목하십시오. 이는  $M$ 이 볼 수 있는 것입니다. 우리는  $p$ 가 문장  $\varphi(\sigma_1, \dots, \sigma_n)$ 을 **강제한다**고 말합니다. 그리고 놀랍게도, 우리는 이 관계를 역도 성립하도록 정의할 수 있습니다: 어떤 문장이 성립하는 것은 어떤  $p$ 가 그것을 강제하는 경우이고 오직 그 경우입니다.

#### 정리 93.4.1 (강제법의 기본 정리)

$M$ 이 ZF의 추이적 모델이라고 합시다.  $\mathbb{P} \in M$ 을 poset이라 하고,  $G \subseteq \mathbb{P}$ 가  $M$ -제네릭 필터라고 합시다. 그러면,

(1)  $\sigma_1, \dots, \sigma_n \in \text{Name}^M$ 을 생각해봅시다. 그러면

$$M[G] \models \varphi[\sigma_1^G, \dots, \sigma_n^G]$$

이는 조건  $p \in G$ 가 존재하여  $p$ 가 문장  $\varphi(\sigma_1, \dots, \sigma_n)$ 을 강제하는 것과 동치입니다. 이를  $p \Vdash \varphi(\sigma_1, \dots, \sigma_n)$ 로 표기합니다.

(2) 이 강제법 관계는  $M$ 에서 (균일하게) 정의 가능합니다.

다음 절에서 이 정의가 어떻게 작동하는지 말씀드리겠습니다.

### §93.5 (선택적) 관계 정의하기

우리가 진행할 방식은 다음과 같습니다. 강제법이 한쪽 방향으로 작동하도록( $p \Vdash \varphi(\sigma_1, \dots, \sigma_n)$ 이  $M[G] \models \varphi[\sigma_1^G, \dots, \sigma_n^G]$ 을 의미하도록) 가능한 가장 관대한 조건을 정의할 것입니다. 그런 다음 그 역도 성립하기를 바라볼 것입니다.

우리는 논리식의 복잡도에 대한 귀납법으로 진행합니다. 이 경우 원자 논리식(기저 경우)이 가장 어렵다는 것이 밝혀지며, 그 자체로 계수에 대한 귀납법이 필요합니다.

동기 부여를 위해, 이미  $p \Vdash \tau_1 = \tau_2$ 를 정의했다고 가정하고  $p \Vdash \tau_1 \in \tau_2$ 를 어떻게 정의해야 할지 생각해봅시다. 우리는 이것이 다음과 동치가 되도록 보장해야 합니다

$$\forall p \in G \text{인 } M\text{-제네릭 } G : M[G] \models \tau_1^G \in \tau_2^G.$$

따라서 임의의 제네릭  $G \ni p$ 가  $\tau_1^G$ 를  $\tau_2^G$ 의 원소  $\tau^G$ 와 같도록 강제하는 조건  $q$ 에 도달함을 보장하는 것으로 충분합니다. 다시 말해, 우리는  $p \Vdash \tau_1 \in \tau_2$ 의 정의를 다음과 동치가 되도록

<sup>1</sup>이것을 좋은 일이라고 말할 수도 있는데, 이유는 다음과 같습니다. 우리는  $\neg\text{CH}$ 가 ZFC와 무모순임을 보이며 하고 있으며, 실제 우주  $V$ 의 모델  $M$ 에서 시작했습니다. 하지만 우리가 아는 한  $V$ 에서  $\text{CH}$ 가 참일 수도 있으므로( $V = L$ 이라면 어떻겠습니까?), 그렇다면  $M$ 에서도 참일 것입니다.

그럼에도 불구하고, 우리는 대담하게 모델  $M$ 의 확장  $M[G]$ 를 구성합니다. 그것이  $M$ 과 다르게 행동하려면,  $M$ 이 도달할 수 없는 범위에 있어야 합니다. 반대로, 만약  $M$ 이  $M[G]$ 에 대한 모든 것을 계산할 수 있다면,  $M[G]$ 는  $M$ 의 믿음에 순응해야 할 것입니다.

그렇기 때문에 우리는  $G \in M[G]$ 이지만  $G \notin M$ 이 되도록 그토록 애를 썼던 것입니다.

선택하고자 합니다

$$\{q \in \mathbb{P} \mid \exists \langle \tau, r \rangle \in \tau_2 (q \leq r \wedge q \Vdash (\tau = \tau_1))\}$$

$p$  아래에서 조밀합니다. 다시 말해, 만약 그 집합이 조밀하다면, 제네릭은 반드시  $q$ 에 도달해야 하고, 따라서  $r$ 에도 도달해야 하며(필터가 위로 닫혀 있음을 기억하십시오), 이는  $\langle \tau, r \rangle \in \tau_2$ 가  $\tau^G \in \tau_2^G$ 가 되도록 해석될 것이며, 게다가  $q \in G$ 는  $\tau_1 = \tau$ 를 강제할 것임을 의미합니다.

이제 그 정의를 써 내려가 봅시다...이하에서  $\Vdash$ 는  $M$ 과  $\mathbb{P}$ 를 생략합니다.

**정의 93.5.1.**  $M$ 을 ZFC의 가산 추이적 모델이라고 합시다.  $\mathbb{P} \in M$ 을 부분 순서라고 합시다.  $p \in \mathbb{P}$ 와 집합론의 언어로 된 논리식  $\varphi(\sigma_1, \dots, \sigma_n)$ 에 대해, 우리는  $p \Vdash \varphi(\sigma_1, \dots, \sigma_n)$ 을 다음을 의미하는 것으로 쓰며, 이는 논리식의 복잡도와 계수에 대한 귀납법으로 정의됩니다.

(1)  $p \Vdash \tau_1 = \tau_2$ 는 다음을 의미합니다

(i) 모든  $\langle \sigma_1, q_1 \rangle \in \tau_1$ 에 대해, 집합

$$D_{\sigma_1, q_1} := \{r \mid r \leq q_1 \rightarrow \exists \langle \sigma_2, q_2 \rangle \in \tau_2 (r \leq q_2 \wedge r \Vdash (\sigma_1 = \sigma_2))\}.$$

은  $p$  아래에서 조밀합니다. (이는 " $\tau_1 \subseteq \tau_2$ "를 부호화합니다.)

(ii) 모든  $\langle \sigma_2, q_2 \rangle \in \tau_2$ 에 대해, 유사하게 정의된 집합  $D_{\sigma_2, q_2}$ 는  $p$  아래에서 조밀합니다.

(2)  $p \Vdash \tau_1 \in \tau_2$ 는 다음을 의미합니다

$$\{q \in \mathbb{P} \mid \exists \langle \tau, r \rangle \in \tau_2 (q \leq r \wedge q \Vdash (\tau = \tau_1))\}$$

$p$  아래에서 조밀합니다.

(3)  $p \Vdash \varphi \wedge \psi$ 는  $p \Vdash \varphi$ 이고  $p \Vdash \psi$ 임을 의미합니다.

(4)  $p \Vdash \neg \varphi$ 는  $\forall q \leq p$ 에 대해  $q \nVdash \varphi$ 임을 의미합니다.

(5)  $p \Vdash \exists x \varphi(x, \sigma_1, \dots, \sigma_n)$ 는 다음 집합이

$$\{q \mid \exists \tau (q \Vdash \varphi(\tau, \sigma_1, \dots, \sigma_n))\}$$

$p$  아래에서 조밀함을 의미합니다.

이것은  $M$ 에서 정의 가능합니다! 우리가 언급한 것은 오직  $\mathbb{P}$ 와 이름들뿐이며, 이들은  $M$ 에 있습니다. (조밀하다는 것이 정의 가능한 성질임에 주목하십시오.) 사실, 위 정의의 (3)항부터 (5)항까지는 논리식의 복잡도에 대한 귀납법을 사용합니다. 하지만 원자적인 경우인 (1)과 (2)에서는 이름의 계수(rank)에 대한 귀납법을 사용하고 있습니다.

그래서 위의 구성은 한쪽 방향을 제공합니다(엄청나게 많은 세부 사항을 생략했습니다만...).

그렇다면 역방향은 어떻게 얻을 수 있을까요: 즉 어떤 문장이 참인 것과 무언가가 그것을 강제하는 것이 동치라는 사실 말입니다. 사실, 귀납법을 사용하면 다음을 보일 수 있습니다:

#### 보조정리 93.5.2 (일관성과 지속성)

다음이 성립합니다

(1) (일관성)  $p \Vdash \varphi$ 이고  $q \leq p$ 이면  $q \Vdash \varphi$ 입니다.

(2) (지속성)  $\{q \mid q \Vdash \varphi\}$ 가  $p$  아래에서 조밀하면  $p \Vdash \varphi$ 입니다.

이 두 가지는 모두 논리식의 복잡도에 대한 귀납법으로 증명할 수 있습니다. 이로부터 다음을 얻습니다:

### 따름정리 93.5.3 (완전성)

집합  $\{p \mid p \Vdash \varphi \text{ 또는 } p \Vdash \neg\varphi\}$ 는 조밀합니다.

증명. 우리는  $p \nVdash \varphi$ 일 때마다 어떤  $\bar{p} \leq p$ 에 대해  $\bar{p} \Vdash \neg\varphi$ 가 성립함을 주장합니다; 이것이 따름정리를 확립할 것입니다.

앞선 보조정리의 대우에 의해,  $\{q \mid q \Vdash \varphi\}$ 는  $p$  아래에서 조밀하지 않으며, 이는 어떤  $\bar{p} \leq p$ 가 존재하여 모든  $q \leq \bar{p}$ 에 대해  $q \nVdash \varphi$ 가 성립함을 의미합니다.  $p \Vdash \neg\varphi$ 의 정의에 의해,  $\bar{p} \Vdash \neg\varphi$ 입니다.  $\square$

그리고 이로써 역방향이 성립합니다:  $M$ -제네릭  $G$ 는 어느 쪽이든 판정을 내리는 어떤 조건에 반드시 도달해야 합니다. 이것으로 기본 정리의 증명이 완료됩니다.

## §93.6 나머지 공리들

### 정리 93.6.1 (제네릭 확장은 ZFC를 만족합니다)

$M$ 이 ZFC의 추이적 모형이라고 가정합니다.  $\mathbb{P} \in M$ 을 부분순서집합(poset)이라 하고,  $G \subseteq \mathbb{P}$ 를  $M$ -제네릭 필터라 합시다. 그러면

$$M[G] \models \text{ZFC}.$$

증명. 나머지 공리들은 유사하므로, 여기서는 Comprehension만 다루겠습니다.

$\sigma^G, \sigma_1^G, \dots, \sigma_n^G \in M[G]$ 가 집합과 매개변수이고,  $\varphi(x, x_1, \dots, x_n)$ 이 집합론 언어의 논리식이라고 합시다. 우리는 다음 집합이

$$A = \{x \in \sigma^G \mid M[G] \models \varphi[x, \sigma_1^G, \dots, \sigma_n^G]\}$$

$M[G]$ 에 속함을, 즉 그것이 어떤 이름의 해석임을 보이고자 합니다.

$\sigma^G$ 의 모든 원소는 어떤  $\rho \in \text{dom}(\sigma)$ 에 대해  $\rho^G$ 의 풀임에 유의하십시오 (여기서 표기가 다소 남용되었는데,  $\sigma$ 는 이름들과  $p$ 들의 순서쌍 뭉치이고, 정의역  $\text{dom}(\sigma)$ 은 그저 이름들의 집합입니다). 따라서 강제법의 기본 정리에 의해, 우리는 다음과 같이 쓸 수 있습니다

$$A = \{\rho^G \mid \rho \in \text{dom}(\sigma) \text{ 그리고 } \exists p \in G (p \Vdash \rho \in \sigma \wedge \varphi(\rho, \sigma_1, \dots, \sigma_n))\}.$$

$A \in M[G]$ 임을 보이려면 이름  $\tau^G$ 가  $A$ 와 일치하는  $\tau$ 를 명시적으로 써 내려야 합니다. 우리는 다음이

$$\tau = \{\langle \rho, p \rangle \in \text{dom}(\sigma) \times \mathbb{P} \mid p \Vdash \rho \in \sigma \wedge \varphi(\rho, \sigma_1, \dots, \sigma_n)\}$$

올바른 선택이라고 주장합니다. 구성에 의해  $\tau^G = A$ 임은 실제로 명백합니다; "본질적인 내용"은  $\tau$ 가 실제로  $M$ 의 이름임을 보이는 것인데, 이는  $M \models \text{Comprehension}$ 으로부터 따라 나옵니다.

그러므로 사실 강제법의 기본 정리의 요점은 단지 이  $\tau$ 를 명시적으로 쓸 수 있게 해준다는 데 있습니다; 그것은 실제로  $G$ 를 참조하지 않고도  $\tau$ 가  $\text{Name}^M$ 에 속함을 보일 수 있게 해줍니다.  $\square$

### §93.7 생각해 볼 만한 조금 더 어려운 문제

**문제 93A.** 필터  $G$ 와 ZFC의 추이적 모형  $M$ 에 대해,  $M[G] \models \text{Union}$ 임을 보이십시오.

**문제 93B** (Rasiowa-Sikorski 보조정리). ZFC의 가산 추이적 모형  $M$ 에서는 임의의 부분 순서 집합 위에서  $M$ -제네릭 필터를 찾을 수 있음을 보이십시오.



# 94 연속체 가설 깨뜨리기

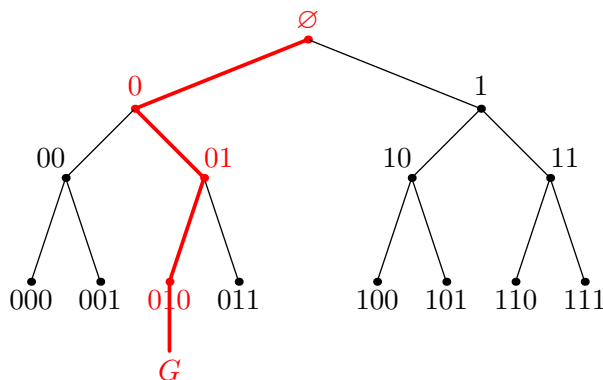
이제 좋은 반순서 집합  $\mathbb{P}$ 를 선택함으로써 강제법 기법을 사용하여 연속체 가설을 깨뜨립니다. 앞서 언급했듯이, 연속체 가설이 참이 되는 모형을 만들 수도 있는데, 이를 구성 가능 전체  $L$ 이라고 부릅니다. 하지만 저는 무언가가 깨질 때가 더 재미있다고 생각합니다...

## §94.1 실수 추가하기

가산 추이적 모형  $M$ 에서 시작합니다.

$(\aleph_2)^M$ 개의 실수가 나타나도록  $\mathbb{P} \in M$ 을 선택하고, 기수 붕괴는 나중에 걱정하고자 합니다.

$\mathbb{P}$ 를 무한 완전 이진 트리로 설정했던 앞의 상황을 떠올려 봅시다. 이 트리의 노드는 부분 함수  $n \rightarrow 2$  (단,  $n < \omega$ )로 생각할 수 있습니다. 그러면  $G$  자체는 이 트리를 따라 내려가는 경로이며, 즉 전함수  $G: \omega \rightarrow 2$ 로 부호화될 수 있고 하나의 실수에 대응됩니다.



이와 비슷한 것을 하고 싶지만, 하나가 아니라  $\omega_2$ 개의 실수로 하고자 합니다. 이를 염두에 두고  $M$ 에서 다음의 반순서 집합을 생각해 봅시다

$$\mathbb{P} = \text{Add}(\omega, \omega_2) := (\{p: \omega_2 \times \omega \rightarrow 2, \text{dom}(p) \text{ 유한합니다}\}, \supseteq).$$

이 원소  $p$ (조건)들은 "부분 함수"로서,  $\omega_2 \times \omega$ 의 어떤 유한 부분집합을 취하여 이를  $2 = \{0, 1\}$ 로 사상하는 것입니다. (여기서  $\text{dom}(p)$ 는  $p$ 의 정의역을 나타내며, 이는 앞서 언급한  $\omega_2 \times \omega$ 의 유한 부분집합입니다.) 또한,  $\text{dom}(p) \supseteq \text{dom}(q)$ 이고 두 함수가  $\text{dom}(q)$  위에서 일치할 때  $p \leq q$ 라고 말합니다.

**질문 94.1.1.** 여기서 최대 원소  $1_{\mathbb{P}}$ 는 무엇입니까?

**연습문제 94.1.2.** 제네릭  $G$ 가 함수  $\omega_2 \times \omega \rightarrow 2$ 로 부호화될 수 있음을 보이십시오.

**보조정리 94.1.3** ( $G$ 는 서로 다른 실수들을 부호화합니다)

$\alpha \in \omega_2$ 에 대해 다음과 같이 정의합니다

$$G_\alpha = \{n \mid G(\alpha, n) = 0\} \in \mathcal{P}(\mathbb{N}).$$

그러면  $\alpha \neq \beta$ 인 임의의  $\alpha, \beta$ 에 대해  $G_\alpha \neq G_\beta$ 입니다.

증명. 다음 집합이

$$D = \{q \mid \exists n \in \omega : q(\alpha, n) \neq q(\beta, n) \text{ 둘 다 정의됩니다}\}$$

조밀하다고 주장합니다.

**질문 94.1.4.** 이를 확인하십시오. (정의역이 모두 유한하다는 사실을 이용하십시오.)

$G$ 는  $M$ -제네릭이므로 이 조밀 집합  $D$ 와 만납니다. 따라서  $G_\alpha \neq G_\beta$ 입니다.  $\square$

$G \in M[G]$ 이고  $M[G] \models \text{ZFC}$ 이므로, 각  $G_\alpha$ 가  $M[G]$ 에 속함을 알 수 있습니다. 따라서  $M[G]$ 에는 적어도  $\aleph_2^M$ 개의 실수가 존재합니다. 기수 붕괴가 없음을 보이기만 하면 끝납니다.

## §94.2 가산 사슬 조건

$\mathbb{P} = \text{Add}(\omega, \omega_2)$ 일 때 다음을 보이는 일이 남아 있습니다

$$\aleph_2^{M[G]} = \aleph_2^M.$$

그 경우,  $M[G]$ 는  $\aleph_2^M = \aleph_2^{M[G]}$ 개의 실수를 갖게 되므로, 이로써 증명이 끝납니다.

이를 위해  $\mathbb{P}$ 의 다음과 같은 조합적 성질에 의존하고자 합니다:

**정의 94.2.1.**  $A \subseteq \mathbb{P}$ 의 서로 다른 임의의  $p$ 와  $q$ 에 대해  $p \perp q$ 일 때,  $A$ 를 **강한 반사슬**이라고 말합니다.

### 예제 94.2.2 (반사슬의 예)

무한 이진 트리에서, 집합  $A = \{00, 01, 10, 11\}$ 은 강 반사슬(strong antichain)입니다 (사실은 포함관계에 대해 극대입니다).

이것은 여러분에게 익숙한 "반사슬(antichain)"이라는 개념보다 더 강한 조건입니다!<sup>1</sup> 우리는 단지 모든 두 원소가 비교 불가능하다는 것만을 요구하는 것이 아니라, 그것들이 실제로 양립 불가능(*incompatible*)하다는 것을 요구합니다.

**질문 94.2.3.** 유한 순서집합과 그 안에서 강하지 않은 반사슬을 그려 보십시오.

**질문 94.2.4.** 무한 이진 트리에서의 모든 반사슬은 강 반사슬이지만, 위에서 정의한 순서집합  $\mathbb{P}$ 에서는 강하지 않은 반사슬이 존재함을 스스로 확인해 보십시오.

**정의 94.2.5.** 순서집합  $\mathbb{P}$ 가  $\kappa$ -**사슬 조건**을 갖는다는 것은 (여기서  $\kappa$ 는 기수)  $\mathbb{P}$ 의 모든 강 반사슬이  $\kappa$ 보다 작은 크기를 가짐을 의미합니다. 특수한 경우  $\kappa = \aleph_1$ 은 **가산 사슬 조건**이라고 불리는데, 이는 모든 강 반사슬이 가산집합임을 함의하기 때문입니다.

**비고 94.2.6 (표기법에 대한 여담: 왜  $\leq$  대신  $<$ 를 쓸까요?)** — 우리는 순서집합  $\mathbb{P}$ 가  $\kappa$ -사슬 조건을 갖는다는 것을,  $\mathbb{P}$ 의 모든 강 반사슬이  $< \kappa$ 인 크기를 갖는 것으로 정의할 수도 있었습니다. 그럼에도 불구하고, 이 대안적 정의는 활용도가 떨어집니다 — 예를 들어,  $\mathbb{P}$ 의 모든 강 반사슬이 유한하다는 것을 표현할 방법이 없게 됩니다!

<sup>1</sup>강제법(forcing)의 맥락에서, 일부 저자들은 "반사슬"이라는 용어를 "강 반사슬"을 가리키는 데 사용합니다. 저는 이것이 별로라고 생각합니다.

우리는 순서집합이  $\kappa$ -사슬 조건을 가지면  $\geq \kappa$ 인 모든 기수를 보존함을 보일 것입니다. 특히, 가산 사슬 조건은  $\mathbb{P}$ 가 모든 기수를 보존함을 보여줄 것입니다. 그런 다음,  $\text{Add}(\omega, \omega_2)$ 가 실제로 이 성질을 가짐을 보일 것입니다. 이로써 증명이 완성됩니다.

유용한 보조정리를 하나 분리해 냅니다:

#### 보조정리 94.2.7 (가능한 값 논법)

$M$ 이 ZFC의 추이적 모형이고  $\mathbb{P}$ 가 부분 순서 집합이며, 이  $\mathbb{P}$ 가  $M$ 에서  $\kappa$ -사슬 조건을 만족한다고 합시다.  $X, Y \in M$ 이라 하고,  $f: X \rightarrow Y$ 가  $M[G]$ 에서의 어떤 함수이지만  $f \notin M$ 이라고 합시다.

그러면  $F \in M$ 이고  $F: X \rightarrow \mathcal{P}(Y)$ 인 함수  $F$ 가 존재하여, 임의의  $x \in X$ 에 대해 다음을 만족합니다,

$$f(x) \in F(x) \quad \text{그리고} \quad |F(x)|^M < \kappa.$$

이것이 말하는 바는,  $f$ 가 새로 생성된 어떤 함수라고 할 때,  $M$ 은 여전히  $f$ 의 값들을  $\kappa$ 보다 적은 수의 값으로 제한할 수 있다는 것입니다.

증명. 증명의 아이디어는 간단합니다:  $f$ 의 가능한 값 각각은 그것을 강제하는 순서집합  $\mathbb{P}$  내의 어떤 조건을 우리에게 제공합니다. 서로 다른 값들은 양립 불가능한 조건을 가져야 하므로,  $\kappa$ -사슬 조건은 그러한 값이 최대  $\kappa$ 개임을 보장합니다.

세부 사항은 다음과 같습니다.  $\dot{f}$ ,  $\dot{X}$ ,  $\dot{Y}$ 를 각각  $f$ ,  $X$ ,  $Y$ 의 이름이라고 합시다.  $p$ 가 다음 문장을 강제하는 조건  $p$ 에서 시작합니다

“ $\dot{f}$ 는  $\dot{X}$ 에서  $\dot{Y}$ 로 가는 함수입니다”.

우리는 바로 아래 지점에서부터 작업할 것입니다.

각  $x \in X$ 에 대해, (선택 공리를 사용하여)  $f(x)$ 가 어떤 값  $y \in Y$ 와 같음을 강제하는,  $q \leq p$ 인 양립 불가능한 조건들의 극대 강 반사슬  $A(x)$ 를 생각할 수 있습니다. 그런 다음,  $F(x)$ 가 그 결과로 나온 모든  $y$ -값들을 모은 것이라고 합시다. 이것들이 모든 가능한 값이며, 그 개수는  $\kappa$ 보다 적습니다.  $\square$

## §94.3 기수의 보존

앞서 보았듯이, 기수 붕괴는 여전히 일어날 수 있습니다. 연속체 가설을 위해서는 이러한 가능성을 피하고자 하므로,  $\aleph_2^M$ 개의 실수를 추가하면서도  $\aleph_2^{M[G]} = \aleph_2^M$ 이 성립하도록 할 수 있습니다. 이를 확인하기 위해서는 더 약한 결과를 확인하면 충분하다는 것이 밝혀져 있습니다.

**정의 94.3.1.**  $M$ 이 ZFC의 추이적 모형이고  $\mathbb{P} \in M$ 이 순서집합일 때,  $\mathbb{P}$ 가 **기수를 보존한다**는 것은,  $\mathbb{P}$ 에 대한 임의의  $M$ -생성 필터  $\forall G \subseteq \mathbb{P}$ 에 대해, 모형  $M$ 과  $M[G]$ 가 모든  $\kappa$ 에 대해 “ $\kappa$ 는 기수이다”라는 문장에 대해 일치함을 의미합니다. 마찬가지로  $\mathbb{P}$ 가 **정칙 기수를 보존한다**는 것은,  $M$ 과  $M[G]$ 가 모든  $\kappa$ 에 대해 “ $\kappa$ 는 정칙 기수이다”라는 문장에 대해 일치함을 의미합니다.

직관: 모형  $M$ 에서는,  $V$ 에서는 전단사 관계에 있는 두 기수가  $M$ 에서는 더 이상 전단사 관계에 있지 않을 수 있습니다. 마찬가지로,  $\kappa \in M$ 인 어떤 기수가 정칙일 수 있지만,  $V$ 에서는  $f: \bar{\kappa} \rightarrow \kappa$ 인 어떤 공종 함수가  $V$ 에만 존재하게 되어 정칙성을 잃을 수도 있습니다. 다시 말하면, “ $\kappa$ 는 정칙 기수이다”라는 것 역시  $\Pi_1$  문장임이 드러납니다.

다행히도 각각은 서로를 함의합니다. 다음을 증명 없이 인용합니다.

**명제 94.3.2** (기수 보존  $\iff$  정칙 기수 보존)

$M$ 을 ZFC의 추이적 모형이라고 합시다.  $\mathbb{P} \in M$ 을 순서집합이라고 합시다. 그러면 임의의  $\lambda$ 에 대해,  $\mathbb{P}$ 가  $\lambda$  이하의 기수를 보존하는 것은  $\mathbb{P}$ 가  $\lambda$  이하의 정칙 기수를 보존하는 것과 동치입니다. 나아가 “이하”를 “이상”으로 바꾸어도 동일한 결과가 성립합니다.

따라서,  $\mathbb{P}$ 가 기수성과 공종성을 보존함을 보이려면  $\mathbb{P}$ 가 정칙성을 보존함을 보이는 것으로 충분합니다. 다음 정리가 이를 가능하게 해 줍니다:

**정리 94.3.3** (사슬 조건은 정칙 기수를 보존합니다)

$M$ 을 ZFC의 추이적 모형이라 하고,  $\mathbb{P} \in M$ 을 포셋이라 하십시오.  $M$ 이 “ $\mathbb{P}$ 는  $\kappa$ -사슬 조건을 가지며  $\kappa$ 는 정칙이다”라는 문장을 만족한다고 가정하십시오. 그러면  $\mathbb{P}$ 는  $\kappa$  이상의 정칙성을 보존합니다.

증명. 가능값 논법을 사용하십시오. **문제 94A.** □

특히,  $\mathbb{P}$ 가 가산 사슬 조건을 가진다면  $\mathbb{P}$ 는 모든 기수(그리고 공종성)를 보존합니다. 따라서  $\text{Add}(\omega, \omega_2)$ 가 가산 사슬 조건을 만족함을 보이는 것만 남았습니다.

**§94.4 무한 조합론**

이제  $\text{Add}(\omega, \omega_2)$ 가 가산 사슬 조건을 만족함을 증명하겠습니다. 이는 순전히 조합론적이므로 간략히 다루겠습니다.

**정의 94.4.1.**  $C$ 를 유한 집합들의 비가산 모임이라 하십시오.  $C$ 의 임의의 서로 다른  $X$ 와  $Y$ 에 대해  $X \cap Y = R$ 이 되는 **균**  $R$ 이 존재하면  $C$ 를  **$\Delta$ -시스템**이라 합니다.

**보조정리 94.4.2** ( $\Delta$ -시스템 정리)

$C$ 가 유한 집합들의 비가산 모임이라고 가정합니다. 그러면  $\exists \bar{C} \subseteq C$ 가 성립하여  $\bar{C}$ 는 비가산  $\Delta$ -시스템이 됩니다.

증명.  $C$ 가 길이  $n$ 인 원소를 비가산 개만큼 가지는 정수  $n$ 이 존재합니다. 따라서 나머지 집합들은 모두 버리고,  $C$ 의 모든 집합이 크기  $n$ 이라고 가정할 수 있습니다.

이제  $n$ 에 대한 귀납법으로 진행하겠습니다. 기저 사례  $n = 1$ 은 자명한데,  $R = \emptyset$ 을 취하면 되기 때문입니다. 귀납 단계에서는 두 가지 경우를 고려합니다.

먼저, 비가산 개의  $F \in C$ 에 속하는 원소  $a$ 가 존재한다고 가정하십시오. 나머지는 모두 버리십시오. 그러면  $a$ 를 그냥 삭제하고 귀납 가정을 적용하면 됩니다.

이제 모든  $a$ 에 대해,  $C$ 의 원소 중  $a$ 를 포함하는 것이 가산 개뿐이라고 가정하십시오. 이 경우  $R = \emptyset$ 인  $\bar{C}$ 까지도 얻을 수 있다고 주장합니다. 먼저  $F_0 \in C$ 를 하나 고르십시오.  $F_1 \cap F_0 = \emptyset$ 이 되는  $F_1$ 을 구성하는 것은 어렵지 않습니다. 그리고  $F_2, F_3, \dots$ 도 마찬가지로 구성할 수 있습니다. □

**보조정리 94.4.3**

모든  $\kappa$ 에 대해,  $\text{Add}(\omega, \kappa)$ 는 가산 사슬 조건을 만족합니다.

증명. 그렇지 않다고 가정하십시오. 다음을 두겠습니다

$$\{p_\alpha \mid \alpha < \omega_1\}$$

강한 반사술이라 하겠습니다. 다음을 두겠습니다

$$C = \{\text{dom}(p_\alpha) \mid \alpha < \omega_1\}.$$

$\bar{C} \subseteq C$ 를  $\bar{C}$ 가 비가산이고  $\bar{C}$ 가 근  $R$ 을 갖는  $\Delta$ -시스템이 되도록 잡습니다. 그러면 다음과 같이 둡니다:

$$B = \{p_\alpha \mid \text{dom}(p_\alpha) \in \bar{C}\}.$$

각  $p_\alpha \in B$ 는 함수  $p_\alpha \upharpoonright R: R \rightarrow \{0, 1\}$ 로 제한되므로, 서로 같은 두 개가 존재합니다.  $\square$

따라서 우리는 연속체 가설이 ZFC에서 증명될 수 없음을 증명했습니다.

## §94.5 생각해 볼 만한 조금 더 어려운 문제

**문제 94A.**  $M$ 을 ZFC의 추이적 모델이라 하고,  $\mathbb{P} \in M$ 을 포셋이라 하십시오.  $M$ 이 " $\mathbb{P}$ 는  $\kappa$ -사슬 조건을 가지며  $\kappa$ 는 정칙이다"라는 문장을 만족한다고 가정하십시오.  $\mathbb{P}$ 가  $\kappa$  이상의 정칙성을 보존함을 보이십시오.



# XXIII

## 부록

## 제XXIII부: 목차

---

|          |                          |             |
|----------|--------------------------|-------------|
| <b>A</b> | <b>교육적 논평과 참고 문헌</b>     | <b>995</b>  |
| A.1      | 기초 대수학과 위상수학 . . . . .   | 995         |
| A.2      | 2학년 주제 . . . . .         | 996         |
| A.3      | 고급 주제 . . . . .          | 997         |
| A.4      | Napkin에 없는 주제들 . . . . . | 998         |
| <b>B</b> | <b>선정된 문제들에 대한 힌트</b>    | <b>999</b>  |
| <b>C</b> | <b>선정된 풀이의 개요</b>        | <b>1011</b> |
| <b>D</b> | <b>표기법 용어집</b>           | <b>1037</b> |
| D.1      | 일반 . . . . .             | 1037        |
| D.2      | 함수와 집합 . . . . .         | 1037        |
| D.3      | 추상대수학과 선형대수학 . . . . .   | 1038        |
| D.4      | 양자 계산 . . . . .          | 1039        |
| D.5      | 위상수학과 실/복소 해석학 . . . . . | 1039        |
| D.6      | 측도론과 확률론 . . . . .       | 1040        |
| D.7      | 대수적 위상수학 . . . . .       | 1040        |
| D.8      | 범주론 . . . . .            | 1041        |
| D.9      | 미분기하학 . . . . .          | 1042        |
| D.10     | 대수적 수론 . . . . .         | 1042        |
| D.11     | 표현론 . . . . .            | 1043        |
| D.12     | 대수기하학 . . . . .          | 1044        |
| D.13     | 집합론 . . . . .            | 1045        |
| <b>E</b> | <b>집합과 함수에 관한 용어</b>     | <b>1047</b> |
| E.1      | 집합 . . . . .             | 1047        |
| E.2      | 함수 . . . . .             | 1048        |
| E.3      | 동치 관계 . . . . .          | 1050        |

---

# A

## 교육적 논평과 참고 문헌

여기서는 특정 주제가 서술된 방식에 대한 더 높은 수준의 논평과 더불어, 추가 읽을거리에 대한 안내를 제공합니다.

### §A.1 기초 대수학과 위상수학

#### §A.1.i 선형대수학과 다변수 미적분학

절 9.9의 논평에 이어, 저는 선형대수학과 다변수 미적분학의 대다수 서술 방식을 좋아하지 않는데, 그 이유는 이들이 두 가지 핵심 아이디어를 놓치고 있기 때문입니다. 즉:

- 선형대수학에서 우리는 공간 사이의 선형 사상을 연구합니다.
- 미적분학에서 우리는 함수를 각 점에서 선형 함수로 근사합니다.

따라서 저는 선형대수학이 다변수 미적분학보다 항상 먼저 가르쳐져야 한다고 생각합니다. 특히 저는 대부분의 선형대수학이나 다변수 미적분학 책을 추천하지 않습니다.

선형대수학에 관해서는, [Ax97]가 이러한 접근법을 따른다고 들었는데, 그래서 "Linear Algebra Done Right"라는 적절한 이름이 붙었습니다. 저는 Math 55a의 강의록을 크게 수정하여 따랐습니다. [Ga14]를 참고하십시오.

다변수 미적분학과 미분기하학에 관해서는, [Sj05] 노트가 유난히 잘 쓰여졌다고 느꼈습니다. 저는 Math 55b [Ga15]를 수강하는 동안 이를 자주 참고했습니다.

#### §A.1.ii 일반위상수학

공간에 대한 저의 개인적인 견해는, 제가 다루는 모든 공간이 거리화 가능하거나 자리스키 위상이라는 것입니다.

저는 [Pu02]의 접근법을 채택하여, 거리 위상수학을 먼저 사용합니다. 저는 거리 공간이 훨씬 더 직관적이며, 열린/닫힌/콤팩트 등의 집합이 어떤 모습인지에 대한 그림을 얻는 데 훨씬 더 나은 방법이라고 생각합니다. 이는 역사가 밝아온 접근법입니다. 일반위상수학은 거리 위상수학으로부터 성장했습니다.

저는 개인적으로 일반적인 위상 공간이 무엇인지를 정의하는 것으로 일반위상수학 수업을 시작하는 것을 좋아하지 않는데, 이는 그림을 그려볼 열린집합과 닫힌집합에 대한 좋은 그림을 전달하지 못하기 때문입니다.

#### §A.1.iii 군과 가환대수학

저는 가환환보다 군을 먼저 가르치지만 나중에 바꿀 수도 있습니다. 환은 더 좋은 예시를 가지고 있고, 덧셈 군에 대한 곱셈 표기법의 혼동이 없으며, 아이디얼로 나누는 것이 더 직관적입니다.

군론에서 제가 못마땅하게 여기는 특정한 사항이 하나 있습니다: 바로 정규 부분군이라는 개념이 도입되는 방식입니다. 오직 [Go11]만이 제가 하는 것과 비슷한 방식을 취합니다. 대부분의 다른 사람들은 그저 정규 부분군  $N$ 을  $gNg^{-1}$ 를 만족하는 것으로 정의하고 나서 이 정의가 어디서 비롯되었는지 설명하는 시간을 들이지 않은 채 몫을 정의하는 것으로 넘어갑니다. 저는 이 개념을 수학을 배우면서 무슨 일이 일어나고 있는지 이해하지 못했던 첫 순간으로 뚜렷이 기억합니다. 돌이켜보아야 비로소 이 정의가 어디서 비롯되었는지 알게 되었으며, 저는 제 자신의 서술 방식에는 이러한 문제가 없도록 애를 썼습니다.

저는 환과 아이디얼에 관한 장을 제외하고는, 오직 가환대수학만을 다루는 장을 의도적으로 포함하지 않았습니다. 그 이유는 저 자신이 대수적 정수론이나 대수기하학 같은 것의 맥락 속에서 가환대수학 정리들을 즉석에서 배우는 것이 항상 더 쉽다고 느꼈기 때문입니다. 예를 들어, 저는 근기(radical)와 힐베르트 영점 정리(Nullstellensatz)가 왜 중요했는지를 대수기하학에서 이들이 어떻게 쓰이는지 보고 나서야 비로소 이해했습니다. 그 전까지는 제가 왜 이것들을 신경 써야 하는지 전혀 이해하지 못했습니다.

### §A.1.iv 미적분학

저는 거리 위상수학과 일반위상수학을 주된 재료로 삼아 실해석학을 다루는데, 이것이 이후에 가장 유용하고 가장 깨우침을 준다고 생각하기 때문입니다. 어떤 의미에서 저는 여전히 [Pu02]를 따르고 있습니다.

## §A.2 2학년 주제

### §A.2.i 측도론과 확률론

이 강의들의 주된 영감은 MIT에서 개설된 Vadim Gorin의 18.175 강의입니다. [Go18]에는 Tony Zhang이 작성한 정말 좋은 강의록이 실려 있습니다. 저는 측도론에 대해서는 조금 더 자세히 다루고, (현재로서는) 확률론에 대해서는 덜 다룹니다. 하지만 저는 확률론이 어쨌든 측도론에 동기를 부여하는 훌륭한 방법이라고 생각하며, 반대로 이는 중심극한정리 같은 것을 진술하기에 적절한 배경이기도 합니다.

저는 또한 [Ch08]가 또 다른 참고 자료로서 상당히 도움이 된다고 느꼈습니다.

### §A.2.ii 복소해석학

저는 코시-구르사 정리를 (슈토크스 정리를 이용해 더 약한 버전을 증명하는 등의 방법 대신) 주어진 것으로 제시한 뒤, 이로부터 정칙 함수가 해석적이라는 핵심 결과를 유도하는 접근법을 선택했습니다. 이 방식이 복소해석학의 “실생활” 활용, 즉 등고선 적분의 계산을 가장 근접하게 반영한다고 생각합니다.

이 장의 주된 참고문헌은 [Ya12]이며, 이를 추천합니다.

### §A.2.iii 범주론

제 장들의 바탕이 된 [Le14]를 적극 추천하며, 이 책은 제가 다룰 시간이 있었던 것보다 훨씬 많은 내용을 담고 있습니다.

다만 2-4장은 역순으로 읽어보셔도 좋을 것입니다: 저는 극한이 딸림 함자보다 훨씬 직관적이라고 느꼈습니다. 하지만 사람마다 다를 수 있습니다.

구조의 예시를 더 많이 배울수록 범주론이 더 이해가 될 것입니다: 예를 들어 군, 환, 가군에 관한 장들을 읽어두면 도움이 될 것입니다.

### §A.2.iv 양자 알고리즘

여기서 제시하는 내용은 세스 로이드가 MIT에서 한 학기 전체에 걸쳐 강의한 18.435J [Li15]를 바탕으로 합니다. 훨씬 더 수학적인 관점에서 서술되어 있습니다.

저는 유한 차원 힐베르트 공간만을 다루는데, 이는 이 장의 목적인 쇼어 알고리즘에 필요한 것이 그것뿐이기 때문입니다. 이는 양자역학을 진지하게 공부하고자 하는 사람을 위한 해설이 아닙니다(다만 첫 입문서로는 적절할 수도 있습니다): 주된 목적은 학생들에게 모두가 계속 이야기하는 이 “쇼어 알고리즘”이 무엇인지에 대한 작은 이해를 주는 것입니다.

## §A.2.v 표현론

저는 대수의 표현을 먼저 가르친 뒤  $k[G]$ 를 살펴봄으로써 군의 경우로 특수화하는 방식을 강력히 지지합니다. 여기 있는 장들의 주된 영향은 [Et11]이며, 여기 있는 내용을 이 자료의 처음 네 장에서 발췌한 일부라고 생각하셔도 좋습니다.

## §A.2.vi 집합론

집합론은 일반적인 경로에서 크게 벗어나 있습니다. 제가 작성한 노트는 하버드 칼리지에서 수강한 Math 145a [Ko14] 수업을 바탕으로 합니다.

제가 집합론을 제시하는 방식(논리의 지뢰밭 속에서 직관적이고 비형식적인 태도를 유지하려는 시도)이 표준적이지 않다는 것이 제 전반적인 인상입니다. 다른 참고문헌으로는 [Mi14]가 가능할 것입니다.

## §A.3 고급 주제

### §A.3.i 대수적 위상수학

저는 기본군  $\pi_1$ 을 먼저 다루는데, 이 방식이 더 직관적이라고 생각하기 때문입니다. 이 주제에 관한 참고문헌으로는 [Mu00]가 가능할 것입니다. 그보다 훨씬 복잡한 호몰로지 군은 나중에야 다룹니다. 대수적 위상수학에서 유명한 표준 참고문헌은 [Ha02]이며, 요즘 거의 모든 사람이 사용하는 자료입니다. 하지만 저는 [Ma13a]도, 특히 코호몰로지 환에 관한 부분에서 매우 유용하다고 느꼈습니다.

저는 사실 대수적 위상수학을 그리 많이 다루지는 않습니다. 특히, 대수적 위상수학을 배우는 주된 이유는 사슬 복합체로부터 호몰로지 군과 코호몰로지 군이 구성되는 과정을 보고, 긴 완전열이 작동하는 모습을 관찰하는 데 있다고 생각합니다. (공)사슬 복합체의 개념은 층의 코호몰로지나 갈루아 코호몰로지처럼 다른 맥락에서도 자주 등장합니다. 대수적 위상수학은 단연 가장 자연스러운 경우입니다.

저는 범주를 사랑하는 사람으로서 범주론을 광범위하게 사용합니다.

### §A.3.ii 대수적 정수론

저는 [Og10]로부터 배웠으며, 체보타랴프 밀도 정리에 관한 부분은 [Le02]를 사용했습니다.

가능한 경우 저는 대수적 정수론 장을 “올림피아드 정신”에 가깝게 유지하려고 노력합니다.  $\mathbb{Z}[i]$ 와  $\mathbb{Z}[\sqrt{-5}]$  같은 환에서의 인수분해는 그 본질에 있어 매우 올림피아드적인 색채를 띠는 주제입니다: 이로부터 자연스럽게 일반적인 정수환에서의 인수분해라는 개념으로 이어지며, 이 서술은 바로 그 개념을 중심으로 구성되어 있습니다. 지금까지 쌓아온 모든 내용에 대한 보상으로, 이 해설은 체보타랴프 밀도 정리를 IMO 2003 6번 문제에 적용하는 것으로 마무리됩니다.

### §A.3.iii 대수기하학

제가 대수기하학을 처음 접할 때 선호하는 입문서는 처음 읽을 때는 [Ga03]이고, 본격적인 버전으로는 [Va17]입니다. 두 강의노트 모두 본질적으로 자기완결적입니다.

지금 고백하자면 저는 대수기하학을 비교적 잘 알지 못하며, 개인적인 의견으로는 대수기하학 부분이 Napkin에서 가장 취약한 부분입니다. 이는 여기서의 작업에도 반영되어 있습니다. 전체 노트에서 저는 이 분야의 첫 번째 핵심 정의인 스킴의 정의를 겨우 마무리하는 데 그칩니다.

그럼에도 불구하고, 저는 무모하게도 제 자신의 학습 경험에 대해 몇 가지 의견을 말해보고자 합니다. 저는 스킴 연구를 시작하는 데 크게 세 가지 접근법이 있다고 생각합니다.

- 전형적인 학부 과정과 같은 “입문” 수업의 일환으로, 아핀 및 사영 다양체만을 살펴보는 방법.
- 아핀 및 사영 다양체를 자세히 공부하여 이를 스킴의 동기가 되는 예시로 사용한 다음, 거기서부터 대수기하학을 전개해 나가는 방법.
- 널리 인정받으면서도 도전적인 [Va17]에서처럼, 스킴의 정의로 곧바로 뛰어드는 방법.

저는 두 번째 접근법을 택했습니다. 저는 스킴이 무엇인지 모른다면 대수기하학을 배운 것이 아니라고 생각합니다. 하지만 다른 한편으로는, 먼저 다양체를 잘 파악하지 않은 상태에서 스킴의 정의를 소화하기 어렵다고 생각합니다.

이러한 의견들은 제가 1년에 걸쳐 세 가지 접근법 모두를 통해 이 분야를 배우려 시도했던 개인적인 경험에 근거한 것입니다. 여러분의 경험은 다를 수 있습니다.

저는 적어도 두 번째 부분에서는 주로 아핀 스킴에 집중하기로 결정했습니다. 이들은 이미 여러 방식으로 다양체를 일반화하고 있으며, 스킴들을 곧바로 접합하기 시작하면 그 도약이 너무 크다고 생각합니다. 저는 학생이 국소적으로 아핀이지만(아마도 그 자체로는 아핀이 아닐) 일반적인 스킴  $X$ 를 다루는 세계로 나아가기 전에, 먼저 아핀 스킴이 어떻게 작동하는지를 정말로 이해했다고 느끼기를 바랍니다. 아핀 스킴의 수많은 예시들에 전적으로 할애된 장은 바로 이 점을 암시합니다.

### §A.3.iv 리만 곡면

제 친구는 [Mi95]를 추천합니다. 이 책의 서문은 다음과 같습니다.

하지만 저는 (대수기하학의 관점에서 볼 때) 주된 예시들이 사영 곡선에서 나온다는 점을 강조하고자 하며, 텍스트는 서서히 그러나 확실하게 대수적 범주로 발전하여, 리만-로흐 정리의 대수적 증명으로 절정에 이릅니다. 아벨의 정리를 위해 해석적 측면으로 돌아온 뒤, 층과 코호몰로지를 논의할 때 이 진행이 다시 반복됩니다. 즉 먼저 해석적 범주, 그다음 대수적 범주 순입니다.

따라서 이 책은 대수기하학을 배우는 자료로도 활용하실 수 있습니다.

때때로 인자, 평면 곡선에 유도된 복소 구조, 혹은 선다발과 같은 몇몇 개념들은 그다지 동기가 잘 설명되어 있지 않습니다. 이러한 경우 저희는 Napkin에서 그 동기를 명확히 설명하고자 노력합니다.

## §A.4 Napkin에 없는 주제들

### §A.4.i 해석적 정수론

저는 이에 대한 노트를 Napkin에 작성할 시간이 없었습니다. 그래도 관심이 있으시다면 [Hi13]를 추천합니다. 이 책은 매우 접근하기 쉽고 읽기에 즐겁습니다. 유일한 실질적인 선행 지식은 코시의 유수 공식에 대한 확실한 이해입니다.

# B 선정된 문제들에 대한 힌트

- 1A. 위수.
- 1B. 보조정리 1.2.5을 사용하여 페르마의 소정리의 증명을 그대로 따라 해보십시오.
- 1C. 전자의 경우, 동형사상이  $r$ 과  $s$ 를 어디로 보내야 하는지 정하면 나머지는 자연스럽게 따라옵니다. 후자의 경우, 위수를 살펴보십시오.
- 1D\*. 생성된 군.
- 1F<sup>†</sup>.  $n = |G|$ 를 사용하십시오.
- 1G. 하한을 위해서는 위수를 고려하십시오(1009가 소수임에 유의하십시오). 상한을 위해서는 정1009각형을 고려하십시오.
- 1H.  $D_6$ 에서 영감을 얻으십시오.
- 1I. 행렬식이  $\pm 1$ 인  $p$  법  $2 \times 2$  행렬들의 군을 살펴봅시다.
- 2B. 아닙니다.  $\mathbb{Q}$ 에서  $\mathbb{N}$ 으로 가는 연속인 단사 사상조차 존재하지 않습니다.
- 2C. 이는 직접 손으로 해도 되고, 합성을 이용해도 됩니다.
- 2D. 적절히 선택한  $\pm$ 에 대한  $\pm x$ 입니다.
- 2E. 틸을  $y$ 축에 사영하십시오. 비가산 개의 양의 실수는 유한한 합을 가질 수 없다는 사실을 이용하십시오.
- 2F. 먼저 다음 질문에 답해 봅시다: " $1/x$ 는 함수인가?".
- 3A. 풀어써 보십시오:  $\phi(ab) = \phi(a)\phi(b)$ .
- 3B. 그렇습니다, 아닙니다.
- 3C. 아닙니다.
- 3D.  $\gcd(1000, 999) = 1$ .
- 3F. 위수 8인 예를 찾으십시오.
- 3G.  $G$ 가 위수 18인 이면체군임을 보이려고 시도해 봅시다. 여기에는 군론적 내용이 많지 않으며 — 단지 계산일 뿐입니다.
- 3H. 영어 동음이의어 목록을 하나 구해 보십시오. 너무 애쓰지는 마십시오. 문자  $v$ 가 가장 까다로운데, 아마  $felt = veldt$ 일 것입니다.
- 4A.  $R = \mathbb{R}[i]$ .
- 4B. 다음 사상이

$$\begin{aligned}\mathbb{C}[x] &\rightarrow \mathbb{C} \times \mathbb{C} \\ p &\mapsto (p(0), p(1))\end{aligned}$$

전사임을 보이고 그 핵을 계산하십시오.

- 4E. (b)의 경우 준동형사상은  $\psi(x) \in R$ 의 선택에 의해 유일하게 결정됩니다
- 5A. 그렇습니다.
- 5B. 핵은  $K$ 의 아이디얼입니다!
- 5C\*. 이는 그저 정의를 따라가는 것입니다.
- 5D\*. 페르마의 소정리 유형의 논증입니다. 정역에서는 소거 법칙이 성립합니다.
- 5E\*. 원소를 계속 추가해 나가면 오름 사슬을 얻을 수 있습니다.
- 5F. 둘 다 PID라는 사실을 이용하십시오.
- 5G<sup>†</sup>. 몫  $\mathbb{Z}[\sqrt{2017}]/I$ 가 임의의 0이 아닌 소 아이디얼  $I$ 에 대해 유한개의 원소를 가짐을 보이십시오. 따라서 이 몫은 정역이며, 또한 체이기도 하므로,  $I$ 는 극대 아이디얼이었습니다.
- 6A<sup>†</sup>. 주된 과제는不動점이 존재함을 보이는 것입니다. 어떤 점  $x_0$ 에서 시작하여 수열  $x_1 = T(x_0)$ ,  $x_2 = T(x_1)$ ,  $x_3 = T(x_2)$ , ...을 생각해봅시다.
- 6B. (a):  $M$ 은 완비이고 유계이지만 전유계는 아닙니다.  $N$ 은 전부 아니오입니다. (b)의 경우  $M \cong \mathbb{R} \cong N$ 임을 보이십시오.
- 6C<sup>†</sup>. 집합으로서,  $\overline{M}$ 을  $M$ 에서의 코시 수열  $(x_n)$ 들의 집합으로 두되,  $\lim_n d(x_n, y_n) = 0$ 이면  $(x_n) \sim (y_n)$ 이라는 관계로 나눈 몫으로 둡니다.
- 6E. 표준적인 풀이는 이른바 "베르 범주 정리"를 통한 것으로 보입니다.
- 7D.  $p$ 를 임의의 점이라 합시다. 만약 어떤  $q \in M$ 에 대해서도  $d(p, q) \neq r$ 을 만족하는 실수  $r$ 이 존재한다면,  $p$ 의  $r$ -근방은 열려 있으면서 닫혀 있습니다.
- 7E. (a)의 답은 예이고, (b)의 답은 거리 공간에 대해서도 아니오입니다. 실제로 완전 비연결 공간이란 모든 연결 성분이 오직 하나의 점으로만 이루어진 공간을 말하며, 이산 위상이 아니면서도 완전 비연결인 거리 공간의 예가 존재합니다.
- 7F. 각  $p$ 에 대해  $p\mathbb{Z}$ 가 닫혀 있음에 유의하십시오. 만약 소수가 유한 개라면  $\bigcup p\mathbb{Z} = \mathbb{Z} \setminus \{-1, 1\}$ 이 닫혀 있어야 하며, 즉  $\{-1, 1\}$ 이 열려 있어야 하는데, 여기서 모든 열린집합은 무한합니다.
- 7G. 0에서의 공은  $n! \cdot \mathbb{Z}$  형태이어야 합니다.
- 7H.  $\mathbb{Q}$ 에 호소하십시오.
- 8A.  $[0, 1]$ 은 콤팩트합니다.
- 8B.  $X$ 가 유한할 때, 그리고 오직 그때만입니다.
- 8E.  $p_i = (x_i, y_i)$ 가  $X \times Y$  안의 수열이라 합시다 ( $i = 1, 2, \dots$ ).  $x$ 좌표가 수렴하도록 부분수열을 취하십시오 (일부 항을 버립니다). 그런 다음 그 부분수열의 부분수열 중  $y$ 좌표가 수렴하는 것을 취하십시오 (더 많은 항을 버립니다).
- 8F<sup>†</sup>. 정리 8.2.2의 증명을 모방하십시오. 전유계 조건이 비둘기집 원리를 사용할 수 있게 해줍니다.

- 8H.**  $M$ 이 콤팩트하지 않다고 가정하고, 유계가 아닌 연속함수  $F: M \rightarrow \mathbb{R}$ 를 구성하십시오. 이러한 함수  $F$ 가 정의되고 나면, 다음 거리가

$$d'(x, y) := d(x, y) + |F(x) - F(y)|$$

이 문제의 대우를 확립할 것입니다.

- 8I.** 두 문제 모두에 대한 답은 아니오입니다.

(a)에는 **문제 8D**를 사용하십시오.

(b)에서는, 분할에 속한 각 원을 그것이  $p$ 는 포함하지만  $q$ 는 포함하지 않는지,  $q$ 는 포함하지만  $p$ 는 포함하지 않는지, 아니면 둘 다 포함하는지에 따라 색칠하십시오.

- 9A<sup>†</sup>.** 랭크-널리티 정리를 사용하십시오. 또한 영사상도 고려하십시오.

**9D.**  $a + b\sqrt{5} \mapsto \sqrt{5}a + 5b.$

**9F.**  $y = -1, 0, 1$ 을 대입하십시오.  $\mathbb{R}[x]$ 의 차원을 사용하십시오.

**9G.** 적절한  $V, W$ 에 대해  $V \oplus V \rightarrow W$ 로 해석하십시오.

- 9I<sup>\*</sup>.** 부분공간들의 다음 무한 사슬이라는 사실을 이용하십시오

$$\ker T \subseteq \ker T^2 \subseteq \ker T^3 \subseteq \dots$$

그리고  $\operatorname{im} T$ 에 대한 유사한 사슬은 (차원상의 이유로) 결국 안정화되어야 합니다.

- 10D.** 답은 그렇다는 것입니다. 사실,  $\mathbb{C}^{\oplus 2}$ 가 임의의 유한차원  $\mathbb{C}$ -벡터 공간이어도 이 결과는 성립합니다.

- 10F.** 0만이 그렇습니다. 차수를 살펴보십시오.

- 10G.** 모두 다입니다!

- 11A.**  $T$ 를 고유기저로 나타내면 따라옵니다: 그러면 대각 성분들이 고윳값들이 됩니다.

- 11B<sup>†</sup>.** 이번에도 그냥 기저를 잡으면 됩니다.

- 11C<sup>†</sup>.** 한 가지 방법은 그냥 기저를 잡는 것입니다. 그렇지 않다면,  $T \otimes S \mapsto \operatorname{Tr}(T \circ S)$ 를 선형 사상  $(V^{\vee} \otimes W) \otimes (W^{\vee} \otimes V) \rightarrow k$ 로 해석하고, 이것이 교환적임을 확인하십시오.

- 11D.**  $T$ 의 대각합을 살펴보십시오.

- 12A.** 핵심은 다음과 같습니다.

$$(v_1 + cv_2) \wedge v_2 \cdots \wedge v_n = v_1 \wedge v_2 \cdots \wedge v_n + c(v_2 \wedge v_2 \cdots \wedge v_n)$$

그리고 뒤의 항은 영입니다.

- 12B.**  $T$ 를 행렬 형태로 써서 이를 보일 수도 있고, 조르당 형식이 주는 기저를 사용하여  $\det T$ 의 켤레 정의를 사용할 수도 있습니다.

- 12C.** 이는 사실  $X$ 가 위삼각 행렬이 되는 임의의 기저를 취하면 즉시 얻어집니다!

- 12D.** 고윳값이 필요하지는 않습니다 (물론 사용해도 될 수는 있습니다). 한 방향에서는, (**문제 9B<sup>†</sup>**에 의해) "동형사상"을 "단사"로 바꿀 수 있음을 기억하십시오. 다른 방향에서는,  $T$ 가 동형사상이라면  $S$ 를 역사상이라 하고  $\det(S \circ T)$ 를 살펴보십시오.

- 12E.** 대각선상의 성분은 0이고 대각선 밖의 성분은  $\pm 1$ 인  $1000 \times 1000$  행렬  $M$ 을 생각하십시오. 법 2로 계산합니다.
- 12F.**  $a = b = c = d$ 만이 아닌 다른 해의 족이 존재합니다.  
 케일리-해밀턴 정리를 이용하여 문제를 풀 수도 있습니다. 좀 더 "직접적인" 접근법은  $((a = b = c = d \text{가 아닌 한})$  행렬이 가역임을 보인 다음 행렬을 다음과 같이 대각화하는 것입니다  $M = \begin{bmatrix} s & -q \\ -r & p \end{bmatrix} \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} ps\lambda_1 - qr\lambda_2 & qs(\lambda_1 - \lambda_2) \\ pr(\lambda_2 - \lambda_1) & ps\lambda_2 - qr\lambda_1 \end{bmatrix}$ .
- 12G.** 기저를 택하여 다소 긴 계산을 수행하십시오.
- 13B\*.** 정규직교 기저  $e_1, \dots, e_n$ 을 고정하십시오.  $\mathbb{R}^n$ 이 완비라는 사실을 이용하십시오.
- 13C.**  $\mathbb{F}_2$ 에서의 내적.
- 13D\*.** 단순 텐서에서 정의한 다음 선형적으로 확장하십시오.
- 13E.**  $k = n^n$ 입니다. 텐서곱에 내적 형식을 부여하십시오. "대각선상 어딘가에 영 원소를 가진다"는 것은 그 원소들의 곱이 영이라는 것과 동치임에 유의하십시오.
- 14A.** 파세발 정리를 다시 사용하되, 이번에는  $f(x) = x^2$ 에 대해 사용하십시오.
- 14B.** 부울 함수  $D: \{\pm 1\}^3 \rightarrow \mathbb{R}$ 를  $D(a, b, c) = ab + bc + ca$ 로 정의합시다. 각  $(a, b, c)$ 에 대해  $D(a, b, c)$ 의 값을 써 보십시오. 그런 다음 그 기댓값을 계산하십시오.
- 15A\*.**  $V$ 의 기저  $e_1, \dots, e_n$ 을 취하여, 이것이  $e_1$ 을 기저  $(e_1^\vee)^\vee$ 로 보내는 선형 사상임을 보이는 것만으로 결과를 증명할 수 있습니다.
- 15B.** 정리 9.7.6를 사용하면 즉시 성립할 것입니다 (네 개의 값이 정리에서의  $k$ 와 같습니다).
- 15C<sup>†</sup>.** 이는 사실 앞 문제를 위장한 것에 불과합니다! 행 계수는  $\dim \operatorname{im} T^\vee$ 이고 열 계수는  $\dim \operatorname{im} T$ 입니다.
- 15F.** 다항식이 존재한다면  $TT^\dagger = T^\dagger T$ 를 직접 확인하십시오.  $T$ 가 정규 사상이라면 이를 대각화하십시오.
- 15H<sup>†</sup>.** 어떤 기저를 선택하는 것도 권장하지 않습니다. 대신, 임의의 사상  $T$ 에 대해  $\ker(T^\dagger T) = \ker(T)$ 임을 직접 보이십시오. (이것이 차원이 같다는 것보다 더 낫습니다: 핵이 실제로 일치하기 때문입니다.)
- 16A.** 번사이드 보조정리(Burnside's lemma)를 직접 적용하면 198이라는 답을 얻습니다(관련 군은  $D_{14}$ 입니다).
- 16B.** 이를 확인하는 방법에는 여러 가지가 있습니다. 하나는 그냥 대수적 조작을 하는 것입니다. 다른 하나는 케일리의 정리(Cayley's theorem)를 사용하여  $G$ 를 대칭군 안에 매장하는 것입니다.
- 16C.**  $g \cdot x = x$ 인 쌍  $(g, x)$ 의 개수를 이중으로 셸하십시오.
- 16E<sup>†</sup>.**  $H$ 가 왼쪽 잉여류  $\{gH \mid g \in G\}$ 에 왼쪽 곱셈  $h \cdot gH = hgH$ 로 작용하게 합시다. 임의의 궤도  $\mathcal{O}$ 를 생각합시다. 궤도-안정자군 정리에 의해  $|\mathcal{O}|$ 는  $|H|$ 를 나누고  $|H|$ 는  $n$ 을 나누므로,  $|\mathcal{O}|$ 는  $n$ 을 나눕니다. 그러나 잉여류가  $p$ 개이므로  $|\mathcal{O}| \leq p$ 입니다. 따라서  $\mathcal{O} = \{H\}$ 이거나  $\mathcal{O}$ 가 모든 잉여류를 포함합니다. 후자가 불가능함을 보이고 결론을 내리십시오.
- 17B.** 실로우 2-군과 7-군의 개수를 세고 그것들이 교차하도록 하십시오.

- 17C. 모든 원소의 위수가 3인 비아벨 군을 구성하십시오.
- 17D. 먼저,  $G$ 가 아벨 군이면 자명합니다. 그렇지 않다면,  $Z(G)$ 를 이 군의 중심이라고 합시다. 이는 항상  $G$ 의 정규 부분군입니다. 켈레 작용을 통한  $\text{mod } p$  논법을 사용하십시오 (또는 류 방정식을 사용하십시오).
- 18A<sup>†</sup>. 구조 정리에서  $k/(s_i) \in \{0, k\}$ 입니다.
- 18B<sup>†</sup>. 정리에 의해 어떤 다항식  $s_i$ 들에 대해  $V \cong \bigoplus_i k[x]/(s_i)$ 입니다. 각 블록을 설명된 형태로 쓰십시오.
- 18C<sup>†</sup>. 앞선 증명을 그대로 따라가되, 구조 정리의 다른 형태를 사용하십시오.  $k[x]$ 가 대수적으로 닫혀 있으므로 각  $p_i$ 는 일차 인수입니다.
- 18D. 여기서 구조 정리는 반대 결과를 줍니다: 이는 유한 생성 아벨 군으로는 성립하지 않음을 어느 정도 함의합니다. 그러므로 무한 생성 예시를 찾아보십시오.
- 18E.  $A$ 가 뇌터 환이라는 가정을 추가하면 이 결과가 참일 것 같으니,  $A$ 가 뇌터 환이 아닌 경우를 택해 문제가 생기는지 찾아보십시오.
- 19B<sup>†</sup>. 임의의  $a \in A$ 에 대해, 사상  $v \mapsto a \cdot v$ 는 교환 사상입니다.
- 19C\*. (b)에 대해서는, 기저를 하나 골라  $T \mapsto (T(e_1), \dots, T(e_n))$ 을 취하십시오.
- 19D\*. 우측 곱셈.
- 19E. **문제 9I\***를 적용하십시오.
- 20A. 이들은 모두 일차원이며, 그 개수는  $n$ 개입니다.  $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{C}^\times$ 인 준동형사상은 무엇입니까?
- 20B.  $(1, 0)$ 의 생성 공간은 부분표현입니다.
- 20C. 이는 사실 쉽습니다.
- 20D. 일차원인 것은 오직 두 개뿐입니다(오직 두 개의 준동형사상  $D_{10} \rightarrow \mathbb{C}^\times$ 에 대응). 따라서 나머지는 이차원입니다.
- 20E.  $r, t \in D_{10}$ 을 각각 회전과 반사라 합시다. 그러면 벌레가 가능한 모든 이동에 대해 합을 취할 수 있습니다.
- $$\frac{1}{10} \text{Tr}(\rho(r) + \rho(t))^{15}.$$
- 그런 다음 **문제 20D**를 사용하여 이 대각합을 계산하십시오.
- 21A<sup>†</sup>. 자명합니다.  $W = \bigoplus_i V_i^{m_i}$ 로 두면 ( $\mathbb{C}[G]$ 가 반단순이므로 가능합니다)  $\chi_W = \sum_i m_i \chi_{V_i}$ 입니다.
- 21B.  $\chi_W = \chi_{\text{refl}_0}^2$ 로 두고 앞 문제를 이용하십시오.
- 21C. 지표를 이용합니다.  $|\chi_W| = 1$ 이 어디서나 성립함에 주목하십시오.
- 21D. 다섯 개의 켈레류가 있습니다:  $1, -1$ , 그리고  $\pm i, \pm j, \pm k$ 입니다. 표현들 중 네 개가 주어지면, 직교성을 통해 다섯 번째를 얻을 수 있습니다.
- 21E\*. 첫 번째 직교성에 의해  $AB$ 가 항등원이 되도록 두 개의 정사각  $r \times r$  행렬  $A$ 와  $B$ 를 구성하십시오. 그런 다음  $BA$ 를 이용하여 두 번째 직교 관계를 증명하십시오.
- 23A.  $|\Psi_-\rangle = -\frac{1}{\sqrt{2}}(|\rightarrow\rangle_A \otimes |\leftarrow\rangle_B - |\leftarrow\rangle_A \otimes |\rightarrow\rangle_B)$ 로 다시 쓰십시오.

- 23B.** 각각 1, 1, 1,  $-1$ 입니다. 이들을 모두 곱하면  $\text{id}^A \otimes \text{id}^B \otimes \text{id}^C$ 의 측정값이  $-1$ 이 되는데, 이것이 바로 역설입니다. 이것이 의미하는 바는 측정값들이 독립적으로 미리 준비될 수 없다는 것입니다. 다시 말해, 이는 특정 국소 숨은 변수 이론들과 모순됩니다.
- 이것은 차일링거가 2022년 노벨상을 (공동) 수상하게 된 여러 결과 중 하나였습니다.
- 24A.** 한 가지 방법은 몇 개의 프레드킨 게이트를 사용하여 CCNOT을 만드는 것입니다.
- 24B.**  $|\psi\rangle = |0\rangle$ ,  $|\psi\rangle = |1\rangle$ ,  $|\psi\rangle = |\rightarrow\rangle$ 를 대입하여 모순을 이끌어내십시오.
- 24C.** 먼저 이 상자가  $|x_1\rangle \otimes \cdots \otimes |x_n\rangle \otimes |\leftarrow\rangle$ 을  $(-1)^{f(x_1, \dots, x_n)}(|x_1\rangle \otimes \cdots \otimes |x_n\rangle \otimes |\leftarrow\rangle)$ 으로 보냈을 보이십시오.
- 24D<sup>†</sup>.** 이는 직접 계산입니다.
- 26B.** 수열이 수렴할 때, 오직 그때만입니다!
- 26D.**  $n$ 번째 부분합은  $\frac{1}{1-r}(1 - r^{n+1})$ 입니다.
- 26F.** 이는 매우 까다로운 대수적 조작입니다.  $x_i \geq 0$ 에 대해  $a_n = x_1 + \cdots + x_n$ 으로 놓아 보십시오.
- 26G.** 이는 보기보다 까다롭습니다.  $x_n = e^{x_n} - e^{x_{n+1}}$ 이지만 수렴을 증명하려면 약간의 주의가 필요합니다. 유용한 힌트: 모든 실수  $t$ 에 대해  $e^t \geq t + 1$ 이므로, 모든  $x_n$ 은 음이 아닙니다.
- 26H.** 극한은 항상 존재하며 0과 같습니다. 따라서  $f$ 는 정확히 무리점에서만 연속입니다.
- 28G.** 먼저 이를  $f(x) = e^{x \log x}$ 로 다시 씁니다.
- 29B<sup>†</sup>.**  $\sin$ 과  $\cos$ 의 모든 도함수를 알고 있으므로,  $\mathbb{R}$  전체에서 수렴하는 이들의 테일러 급수를 계산할 수 있습니다. 동시에  $\exp$ 는 테일러 급수로 정의되었으므로 이 역시 계산할 수 있습니다. 이들을 모두 써서 비교해 보십시오.
- 29C<sup>†</sup>.** 롤의 정리를 반복 적용하십시오. 이를 풀기 위해 이 장의 이론이 전혀 필요하지 않으므로 훨씬 앞에서 제시될 수도 있었지만, 그러면 동기가 상당히 부족했을 것입니다.
- 29D.** 테일러 정리를 사용하십시오.
- 30A.** 모순과 평균값 정리(다시 한 번!).
- 30B\*.** 모든 양의 정수  $n$ 에 대해, 모든 직사각형의 너비가  $w = \frac{b-a}{n}$ 인 분할을 취하십시오. 평균값 정리를 이용하여 첫 번째 직사각형의 넓이가  $f(a+w) - f(a)$ , 두 번째 직사각형의 넓이가  $f(a+2w) - f(a+w)$ , 이렇게 계속되는 태그된 분할을 구성하십시오. 따라서 전체 넓이는  $f(b) - f(a)$ 입니다.
- 30D.** 이것을  $\frac{1}{n} \sum_{k=1}^n \frac{1}{1+\frac{k}{n}}$ 으로 쓰십시오. 그러면 이를 어떤 리만 적분의 직사각형 합으로 해석할 수 있습니다.
- 31A\*.**  $f$ 의 테일러 급수를 살펴보고, 코시 미분 공식을 사용하여 더 큰 계수들이 각각 영이 되어야 함을 보이십시오.
- 31B\*.** 모순을 통해 진행하겠습니다. 즉  $0 = f(z_1) = f(z_2) = \dots$ 이고 모두 서로 다른 수열  $z_1, z_2, \dots \rightarrow z$ 가 존재한다고 하겠습니다.  $f$ 의 테일러 급수를 살펴보고  $z$ 의 인수를 뽑아냄으로써,  $z$ 의 열린 근방에서  $f = 0$ 임을 증명하십시오.
- 31C\*.** 일치하는 점들의 내부를 취하십시오. 이 집합이 닫혀 있음을 보이면 결론이 따라옵니다.

31E. 리우빌 정리를 사용하십시오.  $\frac{1}{f(z)-w}$ 를 살펴보십시오.

31F. 위에서 제시된 코시-구르사 정리 증명의 일부를 변형하고,  $ML$  추정 보조정리를 적용하여  $\oint_{\gamma} f(z) dz = 0$ 을 증명할 수 있습니다. 그러나 이 경우  $f$ 가 정칙 함수임을 이미 알고 있으므로,  $\frac{1}{4}$  인수 없이  $|\oint_{\gamma_i} f dz| \geq |\oint_{\gamma} f dz|$ 가 성립해야 합니다.

32C. 이를 "썰기 윤곽"이라고 합니다. 중심각이  $\frac{2\pi}{n}$ 이고 반지름이  $r$ 인 원의 부채꼴로 이루어진 썰기 모양에 대해 적분해 보십시오. 그런 다음  $r \rightarrow \infty$ 일 때의 극한을 취하십시오.

32D. 이는  $\lim_{a \rightarrow \infty} \int_{-a}^a \frac{\cos x}{x^2+1} dx$ 입니다. 각  $a$ 에 대해 반원을 구성하십시오.

36B. 다음을 보이십시오

$$\mu^*(S) = \begin{cases} 0 & S = \emptyset \\ 1 & S \text{ 유계이고 공집합이 아님} \\ \infty & S \text{ 유계가 아닙니다.} \end{cases}$$

이를 이용하면 (b)를 쉽게 풀 수 있습니다; 답은 그저  $\emptyset$ 과  $\Omega$ 입니다.

39A. 정리 39.3.1에서 바로 읽어낼 수 있습니다.

39B. 폰트랴긴 쌍대성 이후, 우리는  $G$ 가 콤팩트이면  $\hat{G}$ 가 이산이고,  $G$ 가 이산이면  $\hat{G}$ 가 콤팩트임을 보여야 합니다. 둘 다 특별한 것이 필요하지 않습니다: 이는 위상적 사실입니다.

41A. 이것은 보기보다 실제로는 더 까다로운데, (이름과는 달리) 단순히 한정사를 밀어 넣을 수는 없고,  $m = 1, 2, \dots$ 에 대해  $\varepsilon = 1/m$ 에 초점을 맞추어야 합니다.

문제는 각  $\varepsilon > 0$ 에 대해,  $n > N_\varepsilon$ 이면  $\mu(\omega : |X(\omega) - X_n(\omega)| \leq \varepsilon) = 1$ 이라고 말하고 있습니다. 각  $m$ 에 대해 측도가 0인 "나쁜 세계들"이 존재하는데, 그것들의 합집합을 취하십시오.

42B. 귀여운 초등적 풀이가 존재합니다. 마팅게일 기반 풀이를 위해서는, 시각  $n$ 에서 텍에 남은 빨간 카드의 비율이 마팅게일임을 보이십시오.

42E. 문제 42A를 사용하십시오.

42F. 이는 확률 1로 발생합니다.  $X_n$ 이 단계  $n$ 에서 판에 적힌 수이고,  $\mu = \frac{1}{2.01} \int_0^{2.01} \log t dt$ 일 때,  $\log(X_n) - n\mu$ 가 마팅게일임을 보이십시오. (참고로, 큰 수의 법칙을 사용해도 될 수 있습니다.)

43B.  $k = 2$ 인 경우에 대한 작업이 이미 완료되었으므로, 단순히 귀납법을 적용하면 됩니다.

44B. 이것은 단순한 합산입니다. 혼합 편미분이 대칭이라는 사실이 필요할 것입니다.

45A<sup>†</sup>.  $\alpha = f dx + g dy$ 에 스토크스 정리를 직접 적용하십시오.

45B. 이는 시그마 표기법에 대한 단순한 연습 문제입니다.

45D. 이는 간단하지만 (귀찮은) 계산입니다.

45E. 우리는  $\alpha_p(v) = \|v\|$ 이기를 원할 것입니다.

45F.  $d^2 = 0$ 이 완전형식  $\alpha$ 에 대해  $\int_{\partial c} \alpha = 0$ 을 함의함을 보이십시오. 환형(annulus)을 그리십시오.

- 53B.**  $p(x)$ 가  $r$ 의 최소다항식이지만,  $q(x) = x^{\deg p}p(1/x)$  역시 그러하다는 점에 주목하십시오. 따라서  $q$ 와  $p$ 는 서로의 배수여야 합니다.
- 53C\*.**  $\left| \frac{1}{n}(\varepsilon_1 + \cdots + \varepsilon_n) \right| \leq 1$ .
- 53D†.** 자명한 것들뿐입니다.  $\cos(q\pi) \in \mathbb{Q}$ 라고 가정합니다.  $\zeta$ 를 단위근이라 하면 (어떤  $N$ 에 대해  $\zeta^N - 1 = 0$ 이므로 대수적 정수입니다)  $2\cos(q\pi) = \zeta + \zeta^{N-1}$ 이 대수적 정수이자 유리수임에 주목하십시오.
- 53E.** 단위근으로 보십시오.  $\frac{1}{2}$ 는 대수적 정수가 아님에 주목하십시오.
- 53F.**  $\alpha = \alpha_1, \alpha_2, \dots, \alpha_n$ 을 이것의 켈레라고 하십시오.  $e \in \mathbb{N}$ 에 걸쳐 다항식  $(x - \alpha_1^e) \cdots (x - \alpha_n^e)$ 을 살펴보십시오. 가능한 모든 다항식에 대해 비둘기집 원리를 적용하십시오.
- 54A\*.** 노름은 곱셈적이며 갈루아 켈레들의 곱과 같습니다.
- 54B\*.** 그것은  $K$ 와 동형입니다.
- 54C.**  $\mathbb{Q}(\sqrt{2})$  위의 표준 노름을 취하면 이를 무너뜨립니다.
- 54D.**  $\mathbb{Q}(\sqrt[3]{2})$ 에서의 노름.
- 54E†.** 명백히  $\mathbb{Z}[\zeta_p] \subseteq \mathcal{O}_K$ 이므로, 우리의 목표는 역방향 포함 관계를 보이는 것입니다. 임의의  $\alpha \in \mathcal{O}_K$ 에 대하여  $\alpha(1 - \zeta_p)$ 의 대각합이  $p$ 로 나누어짐을 보이십시오.  $x = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2} \in \mathcal{O}_K$  (단,  $a_i \in \mathbb{Q}$ )가 주어졌을 때,  $(1 - \zeta_p)x$ 를 생각해 보십시오.
- 55C.** 보통의 페르마의 소정리의 증명을 그대로 따라 해 보십시오.
- 55D†.** 분모를 없애십시오!
- 55E.** (a)는 간단합니다. (b)의 경우  $p$ 를 법으로 하여 계산하십시오. (c)의 경우 노름을 사용하십시오.
- 55F.**  $\omega$ 를  $k$ 차 단위근이라 합시다.  $\mathfrak{p}$ 를  $K = \mathbb{Q}(\omega)$ 의 정수환에서  $p$  위에 있는 임의의 소 아이디얼이라 합시다.  $2025 - \omega^i$ 와  $2026 - \omega^j$ 가  $\mathfrak{p}$ 에 속하는 지표  $i$ 와  $j$ 가 존재함을 보이십시오. 그런 다음  $1 + \omega^i - \omega^j$ 가 0이 아니며 노름이  $3^k$  이하임을 보이십시오.
- 56A.** 이전 절차를 반복하십시오.
- 56B.** 위수가 3인 군을 얻어야 합니다.
- 56C.** 민코프스키 정리 (a)의 증명을 모방하십시오.
- 56D.** 선형대수학.
- 56E.**  $\mathbb{Q}(i)$ 에서 인수분해하십시오.
- 56F.**  $p$ 를 인수분해하여,  $\mathbb{Q}(\sqrt{-5})$ 의 유수군의 위수가 2임을 보이십시오.
- 56G.**  $n$ 을  $\mathfrak{p}^n$ 이 주 아이디얼이 되는 양의 정수라 하자.
- 57A\*.** 직접적인 선형대수 계산입니다.
- 57B\*.**  $M$ 을 "매장" 행렬이라 합시다.  $M^\top M$ 을 살펴보십시오. 여기서  $M^\top$ 은 전치 행렬입니다.
- 57C\*.** 반데르몽드 행렬.

- 57D.  $M_K \geq 1$ 이 성립해야 합니다. 직접 계산하십시오.
- 59A\*.  $\zeta_p$ 의 상을 살펴보십시오.
- 59C. 반복된 이차 확대는 차수가 2이므로, 2의 거듭제곱만 얻을 수 있습니다.
- 59E. 힌트:  $\sigma(x^2) = \sigma(x)^2 \geq 0$ 와 코시의 함수 방정식을 사용하십시오.
- 59F. 귀납법에 의해,  $\alpha$ 와  $\beta$ 로 표현되는 어떤  $\gamma$ 에 대해  $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\gamma)$ 임을 보이는 것으로 충분합니다. 유한 개를 제외한 모든 유리수  $\lambda$ 에 대해,  $\gamma = \alpha + \lambda\beta$ 로 선택하면 작동합니다.
- 60A<sup>†</sup>. 피보나치 수열은  $F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ 로 주어지며, 여기서  $\alpha = \frac{1+\sqrt{5}}{2}$ 와  $\beta = \frac{1-\sqrt{5}}{2}$ 는  $P(X) = X^2 - X - 1$ 의 두 근입니다. 다항식  $P(X)$ 가 127을 법으로 기약임을 보이십시오. 그런 다음  $P$ 의 분해체, 즉  $\mathbb{F}_{p^2}$ 에서 작업하십시오.  
 $F_p = -1, F_{p+1} = 0, F_{2p+1} = 1, F_{2p+2} = 0$ 임을 보이십시오. ( $P$ 의 근에 대한  $\text{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ 의 작용을 살펴보십시오.)
- 61A<sup>†</sup>.  $\text{Gal}(K/\mathbb{Q})$ 가 순환군이 아니라면 어떤 유리 소수  $p$ 도 비분해(inert)로 남을 수 없음을 보이십시오. 실제로  $p$ 가 비분해라면  $D_p \cong \text{Gal}(K/\mathbb{Q})$ 입니다.
- 62A. 이차상호법칙 증명의 마지막 부분을 수정하십시오.
- 62C<sup>†</sup>.  $\mathbb{Q}(\zeta_m)$ 에서의 체보타레프 밀도.
- 62E. 원시근을 이용하면 이는  $\mathbb{Z}/(p-1)\mathbb{Z}$  위의  $\times 3$  작용과 같습니다.  $\zeta$ 를  $(p-1)$ 차 단위근이라 합시다.  $d = \prod_{i < j} (\zeta^i - \zeta^j)$ 로 두고,  $\mathbb{Q}(d)$ 에 대해 생각한 다음,  $x \mapsto x^3$ 에 의한 작용을 어떻게 할지 알아내십시오.
- 63A<sup>†</sup>.  $f(L/\mathbb{Q}) \mid m^\infty$ 가 되도록  $m$ 을 고릅니다.
- 63B<sup>†</sup>.  $m = 1$ 로 다카기 존재 정리를 적용하십시오.
- 63C. 확대체  $L/\mathbb{Q}$ 는 아벨적이지 않습니다.
- 64C<sup>†</sup>. 콤팩트 공간의 몫이 콤팩트로 남는다는 사실을 증명하고 사용하십시오.
- 65D. 핵심 아이디어는  $\pi_1$ (못 두 개가 박힌 벽)에서  $aba^{-1}b^{-1}$ 를 살펴보는 것입니다.
- 68A. 범주  $\mathcal{A} \times 2$ 는 "중복 사상"을 가지고 있습니다.
- 71A.  $n-1$ 번째 호몰로지 군을 취합니다.
- 71B.  $F$ 를 다음과 같이 구성합니다:  $x$ 에서  $f(x)$ 를 지나는 광선을 그어 경계  $S^{n-1}$ 과 교차시킵니다.
- 72A. 반구를 사용하여  $m$ 에 대한 귀납법을 적용합니다.
- 72B. 한 가지 전략은  $p = 1$ 을 기본 경우로 하여  $p$ 에 대한 귀납법을 사용하는 것입니다. 또 다른 전략은  $U$ 를 원하는 공간으로 놓고,  $V$ 를 서로 교차하지 않는  $p$ 개의 공의 합집합으로 놓는 것입니다.
- 72C\*. 정리 72.2.5을 사용하십시오.  $\mathbb{R}^n \setminus \{0\}$ 이  $S^{n-1}$ 과 호모토피 동치임에 유의하십시오.
- 72D.  $0 \rightarrow A_\bullet \rightarrow B_\bullet \rightarrow C_\bullet \rightarrow 0$ 은 사슬 복합체의 짧은 완전열입니다. 이에 대응하는 긴 완전열을 써 보십시오. 거의 모든 항이 소멸할 것입니다.

**72E\***.  $U$ 와  $V$ 로 두 개의 원기둥을 사용하는 것도 가능합니다. 이번에는 행렬이  $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$  또는 그 변형이지만, 특히 이는 단사이므로  $\tilde{H}_2(X) = 0$ 입니다.

**72F\***. 정리 72.2.1를 적용할 새로운 짧은 완전열을 찾으십시오.

**73B**. 정리 72.2.5을 사용하십시오.

**73E**. 임의의  $n$ 에 대해,  $k = 1, \dots, n-1$ 에 대한 귀납법으로 다음을 증명하십시오. (a)  $X$ 가  $D^k$ 와 위상동형인  $S^n$ 의 부분집합이면  $\tilde{H}_i(S^n \setminus X) = 0$ 입니다; (b)  $X$ 가  $S^k$ 와 위상동형인  $S^n$ 의 부분집합이면  $i = n - k - 1$ 일 때  $\tilde{H}_i(S^n \setminus X) = \mathbb{Z}$ 이고 그 외의 경우에는 0입니다.

**74A†**.  $\mathbb{CP}^n$ 은 인접한 차원에 세포가 없으므로, 모든  $d_k$  사상은 영이어야 합니다.

**74B**. 공간  $S^n - \{x_0\}$ 는 수축 가능합니다.

**74D**. 원소를 참조할 필요는 없습니다. 예를 들어

$$H_2(X) \cong H_2(X^3) \cong H_2(X^2) / \ker [H_2(X^2) \rightarrow H_2(X^3)],$$

로 시작하십시오. 표시된 단사 사상과 전사 화살표에 주목하십시오.

**74E†**. 각 차원마다 하나의 세포가 있습니다.  $d_k$ 의 차수가  $\deg(\text{id}) + \deg(-\text{id})$ 임을 보이십시오. 따라서  $k$ 가 짝수인지 홀수인지에 따라  $d_k$ 는 영이거나 2입니다.

**76A†**. UCT를 이용하여  $H^k(M; \mathbb{Z})$ 를  $H_k(M)$ 의 관점에서 표현하고, 계수(rank)를 분석하십시오.

**76B**. 베티수에 관한 이전 결과를 이용하십시오.

**76C**.  $\mathbb{Z}/2\mathbb{Z}$  코호몰로지를 이용하여 컵 곱을 구하십시오.

**76D**.  $r: S^m \times S^n \rightarrow S^m \vee S^n$ 이 그러한 사상이라고 가정하십시오. 역사상  $i$ 가 존재하므로, 유도된 사상  $H^\bullet(S^m \vee S^n; \mathbb{Z}) \rightarrow H^\bullet(S^m \times S^n; \mathbb{Z})$ 이 그들의 코호몰로지 환 사이에서 단사 사상임을 보이십시오.

**77B**. 제곱은 음이 아닙니다.

**77C**. 이것은 사실 약한 영점 정리의 동치인 표현입니다.

**77D**.  $n+1$ 차원에서의 약한 영점정리를 사용하십시오. 모든 곳에서 소멸하는  $f$ 가 주어졌을 때,  $x_{n+1}f - 1$ 을 생각해 보십시오.

**80B**. 이 문제를 풀려면 유클리드 기하학에서의 복소수에 대해 알아야 합니다.

**81B†**. 표준 아핀 좌표계를 사용하십시오.

**81C**. 대역적 정칙함수를 살펴보십시오.

**81D**.  $f$ 가 동형사상이라고 가정하십시오. 그러면 이는 동형사상  $f^\sharp: \mathcal{O}_V(V) \rightarrow \mathcal{O}_X(X) = \mathbb{C}[x, y]$ 를 줍니다. 따라서  $\mathcal{O}_V(V) = \mathbb{C}[a, b]$ 로 쓸 수 있으며, 여기서  $f^\sharp(a) = x$ 이고  $f^\sharp(b) = y$ 입니다.  $\mathcal{V}(a, b) = \{q\}$ 일 때  $f(p) = q$ 라 하십시오. 당겨오기의 정의를 사용하여  $p \in \mathcal{V}(x, y)$ 임을 증명하여 모순을 이끌어내십시오.

**82C**. 줄기는  $\{p\}$ 의 폐포에 속한 점들에서는  $R$ 이고, 그 외의 곳에서는 0입니다.

- 82D. 여집합  $\{p \mid [s]_p = 0\}$ 이 열린집합임을 보이십시오.
- 83B. 영인자를 생각해 보십시오.
- 83C\*. 오직 하나입니다! 증명은 몇 장 뒤에 제시될 것입니다.
- 83D. 아닙니다. 곱환을 사용하십시오.
- 84A. 갈루아 켄레.
- 85B.  $k[x, y] \times k[z, z^{-1}]$ .
- 85D. 이것은  $R$ 과 동형입니다!
- 87A.  $\text{AffSch} \simeq \text{CRing}$ 이라는 사실을 이용하십시오.
- 88A.  $\varepsilon = \pi - 3.141592653 < 10^{-9}$ 라 하십시오.  $f(\varepsilon)$ 를 구하십시오.
- 89E. 이것은 선택 공리의 응용입니다.
- 91A.  $\sup_{k \in \omega} |V_k|$ .
- 91B. 공종 사상들을 감소하지 않도록 재배열하십시오.
- 92C†. 이는 뢰벤하임-스콜렘(Löwenheim-Skolem) 정리의 증명과 매우 유사합니다. 문장  $\phi$ 에 대해,  $f_\phi$ 가  $\alpha$ 를 다음과 같은 최소의  $\beta < \kappa$ 로 보낸다고 합시다: 모든  $\vec{b} \in V_\alpha$ 에 대해,  $V_\kappa \models \phi[a, \vec{b}]$ 인  $a \in V_\kappa$ 가 존재하면,  $V_\kappa \models \phi[a, \vec{b}]$ 인  $\exists a \in V_\beta$ 입니다. (이  $\beta$ 가 존재함을 증명하려면  $\kappa$ 가 정칙(regular)이라는 사실을 이용하십시오.) 그런 다음, 각  $\alpha$ 에 대해 가산 개의 문장들에 걸친 상한을 취합니다.
- 92D\*. 보조정리 92.5.1를 사용하십시오.  $V_\kappa \models \text{PowerSet}$ 을 증명하려면  $\kappa$ 가 강한 극한 기수여야 하고,  $V_\kappa \models \text{Replacement}$ 를 증명하려면  $\kappa$ 가 비가측 기수여야 합니다 — 이것이 우리가 공종성과 비가측성에 관심을 가졌던 이유입니다.
- 93B.  $D_1, D_2, \dots$ 를 조밀 집합들이라고 합시다 (이들은 가산 개 있습니다).
- 94A. 그렇지 않다고 가정하고,  $M$ 에서 정칙인  $\lambda > \kappa$ 를 취하십시오.  $f: \bar{\lambda} \rightarrow \lambda$ 일 때,  $f$ 에 가능값 논법을 사용하여  $M$  안에서  $\lambda$ 의 공종성을 깨는 함수를 만들어내십시오.



# C 선정된 풀이의 개요

- 1A. 요점은  $\heartsuit$ 가 군이고,  $G \subsetneq \heartsuit$ 가 부분군이며,  $G \cong \heartsuit$ 라는 것입니다. 이는  $|\heartsuit| = \infty$ 일 때만 일어날 수 있습니다. 그렇지 않으면 진부분군은 원래의 군보다 엄밀하게 더 작은 크기를 가질 것입니다.
- 1B.  $\{g_1, g_2, \dots, g_n\}$ 을  $G$ 의 원소들이라고 합시다. 임의의  $g \in G$ 에 대해, 이는 집합  $\{gg_1, \dots, gg_n\}$ 과 같습니다. 전체 곱을 취하고 교환법칙을 이용하면  $g^n \cdot g_1g_2 \dots g_n = g_1g_2 \dots g_n$ 을 얻으며, 따라서  $g^n = 1$ 입니다.
- 1C.  $r \mapsto (1\ 2\ 3)$ 과  $s \mapsto (1\ 2)$ 로의 사상을 이용하면  $D_6 \cong S_3$ 임을 직접 확인할 수 있습니다. (우변은 [절 6.iv](#)에서 언급했던 "순환 표기법"으로 쓰여 있습니다.) 반면  $D_{24}$ 는 위수가 12인 원소를 갖지만  $S_4$ 는 그렇지 않습니다.
- 1D\*.  $G$ 를 위수  $p$ 인 군이라 하고,  $1 \neq g \in G$ 라 합시다.  $g$ 로 생성된 군  $H$ 를 살펴보고 라그랑주 정리를 사용하십시오.
- 1F†. 아이디어는 각 원소  $g \in G$ 를  $x \mapsto gx$ 에 의한 순열  $G \rightarrow G$ 로 생각할 수 있다는 것입니다.
- 1G. 답은  $n = 1009$ 입니다. 이 풀이는 1009가 소수라는 사실을 사용합니다.  
더 작은  $m$ 이 불가능함을 보이려면,  $D_{2018}$ 이 소수인 1009의 위수를 가진 원소를 갖는다는 점에 유의하십시오.  $n < 1009$ 일 때  $S_n$ 은 이러한 위수를 가진 원소가 없으므로,  $n \geq 1009$ 가 필요합니다.  
 $n = 1009$ 로부터 구성을 제시하기 위해,  $D_{2018}$ 을 정1009각형의 대칭들로 생각할 수 있음에 유의하십시오. 정1009각형의 꼭짓점들을  $S := \{1, 2, \dots, 1009\}$ 로 라벨링하면,  $D_{2018}$ 의 원소들은  $S$  위의 순열을 유도하며, 이렇게 얻어지는 순열들의 집합이 원하는 부분군입니다.
- 1H.  $www = bb$ ,  $bww = wb$ ,  $wbw = bw$ ,  $bwb = ww$ 가 성립합니다. 이를  $D_6$ 의 원소로 해석하십시오.
- 1I. 행렬식이  $\pm 1$ 인 (성분이  $p$ 를 법으로 하는 정수인)  $p$ 를 법으로 하는  $2 \times 2$  행렬들의 군  $G$ 를 살펴보십시오.  $g = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ 이라 하고, 그런 다음  $g^{|G|} = 1_G$ 를 사용하십시오.
- 2B. 가능한 두 가지 접근법이 있는데, 하나는 거리의 정의를 사용하고 다른 하나는 열린집합을 사용합니다.  
거리 방식:  $\mathbb{Q}$ 에서  $\mathbb{N}$ 으로 가는 연속인 단사 사상은 존재하지 않는다고 주장합니다. 실제로  $f$ 가 그런 사상이고  $f(x) = n$ 이라고 합시다. 그러면  $\varepsilon = 1/2$ 을 선택합니다.  $\mathbb{Q}$  안에서  $x$ 의  $\delta$  이내에 있는 모든 것이  $n \in \mathbb{N}$ 의  $\varepsilon$  이내에 놓여야 한다는, 즉  $n$ 과 같아야 한다는  $\delta > 0$ 이 존재해야 합니다. 이는 단사성에 명백히 모순됩니다.  
열린집합 접근법:  $\mathbb{Q}$ 에서는 어떤 한원소 집합도 열려 있지 않은 반면,  $\mathbb{N}$ 에서는 모두 열려 있습니다(사실  $\mathbb{N}$ 은 이산적입니다). [장 7](#)의 시작 부분에서 보시겠지만, "동형사상"의 새롭고 개선된 정의를 통해  $\mathbb{Q}$ 와  $\mathbb{N}$  위의 열린집합의 구조가 다르다는 것을 알게 되므로, 이들은 동형이 아닙니다.
- 2C. 뺄셈의 경우, 사상  $x \mapsto -x$ 는 연속이므로 이를 다음과 같은 합성 사상으로 볼 수 있습니다

$$\mathbb{R} \times \mathbb{R} \xrightarrow{(\text{id}, -x)} \mathbb{R} \times \mathbb{R} \xrightarrow{+} \mathbb{R}$$

$$(a, b) \longmapsto (a, -b) \longmapsto a - b.$$

마찬가지로,  $x \mapsto 1/x$ 가 연속 함수라고 믿고자 한다면, 나눗셈은 다음의 합성입니다

$$\mathbb{R} \times \mathbb{R}_{>0} \xrightarrow{(\text{id}, 1/x)} \mathbb{R} \times \mathbb{R}_{>0} \xrightarrow{\times} \mathbb{R}$$

$$(a, b) \longmapsto (a, 1/b) \longmapsto a/b.$$

어떤 이유로든  $x \mapsto 1/x$ 가 연속이라는 것이 의심스럽다면, 여기 순열 연속성을 이용한 증명이 있습니다.  $x_n \rightarrow x$ 이고  $x_n > 0$ ,  $x > 0$ 이라고 합시다( $x$  역시  $\mathbb{R}_{>0}$ 에 속해야 하기 때문입니다). 그러면

$$\left| \frac{1}{x} - \frac{1}{x_n} \right| = \frac{|x_n - x|}{|xx_n|}.$$

$n$ 이 충분히 크면  $|x_n| > x/2$ 이므로, 분모는 최소  $x^2/2$ 이고, 따라서 전체 분수는 최대  $\frac{2}{x^2} |x_n - x|$ 이며, 이는  $n \rightarrow \infty$ 일 때 0으로 수렴합니다.

**2D.**  $x \in \mathbb{Q}$ 일 때  $f(x) = x$ 로, 무리수  $x$ 일 때  $f(x) = -x$ 로 놓습니다.

**2E.** 모순을 이끌어내기 위해 이 함수가 완전히 불연속이라고 가정합시다. 스케일링을 통해  $f(0) = 0$ ,  $f(1) = 1$ 로 설정하고,  $f: [0, 1] \rightarrow [0, 1]$ 에만 집중합시다. 이 함수는 모든 점에서 불연속이므로, 모든  $x \in [0, 1]$ 에 대해 연속성 조건이 성립하지 않는 어떤  $\varepsilon_x > 0$ 가 존재합니다. 함수가 강증가하므로, 이는 함수가 구간  $(f(x) - \varepsilon_x, f(x))$  또는  $(f(x), f(x) + \varepsilon_x)$ (혹은 둘 다)에 속한 모든  $y$ 값을 놓칠 때에만 일어날 수 있습니다.

이 빠진 구간들을  $y$ 축으로 사영하면, 서로소인 비가산 개의 구간들( $x \in [0, 1]$ 마다 하나씩)을 얻게 됩니다. 특히,  $\varepsilon_x$ 들을 모두 더하면 비가산 개의 양의 실수의 합이 최대 1임을 얻게 됩니다.

하지만 일반적으로 양의 실수로 이루어진 비가산 족  $\mathcal{I}$ 가 유한한 합을 갖는 것은 불가능합니다. 실제로 실수들을 구간  $\frac{1}{k} \leq x < \frac{1}{k-1}$ 의 버킷으로 분류해 보십시오. 만약 합이 실제로 유한하다면 각 버킷은 유한해야 하므로, 모임  $\mathcal{I}$ 는 가산이어야 하며, 이는 모순입니다.

**2F.** 수학에 대한 대부분의 인터넷 "논쟁"이 그렇듯, 이 질문 또한 허술한 정의를 둘러싸고 벌어집니다. 처음 제기된 질문(형식이 갖추어지지 않은)은 다음과 같습니다

(1)  $1/x$ 는 연속 함수인가?

이를 형식이 갖추어진 질문으로 만들기 위해, 저는 먼저 다음 질문을 제기하고자 합니다:

(2)  $1/x$ 는 함수인가?

엄밀히 말하면, 이 질문 역시 함수를 명시하는 데 필요한 데이터의 일부인 함수의 정의역을 명시하지 않았으므로 형식이 갖추어지지 않았습니다. 질문자가 의도했을 법한 합리적인 추측 하나는  $\mathbb{R} \setminus \{0\}$ , 즉 0이 아닌 실수들의 집합일 것이며, 이 경우 다음 질문을 얻게 됩니다

(2')  $1/x$ 는  $\mathbb{R} \setminus \{0\}$ 에서  $\mathbb{R}$ 로 가는 함수를 정의하는가?

이 질문에는 확고하게 ”예”라는 답이 있습니다.

반면,  $1/x$ 를  $\mathbb{R}$  위의 함수로 정의하려는 시도는 말이 되지 않습니다. 함수의 정의는 모든 입력에 대해 출력값을 명시할 것을 요구하므로, 적어도 실숫값 함수<sup>1</sup>를 원한다면,  $1/x$ 를  $\mathbb{R}$  전체에서의 함수로 해석할 방법은 존재하지 않습니다.

이제 (1)로 돌아가서, 우리는 다음과 같은 정형화된 질문을 던질 수 있습니다

(1')  $1/x$ 는  $\mathbb{R} \setminus \{0\} \rightarrow \mathbb{R}$ 인 연속함수를 나타냅니까?

이 질문 역시 확고하게 YES라는 답을 가집니다.

물론 “ $1/x$ 는 연속함수  $\mathbb{R} \rightarrow \mathbb{R}$ 를 나타냅니까?”와 같은 질문을 던질 수도 있습니다. 그러나 이는 오해를 불러일으키는 것처럼 느껴집니다. 마치 “ $\sqrt{2}$ 는 짝수 정수입니까?”라고 묻는 것과 같기 때문입니다. 이 질문은 애초에 말이 되지 않는데,  $\sqrt{2}$ 는 정수가 아니고, “짝수”는 정수에 대해 사용되는 형용사이므로 이것이  $\sqrt{2}$ 에 적용되는지 묻는 것은 **유형 오류(type-error)**이기 때문입니다. 마찬가지로, “연속”은 함수에 대해 사용되는 형용사이며, 함수가 아닌 대상에 이것이 적용되는지 묻는 것은 말이 되지 않습니다.

트위터 게시물(스페인어)은 <https://twitter.com/davidcpvm/status/1481024944830046209>를, 함께 올라온 레딧 게시물(여러 개 중 하나)은 <https://www.reddit.com/r/math/comments/s82vf8>를 참고하십시오.

**3A.** 아벨 군:  $abab = a^2b^2 \iff ab = ba$ .

**3B.** (a)에 대해서는 그렇습니다: 이는  $ghg^{-1}$  정의로부터 직접 확인할 수 있습니다. 예를 들어 (a)에 대해서는  $(r^a s)r^n(r^a s)^{-1} = r^{-n} \in H$ 를 계산하는 것으로 충분합니다. 몫군은  $\mathbb{Z}/2\mathbb{Z}$ 입니다.

**예제 3.5.2**를 따르면 (b)에 대한 답은 아닙니다.

**3C.** 위수 3인 부분군은 3이 소수이므로 위수 3인 원소에 의해 생성되어야 합니다. 따라서 (적절히 원소들의 이름을 바꾸어) 일반성을 잃지 않고  $H = \langle (1\ 2\ 3) \rangle$ 이라고 가정할 수 있습니다. 그런데  $g = (3\ 4)$ 라 하면,  $gHg^{-1} \neq H$ 임을 확인할 수 있습니다.

**3D.**  $\phi: G \rightarrow H$ 를 준동형사상이라 합시다. 그러면  $G/\ker \phi$ 는  $H$ 의 어떤 부분군과 동형입니다. 전자의 위수는 1000을 나누고, 후자의 위수는 999를 나눕니다. 이는  $G/\ker \phi = \{1\}$ 인 경우에만 일어날 수 있으므로  $\ker \phi = G$ 입니다.

**3F.** 사원수군입니다.

**3G.** 답은  $|G| = 18$ 입니다.

먼저, 귀납법에 의해 다음이 성립함을 관찰합니다

$$a^n c = c a^{8n}$$

모든  $n \geq 1$ 에 대해. 이제 다음을 주목합니다

$$\begin{aligned} a(bc) &= (ab)c \\ a \cdot c a^6 &= c^2 a^4 \cdot c \\ c a^8 \cdot a^6 &= c^2 a^4 \cdot c \\ a^{14} &= c(a^4 c) = c^2 a^{32}. \end{aligned}$$

<sup>1</sup> $\mathbb{RP}^1$ 이 무엇인지 아는 분이라면 굳이 원한다면 이를  $\mathbb{RP}^1 \rightarrow \mathbb{RP}^1$ 인 함수로 생각할 수도 있습니다. 하지만 그 경우에도 이는 연속입니다.

따라서  $c^2 = a^{-18}$ 임을 결론지을 수 있습니다. 그러면  $ab = c^2a^4 \implies b = a^{-15}$ 입니다.

그 경우,  $c^{2018} = b^{2019}$ 이므로  $1 = a^{-1009 \cdot 18 + 2019 \cdot 15} = a^{12123}$ 임을 결론지을 수 있습니다. 마지막으로,

$$\begin{aligned} bc &= ca^6 \\ a^{-15}c &= ca^6 \\ a^{-15}c^2 &= c(a^6c) = c^2a^{48} \\ a^{-33} &= a^{30} \\ \implies a^{63} &= 1. \end{aligned}$$

$\gcd(12123, 63) = 9$ 이므로  $a^9 = 1$ 을 얻고, 따라서 마지막으로  $c^2 = 1$ 입니다. 그러므로 위의 표시(presentation)는 다음과 같이 단순화됩니다

$$G = \langle a, c \mid a^9 = c^2 = 1, ac = ca^{-1} \rangle$$

이는 위수 18의 이면체군의 표시입니다. 이로써 증명이 완료됩니다.

**3H.** "homophone group" 검색으로 많은 풀이를 찾을 수 있습니다. 그중 하나는 <https://math.stackexchange.com/q/843966/229197>입니다.

**4A.** 이것은 단지  $\mathbb{R}[i] = \mathbb{C}$ 입니다. 이 동형사상은  $x \mapsto i$ 로 주어지며, 핵은  $(x^2 + 1)$ 입니다.

**4B.** 다음 사상이

$$\begin{aligned} \mathbb{C}[x] &\rightarrow \mathbb{C} \times \mathbb{C} \\ p &\mapsto (p(0), p(1)) \end{aligned}$$

실제로 전사 환 준동형사상입니다. 그 핵은  $p(0) = p(1) = 0$ 을 만족하는 다항식  $p$ 들로 이루어지며, 이는  $x$ 와  $x - 1$  둘 다로 나누어떨어지는 다항식들의 집합이므로  $x(x - 1)$ 입니다.

**5C\*.**  $ab \in \phi^{\text{pre}}(I)$ 를 생각해 봅시다. 이는  $\phi(ab) = \phi(a)\phi(b) \in I$ 를 의미합니다.  $I$ 가 소 아이디얼이므로,  $\phi(a) \in I$ 이거나  $\phi(b) \in I$ 입니다. 전자의 경우 필요한 대로  $a \in \phi^{\text{pre}}(I)$ 를 얻고, 후자의 경우  $b \in \phi^{\text{pre}}(I)$ 를 얻습니다.

**5D\*.**  $x \neq 0$ 인  $x \in R$ 를 생각해 봅시다. 거듭제곱  $x, x^2, \dots$ 를 살펴봅시다. 비둘기집 원리에 의해, 결국 그중 두 개가 같아집니다. 그러므로  $m < n$ 에 대해  $x^m = x^n$ 이라고 가정합시다. 이는 다음과 동치입니다.

$$0 = x \cdot x \cdot \dots \cdot x \cdot (x^{n-m} - 1).$$

$x \neq 0$ 이므로,  $x^{n-m} - 1 = 0$ , 즉  $x^{n-m} = 1$ 을 얻습니다. 따라서  $x^{n-m-1}$ 은  $x$ 의 역원입니다.

이는 모든 0이 아닌 원소가 역원을 가진다는 것을 의미하므로,  $R$ 은 체입니다.

**5E\*.** (b)에서는 진 아이디얼들의 순서 집합을 살펴보십시오. 초른의 보조정리를 적용하십시오(이번에도 조건을 확인하기 위해 합집합 트릭을 사용합니다. 그 합집합이 진 아이디얼임을 반드시 확인하십시오!). (a)에서는 무한 오름 사슬이 주어지지 않으므로, 초른의 보조정리를 사용할 필요가 없습니다.

**5F.** 아이디얼  $(0)$ 은 물론 둘 다에서 소 아이디얼입니다. 또한, 두 환 모두 PID입니다.

$\mathbb{C}[x]$ 의 경우, 각  $z \in \mathbb{C}$ 에 대해 소 아이디얼  $(x - z)$ 를 얻습니다.

$\mathbb{R}[x]$ 의 경우, 각  $a \in \mathbb{R}$ 에 대해 소 아이디얼  $(x - a)$ 를 얻고, 켈레 관계에 있는 두 개의 비실수근을 갖는 각 이차식에 대해 소 아이디얼  $(x^2 - ax + b)$ 를 얻습니다.

**5G<sup>†</sup>.** 하나뿐이며, 극대가 아닌 아이디얼  $(0)$ 입니다. 그 외의 모든 소 아이디얼은 극대라고 주장합니다.

실제로,  $I$ 를 임의의 아이디얼(반드시 소 아이디얼일 필요는 없음)이라 하고,  $a + b\sqrt{2017}$ 을 그 안의 0이 아닌 원소라 하겠습니다. 그러면  $I$ 는  $(a^2 - 2017b^2)$ 도 포함합니다. 이는  $I$ 를 법으로 취할 때 정수  $n := |a^2 - 2017b^2| \neq 0$ 을 법으로 취해도 됨을 의미합니다.

따라서  $R$ 의 모든 원소는  $I$ 를 법으로 하여  $x + y\sqrt{2017}$  형태의 원소와 동치이며, 여기서  $x, y \in \{0, 1, \dots, n-1\}$ 입니다. 다시 말해, 몫  $R/I$ 는 많아야 유한개의 원소를 가집니다.

$I$ 가 소 아이디얼일 때,  $R/I$  역시 정역임이 따라 나옵니다. 유한개의 원소를 가지는 정역은 반드시 체여야 합니다. 따라서  $R/I$ 가 체라는 사실로부터,  $I$ 가 극대 아이디얼임을 결론지을 수 있습니다.

**5H.** 아이디얼은  $(0)$ ,  $(1) = R$ , 그리고 각  $n \geq 1$ 에 대해  $(5^n) = 5^n R$ 입니다. 아이디얼  $(0)$ 은 소 아이디얼이고 아이디얼  $(5)$ 는 극대 아이디얼입니다 (몫  $R/(5) \cong \mathbb{F}_5$ 가 체이기 때문입니다).

**6A<sup>†</sup>.** 부동점의 유일성은,  $T(p) = p$ 이고  $T(q) = q$ 이면서  $p \neq q$ 라면 이를 주어진 식에 대입했을 때 바로 모순이 나온다는 사실로부터 따라 나옵니다. 따라서 주된 과제는 부동점이 존재함을 보이는 것입니다.

임의의 점  $x_0$ 에서 시작합시다.  $x_1 = T(x_0)$ ,  $x_2 = T(x_1)$ ,  $x_3 = T(x_2)$ , ...라 합시다. 우리는  $(x_0, x_1, x_2, \dots)$ 가 코시 수열임을 주장합니다. 실제로,  $r := 0.999 < 1$ 이고  $c := d(x_0, x_1)$ 이라 하면,

$$\begin{aligned} d(x_1, x_2) &< r \cdot c \\ d(x_2, x_3) &< r^2 \cdot c \\ d(x_3, x_4) &< r^3 \cdot c \\ &\vdots \end{aligned}$$

따라서 충분히 큰  $M < N$ 에 대해 다음이 성립합니다.

$$d(x_M, x_N) < (r^M + r^{M+1} + \dots + r^{N-1}) \cdot c < \frac{r^M}{1-r} \cdot c$$

이는  $M$ 이 충분히 크면 0으로 수렴합니다.

따라서  $M$ 이 완비이므로, 수열은 어떤 극한  $x$ 로 수렴해야 합니다.  $T$ 가 연속이므로 다음을 얻습니다.

$$T(x) = T\left(\lim_{n \rightarrow \infty} x_n\right) = \lim_{n \rightarrow \infty} T(x_n) = \lim_{n \rightarrow \infty} x_{n+1} = x$$

원하는 바와 같습니다.

**6B.** (a) 부분은 본질적으로 정의에 의해 성립합니다. 공간  $M$ 은 거리가 1을 넘지 않으므로 유계이지만, 유한 개의  $\frac{1}{2}$ -근방으로  $M$ 을 덮을 수 없으므로 전유계는 아닙니다. 공간  $M$ 은 실수의 수열이 통상적인 의미로 수렴하면  $M$ 에서도 수렴하므로 완비입니다.  $N$ 의 경우, 수열  $-1, -2, \dots$ 은 코시 수열이지만 수렴하지 않으며, 명백히 유계도 아닙니다.

(b)를 보이기 위해, 항등 사상(!)이 연속이므로 이는  $M \cong \mathbb{R}$ 과  $\mathbb{R} \cong N$ 의 위상동형사상이 됩니다.

이는  $M$ 이 완비이면서 유계임에도 불구하고  $N$ 은 완비도 유계도 아니지만  $M \cong N$ 임을 보여줍니다. 반면, 나중에 우리는 완비이면서 전유계인 것이 콤팩트함을 함의함을 보게 될 것인데, 이는 위상동형사상 아래 보존되는 매우 강력한 성질입니다.

**6D.** <https://math.stackexchange.com/q/556150/229197>를 참조하십시오.

**7E.** (a)는 간단합니다: 모순을 가정하여  $p$ 의 연결 성분이  $X$ 에서 열려 있는 두 공집합이 아닌 집합  $U \sqcup V$ 의 서로소인 합집합이라 합시다. 일반성을 잃지 않고  $p \in U$ 라 가정합니다.  $S$ 를  $p$ 를 포함하면서  $V$ 와 교차하는 부분공간 중 하나라 합시다. 그러면  $S = (S \cap U) \sqcup (S \cap V)$ 는  $S$ 를  $S$ 에서 열려 있는 두 집합의 서로소인 합집합으로 다시 쓴 것이 되어,  $S$ 의 연결성과 모순됩니다.

(다만  $S$ 가  $X$ 에서 반드시 열려 있는 것은 아니므로, 집합  $S \cap U$ 와  $S \cap V$  역시  $X$ 에서 반드시 열려 있는 것은 아님에 유의하십시오.)

(b)에 대해서는, 칸토어 집합이나  $p$ 진수와 같은 임의의 완전 비연결 공간을 취하는 것이 반례가 됩니다.

**7G.**  $d(x, y) = 2017^{-n}$ 이라 합시다. 여기서  $n$ 은  $n!$ 이  $|x - y|$ 을 나누는 가장 큰 정수입니다.

**7H.** 각 구간에서 유리수를 하나씩 고를 수 있으며, 유리수는 가산개밖에 없습니다. 끝!

**8A.** 콤팩트성은 동형사상 아래 보존되지만,  $[0, 1]$ 은 콤팩트한 반면  $(0, 1)$ 은 그렇지 않습니다.

**8E.**  $p_i = (x_i, y_i)$ 가  $X \times Y$  안의 수열이라 합시다 ( $i = 1, 2, \dots$ ).  $X$ 쪽을 보면, 어떤 부분 수열이 수렴합니다: 예시를 위해 그것이  $x_1, x_4, x_9, x_{16}, \dots \rightarrow x$ 라고 합시다. 그러면 대응하는 수열  $y_1, y_4, y_9, y_{16}, \dots$ 을 살펴봅시다.  $Y$ 의 콤팩트성을 이용하면, 이는 수렴하는 부분수열을 가지며, 예를 들어  $y_1, y_{16}, y_{81}, y_{256}, \dots \rightarrow y$ 라고 합시다. 그러면  $p_1, p_{16}, p_{81}, \dots$ 는  $(x, y)$ 로 수렴할 것입니다.

흔한 실수 하나는 그저  $(x_n)$ 이 수렴하는 부분수열을 가지고  $(y_n)$ 도 마찬가지라고 결론짓는 것입니다. 하지만 이 수열들은 전혀 무관할 수 있습니다. 이 증명이 성립하려면, 먼저  $X$ 의 콤팩트성을 적용하고, 그 다음 여기서 한 것처럼 결과로 얻은 걸러진 수열에  $Y$ 의 콤팩트성을 적용해야 합니다.

**8H.** 다음 풀이는 Royce Yao의 것입니다. 우리는 대우를 보입니다:  $M$ 이 콤팩트하지 않으면, 동형사상이면서 유계가 아닌 거리가 존재합니다.

주요 단계는 유계가 아닌 연속 함수  $F: M \rightarrow \mathbb{R}$ 를 구성하는 것입니다. 이러한 함수  $F$ 가 정의되고 나면, 거리는

$$d'(x, y) := d(x, y) + |F(x) - F(y)|$$

문제를 해결할 것입니다.

그러면, 수렴하는 부분수열이 없는  $M$ 의 수열  $a_1, a_2, \dots$ 를 생각합시다. 각  $a_i$ 에 대해, 다음을 만족하는 반지름  $r_i$ 가 존재합니다

$$0 < r_i < \frac{1}{2} \min_{j \neq i} d(a_i, a_j)$$

$C_i$ 를  $a_i$ 를 중심으로 하고 반지름이  $r_i$ 인 열린 공으로 정의합니다. 모든 공은 서로소임에 주의하십시오. 그러면,  $F$ 를 다음과 같이 정의합니다

$$F(x) = \begin{cases} 0 & x \notin C_i \\ \frac{i}{r_i}(r_i - d(x, a_i)) & x \in C_i \end{cases}$$

이는 연속함수임을 알 수 있습니다. 그러면,  $i$ 가 무한대로 갈 때  $F(a_i)$ 를 고려함으로써  $F$ 가 유계가 아님을 알 수 있습니다.

- 8I. (a) 부분은 칸토어 교집합 정리(문제 8D)로부터 따라옵니다. 귀류법을 위해 그러한 분할이 존재한다고 가정합니다. 원  $C_0$  중 아무거나 하나를 택하고,  $K_0$ 를 경계가  $C_0$ 인 닫힌 원판이라 합시다. 이제  $C_0$ 의 중심을 지나는 원  $C_1$ 을 택하고,  $K_1$ 을 경계가  $C_1$ 인 닫힌 원판이라 합시다. 이런 방식을 반복하면, 중첩된 수열  $K_0 \supseteq K_1 \supseteq \dots$ 를 얻으며  $C_i$ 의 반지름은 0에 수렴합니다(각각이 이전 것의 절반 이하이기 때문입니다). 따라서 어떤 점  $p$ 가  $\bigcap_n K_n$ 에 속하게 되는데 이는 불가능합니다.

이제 (b) 부분에 대해, 다시 귀류법을 위해 원들의 분할이 존재한다고 가정합니다.  $p$ 는 포함하지만  $q$ 는 포함하지 않는 원은 마젠타색으로,  $q$ 는 포함하지만  $p$ 는 포함하지 않는 원은 시안색으로 칠합니다.  $p$  자신은 마젠타색으로,  $q$  자신은 시안색으로 칠합니다. 마지막으로,  $p$ 와  $q$ 를 모두 포함하는 원은 네온 옐로우색으로 칠합니다. (원을 색칠한다고 할 때는, 그 위의 모든 점을 색칠한다는 뜻입니다.)

(a)의 논증을 반복하면  $p$ 도  $q$ 도 둘러싸지 않는 원은 존재하지 않습니다. 따라서 모든 점은 마젠타색, 시안색, 또는 네온 옐로우색 중 하나입니다. 이제 임의의 마젠타색 원이 주어지면, 그 내부는 전부 마젠타색임에 주의하십시오. 사실, 마젠타색 원들은 (서로 교차할 수 없으므로) 포함 관계에 의해 전순서를 이룰 수 있습니다. 그러므로 두 경우를 고려합니다.

- 만약 포함 관계에서 극대인 마젠타색 원(즉, 다른 어떤 마젠타색 원에도 포함되지 않는 마젠타색 원)이 존재한다면, 모든 마젠타색 점들의 집합은 단지 하나의 닫힌 원판입니다.
- 그러한 마젠타색 원이 존재하지 않는다면, 마젠타색 점들의 집합은 모든 마젠타색 원들의 내부의 합집합으로도 표현할 수 있습니다. 이는 열린집합들의 합집합이므로, 그 자체가 열려 있습니다.

결론적으로 마젠타색 점들의 집합은 닫힌 원판이거나 열린집합입니다. 시안색 점들의 집합에 대해서도 마찬가지입니다. 더욱이, 이러한 점들의 집합은 불록합니다.

문제를 마무리하기 위해:

- 네온 옐로우색 점이 없다고 가정합니다. 마젠타색 점들이 닫힌 원판을 이룬다면, 시안색 점들은  $\mathbb{R}^2$ 에서 원판을 뺀 것이 되는데 이는 불록하지 않습니다. 모순입니다. 그러므로 마젠타색 점들은 열려 있어야 합니다. 마찬가지로 시안색 점들도 열려 있어야 합니다. 그러나  $\mathbb{R}^2$ 는 연결되어 있으므로, 두 열린집합의 합집합으로 쓰일 수 없습니다.
- 이제 네온 옐로 점들이 있다고 가정합니다. 포함관계에 대해 극소인 네온 옐로 원이 존재함을 주장합니다. 만약 그렇지 않다면, (a)의 논증을 반복하여 모순을 얻습니다. 왜냐하면 어떠한 네온 옐로 원이라도 지름이  $p$ 에서  $q$ 까지의 거리 이상이어야 하기 때문입니다. 따라서 내부가 모두 마젠타와 시안으로 이루어진 네온 옐로 원  $\mathcal{C}$ 를 찾을 수 있습니다. 이제 앞부분의 논증을 반복하되,  $\mathbb{R}^2$ 를  $\mathcal{C}$ 의 내부로 대체합니다.

|                   |                           | $T$ 단사 | $T$ 가 전사 | $T$ 가 동형사상 |
|-------------------|---------------------------|--------|----------|------------|
| 9A <sup>†</sup> . | $\dim V > \dim W$ 인 경우... | 없음     | 있음       | 없음         |
|                   | $\dim V = \dim W$ 인 경우... | 있음     | 가능       | 있음         |
|                   | $\dim V < \dim W$ 인 경우... | 있음     | 없음       | 없음         |

각 "결코 아님"은 랭크-널리티 정리에 의한 것입니다. 각 반례는  $V$ 의 모든 원소를 영으로 보내는 영사상으로 얻어지며, 이 사상은 확실히 단사도 전사도 아닙니다.

9B<sup>†</sup>. 이는 본질적으로 정리 9.7.6에 의해 따릅니다.

9D.  $1 \mapsto \sqrt{5}$ 이고  $\sqrt{5} \mapsto 5$ 이므로, 그 행렬은  $\begin{bmatrix} 0 & 5 \\ 1 & 0 \end{bmatrix}$ .

9G.  $V$ 를 차수가  $d/2$  이하인 실계수 다항식들의 공간(차원은  $1 + \lfloor d/2 \rfloor$ )이라 하고,  $W$ 를  $P$ 를 법으로 한 실계수 다항식들의 공간(차원은  $d$ )이라 합시다. 그러면  $\dim(V \oplus V) > \dim W$ 입니다. 따라서  $(A, B) \mapsto A + Q \cdot B$ 로 정의되는 선형 사상  $V \oplus V \rightarrow W$ 는 (예를 들어 계수-퇴화차수 정리에 의해) 양의 차원을 가지는 핵을 갖습니다.

9I<sup>\*</sup>. 다음을 고려하십시오

$$\{0\} \subsetneq \ker T \subseteq \ker T^2 \subseteq \ker T^3 \subseteq \dots \text{ 그리고 } V \supsetneq \operatorname{im} T \supseteq \operatorname{im} T^2 \supseteq \operatorname{im} T^3 \supseteq \dots$$

차원의 이유로, 이 부분공간들은 결국 안정화되어야 합니다: 어떤 큰 정수  $N$ 에 대해  $\ker T^N = \ker T^{N+1} = \dots$  이고  $\operatorname{im} T^N = \operatorname{im} T^{N+1} = \operatorname{im} T^{N+2} = \dots$  입니다. 이런 일이 일어나면,  $T^N$ 이  $\operatorname{im} T^N$ 의 자기동형사상이므로  $\ker T^N \cap \operatorname{im} T^N = \{0\}$ 입니다. 한편, 계수-퇴화차수 정리에 의해  $\dim \ker T^N + \dim \operatorname{im} T^N = \dim V$ 도 성립합니다. 따라서 차원의 이유로  $V = \ker T^N \oplus \operatorname{im} T^N$ 입니다.

10A. 그것은 그냥  $\dim V = 2018$ 입니다. 결국 조르당 블록들의 차원을 더하는 것이기 때문입니다...

10B. (a):  $T$ 를 그러한 기저에서 행렬로 표현하면 대각행렬을 얻습니다. (b): 이는 단지 각 조르당 블록의 차원이 1이라는 것을 말하는 것이며, 이것이 우리가 원했던 바입니다. (여기서는 조르당 표준형의 유일성을 암묵적으로 사용하고 있습니다.)

10C.  $+1$  고유공간은  $e_1 + e_2$ 로 생성됩니다.  $-1$  고유공간은  $e_1 - e_2$ 로 생성됩니다.

10E.  $+1$  고유공간은  $1 + x^2$ 과  $x$ 로 생성됩니다.  $-1$  고유공간은  $1 - x^2$ 으로 생성됩니다.

10F. 상수 함수는 미분하면 0이 되며, 이들이 유일한 0-고유벡터입니다. 다른 고유벡터는 있을 수 없습니다. 왜냐하면  $\deg p > 0$ 이면  $\deg p' = \deg p - 1$ 이므로,  $p'$ 이  $p$ 의 상수 실수배라면 반드시  $p' = 0$ 이어야 하고, 따라서  $p$ 는 상수이기 때문입니다.

10G.  $e^{cx}$ 는 모든  $c$ 에 대한  $c$ -고유벡터의 예시입니다. 미분방정식을 알고 있다면, 이것들이 모든 예시를 생성한다는 것을 알 수 있습니다!

11A. 우리는 이미 어떤 기저에서든 대각합이 항상 고윳값들의 합임을 보았습니다. 특히, 앞 장에서의 조르당 표준형 기저를 선택하면, 조르당 표준형이 그 대각 성분으로 고윳값들을 가지므로 결과가 성립합니다.

11C<sup>†</sup>. 좌표를 이용한 계산을 제시할 수도 있지만, 우리는 대신 더 깔끔한 증명을 제시하고자 합니다. 이는 다음 도식을 그리는 것과 같습니다.

$$\begin{array}{ccccc}
 & (W^\vee \otimes V) \otimes (V^\vee \otimes W) = (V^\vee \otimes W) \otimes (W^\vee \otimes V) & & & \\
 \swarrow \text{compose} & \downarrow & & \downarrow & \searrow \text{compose} \\
 \operatorname{Hom}(W, W) & \longleftrightarrow & W^\vee \otimes W & & V^\vee \otimes V \longleftrightarrow \operatorname{Hom}(V, V) \\
 & \searrow \text{Tr} & \downarrow \text{ev} & & \downarrow \text{ev} \quad \swarrow \text{Tr} \\
 & & k & \xlongequal{\quad} & k
 \end{array}$$

순수 텐서  $\xi_W \otimes v \otimes \xi_V \otimes w$ 에서 확인함으로써 가운데 사각형이 가환함을 쉽게 확인할 수 있습니다. 따라서 바깥쪽 육각형이 가환하며 이것으로 증명이 끝납니다. 이는 사실 기저를 이용한 증명과 동일한데, 결국 어딘가에 1이 있고 나머지는 0인 행렬에 대해 주장이 성립함을 확인한 다음 선형성으로 확장하는 것에 해당합니다.

11D. <https://mks.mff.cuni.cz/kalva/putnam/psoln/psol1886.html>를 참조하십시오.

12D. (문제 9B<sup>†</sup>에 의해) "동형사상"을 "단사"로 바꿔 쓸 수 있음을 기억하십시오.

0이 아닌 어떤  $v$ 에 대해  $T(v) = 0$ 이면,  $e_1 = v$ 가 되도록 기저를 택했을 때  $\wedge^n(T)$ 가  $e_1 \wedge \dots$ 를  $0 \wedge T(e_2) \wedge \dots = 0$ 으로 보낸다는 것을 알 수 있으므로, 이는 영사상이 되고 따라서  $\det T = 0$ 입니다.

반대로  $T$ 가 동형사상이면  $S$ 를 그 역사상이라고 합시다. 그러면  $1 = \det(\text{id}) = \det(S \circ T) = \det S \det T$ 이므로  $\det T \neq 0$ 입니다.

12E. 귀류법으로 증명합니다.  $v$ 를 소들의 무게를 성분으로 하는 길이 1000의 벡터라고 합시다. 대각선 성분은 0이고 비대각선 성분은  $\pm 1$ 인 행렬  $M$ 이 존재하여  $Mv = 0$ 이라고 가정합니다. 하지만  $\det M \pmod{2}$ 는  $\{1, \dots, 1000\}$ 의 교란순열 개수와 같으며, 이는 홀수입니다. 따라서  $\det M$ 은 홀수이고 특히 0이 아니므로,  $M$ 은 가역입니다. 따라서  $Mv = 0 \implies v = 0$ 이 되어 모순입니다.

12F. 답은 다음과 같습니다

$$\begin{bmatrix} t & t \\ t & t \end{bmatrix} \quad \text{그리고} \quad \begin{bmatrix} -3t & -t \\ t & 3t \end{bmatrix}$$

$t \in \mathbb{R}$ 에 대해서입니다. 이들은  $k = 3$ 을 취함으로써 성립합니다.

이제 이것들이 유일한 해임을 보이기 위해, 등차수열 행렬을 생각합시다

$$M = \begin{bmatrix} a & a+e \\ a+2e & a+3e \end{bmatrix}.$$

단  $e \neq 0$ 입니다. 이 행렬의 특성다항식은  $t^2 - (2a+3e)t - 2e^2$ 이고, 판별식은  $(2a+3e)^2 + 8e^2$ 이므로 서로 다른 두 실근을 가집니다. 더욱이  $-2e^2 \leq 0$ 이므로 두 근 중 하나가 0이거나 두 근의 부호가 서로 반대입니다. 이제 다음과 같이 써서  $M$ 을 대각화할 수 있습니다

$$M = \begin{bmatrix} s & -q \\ -r & p \end{bmatrix} \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} ps\lambda_1 - qr\lambda_2 & qs(\lambda_1 - \lambda_2) \\ pr(\lambda_2 - \lambda_1) & ps\lambda_2 - qr\lambda_1 \end{bmatrix}$$

단  $ps - qr = 1$ 입니다. 대각선 성분들의 합이 대각선 밖 성분들과 같다는 사실을 이용하면 다음을 얻습니다

$$(ps - qr)(\lambda_1 + \lambda_2) = (qs - pr)(\lambda_1 - \lambda_2) \implies qs - pr = \frac{\lambda_1 + \lambda_2}{\lambda_1 - \lambda_2}.$$

이제  $M^k \in S$ 도 성립한다면 같은 계산으로부터 다음을 얻습니다

$$qs - pr = \frac{\lambda_1^k + \lambda_2^k}{\lambda_1^k - \lambda_2^k}.$$

$x = \lambda_1/\lambda_2 < 0$ 이라고 합시다 ( $-2e^2 < 0$ 이기 때문입니다). 적절히 계산하면 다음을 얻습니다

$$\frac{x+1}{x-1} = \frac{x^k+1}{x^k-1} \implies \frac{2}{x-1} = \frac{2}{x^k-1} \implies x = x^k \implies x = -1 \text{ 또는 } x = 0$$

그리고  $k$ 는 홀수입니다.  $x = 0$ 이면  $e = 0$ 을 얻고,  $x = -1$ 이면  $2a + 3e = 0$ 을 얻는데, 이는 우리가 주장한 해들의 곡선을 줍니다.

더 깔끔한 접근법은 케일리-해밀턴 정리를 이용하는 것입니다.  $e \neq 0$ 이라고 가정하면, 위에서와 같이  $M$ 은 서로 다른 두 실수 고윳값을 가집니다.  $M$ 이 어떤 이차다항식을 만족시키므로, 어떤 상수  $c, d$ 에 대해  $M^k = cM + did$ 입니다.  $M \in S$ 이고  $M^k \in S$ 이므로  $d = 0$ 을 얻습니다. 따라서  $M^k = cM$ 이 되고, 이로부터  $M$ 의 고윳값들이 서로 음수 관계임이 따라옵니다. 이는  $\text{Tr } M = 0$ 을 의미하며, 나머지는 명백합니다.

- 12G.**  $V$ 의 기저  $e_1, \dots, e_n$ 을 택하십시오.  $T$ 가 행렬  $(x_{ij})$ 를 가진다고 하고,  $m = \dim V$ 라고 하십시오.  $\delta_{ij}$ 를 크로네커 델타라고 하십시오. 또한  $\text{Fix}(\sigma)$ 는 순열  $\sigma$ 의 고정점을 나타내고  $\text{NoFix}(\sigma)$ 는 고정되지 않은 점을 나타낸다고 하십시오.

전개하면 다음을 얻습니다.

$$\begin{aligned}
 & \det(a \cdot \text{id} - T) \\
 &= \sum_{\sigma \in S_m} \left( \text{sign}(\sigma) \cdot \prod_{i=1}^m (a \cdot \delta_{i\sigma(i)} - x_{i\sigma(i)}) \right) \\
 &= \sum_{s=0}^m \sum_{1 \leq i_1 < \dots < i_s \leq m} \sum_{\substack{\sigma \in S_m \\ \sigma \text{ 고정합니다 } i_k}} \left( \text{sign}(\sigma) \cdot \prod_{i=1}^m (a \cdot \delta_{i\sigma(i)} - x_{i\sigma(i)}) \right) \\
 &= \sum_{s=0}^m \sum_{1 \leq i_1 < \dots < i_s \leq m} \sum_{\substack{\sigma \in S_m \\ \sigma \text{ 고정합니다 } (i_k)}} \left( \text{sign}(\sigma) \cdot \prod_{i \notin (i_k)} -x_{i\sigma(i)} \prod_{i \in (i_k)} (a - x_{ii}) \right) \\
 &= \sum_{\sigma \in S_m} \left( \text{sign}(\sigma) \cdot \prod_{i \in \text{NoFix}(\sigma)} -x_{i\sigma(i)} \prod_{i \in \text{Fix} \sigma} (a - x_{ii}) \right) \\
 &= \sum_{\sigma \in S_m} \left( \text{sign}(\sigma) \cdot \left( \prod_{i \in \text{NoFix}(\sigma)} -x_{i\sigma(i)} \right) \left( \sum_{t=0}^{|\text{Fix}(\sigma)|} a^{|\text{Fix}(\sigma)|-t} \cdot \sum_{i_1 < \dots < i_t \in \text{Fix}(\sigma)} \prod_{k=1}^t -x_{i_k i_k} \right) \right) \\
 &= \sum_{\sigma \in S_m} \left( \text{sign}(\sigma) \left( \sum_{t=0}^{|\text{Fix}(\sigma)|} a^{m-t-|\text{NoFix}(\sigma)|} \sum_{\substack{X \subseteq \{1, \dots, m\} \\ \text{NoFix}(\sigma) \subseteq X \\ X \text{ 정확히 } t \text{ 개의 고정점을 가집니다}}} \prod_{i \in X} -x_{i\sigma(i)} \right) \right) \\
 &= \sum_{n=0}^m a^{m-n} \left( \sum_{\sigma \in S_m} \text{sign}(\sigma) \sum_{\substack{X \subseteq \{1, \dots, m\} \\ \text{NoFix}(\sigma) \subseteq X \\ |X|=n}} \prod_{i \in X} -x_{i\sigma(i)} \right) \\
 &= \sum_{n=0}^m a^{m-n} (-1)^n \left( \sum_{\substack{X \subseteq \{1, \dots, m\} \\ |X|=n}} \sum_{\substack{\sigma \in S_m \\ \text{NoFix}(\sigma) \subseteq X}} \text{sign}(\sigma) \prod_{i \in X} x_{i\sigma(i)} \right).
 \end{aligned}$$

따라서 다음을 보이는 것과 동치입니다.

$$\sum_{\substack{X \subseteq \{1, \dots, m\} \\ |X|=n}} \sum_{\substack{\sigma \in S_m \\ \text{NoFix}(\sigma) \subseteq X}} \text{sign}(\sigma) \prod_{i \in X} x_{i\sigma(i)} = \text{Tr} \bigwedge^n(V) \left( \bigwedge^n(T) \right)$$

이 모든  $n$ 에 대해 성립합니다.

기저 원소를 사용하여 대각합의 정의를 다음과 같이 전개할 수 있습니다.

$$\begin{aligned}
 \text{Tr} \left( \bigwedge^n(T) \right) &= \sum_{1 \leq i_1 < \dots < i_n \leq m} \left( \bigwedge_{k=1}^n e_{i_k} \right)^\vee \left( \bigwedge_{k=1}^n T(e_{i_k}) \right) \\
 &= \sum_{1 \leq i_1 < \dots < i_n \leq m} \left( \bigwedge_{k=1}^n e_{i_k} \right)^\vee \left( \bigwedge_{k=1}^n T(e_{i_k}) \right) \\
 &= \sum_{1 \leq i_1 < \dots < i_n \leq m} \left( \bigwedge_{k=1}^n e_{i_k} \right)^\vee \left( \bigwedge_{k=1}^n \left( \sum_{j=1}^m x_{i_k j} e_j \right) \right) \\
 &= \sum_{1 \leq i_1 < \dots < i_n \leq m} \sum_{\pi \in S_n} \text{sign}(\pi) \prod_{k=1}^n x_{i_{\pi(k)} k} \\
 &= \sum_{\substack{X \subseteq \{1, \dots, m\} \\ |X|=n}} \sum_{\pi \in S_X} \text{sign}(\pi) \prod_{t \in X} x_{t\pi(t)}
 \end{aligned}$$

따라서  $X$ 에 대한 순열이  $\{1, \dots, m\} - X$ 를 고정하는  $S_m$ 에 대한 순열과 전단사 관계에 있음을 보이면 충분한데, 이는 명백하며, 더욱이 부호도 명백히 일치합니다.

**12H.** <https://www3.nd.edu/~andyp/notes/CauchyBinet.pdf>를 참고하십시오.

**13C.** 동아리들을 벡터 공간  $\mathbb{F}_2^n$  안의 벡터로 해석하십시오. “내적”을 고려하여  $k$ 개의 벡터가 모두 선형독립임을 보이십시오: 서로 다른 두 동아리-벡터의 내적은 0이고, 각 동아리 벡터와 자기 자신의 내적은 1입니다. 따라서 이 벡터들은 정규직교이고, 그러므로 선형독립입니다. 따라서  $k \leq \dim \mathbb{F}_2^n = n$ 입니다.

**13D\*.** 다음과 같이 주어지는 내적 형식은

$$\langle v_1 \otimes w_1, v_2 \otimes w_2 \rangle_{V \otimes W} = \langle v_1, v_2 \rangle_V \langle w_1, w_2 \rangle_W$$

순수 텐서에 대해 정의한 다음, 선형적으로 확장합니다. (b)의 경우  $1 \leq i \leq n$ ,  $1 \leq j \leq m$ 에 대해  $e_i \otimes f_j$ 를 취하십시오.

**14B.** 부울 함수  $D: \{\pm 1\}^3 \rightarrow \mathbb{R}$ 를 다음과 같이 정의하십시오

$$D(a, b, c) = ab + bc + ca = \begin{cases} 3 & a, b, c \text{ 모두 같은} \\ -1 & a, b, c \text{ 모두 같지는 않음.} \end{cases}$$

따라서 역설적인 결과는  $D(f(x_\bullet), g(y_\bullet), h(z_\bullet)) = 3$ 일 때 발생합니다. 이제 무작위로 선택된  $x_\bullet, y_\bullet, z_\bullet$ 에 대해 다음을 계산합니다

$$\begin{aligned}
 \mathbb{E}D(f(x_\bullet), g(y_\bullet), h(z_\bullet)) &= \mathbb{E} \sum_S \sum_T \left( \hat{f}(S) \hat{g}(T) + \hat{g}(S) \hat{h}(T) + \hat{h}(S) \hat{f}(T) \right) (\chi_S(x_\bullet) \chi_T(y_\bullet)) \\
 &= \sum_S \sum_T \left( \hat{f}(S) \hat{g}(T) + \hat{g}(S) \hat{h}(T) + \hat{h}(S) \hat{f}(T) \right) \mathbb{E}(\chi_S(x_\bullet) \chi_T(y_\bullet)).
 \end{aligned}$$

이제 다음을 관찰합니다.

- $S \neq T$ 이면  $\mathbb{E} \chi_S(x_\bullet) \chi_T(y_\bullet) = 0$ 인데, 이는 예를 들어  $s \in S, s \notin T$ 인 경우  $x_s$ 가 곱의 홀짝성에 양쪽 방향으로 각각 50%의 확률로 영향을 미치며, 곱 안의 다른 변수들과 독립적이기 때문입니다.

- 반면,  $S = T$ 라고 합시다. 그러면

$$\chi_S(x_\bullet)\chi_T(y_\bullet) = \prod_{s \in S} x_s y_s.$$

$x_s y_s$ 는 확률  $\frac{1}{3}$ 로 1이고 확률  $\frac{2}{3}$ 로  $-1$ 임에 유의하십시오( $(x_s, y_s, z_s)$ 가  $3! = 6$ 가지 선택지로부터 균등하게 뽑히며, 이를 나열할 수 있기 때문입니다). 이로부터  $|S|$ 에 대한 귀납적 계산을 하면 다음을 얻습니다.

$$\prod_{s \in S} x_s y_s = \begin{cases} +1 & \text{확률로 } \frac{1}{2}(1 + (-1/3)^{|S|}) \\ -1 & \text{확률로 } \frac{1}{2}(1 - (-1/3)^{|S|}). \end{cases}$$

따라서

$$\mathbb{E}\left(\prod_{s \in S} x_s y_s\right) = \left(-\frac{1}{3}\right)^{|S|}.$$

이 모든 것을 종합하면, 이제 다음을 얻습니다.

$$\mathbb{E}D(f(x_\bullet), g(y_\bullet), h(z_\bullet)) = \sum_S \left( \hat{f}(S)\hat{g}(S) + \hat{g}(S)\hat{h}(S) + \hat{h}(S)\hat{f}(S) \right) \left(-\frac{1}{3}\right)^{|S|}.$$

그러면 다음을 얻습니다.

$$\begin{aligned} & \mathbb{E}\frac{1}{4}(1 + D(f(x_\bullet), g(y_\bullet), h(z_\bullet))) \\ &= \frac{1}{4} + \frac{1}{4} \sum_S \left( \hat{f}(S)\hat{g}(S) + \hat{g}(S)\hat{h}(S) + \hat{h}(S)\hat{f}(S) \right) \left(-\frac{1}{3}\right)^{|S|}. \end{aligned}$$

이를  $D$ 의 정의와 비교하면 원하는 결과를 얻습니다.

**15B.** 정리 9.7.6에 의해,  $V$ 의 기저  $e_1, \dots, e_n$ 과  $W$ 의 기저  $f_1, \dots, f_m$ 을  $i \leq k$ 에 대해  $T(e_i) = f_i$ 이고  $i > k$ 에 대해  $T(e_i) = 0$ 이 되도록 선택할 수 있습니다. 그러면  $i \leq k$ 에 대해  $T^\vee(f_i^\vee) = e_i^\vee$ 이고  $i > k$ 에 대해  $T^\vee(f_i^\vee) = 0$ 입니다. 위의 네 값은 모두  $k$ 와 같습니다.

**15F.** 먼저,  $T^* = p(T)$ 라고 합시다. 그러면  $T^*T = p(T) \cdot T = T \cdot p(T) = TT^*$ 이므로 완료됩니다.

역으로,  $T$ 가 내적 형식과 양립하는 방식으로 대각화 가능하다고 합시다( $V$ 가 유한 차원이므로 이는 성립합니다). 정규직교 기저를 생각합시다. 그러면  $T$ 는 주대각선상에 고윳값들을, 그 외 자리에는 0을 가지며, 이를

$$T = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}.$$

이 경우, 임의의 다항식  $q$ 에 대해 다음이 성립함을 알 수 있습니다

$$q(T) = \begin{pmatrix} q(\lambda_1) & 0 & \dots & 0 \\ 0 & q(\lambda_2) & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & q(\lambda_n) \end{pmatrix}.$$

그리고

$$T^* = \begin{pmatrix} \overline{\lambda_1} & 0 & \dots & 0 \\ 0 & \overline{\lambda_2} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \overline{\lambda_n} \end{pmatrix}.$$

따라서 우리는 단순히 모든  $i$ 에 대해  $q(\lambda_i) = \overline{\lambda_i}$ 가 되는 다항식  $q$ 만 있으면 됩니다.  $\lambda_i$ 가 유한 개이므로, 라그랑주 보간법을 이용하여 이러한 다항식을 구성할 수 있습니다.

16E<sup>†</sup>. <https://math.stackexchange.com/a/3012179/229197>

17B.  $|G| = 56$ 이고  $G$ 가 단순군이라고 가정합시다. 실로우 7-부분군을 생각해봅시다; 그 개수가  $n_7$ 이라면 ( $G$ 가 단순군이므로)  $n_7 > 1$ 이고  $n_7 \equiv 1 \pmod{7}$ 이라고 가정할 수 있으므로  $n_7 = 8$ 입니다. 이는  $G$ 에 위수 7인 원소가  $(7-1) \cdot 8 = 48$ 개 있음을 의미합니다.

그러나 실로우 2-부분군을 생각해봅시다. 이들은 각각 8개의 원소를 가지며, 따라서 실로우 2-부분군이 정확히 하나 존재한다고 결론지을 수 있습니다. 그 부분군은 정규 부분군이므로, 모순입니다.

17C. 한 가지 예시는  $\mathbb{F}_3$ 에 성분을 가지는, 다음과 같은 형태의  $3 \times 3$  행렬들로 이루어진 군입니다:

$$\begin{bmatrix} 1 & x & y \\ & 1 & z \\ & & 1 \end{bmatrix}.$$

17D.  $G$ 를 앞서 언급한 군이라 하십시오.  $G$ 가 아벨 군이면 모든 부분군이 정규 부분군이 되고,  $G$ 가 단순군이므로  $G$ 는 어떠한 부분군도 가질 수 없습니다. 위수  $p$ 인 원소를 명백히 찾을 수 있으므로,  $G$ 는 위수  $p$ 인 부분군을 가지며, 이는  $n = 1$ 인 경우에만 일어날 수 있으므로,  $G \cong \mathbb{Z}/p\mathbb{Z}$ 입니다.

따라서  $G$ 가 아벨 군이 될 수 없음을 보이는 것으로 충분합니다. 이를 위해 유군방정식을 사용할 수도 있지만, 그 대신 직접 해보겠습니다:

그렇지 않다고 가정하고,  $Z(G) = \{g \in G \mid xg = gx \forall x \in G\}$ 를 그 군의 중심이라고 하겠습니다.  $Z(G)$ 가  $G$ 에서 정규부분군이고  $G$ 가 단순군이므로,  $Z(G) = \{1_G\}$ 임을 알 수 있습니다. 하지만 이제  $G$ 가 켈레작용  $g \cdot x = gxg^{-1}$ 을 통해 자기 자신에 작용한다고 하겠습니다. 이는  $G$ 를  $\mathcal{O}_0 = \{1_G\}$ ,  $\mathcal{O}_1, \mathcal{O}_2, \dots$ 와 같은 여러 궤도로 나누며, 정의상  $1_G$ 만이 유일한 고정점이므로 다른 모든 궤도는 크기가 1보다 큽니다. 궤도-안정자군 정리에 따르면 이제 각 궤도의 크기는  $p^n$ 을 나누므로, 그 크기는 모두  $p$ 로 나눈 나머지가 0이어야 합니다.

그런데  $G$ 를 분할하는 모든 궤도에 걸쳐 합을 구하면  $|G| \equiv 1 \pmod{p}$ 를 얻게 되는데, 이는 모순입니다.

17E. 이 문제를 추가했을 때 어떤 풀이를 염두에 두었는지 기억이 나지 않습니다. <https://github.com/vEnhance/napkin/pull/268#issuecomment-2767676253>에 더 기술적인 풀이가 설명되어 있지만, 제가 원래 생각했던 것은 아닌 것 같습니다.

18D.  $G = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \dots$  이고  $H = \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \dots$  라고 합시다. 그러면 사상  $G \hookrightarrow H$ 와  $H \hookrightarrow G$ 가 존재하지만, 이 군들은 동형이 아닙니다. 예를 들어  $G$ 에는 위수가 3인 원소  $g \in G$ 가 있는데,  $g = 3g'$ 를 만족하는  $g' \in G$ 가 존재하지 않기 때문입니다.

18E. 아닙니다! 다음을 고르십시오

$$A = \mathbb{Z}[x_1, x_2, \dots]$$

$$B = \mathbb{Z}[x_1, x_2, \dots, \varepsilon x_1, \varepsilon x_2, \dots]$$

$$C = \mathbb{Z}[x_1, x_2, \dots, \varepsilon].$$

여기서  $\varepsilon \neq 0$ 이지만  $\varepsilon^2 = 0$ 입니다.  $A$ 가 뇌터 환이라는 가정을 추가하면 이 결과가 참일 것 같습니다.

19D\*. 그 연산자들은 고정된  $b \in A$ 에 대해  $T(a) = ab$  꼴인 것들입니다. 이것들이 성립함을 확인할 수 있는데,  $c \in A$ 에 대해  $T(c \cdot a) = cab = c \cdot T(a)$ 이기 때문입니다. 이것들이 전부임을 보려면, 임의의  $a \in A$ 에 대해  $T(a) = T(a \cdot 1_A) = a \cdot T(1_A)$ 임에 유의하십시오.

20C. 임의로  $v \in V$ 를 선택하면,  $v \in V$ 에 대해 원소  $g \cdot v$ 들로 생성된 부분공간은  $G$ -불변입니다; 이는 유한 차원 부분공간이므로  $V$  전체와 같아야 합니다.

21B.  $\mathbb{C}_{\text{sign}} \oplus \mathbb{C}^2 \oplus \text{refl}_0 \oplus (\text{refl}_0 \otimes \mathbb{C}_{\text{sign}})$ .

21C. 먼저, 모든  $g \in G$ 에 대해  $|\chi_W(g)| = 1$ 임을 관찰하십시오.

$$\begin{aligned} \langle \chi_{V \otimes W}, \chi_{V \otimes W} \rangle &= \langle \chi_V \chi_W, \chi_V \chi_W \rangle \\ &= \frac{1}{|G|} \sum_{g \in G} |\chi_V(g)|^2 |\chi_W(g)|^2 \\ &= \frac{1}{|G|} \sum_{g \in G} |\chi_V(g)|^2 \\ &= \langle \chi_V, \chi_V \rangle = 1. \end{aligned}$$

21D. 표는 다음과 같이 주어집니다

| $Q_8$                      | 1 | -1 | $\pm i$ | $\pm j$ | $\pm k$ |
|----------------------------|---|----|---------|---------|---------|
| $\mathbb{C}_{\text{triv}}$ | 1 | 1  | 1       | 1       | 1       |
| $\mathbb{C}_i$             | 1 | 1  | 1       | -1      | -1      |
| $\mathbb{C}_j$             | 1 | 1  | -1      | 1       | -1      |
| $\mathbb{C}_k$             | 1 | 1  | -1      | -1      | 1       |
| $\mathbb{C}^2$             | 2 | -2 | 0       | 0       | 0       |

일차원 표현들 (처음 네 행)은 준동형사상  $Q_8 \rightarrow \mathbb{C}^\times$ 를 생각함으로써 얻어집니다. 마지막 행은 이차원이며 직교성 공식을 이용해 복원할 수 있습니다.

23A. 간단한 계산에 의해,  $|\Psi\rangle = -\frac{1}{\sqrt{2}}(|\rightarrow\rangle_A \otimes |\leftarrow\rangle_B - |\leftarrow\rangle_A \otimes |\rightarrow\rangle_B)$ 입니다. 이제  $|\rightarrow\rangle_A \otimes |\rightarrow\rangle_B$ ,  $|\rightarrow\rangle_A \otimes |\leftarrow\rangle_B$ 는  $\sigma_x^A \otimes \text{id}_B$ 의 한 고유공간을 생성하고,  $|\leftarrow\rangle_A \otimes |\rightarrow\rangle_B$ ,  $|\leftarrow\rangle_A \otimes |\leftarrow\rangle_B$ 는 다른 고유공간을 생성합니다. 따라서 이는 이전과 동일합니다: +1은  $|\leftarrow\rangle_B$ 를, -1은  $|\rightarrow\rangle_B$ 를 줍니다.

24A. 프레드킨 게이트가 보편적임을 보이려면 이를 이용해 가역적으로 CCNOT 게이트를 만드는 것으로 충분합니다. 다음과 같이 시스템을 씁니다

$$\begin{aligned} (z, \neg z, -) &= \text{Fred}(z, 1, 0) \\ (x, a, -) &= \text{Fred}(x, 1, 0) \\ (y, b, -) &= \text{Fred}(y, a, 0) \\ (-, c, -) &= \text{Fred}(b, 0, 1) \\ (-, d, -) &= \text{Fred}(c, z, \neg z). \end{aligned}$$

직접 계산하면  $d = z + xy \pmod{2}$ 임을 알 수 있습니다.

**24C.**  $|\leftarrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ 로 둡니다. 그러면  $U_f$ 가 다음과 같이 보냄을 알 수 있습니다

$$|x_1\rangle \dots |x_n\rangle |0\rangle - |x_1\rangle \dots |x_n\rangle |1\rangle \xrightarrow{U_f} \pm |x_1\rangle \dots |x_n\rangle |0\rangle \mp |x_1\rangle \dots |x_n\rangle |1\rangle$$

부호는  $f(x_1, \dots, x_n) = 1$ 일 때 정확히  $+$ ,  $-$ 가 됩니다.

이제  $|0\rangle \dots |0\rangle |1\rangle$ 을 입력하면,  $H^{\otimes n+1}$ 이 이를 다음으로 사상함을 알 수 있습니다

$$2^{-n/2} \sum_{x_1, \dots, x_n} |x_1\rangle \dots |x_n\rangle |\leftarrow\rangle.$$

그러면  $U_f$  아래에서의 상은 다음과 같습니다

$$2^{-n/2} \sum_{x_1, \dots, x_n} (-1)^{f(x_1, \dots, x_n)} |x_1\rangle \dots |x_n\rangle |\leftarrow\rangle.$$

이제 마지막 큐비트를 버리면 다음이 남습니다

$$2^{-n/2} \sum_{x_1, \dots, x_n} (-1)^{f(x_1, \dots, x_n)} |x_1\rangle \dots |x_n\rangle.$$

여기에  $H^{\otimes n}$ 을 적용하면 다음을 얻습니다

$$2^{-n/2} \sum_{x_1, \dots, x_n} (-1)^{f(x_1, \dots, x_n)} \cdot \left( 2^{-n/2} \sum_{y_1, \dots, y_n} (-1)^{x_1 y_1 + \dots + x_n y_n} |y_1\rangle |y_2\rangle \dots |y_n\rangle \right)$$

$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ 이고  $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ 이므로,  $x_i = 1$ 이고  $y_i = 1$ 이 동시에 성립할 때 정확히 음의 부호가 나타나며, 따라서  $(-1)^{x_1 y_1 + \dots + x_n y_n}$  항이 생깁니다. 합의 순서를 바꾸면 다음을 얻습니다

$$2^{-n} \sum_{y_1, \dots, y_n} C(y_1, \dots, y_n) |y_1\rangle |y_2\rangle \dots |y_n\rangle$$

여기서  $C(y_1, \dots, y_n) = \sum_{x_1, \dots, x_n} (-1)^{f(x_1, \dots, x_n) + x_1 y_1 + \dots + x_n y_n}$ 입니다. 이제 마지막으로 두 경우를 고려합니다.

- $f$ 가 상수 함수라면, 다음을 알 수 있습니다

$$C(y_1, \dots, y_n) = \begin{cases} \pm 1 & y_1 = \dots = y_n = 0 \\ 0 & \text{그 외의 경우.} \end{cases}$$

이를 확인하려면,  $y_1 = \dots = y_n = 0$ 인 경우 결과가 명백함에 주목하십시오. 그렇지 않고 일반성을 잃지 않고  $y_1 = 1$ 이라 하면,  $x_1 = 0$ 에 대한 항들이 쌍을 이루어  $x_1 = 1$ 에 대한 항들과 정확히 상쇄됩니다. 따라서 이 상태에서는 측정 결과가 모두  $|0\rangle \dots |0\rangle$ 이 됩니다.

- 반면  $f$ 가 균형 함수라면, 다음을 유도할 수 있습니다

$$C(0, \dots, 0) = 0.$$

따라서 측정 결과가  $|0\rangle \dots |0\rangle$ 이 되는 경우는 전혀 없습니다.

이런 방식으로  $f$ 가 균형 함수인지 아닌지를 알 수 있습니다.

**26E.** 이는 코시 수렴의 한 응용으로, 다음을 보일 수 있기 때문입니다

$$\left| \sum_{n=M}^N (-1)^n a_n \right| \leq a_{\min\{M, N\}}.$$

실제로,  $M$ 과  $N$ 이 짝수이면 (단순화를 위해서이며, 다른 경우도 동일합니다) 다음이 성립합니다

$$\begin{aligned} a_M - a_{M+1} + a_{M+2} - \dots &= a_M - (a_{M+1} - a_{M+2}) - (a_{M+3} - a_{M+4}) \\ &\quad - \dots - (a_{N-1} - a_N) \\ &\leq a_M \\ a_M - a_{M+1} + a_{M+2} - \dots &= a_M - a_{M+1} + (a_{M+2} - a_{M+3}) + (a_{M+4} - a_{M+5}) \\ &\quad + \dots + (a_{N-2} - a_{N-1}) + a_N \\ &\geq -a_{M+1}. \end{aligned}$$

이렇게 하여 부분합의 수열이 코시 수열임을, 따라서 어떤 극한으로 수렴함을 알 수 있습니다.

**26F.** 단조이고 유계라는 가정을 포착하기 위해, 어떤  $x_i$ 에 대해  $a_n = x_1 + \dots + x_n$ 이라 씁니다. 그러면  $x_2, \dots$  는 모두 같은 부호를 가지므로 어떤 상수  $A$ 에 대해  $\sum |x_i| = A < \infty$ 입니다.

이제  $\sum a_n b_n$ 의 부분합이 코시 수열임을 증명합니다. 임의의  $\varepsilon > 0$ 을 생각합시다.  $K$  이후부터 시작하는  $b_n$ 의 꼬리 부분의 절댓값이  $\frac{\varepsilon}{A}$ 보다 작도록  $K$ 를 잡습니다. 그러면 임의의  $N > M \geq K$ 에 대해 다음이 성립합니다

$$\begin{aligned} \left| \sum_{k=M}^N a_k b_k \right| &= \left| \sum_{k=M}^N \sum_{j=1}^k b_k x_j \right| \\ &= \left| \sum_{j=1}^N \sum_{k=\max\{j, M\}}^N b_k x_j \right| \\ &= \left| \sum_{j=1}^N x_j \cdot \sum_{k=\max\{j, M\}}^N b_k \right| \\ &\leq \sum_{j=1}^N |x_j| \left| \sum_{k=\max\{j, M\}}^N b_k \right| \\ &< \sum_{j=1}^N |x_j| \cdot \frac{\varepsilon}{A} \\ &< \varepsilon \end{aligned}$$

원하는 대로입니다.

**26G.** 답은  $e - 1$ 입니다.

먼저  $e^t \geq 1 + t$ 이므로  $x_{n+1} = \log(e^{x_n} - x_n) \geq \log 1 = 0$ 임을 주목합니다. 따라서 모든  $n$ 에 대해  $x_n \geq 0$ 입니다.

다음으로 다음을 주목하십시오.

$$x_{n+1} = \log(e^{x_n} - x_n) < \log e^{x_n} = x_n.$$

따라서  $x_1, x_2, \dots$  는 음이 아닐 뿐 아니라 엄격히 감소합니다. 그러므로 어떤 극한값  $L$ 로 수렴해야 합니다.

셋째로, 다음을 관찰하십시오.

$$x_n = e^{x_n} - e^{x_{n+1}} \implies x_0 + x_1 + \dots + x_n = e^{x_0} - e^{x_n} = e - e^{x_n} < e.$$

부분합이  $e$ 로 유계이고  $x_i \geq 0$ 이므로,  $L = 0$ 임을 결론지을 수 있습니다.

마지막으로, 부분합의 극한은 다음과 같습니다.

$$\lim_{n \rightarrow \infty} e - e^{x_n} = e - e^0 = e - 1.$$

**28G.**  $f(x) = e^{x \log x}$  라고 쓴 다음 연쇄 법칙과 곱 법칙을 적용합니다:

$$\begin{aligned} f'(x) &= e^{x \log x} \cdot (x \log x)' \\ &= e^{x \log x} \cdot (1 + \log x) \\ &= x^x (1 + \log x). \end{aligned}$$

**29E.** <https://mathoverflow.net/q/81613>과 특히 <https://web.archive.org/web/20161009194815/http://mathforum.org/kb/message.jspa?messageID=387148>을 참고하십시오.

**31B\*.** 모순을 통해 진행하겠습니다. 즉  $0 = f(z_1) = f(z_2) = \dots$  이고 모두 서로 다른 수열  $z_1, z_2, \dots \rightarrow z$ 가 존재한다고 하겠습니다. 일반성을 잃지 않고  $z = 0$ 으로 두겠습니다.  $z = 0$  주변에서  $f$ 의 테일러 급수를 살펴보십시오. 가정에 의해 이 급수가 항등적으로 영이 아니므로, 이를  $a_N z^N + a_{N+1} z^{N+1} + \dots$ ,  $a_N \neq 0$ 으로 쓰겠습니다. 그러나  $h(z) = a_N + a_{N+1} z + \dots$ 의 연속성에 의해,  $h(z) \neq 0$ 인 영의 열린 근방이 존재합니다.

**31C\*.**  $S$ 를  $f = g$ 를 만족하는 점들의 내부라 하겠습니다. 정의에 의해  $S$ 는 열린집합입니다. 앞부분에 의해  $S$ 는 닫힌집합입니다:  $z_i \rightarrow z$ 이고  $z_i \in S$ 이면,  $z$ 의 어떤 열린 근방에서  $f = g$ 이므로  $z \in S$ 입니다.  $S$ 가 닫혀 있으면서 열려 있고 공집합이 아니므로,  $S = U$ 입니다.

**31E.** 주어진 점  $w \in \mathbb{C}$ 의  $\varepsilon$  이내에 상의 한 점이 있음을 보이려고 한다고 가정합니다.  $\frac{1}{f(z)-w}$ 를 살펴보고 리우빌 정리를 사용하십시오.

**32C.** <https://math.stackexchange.com/q/242514/229197>을 참고하십시오. 여기서는 2019가 3으로 대체되어 있습니다.

**39A.** 그것은 셈 측도입니다.

**41A.** 각 양의 정수  $m$ 에 대해,  $\varepsilon = 1/m$ 일 때 어떤 일이 일어나는지 생각해 봅시다. 그러면 가정에 의해, 문턱값  $N_m$ 이 존재하여 이상 집합이

$$A_m := \left\{ \omega : |X(\omega) - X_n(\omega)| \geq \frac{1}{m} \text{ 어떤 } n \text{에 대해 } n > N_m \right\}$$

측도  $\mu(A_m) = 0$ 을 갖도록 하는 문턱값  $N_m$ 이 존재합니다. 따라서 가산 합집합  $A = \bigcup_{m \geq 1} A_m$ 도 측도가 0입니다.

그러므로  $A$ 의 여집합은 측도 1을 갖습니다.  $A$ 에 속하지 않는 임의의 세계  $\omega \notin A$ 에 대해, 다음을 얻습니다

$$\lim_n |X(\omega) - X_n(\omega)| = 1$$

왜냐하면  $n > N_m$ 일 때 그 절댓값은 ( $\omega \notin A_m$ 이므로) 항상  $1/m$  이하이기 때문입니다.

41B. <https://math.stackexchange.com/a/2201906/229197>

55C.  $\alpha \equiv 0 \pmod{\mathfrak{p}}$ 이면 자명하므로, 그렇지 않은 경우를 가정합니다. 그러면  $\mathcal{O}_K/\mathfrak{p}$ 는  $N(\mathfrak{p})$ 개의 원소를 갖는 유한체입니다.  $(\mathcal{O}_K/\mathfrak{p})^*$ 를 살펴보면, 이는  $N(\mathfrak{p}) - 1$ 개의 원소를 갖는 곱셈군이므로,  $\alpha^{N(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}}$ 이며, 원하는 결과를 얻습니다.

55D<sup>†</sup>.  $J$ 가  $K$ 의 몇몇 원소들에 의해 생성된다고 가정합시다; 이들을  $\alpha_i, \beta_i \in \mathcal{A}$ 에 대해  $\frac{\beta_i}{\alpha_i}$ 로 쓸 수 있습니다. 따라서

$$J = \left\{ \sum_i \gamma_i \cdot \frac{\beta_i}{\alpha_i} \mid \alpha_i, \beta_i, \gamma_i \in \mathcal{O}_K \right\}.$$

이제 "분모를 없애 봅시다".  $\alpha = \alpha_1 \dots \alpha_n$ 이라 두고,  $\alpha J$ 가 정수 아이디얼임을 보이십시오.

55E. (a) 부분에서,  $\mathfrak{p}_i$ 가 소 아이디얼인 이유는 단지 다음이

$$\mathcal{O}_K/\mathfrak{p}_i \cong (\mathbb{Z}[x]/f)/(p, f_i) \cong \mathbb{F}_p[x]/(f_i)$$

체이기 때문이며, 이는  $f_i$ 가 기약이기 때문입니다.

(b)를 확인해 봅시다.  $p$ 를 법으로 하여 곱을 계산하면 다음을 얻습니다<sup>2</sup>

$$\prod_{i=1}^g (f_i(\theta))^{e_i} \equiv (f(\theta)) \equiv 0 \pmod{p}$$

따라서  $I \subseteq (p)$ 임을 보였습니다.

마지막으로, 크기 논증을 통해 (c)를 증명합니다. 핵심 아이디어는  $I$ 와  $(p)$ 가 실제로 같은 크기를 가져야 한다는 것이며, 이를 정확히 확인하기 위해 아이디얼 노름을 사용할 것입니다.  $(p)$ 가  $I$ 를 나누므로,  $(p) = \prod_{i=1}^g \mathfrak{p}_i^{e'_i}$ 로 쓸 수 있으며, 여기서 각  $i$ 에 대해  $e'_i \leq e_i$ 입니다.  $\mathcal{O}_K/(p) \cong \mathbb{Z}/p\mathbb{Z}[x]/(f)$ 의 크기가  $p^{\deg f}$ 임에 주목하십시오. 마찬가지로, 각  $i$ 에 대해  $\mathcal{O}_K/\mathfrak{p}_i$ 의 크기는  $p^{\deg f_i}$ 입니다. 이제  $e'_i$ 를 사용하여  $N((p))$ 를 계산하고 결과를 비교하십시오.

55F. 앞서와 같이,  $\omega := e^{\frac{2i\pi}{k}}$ 로 둡시다.  $K = \mathbb{Q}(\omega)$ 라 하고,  $p\mathbb{Z}$  위에 있는  $\mathcal{O}_K$ 의 임의의 소 아이디얼  $\mathfrak{p}$ 를 선택합시다.

다음은 알고 있습니다

$$\prod_{i=0}^{k-1} (2025 - \omega^i) = 2025^k - 1 \in (p) \subseteq \mathfrak{p}$$

그리고  $\mathfrak{p}$ 는 소 아이디얼이므로, 어떤  $i$ 에 대해  $2025 - \omega^i \in \mathfrak{p}$ 임을 알 수 있습니다. 마찬가지로 어떤  $j$ 에 대해  $2026 - \omega^j \in \mathfrak{p}$ 입니다. 빼면,

$$(2026 - \omega^j) - (2025 - \omega^i) = 1 + \omega^i - \omega^j \in \mathfrak{p} \implies p \mid N_{K/\mathbb{Q}}(1 + \omega^i - \omega^j).$$

$6 \nmid k$ 이므로  $1 + \omega^i - \omega^j \neq 0$ 이 성립하고, 따라서  $p$ 는 위의 노름 이하입니다. 그러나 정의로부터 직접,

$$\left| N_{\mathbb{Q}(\omega)/\mathbb{Q}}(1 + \omega^i - \omega^j) \right| = \prod_{\gcd(m,k)=1, 1 \leq m \leq k} |1 + \omega^{mi} - \omega^{mj}| \leq 3^k.$$

<sup>2</sup>예를 들어,  $(3, 1 + \sqrt{7})(3, 1 - \sqrt{7})$ 이 (3)에 포함됨을 알고 싶다고 합시다. 전체 계산을 수행하여  $(9, 3 + 3\sqrt{7}, 3 - 3\sqrt{7}, 6)$ 을 얻을 수 있습니다. 하지만 모든 원소가 3으로 나누어떨어진다는 사실만 필요하다면, 처음부터 "3을 법으로 하여"  $(1 + \sqrt{7})(1 - \sqrt{7}) = (6)$ 만 살펴봐도 충분합니다. 나머지 곱들은 모두 명백히 3의 인수를 가질 것입니다.

**56F.**  $K = \mathbb{Q}(\sqrt{-5})$ 라 하자. 민코프스키 경계를 이용하여  $\text{Cl}_K$ 의 위수가 2임을 확인하십시오; 또한  $\Delta_K = -20$ 입니다. 이제  $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ 이고,  $x^2 + 5$ 는  $p$ 를 법으로  $(x+k)(x-k)$ 로 인수분해됨에 주목하십시오; 따라서  $\mathcal{O}_K$ 에서  $(p) = (p, \sqrt{-5} + k)(p, \sqrt{-5} - k) = \mathfrak{p}_1 \mathfrak{p}_2$ 가 성립합니다.  $p > 5$ 인 경우 소수  $p$ 는 분기하지 않으며  $\mathfrak{p}_1 \neq \mathfrak{p}_2$ 입니다, 이는  $\Delta_K = -20$ 이기 때문입니다.

그러면  $(p^2) = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2^2$ 입니다. 유수군의 위수가 2이므로  $\mathfrak{p}_1^2$ 과  $\mathfrak{p}_2^2$ 은 모두 주 아이디얼이며,  $\mathfrak{p}_1 \neq \mathfrak{p}_2$ 이므로 이 둘은 서로 다릅니다. 따라서  $p^2$ 은  $\mathcal{O}_K$ 의 두 원소의 자명하지 않은 곱이며, 이로부터 원하는 인수분해를 이끌어낼 수 있습니다.

**56G.**  $\mathfrak{p}^n$ 이 주 아이디얼이 되는 양의 정수  $n$ 을 잡습니다(예를 들어  $n = |\text{Cl}_K|$ ).  $\mathfrak{p}^n = (x)$ 이면,  $x$ 가 원하는 조건을 만족합니다.

**59A\*.** 이는 단순히  $\mathbb{Z}/p - 1\mathbb{Z}$ 인데, 이는  $\zeta_p$ 가  $p - 1$ 개의 원시 단위근 중 하나(임의의 것)로 보내져야 하기 때문입니다.

**59D.** 비슷하지만 동일하지는 않은 문제가 여기에서 풀렸습니다: <https://aops.com/community/c6h149153p842956>.

**59F.** <https://www.math.cornell.edu/~kbrown/6310/primitive.pdf>

**60A<sup>†</sup>.** 피보나치 수열이 다음과 같이 주어짐을 상기하십시오.

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

여기서  $\alpha = \frac{1+\sqrt{5}}{2}$ 와  $\beta = \frac{1-\sqrt{5}}{2}$ 는  $P(X) := X^2 - X - 1$ 의 두 근입니다.

$p = 127$ 이라 하고  $p$ 를 법으로 작업합니다.

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{2}{5}\right) = -1$$

이므로, 5가 127을 법으로 이차 잉여가 아님을 알 수 있습니다. 따라서 다항식  $P(X)$ 는  $\mathbb{F}_p[X]$ 의 다항식으로 볼 때 기약다항식입니다(직관적으로,  $\alpha$ 와  $\beta$ 는  $\mathbb{F}_p$ 의 원소가 아닙니다). 따라서 우리는 유한체  $\mathbb{F}_{p^2}$ 에서 작업할 것인데, 이는  $\mathbb{F}_p$  위에서  $P(X)$ 의 분해체입니다. 다시 말해,  $\alpha$ 와  $\beta$ 를  $\mathbb{F}_{p^2}$ 의 원소로 해석하되, 이는  $\mathbb{F}_p$ 에는 속하지 않습니다.

$\sigma: \mathbb{F}_{p^2} \rightarrow \mathbb{F}_{p^2}$ 을  $t \mapsto t^p$ 로 정의하고, 이를  $\text{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ 의 비자명한 원소라 하겠습니다; 다시 말해,  $\sigma$ 는  $\mathbb{F}_{p^2}$ 의 항등이 아닌 자기동형사상입니다.  $\sigma$ 의 고정점이  $\mathbb{F}_p$ 의 원소들이므로, 이는  $\sigma$ 가  $P$ 의 두 근 중 어느 것도 고정하지 않음을 의미합니다; 따라서 다음이 성립해야 합니다

$$\begin{aligned}\alpha^p &= \sigma(\alpha) = \beta \\ \beta^p &= \sigma(\beta) = \alpha.\end{aligned}$$

이제 다음을 계산합니다

$$\begin{aligned}F_p &= \frac{\alpha^p - \beta^p}{\alpha - \beta} = \frac{\beta - \alpha}{\alpha - \beta} = -1. \\ F_{p+1} &= \frac{\alpha^{p+1} - \beta^{p+1}}{\alpha - \beta} = \frac{\alpha\beta - \beta\alpha}{\alpha - \beta} = 0. \\ F_{2p+1} &= \frac{\alpha^{2p+1} - \beta^{2p+1}}{\alpha - \beta} = \frac{\beta^2\alpha - \alpha^2\beta}{\alpha - \beta} = -\alpha\beta = 1. \\ F_{2p+2} &= \frac{\alpha^{2p+2} - \beta^{2p+2}}{\alpha - \beta} = \frac{\beta^2\alpha^2 - \alpha^2\beta^2}{\alpha - \beta} = 0.\end{aligned}$$

따라서 주기는  $2p+2$ 를 나누어야 하지만  $p+1$ 은 나누지 않아야 합니다.

이제 처음으로 정확한 수치  $p=127$ 을 사용하여 주기가  $2p+2=256=2^8$ 을 나누지만  $p+1=128=2^7$ 은 나누지 않음을 확인합니다. (이전에는  $(5/p)=-1$ 이라는 사실만 사용했습니다.) 따라서 주기는 정확히 256이어야 합니다.

**62A.** 다음은 여전히 참입니다

$$\left(\frac{2}{q}\right) = 1 \iff \sigma_2 \in H \iff 2 \text{는 } \mathbb{Z}\left[\frac{1}{2}(1+\sqrt{q^*})\right] \text{에서 분해합니다.}$$

이제, 2가 이 환에서 분해될 필요충분조건은  $t^2-t-\frac{1}{4}(1-q^*)$ 가 법 2에서 인수분해되는 것입니다. 이는  $q^* \equiv 1 \pmod{8}$ 일 필요충분조건으로 일어납니다. 이것이 정확히  $q \equiv \pm 1 \pmod{8}$ 일 때임을 확인할 수 있으며, 이로부터 결론이 얻어집니다.

**62C<sup>†</sup>.**  $K = \mathbb{Q}(\zeta_m)$ 이라 합시다. 이전과 정확히 같은 방식으로  $\text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ 임을 보일 수 있습니다. 특히,  $\text{Gal}(K/\mathbb{Q})$ 는 아벨 군이므로 그 켄레류들은 단원소 집합이며, 그 개수는  $\phi(m)$ 개입니다.

$p$ 가 충분히 크기만 하면, 그것은 비분기이며  $p$  위의 임의의  $\mathfrak{p}$ 에 대해  $\sigma_p = \text{Frob}_{\mathfrak{p}}$ 입니다( $m$ 제곱근들이 법  $p$ 에서 서로 다를 것이기 때문입니다; 법  $p$ 에서  $x^m - 1$ 을 다시 미분해 보십시오).

**62E.** 이 풀이는 David Corwin에 의한 것입니다. 원시근에 의해, 이는  $\mathbb{Z}/(p-1)\mathbb{Z}$  위에서의  $\times 3$  작용과 같습니다.  $\zeta$ 를  $(p-1)$ 차 단위근이라 하십시오.

다음을 생각해봅시다

$$d = \prod_{0 \leq i < j < p-1} (\zeta^i - \zeta^j).$$

이는 다항식  $X^{p-1} - 1$ 의 판별식의 제곱근입니다. 다시 말해  $d^2 \in \mathbb{Z}$ 입니다. 실제로 초등적인 방법으로 다음을 계산할 수 있습니다

$$(-1)^{\binom{p-1}{2}} d^2 = -(p-1)^{p-1}$$

이제 확대체  $K = \mathbb{Q}(d)$ 를 취하고, 다음을 주목하십시오

- $p \equiv 3 \pmod{4}$ 이면,  $d = (p-1)^{\frac{1}{2}(p-1)}$ 이므로  $K = \mathbb{Q}$ 입니다.
- $p \equiv 1 \pmod{4}$ 이면,  $d = i(p-1)^{\frac{1}{2}(p-1)}$ 이므로  $K = \mathbb{Q}(i)$ 입니다.

어느 쪽이든,  $\mathcal{O}_K$ 에서  $(3) \subseteq \mathcal{O}_K$  위에 있는 소 아이디얼을  $\mathfrak{p}$ 라 하십시오. 그러면  $\sigma = \text{Frob}_{\mathfrak{p}}$ 를 모든  $x$ 에 대해  $\sigma(x) = x^3 \pmod{\mathfrak{p}}$ 를 만족하는 유일한 원소라고 하십시오. 그러면 다음을 관찰할 수 있습니다

$$\sigma(d) \equiv \prod_{0 \leq i < j < p-1} (\zeta^{3i} - \zeta^{3j}) \equiv \begin{cases} +d & \pi \text{가 짝수이면} \\ -d & \pi \text{가 홀인 경우} \end{cases} \pmod{\mathfrak{p}}.$$

이제  $K = \mathbb{Q}$ 이면,  $\sigma$ 는 항등원이므로  $\sigma$ 는 짝순열입니다. 반대로  $K = \mathbb{Q}(i)$ 이면, 3이 분해되지 않으므로  $\sigma(d) = -d$ 이고(실제로  $\sigma$ 는 복소켄레입니다) 따라서  $\pi$ 는 홀순열입니다.

$p \equiv 2 \pmod{3}$ 이라는 조건은 오직  $\pi$ 가 실제로 순열임을(따라서  $d \neq 0$ 임을) 보장하기 위해서만 쓰인다는 점에 주의하십시오. 이 조건은 풀이에서 본질적인 역할을 하지 않습니다.

**63A<sup>†</sup>.** 어떤  $m$ 에 대해  $f(L/\mathbb{Q}) \mid m\infty$ 라고 합시다. 그러면 앞서 나온 예에 의해 다음 연쇄를 얻습니다.

$$P_{\mathbb{Q}}(m\infty) = H(\mathbb{Q}(\zeta)/\mathbb{Q}, m\infty) \subseteq H(L/\mathbb{Q}, m\infty) \subseteq I_{\mathbb{Q}}(m\infty).$$

따라서 포함 관계 역전에 의해 완료됩니다.

**63B<sup>†</sup>.**  $m = 1$ 로 다카기 존재 정리를 적용하여  $H(E/K, 1) = P_K(1)$ 을 만족하는 비분기 확장  $E/K$ 를 얻습니다. 이것이 원하는 것임을 주장합니다:

- 포함관계에 대해 극대임을 보이려면, 이러한 성질을 갖는 다른 임의의 확장  $M/K$ 가 도체 1을 가짐(도체를 나누는 소수가 없음)을 주목하십시오. 그러면  $P_K(1) = H(E/K, 1) \subseteq H(M/K, 1) \subseteq I_K(1)$ 이 성립하므로, 포함관계를 뒤집으면  $M \subseteq E$ 를 얻습니다.
- $\text{Gal}(E/K) \cong I_K(1)/P_K(1) = C_K(1)$ 이 성립하며, 이는 유수군입니다.
- 앞 부분의 동형사상은 아르틴 기호로 주어집니다. 따라서  $\mathfrak{p}$ 가 완전분해된다는 것은  $\left(\frac{E/K}{\mathfrak{p}}\right) = \text{id}$ 인 것과 동치이며, 이는 다시  $\mathfrak{p}$ 가 주 아이디얼( $C_K(1)$ 에서 자명함)인 것과 동치입니다.

이로써 증명이 완료됩니다.

**68A.** 주된 관찰은  $\mathcal{A} \times \mathbf{2}$ 에는  $\mathcal{A}$  안의 사상( $(f, \text{id}_2)$  꼴)이 있고, 그다음  $\mathcal{A}$ 의 두 복사본을 가로지르는 사상( $(\text{id}_A, 0 \leq 1)$  꼴)이 있다는 것입니다. 하지만 사상  $(f, 0 \leq 1)$ 이 더 있습니다: 그럼에도 이들은 다음과 같은 합성으로 생각될 수 있습니다.

$$(f, 0 \leq 1) = (f, \text{id}_2) \circ (\text{id}_A, 0 \leq 1) = (\text{id}_A, 0 \leq 1) \circ (f, \text{id}_2).$$

이제 함수  $\alpha: \mathcal{A} \times \mathbf{2} \rightarrow \mathcal{B}$ 를 지정하려면, 이 두 가지 더 기본적인 것들이 각각 어디로 가지만 지정하면 됩니다.  $\alpha$ 에 대한 조건들은 이미  $(f, \text{id}_2)$ 가  $F(f)$  또는  $G(f)$ 로 대응되어야 함을(위 사상이  $\mathcal{A} \times \{0\}$ 에 있는지  $\mathcal{A} \times \{1\}$ 에 있는지에 따라) 알려주며, 사상  $(\text{id}_A, 0 \leq 1)$ 을 지정하는 것은  $A$ 번째 성분을 지정하는 것과 마찬가지로입니다. 그렇다면 자연성은 어디서 들어오는 것입니까?

위의 논의는 일반적으로 범주들의 곱으로 옮겨집니다: 일반적인 사상  $(f, g) = (f, \text{id}) \circ (\text{id}, g) = (\text{id}, g) \circ (f, \text{id})$ 를 얻기 위해서는 실제로  $(f, \text{id})$ 와  $(\text{id}, g)$  사상만 생각하면 됩니다.

**70A.**  $\gamma(c) = 0$ 인  $c \in C$ 가 있다고 합시다.  $c = 0$ 임을 보이겠습니다. 이는 다음과 같은 도식 추적으로 진행됩니다:

- $0 = r'(\gamma(c)) = \delta(r(c))$ 임에 유의하십시오.  $\delta$ 가 단사이므로,  $r(c) = 0$ 이 따라 나옵니다.
- 위쪽 행이 완전하므로, 어떤  $b \in B$ 에 대해  $c = q(b)$ 가 따라 나옵니다.
- 그러면  $q'(\beta(b)) = 0$ 이므로,  $b' = \beta(b)$ 라 하면  $b' \in \ker(q')$ 입니다. 아래쪽 행이 완전하므로,  $p'(a') = b'$ 인  $a'$ 가 존재합니다.
- $\alpha$ 가 전사이므로,  $\alpha(a) = a'$ 인  $a \in A$ 가 존재합니다.
- $\beta$ 가 단사이므로,  $p(a) = b$ 가 따라 나옵니다.
- 위쪽 행이 완전하고,  $b$ 가  $p$ 의 상에 속하므로, 필요한 대로  $0 = q(b) = c$ 가 따라 나옵니다.

**71A.** 함수  $H_{n-1}$ 을 적용하면 합성  $\mathbb{Z} \rightarrow 0 \rightarrow \mathbb{Z}$ 이 항등사상이 되는데, 이는 명백히 불가능합니다.

**72B.** 답은  $\tilde{H}_{n-1}(X) \cong \mathbb{Z}^{\oplus p}$ 이며, 다른 모든 군은 소멸합니다.  $p = 1$ 인 경우,  $\mathbb{R}^n - \{*\} \cong S^{n-1}$ 이므로 증명이 끝났습니다. 다른 모든  $p$ 에 대해서는,  $p$ 개의 점을 한쪽에  $a$ 개, 다른 쪽에  $b$ 개가 있도록 두 부분으로 나누는 초평면을 그립니다(따라서  $a + b = p$ ).  $U$ 와  $V$ 를 설정하고 귀납법을 사용합니다.

또는,  $U$ 를 원하는 공간으로 놓고,  $V$ 를 각 점 주위에 하나씩 있는  $p$ 개의 서로소인 공의 합집합으로 놓습니다. 그러면  $U \cup V = \mathbb{R}^n$ 은 모든 축소 호몰로지 군이 자명합니다. 마이어-비토리스 열로부터  $\tilde{H}_k(U \cap V) \cong \tilde{H}_k(U) \oplus \tilde{H}_k(V)$ 임을 읽어낼 수 있습니다. 그러면  $U \cap V$ 는  $p$ 개의 구멍 뚫린 공이며, 각각은  $S^{n-1}$ 과 같습니다. 여기서부터 결론을 읽어낼 수 있습니다.

**72C\*.**  $k = n$ 일 때는  $\mathbb{Z}$ 이고, 그렇지 않으면 0입니다.

**72F\*.** 다음 짧은 완전열을 사용하십시오

$$0 \rightarrow C_\bullet(B, A) \rightarrow C_\bullet(X, A) \rightarrow C_\bullet(X, B) \rightarrow 0$$

사슬 복합체의

**73B.** 다음과 같은 완전열이 있습니다

$$\underbrace{\tilde{H}_1(\mathbb{R})}_{=0} \rightarrow \tilde{H}_1(\mathbb{R}, \mathbb{Q}) \rightarrow \tilde{H}_0(\mathbb{Q}) \rightarrow \underbrace{\tilde{H}_0(\mathbb{R})}_{=0}.$$

이제,  $\mathbb{Q}$ 가 경로 비연결(즉, 그 어떤 두 점도 경로로 연결되어 있지 않음)이므로,  $\tilde{H}_0(\mathbb{Q})$ 는 가산 무한히 많은  $\mathbb{Z}$ 의 복사본으로 이루어짐이 따라 나옵니다.

**73E.** 이는 Hatcher의 2.B절에 자세히 설명되어 있습니다.

**74D.** 구체적으로,  $H_2(X^2, X^1)$ 에서의 호몰로지만 살펴보고 이것이  $H_2(X)$ 와 동형사상임을 보이겠습니다. 다음 도식에 따르면

$$\begin{aligned} H_2(X) &\cong H_2(X^3) \\ &\cong H_2(X^2) / \ker [H_2(X^2) \rightarrow H_2(X^3)] \\ &\cong H_2(X^2) / \operatorname{im} \partial_3 \\ &\cong \operatorname{im} [H_2(X^2) \hookrightarrow H_2(X^2, X^1)] / \operatorname{im} \partial_3 \\ &\cong \ker(\partial_2) / \operatorname{im} \partial_3 \\ &\cong \ker d_2 / \operatorname{im} d_3. \end{aligned}$$

**76D.** [Ma13a, 예제 3.3.14, 68–69쪽]를 참조하십시오.

**77B.**  $V = \mathcal{V}(I)$ 이고  $I = (f_1, \dots, f_m)$ 일 때(늘 그렇듯이  $\mathbb{R}[x_1, \dots, x_n]$ 이 뇌터 환이므로 유한 개의 다항식만 있습니다),  $f = f_1^2 + \dots + f_m^2$ 로 잡을 수 있습니다.

**77C.**  $I$ 를 아이디얼이라 하고,  $\mathfrak{m}$ 을 그 안에 포함된 극대 아이디얼이라 합시다. ( $\mathfrak{m}$ 의 존재가 걱정된다면, 이는 크룰의 정리(문제 5E\*)로부터 따라 나옵니다.) 그러면 약한 영점 정리에 의해  $\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$ 입니다. 따라서  $(a_1, \dots, a_n)$ 은  $\mathcal{V}(\mathfrak{m})$ 의 유일한 점이며, 그러므로 이 점은  $\mathcal{V}(I)$ 에도 속합니다.

**77D.** 핵심은 만약  $f$ 가  $\mathcal{V}(I)$  전체에서 소멸한다면,  $f \in \sqrt{I}$ 임을 확인하는 것입니다.

원래 환  $\mathbb{C}[x_1, \dots, x_n]$ 에서 생성원들의 집합  $f_1, \dots, f_m$ 을 취하십시오; 힐베르트 기저 정리에 의해 이것이 유한하다고 가정할 수 있습니다.

이제 트릭을 하나 사용해 보겠습니다: 대신  $S = \mathbb{C}[x_1, \dots, x_n, x_{n+1}]$ 을 생각하십시오. 더 큰 환에서  $\{f_1, \dots, f_m\}$ 과 다항식  $x_{n+1}f - 1$ 로 생성되는 아이디얼  $I' \subseteq S$ 를 생각하십시오. 마지막 녀석의 핵심은 그 영점 집합이  $\mathbb{A}^n$ 의 우리 사본인  $x_{n+1} = 0$ 에도,  $\mathbb{A}^{n+1}$ 을 통한  $f$ 의 “사영”에 속하는 어떤 점에도 닿지 않는다는 것입니다 (이는 더 작은 환에서의  $\mathcal{V}(I)$ 에  $\mathbb{C}$ 를 직접 곱한 것으로 생각할 수 있습니다). 따라서  $\mathcal{V}(I') = \emptyset$ 이고, 약한 영점정리에 의해 실제로  $I' = \mathbb{C}[x_1, \dots, x_{n+1}]$ 을 얻습니다. 그러므로

$$1 = g_1 f_1 + \dots + g_m f_m + g_{m+1} (x_{n+1} f - 1).$$

이제 트릭입니다:  $x_{n+1}$ 의 모든 자리를  $\frac{1}{f}$ 로 치환하고, 모든 분모를 제거하십시오. 따라서 충분히 큰 어떤 정수  $N$ 에 대해 다음을 얻을 수 있습니다

$$f^N = f^N (g_1 f_1 + \dots + g_m f_m)$$

이는 우변에서  $f$ 의 분수 거듭제곱을 모두 제거합니다. 따라서  $f^N \in I$ 가 성립합니다.

**80A.** 완전성으로부터,  $h_I(d) = h_I(d-k) + h_{I+(f)}(d)$ 이며, 다음이 성립함을 알 수 있습니다

$$\chi_{I+(f)}(d) = \chi_I(d) - \chi_I(d-k).$$

$m = \dim \mathcal{V}_{\text{pr}}(I) \geq 1$ 이라 합시다. 이제  $\dim \mathcal{V}_{\text{pr}}(I + (f)) = m - 1$ 이므로, 다음이 성립합니다

$$\frac{\deg(I + (f))d^{m-1} + \dots}{(m-1)!} = \frac{1}{m!} (\deg I(d^m - (d-k)^m) + \text{저차항})$$

여기서 다음을 읽어낼 수 있습니다

$$\deg(I + (f)) = \frac{(m-1)!}{m!} \cdot k \binom{m}{1} \deg I = k \deg I$$

필요에 따라.

**80B.**  $ABC$ 를 단위원으로 하는 복소수를 사용하면, 이는 두 개의 삼차 방정식을 푸는 것과 동치입니다

$$\begin{aligned} (p-a)(p-b)(p-c) &= (abc)^2 (q-1/a)(q-1/b)(q-1/c) \\ 0 &= \prod_{\text{순환}} (p+c-b-bcq) + \prod_{\text{순환}} (p+b-c-bcq) \end{aligned}$$

$p$ 와  $q = \bar{p}$ 에 대한 것입니다. 이를  $(p, q) \in \mathbb{C}^2$ 에서의 두 삼차 곡선으로 보면, 베주 정리에 의해 해는 최대 아홉 개임을 알 수 있습니다(두 곡선이 모두 기약이 아닌 경우는 제외해야 하지만, 첫 번째 곡선은 인수분해될 수 없음을 확인할 수 있습니다). 게다가 아홉 개의 해를 나열하는 것은 쉽습니다( $ABC$ 가 부등변삼각형인 경우): 세 꼭짓점, 세 방심, 그리고  $I$ ,  $O$ ,  $H$ 입니다. 따라서 답은 바로 이 세 삼각형 중심  $I$ ,  $O$ ,  $H$ 입니다.

**81C.** 만약 이들이 동형이라면,  $\mathcal{O}_V(V) \cong \mathcal{O}_W(W)$ 가 성립할 것입니다. 기약 사영 다양체에 대해서는  $\mathcal{O}_W(W) \cong \mathbb{C}$ 이고, 아핀 다양체에 대해서는  $\mathcal{O}_V(V) \cong \mathbb{C}[V]$ 입니다. 따라서  $V$ 는 반드시 단일 점이어야 함을 결론지을 수 있습니다.

**81D.** 모순을 위해 아핀 다양체  $V$ 와 동형사상이 존재한다고 가정하십시오

$$f: X \rightarrow V.$$

그러면 당겨오기를 취하면 환 동형사상을 얻습니다

$$f^\sharp: \mathcal{O}_V(V) \rightarrow \mathcal{O}_X(X) = \mathbb{C}[x, y].$$

이제  $\mathcal{O}_V(V) = \mathbb{C}[a, b]$ 라 하겠습니다. 여기서  $f^\sharp(a) = x$ ,  $f^\sharp(b) = y$ 입니다. 특히, 실제로  $V \cong \mathbb{A}^2$ 이어야 합니다.

이제 아핀 다양체  $V$ 에서  $\mathcal{V}(a)$ 와  $\mathcal{V}(b)$ 를 취할 수 있습니다. 이들은 공집합이 아닌 교집합을 가지는데,  $(a, b)$ 가  $\mathcal{O}_V(V)$ 에서 극대 아이디얼이기 때문입니다. 이 점을  $q$ 라 부르고,  $f(p) = q$ 인 점  $p$ 를 취하십시오.

그러면

$$0 = a(q) = (f^\sharp a)(p) = x(p)$$

따라서  $p \in \mathcal{V}(x) \subseteq X$ 입니다. 마찬가지로  $p \in \mathcal{V}(y) \subseteq X$ 이지만,  $\mathcal{V}(x, y) = \emptyset$ 이므로 이는 모순입니다.

- 82A.** 줄기가 층화에 의해 보존되므로, 증명할 것이 사실상 없습니다: 양변 모두  $U$  위의 호환되는  $\mathcal{F}$ -빚들의 수열에 대응합니다.
- 83A.**  $A[1/60] = \mathbb{Z}/7\mathbb{Z}$ 를 얻어야 합니다.
- 83B.**  $S$ 가 영인자를 가지지 않을 때, 그리고 그때에만 성립합니다.
- 83D.**  $A = \mathbb{C} \times \mathbb{C}$ 로 놓거나, 더 일반적으로 두 개 이상의 정역의 곱으로 놓으십시오.
- 85B.**  $V = D(x) \cup D(y) \subset U$ 를 뚫린 평면이라 합시다. 그러면 그 여집합  $D(z)$ 는 뚫린 직선처럼 보입니다. 이때  $V \cap D(z) = \emptyset$ 이며, 다음 제한 사상들의 도식이 가환합니다

$$\begin{array}{ccccc}
 & & \mathcal{O}_X(X) = A & & \\
 & \swarrow & \downarrow & \searrow & \\
 & & \mathcal{O}_X(U) & & \\
 \swarrow & & & & \searrow \\
 \mathcal{O}_X(D(z)) & & & & \mathcal{O}_X(V) \\
 & \searrow & & \swarrow & \\
 & & \mathcal{O}_X(\emptyset) = 0 & & 
 \end{array}$$

층 공리에 의해 실제로는 다음이 성립해야 합니다

$$\mathcal{O}_X(U) = \mathcal{O}_X(D(z)) \times \mathcal{O}_X(V).$$

$\mathcal{O}_X(D(z)) = A_z = k[x, y, z, z^{-1}]/(xz, yz) \cong k[z, z^{-1}]$ 입니다. 한편 Vakil의 §4.4.1에 나타난 바와 같이  $\mathcal{O}_X(V) = k[x, y]$ 입니다. 따라서

$$\mathcal{O}_X(U) = k[x, y] \times k[z, z^{-1}].$$

- 87A.**  $\mathbb{Z}$ 가 CRing의 시작 대상이므로,  $\text{Spec } \mathbb{Z}$ 는  $\text{AffSch}$ 의 끝 대상이 됩니다.  $\mathfrak{p}$ 는 체  $\mathcal{O}_{X, \mathfrak{p}}/\mathfrak{m}_{X, \mathfrak{p}}$ 의 표수로 보내집니다.
- 88A.**  $\varepsilon = \pi - 3.141592653 < 10^{-9}$ 라 하십시오. 그러면

$$\frac{22}{7} = f(\pi) = f(3.141592653) + f(\varepsilon) = 3.141592653 + f(\varepsilon).$$

따라서,

$$f(\varepsilon) = \frac{22}{7} - 3.141592653 = \frac{22 - 21.991148571}{7} > \frac{0.008}{7} > 10^{-3}.$$

그러므로

$$f(10^8 \varepsilon) = 10^8 f(\varepsilon) > 10^5 > 9000$$

그리고 필요한 대로  $10^8 \varepsilon < 1$ 입니다.

**88B.** 모든 명제는 참입니다.

첫 번째 명제는 다음을 통해  $f$ 를 단순히 확장함으로써 따라옵니다

$$x \mapsto \begin{cases} f(x) & x > 0 \\ 0 & x = 0 \\ -f(-x) & x < 0. \end{cases}$$

두 번째 명제는 임의의 가법 함수  $\mathbb{R} \rightarrow \mathbb{R}$ 에 대해 참입니다. 실제로  $f(0) = f(0) + f(0) \implies f(0) = 0$ 이며, 기함수성은 이로부터 따라옵니다.

세 번째와 네 번째 명제는 [https://en.wikipedia.org/wiki/Cauchy%27s\\_functional\\_equation#Properties\\_of\\_nonlinear\\_solutions\\_over\\_the\\_real\\_numbers](https://en.wikipedia.org/wiki/Cauchy%27s_functional_equation#Properties_of_nonlinear_solutions_over_the_real_numbers)로부터 따라옵니다.

다섯 번째 명제는 다소 단순합니다. 만약  $f$ 가 전사였다면,  $f(a) = 0$ 인  $a > 0$ 이 존재해야 합니다. 하지만 그렇다면  $f(2a) = f(a) + f(a) = 0$ 이므로,  $f$ 는 단사가 아닙니다.

나머지를 위해, 하멜 기저를 고정합니다

$$E = \{e_\alpha \mid \alpha \in S := \{0, 1, 2, \dots\} \dots\}.$$

여기서  $S$ 는 순서수들로 이루어진 비가산 집합입니다. 일반성을 잃지 않고,  $e_0 = 1$ 이고 모든  $\alpha \in S$ 에 대해  $e_\alpha > 0$ 이라 합시다. 그러면  $f$ 는 각  $\alpha \in S$ 에 대한  $f(e_\alpha)$ 의 값에 의해 유일하게 결정됩니다.

- 여섯 번째 명제를 위해,  $f(e_0) = e_1$ ,  $f(e_1) = e_0$ , 그리고 그 외의 모든  $\alpha \geq 2$ 에 대해  $f(e_\alpha) = e_\alpha$ 라고 합시다.
- 일곱 번째 명제가 가장 복잡합니다.  $S$ 가 무한하므로, 2-대-1 사상  $\psi: S \rightarrow S$ 를 구성하는 것이 가능한데, 이는 공역의 모든 원소가 정의역의 정확히 두 원소의 상이 됨을 의미합니다. 그러면  $\alpha \neq \beta$ 에 대해  $\psi(\alpha) = \psi(\beta) = \gamma$ 이면,  $f(e_\alpha) = e_\gamma$ ,  $f(e_\beta) = -e_\gamma$ 로 설정합니다.
- 여덟 번째 명제를 위해, 모든  $\alpha \in S$ 에 대해  $f(e_\alpha) = 1$ 이라 합시다.
- 아홉 번째 명제를 위해, 모든  $\alpha \in S$ 에 대해  $f(e_\alpha)$ 가 선형독립인 무리수라고 합시다.

**89E.** 두 모자 배치가 유한하게 많은 곳에서만 다를 경우 이를 동치로 간주하는 동치 관계를 정의합니다. 이제 각 동치류에 대해, 모두가 특정한 대표원에 미리 합의합니다. 마지막으로, 한 사람이 자신의 모자 색깔을 모르더라도 그룹이 어떤 동치류에 속하는지 판단할 수 있다는 점에 주목하십시오. 따라서 모두가 만장일치로 같은 대표원을 선택하게 되며, 증명 완료입니다.

**92C<sup>†</sup>.** 문장  $\phi$ 에 대해

$$f_\phi: \kappa \rightarrow \kappa$$

가  $\alpha$ 를 다음과 같은 최소의  $\beta < \kappa$ 로 보낸다고 합시다: 모든  $\vec{b} \in V_\alpha$ 에 대해,  $V_\kappa \models \phi[a, \vec{b}]$ 인  $a \in V_\beta$ 가 존재하면,  $V_\kappa \models \phi[a, \vec{b}]$ 인  $\exists a \in V_\beta$ 입니다.

이것이 잘 정의됨을 주장합니다.  $\vec{b}$ 의 가능한 선택지는 오직  $|V_\alpha|^n$ 개뿐이며, 특히 이는  $\kappa$ 보다 적습니다(우리는  $|V_\alpha| < \kappa$ 임을 알고 있기 때문입니다; **문제 91C\***과 비교해 보십시오). 그렇지 않다면, 명제가 성립하지 않는  $\beta$ 로 각 벡터  $\vec{b}$ 를 대응시킴으로써  $|V_\alpha^n|$ 에서  $\kappa$ 로의 공종 사상을 구성할 수 있습니다. 그리고 그것은  $\kappa$ 가 정칙이므로 불가능합니다!

다시 말해, 우리가 한 일은  $\phi$ 를 고정한 다음 모든  $\vec{b} \in V_\alpha^n$ 에 대해 타르스키-보트 정리를 사용한 것입니다. 이제  $g: \kappa \rightarrow \kappa$ 를 다음과 같이 정의합시다.

$$\alpha \mapsto \sup f_\phi(\alpha).$$

$\kappa$ 가 정칙이고 논리식이 가산 개뿐이므로,  $g(\alpha)$ 는 잘 정의됩니다.

$\alpha$ 가  $g$ 에 의해  $\alpha$  자신으로 사상되는 성질을 가진다면(다시 말해,  $\alpha$ 가  $g$  아래에서 닫혀 있다면), 타르스키-보트 검사법에 의해  $V_\alpha < V_\kappa$ 임을 확인하십시오.

따라서  $g$  아래에서 닫혀 있는 임의로 큰  $\alpha < \kappa$ 가 존재함을 보이면 충분합니다.  $\alpha_0$ 을 고정합시다.  $\alpha_1 = g(\alpha_0)$ 라 하고, 이런 식으로 계속하여 다음과 같이 정의합시다:

$$\alpha = \sup_{n < \omega} \alpha_n.$$

이  $\alpha$ 는  $g$ 에 대해 닫혀 있으며,  $\alpha_0$ 을 임의로 크게 함으로써  $\alpha$ 도 원하는 만큼 크게 만들 수 있습니다.

**93B.**  $M$ 은 가산이므로, 조밀 집합은 가산 개만 존재합니다(이들은  $M$  안에 있습니다!) —

$$D_1, D_2, \dots, D_n, \dots \in M.$$

이라 합시다. 선택공리를 사용하여  $p_1 \in D_1$ 을 취하고, 그다음  $p_2 \leq p_1$ 이면서  $p_2 \in D_2$ 인  $p_2$ 를 취하고( $D_2$ 가 조밀하므로 이것이 가능합니다), 이런 식으로 계속합니다. 이러한 방식으로 다음 사슬을 귀납적으로 제시할 수 있습니다

$$p_1 \geq p_2 \geq p_3 \geq \dots$$

여기서 모든  $i$ 에 대해  $p_i \in D_i$ 입니다.

따라서 우리는  $\{p_i\}$ 로부터 필터를 생성하고자 합니다. 위쪽 폐포를 취하기만 하면 됩니다 — 어떤  $n$ 에 대해  $q \geq p_n$ 을 만족하는  $q \in \mathbb{P}$ 의 집합을  $G$ 라 합시다. 구성에 의해  $G$ 는 필터입니다(이는 사실 자명합니다). 게다가 구성에 의해  $G$ 는 모든 조밀 집합과 교차합니다.

**94A.**  $\mathbb{P}$ 가  $\kappa$  이상의 정칙성을 보존함을 보이는 것으로 충분합니다.  $M$ 에서 정칙인  $\lambda > \kappa$ 를 생각하고, 귀류법으로  $\lambda$ 가  $M[G]$ 에서 정칙이 아니라고 가정합니다. 이는 공종인 함수  $f \in M[G]$ ,  $f: \bar{\lambda} \rightarrow \lambda$ 가 존재하여  $\bar{\lambda} < \lambda$ 인 것과 같습니다. 그러면 가능값 논법에 의해,  $F \in M$ 인 함수가 존재하여  $\bar{\lambda} \rightarrow \mathcal{P}(\lambda)$ 이고, 모든  $\alpha$ 에 대해  $f(\alpha) \in F(\alpha)$ 이며  $|F(\alpha)|^M < \kappa$ 입니다.

이제 다시  $M$  안에서 작업하겠습니다. 각  $\alpha \in \bar{\lambda}$ 에 대해,  $\lambda$ 가  $M$ 에서 정칙이고  $|F(\alpha)|$ 보다 크므로  $F(\alpha)$ 는  $\lambda$ 에서 유계임에 주목하십시오. 이제  $M$  안에서 다음과 같이 정의되는 함수  $\bar{\lambda} \rightarrow \lambda$ 를 살펴보십시오

$$\alpha \mapsto \cup F(\alpha) < \lambda.$$

이는  $M$ 에서 공종이며, 모순입니다.

# D 표기법 용어집

## §D.1 일반

- $\forall$ : 모든
- $\exists$ : 존재한다
- $\text{sign}(\sigma)$ : 순열  $\sigma$ 의 부호
- $X \implies Y$ :  $X$ 는  $Y$ 를 함의합니다

## §D.2 함수와 집합

- $f^{\text{img}}(S)$ 는  $S \subseteq X$ 일 때  $f: X \rightarrow Y$ 에 의한 상입니다.
- $f^{-1}(y)$ 는  $y \in Y$ 일 때  $f: X \rightarrow Y$ 의 역입니다.
- $f^{\text{pre}}(T)$ 는  $T \subseteq Y$ 일 때  $f: X \rightarrow Y$ 의 원상입니다.
- $f|_S$ 는  $f: X \rightarrow Y$ 를  $S \subseteq X$ 로 제한한 것입니다.
- $f^n$ 은 함수  $f$ 를  $n$ 번 적용한 함수입니다

아래는 몇 가지 흔한 집합입니다. 이들은 자명한 방식으로 군, 환, 체 등으로도 생각할 수 있습니다.

- $\mathbb{C}$ : 복소수의 집합
- $\mathbb{R}$ : 실수의 집합
- $\mathbb{N}$ : 양의 정수의 집합
- $\mathbb{Q}$ : 유리수의 집합
- $\mathbb{Z}$ : 정수의 집합
- $\emptyset$ : 공집합

집합에 관한 몇 가지 흔한 표기법:

- $A \subset B$ :  $A$ 는  $B$ 의 임의의 부분집합입니다
- $A \subseteq B$ :  $A$ 는  $B$ 의 임의의 부분집합입니다
- $A \subsetneq B$ :  $A$ 는  $B$ 의 진부분집합입니다
- $S \times T$ : 집합  $S$ 와  $T$ 의 데카르트 곱
- $S \setminus T$ : 집합  $S$ 와  $T$ 의 차집합
- $S \cup T$ :  $S$ 와  $T$ 의 합집합
- $S \cap T$ :  $S$ 와  $T$ 의 교집합

- $S \sqcup T$ :  $S$ 와  $T$ 의 분리 합집합
- $|S|$ :  $S$ 의 농도
- $S/\sim$ :  $\sim$ 가  $S$  위의 동치 관계라면, 이는 동치류들의 집합입니다.
- $x + S$ : 집합  $\{x + s \mid s \in S\}$ 를 나타냅니다.
- $xS$ : 집합  $\{xs \mid s \in S\}$ 를 나타냅니다.

### §D.3 추상대수학과 선형대수학

몇 가지 흔한 군/환/체:

- $\mathbb{Z}/n\mathbb{Z}$ : 위수  $n$ 인 순환군
- $(\mathbb{Z}/n\mathbb{Z})^\times$ :  $\mathbb{Z}/n\mathbb{Z}$ 의 단원들의 집합입니다.
- $S_n$ :  $\{1, \dots, n\}$  위의 대칭군
- $D_{2n}$ : 위수  $2n$ 인 이면체군입니다.
- $0, 1$ : 자명군 (문맥에 따라 다름)
- $\mathbb{F}_p$ :  $p$ 를 법으로 하는 정수

군에 관한 표기법:

- $1_G$ : 군  $G$ 의 항등원
- $N \leq G$ : 부분군  $N$ 이  $G$ 의 정규 부분군임을 나타냅니다.
- $G/N$ : 정규 부분군  $N$ 에 의한  $G$ 의 몫군
- $Z(G)$ : 군  $G$ 의 중심
- $N_G(H)$ :  $G$ 의 부분군  $H$ 의 정규화군
- $G \times H$ :  $G$ 와  $H$ 의 곱군
- $G \oplus H$ : 이 또한 곱군이지만,  $G$ 와  $H$ 가 아벨 군일 때(따라서 이들을  $\mathbb{Z}$ -가군으로 생각할 수 있을 때) 자주 사용됩니다.
- $\text{Stab}_G(x)$ :  $X$ 가  $G$ 의 작용을 받는 경우,  $x \in X$ 의 안정화 부분군
- $\text{FixPt } g$ , (군의 작용 아래)  $g \in G$ 에 의한 고정점들의 집합

환에 관한 표기법:

- $R/I$ : 환  $R$ 을 아이디얼  $I$ 로 나눈 몫
- $(a_1, \dots, a_n)$ :  $a_i$ 들로 생성된 아이디얼
- $R^\times$ :  $R$ 의 단원군
- $R[x_1, \dots, x_n]$ :  $x_i$ 들에 대한 다항식환, 즉  $R$ 에  $x_i$ 들을 첨가하여 얻은 환
- $F(x_1, \dots, x_n)$ :  $F$ 에  $x_i$ 들을 첨가하여 얻은 체
- $R^d$ : 등급 (유사)환  $R$ 의  $d$ 번째 등급 부분

선형대수학:

- $\text{id}$ : 항등행렬
- $V \oplus W$ : 직합
- $V^{\oplus n}$ :  $V$ 의  $n$ 개 직합
- $V \otimes W$ : 텐서곱
- $V^{\otimes n}$ :  $V$ 의  $n$ 개 텐서곱
- $V^\vee$ : 쌍대 공간
- $T^\vee$ : ( $T$ 가 선형 사상일 때) 쌍대 사상
- $T^\dagger$ : ( $T$ 가 선형 사상일 때) 켈레 전치
- $\langle -, - \rangle$ : 쌍선형 형식
- $\text{Mat}(V)$ :  $V$ 의 자기준동형사상, 즉  $\text{Hom}_k(V, V)$
- $\mathbf{e}_1, \dots, \mathbf{e}_n$ :  $k^{\oplus n}$ 의 “표준 기저”

## §D.4 양자 계산

- $|\psi\rangle$ : 어떤 벡터 공간  $H$ 의 벡터
- $\langle\psi|$ :  $|\psi\rangle$ 에 쌍대인, 어떤 벡터 공간  $H^\vee$ 의 벡터.
- $\langle\phi|\psi\rangle$ :  $\langle\phi| \in H^\vee$ 의 원소를  $|\psi\rangle \in H$ 에서 평가한 값입니다.
- $|\uparrow\rangle, |\downarrow\rangle$ : 스핀  $z$ -업, 스핀  $z$ -다운
- $|\rightarrow\rangle, |\leftarrow\rangle$ : 스핀  $x$ -업, 스핀  $x$ -다운
- $|\otimes\rangle, |\odot\rangle$ : 스핀  $y$ -업, 스핀  $y$ -다운

## §D.5 위상수학과 실/복소 해석학

흔히 쓰이는 위상 공간들:

- $S^1$ : 단위원
- $S^n$ :  $n$ -구의 표면( $\mathbb{R}^{n+1}$  안에서)
- $D^{n+1}$ : 닫힌  $n+1$ 차원 공( $\mathbb{R}^{n+1}$  안에서)
- $\mathbb{RP}^n$ : 실 사영  $n$ -공간
- $\mathbb{CP}^n$ : 복소 사영  $n$ -공간

몇 가지 위상수학적 표기법:

- $\partial Y$ : (어떤 위상 공간 안에서) 집합  $Y$ 의 경계
- $X/S$ :  $S \subseteq X$ 에 의한  $X$ 의 몫위상
- $X \times Y$ : 공간  $X$ 와  $Y$ 의 곱위상

- $X \amalg Y$ : 공간  $X$ 와  $Y$ 의 분리합집합
- $X \vee Y$ : (점을 가진) 공간  $X$ 와  $Y$ 의 켜기곱

실해석학(미적분학 개론):

- $\liminf$ : 하극한
- $\limsup$ : 상극한
- $\inf$ : 하한
- $\sup$ : 상한
- $\mathbb{Z}_p$ :  $p$ 진 정수
- $\mathbb{Q}_p$ :  $p$ 진 수
- $f'$ :  $f$ 의 도함수
- $\int_a^b f(x) dx$ :  $[a, b]$ 에서  $f$ 의 리만 적분

복소해석학:

- $\int_\alpha f dz$ : 경로  $\alpha$ 를 따른  $f$ 의 경로 적분
- $\text{Res}(f; p)$ : 유리형 함수  $f$ 의 점  $p$ 에서의 유수
- $\mathbf{I}(\gamma, p)$ :  $p$ 를 중심으로 한  $\gamma$ 의 감김수

## §D.6 측도론과 확률론

- $\mathcal{A}^{\text{cm}}$ : Carathéodory-측정 가능 집합들의  $\sigma$ -대수
- $\mathcal{B}(X)$ :  $X$ 에 대한 보렐 공간
- $\mu^{\text{cm}}$ :  $\mathcal{A}^{\text{cm}}$  위에서 유도된 측도
- $\lambda$ : 르베그 측도
- $\mathbf{1}_A$ :  $A$ 의 지시함수
- $\int_\Omega f d\mu$ :  $f$ 의 르베그 적분
- $\lim_{n \rightarrow \infty} f_n$ :  $f_n$ 의 점별 극한
- $\hat{G}$ :  $G$ 의 폰트랴긴 쌍대

## §D.7 대수적 위상수학

- $\alpha \simeq \beta$ : 경로에 대해, 이는 경로 호모토피를 나타냄
- $*$ : 경로 이음
- $\pi_1(X) = \pi_1(X, x_0)$ : (점을 가진) 공간  $X$ 의 기본군
- $\pi_n(X) = \pi_n(X, x_0)$ : (점을 가진) 공간  $X$ 의  $n$ 번째 호모토피 군
- $f_\#$ :  $f: X \rightarrow Y$ 에 의해 유도된 사상  $\pi_1(X) \rightarrow \pi_1(Y)$

- $\Delta^n$ : 표준  $n$ -단체
- $\partial\sigma$ : 특이  $n$ -단체  $\sigma$ 의 경계
- $H_n(A_\bullet)$ : 사슬 복합체  $A_\bullet$ 의  $n$ 번째 호몰로지 군
- $H_n(X)$ : 공간  $X$ 의  $n$ 번째 호몰로지 군
- $\tilde{H}_n(X)$ :  $X$ 의  $n$ 번째 축소 호몰로지 군
- $H_n(X, A)$ :  $X$ 와  $A \subseteq X$ 의  $n$ 번째 상대 호몰로지 군
- $f_*: f: A_\bullet \rightarrow B_\bullet$ 에 의한  $H_n(A_\bullet) \rightarrow H_n(B_\bullet)$  위의 유도 사상, 또는  $f: X \rightarrow Y$ 에 대한  $H_n(X) \rightarrow H_n(Y)$
- $\chi(X)$ : 공간  $X$ 의 오일러 지표
- $H^n(A^\bullet)$ : 코사슬 복합체  $A^\bullet$ 의  $n$ 번째 코호몰로지 군
- $H^n(A_\bullet; G)$ :  $A_\bullet$ 에  $\text{Hom}(-, G)$ 를 적용하여 얻은 코사슬 복합체의  $n$ 번째 코호몰로지 군
- $H^n(X; G)$ :  $G$ -계수를 갖는  $X$ 의  $n$ 번째 코호몰로지 군/환
- $\tilde{H}^n(X; G)$ :  $G$ -계수를 갖는  $X$ 의  $n$ 번째 축소 코호몰로지 군/환
- $H^n(X, A; G)$ :  $G$ -계수를 갖는  $X$ 와  $A \subset X$ 의  $n$ 번째 상대 코호몰로지 군/환
- $f^\sharp: f: A^\bullet \rightarrow B^\bullet$ 에 의한  $H^n(A^\bullet) \rightarrow H^n(B^\bullet)$  위의 유도 사상, 또는  $f: X \rightarrow Y$ 에 대한  $H^n(X) \rightarrow H^n(Y)$
- $\text{Ext}(-, -)$ : Ext 함자
- $\phi \smile \psi$ : 코사슬  $\phi$ 와  $\psi$ 의 컵 곱

## §D.8 범주론

몇 가지 흔한 범주들(알파벳순):

- Grp: 군의 범주
- CRing: 가환환의 범주
- Top: 위상 공간의 범주
- $\text{Top}_*$ : 점을 갖는 위상 공간의 범주
- $\text{Vect}_k$ :  $k$ -벡터 공간의 범주
- $\text{FDVect}_k$ : 유한 차원 벡터 공간의 범주
- Set: 집합의 범주
- hTop: 위상 공간의 범주로, 그 사상은 사상들의 호모토피 류입니다
- $\text{hTop}_*$ : hTop의 점을 갖는 버전
- hPairTop: 사상이 쌍-호모토피 동치류인 쌍  $(X, A)$ 의 범주

- $\text{OpenSets}(X)$ : 반순서 집합으로서의  $X$ 의 열린집합의 범주

범주에 대한 연산:

- $\text{obj } \mathcal{A}$ : 범주  $\mathcal{A}$ 의 대상들
- $\mathcal{A}^{\text{op}}$ : 반대 범주
- $\mathcal{A} \times \mathcal{B}$ : 곱 범주
- $[\mathcal{A}, \mathcal{B}]$ :  $\mathcal{A}$ 에서  $\mathcal{B}$ 로 가는 함수들의 범주
- $\ker f: \text{Ker } f \rightarrow B: f: A \rightarrow B$ 에 대해, 범주론적 핵
- $\text{coker } f: A \rightarrow \text{Coker } f: f: A \rightarrow B$ 에 대한 범주론적 여핵
- $\text{im } f: A \rightarrow \text{Im } f: f: A \rightarrow B$ 에 대한 범주론적 상

## §D.9 미분기하학

- $Df$ :  $f$ 의 전미분
- $(Df)_p$ : 점  $p$ 에서의  $f$ 의 전미분
- $\frac{\partial f}{\partial e_i}$ :  $i$ 번째 편도함수
- $\alpha_p$ :  $k$ -형식  $\alpha$ 를  $p$ 에서 계산한 값
- $\int_c \alpha$ : 미분 형식  $\alpha$ 의 셀  $c$  위에서의 적분
- $d\alpha$ :  $k$ -형식  $\alpha$ 의 외미분
- $\phi^*\alpha$ :  $\phi$ 에 의한  $k$ -형식  $\alpha$ 의 당겨오기

## §D.10 대수적 수론

- $\overline{\mathbb{Q}}$ : 대수적 수들의 환
- $\overline{\mathbb{Z}}$ : 대수적 정수들의 환
- $\overline{F}$ : 체  $F$ 의 대수적 폐포
- $N_{K/\mathbb{Q}}(\alpha)$ : 확장  $K/\mathbb{Q}$ 에서  $\alpha$ 의 노름
- $\text{Tr}_{K/\mathbb{Q}}(\alpha)$ : 확장  $K/\mathbb{Q}$ 에서  $\alpha$ 의 트레이스
- $\mathcal{O}_K$ :  $K$ 의 정수환
- $\mathfrak{a} + \mathfrak{b}$ : 두 아이디얼  $\mathfrak{a}$ 와  $\mathfrak{b}$ 의 합
- $\mathfrak{a}\mathfrak{b}$ : 아이디얼  $\mathfrak{a}$ 와  $\mathfrak{b}$ 의 원소들의 곱으로 생성된 아이디얼
- $\mathfrak{a} \mid \mathfrak{b}$ : 아이디얼  $\mathfrak{a}$ 가 아이디얼  $\mathfrak{b}$ 를 나눔
- $\mathfrak{a}^{-1}$ : 아이디얼 군에서  $\mathfrak{a}$ 의 역원
- $N(I)$ : 아이디얼 노름

- $\text{Cl}_K$ :  $K$ 의 유수군
- $\Delta_K$ : 수체  $K$ 의 판별식
- $\mu(\mathcal{O}_K)$ :  $\mathcal{O}_K$ 에 포함된 단위근들의 집합
- $[K : F]$ : 체 확장의 차수
- $\text{Aut}(K/F)$ :  $F$ 를 고정하는  $K$ 의 체 자기동형사상들의 집합
- $\text{Gal}(K/F)$ :  $K/F$ 의 갈루아 군
- $D_{\mathfrak{p}}$ : 소 아이디얼  $\mathfrak{p}$ 의 분해군
- $I_{\mathfrak{p}}$ : 소 아이디얼  $\mathfrak{p}$ 의 관성군
- $\text{Frob}_{\mathfrak{p}}$ :  $\mathfrak{p}$ 의 프로베니우스 원소 ( $\text{Gal}(K/\mathbb{Q})$ 의 원소)
- $P_K(\mathfrak{m})$ : 모듈러스  $\mathfrak{m}$ 의 주 아이디얼들의 광선
- $I_K(\mathfrak{m})$ : 모듈러스  $\mathfrak{m}$ 의 분수 아이디얼들
- $C_K(\mathfrak{m})$ : 모듈러스  $\mathfrak{m}$ 의 광선 유수군
- $\left(\frac{L/K}{\bullet}\right)$ : 아르틴 기호
- $\text{Ram}(L/K)$ :  $L$ 에서 분지하는  $K$ 의 소수들
- $f(L/K)$ :  $L/K$ 의 도체

## §D.11 표현론

- $k[G]$ : 군 대수
- $V \oplus W$ : 대수  $A$ 의 표현  $V = (V, \rho_V)$ 와  $W = (W, \rho_W)$ 의 직합
- $V^\vee$ : 표현  $V = (V, \rho_V)$ 의 쌍대 표현
- $\text{Reg}(A)$ : 대수  $A$ 의 정규 표현
- $\text{Hom}_{\text{rep}}(V, W)$ : 표현의 사상  $V \rightarrow W$ 의 대수
- $\chi_V$ :  $A$ -표현  $V$ 에 부착된 지표  $A \rightarrow k$
- $\text{Classes}(G)$ :  $G$ 의 켈레류의 집합
- $\text{Fun}_{\text{class}}(G)$ : 함수  $\text{Classes}(G) \rightarrow \mathbb{C}$ 의 복소 벡터 공간
- $V \otimes W$ : 군  $G$ (대수가 아니라)의 표현  $V = (V, \rho_V)$ 와  $W = (W, \rho_W)$ 의 텐서곱
- $\mathbb{C}_{\text{triv}}$ : 자명 표현
- $\mathbb{C}_{\text{sign}}$ : 부호 표현

## §D.12 대수기하학

- $\mathcal{V}(-)$ : 집합 또는 아이디얼의 소멸 궤적
- $\mathbb{A}^n$ :  $n$ 차원 (복소) 아핀 공간
- $\sqrt{I}$ : 아이디얼  $I$ 의 근기
- $\mathbb{C}[V]$ : 아핀 다양체  $V$ 의 좌표환
- $\mathcal{O}_V(U)$ :  $U$  위의 유리 함수의 환
- $D(f)$ : 판별 열린집합
- $\mathbb{CP}^n$ : 복소 사영  $n$ -공간 (사영 다양체의 주변 공간)
- $(x_0 : \cdots : x_n)$ : 사영 공간의 좌표
- $U_i$ : 표준 아핀 차트
- $\mathcal{V}_{\text{pr}}(-)$ : 사영 소멸 궤적.
- $h_I, h_V$ : 아이디얼  $I$  또는 사영 다양체  $V$ 의 힐베르트 함수
- $\pi^\sharp$  또는  $\pi_U^\sharp$ :  $\pi: X \rightarrow Y$ 로부터 얻어지는 당겨오기  $\mathcal{O}_Y \rightarrow \mathcal{O}_X(\pi^{\text{pre}}(U))$
- $\mathcal{F}_p$ : 점  $p$ 에서의 (준)층  $\mathcal{F}$ 의 줄기
- $[s]_p$ : 점  $p$ 에서의  $s \in \mathcal{F}(U)$ 의 배아
- $\mathcal{O}_{X,p}$ :  $(\mathcal{O}_X)_p$ 의 축약형입니다.
- $\mathcal{F}^{\text{sh}}$ : 전층  $\mathcal{F}$ 의 층화입니다.
- $\alpha_p: \mathcal{F}_p \rightarrow \mathcal{G}_p$ :  $\alpha: \mathcal{F} \rightarrow \mathcal{G}$ 로부터 얻어지는 줄기 사이의 사상입니다.
- $\mathfrak{m}_{X,p}$ :  $\mathcal{O}_{X,p}$ 의 극대 아이디얼입니다.
- $\text{Spec } A$ : 환  $A$ 의 스펙트럼입니다.
- $S^{-1}A$ : 환  $A$ 를 집합  $S$ 에서 국소화한 것입니다.
- $A[1/f]$ : 환  $A$ 를 원소  $f$  바깥에서 국소화한 것입니다.
- $A_{\mathfrak{p}}$ : 환  $A$ 를 소 아이디얼  $\mathfrak{p}$ 에서 국소화한 것입니다.
- $f(\mathfrak{p})$ :  $\mathfrak{p}$ 에서의  $f$ 의 값, 즉  $f \pmod{\mathfrak{p}}$ 입니다.
- $\kappa(\mathfrak{p})$ :  $\text{Spec } A$ 의 원소  $\mathfrak{p}$ 에서의 잉여체입니다.
- $\pi_{\mathfrak{p}}^\sharp$ :  $\pi^\sharp$ 에서 유도되는 줄기 사이의 사상입니다.

## §D.13 집합론

- ZFC: 표준적인 ZFC 이론입니다.
- $ZFC^+$ : 표준적인 ZFC 이론에 “강한 비가측 기수가 존재한다”라는 문장을 추가한 것입니다.
- $2^S$  또는  $\mathcal{P}(S)$ :  $S$ 의 멱집합입니다.
- $A \wedge B$ :  $A$ 이고  $B$ 입니다.
- $A \vee B$ :  $A$ 이거나  $B$ 입니다.
- $\neg A$ :  $A$ 가 아닙니다.
- $V$ : 모든 집합의 클래스(폰 노이만 우주)입니다.
- $\omega$ : 첫 번째 무한 순서수이며, 음이 아닌 정수 전체의 집합이기도 합니다.
- $V_\alpha$ : 폰 노이만 우주의 단계입니다.
- $On$ : 순서수의 클래스입니다.
- $\bigcup A$ :  $A$  내부 원소들의 합집합입니다.
- $A \approx B$ : 집합  $A$ 와  $B$ 가 동수(equinumerous)입니다.
- $\aleph_\alpha$ : 알레프 수
- $\text{cof } \lambda$ :  $\lambda$ 의 공종도
- $\mathcal{M} \models \phi[b_1, \dots, b_n]$ : 모델  $\mathcal{M}$ 이 매개변수  $b_1, \dots, b_n$ 을 가진 문장  $\phi$ 를 만족합니다
- $\Delta_n, \Sigma_n, \Pi_n$ : 레비 계층의 단계
- $\mathcal{M}_1 \subseteq \mathcal{M}_2$ :  $\mathcal{M}_1$ 은  $\mathcal{M}_2$ 의 부분구조입니다
- $\mathcal{M}_1 \prec \mathcal{M}_2$ :  $\mathcal{M}_1$ 은  $\mathcal{M}_2$ 의 초등 부분구조입니다
- $p \parallel q$ : 포셋  $\mathbb{P}$ 의 원소  $p$ 와  $q$ 가 양립 가능합니다
- $p \perp q$ : 포셋  $\mathbb{P}$ 의 원소  $p$ 와  $q$ 가 양립 불가능합니다
- $\text{Name}_\alpha$ :  $\mathbb{P}$ -이름의 계층
- $\tau^G$ : 필터  $G$ 에 의한 이름  $\tau$ 의 해석
- $M[G]$ : 강제 포셋  $G \subseteq \mathbb{P}$ 로부터 얻은 모델
- $p \Vdash \varphi(\sigma_1, \dots, \sigma_n)$ :  $p \in \mathbb{P}$ 가 문장  $\varphi$ 를 강제합니다
- $\dot{x}$ : 해석되었을 때  $x \in M$ 을 주는 이름
- $\dot{G}$ : 해석될 때  $G$ 에 주어지는 이름



# E 집합과 함수에 관한 용어

이 부록에서는 "전단사", "동치류" 등과 같이 집합과 함수에 관한 몇 가지 개념을 다룰 것입니다.

전문가를 위한 참고: 이 장에서는 기초론적 문제를 다루지 않습니다. 관심이 있다면 [장 89](#)(및 이후 장)를 참고하십시오. 따라서 대부분의 주장에 대해 증명하지 않을 것입니다.

## §E.1 집합

우리에게 **집합**이란 그저 원소들의 모임입니다(그것이 무엇이든 간에). 예를 들어, 집합  $\mathbb{N} = \{1, 2, 3, 4, \dots\}$ 는 양의 정수들이고,  $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ 는 모든 정수의 집합입니다. 또 다른 예로, 우리는 사람들의 집합을 가지고 있습니다:

$$H = \{x \mid x \text{는 깃털 없는 두발 동물입니다}\}.$$

(여기서 "|"는 "다음을 만족하는"을 의미합니다.)

원소가 하나도 없는 집합도 있는데, 이를 **공집합**이라고 부릅니다. 이는  $\emptyset$ 으로 표시됩니다.

관계적으로 집합에는 대문자를 사용하고(예:  $H$ ), 집합의 원소에는 소문자를 사용합니다(예:  $x$ ).

**정의 E.1.1.** 우리는 " $x$ 가  $S$ 에 속한다"는 것을 나타내기 위해  $x \in S$ 라고 씁니다. 예를 들어  $3 \in \mathbb{N}$ 입니다.

**정의 E.1.2.** 집합  $A$ 의 모든 원소가 집합  $B$ 에도 속한다면,  $A$ 는  $B$ 의 **부분집합**이라고 하며, 이를  $A \subseteq B$ 로 표시합니다. 만약 더 나아가  $A \neq B$ 라면,  $A$ 를 **진부분집합**이라고 하며  $A \subsetneq B$ 라고 씁니다. (이는  $\leq$ 와  $<$ 의 관계와 유사합니다.)

집합  $A$ 가 주어졌을 때, 모든 부분집합의 집합을  $2^A$  또는  $\mathcal{P}(A)$ 로 표시하며, 이를  $A$ 의 **멱집합**이라고 부릅니다.

### 예제 E.1.3 (부분집합의 예)

- (a)  $\{1, 2, 3\} \subseteq \mathbb{N} \subseteq \mathbb{Z}$ .
- (b) 임의의 집합  $A$ 에 대해  $\emptyset \subseteq A$ 입니다. (왜 그럴까요?)
- (c) 임의의 집합  $A$ 에 대해  $A \subseteq A$ 입니다.
- (d)  $A = \{1, 2\}$ 라면  $2^A = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$ 입니다.

**정의 E.1.4.** 우리는 다음과 같이 씁니다

- $A \cup B$ 는  $A$  또는  $B$  둘 중 하나(어쩌면 둘 다)에 속하는 원소들의 집합으로,  $A$ 와  $B$ 의 **합집합**이라고 부릅니다.
- $A \cap B$ 는  $A$ 와  $B$  둘 다에 속하는 원소들의 집합으로,  $A$ 와  $B$ 의 **교집합**이라고 부릅니다.
- $A \setminus B$ 는  $A$ 에는 속하지만  $B$ 에는 속하지 않는 원소들의 집합입니다.

**예제 E.1.5 (집합 연산의 예)**

$A = \{1, 2, 3\}$ 이고  $B = \{3, 4, 5\}$ 라고 합시다. 그러면

$$A \cup B = \{1, 2, 3, 4, 5\}$$

$$A \cap B = \{3\}$$

$$A \setminus B = \{1, 2\}.$$

**연습문제 E.1.6.** 스스로 확인해 보십시오: 임의의 집합  $A$ 와  $B$ 에 대해  $A \cap B \subseteq A \subseteq A \cup B$ 입니다.

자주 등장하는 몇 가지 집합은 다음과 같습니다:

- $\mathbb{C}$ 는  $3.2 + \sqrt{2}i$ 와 같은 복소수들의 집합입니다.
- $\mathbb{R}$ 은  $\sqrt{2}$ 나  $\pi$ 와 같은 실수들의 집합입니다.
- $\mathbb{N}$ 은 5나 9와 같은 양의 정수의 집합입니다.
- $\mathbb{Q}$ 은  $7/3$ 과 같은 유리수의 집합입니다.
- $\mathbb{Z}$ 는  $-2$ 나 8과 같은 정수의 집합입니다.

(이들은 여러분이 예상하는 대로 발음됩니다: “씨”, “아르”, “엔”, “큐”, “제드”).

**§E.2 함수**

두 집합  $A$ 와  $B$ 가 주어졌을 때,  $A$ 에서  $B$ 로 가는 **함수**  $f$ 는  $A$ 의 모든 원소를  $B$ 의 어떤 원소로 대응시키는 사상입니다.

$A$ 를  $f$ 의 **정의역**이라 부르고,  $B$ 를 **공역**이라 부릅니다. 이를  $f: A \rightarrow B$  또는  $A \xrightarrow{f} B$ 로 씁니다.

**표기의 남용 E.2.1.**  $f$ 라는 이름이 중요하지 않다면, 종종 그냥  $A \rightarrow B$ 로 쓰겠습니다.

$f$ 가  $a$ 를  $b$ 로 보낸다는 것을 나타내기 위해  $f(a) = b$  또는  $a \mapsto b$ 로 씁니다.

$B$ 가 원소로 0을 가지고  $f(a) = 0$ 이면, 우리는 종종  $a$ 가  $f$ 의 **근** 또는 **영점**이라고 말하며,  $f$ 가  $a$ 에서 **소멸한다**고 말합니다.

**§E.2.i 단사, 전사, 전단사 함수**

**정의 E.2.2.** 함수  $f: A \rightarrow B$ 가 다음과 같은 의미에서 “일대일”이면 **단사**라고 합니다:  $f(a) = f(a')$ 이면  $a = a'$ 입니다. 다시 말해, 임의의  $b \in B$ 에 대해,  $f(a) = b$ 인  $a \in A$ 가 많아야 하나 존재합니다.

이를 강조하기 위해 종종  $f: A \hookrightarrow B$ 로 쓰겠습니다.

**정의 E.2.3.** 함수  $f: A \rightarrow B$ 가 다음과 같은 의미에서 “위로의” 함수이면 **전사**라고 합니다: 임의의  $b \in B$ 에 대해,  $f(a) = b$ 인  $a \in A$ 가 적어도 하나 존재합니다.

이를 강조하기 위해 종종  $f: A \twoheadrightarrow B$ 로 쓰겠습니다.

**정의 E.2.4.** 함수  $f: A \rightarrow B$ 가 단사이면서 동시에 전사이면 **전단사**라고 합니다. 다시 말해, 각  $b \in B$ 에 대해,  $f(a) = b$ 인  $a \in A$ 가 정확히 하나 존재합니다.

**예제 E.2.5 (함수의 예시)**

“인간”이란 “깃털 없는 두 발 생명체”를 뜻합니다.

- (a) 모든 인간을 (가장 가까운 정수로 반올림한) 나이(년 단위)로 보내는 함수가 있습니다. 이 함수는 예를 들어 나이가 20인 사람이 많기 때문에 **단사가 아닙니다**. 이 함수는 또한 나이가 10000인 사람이 없으므로 **전사도 아닙니다**.
- (b) 모든 미국 시민을 그들의 사회보장번호로 보내는 함수가 있습니다. 이 함수 역시 SSN이 3인 사람이 없으므로 **전사가 아니지만**, 적어도 동일한 SSN을 가진 두 사람이 없으므로 **단사이기는 합니다**.

**예제 E.2.6 (전단사의 예시)**

- (a)  $A = \{1, 2, 3, 4, 5\}$ 이고  $B = \{6, 7, 8, 9, 10\}$ 이라고 합시다. 그러면  $a \mapsto a + 5$ 로 정의되는 함수  $f: A \rightarrow B$ 는 전단사입니다.
- (b) 좌석이 30개인 교실에서, 모든 좌석에는 정확히 한 명의 학생이 있습니다. 따라서 각 학생을 그가 앉은 좌석으로 보내는 함수는 전단사입니다. 특히, 학생은 정확히 30명입니다.

**비고 E.2.7** — 편의를 위해  $A$ 와  $B$ 가 유한 집합이라고 가정합시다. 그러면 다음이 성립합니다:

- $f: A \hookrightarrow B$ 가 단사이면,  $A$ 의 크기는  $B$ 의 크기 이하입니다.
- $f: A \twoheadrightarrow B$ 가 전사 함수라면,  $A$ 의 크기는  $B$ 의 크기 이상입니다.
- $f: A \rightarrow B$ 가 전단사라면,  $A$ 의 크기는  $B$ 의 크기와 같습니다.

이제  $f: A \rightarrow B$ 가 전단사라면, “ $f$ 를 거꾸로 적용”할 수 있다는 점에 주목하십시오: (예를 들어, 각 학생을 그가 앉아 있는 좌석으로 대응시키는 대신, 각 좌석을 그 좌석에 앉아 있는 학생으로 대응시킵니다). 이를 **역함수**라 하며,  $f^{-1}: B \rightarrow A$ 로 표기합니다.

**§E.2.ii 상과 원상**

$X \xrightarrow{f} Y$ 를 함수라 합시다.

**정의 E.2.8.**  $T \subseteq Y$ 라 합시다. **원상**  $f^{\text{pre}}(T)$ 는  $f(x) \in T$ 를 만족하는 모든  $x \in X$ 의 집합입니다. 따라서  $f^{\text{pre}}(T)$ 는  $X$ 의 부분집합입니다.

**예제 E.2.9 (원상의 예)**

앞서 나온 나이 함수  $f: H \rightarrow \mathbb{Z}$ 를 생각합시다. 그러면

- (a)  $f^{\text{pre}}(\{13, 14, 15, 16, 17, 18, 19\})$ 는 십대들의 집합입니다.
- (b)  $f^{\text{pre}}(\{0\})$ 는 신생아들의 집합입니다.
- (c)  $f^{\text{pre}}(\{1000, 1001, 1002, \dots\}) = \emptyset$ 인데, 그렇게 나이가 많은 사람은 없다고 생각하기 때문입니다.

**표기의 남용 E.2.10.** 표기의 남용으로,  $f^{\text{pre}}(\{y\})$ 를  $f^{\text{pre}}(y)$ 로 줄여 쓸 수 있습니다. 예를 들어 위의  $f^{\text{pre}}(\{0\})$ 는  $f^{\text{pre}}(0)$ 으로 줄여 씁니다.

쌍대 개념은 다음과 같습니다:

**정의 E.2.11.**  $S \subseteq X$ 라 합시다. 상  $f^{\text{img}}(S)$ 는  $f(s)$  꼴인 모든 것들의 집합입니다.

**예제 E.2.12 (상의 예)**

$A = \{1, 2, 3, 4, 5\}$ 이고  $B = \mathbb{Z}$ 라 합시다. 다음과 같이 주어진 함수  $f: A \rightarrow B$ 를 생각 합시다

$$f(1) = 17 \quad f(2) = 17 \quad f(3) = 19 \quad f(4) = 30 \quad f(5) = 234.$$

(a) 상  $f^{\text{img}}(\{1, 2, 3\})$ 는 집합  $\{17, 19\}$ 입니다.

(b) 상  $f^{\text{img}}(A)$ 는 집합  $\{17, 19, 30, 234\}$ 입니다.

**질문 E.2.13.**  $f: A \rightarrow B$ 가 전사 함수라 합시다.  $f^{\text{img}}(A)$ 는 무엇입니까?

### §E.3 동치 관계

이제  $X$ 를 고정된 집합이라 합시다.  $X$  위의 이항 관계  $\sim$ 는 각  $x$ 와  $y$ 에 대해  $x \sim y$ 에 “참” 또는 “거짓”이라는 진리값을 부여합니다. 이제  $X$  위의 **동치 관계**  $\sim$ 는 다음 공리들을 만족 하는 이항 관계입니다:

- 반사성:  $x \sim x$ 가 성립합니다.
- 대칭성:  $x \sim y$ 이면  $y \sim x$ 입니다
- 추이성:  $x \sim y$ 이고  $y \sim z$ 이면  $x \sim z$ 입니다.

그러면 **동치류**는 서로 동치인 모든 것들의 집합입니다. 이러한 동치류들에 의해  $X$ 가 분할 됨을 보일 수 있습니다:

**예제 E.3.1 (동치 관계의 예)**

$\mathbb{N}$ 을 양의 정수들의 집합이라 합시다. 그러면  $a$ 와  $b$ 의 마지막 자릿수가 같을 때  $a \sim b$  라고 정의한다고 합시다. 예를 들어  $131 \sim 211$ ,  $45 \sim 125$  등입니다.

그러면  $\sim$ 는 동치 관계입니다. 이는  $\mathbb{N}$ 을 마지막 자리 숫자별로 열 개의 동치류로 분할 합니다.

종종 동치류들의 집합은  $X/\sim$ 로 표기됩니다 (“ $X \bmod \sim$ ”이라고 읽습니다).

# 이미지 저작자 표시

- [1207] 127“RECT”. *Cantor set in seven iterations*. Public domain. 2007. URL: [https://en.wikipedia.org/wiki/File:Cantor\\_set\\_in\\_seven\\_iterations.svg](https://en.wikipedia.org/wiki/File:Cantor_set_in_seven_iterations.svg) (cited p. 400)
- [ca] POP-UP CASKET. *Omega exp*. Public domain. URL: <https://commons.wikimedia.org/wiki/File:Omega-exp-omega-labeled.svg> (cited p. 927)
- [Ee] EYORE22. *Weierstrass function*. Public domain. URL: <https://commons.wikimedia.org/wiki/File:WeierstrassFunction.svg> (cited p. 350)
- [Fr] FROPUFF. *Klein bottle*. Public domain. URL: <https://en.wikipedia.org/wiki/File:KleinBottle-01.png> (cited p. 662)
- [Ge] TOPOLOGICAL GIRL’S GENERATION. *Topological Girl’s Generation*. (dead link). URL: <https://topologicalgirlsgeneration.tumblr.com/> (cited p. 53)
- [gk] G.KOV. *Normal surface vector*. URL: <https://tex.stackexchange.com/a/235142/76888> (cited p. 454)
- [Go08] ABSTRUSE GOOSE. *Math Text*. CC 3.0. 2008. URL: <https://abstrusegoose.com/12> (cited p. x)
- [Go09] ABSTRUSE GOOSE. *Zornaholic*. CC 3.0. 2009. URL: <https://abstrusegoose.com/133> (cited p. 931)
- [Ho] GEORGE HODAN. *Apple*. Public domain. URL: <https://www.publicdomainpictures.net/view-image.php?image=20117> (cited p. 941)
- [In] INDUCTIVELOAD. *Klein Bottle Folding*. Public domain. URL: [https://commons.wikimedia.org/wiki/File:Klein\\_Bottle\\_Folding\\_1.svg](https://commons.wikimedia.org/wiki/File:Klein_Bottle_Folding_1.svg) (cited p. 662)
- [Kr] PETR KRATOCHVIL. *Velociraptor*. Public domain. URL: <https://www.publicdomainpictures.net/view-image.php?image=93881> (cited p. 941)
- [Ma12] MATHMATHSMATHEMATICS. *How to Multiply Matrices - A 2x2 Matrix by various sizes*. May 2012. URL: <https://youtu.be/pJwslaulUMU> (cited p. 149)
- [Mu] RANDALL MUNROE. *Rolle’s theorem*. CC 2.5. URL: <https://xkcd.com/2042/> (cited p. 326)
- [Na] KRISH NAVEDALA. *Stokes patch*. Public domain. URL: [https://en.wikipedia.org/wiki/File:Stokes\\_patch.svg](https://en.wikipedia.org/wiki/File:Stokes_patch.svg) (cited p. 464)
- [Or] BEN ORLIN. *The Math Major Who Never Reads Math*. URL: <https://mathwithbaddrawings.com/2015/03/17/the-math-major-who-never-reads-math/> (cited p. xi)
- [To] TOAHIGHERLEVEL. *Projection color torus*. Public domain. URL: [https://en.wikipedia.org/wiki/File:Projection\\_color\\_torus.jpg](https://en.wikipedia.org/wiki/File:Projection_color_torus.jpg) (cited p. 660)
- [Wa] BILL WATTERSON. *Calvin and Hobbes*. I think this is fair use. (cited p. 879)



## 참고 문헌

- [Al09] PAOLO ALUFFI. *Algebra: chapter 0*. Vol. 104. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2009, pp. xx+713. ISBN: 978-0-8218-4781-7. DOI: [10.1090/gsm/104](https://doi.org/10.1090/gsm/104). URL: <https://doi.org/10.1090/gsm/104> (cited p. 723)
- [Ax97] SHELDON AXLER. *Linear algebra done right*. New York: Springer, 1997. ISBN: 978-0-387-98258-8 (cited pp. 159, 995)
- [Ba10] JOSEPH BAK. *Complex analysis*. New York: Springer Science+Business Media, LLC, 2010. ISBN: 978-1-4419-7287-3 (cited p. 349)
- [Ch08] STEVE CHENG. “A Crash Course on the Lebesgue Integral and Measure Theory”. Apr. 2008. URL: <https://www.gold-saucer.org/math/lebesgue/lebesgue-new.pdf> (cited p. 996)
- [Et11] PAVEL ETINGOF. “Introduction to Representation Theory”. 2011. URL: <https://math.mit.edu/~etingof/replect.pdf> (cited pp. vii, 997)
- [Ga03] ANDREAS GATHMANN. “Algebraic Geometry”. 2003. URL: <https://www.mathematik.uni-kl.de/~gathmann/de/alggeom.php> (cited pp. vii, 922, 997)
- [Ga14] DENNIS GAITSGORY. “Math 55a: Honors Abstract and Linear Algebra”. 2014. URL: <https://web.evanchen.cc/coursework.html> (cited pp. vii, 995)
- [Ga15] DENNIS GAITSGORY. “Math 55b: Honors Real and Complex Analysis”. 2015. URL: <https://web.evanchen.cc/coursework.html> (cited pp. 339, 995)
- [Go11] TIMOTHY GOWERS. “Normal subgroups and quotient groups”. 2011. URL: <https://gowers.wordpress.com/2011/11/20/normal-subgroups-and-quotient-groups/> (cited pp. 73, 995)
- [Go18] VADIM GORIN. “18.175: Theory of Probability”. 2018. URL: <https://web.archive.org/web/20190617235844/http://web.mit.edu/txz/www/links.html> (cited pp. vii, 996)
- [Ha02] ALLEN HATCHER. *Algebraic topology*. Cambridge, New York: Cambridge University Press, 2002. ISBN: 0-521-79160-X. URL: <https://opac.inria.fr/record=b1122188> (cited pp. 659, 745, 756, 766, 773, 785, 790, 795, 997)
- [Hi13] A. J. HILDEBRAND. “Introduction to Analytic Number Theory”. 2013. URL: <https://web.archive.org/web/20230326025121/https://faculty.math.illinois.edu/~hildebr/ant/main.pdf> (cited p. 998)
- [Ko14] PETER KOELLNER. “Math 145a: Set Theory I”. 2014. URL: <https://web.evanchen.cc/coursework.html> (cited pp. vii, 997)
- [Le] HOLDEN LEE. “Number Theory”. URL: <https://github.com/holdenlee/number-theory> (cited p. 630)
- [Le02] HENDRIK LENSTRA. “The Chebotarev Density Theorem”. 2002. URL: <https://websites.math.leidenuniv.nl/algebra/> (cited pp. 635, 997)
- [Le14] TOM LEINSTER. *Basic category theory*. Cambridge: Cambridge University Press, 2014. ISBN: 978-1-107-04424-1. URL: <https://arxiv.org/abs/1612.09375> (cited pp. vii, 691, 694, 712, 715, 933, 996)

- [Ll15] SETH LLOYD. “18.435J: Quantum Computation”. 2015. URL: <https://web.evanchen.cc/coursework.html> (cited pp. vii, 996)
- [Ma13a] LAURENTIU MAXIM. “Math 752 Topology Lecture Notes”. 2013. URL: <https://www.math.wisc.edu/~maxim/752notes.pdf> (cited pp. 785, 997, 1032)
- [Ma13b] MAXIMA. “Burnside’s Lemma, post 6”. 2013. URL: <https://www.aops.com/Forum/viewtopic.php?p=3089768#p3089768> (cited p. 216)
- [Mi14] ALEXANDRE MIQUEL. “An Axiomatic Presentation of the Method of Forcing”. 2014. URL: <https://www.fing.edu.uy/~amiquel/forcing/> (cited p. 997)
- [Mi95] R. MIRANDA. *Algebraic Curves and Riemann Surfaces*. Dimacs Series in Discrete Mathematics and Theoretical Comput. American Mathematical Society, 1995. ISBN: 9780-8218-0268-7 (cited pp. 498, 528, 998)
- [Mu00] JAMES MUNKRES. *Topology*. 2nd. Prentice-Hall, Inc., Jan. 2000. ISBN: 97881-203-2046-8. URL: <https://amazon.com/o/ASIN/8120320468/> (cited p. 997)
- [Og10] FREDERIQUE OGGIER. “Algebraic Number Theory”. 2010. URL: <https://feog.github.io/ANT10.pdf> (cited pp. 537, 997)
- [Pu02] C. C. PUGH. *Real mathematical analysis*. New York: Springer, 2002. ISBN: 978-0-387-95297-0 (cited pp. vii, 109, 123, 298, 306, 350, 454, 459, 995, 996)
- [Sc07] W. H. SCHIKHOF. *Ultrametric Calculus: An Introduction to P-Adic Analysis*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2007. ISBN: 9780-521-03287-2. URL: <https://books.google.com/books?id=cBT05R7TH1QC> (cited p. 316)
- [Sj05] REYER SJAMAAR. “Manifolds and Differential Forms”. 2005. URL: <https://pi.math.cornell.edu/~sjamaar/manifolds/manifold.pdf> (cited pp. vii, 488, 490, 995)
- [Ul08] BROOKE ULLERY. “Minkowski Theory and the Class Number”. 2008. URL: <https://www.math.uchicago.edu/~may/VIGRE/VIGRE2008/REUPapers/Ullery.pdf> (cited p. 558)
- [Va17] RAVI VAKIL. “The Rising Sea: Foundations of Algebraic Geometry”. Nov. 2017. URL: <https://math.stanford.edu/~vakil/216blog/> (cited pp. iii, vii, 811, 812, 818, 819, 889, 901, 922, 997, 998)
- [Ya12] ANDREW YANG. “Math 43: Complex Analysis”. 2012. URL: <https://math.dartmouth.edu/~m43s12/syllabus.html> (cited pp. 349, 355, 996)