CHEONSANG LAB REFERENCE SERIES

수학 마스터 레퍼런스

정의 · 정리 · 조건 · 예제 · 핵심 증명

백과사전식 개정판 · 3차 집필본 0.3.0

2026년 11월 13일

CHEONSANG LAB 천상 연구실

이 판에 대하여

백과사전식 개정판 3차 집필본 0.3.0은 직전 판인 2차 집필본 0.2.1(699쪽)을 처음부터 LaTeX 로 다시 조판한 판이다. 직전 판의 쪽을 그대로 옮기거나 덧붙인 것이 아니라, 모든 식과 문장을 새로 입력하여 표제어의 정의, 핵심 식, 유도, 적용 조건, 예의 순서로 다시 짰다. 직전 판의 정의, 정리, 식, 유도는 빠뜨리지 않고 옮겼으며, 고친 곳은 책 끝의 「개정 내역」에 기록했다.

구성

본문은 19권 149장이다. 수와 계산(제1권), 문자식·방정식·부등식(제2권), 함수·삼각법·초등기하(제3권), 증명·명제논리·술어논리(제4권), 집합·수 체계·수학기초론(제5권), 선형대수(제7권), 미분·적분·급수(제8권), 다변수·벡터해석(제9권), 실해석·측도·적분(제10권), 복소해석(제11권), 미분방정식·동역학(제12권), 함수해석·편미분방정식(제13권), 군·환·체·갈루아 이론(제14권), 정수론·대수적 정수론(제15권), 조합론·그래프·이산수학(제19권), 확률론(제20권), 확률과정(제21권), 수리통계·추론(제22권), 현대 연구 지도·증명 보조기(제28권)의 차례로 이어진다. 각 권의 첫머리에 그 권의 내용과 장 사이의 연결을 적었다.

권 번호는 전체 편집 계획의 번호를 그대로 쓴다. 전체 계획은 28권이며, 이 판에는 제1–5권, 제7–15권, 제19–22권, 제28권의 19권이 실려 있다. 제6권(모형론·증명론·계산가능성), 제16권(위상수학·대수적 위상), 제17권(미분기하·다양체), 제18권(대수기하·가환대수), 제23권(회귀·다변량·베이지안 통계), 제24권(실험설계·인과·비모수 통계), 제25권(수치해석·최적화), 제26권(정보론·계산복잡도·기계학습의 수학), 제27권(범주론·호몰로지·유형이론)은 아직 집필되지 않았으며, 이 판에는 본문이 없다.

본문 뒤에는 부록 「개정 기록」이 있고, 그 안의 「개정 내역」은 직전 판에서 바로잡은 오류와 보충한 내용을 작업 단위별로 기록한다. 끝에 찾아보기가 있다.

조판

본문 글꼴은 Times New Roman이고 한글은 Noto Serif CJK KR이며, 수식은 `newtxmath`로 조판했다. 권·장의 번호와 상호 참조, 차례, 찾아보기는 모두 조판 도구가 원고에서 자동으로 만든다.

개정의 방향

개정은 세 가지를 목표로 했다. 첫째는 오류 수정이다. 식의 부호와 계수, 용어, 인명과 연도, 논리의 비약을 하나씩 확인하여 바로잡았다. 둘째는 내용의 보충이다. 기호의 뜻, 정리가 성립하는 조건, 유도의 빠진 단계, 대표 예제, 다른 장으로의 연결을 채웠다. 셋째는 문체의 정리이다. 어느 주제에나 붙일 수 있는 반복 문장을 옮기지 않고, 그 자리에 해당 정리와 주제에만 적용되는 구체적인 조건과 검산을 적었다.

일러두기

범위와 읽는 법

이 책은 기초 계산부터 대학 수학과 현대 연구의 입구까지를 연결하는 한국어 참고서이다. 정의와 정리의 가정을 먼저 제시하고, 계산 예제와 반례를 통해 적용 범위를 확인한다. 중요한 작은 정리는 증명을 수록하고, 큰 연구 정리는 원출처와 증명 범위를 구분한다. 논리학·수학기초론·확률론·통계학도 독립적인 축으로 다룬다. 이 책은 완성된 전집이 아니다. 전체 편집 계획 28권 가운데 19권만 실려 있으며(「이 판에 대하여」), 수록된 권도 해당 분야의 완결을 뜻하지 않는다.

각 장의 선행 지식을 먼저 확인한다. 처음 읽을 때는 정의와 예제를 중심으로 한 번 읽고, 두 번째에는 정리의 가정이 증명의 어디에서 쓰이는지 표시하며 읽는다. 연습문제는 풀이를 가린 상태에서 시도한 뒤 비교한다. 참고서는 필요한 내용을 찾아보는 데에도 적합하지만, 선행 개념이 없는 연구 장을 순서만 따라 읽는 것으로 모든 배경을 익힐 수는 없다.

분야 사이의 연결

기초 학습은 수와 계산(제1권), 문자식·방정식(제2권), 함수·기하(제3권)를 이어 읽는다. 증명·논리(제4권)와 집합·기초론(제5권)은 이후 정리의 언어를 이해하는 기반이다. 선형대수(제7권)와 미적분(제8권)은 다변수 해석(제9권), 실해석(제10권), 복소해석(제11권), 미분방정식(제12권), 함수해석(제13권), 확률과 통계에 반복해서 등장한다. 대수학(제14권)과 정수론(제15권)은 서로를 보강한다. 확률론(제20권)에서는 분포와 기댓값을 익힌 뒤 수렴과 극한정리로, 수리통계(제22권)에서는 모형과 추정대상을 정한 뒤 추론의 불확실성으로 이동한다. 현대 연구 장(제28권)은 기초 과목을 모두 대체하는 입문서가 아니라, 무엇을 더 배워야 연구 문장을 읽을 수 있는지 보여 주는 지도이며, 소개한 연구 주제는 선택된 사례이다.

장의 구성

장은 정의문으로 시작하는 요약(장의 내용, 증명하는 사실, 선행 지식)으로 열고, 절마다 정의, 정리, 증명, 예제를 차례로 배치한다. 정리에는 그 정리가 성립하는 조건을 명시하고, 중요한 작은 정리에는 증명을 붙인다. 증명하지 않고 인용하는 큰 결과는 그렇다고 밝힌다. 정의·정리·보조정리·명제·따름정리·예제·연습문제는 장마다 하나의 번호로 이어 매기며(예: 정리 5.3), 번호 없는 주석(참고, 주의, 흔한 오류, 핵심, 검산 등)은 해당 위치에서 보충한다. 장 끝에는 연습문제와 풀이를 둔다. 풀이는 결과만 적지 않고, 그 풀이가 쓰는 정리와 확인해야 할 조건을 함께 적는다. 일부 권의 끝에는 그 권의 범위와 다음 읽기를 안내하는 글이 있다.

표기 규약

본문 수식은 LaTeX 로 조판했다. 자연수는 별도 언급이 없으면 0을 포함한다. 실수, 복소수, 확률공간 등 대상의 범위는 장마다 확인한다. $\Rightarrow$와 $\Leftrightarrow$, 최댓값과 상한, 점별수렴과 균등수렴처럼 비슷해 보이는 개념은 구분하여 쓴다. 같은 기호가 서로 다른 분야에서 다른 뜻으로 쓰이면 그 장의 정의를 우선한다. 예를 들어 제13권은 함수해석의 관례에 따라 내적의 둘째 변수에 켤레를 둔다.

정의되는 용어는 굵은 글씨로 쓰고 찾아보기에 올렸으며, 영어 원어는 처음 나올 때 기울임꼴로 병기했다. 인명은 원어 로마자로 적는다. 두 사람의 이름을 잇는 경우에는 Cauchy–Riemann과 같이 줄표로 연결한다.

상호 참조

권은 전체 계획의 번호를 쓰고, 장은 권마다 1부터 다시 센다. 다른 권의 장을 가리킬 때는 ‘제7권 제3장’ 처럼 권과 장의 번호를 함께 적으며, 같은 권 안에서는 ‘제3장’ 으로 줄여 쓴다. 절은 장 번호를 앞에 붙여 5.2절처럼 쓴다. 식은 괄호 안의 번호로, 정리 등은 장 번호와 일련번호로 가리킨다. 번호는 모두 조판 도구가 자동으로 부여하므로, 본문의 상호 참조는 조판할 때마다 새로 계산된다.

검토 범위

이 판은 수식 조판, 목차 연결, 대표 수치 예제와 기본 논증을 검토한 원고이다. 모든 정리를 기계적으로 인증한 문서는 아니다. 제28권의 연구 동향은 해당 권에 적힌 확인 기준일의 원논문과 공식 발표를 바탕으로 하며, 공개된 주장, 검토 중인 결과, 조건부 형식화를 구분하여 적었다. 설명과 예제는 이 참고서를 위해 작성했으며, 추가 읽기로 적은 자료는 관련 원자료를 찾아가기 위한 안내이지 원문 전체의 재사용 허가를 뜻하지 않는다.

차례

이 판에 대하여 i
일러두기 ii

I 수와 계산 **1**

1 수, 표현, 연산의 약속 2
2 정수의 나눗셈과 약수 9
3 소수와 정수의 구조 16
4 분수, 유리수, 소수 표현 23
5 순서, 절댓값, 기본 부등식 30
6 무리수와 실수의 완비성 34
7 거듭제곱, 근호, 지수와 로그 43
8 근사값, 오차, 수치 표현 50
9 합동식과 나머지 계산 54
10 복소수의 첫 구조 58
11 유한한 합과 계산 구조 64

II 문자식·방정식·부등식 **69**

1 문자식과 동치 변형 70
2 다항식의 계산과 나눗셈 73
3 인수분해와 유리식 77
4 일차방정식과 연립방정식 81
5 이차방정식과 근의 구조 85
6 유리방정식과 무리방정식 88
7 부등식의 해집합과 부호표 91
8 부등식의 증명과 최댓값·최솟값 95
9 지수·로그 방정식과 매개변수 99

III 함수·삼각법·초등기하 **102**

1 함수와 그래프의 언어 103
2 좌표, 직선, 거리 107

3 각도와 삼각함수 . . . 110
4 삼각형과 원의 기하 . . . 118
5 이차곡선과 극좌표 . . . 125

IV 증명·명제논리·술어논리 135

1 수학적 진술과 양화사의 언어 . . . 136
2 명제논리: 진리표에서 논리적 귀결까지 . . . 142
3 증명 방법과 반례의 설계 . . . 148
4 술어논리의 구문, 의미, 치환 . . . 155
5 자연연역과 시퀀트의 첫걸음 . . . 161
6 귀납법과 재귀적 정의 . . . 168
7 관계, 분할, 몫집합 . . . 175
8 함수, 섬유, 역함수와 크기 비교 . . . 180
9 부분순서, 정렬, 최대성 원리 . . . 186
10 정규형, 해결법, 유한 SAT의 완전성 . . . 192
11 유한 조건과 무한 조건: 콤팩트성의 의미 . . . 199
12 증명 교정 실습과 반례 설계 . . . 205

V 집합·수 체계·수학기초론 212

1 집합을 말하는 언어와 역설의 경계 . . . 213
2 ZFC 공리: 존재를 허용하는 정확한 규칙 . . . 218
3 자연수에서 정수와 유리수까지 . . . 223
4 데데킨트 절단으로 실수를 구성하기 . . . 229
5 가산성, 대각선, 기수와 서수의 입문 . . . 235
6 선택공리, 독립성, 불완전성의 정확한 범위 . . . 241

VII 선형대수 249

1 연립일차방정식과 소거법 . . . 250
2 벡터공간과 부분공간 . . . 258
3 선형독립·기저·차원 . . . 265
4 선형사상·핵·상과 차원 정리 . . . 271
5 행렬표현과 기저변환 . . . 277
6 행렬식: 가역성·부피·방향 . . . 285
7 고유값·고유벡터와 대각화 . . . 293

8 내적·직교·최소제곱 . . . 302

VIII 미분·적분·급수 314

1 함수의 극한과 연속 . . . 315
2 미분과 계산법 . . . 321
3 평균값정리와 최적화 . . . 327
4 리만적분과 미적분 기본정리 . . . 334
5 적분기법과 이상적분 . . . 342
6 수열·급수와 Taylor 근사의 조건 및 오차 . . . 350

IX 다변수·벡터해석 361

1 $\mathbb{R}^n$의 거리, 열린집합, 극한과 연속 . . . 362
2 미분가능성: 편미분, 전미분, 연쇄법칙 . . . 367
3 고계 도함수, Taylor 정리, 극값 판정 . . . 371
4 역함수 정리, 음함수 정리, Lagrange 승수법 . . . 375
5 중적분: Fubini 정리와 변수변환 . . . 379
6 선적분, 보존장, 면적분 . . . 385
7 Green·Stokes·발산 정리와 벡터 항등식 . . . 389
8 미분형식과 일반화된 Stokes 정리 . . . 393

X 실해석·측도·적분 397

1 실수의 위상과 상극한 . . . 398
2 함수열과 균등수렴 . . . 402
3 σ-대수와 측도 . . . 406
4 가측함수와 Lebesgue 적분 . . . 410
5 지배수렴정리와 적분의 계산 . . . 414
6 곱측도와 Fubini–Tonelli 정리 . . . 417
7 L^p 공간 . . . 423
8 미분과 적분: 유계변동, 절대연속, 미분정리 . . . 427

XI 복소해석 433

1 복소함수와 정칙성: Cauchy–Riemann 방정식 . . . 434
2 멱급수와 초등함수: 지수, 로그, 거듭제곱 . . . 440
3 복소 선적분과 Cauchy 정리 . . . 447

4 Cauchy 적분공식과 그 결과 . . . 454
5 Laurent 급수와 고립특이점 . . . 458
6 유수 정리와 실적분의 계산 . . . 461
7 편각 원리, Rouché 정리, 열린사상 정리 . . . 465
8 등각사상과 Riemann 사상정리 . . . 468

XII 미분방정식·동역학 472

1 미분방정식의 언어와 1계 방정식 . . . 473
2 해의 존재와 유일성, 연장과 의존성 . . . 477
3 고계 선형 방정식과 급수해 . . . 480
4 선형계와 행렬지수, 상평면 . . . 484
5 Laplace 변환과 전달함수 . . . 488
6 비선형계의 평형점과 안정성 . . . 492
7 극한주기와 분기 . . . 495
8 이산 동역학과 혼돈 . . . 499

XIII 함수해석·편미분방정식 504

1 노름공간과 유계 선형 작용소 . . . 505
2 Hilbert 공간과 Fourier 급수 . . . 509
3 Banach 공간의 세 기둥 . . . 513
4 스펙트럼과 콤팩트 작용소 . . . 517
5 편미분방정식의 분류, 특성곡선, 파동방정식 . . . 522
6 변수분리와 Sturm–Liouville 문제 . . . 526
7 Laplace 방정식, Green 함수, Fourier 변환 . . . 530
8 약해, Sobolev 공간, Lax–Milgram 정리 . . . 533

XIV 군·환·체·갈루아 이론 537

1 군의 정의, 부분군, 순환군, Lagrange 정리 . . . 538
2 정규부분군, 몫군, 동형정리 . . . 544
3 군의 작용과 Sylow 정리 . . . 549
4 환, 아이디얼, 몫환 . . . 553
5 다항식환, 주아이디얼정역, 유일인수분해 . . . 557
6 가군과 PID 위의 유한생성 가군 . . . 562
7 체의 확대, 분해체, 유한체, 작도 문제 . . . 566

8 Galois 이론과 근의 공식 571

XV 정수론·대수적 정수론 575

1 합동, Euler 함수, 원시근 576
2 이차잉여와 이차상호법칙 579
3 산술함수, Dirichlet 합성곱, Möbius 반전 584
4 연분수, Diophantus 근사, Pell 방정식 589
5 소수의 분포와 Riemann zeta 함수 593
6 대수적 정수와 수체의 정수환 596
7 Dedekind 정역, 아이디얼 분해, 이데알류군 599
8 p 진수와 국소–대역 원리 602

XIX 조합론·그래프·이산수학 608

1 세는 대상과 일대일 대응 609
2 포함과 배제, 대칭을 가진 계수 613
3 점화식과 생성함수 617
4 그래프, 연결, 나무와 순회 621
5 이분 그래프, 색칠과 평면성 625
6 매칭과 네트워크 흐름 629

XX 확률론 634

1 표본공간, 사건, 확률의 공리 635
2 계수법과 유한 확률모형 641
3 조건부 확률, 베이즈 공식, 독립성 647
4 확률변수, 분포함수, 확률질량과 밀도 653
5 기댓값, 분산, 공분산 659
6 핵심 확률분포와 변환 도구 668
7 결합분포와 다변수 변환 681
8 조건부 기댓값과 정보의 수학 687
9 변환함수, 분포의 식별, 모멘트 692
10 확률변수열의 수렴과 반례 698
11 큰수법칙, 중심극한정리, 델타 방법 704
12 확률 부등식, 집중, 큰편차의 입문 710

XXI 확률과정 **717**

1 시간지표, 분포, 경로, 정상성 . . . 718
2 이산시간 Markov 연쇄와 정상분포 . . . 722
3 흡수, 도달시간, 기본행렬 . . . 726
4 Poisson 과정과 지수 대기시간 . . . 731
5 마팅게일과 정지 규칙 . . . 735
6 Brownian 운동, Itô 적분, 확률미분방정식 . . . 742

XXII 수리통계·추론 **752**

1 통계적 모형, 표본, 추정대상 . . . 753
2 점추정, 편향, 평균제곱오차 . . . 758
3 우도, 최대우도추정, 충분성 . . . 763
4 신뢰구간과 예측구간 . . . 769
5 가설검정, 검정력, 다중검정 . . . 775
6 베이지안 추론의 기본 . . . 781

XXVIII 현대 연구 지도·증명 보조기 **788**

1 현재의 수학을 읽는 법 . . . 789
2 소수의 분포와 덧셈의 구조 . . . 795
3 Langlands: 수론·표현·기하를 잇는 대응 . . . 802
4 기하와 위상: 공간에서 어떤 정보를 남길 것인가 . . . 808
5 PDE·동역학·확률: 해가 존재한다는 말의 여러 의미 . . . 816
6 증명 보조기·mathlib·AI: 무엇을 검증했는가 . . . 823

XXIX 개정 기록 **831**

A 개정 내역 . . . 832
찾아보기 . . . 838

제 1 권

수와 계산

제1권은 수의 표현과 계산을 정확한 규칙 위에 세우는 권이다. 제1장은 이후 모든 권이 쓰는 수 집합의 기호, 위치적 기수법, 사칙연산의 법칙과 연산 순서의 규약을 정한다. 제2–3장은 나눗셈 정리에서 최대공약수와 베주 항등식을 거쳐 소수와 산술의 기본정리에 이르고, 제4–6장은 유리수와 소수 표현, 순서와 절댓값, $\sqrt{2}$의 무리성과 실수의 완비성으로 수의 범위를 넓힌다. 제7장 이하는 지수와 로그, 근사값과 오차, 합동식, 복소수의 첫 구조, 유한합을 차례로 다루어 정수론, 해석학, 수치 계산으로 이어지는 계산의 기초를 마련한다.

제 1 장

수, 표현, 연산의 약속

개요 수는 양이나 순서를 나타내는 수학적 대상이고, 숫자와 기호는 그 대상을 적는 표현이다. 이 장은 이후 모든 권에서 쓰는 수 집합의 기호, 위치적 기수법, 사칙연산의 법칙, 괄호와 연산 순서의 규약을 정하고, 계산 결과를 다른 원리로 확인하는 검산법을 정리한다. 증명하는 사실은 b진법 표현의 존재와 유일성, 그리고 부호 계산 규칙 $0a = 0$, $(-a)b = -(ab)$, $(-a)(-b) = ab$이다. 선행 지식: 자연수의 덧셈과 곱셈.

1.1 수와 숫자는 다르다

수(*number*)는 양이나 순서 등을 나타내는 수학적 대상이고, **숫자**(*numeral*)와 기호는 그 대상을 표현하는 방법이다. 예를 들어 12, 3×4, $24/2$는 서로 다른 표현이지만 같은 수를 가리킨다. 표현이 달라도 값이 같다는 판단은 계산과 증명의 출발점이다. 반대로 기호의 모습이 비슷하다고 해서 뜻까지 같은 것은 아니다. 정수 1, 1×1 행렬, 항등함수는 문맥에 따라 비슷한 역할을 하지만 같은 종류의 대상이 아니다.

이 책에서 **자연수**는 별도의 언급이 없으면

$$\mathbb{N} = \{0, 1, 2, \dots\}$$

로 정한다. 양의 자연수의 집합은 $\mathbb{N}_{>0}$으로 쓴다. 자연수에 0을 포함하는지는 책마다 다르므로, 다른 자료를 읽을 때에는 저자의 규약을 먼저 확인해야 한다. **정수**, **유리수**, **실수**, **복소수**의 집합은 각각 $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$로 표기하며, 다음 포함 관계가 성립한다.

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}. \tag{1.1}$$

이 포함 관계는 기존 수의 계산을 보존하면서 계산할 수 있는 범위를 넓힌다는 뜻이다. 정수에서는 뺄셈을 항상 할 수 있고, 유리수에서는 0이 아닌 수로 나눌 수 있으며, 실수에서는 유리수만으로 표현하지 못하는 길이와 극한을 다룬다. 복소수에서는 $x^2 + 1 = 0$ 같은 방정식의 해를 다룰 수 있다. 단, 복소수까지 확장해도 0으로 나누는 연산이 생기지는 않는다. 각 수 체계를 앞 단계로부터 구성하는 방법은 제5권 제3장과 제5권 제4장에서, 실수의 완비성은 제1권 제6장에서, 복소수는 제1권 제10장에서 다룬다. 표 1.1는 각 단계에서 새로 가능해지는 계산과 여전히 불가능한 계산을 요약한다.

표 1.1 수 체계의 확장

집합	이름	새로 가능해지는 계산	그 안에서 할 수 없는 계산의 예
$\mathbb{N}$	자연수	덧셈, 곱셈	$3-5$
$\mathbb{Z}$	정수	뺄셈	$1\div 2$
$\mathbb{Q}$	유리수	0이 아닌 수로 나누기	$x^2=2$의 해
$\mathbb{R}$	실수	극한, 길이($\sqrt{2}$, π)	$x^2+1=0$의 해
$\mathbb{C}$	복소수	상수가 아닌 모든 다항방정식의 풀이	0으로 나누기, 연산과 어울리는 대소 비교

예제 1.1 분수 2/4와 1/2가 같은 수라는 말은 분자와 분모의 모양이 같다는 뜻이 아니다. 유리수의 표현에서는 정수의 쌍 (a,b)와 (c,d)가 $ad=bc$를 만족하면 같은 수 $a/b=c/d$를 표현한다. 여기서 $b,d\neq 0$이다. 따라서 $2\cdot 2=1\cdot 4$를 이용해 $2/4=1/2$임을 확인한다. 한 유리수를 나타내는 분수는 무한히 많고, 그 가운데 분자와 분모의 양의 공약수가 1뿐인 것이 기약분수이다(제1권 제4장).

흔한 오류 (등호의 연쇄). 등호 =는 "다음 계산을 한다"는 표시가 아니라 양쪽의 값이 같다는 주장이다. $3+4=7\times 2=14$라고 쓰면 $3+4=14$까지 주장하게 되므로 틀린 식이다. "$3+4=7$, 따라서 두 배는 $2\cdot 7=14$"처럼 계산 대상이 바뀌었음을 명시해야 한다.

1.2 위치적 기수법

위치적 기수법(*positional numeral system*)은 숫자가 놓인 자리에 따라 그 숫자가 나타내는 크기가 달라지는 수 표기법이다. 정수 $b\geq 2$를 **밑**으로 하는 위치적 기수법에서 각 자릿수 a_j는 $0\leq a_j<b$를 만족하는 정수이다. 유한한 숫자열 $(a_m a_{m-1}\cdots a_0)_b$의 값은

$$(a_m a_{m-1}\cdots a_0)_b=\sum_{j=0}^{m} a_j b^j \tag{1.2}$$

로 정의한다. **십진법**은 $b=10$, **이진법**은 $b=2$인 경우이다. 밑을 적지 않은 숫자열은 십진법으로 읽는다. 맨 왼쪽의 불필요한 0을 제외하면 각 자연수의 이러한 표현은 유일하다(명제 1.3). 이 사실은 나눗셈 정리(제1권 제2장, 정리 2.1)를 반복하여 증명한다.

예제 1.2 $(101101)_2$의 값은 식 (1.2)에 따라

$$1\cdot 2^5+0\cdot 2^4+1\cdot 2^3+1\cdot 2^2+0\cdot 2+1=45$$

이다. 반대로 45를 2로 계속 나누면

$$45=2\cdot 22+1,\qquad 22=2\cdot 11+0,$$
$$11=2\cdot 5+1,\qquad 5=2\cdot 2+1,$$
$$2=2\cdot 1+0,\qquad 1=2\cdot 0+1.$$

나머지를 마지막 것부터 거꾸로 읽으면 101101을 얻는다. 처음 나온 나머지가 가장 낮은 자리의 숫자이다.

명제 1.3 (b진법 표현의 존재와 유일성) 정수 $b \geq 2$를 고정하면 모든 자연수 n은 유한한 b진법 표현을 갖는다. 선행하는 0을 허용하지 않으면 표현은 유일하다.

증명. $n = 0$은 한 자리 0으로 표현한다. 이하 $n > 0$이라 하고, 표현의 맨 앞자리는 0이 아니라고 약속한다.

존재. n을 b로 나누어 $n = bq + a_0$, $0 \leq a_0 < b$로 쓴다. $b \geq 2$이므로 $q \leq n/b < n$이다. $q > 0$이면 몫 q에 같은 과정을 반복한다. 몫은 매번 엄격히 작아지는 자연수이므로 유한 번 뒤에 0에 도달한다. $q_0 = n$으로 두고 이때 얻은 식 $q_0 = bq_1 + a_0$, $q_1 = bq_2 + a_1$, $\ldots$, $q_m = b \cdot 0 + a_m$을 역으로 대입하면

$$n = a_0 + b\big(a_1 + b(a_2 + \cdots + b\,a_m)\big) = \sum_{j=0}^{m} a_j b^{\,j}$$

이고, 마지막 몫 $q_m = a_m$은 0이 아니므로 맨 앞자리가 0이 아닌 표현을 얻는다.

유일성. 두 표현 $(a_m \cdots a_0)_b$와 $(c_k \cdots c_0)_b$가 같은 수 n을 나타낸다고 가정한다. 가장 낮은 자리를 뗀 숫자열 $(a_m \cdots a_1)_b$는 $m = 0$이면 빈 숫자열이며 그 값은 0으로 본다.

$$n = b\,(a_m \cdots a_1)_b + a_0 = b\,(c_k \cdots c_1)_b + c_0$$

이고 $0 \leq a_0, c_0 < b$이므로, 나눗셈 정리의 유일성에 의해 나머지 $a_0 = c_0$과 몫 $(a_m \cdots a_1)_b = (c_k \cdots c_1)_b$가 각각 같다. 몫은 n보다 작으므로 같은 논법을 몫에 반복하면 낮은 자리부터 차례로 모든 자릿수가 같다. 두 표현의 맨 앞자리가 0이 아니므로 몫이 0이 되는 단계도 같고, 따라서 $m = k$이다. □

소수점 아래의 유한한 자릿수도 같은 원리로 해석한다. 일반적으로

$$(a_m \cdots a_0\,.\,a_{-1}a_{-2}\cdots a_{-k})_b = \sum_{j=-k}^{m} a_j b^{\,j}$$

로 정의한다. 예를 들어 $(0.101)_2 = 2^{-1} + 2^{-3} = 5/8$이다. 한 기수법에서 유한하게 표현되는 수가 다른 기수법에서도 유한하게 표현되는 것은 아니다. 십진수 $0.1 = 1/10$은 이진법에서

$$\frac{1}{10} = (0.0001100110011\cdots)_2$$

와 같이 0011이 끝없이 반복된다. 이 차이는 컴퓨터의 부동소수점 계산에서 중요하다. 이진 부동소수점 수는 0.1을 정확히 저장하지 못하고 가까운 이진 유한소수로 대신한다(제1권 제8장).

참고 (유한하게 표현되는 조건). 기약분수 p/q $(q > 0)$가 b진법에서 소수점 아래 k자리 이하로 표현된다는 것은 $b^k p/q$가 정수라는 뜻이고, p와 q가 서로소이므로 이는 $q \mid b^k$와 같다. 따라서 p/q가 b진법의 유한소수가 될 필요충분조건은 q의 모든 소인수가 b를 나누는 것이다. $1/10$의 분모는 소인수 5를 가지므로 이진법에서 유한하게 표현되지 않고, $5/8$의 분모는 소인수가 2뿐이므로 유한하게 표현된다. 무한소수 표현과 순환은 제1권 제4장에서 다룬다.

역사 (위치적 기수법). 자리의 값을 이용한 표기는 고대 메소포타미아의 육십진법에서 이미 쓰였다. 시간과 각도를 60으로 나누는 관습은 그 흔적이다. 0을 하나의 숫자로 갖춘 십진 위치 기수법은 인도에서 정립되어 아랍 세계를 거쳐 유럽에 전해졌고, Fibonacci의 『Liber Abaci』(1202)가 이 표기법을 유럽에 널리 알렸다.

1.3 사칙연산의 법칙과 적용 범위

실수의 덧셈과 곱셈은 모든 실수 a, b, c에 대하여 다음 법칙을 만족한다.

$$a + b = b + a, \qquad ab = ba, \tag{1.3}$$

$$(a + b) + c = a + (b + c), \qquad (ab)c = a(bc), \tag{1.4}$$

$$a(b + c) = ab + ac. \tag{1.5}$$

식 (1.3)은 **교환법칙**, 식 (1.4)은 **결합법칙**이며, 식 (1.5)는 **분배법칙**이다. 0은 덧셈의 **항등원**이고 1은 곱셈의 항등원이다. 즉 모든 a에 대하여

$$a + 0 = a, \qquad a \cdot 1 = a$$

이다. 각 실수 a에는 $a + (-a) = 0$을 만족하는 덧셈의 **역원** $-a$가 있으며, $a \neq 0$이면 $a\,a^{-1} = 1$을 만족하는 곱셈의 역원 a^{-1}이 있다. 이 법칙들은 유리수와 복소수에서도 그대로 성립하며, 추상대수에서는 이 법칙들을 만족하는 체계를 체(*field*)라고 부른다(제14권 제4장). 자연수에는 0 이외의 수의 덧셈 역원이 없고, 정수에는 ± 1 이외의 수의 곱셈 역원이 없다.

뺄셈과 나눗셈은 별개의 기본 법칙을 외우기보다 역원을 이용하여

$$a - b = a + (-b), \qquad \frac{a}{b} = a\,b^{-1} \quad (b \neq 0) \tag{1.6}$$

로 이해하면 계산 규칙의 이유를 설명할 수 있다. 뺄셈과 나눗셈은 일반적으로 교환법칙도 결합법칙도 만족하지 않는다. 예를 들어 $8 - 3 \neq 3 - 8$이고, $(8/4)/2 = 1$이지만 $8/(4/2) = 4$이다.

명제 1.4 (부호 규칙) 모든 실수 a, b에 대하여 $0a = 0$, $(-a)b = -(ab)$, $(-a)(-b) = ab$이다.

증명. 먼저 덧셈 역원은 유일하다. $a + x = 0$이고 $a + y = 0$이면 $x = x + (a + y) = (x + a) + y = y$이기 때문이다. 따라서 어떤 수 x가 $a + x = 0$을 만족하면 $x = -a$이고, 특히 $-(-a) = a$이다.

분배법칙으로 $0a = (0 + 0)a = 0a + 0a$이다. 양변에 $-(0a)$를 더하면 $0a = 0$을 얻는다. 다음으로 $ab + (-a)b = \big(a + (-a)\big)b = 0b = 0$이므로 $(-a)b$는 ab의 덧셈 역원, 곧 $-(ab)$이다. 마지막으로

$$(-a)b + (-a)(-b) = (-a)\big(b + (-b)\big) = (-a) \cdot 0 = 0$$

이므로 $(-a)(-b)$는 $(-a)b = -(ab)$의 덧셈 역원, 즉 ab이다. □

참고 (0으로 나눌 수 없는 이유). 명제 1.4에 의해 모든 x에 대하여 $0 \cdot x = 0 \neq 1$이므로 0의 곱셈 역원은 존재하지 않는다. 식 (1.6)에서 $b \neq 0$이라는 조건은 임의로 붙인 제한이 아니라 덧셈·곱셈의 법칙에서 나오는 결과이다. 이 논증은 위 법칙만 사용하므로 유리수, 실수, 복소수 어디에서나 성립한다.

흔한 오류 (법칙의 적용 범위). 실수의 곱셈 법칙을 모든 대상에 그대로 적용하면 안 된다. 행렬에서는 일반적으로 $AB \neq BA$이다. 예를 들어

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \quad \text{이면} \quad AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad BA = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

이다. 함수의 합성과 사원수의 곱셈도 순서를 바꾸면 결과가 달라질 수 있다. $f(x) = x+1$, $g(x) = 2x$이면 $f(g(x)) = 2x + 1$이지만 $g(f(x)) = 2x + 2$이다. 어떤 계산을 시작하기 전에 대상과 연산을 확인해야 한다.

1.4 괄호와 연산 순서

연산 순서의 규약은 괄호를 생략한 식을 한 가지로 읽기 위한 약속이다. 괄호 안을 가장 먼저 계산하고, 거듭제곱을 먼저, 그다음 곱셈과 나눗셈, 마지막으로 덧셈과 뺄셈을 계산한다. 이 약속은 긴 식을 짧게 쓰기 위한 문법이다. 곱셈과 나눗셈이 같은 단계에 연이어 나타나면 일반적으로 왼쪽부터 해석하며, 덧셈과 뺄셈도 마찬가지이다. 거듭제곱이 겹치면 위쪽부터 읽어 $a^{b^c} = a^{(b^c)}$로 해석한다. 예를 들어 $2^{3^2} = 2^9 = 512$이고 $(2^3)^2 = 64$이다. 그러나 오해하기 쉬운 식은 이 약속에 기대기보다 분수선이나 괄호를 써서 뜻을 명확히 해야 한다.

$$-3^2 = -(3^2) = -9, \qquad (-3)^2 = 9.$$

마이너스 부호와 거듭제곱이 미치는 범위가 다르기 때문에 결과가 다르다. 마찬가지로 $1/(a+b)$는 $1/a + b$와 다르며, 분모의 괄호를 생략하면 계산 대상 자체가 바뀐다.

음의 수의 제곱근을 다루기 전까지는 $\sqrt{x}$를 실수 $x \geq 0$에 대하여 제곱하면 x가 되는 음이 아닌 실수로 정의한다. 이 정의에서 $\sqrt{x^2} = |x|$이며, 일반적으로 $\sqrt{x^2} = x$는 성립하지 않는다(제1권 제7장).

> **예제 1.5** 식 $18-6/3\cdot 2+1$의 값은 $18-2\cdot 2+1 = 15$이다. $6/(3\cdot 2)$를 의도했다면 $18-6/(3\cdot 2)+1 = 18$로 다른 식을 써야 한다. 계산기나 프로그램의 표시 방식이 모호하다면 입력을 괄호로 분명하게 만드는 것이 안전하다.

문자식을 계산할 때에는 값의 대입을 먼저 할 수도 있고, 허용되는 법칙으로 식을 정리한 다음 대입할 수도 있다. 두 방법은 같은 정의역 안에서는 같은 답을 주어야 한다. 두 답이 다르면 연산 순서, 부호, 정의역 제한 중 무엇을 놓쳤는지 확인한다. 예를 들어 $(x^2-1)/(x-1)$은 $x \neq 1$에서 $x+1$과 값이 같지만 $x = 1$에서는 정의되지 않는다(제2권 제1장).

1.5 역산과 크기 추정으로 검산하기

검산은 계산 결과가 옳은지를 별도의 계산으로 확인하는 일이다. 계산 결과를 다시 같은 방식으로 계산하는 것만으로는 같은 실수를 반복할 수 있으므로, 다른 원리를 이용한 검산이 더 유용하다. 덧셈의 결과는 뺄셈으로, 곱셈의 결과는 나눗셈으로 확인할 수 있다. 또한 대략적인 크기, 부호, 홀짝성, 마지막 자리처럼 전체 계산보다 쉽게 얻는 정보를 비교할 수 있다. 이러한 검사는 틀린 답을 걸러 내는 필요조건이며 옳은 답임을 보증하는 충분조건은 아니다. 자릿수의 합을 이용한 9의 나머지 검산은 제1권 제9장에서 다룬다.

> **예제 1.6** 48×51은
>
> $$(50-2)(50+1) = 2500 + 50 - 100 - 2 = 2448$$
>
> 이다. 결과는 약 $50^2 = 2500$ 근처여야 하고, 더 정확히는 $48\cdot 50 = 2400$과 $50\cdot 51 = 2550$ 사이에 있어야 한다. 마지막 자리는 8×1의 마지막 자리인 8이어야 한다. 두 검사는 정답을 단독으로 증명하지는 않지만 24480, 2248 같은 일부 오류를 빠르게 발견한다. 24480은 크기와 마지막 자리가 모두 맞지 않고, 2248은 마지막 자리는 맞지만 하한 2400보다 작다.

예제 1.7 $7/12 + 5/18$의 공통분모로 36을 선택하면 $21/36 + 10/36 = 31/36$이다. $7/12$는 $1/2$보다 조금 크고 $5/18$은 $1/3$보다 조금 작으므로 합이 $1/2+1/3 = 5/6$ 근처라는 추정과도 맞는다. 분자는 분자끼리, 분모는 분모끼리 더한 $12/30$은 덧셈의 정의와 맞지 않으며, 크기 추정에서도 의심할 수 있다. $12/30 = 2/5$는 더하는 한 항 $7/12$보다도 작기 때문이다.

핵심 수식

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}, \qquad (a_m \cdots a_0)_b = \sum_{j=0}^{m} a_j b^j \quad (0 \le a_j < b),$$

$$a - b = a + (-b), \quad \frac{a}{b} = a\,b^{-1}\ (b \neq 0), \quad 0a = 0, \quad (-a)b = -(ab), \quad (-a)(-b) = ab.$$

1.6 문제와 풀이

연습문제 1.8 $(2031)_4$를 십진수로 바꾸고, 87을 삼진수로 나타내어라.

풀이. $(2031)_4 = 2\cdot 64 + 0\cdot 16 + 3\cdot 4 + 1 = 141$이다. 87을 3으로 계속 나누면

$$87 = 3\cdot 29 + 0, \quad 29 = 3\cdot 9 + 2, \quad 9 = 3\cdot 3 + 0, \quad 3 = 3\cdot 1 + 0, \quad 1 = 3\cdot 0 + 1$$

이므로 나머지를 거꾸로 읽어 $87 = (10020)_3$이다. 실제로 $3^4 + 2\cdot 3 = 87$이다.

연습문제 1.9 $a \neq 0$일 때 a^{-1}이 유일함을 보여라.

풀이. $ab = ac = 1$을 만족하는 b, c가 있다고 하자. 그러면

$$b = b\cdot 1 = b(ac) = (ba)c = (ab)c = 1\cdot c = c$$

이다. 이 증명에는 곱셈의 결합법칙과 항등원의 성질, 그리고 $ba = ab$에서 교환법칙이 사용된다.

연습문제 1.10 $a - b = b - a$를 만족하는 실수 a, b의 관계를 구하여라.

풀이. 양변에 $a + b$를 더하면 $2a = 2b$이고, $2 \neq 0$이므로 양변에 2^{-1}을 곱하여 $a = b$를 얻는다. 역으로 $a = b$이면 양변은 모두 0이다. 따라서 구하는 관계는 $a = b$이다.

연습문제 1.11 $99\cdot 101$을 긴 곱셈 없이 계산하고, 사용한 항등식을 밝혀라.

풀이. $(100-1)(100+1) = 100^2 - 1^2 = 9999$이다. 일반적으로 $(x-y)(x+y) = x^2 - y^2$이며, 이는 분배법칙을 적용했을 때 두 교차항 xy와 $-yx$가 상쇄되기 때문이다.

연습문제 1.12 십진수 0.6875를 이진법으로 나타내고, $1/3$이 이진법에서 유한하게 표현되지 않음을 설명하여라.

풀이. 소수 부분에 2를 곱할 때마다 나오는 정수 부분이 차례로 소수점 아래 자릿수가 된다.

$$0.6875\cdot 2 = 1.375, \quad 0.375\cdot 2 = 0.75, \quad 0.75\cdot 2 = 1.5, \quad 0.5\cdot 2 = 1$$

이므로 $0.6875 = (0.1011)_2$이다. 실제로 $2^{-1} + 2^{-3} + 2^{-4} = 11/16 = 0.6875$이다. $1/3$의 분모는 2를 나누지 않는 소인수 3을 가지므로 이진법의 유한소수가 아니다. 같은 방법을 적용하면 $1/3 \to$

$2/3 \to 4/3$에서 자릿수 $0, 1$이 나온 뒤 소수 부분이 다시 $1/3$으로 돌아오므로 $1/3 = (0.010101\cdots)_2$이다.

참고 (다음 연결). 기수법은 정수의 나눗셈(제1권 제2장)과 합동식(제1권 제9장), 그리고 수의 컴퓨터 표현(제1권 제8장)으로 이어진다. 연산 법칙은 추상대수의 군·환·체(제14권 제1장, 제14권 제4장)로 이어진다. 그 단계에서는 계산 규칙을 사용하는 데 그치지 않고 어떤 공리에서 규칙이 나오는지를 살핀다.

제 2 장

정수의 나눗셈과 약수

개요 정수의 나눗셈은 정수 a를 양의 정수 b로 나누어 몫과 나머지를 정하는 연산이고, 약수 관계는 나머지가 0인 경우를 가리킨다. 이 장은 나눗셈 정리에서 출발하여 약수와 배수, 최대공약수, 유클리드 알고리즘, 베주 항등식을 차례로 세우고, 이를 일차 디오판토스 방정식 $ax + by = c$의 풀이와 최소공배수의 공식에 적용한다. 모든 결과는 소인수분해를 쓰지 않고 나눗셈만으로 증명한다. 선행 지식: 정수의 사칙연산과 부등식의 기본 의미.

2.1 나눗셈 알고리즘

정수의 나눗셈은 몫과 나머지가 유일하게 정해진다는 다음 정리에 근거한다. 이 정리는 관례상 나눗셈 알고리즘(*division algorithm*)이라고도 불리지만, 내용은 계산 절차가 아니라 존재와 유일성의 진술이다.

정리 2.1 (나눗셈 정리) 정수 a와 양의 정수 b에 대하여

$$a = bq + r, \qquad 0 \le r < b \tag{2.1}$$

를 만족하는 정수 q, r가 유일하게 존재한다. q를 **몫**, r를 **나머지**라고 한다.

증명. 존재. $a - bq \ge 0$이 되는 정수 q를 생각한다. 그러한 q는 충분히 작게 선택하면 존재한다. 실제로 $q = -|a|$로 놓으면 $b \ge 1$이므로 $a - bq = a + b|a| \ge a + |a| \ge 0$이다. 따라서 $a - bq$ 꼴의 음이 아닌 정수의 집합은 비어 있지 않고, 자연수의 공집합이 아닌 부분집합에는 가장 작은 원소가 있으므로 그 가운데 가장 작은 것을 $r = a - bq$로 선택할 수 있다. $r \ge b$라면 $r - b = a - b(q+1)$도 음이 아니면서 r보다 더 작으므로 r의 선택에 모순이다. 따라서 $0 \le r < b$이다.

유일성. 두 표현 $a = bq + r = bq' + r'$가 있고 $0 \le r, r' < b$라 하면 $b(q - q') = r' - r$이고 $|r' - r| < b$이다. 절댓값이 b보다 작은 b의 정수배는 0뿐이다. $q \ne q'$이면 $|b(q-q')| \ge b$이기 때문이다. 따라서 $q = q'$이고 $r = r'$이다. □

참고 (몫의 공식과 음의 제수). 식 (2.1)의 몫은 a/b를 넘지 않는 가장 큰 정수, 곧 $q = \lfloor a/b \rfloor$이고 $r = a - b\lfloor a/b \rfloor$이다. 증명에 쓰인 "자연수의 공집합이 아닌 부분집합에는 가장 작은 원소가 있다"는 성질은 정렬 원리이며 수학적 귀납법과 동치이다(제4권 제6장). 제수가 음수인 경우에도 $b \ne 0$이면 $a = bq + r,\ 0 \le r < |b|$를 만족하는 정수 q, r가 유일하게 존재한다. $|b|$로 나눈 식 $a = |b|\,q_1 + r$에서 $b < 0$이면 $q = -q_1$로 놓으면 된다.

양수인 피제수를 나누는 계산은 익숙하지만, 음수인 피제수에서도 나머지를 음이 아닌 수로 정한다는 점이 중요하다. $-17 = 5(-4) + 3$이므로 이 규약에서 -17을 5로 나눈 몫은 -4, 나머지는 3이다. $-17 = 5(-3) - 2$도 참인 등식이지만, 두 번째 나머지 -2는 정한 범위 $0 \le r < 5$를 만족하지 않는다. 프로그래밍 언어의 나머지 연산은 음수에서 서로 다른 규칙을 사용할 수 있으므로 수학의

규약과 자동으로 같다고 가정해서는 안 된다. 예를 들어 C 언어(C99 이후)의 정수 나눗셈은 몫을 0 쪽으로 버리므로 -17을 5로 나눈 몫과 나머지로 -3과 -2를 주고, Python의 연산자는 몫을 내림하므로 -4와 3을 준다.

2.2 약수와 배수

> **정의 2.2 (약수 관계)** 정수 a, b에 대하여 어떤 정수 k가 존재하여 $b = ak$이면 a가 b를 **나눈다**고 하고 $a \mid b$로 쓴다. 이때 a를 b의 **약수**, b를 a의 **배수**라고 한다. a가 b를 나누지 않으면 $a \nmid b$로 쓴다.

이 정의에서는 모든 정수 a에 대해 $a \mid 0$이 성립한다. $0 \mid b$는 $b = 0$인 경우에만 성립한다. "약수의 개수"를 셀 때에는 보통 양의 정수의 양의 약수만 센다는 별도의 문맥을 사용한다. 음의 약수까지 포함하면 개수가 두 배가 되므로 어떤 약수를 세는지 분명히 해야 한다.

참고 (약수와 크기). $a \mid b$이고 $b \neq 0$이면 $b = ak$에서 $k \neq 0$이므로 $|b| = |a|\,|k| \geq |a|$이다. 따라서 0이 아닌 정수의 약수는 유한 개이고, $a \mid b$이면서 $b \mid a$이면 $a = \pm b$이다. $a > 0$일 때 $a \mid b$는 b를 a로 나눈 나머지가 0이라는 것과 같다.

> **명제 2.3 (약수 관계의 선형성과 추이성)** $a \mid b$, $a \mid c$이면 모든 정수 u, v에 대하여 $a \mid ub + vc$이다. 또한 $a \mid b$, $b \mid c$이면 $a \mid c$이다.

증명. $b = ar$, $c = as$로 쓰면 $ub + vc = a(ur + vs)$이다. 두 번째 명제에서는 $b = ar$, $c = bt$로 놓아 $c = a(rt)$를 얻는다. □

> **예제 2.4** $7 \mid 35$, $7 \mid 56$이므로 7은 $3 \cdot 35 - 2 \cdot 56 = -7$도 나눈다. 반면 $6 \mid ab$라고 해서 $6 \mid a$ 또는 $6 \mid b$라고 결론 내릴 수는 없다. $a = 2$, $b = 3$이 반례이다. 소수에 대해서는 이와 다른 성질, 곧 소수 p가 ab를 나누면 a 또는 b를 나눈다는 성질이 성립한다(제1권 제3장).

2.3 최대공약수와 유클리드 알고리즘

두 정수 a, b를 모두 나누는 정수를 a, b의 **공약수**라고 한다. 둘 다 0은 아닌 정수 a, b의 공통된 양의 약수 중 가장 큰 것을 **최대공약수**(*greatest common divisor*)라고 하고 $\gcd(a, b)$로 쓴다. 1은 항상 공약수이고 0이 아닌 정수의 약수는 유한 개이므로 최대공약수는 존재한다. 음수의 부호는 약수 관계에 영향을 주지 않으므로 $\gcd(a, b) = \gcd(|a|, |b|)$이다. $a \neq 0$이면 $\gcd(a, 0) = |a|$이다. 관례적으로 $\gcd(0, 0) = 0$으로 확장하기도 하지만, 모든 정수가 0의 약수이므로 "가장 큰 양의 공약수"라는 정의 자체로는 이 경우를 설명할 수 없다.

> **정리 2.5 (나머지로 바꾸기)** 정수 a, b, q, r가 $a = bq + r$를 만족하면 a, b의 공약수와 b, r의 공약수는 같다. 따라서 둘 다 0인 예외를 제외하면
>
> $$\gcd(a, b) = \gcd(b, r) \tag{2.2}$$
>
> 이다.

증명. $d \mid a, d \mid b$이면 명제 2.3에 의해 $d \mid (a - bq) = r$이다. 역으로 $d \mid b, d \mid r$이면 $d \mid (bq + r) = a$이다. 두 공약수 집합이 같으므로 최대공약수도 같다. □

방법 (유클리드 알고리즘). **유클리드 알고리즘**(*Euclidean algorithm*)은 식 (2.2)을 반복하여 최대공약수를 구하는 절차이다. 정수 $a \geq b > 0$에 대하여 $r_0 = a$, $r_1 = b$로 놓는다.

1단계. $r_k > 0$인 동안 r_{k-1}을 r_k로 나누어 $r_{k-1} = q_k r_k + r_{k+1}$, $0 \leq r_{k+1} < r_k$를 구한다.

2단계. 나머지가 $r_{n+1} = 0$이 되면 멈춘다.

3단계. 마지막으로 나온 0이 아닌 나머지 r_n이 $\gcd(a, b)$이다.

$r_1 > r_2 > \cdots \geq 0$은 엄격히 감소하는 음이 아닌 정수의 열이므로 절차는 많아야 b번의 나눗셈 안에 끝난다. 정리 2.5에 의해 $\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_n, 0) = r_n$이다.

예제 2.6 $\gcd(252, 198)$을 유클리드 알고리즘으로 구한다.

$$252 = 1 \cdot 198 + 54,$$
$$198 = 3 \cdot 54 + 36,$$
$$54 = 1 \cdot 36 + 18,$$
$$36 = 2 \cdot 18.$$

마지막으로 나온 0이 아닌 나머지가 18이므로 최대공약수는 18이다. 제수와 나머지의 열은 $198 > 54 > 36 > 18 > 0$으로 엄격히 작아지는 음이 아닌 정수이므로 이 과정은 유한 번 안에 끝난다.

큰 수를 소인수분해한 뒤 최대공약수를 구할 수도 있지만, 소인수분해 자체가 어려울 수 있다. 위의 예에서는 $252 = 2^2 \cdot 3^2 \cdot 7$, $198 = 2 \cdot 3^2 \cdot 11$이므로 공통 소인수를 모아 $2 \cdot 3^2 = 18$을 얻는다. 유클리드 알고리즘은 소인수를 찾지 않고도 최대공약수를 계산한다. 구해야 하는 것(최대공약수)과 굳이 구할 필요가 없는 정보(소인수)를 구별하면 계산이 쉬워지는 예이다.

역사 (유클리드 알고리즘). 이 절차는 Euclid의 『원론』 제7권 첫머리의 명제에 실려 있으며, 지금까지 쓰이는 가장 오래된 알고리즘 가운데 하나이다. Lamé는 1844년에 나눗셈 횟수가 두 수 중 작은 수의 십진 자릿수의 다섯 배를 넘지 않음을 증명하였다. 정해진 횟수의 나눗셈이 필요한 가장 작은 입력은 이웃한 Fibonacci 수의 쌍이다.

2.4 베주 항등식

정리 2.7 (베주 항등식) 둘 다 0은 아닌 정수 a, b에 대하여 정수 x, y가 존재하여

$$ax + by = \gcd(a, b) \tag{2.3}$$

를 만족한다.

증명. 먼저 $a \geq b > 0$이라 하고 유클리드 알고리즘의 나머지 열 $r_0 = a$, $r_1 = b$, $r_{k+1} = r_{k-1} - q_k r_k$를 생각한다. 각 나머지는 앞의 두 수의 정수 계수 일차결합이다. 처음 두 수는 $r_0 = a \cdot 1 + b \cdot 0$,

$r_1 = a\cdot 0 + b\cdot 1$이고, $r_{k-1} = ax_{k-1} + by_{k-1}$, $r_k = ax_k + by_k$이면

$$r_{k+1} = a\,(x_{k-1} - q_k x_k) + b\,(y_{k-1} - q_k y_k)$$

이므로 귀납적으로 모든 나머지는 a, b의 정수 계수 일차결합이다. 마지막 0이 아닌 나머지가 최대공약수이므로 원하는 표현을 얻는다. a나 b가 음수이면 $|a|, |b|$에 대한 표현에서 해당 계수의 부호를 바꾸고, $a < b$이면 두 수의 역할을 바꾼다. 한 수가 0인 경우, 예를 들어 $b = 0$이면 $\gcd(a, 0) = |a|$이므로 a의 부호에 맞게 x를 1 또는 -1로, $y = 0$으로 선택하면 된다. □

식 (2.3)의 x, y를 **베주 계수**(*Bézout coefficients*)라고 한다.

예제 2.8 예제 2.6의 계산을 거꾸로 대입하면

$$\begin{aligned} 18 &= 54 - 36 \\ &= 54 - (198 - 3\cdot 54) \\ &= 4\cdot 54 - 198 \\ &= 4(252 - 198) - 198 \\ &= 4\cdot 252 - 5\cdot 198. \end{aligned}$$

따라서 $252x + 198y = 18$의 베주 계수의 한 쌍은 $(x, y) = (4, -5)$이다. 실제 곱셈으로 $1008 - 990 = 18$인지 확인하면 역대입의 부호 오류를 점검할 수 있다. 베주 계수는 유일하지 않다. $(4 - 11t,\ -5 + 14t)$는 모든 정수 t에 대하여 같은 식을 만족하며, $t = 1$이면 $(-7, 9)$이다.

흔한 오류 (값이 양수인 것과 계수가 양수인 것). 최대공약수는 양의 정수 계수 조합의 최솟값이 아니다. 계수 x, y는 음수여도 된다. 정확한 진술은 $ax + by$ 꼴로 나타나는 '양의 값' 가운데 가장 작은 값이 최대공약수라는 것이다. $d = \gcd(a, b)$는 a와 b를 나누므로 모든 값 $ax + by$를 나누고, 따라서 양의 값은 d 이상이다. 한편 정리 2.7에 의해 d 자신이 그러한 값이다. 같은 이유로 $ax + by$ 꼴의 정수 전체는 정확히 d의 배수 전체이다. 값이 양수라는 조건과 계수가 양수라는 조건을 혼동하면 안 된다.

참고 (베주 항등식의 직접적인 결과). $d = \gcd(a, b) = ax + by$라 하자.

(1) a, b의 모든 공약수 e는 $ax + by = d$를 나눈다. 곧 최대공약수는 크기뿐 아니라 약수 관계에서도 가장 큰 공약수이다.

(2) $(a/d)x + (b/d)y = 1$이므로 a/d와 b/d의 양의 공약수는 1뿐이다. 곧 $\gcd(a/d, b/d) = 1$이다.

(3) $\gcd(a, b) = 1$일 필요충분조건은 $ax + by = 1$을 만족하는 정수 x, y가 존재하는 것이다.

역사 (베주 항등식). 정수에 대한 이 결과는 Bachet de Méziriac의 저서(1624년 제2판)에 실려 있다. Bézout는 18세기에 같은 꼴의 항등식을 다항식에 대하여 증명하였고, 그의 이름이 정수의 경우에도 붙게 되었다.

2.5 일차 디오판토스 방정식

디오판토스 방정식(*Diophantine equation*)은 정수 계수의 다항방정식 가운데 정수해만을 구하는 방정식이다. 가장 간단한 경우인 이변수 일차 방정식 $ax + by = c$의 해는 최대공약수로 완전히 기술된다.

> **정리 2.9 (일차 디오판토스 방정식의 가해 조건)** 둘 다 0은 아닌 정수 a, b와 정수 c에 대하여 $ax + by = c$가 정수해를 가질 필요충분조건은 $\gcd(a, b) \mid c$이다.

증명. $d = \gcd(a, b)$라 하자. 정수해가 있으면 d는 $ax + by$를 나누므로 $d \mid c$이다. 역으로 $c = dk$라면 베주 항등식 $au + bv = d$에 k를 곱하여 해 $(x, y) = (ku, kv)$를 얻는다. □

a, b가 모두 0이 아니고 $d = \gcd(a, b)$이며 (x_0, y_0)가 $ax + by = c$의 한 해라면 모든 정수해는

$$x = x_0 + \frac{b}{d}t, \qquad y = y_0 - \frac{a}{d}t, \qquad t \in \mathbb{Z} \tag{2.4}$$

로 주어진다. 실제로 대입하면 교차하는 두 항 $\pm abt/d$가 상쇄되어 $ax+by = ax_0+by_0 = c$이다. 모든 해가 이 형태라는 사실은 다음과 같이 따른다. (x, y)가 해이면 두 식을 빼서 $a(x - x_0) = -b(y - y_0)$를 얻고, 양변을 d로 나누면

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0)$$

이다. a/d와 b/d는 서로소이므로 b/d는 $x - x_0$을 나눈다(연습문제 2.15). $x - x_0 = (b/d)t$로 놓고 대입한 뒤 $b/d \neq 0$으로 나누면 $y - y_0 = -(a/d)t$이다.

> **예제 2.10** $15x + 21y = 6$은 $d = \gcd(15, 21) = 3$이 6을 나누므로 정수해를 갖는다. $15 \cdot 3 + 21 \cdot (-2) = 3$이므로 양변에 2를 곱하여 $(x_0, y_0) = (6, -4)$가 한 해이며,
>
> $$x = 6 + 7t, \qquad y = -4 - 5t \qquad (t \in \mathbb{Z})$$
>
> 가 모든 정수해이다. 여기에 $x, y \geq 0$까지 요구하면 $t \geq -6/7$과 $t \leq -4/5$를 동시에 만족해야 하므로 그러한 정수 t는 없다. 정수해의 존재와 음이 아닌 정수해의 존재는 서로 다른 문제이다.

2.6 서로소와 최소공배수

$\gcd(a, b) = 1$이면 a, b가 **서로소**(*coprime*)라고 한다. 서로소인 두 수가 반드시 각각 소수일 필요는 없다. 예를 들어 8과 9는 둘 다 합성수이지만 서로소이다. 두 정수의 공통된 배수를 **공배수**라고 하고, 양의 정수 a, b의 공통된 양의 배수 중 가장 작은 것을 **최소공배수**(*least common multiple*)라고 하며 $\operatorname{lcm}(a, b)$로 쓴다. ab가 양의 공배수이므로 최소공배수는 존재한다.

> **정리 2.11 (최대공약수와 최소공배수의 곱)** 양의 정수 a, b에 대하여
>
> $$\gcd(a, b)\ \operatorname{lcm}(a, b) = ab \tag{2.5}$$
>
> 이다.

증명. $d = \gcd(a, b)$라 하고 $a = du$, $b = dv$로 쓴다. 그러면 $\gcd(u, v) = 1$이다. 실제로 베주 항등식 $ax + by = d$를 d로 나누면 $ux + vy = 1$이므로 u, v의 양의 공약수는 1뿐이다. $duv = av = bu$는

a, b의 공배수이다. 임의의 양의 공배수 m은 $a = du$의 배수이므로 $m = duk$로 쓸 수 있고, 이것이 dv로도 나누어지므로 $v \mid uk$이다. u, v가 서로소이므로 베주 항등식으로부터 $v \mid k$임을 얻는다 (연습문제 2.15). 따라서 $duv \mid m$이고, 특히 $duv \le m$이다. 그러므로 최소공배수는 $duv = ab/d$이다. □

이 증명은 모든 공배수가 최소공배수의 배수라는 사실도 함께 보인다. 예제 2.6의 두 수에 대해서는 $\operatorname{lcm}(252, 198) = 252 \cdot 198/18 = 2772$이다.

주의 (세 수 이상). 식 (2.5)은 두 수에 대한 등식이며 세 수에 대해서는 같은 꼴로 성립하지 않는다. $a = b = c = 2$이면 세 수의 최대공약수와 최소공배수가 모두 2여서 곱은 4이지만 $abc = 8$이다.

핵심 수식

$$a = bq + r, \quad 0 \le r < b, \qquad a = bq + r \implies \gcd(a, b) = \gcd(b, r),$$

$$ax + by = \gcd(a, b), \qquad ax + by = c \text{ 가 정수해를 가진다} \iff \gcd(a, b) \mid c,$$

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t, \qquad \gcd(a, b)\,\operatorname{lcm}(a, b) = ab \quad (a, b > 0).$$

2.7 문제와 풀이

연습문제 2.12 -29를 6으로 나눌 때의 몫과 음이 아닌 나머지를 구하여라.

풀이. $-29 = 6(-5) + 1$이므로 몫은 -5, 나머지는 1이다. 나머지의 범위 $0 \le 1 < 6$도 만족한다.

연습문제 2.13 $\gcd(414, 662)$를 구하고 베주 계수를 한 쌍 찾아라.

풀이. 유클리드 알고리즘을 적용하면

$$662 = 414 + 248, \quad 414 = 248 + 166, \quad 248 = 166 + 82, \quad 166 = 2 \cdot 82 + 2, \quad 82 = 41 \cdot 2$$

이므로 최대공약수는 2이다. 역대입하면

$$\begin{aligned} 2 &= 166 - 2 \cdot 82 = 166 - 2(248 - 166) = 3 \cdot 166 - 2 \cdot 248 \\ &= 3(414 - 248) - 2 \cdot 248 = 3 \cdot 414 - 5 \cdot 248 \\ &= 3 \cdot 414 - 5(662 - 414) = 8 \cdot 414 - 5 \cdot 662 \end{aligned}$$

이다. 따라서 $414x + 662y = 2$의 베주 계수의 한 쌍은 $(x, y) = (8, -5)$이고, 실제로 $3312 - 3310 = 2$이다.

연습문제 2.14 $12x + 18y = 7$의 정수해가 없는 이유를 계산 없이 설명하여라.

풀이. x, y가 정수이면 왼쪽은 항상 6의 배수이지만 오른쪽 7은 6의 배수가 아니다. $\gcd(12, 18) = 6 \nmid 7$이므로 정리 2.9의 최대공약수 조건만으로 불가능함을 알 수 있다.

연습문제 2.15 $\gcd(a, b) = 1$이고 $a \mid bc$이면 $a \mid c$임을 보여라.

풀이. 베주 항등식 $au + bv = 1$에 c를 곱하면 $acu + bcv = c$이다. 왼쪽의 첫째 항은 a의 배수이고, $a \mid bc$이므로 둘째 항도 a로 나누어진다. 따라서 오른쪽 c도 a로 나누어진다. 이 결과는 일반

정수에 대한 잘못된 추론 “$a \mid bc$이면 $a \mid b$ 또는 $a \mid c$”(예제 2.4)에 어떤 추가 조건이 필요한지 보여 준다. a와 b가 서로소라는 조건이 있으면 $a \mid c$라는 결론이 성립한다.

> **연습문제 2.16** 모든 정수 n에 대하여 $\gcd(n, n+1) = 1$이고 $\gcd(21n+4,\, 14n+3) = 1$임을 보여라.

풀이. $(n+1) - n = 1$이므로 n과 $n+1$의 공약수는 1을 나눈다. 따라서 $\gcd(n, n+1) = 1$이다. 마찬가지로

$$3(14n+3) - 2(21n+4) = 42n + 9 - 42n - 8 = 1$$

이므로 $21n+4$와 $14n+3$의 공약수도 1을 나눈다. 두 경우 모두 $ax + by = 1$ 꼴의 정수 계수 표현 하나가 서로소임을 증명한다.

참고 (다음 연결). 최대공약수는 합동식에서의 역원(제1권 제9장), 중국인의 나머지 정리와 Euler 함수(제15권 제1장), 다항식의 유클리드 알고리즘(제2권 제2장), 주아이디얼 정역의 구조(제14권 제5장)로 확장된다. 소수와 소인수분해의 유일성은 이 장의 결과를 바탕으로 제1권 제3장에서 증명한다.

제 3 장

소수와 정수의 구조

개요 소수는 1보다 큰 정수 가운데 양의 약수가 1과 자기 자신뿐인 수이다. 이 장은 소수가 곱을 나누면 인수 가운데 하나를 나눈다는 유클리드의 보조정리를 베주 항등식으로부터 증명하고, 이를 이용하여 1보다 큰 모든 정수가 소수의 곱으로, 순서를 제외하면 한 가지 방법으로만 표현된다는 산술의 기본정리를 세운다. 이어서 소인수의 지수 $v_p(n)$으로 약수 관계, 약수의 개수와 합, 최대공약수와 최소공배수를 기술하고, 소수가 무한히 많다는 정리와 에라토스테네스의 체를 다룬다. 선행 지식: 약수, 최대공약수, 베주 항등식(제1권 제2장).

3.1 소수, 합성수, 단위

정의 3.1 (소수와 합성수) 정수 $p > 1$의 양의 약수가 $1, p$뿐이면 p를 **소수**(*prime number*)라고 한다. 정수 $n > 1$이 소수가 아니면 **합성수**(*composite number*)라고 한다.

정의에 따라 $n > 1$이 합성수라는 것은 $n = ab$, $1 < a, b < n$인 정수 a, b가 존재한다는 것과 같다. 가장 작은 소수들은 $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$이다. 2보다 큰 짝수는 2를 약수로 가지므로 2는 유일한 짝수 소수이다.

1은 소수도 합성수도 아니다. 1을 소수에 포함하면 $6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3 = 1 \cdot 1 \cdot 2 \cdot 3$처럼 불필요한 인수의 개수가 끝없이 달라져 소인수분해의 유일성을 말하기 어렵다. 추상대수에서는 곱셈 역원이 있는 원소를 **단위**(*unit*)라고 부르며, 정수의 단위는 $1, -1$이다. 소수와 단위를 분리하는 약속은 계산상의 편의 이상으로 구조적인 의미를 갖는다. 양의 정수는 곱셈에 관하여 단위 1, 소수, 합성수의 세 종류로 나뉘고, 소인수분해에서 단위는 "인수가 하나도 없는 곱"의 값으로만 나타난다.

명제 3.2 (합성수의 작은 소인수) 합성수 $n > 1$은 $\sqrt{n}$ 이하의 소인수를 갖는다.

증명. $n = ab$이고 $1 < a \le b < n$인 정수 a, b를 선택한다. $a^2 \le ab = n$이므로 $a \le \sqrt{n}$이다. a가 소수이면 a가 원하는 소인수이다. a가 합성수이면 a를 더 작은 인수의 곱으로 쓰고, 그 인수가 합성수이면 다시 분해하는 일을 반복한다. 인수는 계속 작아지는 1보다 큰 정수이므로 이 과정은 유한 번 뒤에 끝나고, 끝에서 얻는 인수는 소수이다. 같은 내용을 한 번에 말하면 다음과 같다. a의 1보다 큰 약수 가운데 가장 작은 것을 p라 하자. a 자신이 그러한 약수이므로 p는 존재한다. p에 $1 < d < p$인 약수 d가 있다면 $d \mid p$, $p \mid a$에서 $d \mid a$이므로 p가 가장 작다는 것에 모순이다. 따라서 p는 소수이다. 어느 경우에나 얻은 소수 p는 $p \mid a$, $a \mid n$에서 n의 약수이고 $p \le a \le \sqrt{n}$이다. □

증명의 뒷부분은 1보다 큰 모든 정수가 적어도 하나의 소인수를 갖는다는 사실도 보인다. 명제 3.2의 대우는 소수 판정의 기준이 된다. 정수 $n > 1$이 $\sqrt{n}$ 이하의 어떤 소수로도 나누어지지 않으면 n은 소수이다.

이 명제는 작은 정수의 소수 판정에 직접 쓰인다. 97이 소수인지 확인하려면 $\sqrt{97} < 10$이므로 $2, 3, 5, 7$로만 나누어 보면 충분하다. 실제로 $97 = 2\cdot 48 + 1 = 3\cdot 32 + 1 = 5\cdot 19 + 2 = 7\cdot 13 + 6$이므로 97은 소수이다. 같은 방법으로 91을 조사하면 $\sqrt{91} < 10$이고 $91 = 7\cdot 13$이므로 91은 합성수이다. 반면 큰 정수에 같은 시행 나눗셈(*trial division*)을 적용하면 계산량이 커질 수 있다. 소수의 정의가 간단하다는 사실과 소수 판정의 효율적인 알고리즘이 자동으로 주어진다는 사실은 다르다.

참고 (시행 나눗셈의 비용). 시행 나눗셈은 최악의 경우 $\sqrt{n}$에 가까운 횟수의 나눗셈을 요구한다. n이 십진법으로 k자리이면 $\sqrt{n}$은 대략 $10^{k/2}$이므로 필요한 계산량은 자릿수 k에 대하여 지수적으로 늘어난다. 자릿수의 다항식 시간 안에 소수 여부를 결정하는 알고리즘이 존재한다는 사실은 2002년에 Agrawal, Kayal, Saxena가 증명하였다. 소수 여부를 판정하는 문제와 소인수를 실제로 찾는 문제는 서로 다르며, 뒤의 문제에 대해서는 다항식 시간 알고리즘이 알려져 있지 않다.

3.2 유클리드의 보조정리

보조정리 3.3 (유클리드의 보조정리) 소수 p가 정수의 곱 ab를 나누면 $p \mid a$ 또는 $p \mid b$이다.

증명. $p \nmid a$라 하자. p의 양의 약수는 $1, p$뿐이고 p는 a의 약수가 아니므로 $\gcd(p, a) = 1$이다. 베주 항등식으로 $pu + av = 1$인 정수 u, v가 존재한다. 양변에 b를 곱하면 $pub + abv = b$이다. 왼쪽의 첫째 항은 p의 배수이고 둘째 항은 $p \mid ab$에서 p의 배수이므로 왼쪽은 p로 나누어진다. 따라서 $p \mid b$이다. □

소수 조건을 지우면 명제는 실패한다. $6 \mid 2\cdot 3$이지만 6은 어느 인수도 나누지 않는다. 반면 $p \mid a_1 \cdots a_k$에 보조정리를 반복하면 p가 적어도 한 인수를 나눈다는 결론을 얻는다. 실제로 k에 대한 귀납법을 쓰면, $p \mid (a_1 \cdots a_{k-1})a_k$에서 $p \mid a_k$이거나 $p \mid a_1 \cdots a_{k-1}$이고, 뒤의 경우에는 귀납 가정에 의해 p가 $a_1, \dots, a_{k-1}$ 가운데 하나를 나눈다. 이 형태가 소인수분해의 유일성에 사용된다.

참고 (보조정리의 성질은 소수를 특징짓는다). 정수 $n > 1$이 "$n \mid ab$이면 $n \mid a$ 또는 $n \mid b$"라는 성질을 가지면 n은 소수이다. n이 합성수라면 $n = ab$, $1 < a, b < n$으로 쓸 수 있고, 이때 $n \mid ab$이지만 $0 < a, b < n$이므로 $n \nmid a$, $n \nmid b$이기 때문이다. 따라서 정수에서는 "더 작은 인수로 분해되지 않는다"는 성질과 "곱을 나누면 인수 하나를 나눈다"는 성질이 같은 수를 가리킨다. 일반적인 환에서는 앞의 성질을 가진 원소를 기약원, 뒤의 성질을 가진 원소를 소원이라고 하여 구별하며, 두 개념이 일치하지 않는 환에서는 인수분해의 유일성이 깨진다(제14권 제5장).

역사 (유클리드의 보조정리). 이 보조정리는 Euclid의 『원론』 제7권 명제 30에 해당한다. 『원론』은 최대공약수를 구하는 절차(제7권 명제 1, 2)에서 출발하여 이 명제에 이르며, 이 장의 논리 순서도 그와 같다.

3.3 산술의 기본정리

정리 3.4 (산술의 기본정리) 모든 정수 $n > 1$은 소수들의 곱으로 표현된다. 소인수의 순서를 제외하면 이 표현은 유일하다.

증명. 여기에서 소수 하나도 인수가 하나인 곱으로 본다.

존재는 강한 귀납법으로 보인다. $1 < m < n$인 모든 정수 m이 소수의 곱으로 표현된다고 가정한다. n이 소수이면 자명하다. 합성수이면 $n = ab$, $1 < a, b < n$으로 쓰고 귀납 가정을 두 인수에 적용한다. a와 b의 표현을 이어 쓰면 n의 표현이 된다.

유일성을 위해

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

가 모두 소수의 곱이라고 하자. p_1은 오른쪽의 곱을 나누므로 유클리드의 보조정리에 의해 어떤 q_j를 나눈다. q_j의 양의 약수는 $1, q_j$ 뿐이고 $p_1 > 1$이므로 $p_1 = q_j$이다. 순서를 바꾸어 $j = 1$이라 하고 양변을 p_1로 나누면 $p_2 \cdots p_r = q_2 \cdots q_s$이다. 이 과정을 반복한다. 한쪽의 인수가 먼저 없어지고 다른 쪽에만 인수가 남으면 남은 인수의 곱이 1이 되어야 하지만, 모든 인수가 1보다 크므로 불가능하다. 따라서 $r = s$이고 소인수들과 그 중복 횟수가 같다. □

서로 다른 소수를 $p_1, \ldots, p_r$라 하면 같은 소수를 거듭제곱으로 모아 소인수분해를

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}, \qquad \alpha_j \in \mathbb{N}_{>0} \tag{3.1}$$

로 쓸 수 있다. $p_1 < \cdots < p_r$로 정하면 이 표현은 n에 의해 완전히 결정되며, 이를 n의 **표준분해**라고 한다. $n = 1$은 인수가 없는 곱($r = 0$)에 해당한다.

소수 p가 양의 정수 n의 소인수분해에 나타나는 횟수를 $v_p(n)$으로 쓴다. $p \nmid n$이면 $v_p(n) = 0$이다. 유일성 덕분에 $v_p(n)$은 n만으로 정해지고, $p^k \mid n$을 만족하는 가장 큰 정수 k와 같다. 두 수의 소인수분해를 이어 쓰면 곱의 소인수분해가 되므로

$$v_p(ab) = v_p(a) + v_p(b) \tag{3.2}$$

이다. 이 간단한 식은 나중에 p진 값매김(*p-adic valuation*)으로 일반화된다(제15권 제8장). 여기서는 n이 양의 정수일 때의 뜻만 사용한다. 예를 들어 $360 = 2^3 \cdot 3^2 \cdot 5$에서 $v_2(360) = 3$, $v_3(360) = 2$, $v_5(360) = 1$, $v_7(360) = 0$이다.

참고 (약수 관계의 지수 판정). 양의 정수 a, b에 대하여

$$a \mid b \iff \text{모든 소수 } p \text{에 대하여 } v_p(a) \le v_p(b) \tag{3.3}$$

이다. $b = ac$이면 식 (3.2)에 의해 $v_p(b) = v_p(a) + v_p(c) \ge v_p(a)$이다. 역으로 오른쪽 조건이 성립하면 각 소수 p를 $v_p(b) - v_p(a)$번씩 곱한 양의 정수 c가 $ac = b$를 만족한다.

참고 (음의 정수와 유일성의 의미). 0이 아닌 정수 n은 단위 ± 1과 소수들의 곱으로 $n = \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$와 같이 유일하게 표현된다. 유일성은 당연한 성질이 아니다. 4로 나눈 나머지가 1인 양의 정수 $1, 5, 9, 13, \ldots$ 만으로 이루어진 체계는 곱셈에 대하여 닫혀 있고, 그 안에서 9, 21, 49는 더 작은 원소의 곱으로 분해되지 않는다. 그런데 $441 = 21 \cdot 21 = 9 \cdot 49$이므로 이 체계에서는 분해가 유일하지 않다. 이 체계에는 덧셈이 없어 베주 항등식을 쓸 수 없고, 따라서 유클리드의 보조정리에 해당하는 성질도 성립하지 않는다. $9 \mid 21 \cdot 21$이지만 $9 \nmid 21$이다.

역사 (산술의 기본정리). 소인수분해의 존재와 유일성에 필요한 명제들은 Euclid의 『원론』 제7권과 제9권에 들어 있다. 정리를 지금의 형태로 명시하고 증명한 것은 Gauss의 『산술 연구』(*Disquisitiones Arithmeticae*, 1801)이다.

3.4 약수의 개수와 약수의 합

양의 정수 n의 양의 약수의 개수를 $\tau(n)$, 양의 약수의 합을 $\sigma(n)$으로 쓴다.

명제 3.5 (약수의 개수와 합) $n = \prod_{j=1}^{r} p_j^{\alpha_j}$의 양의 약수의 개수와 합은 각각

$$\tau(n) = \prod_{j=1}^{r} (\alpha_j + 1), \qquad \sigma(n) = \prod_{j=1}^{r} \left(1 + p_j + \cdots + p_j^{\alpha_j}\right) = \prod_{j=1}^{r} \frac{p_j^{\alpha_j+1} - 1}{p_j - 1} \tag{3.4}$$

이다.

증명. 식 (3.3)에 의해 양의 약수는 $d = \prod_j p_j^{\beta_j}$, $0 \le \beta_j \le \alpha_j$와 정확히 대응한다. 소인수분해의 유일성에 의해 지수의 조 $(\beta_1, \ldots, \beta_r)$가 다르면 약수도 다르다. 각 지수의 선택은 독립적이고 β_j가 가질 수 있는 값은 $\alpha_j + 1$가지이므로, 선택 수를 곱하면 약수의 개수를 얻는다. 곱 $\prod_j (1 + p_j + \cdots + p_j^{\alpha_j})$를 전개하면 각 괄호에서 한 항씩 골라 곱한 $p_1^{\beta_1} \cdots p_r^{\beta_r}$가 정확히 한 번씩 나타난다. 따라서 약수를 모두 더하는 것은 각 지수의 가능한 항을 담은 다항식들의 곱을 전개하는 것과 같고, 두 번째 식을 얻는다. 마지막 등식은 유한 등비급수의 공식 $1 + x + \cdots + x^{\alpha} = (x^{\alpha+1} - 1)/(x - 1)$ $(x \ne 1)$이다. $\square$

예제 3.6 $360 = 2^3 \cdot 3^2 \cdot 5$이므로 양의 약수는 $(3+1)(2+1)(1+1) = 24$개이다. 약수의 합은

$$(1 + 2 + 4 + 8)(1 + 3 + 9)(1 + 5) = 15 \cdot 13 \cdot 6 = 1170$$

이다. 이 계산은 약수를 하나씩 열거할 때 생길 수 있는 누락을 피한다.

참고 (곱셈적 함수). m, n이 서로소이면 두 수의 소인수가 겹치지 않으므로 식 (3.4)에서 $\tau(mn) = \tau(m)\tau(n)$, $\sigma(mn) = \sigma(m)\sigma(n)$이다. 서로소라는 조건은 뺄 수 없다. $\tau(4) = 3$이지만 $\tau(2)\tau(2) = 4$이다. 이러한 성질을 가진 함수를 곱셈적 함수라고 하며 제15권 제3장에서 체계적으로 다룬다. $\sigma(n) = 2n$인 양의 정수를 완전수라고 한다. $\sigma(6) = 12$, $\sigma(28) = 56$이므로 6과 28은 완전수이다.

최대공약수와 최소공배수도 소수별 지수로 표현된다. 양의 정수 a, b와 모든 소수 p에 대하여

$$v_p(\gcd(a,b)) = \min\bigl(v_p(a), v_p(b)\bigr), \qquad v_p(\operatorname{lcm}(a,b)) = \max\bigl(v_p(a), v_p(b)\bigr) \tag{3.5}$$

이다. 실제로 식 (3.3)에 의해 e가 a, b의 공약수라는 것은 모든 p에 대해 $v_p(e) \le \min(v_p(a), v_p(b))$라는 것과 같으므로, 가장 큰 공약수는 각 지수가 최솟값인 수이다. 공배수에 대해서도 부등호의 방향을 바꾸어 같은 논증이 성립한다. 최솟값과 최댓값의 합이 두 값의 합과 같으므로 $\gcd(a,b)\,\operatorname{lcm}(a,b) = ab$를 다른 관점에서 검산할 수 있다. 예를 들어 $252 = 2^2 \cdot 3^2 \cdot 7$, $198 = 2 \cdot 3^2 \cdot 11$에서

$$\gcd(252, 198) = 2 \cdot 3^2 = 18, \qquad \operatorname{lcm}(252, 198) = 2^2 \cdot 3^2 \cdot 7 \cdot 11 = 2772$$

이고 $18 \cdot 2772 = 49896 = 252 \cdot 198$이다. 이 방법은 두 수의 소인수분해를 알 때에만 쓸 수 있다. 소인수분해를 모르는 큰 수의 최대공약수는 유클리드 알고리즘으로 구한다(제1권 제2장).

3.5 소수는 무한히 많다

정리 3.7 (소수의 무한성) 소수는 무한히 많다.

증명. 소수가 유한히 많아 전부 $p_1, \dots, p_r$ 라고 가정하자. $N = p_1 \cdots p_r + 1 > 1$은 어떤 소수 q로 나누어진다. 그러나 N을 각 p_j로 나누면 나머지가 1이므로 q는 그 목록에 속하지 않는다. 모든 소수를 적었다는 가정과 모순이다. □

흔한 오류 ($p_1 \cdots p_r + 1$은 소수일 필요가 없다). 이 증명은 $p_1 \cdots p_r + 1$ 자체가 반드시 소수라고 주장하지 않는다. 그 수를 나누는 소수가 기존 목록 밖에 있다는 것만 필요하다. 예를 들어 $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$는 합성수이다.

증명의 논증은 모순을 쓰지 않고도 읽을 수 있다. 소수의 유한한 목록이 어떤 것이든 그 목록에 없는 소수가 하나 더 있다는 것이 논증의 내용이다.

무한히 많다는 사실은 소수가 일정한 간격으로 나타난다는 뜻도 아니다. 임의의 양의 정수 m에 대해

$$(m+1)!+2, \quad (m+1)!+3, \quad \dots, \quad (m+1)!+(m+1)$$

은 각각 $2, 3, \dots, m+1$로 나누어지고 그 약수보다 크므로 연속된 m개의 합성수를 만든다. $m = 5$이면 $722, 723, 724, 725, 726$이 차례로 $2, 3, 4, 5, 6$의 배수이다. 따라서 소수 사이의 간격에는 임의로 긴 경우가 존재한다. 이 구성은 존재를 보일 뿐 가장 먼저 나타나는 위치를 주지는 않는다. 연속된 다섯 합성수는 이미 $24, 25, 26, 27, 28$에서 나타난다. 한편 작은 간격이 얼마나 자주 나타나는지는 훨씬 깊은 정수론 문제이다.

역사 (소수의 무한성과 분포). 정리 3.7과 그 증명은 Euclid의 『원론』 제9권 명제 20에 실려 있다. N 이하의 소수의 개수를 $\pi(N)$이라 하면 N이 커질 때 $\pi(N)$과 $N/\ln N$의 비가 1로 수렴한다. 이 소수 정리는 1896년에 Hadamard와 de la Vallée Poussin이 서로 독립적으로 증명하였다(제15권 제5장). 예를 들어 $\pi(10^6) = 78498$이고 $10^6/\ln 10^6 \approx 72382$이다. 차가 2인 소수의 쌍이 무한히 많다는 쌍둥이 소수 추측은 증명되지 않았다. Zhang은 2013년에 차가 7×10^7 이하인 소수의 쌍이 무한히 많음을 증명하였고, 이 한계는 그 뒤의 공동 연구로 246까지 낮아졌다(제28권 제2장).

3.6 체로 소수 목록 만들기

에라토스테네스의 체(*sieve of Eratosthenes*)는 주어진 상한 N 이하의 소수를 모두 찾는 방법이다.

방법 (에라토스테네스의 체).

1단계. 2부터 N까지의 정수를 나열한다.

2단계. 아직 지워지지 않았고 소수로 선택되지도 않은 가장 작은 수 p를 소수로 선택한다.

3단계. p 자신을 제외한 p의 배수를 p^2부터 차례로 지운다. 곧 $p^2,\ p^2+p,\ p^2+2p,\ \dots$ 가운데 N 이하인 수를 지운다.

4단계. $p^2 > N$이 될 때까지 2단계와 3단계를 반복한다. 그때 남은 수는 모두 소수이다.

p^2보다 작은 p의 배수 kp $(2 \le k < p)$는 k의 소인수, 곧 p보다 작은 소수의 배수로서 이미 지워졌으므로 p^2부터 시작해도 된다. 2단계에서 선택한 수가 실제로 소수인 까닭은, 그 수가 합성수라면 자신보다 작은 소인수를 갖고 그 소인수의 배수로서 이미 지워졌어야 하기 때문이다. 이 알고리즘의 정당성은 "모든 합성수는 제곱근 이하의 소인수를 갖는다"는 명제 3.2로 보장된다. N 이하의 합성수는 $\sqrt{N}$ 이하의 소인수를 가지므로 $p^2 > N$이 되기 전에 지워진다.

$N = 50$이면 $7^2 = 49 \le 50 < 11^2$이므로 $p = 2, 3, 5, 7$의 네 번으로 끝난다. $p = 2$에서 4 이상의 짝수가, $p = 3$에서 $9, 15, 21, 27, 33, 39, 45$가, $p = 5$에서 $25, 35$가, $p = 7$에서 49가 새로 지워진다. 남는 수는

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47$$

의 15개이고, 이것이 50 이하의 소수 전부이다.

목록을 만드는 문제와 하나의 거대한 수가 소수인지 판정하는 문제는 서로 다르다. 체는 N 이하의 수를 모두 기억해야 하므로 N에 비례하는 기억 공간이 필요하다. 자릿수가 수백 개인 수 하나의 소수 여부를 묻는 문제에는 체를 쓸 수 없고 다른 판정법이 필요하다. 실제 계산에서는 문제의 형태에 따라 알고리즘을 골라야 한다.

역사 (에라토스테네스의 체). 이 방법은 기원전 3세기의 Eratosthenes에게서 비롯된 것으로 전하며, Nicomachus의 『산술 입문』에 그의 이름과 함께 기록되어 있다.

핵심 수식

$$p \mid ab \implies p \mid a \text{ 또는 } p \mid b \quad (p\text{는 소수}), \qquad n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \quad (\text{순서를 제외하고 유일}),$$

$$v_p(ab) = v_p(a) + v_p(b), \qquad a \mid b \iff v_p(a) \le v_p(b) \ \ (\text{모든 소수 } p),$$

$$\tau(n) = \prod_{j=1}^{r} (\alpha_j + 1), \qquad \sigma(n) = \prod_{j=1}^{r} \frac{p_j^{\alpha_j+1} - 1}{p_j - 1},$$

$$v_p(\gcd(a,b)) = \min\bigl(v_p(a), v_p(b)\bigr), \qquad v_p(\operatorname{lcm}(a,b)) = \max\bigl(v_p(a), v_p(b)\bigr).$$

3.7 문제와 풀이

연습문제 3.8 756의 소인수분해, 양의 약수의 개수, 양의 약수의 합을 구하여라.

풀이. $756 = 2 \cdot 378 = 2^2 \cdot 189 = 2^2 \cdot 3^3 \cdot 7$이다. 따라서 양의 약수의 개수는 $3 \cdot 4 \cdot 2 = 24$이고, 합은

$$(1 + 2 + 4)(1 + 3 + 9 + 27)(1 + 7) = 7 \cdot 40 \cdot 8 = 2240$$

이다.

연습문제 3.9 양의 정수 n이 완전제곱수일 필요충분조건이 모든 소인수의 지수가 짝수인 것임을 보여라.

풀이. $n = m^2$이면 식 (3.2)에 의해 모든 소수 p에 대하여 $v_p(n) = 2v_p(m)$이다. 곧 제곱하면 각 지수가 두 배가 되고, 소인수분해의 유일성에 의해 이것이 n의 지수이므로 모두 짝수이다. 역으로 모든 지수가 짝수여서 $n = \prod_j p_j^{2\beta_j}$이면 지수를 절반으로 줄인 정수 $m = \prod_j p_j^{\beta_j}$가 $m^2 = n$을 만족한다. $n = 1$은 소인수가 없는 경우로서 $1 = 1^2$이다.

연습문제 3.10 양의 약수의 개수가 홀수인 양의 정수는 정확히 완전제곱수임을 보여라.

풀이. 약수의 개수 $\prod_j (\alpha_j + 1)$이 홀수일 조건은 모든 인수 $\alpha_j + 1$이 홀수인 것, 곧 모든 α_j가 짝수인 것이다. 연습문제 3.9에 의해 이는 완전제곱수 조건과 같다. 약수를 d와 n/d로 짝지어 보아도 같은 결론을 얻는다. $d \neq n/d$인 약수는 둘씩 짝을 이루므로, 개수가 홀수이려면 $d = n/d$, 곧 $d^2 = n$인 약수가 있어야 한다.

연습문제 3.11 정수 $n \geq 2$에 대하여 $n! + 1$이 $2, 3, \ldots, n$ 중 어느 수로도 나누어지지 않음을 보여라.

풀이. $2 \leq k \leq n$이면 $k \mid n!$이므로 $n! + 1$을 k로 나눈 나머지는 1이다. 따라서 $n! + 1$의 소인수는 모두 n보다 크지만, $n! + 1$ 자체가 소수일 필요는 없다. $4! + 1 = 25 = 5^2$와 $5! + 1 = 121 = 11^2$가 그 예이다. 이 논증은 임의의 n보다 큰 소수가 존재함을 보이므로 정리 3.7의 또 다른 증명이 된다.

연습문제 3.12 221과 223이 소수인지 판정하여라.

풀이. $15^2 = 225$이므로 두 수 모두 $\sqrt{n} < 15$이고, 소수 $2, 3, 5, 7, 11, 13$으로만 나누어 보면 충분하다. $221 = 13 \cdot 17$이므로 221은 합성수이다. 223은 홀수이고, 자릿수의 합 7이 3의 배수가 아니며, 끝자리가 0이나 5가 아니다. 또 $223 = 7 \cdot 31 + 6 = 11 \cdot 20 + 3 = 13 \cdot 17 + 2$이므로 여섯 소수 어느 것으로도 나누어지지 않는다. 명제 3.2에 의해 223은 소수이다.

연습문제 3.13 $100!$을 십진법으로 썼을 때 끝에 이어지는 0의 개수를 구하여라.

풀이. 끝에 이어지는 0의 개수는 $10^k \mid 100!$인 가장 큰 k이고, 식 (3.3)에 의해 이는 $v_2(100!)$과 $v_5(100!)$ 가운데 작은 값이다. 1부터 100까지의 수 가운데 5의 배수는 20개이고, 그중 25의 배수 4개는 5를 한 번씩 더 포함하며, 125의 배수는 없다. 식 (3.2)에 의해 $v_5(100!) = 20 + 4 = 24$이다. 같은 방법으로 $v_2(100!) = 50 + 25 + 12 + 6 + 3 + 1 = 97$이다. 따라서 끝에 이어지는 0은 24개이다. 일반적으로 $v_p(n!) = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \cdots$이며, 이를 Legendre 공식이라고 한다.

참고 (다음 연결). 소인수의 지수는 유한소수의 판정(제1권 제4장)과 $\sqrt{2}$가 유리수가 아니라는 증명(제1권 제6장)에 쓰인다. 소수를 법으로 하는 합동식은 제1권 제9장와 제15권 제1장에서, 유일한 인수분해가 성립하는 환의 일반론은 제14권 제5장에서 다룬다.

제 4 장

분수, 유리수, 소수 표현

개요 유리수는 정수 a와 0이 아닌 정수 b의 몫 a/b로 나타낼 수 있는 수이고, 분수는 그 수를 적는 표기이다. 이 장은 한 유리수를 나타내는 여러 분수 가운데 기약분수가 유일함을 증명하고, 분수의 사칙연산과 약분·크기 비교의 규칙, 비율과 백분율의 기준량 문제를 정리한다. 이어서 유리수의 십진 소수 표현을 다룬다. 기약분수가 유한소수가 되는 조건, 유리수와 순환소수의 동치, $0.999\ldots = 1$의 뜻, 유리수의 조밀성이 그 내용이다. 이 장에서 '소수'는 소수점 아래 자리를 가진 표기(*decimal*)를 가리키며, 앞 장의 소수(*prime number*)와 구별하기 위하여 후자는 '소인수'라는 말로만 쓴다. 선행 지식: 최대공약수와 소인수분해(제1권 제2장, 제1권 제3장).

4.1 분수의 동치와 기약분수

유리수(*rational number*)는 정수 a와 0이 아닌 정수 b를 이용해 a/b로 표현할 수 있는 수이다. 표기 a/b를 **분수**라고 하고 a를 **분자**, b를 **분모**라고 한다. 유리수 전체의 집합을 $\mathbb{Q}$로 쓴다. 정수 a는 $a/1$로 표현되므로 유리수이다. 두 분수가 같은 수를 나타낼 조건은

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc \qquad (b, d \neq 0) \tag{4.1}$$

이다. 양변에 $bd \neq 0$을 곱하거나 나누면 두 조건이 서로 바뀐다. 특히 0이 아닌 정수 k에 대하여 $a/b = (ka)/(kb)$이고, 분자와 분모를 공통인수로 나누는 **약분**은 이 등식을 오른쪽에서 왼쪽으로 읽은 것이다. 같은 수에 여러 분수 표현이 있으므로 표준 형태를 정해 두면 비교하기 편하다. 분모를 양수로 만들고 분자와 분모를 최대공약수로 나누면 **기약분수**를 얻는다.

> **정리 4.1 (기약분수의 유일성)** 모든 유리수는 $b > 0$, $\gcd(|a|, b) = 1$을 만족하는 기약분수 a/b로 유일하게 표현된다.

증명. 존재. 유리수를 a_0/b_0 $(b_0 \neq 0)$로 쓴다. $b_0 < 0$이면 분자와 분모에 -1을 곱하여 분모의 부호를 정리하므로 $b_0 > 0$이라 해도 된다. $g = \gcd(|a_0|, b_0)$로 놓고 $a_0 = ga$, $b_0 = gb$로 쓰면 $a_0/b_0 = a/b$, $b > 0$이고, 최대공약수로 나눈 두 수는 서로소이므로(제1권 제2장) $\gcd(|a|, b) = 1$이다.

유일성. 두 기약분수 $a/b = c/d$가 같으면 식 (4.1)에 의해 $ad = bc$이다. $b \mid ad$이고 a, b가 서로소이므로 $b \mid d$이다. 여기에는 서로소인 수가 곱을 나누면 나머지 인수를 나눈다는 제1권 제2장의 결과를 썼다. 같은 이유로 $d \mid bc$와 $\gcd(c, d) = 1$에서 $d \mid b$이다. 두 분모가 양수이므로 $b = d$, 이어서 $ad = bc$를 $b \neq 0$으로 나누어 $a = c$이다. 0의 기약분수는 $0/1$이다. $\gcd(0, b) = b$이므로 서로소 조건이 $b = 1$을 요구하기 때문이다. □

> **예제 4.2** $-84/126$에서 $\gcd(84, 126) = 42$이므로 기약분수는 $-2/3$이다. 부호를 분모에 두어 $2/(-3)$로 써도 값은 같지만, 분모가 양수라는 표준 형태를 지키면 크기 비교에서 부등호 방향을 덜 혼동한다.

참고 (동치류로서의 유리수). 식 (4.1)는 $b \neq 0$인 정수의 순서쌍 (a,b) 사이의 동치관계 $(a,b) \sim (c,d) \iff ad = bc$를 정한다. 유리수를 정수로부터 엄밀하게 구성할 때에는 이 관계의 동치류 하나하나를 유리수로 정의한다(제5권 제3장). 정리 4.1은 각 동치류에서 대표를 정확히 하나씩 고르는 규칙을 준다.

4.2 사칙연산과 약분의 범위

분수의 연산은

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \qquad \frac{a/b}{c/d} = \frac{ad}{bc} \tag{4.2}$$

로 정의된다. 첫 두 식에서 $b, d \neq 0$이고, 마지막 식에는 $c \neq 0$도 필요하다. 뺄셈은 c를 $-c$로 바꾼 덧셈이다. 이 정의는 분수의 표현을 바꾸어도 결과가 같은 수가 되도록 정해져 있다. 예를 들어 a/b를 $(ka)/(kb)$로 바꾸면 합은 $(kad + kbc)/(kbd)$가 되어 분자와 분모에 같은 k가 곱해질 뿐이다.

덧셈 공식의 분모 bd 대신 최소공배수 $\operatorname{lcm}(b,d)$를 공통분모로 써도 같은 수를 얻는다. 1/6+1/10을 공식대로 계산하면 16/60이고 공통분모 30을 쓰면 $5/30 + 3/30 = 8/30$이며, 둘 다 기약분수 4/15와 같다. 어느 쪽이든 결과가 기약분수라는 보장은 없으므로 마지막에 약분 여부를 확인한다.

분수식의 일부를 약분할 때에는 곱의 공통인수만 없앨 수 있다.

$$\frac{a(b+c)}{a} = b + c \quad (a \neq 0), \qquad \frac{a+b}{a} \neq b \quad (\text{일반적으로}). \tag{4.3}$$

두 번째 식의 왼쪽은 $1 + b/a$이다. 분자 전체의 합과 한 항을 혼동하면 약분 오류가 생긴다.

흔한 오류 (합의 한 항을 약분하는 오류). $(2+6)/2$에서 2를 지워 6이라고 하면 틀린다. 올바른 값은 $8/2 = 4 = 1 + 6/2$이다. 잘못된 약분이 우연히 맞는 값을 줄 수도 있다. $a = b = 2$이면 $(a+b)/a = 2 = b$이다. $(a+b)/a = b$는 $a + b = ab$일 때에만 성립하므로, 한 번 맞았다는 사실이 규칙을 정당화하지 않는다.

> **예제 4.3** $\dfrac{14}{45} \cdot \dfrac{15}{28}$는 곱셈을 하기 전에 14와 28, 15와 45를 약분하여
>
> $$\frac{14}{45} \cdot \frac{15}{28} = \frac{14 \cdot 15}{28 \cdot 45} = \frac{14}{28} \cdot \frac{15}{45} = \frac{1}{2} \cdot \frac{1}{3} = \frac{1}{6}$$
>
> 로 구할 수 있다. 이는 분자와 분모의 인수 배열을 교환법칙으로 바꾸어 공통인수를 제거한 것이다.

분모가 양수인 두 분수의 크기 비교에서는 교차곱을 사용할 수 있다.

$$\frac{a}{b} < \frac{c}{d} \iff ad < bc \qquad (b, d > 0). \tag{4.4}$$

양수 bd를 양변에 곱해도 부등호의 방향이 유지되기 때문이다(제1권 제5장). 분모의 부호를 확인하지 않고 양변에 분모의 곱을 곱하면 부등호 방향을 잘못 유지할 수 있다. 예를 들어 $1/(-2) < 1/3$은 참이지만 교차곱 $3 < -2$는 거짓이다. 이 경우 $bd = -6 < 0$을 곱하였으므로 부등호가 뒤집혀야 한다.

4.3 비율, 비례, 백분율

비율은 기준량에 대한 비교량의 몫이고, **백분율**은 비율에 100을 곱하여 %로 나타낸 것이다. 어떤 양이 x_0에서 x_1로 바뀔 때의 변화율은 처음 값을 기준량으로 하여

$$\frac{x_1 - x_0}{x_0} \qquad (x_0 \neq 0) \tag{4.5}$$

으로 정한다. 기준량이 달라지면 같은 차이도 다른 비율이 된다. 100에서 120으로 늘어난 증가는 20%이지만, 120에서 100으로 줄어든 감소는 $20/120 = 1/6$, 즉 약 16.67%이다. 두 변화량의 절댓값이 같아도 분모가 다르기 때문이다.

> **예제 4.4** 어떤 양을 20% 늘린 다음 다시 20% 줄이면 원래 값으로 돌아오지 않는다. 원래 값을 x라 하면 최종 값은 $1.2 \cdot 0.8\,x = 0.96x$이다. 일반적으로 비율 r만큼 늘리고 같은 비율로 줄이면 $(1+r)(1-r)x = (1-r^2)x$이다.

비율 r만큼 늘린 양 $(1+r)x$를 원래 값 x로 되돌리려면 늘어난 값을 기준으로 $r/(1+r)$만큼 줄여야 한다. $1 - r/(1+r) = 1/(1+r)$이기 때문이다. $r = 0.2$이면 이 비율은 $1/6$이며 위의 계산과 일치한다.

주의 (퍼센트와 퍼센트포인트). 백분율로 표시된 두 값의 차는 **퍼센트포인트**로 말한다. 어떤 비율이 2%에서 3%로 바뀌면 차는 1퍼센트포인트이고, 식 (4.5)의 변화율은 $(3-2)/2 = 50\%$이다. "1% 올랐다"는 말이 둘 중 무엇을 뜻하는지는 기준량을 밝혀야 정해진다.

비례 $y = kx$와 일차관계 $y = kx + b$도 다르다. 비례에서는 x를 두 배로 하면 y도 두 배가 되고 그래프가 원점을 지난다. 일정한 기본요금이 추가되는 요금 체계는 일차관계일 수 있지만 엄밀한 의미의 비례는 아니다. 기본요금이 b, 단위 사용량당 요금이 k이면 사용량 x와 $2x$의 요금은 $kx+b$와 $2kx+b$이고, 뒤의 값은 $b = 0$일 때에만 앞의 값의 두 배이다. 일상어의 "비례한다"를 수학적 진술로 옮길 때에는 절편이 있는지 확인한다.

4.4 유한소수의 판정

소수점 아래 유한 개의 자리만으로 적을 수 있는 수, 곧 어떤 정수 A와 자연수 m에 대하여 $A/10^m$ 꼴인 수를 십진법의 **유한소수**라고 한다.

> **정리 4.5 (유한소수의 판정)** 기약분수 a/b에서 $b > 0$일 때 십진법 유한소수로 표현될 필요충분조건은 b의 소인수가 2와 5뿐인 것이다. $b = 1$도 포함한다.

증명. 유한소수이면 어떤 자연수 m과 정수 A에 대해 $a/b = A/10^m$이다. 그러면 $10^m a = Ab$에서 $b \mid 10^m a$이고 a, b가 서로소이므로 $b \mid 10^m$이다. $10^m = 2^m 5^m$이므로 b의 소인수는 2, 5뿐이다. 역으로 $b = 2^u 5^v$이면 $m = \max(u, v)$를 택해 분자와 분모에 $2^{m-u}5^{m-v}$를 곱한다. 분모가 10^m이 되므로 유한소수가 된다. □

> **예제 4.6** $7/40$은 분모가 $2^3 \cdot 5$이므로 유한소수이며 $7/40 = 175/1000 = 0.175$이다. $7/30$은 분모에 3이 있으므로 유한소수가 아니다. 단, 먼저 기약분수로 만들어야 한다. $3/6$의 분모에는 3이 보이지만 기약분수 $1/2$는 유한소수이다.

참고 (필요한 자릿수). 증명에서 선택한 $m = \max(u, v)$는 가능한 가장 작은 값이다. $b = 2^u 5^v$가 10^m을 나누려면 $u \le m$, $v \le m$이어야 하기 때문이다. 따라서 분모가 $2^u 5^v$인 기약분수는 소수점 아래 정확히 $\max(u, v)$자리에서 끝난다. $7/40$은 $\max(3, 1) = 3$자리, $13/80$은 $\max(4, 1) = 4$자리이다.

일반적인 β진법($\beta \ge 2$)에서도 같은 논리가 성립한다. 기약분수의 분모가 어떤 β^m을 나누면, 그리고 그 경우에만 유한한 β진 소수 표현을 갖는다. 따라서 허용되는 소인수는 기수 β를 나누는 소인수들이다(제1권 제1장). $1/3$은 십진법에서 유한소수가 아니지만 삼진법에서는 $(0.1)_3$이고, $1/10$은 분모에 소인수 5가 있으므로 이진법에서 유한하게 표현되지 않는다. 유한소수인지 아닌지는 수의 성질이 아니라 수와 기수의 관계이다.

4.5 순환소수와 유리수의 동치

십진 표현에서 어느 자리 이후로 같은 숫자열이 끝없이 되풀이되는 소수를 **순환소수**라고 하고, 되풀이되는 가장 짧은 숫자열을 **순환마디**라고 한다. 순환마디는 윗줄로 표시한다. 예를 들어 $0.1363636\ldots = 0.1\overline{36}$이다. 유한소수는 순환마디가 0인 경우로 볼 수 있다.

분수를 소수로 바꾸는 긴 나눗셈에서는 나머지에 10을 곱하여 다시 분모로 나누는 일을 되풀이한다. $3/7$의 경우 나머지 3에서 출발하여

$$30 = 4\cdot 7 + 2,\qquad 20 = 2\cdot 7 + 6,\qquad 60 = 8\cdot 7 + 4,$$
$$40 = 5\cdot 7 + 5,\qquad 50 = 7\cdot 7 + 1,\qquad 10 = 1\cdot 7 + 3$$

이고, 여섯 번째 단계에서 처음의 나머지 3이 다시 나타난다. 몫을 차례로 읽으면 $3/7 = 0.\overline{428571}$이다.

> **정리 4.7 (유리수와 순환소수)** 실수의 십진 표현이 어느 자리 이후부터 주기적으로 반복되거나 유한하게 끝나면 그 수는 유리수이다. 역으로 모든 유리수의 십진 표현은 이 두 형태 중 하나이다.

증명. 뒤의 주장부터 보인다. 음수는 부호를 떼어 생각하면 되므로 유리수 a/b에서 $a \ge 0$, $b > 0$이라 하자. 긴 나눗셈은 $a = bq_0 + r_0$으로 정수 부분 q_0과 나머지 r_0을 구한 뒤, $k \ge 1$에 대하여

$$10\,r_{k-1} = b\,d_k + r_k,\qquad 0 \le r_k < b$$

로 소수점 아래 k번째 숫자 d_k와 다음 나머지 r_k를 정하는 절차이다. $0 \le 10r_{k-1} < 10b$이므로 d_k는 0부터 9까지의 숫자이고, 각 단계의 나머지는 $0, 1, \ldots, b-1$ 중 하나이다. 나머지가 0이면 그 뒤의 숫자는 모두 0이므로 표현이 끝난다. 끝나지 않으면 나머지 $r_0, r_1, \ldots, r_{b-1}$의 b개는 $1, \ldots, b-1$의 $b-1$가지 값만 가질 수 있으므로 그중 둘이 같다. 숫자 d_{k+1}과 나머지 r_{k+1}은 r_k만으로 정해지므로, 같은 나머지 뒤의 계산은 동일하고 이후 숫자열이 반복된다.

앞의 주장을 보인다. 유한하게 끝나는 표현은 $A/10^m$ 꼴이므로 유리수이다. 소수점 아래 s자리 이후 길이 t의 주기가 시작한다고 하고 원래 수를 x라 하자. $10^{s+t}x$와 $10^s x$는 소수점 아래의 숫자열이 같으므로 $10^{s+t}x - 10^s x$에서 반복 꼬리가 상쇄되어 정수 M이 된다. 따라서

$$x = \frac{M}{10^s(10^t - 1)}$$

는 정수와 $10^{s}(10^{t}-1)$의 몫이다. $\square$

> **예제 4.8** $x = 0.1\overline{36} = 0.1363636\ldots$라 하자. $1000x = 136.3636\ldots$, $10x = 1.3636\ldots$이므로 $990x = 135$이다. 따라서 $x = 135/990 = 3/22$이다. 반복 부분만 보고 $136/999$로 쓰면 반복이 시작되는 위치를 놓친 것이다. $136/999 = 0.\overline{136}$은 다른 수이다.

참고 (순환마디의 길이와 무리수). 증명에서 서로 다른 0이 아닌 나머지는 많아야 $b-1$가지이므로, 분모가 b인 분수의 순환마디의 길이는 $b-1$ 이하이다. $3/7$은 이 상한에 도달하는 예이고, $1/3 = 0.\overline{3}$과 $1/11 = 0.\overline{09}$는 그보다 훨씬 짧은 예이다. 분모가 10과 서로소일 때 순환마디의 길이는 $10^{t}-1$이 분모로 나누어지는 가장 작은 양의 정수 t이며, 이 수는 합동식의 위수로 설명된다(제15권 제1장). 정리 4.7의 대우에 의해 끝나지도 않고 순환하지도 않는 십진 표현은 유리수가 아닌 수를 나타낸다. 1 사이에 놓이는 0의 개수가 하나씩 늘어나는 $0.101001000100001\ldots$이 그 예이다(제1권 제6장).

4.6 왜 $0.999\ldots = 1$인가

무한소수는 끝없이 긴 유한한 문자열이라는 막연한 대상이 아니라, 유한한 부분합의 극한으로 해석한다. 곧 $0.d_1d_2d_3\ldots$은 수열 $\sum_{k=1}^{n} d_k/10^{k}$ $(n=1,2,\ldots)$의 극한을 가리키는 표기이다. n자리까지 9를 쓴 수는

$$s_n = \sum_{k=1}^{n} \frac{9}{10^{k}} = 1 - 10^{-n} \tag{4.6}$$

이다. $10^{-n} \to 0$이므로 이 수열의 극한은 1이다. 따라서 $0.999\ldots = 1$이다. 두 수 사이에 "아주 작은 양의 틈" $\varepsilon > 0$이 있다고 생각하면, 그 틈보다 작은 10^{-n}을 선택할 수 있다는 성질과 모순된다. 모든 n에 대하여 $1 - s_n = 10^{-n}$이 ε 이상이어야 하기 때문이다.

이 현상은 실수의 값이 모호하다는 뜻이 아니라 표현이 유일하지 않을 수 있다는 뜻이다. 0이 아닌 유한소수는 마지막 비영 숫자를 하나 줄이고 그 뒤를 9로 채운 표현을 갖는다. 예를 들어 $0.25000\ldots = 0.24999\ldots$이다. 십진 표현이 둘인 실수는 0이 아닌 유한소수뿐이고, 그 밖의 실수는 표현이 하나뿐이다. 십진 표현의 유일성을 원하면 끝없이 9가 이어지는 표현을 제외한다는 약속을 덧붙인다.

참고 (극한이 존재한다는 전제). $x = 0.999\ldots$로 놓고 $10x - x = 9$에서 $x = 1$을 얻는 계산이나 $1/3 = 0.333\ldots$의 양변에 3을 곱하는 계산은 무한소수가 하나의 실수를 나타내고 그 위에서 사칙연산을 자리별로 할 수 있다는 사실을 전제한다. 그 전제의 근거가 식 (4.6)과 같은 부분합의 극한이다. 모든 무한소수의 부분합이 수렴한다는 사실은 실수의 완비성에서 나온다(제1권 제6장). 일반적인 등비급수의 합은 제8권 제6장에서 다룬다.

4.7 유리수의 조밀성

> **명제 4.9 (유리수 사이의 유리수)** 서로 다른 두 유리수 $a < b$ 사이에는 유리수가 무한히 많다.

증명. 중점 $(a+b)/2$는 유리수이고 두 수 사이에 있다. $a < b$의 양변에 a 또는 b를 더하고 2로 나누면 $a < (a+b)/2 < b$이기 때문이다. a와 이 중점 사이에 다시 중점을 만들고 반복하면 서로

다른 유리수를 끝없이 얻는다. 구체적으로 k 번째로 얻는 수는 $a + (b-a)/2^k$ 이고, 이들은 k 가 커질수록 엄격히 작아지면서 모두 a 와 b 사이에 있다. $\square$

이 성질 때문에 유리수에는 "바로 다음 수"가 없다. 정수에서는 n 다음 수가 $n+1$ 이지만, 어떤 유리수보다 큰 유리수 가운데 가장 작은 것은 존재하지 않는다.

더 강하게, 임의의 서로 다른 두 실수 사이에도 유리수가 존재한다. 이 명제는 실수의 아르키메데스 성질(*Archimedean property*)을 이용해 제1권 제6장에서 증명한다. 그러나 유리수가 조밀하다는 사실은 유리수만으로 실수의 모든 점을 표현할 수 있다는 뜻이 아니다. $\sqrt{2}$는 유리수들로 임의로 가깝게 근사할 수 있지만 그 자체는 유리수가 아니다. 조밀성과 집합의 동일성은 구별해야 한다.

핵심 수식

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc, \qquad \frac{a}{b} < \frac{c}{d} \iff ad < bc \quad (b,d>0),$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \qquad \frac{a}{b}\cdot\frac{c}{d} = \frac{ac}{bd}, \qquad \frac{a/b}{c/d} = \frac{ad}{bc} \quad (c \neq 0),$$

$$\text{기약분수 } \frac{a}{b} \text{가 유한소수} \iff b = 2^u 5^v, \qquad 0.999\ldots = \lim_{n\to\infty}\left(1 - 10^{-n}\right) = 1.$$

4.8 문제와 풀이

연습문제 4.10 $13/80$ 이 유한소수인지 판정하고 값을 구하여라.

풀이. $13/80$ 은 기약분수이고 $80 = 2^4 \cdot 5$ 이므로 유한소수이다. 분자와 분모에 $5^3 = 125$ 를 곱하여 분모를 10000 으로 만들면 $13/80 = 1625/10000 = 0.1625$ 이다.

연습문제 4.11 $0.\overline{27}$ 과 $0.2\overline{7}$ 을 각각 분수로 바꾸어라.

풀이. 첫 수 x 는 $100x - x = 27$ 이므로 $x = 27/99 = 3/11$ 이다. 둘째 수 y 는 $100y - 10y = 27.777\ldots - 2.777\ldots = 25$ 이므로 $y = 25/90 = 5/18$ 이다.

연습문제 4.12 가격을 25% 올린 뒤 원래 가격으로 되돌리려면 인상된 가격에서 몇 퍼센트를 내려야 하는가?

풀이. 원래 가격을 x 라 하면 현재 가격은 $1.25x$ 이다. 줄여야 하는 비율은 인상된 가격을 기준으로 $0.25x/(1.25x) = 1/5 = 20\%$ 이다.

연습문제 4.13 $1/12$ 이 유한하게 표현되는 가장 작은 정수 기수 $\beta \geq 2$ 를 구하여라.

풀이. 분모 $12 = 2^2 \cdot 3$ 의 소인수 $2, 3$ 이 모두 β 를 나누어야 한다. 가장 작은 기수는 $\beta = 6$ 이다. 실제로 $1/12 = 3/36 = (0.03)_6$ 이다.

연습문제 4.14 $7/12$ 을 십진 소수로 나타내고, 순환하지 않는 부분의 길이를 분모의 소인수분해로 설명하여라.

풀이. 긴 나눗셈을 하면 $70 = 5\cdot 12 + 10$, $100 = 8\cdot 12 + 4$, $40 = 3\cdot 12 + 4$이고 이후 나머지 4가 반복되므로 $7/12 = 0.58\overline{3}$이다. 분모는 $12 = 2^2\cdot 3$이다. $100 = 2^2\cdot 5^2$을 곱하면 분모의 2^2이 없어져

$$100\cdot \frac{7}{12} = \frac{175}{3} = 58 + \frac{1}{3} = 58.\overline{3}$$

이 된다. 따라서 소수점을 두 자리 옮긴 뒤부터 순환이 시작되고, 순환하지 않는 부분의 길이는 분모에 들어 있는 2와 5의 지수 가운데 큰 값 2이다.

> **연습문제 4.15** $b, d > 0$이고 $a/b < c/d$이면 $\dfrac{a}{b} < \dfrac{a+c}{b+d} < \dfrac{c}{d}$임을 보여라.

풀이. 가정은 식 (4.4)에 의해 $ad < bc$와 같다. 분모 b, d, $b+d$가 모두 양수이므로 교차곱으로 비교한다. 왼쪽 부등식은 $a(b+d) < b(a+c)$, 곧 $ad < bc$와 동치이고, 오른쪽 부등식은 $(a+c)d < c(b+d)$, 곧 $ad < bc$와 동치이다. 분자끼리, 분모끼리 더한 분수는 두 분수의 합이 아니라 두 분수 사이에 있는 수이다(제1권 제1장).

참고 (다음 연결). 유리수로 채워지지 않는 수직선의 빈자리와 실수의 완비성은 제1권 제6장에서, 소수의 자릿수를 제한할 때 생기는 반올림 오차는 제1권 제8장에서 다룬다. 순환마디의 길이를 결정하는 합동식의 위수는 제1권 제9장와 제15권 제1장의 주제이다.

제 5 장

순서, 절댓값, 기본 부등식

개요 실수의 **순서**(*order*)는 덧셈과 양수의 곱셈에 호환되는 전순서이며, 이 호환성만으로 부등식을 변형하는 모든 규칙이 따라 나온다. 이 장은 부등식을 바꾸는 규칙에서 출발하여 구간의 표기, 절댓값의 정의와 성질, 삼각부등식, 산술평균-기하평균 부등식, 코시-슈바르츠 부등식의 2차원 형태를 차례로 세운다. 이 부등식들은 이후 극한의 ε-논법, 노름과 거리, 최적화 문제에서 오차와 크기를 추정하는 기본 도구로 쓰인다. 실수의 완비성(상한의 존재)은 이 장에서 다루지 않고 다음 장에서 따로 다룬다. 선행 지식: 실수의 사칙연산.

5.1 부등식을 바꾸는 규칙

실수의 순서는 덧셈과 양수의 곱셈에 호환된다. $a < b$이면 모든 실수 c에 대해 $a + c < b + c$이고, $c > 0$이면 $ac < bc$이다. $c < 0$일 때에는 부등호가 뒤집혀 $ac > bc$이다. $c = 0$이면 양변이 모두 0이 되어 등식이 되므로 엄격한 부등호를 유지할 수 없다. 이 세 가지 규칙만으로 일차부등식의 해를 구하는 모든 조작이 설명된다.

> **예제 5.1** $-3x + 5 < 11$에서 양변에서 5를 빼면 $-3x < 6$을 얻는다. 음수 -3으로 나누면 부등호가 뒤집혀 $x > -2$이다. 최종 답의 방향은 처음 계수의 부호와 관련된다. 예를 들어 $x = 0$을 원래 식에 대입하면 $5 < 11$로 참이고, 해집합 바깥의 점 $x = -3$을 대입하면 $14 < 11$로 거짓이므로 방향을 검산할 수 있다.

$0 < a < b$일 때 역수를 취하면 $1/a > 1/b$이다. 양수 ab로 부등식 $a < b$의 양변을 나누면 $a/(ab) < b/(ab)$, 곧 $1/b < 1/a$를 얻어 바로 증명된다. 하지만 $a < 0 < b$처럼 구간이 0을 가로지르면 같은 문장을 무작정 적용할 수 없다.

흔한 오류 (부호가 바뀌는 구간에서의 역수). $a < 0 < b$이면 $1/a < 0 < 1/b$이므로 $1/a < 1/b$이지 $1/a > 1/b$가 아니다. 역수 함수 $x \mapsto 1/x$는 $x = 0$에서 정의되지 않으며, $(-\infty, 0)$과 $(0, \infty)$ 각 구간에서는 감소하지만 두 구간에 걸쳐 전체적으로 감소하는 것은 아니다. 구간이 0을 가로지르는지부터 확인하지 않고 "역수를 취하면 부등호가 뒤집힌다"는 규칙만 외워 적용하면 틀린다.

5.2 구간과 경계점

구간 (a, b)는 $a < x < b$를, $[a, b]$는 $a \le x \le b$를 만족하는 실수들의 집합이다. 반열린구간 $[a, b)$와 $(a, b]$도 사용할 수 있다. 무한대를 경계로 쓸 때에는 $[a, \infty)$처럼 괄호를 쓴다. ∞는 이 문맥에서 실수 집합의 원소가 아니므로 닫힌 끝점으로 포함할 수 없다.

부등식의 해를 구할 때에는 계산으로 경계점 후보를 찾는 일과 그 점을 실제 해에 포함할지 판단하는 일을 구별한다. 분모가 0이 되는 점은 등식의 부호와 무관하게 원래 식의 정의역에서 제외된다.

예제 5.2 $\dfrac{x-1}{x+2} \geq 0$의 부호가 바뀔 수 있는 점은 $-2, 1$이다. 세 구간 $(-\infty,-2)$, $(-2,1)$, $(1,\infty)$에서 대푯값 $x=-3, 0, 2$를 대입하면 부호는 각각 $(-4)/(-1)=4$로 양, $-1/2$로 음, $1/4$로 양이다. $x=1$에서는 값이 0이므로 포함하고, $x=-2$에서는 정의되지 않으므로 제외한다. 해는 $(-\infty,-2)\cup[1,\infty)$이다.

5.3 절댓값과 거리

정의 5.3 (절댓값) 실수 x의 **절댓값**(*absolute value*)은 $x\geq 0$이면 $|x|=x$, $x<0$이면 $|x|=-x$로 정의한다. 두 실수 a, b 사이의 **거리**(*distance*)는 $|a-b|$이다.

절댓값은 항상 비음수이고, $|x|=0$일 필요충분조건은 $x=0$이다. 또한 $|xy|=|x||y|$, $|x|^2=x^2$이며 $\sqrt{x^2}=|x|$이다.

주의 (제곱근을 함부로 줄이는 오류). 마지막 식을 $\sqrt{x^2}=x$라고 줄이면 $x<0$에서 틀린다. 제곱근 기호 $\sqrt{\ }$는 항상 비음의 값을 뜻하므로, $\sqrt{x^2}$은 x 자신이 아니라 x의 절댓값과 같다. 예를 들어 $x=-3$이면 $\sqrt{x^2}=\sqrt{9}=3=|x|$이지 $x=-3$이 아니다.

$r>0$일 때

$$|x-a|<r \iff a-r<x<a+r \tag{5.1}$$

이다. 반대로 $|x-a|>r$은 $x<a-r$ 또는 $x>a+r$이라는 뜻이다. 안쪽 구간을 나타내는 조건과 바깥쪽 두 구간을 나타내는 조건을 구별하면 절댓값 부등식을 그림 없이도 해석할 수 있다.

예제 5.4 $|2x-3|\leq 5$는 $-5\leq 2x-3\leq 5$와 동치이므로 $-1\leq x\leq 4$이다. 한편 $|2x-3|\geq 5$는 $2x-3\leq -5$ 또는 $2x-3\geq 5$이므로 $x\leq -1$ 또는 $x\geq 4$이다.

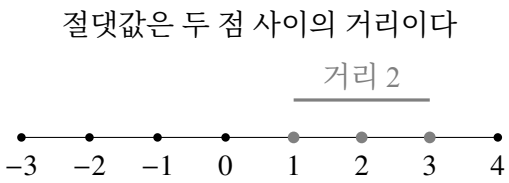

그림 5.1 절댓값으로 나타낸 두 점 사이의 거리. $|3-1|=2$이고 거리에는 방향의 부호가 붙지 않는다.

5.4 삼각부등식과 역삼각부등식

정리 5.5 (삼각부등식) 모든 실수 x, y에 대하여

$$|x+y|\leq |x|+|y|, \qquad \bigl||x|-|y|\bigr|\leq |x-y| \tag{5.2}$$

이다.

증명. $-|x|\leq x\leq |x|$와 $-|y|\leq y\leq |y|$를 변끼리 더하면 $-(|x|+|y|)\leq x+y\leq |x|+|y|$이므로 첫 식을 얻는다. 이어서 $|x|=|(x-y)+y|\leq |x-y|+|y|$이므로 $|x|-|y|\leq |x-y|$이다. x, y를 바꾸면 $|y|-|x|\leq |y-x|=|x-y|$를 얻어 $-|x-y|\leq |x|-|y|\leq |x-y|$가 되고, 이는 두 번째 식과 같다. $\square$

삼각부등식은 실제 삼각형에서 두 변의 길이의 합이 나머지 변의 길이 이상이라는 사실을 수직선 위에서 표현한 것이다. 이 부등식은 이후 벡터, 함수, 확률변수의 크기를 측정하는 노름(*norm*)으로 확장된다. 합을 다룰 때 각 항의 오차를 따로 추정하여 전체 오차의 상한을 얻는 데 특히 유용하다.

> **예제 5.6** 참값이 a, b이고 근삿값이 $\tilde{a}, \tilde{b}$이며 각각의 절대오차가 ε, δ 이하라고 하자. 그러면
>
> $$\bigl|(\tilde{a}+\tilde{b})-(a+b)\bigr| \le |\tilde{a}-a| + |\tilde{b}-b| \le \varepsilon + \delta$$
>
> 이다. 오차의 부호가 우연히 상쇄될 수도 있지만, 부호를 모를 때 항상 보장할 수 있는 상한은 두 오차의 합이다.

5.5 산술평균과 기하평균

> **정리 5.7 (산술평균-기하평균 부등식)** 비음수 실수 a, b에 대하여
>
> $$\sqrt{ab} \le \frac{a+b}{2}, \tag{5.3}$$
>
> 등호는 $a = b$일 때, 그리고 그때에만 성립한다.

증명. $(\sqrt{a}-\sqrt{b})^2 \ge 0$을 전개하면 $a+b-2\sqrt{ab} \ge 0$이다. 제곱이 0일 필요충분조건은 두 제곱근이 같은 것이므로 등호 조건도 얻는다. □

> **예제 5.8** 양수 x, y가 $x + y = 10$을 만족하면 식 (5.3)에 의해 $\sqrt{xy} \le 5$이므로 $xy \le 25$이다. 등호는 $x = y = 5$에서 성립한다. 합이 고정된 두 양수의 곱을 미분 없이 최대화한 것이다.

음수에 같은 공식을 적용할 때에는 기하평균의 실수 정의부터 문제가 된다. 일반적인 양수 여러 개에 대한 산술평균-기하평균 부등식과 가중 버전은 이후 볼록성, 옌센 부등식과 연결하여 다룬다(제8권 제3장). 식만 외우기보다 변수의 허용 범위와 등호 조건을 함께 기억해야 한다.

5.6 코시-슈바르츠 부등식의 첫 형태

> **정리 5.9 (코시-슈바르츠 부등식)** 실수 a, b, c, d에 대하여
>
> $$(ac+bd)^2 \le (a^2+b^2)(c^2+d^2). \tag{5.4}$$

증명. 오른쪽에서 왼쪽을 빼면

$$(a^2+b^2)(c^2+d^2) - (ac+bd)^2 = a^2d^2 + b^2c^2 - 2abcd = (ad-bc)^2$$

이므로 비음수이다. 따라서 부등식이 성립하고, 등호는 $ad = bc$일 때 성립한다. □

벡터 (a, b)와 (c, d)가 0이 아닌 경우 등호 조건 $ad = bc$는 두 벡터가 같은 직선 위에 있다는 뜻이다. 하나가 영벡터인 경우에도 등호가 성립한다. 높은 차원에서는 제곱의 합과 내적을 이용하여 같은 구조의 부등식이 성립한다(제7권 제8장).

예제 5.10 실수 x, y에 대해 $(a,b)=(x,y)$, $(c,d)=(1,2)$를 식 (5.4)에 대입하면 $(x+2y)^2 \le 5(x^2+y^2)$이다. 따라서 $x^2+y^2=1$이면 $|x+2y| \le \sqrt{5}$이며, 등호 조건 $ad=bc$, 곧 $2x=y$를 $x^2+y^2=1$과 연립하면 $(x,y)=\pm(1,2)/\sqrt{5}$에서 등호가 된다.

5.7 문제와 풀이

연습문제 5.11 $|x-2|+|x+2|$의 최솟값과 이를 달성하는 모든 x를 구하여라.

풀이. 삼각부등식으로 $|x-2|+|x+2| \ge |(x+2)-(x-2)| = 4$이다. $-2 \le x \le 2$이면 합이 $(2-x)+(x+2)=4$이다. 바깥에서는 각각 $-2x$ 또는 $2x$가 더해져 값이 4보다 커진다. 따라서 최솟값은 4이고, 달성 집합은 $[-2,2]$이다.

연습문제 5.12 $x>0$일 때 $x+1/x \ge 2$임을 보이고 등호 조건을 구하여라.

풀이. 산술평균-기하평균 부등식으로 $(x+1/x)/2 \ge \sqrt{x\cdot(1/x)}=\sqrt{1}=1$이므로 $x+1/x \ge 2$이다. 등호는 $x=1/x$이고 $x>0$일 때이므로 $x=1$이다. 또는 $(x-1)^2/x \ge 0$을 전개해도 된다.

연습문제 5.13 $|x|<3$이고 $|y|<2$일 때 $|2x-y|<8$임을 보여라.

풀이. 삼각부등식으로 $|2x-y| \le 2|x|+|y| < 2\cdot 3+2 = 8$이다. 최종 엄격 부등호는 입력 조건이 엄격하다는 점에서 나온다. x, y의 부호를 정할 필요가 없다.

연습문제 5.14 $a,b>0$일 때 $\dfrac{1}{a}+\dfrac{1}{b} \ge \dfrac{4}{a+b}$를 증명하여라.

풀이. 양수 $ab(a+b)$를 곱하면 $(a+b)^2 \ge 4ab$와 동치이고, 이는 $(a-b)^2 \ge 0$이다. 등호는 $a=b$일 때 성립한다.

참고 (다음 연결). 이 장의 부등식들은 유리수의 조밀성(제1권 제4장)과 함께, 실수의 완비성을 상한의 존재로 공리화하는 다음 장(제1권 제6장)의 증명에서 되풀이하여 쓰인다. 삼각부등식과 코시-슈바르츠 부등식은 벡터공간의 노름과 내적(제7권 제8장)으로, 산술평균-기하평균 부등식은 볼록함수와 옌센 부등식(제8권 제3장)으로 일반화된다.

제 6 장

무리수와 실수의 완비성

개요 무리수는 유리수가 아닌 실수이고, 실수의 완비성은 위로 유계인 공집합 아닌 실수 집합이 언제나 실수인 상한을 갖는다는 성질이다. 이 장은 $\sqrt{2}$가 유리수가 아님을 증명하여 유리수만으로는 길이를 모두 나타낼 수 없음을 보이고, 상계·상한·최댓값을 구별한 뒤 완비성 공리를 진술한다. 이어서 완비성으로부터 아르키메데스 성질, 유리수와 무리수의 조밀성, 단조수렴 정리, 코시 수열의 수렴을 차례로 이끌어 낸다. 수열의 극한은 직관에 기대지 않고 ε과 N을 쓰는 정확한 정의로 다룬다. 선행 지식: 유리수(제1권 제4장), 순서와 절댓값(제1권 제5장).

6.1 유리수만으로는 부족한 이유

한 변의 길이가 1인 정사각형의 대각선 길이는 피타고라스 정리에 의해 제곱이 2인 양수이다. 이 길이는 분수로 나타낼 수 있을 것처럼 보이지만 실제로는 불가능하다. 계산이 덜 되어서가 아니라 그 수가 유리수의 범위 밖에 있기 때문이다. 유리수가 아닌 실수를 **무리수**(*irrational number*)라고 한다. 제곱이 2인 양의 실수를 $\sqrt{2}$로 쓰며, 그러한 실수가 존재한다는 사실은 완비성에서 나온다(6.3절).

정리 6.1 $\sqrt{2}$는 유리수가 아니다.

증명. $\sqrt{2} = a/b$인 기약분수가 존재한다고 가정한다. 여기서 a, b는 정수이고 $b > 0$이다. 양변을 제곱하면 $a^2 = 2b^2$이므로 a^2은 짝수이다. 홀수의 제곱은 홀수이므로 a는 짝수이고 $a = 2k$(k는 정수)로 쓸 수 있다. 대입하면 $4k^2 = 2b^2$, 곧 $b^2 = 2k^2$이므로 같은 이유로 b도 짝수이다. 따라서 a, b가 모두 2로 나누어지며, 이는 a/b가 기약분수라는 가정에 모순이다. □

명제 6.2 양의 정수 n에 대하여 $\sqrt{n}$이 유리수이면 $\sqrt{n}$은 정수이다.

증명. $\sqrt{n} = a/b$인 기약분수를 택하면(a, b는 양의 정수) $a^2 = nb^2$이다. $b > 1$이라면 b를 나누는 소수 p가 있고, $p \mid nb^2 = a^2$이다. 소수가 곱을 나누면 인수 가운데 하나를 나누므로(제1권 제3장) $p \mid a$이다. 그러면 p가 a와 b의 공약수가 되어 기약 조건에 모순이다. 따라서 $b = 1$이고 $\sqrt{n} = a$는 정수이다. □

참고 (완전제곱수가 아닌 수의 제곱근). 명제 6.2의 대우에 따라, 양의 정수 n이 완전제곱수가 아니면 $\sqrt{n}$은 무리수이다. 예를 들어 $1^2 < 2 < 2^2$, $1^2 < 3 < 2^2$, $2^2 < 5 < 3^2$이므로 $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$는 정수가 아니고, 따라서 무리수이다. 같은 증명은 세제곱근 이상에도 적용된다. 양의 정수 n과 $k \geq 2$에 대하여 $\sqrt[k]{n} = a/b$가 기약분수이면 $a^k = nb^k$에서 $b = 1$이 나온다.

무리수는 "계산할 수 없는 수"와 같은 말이 아니다. $\sqrt{2}$는 유리수가 아니지만 이분법이나 뉴턴 방법(*Newton's method*)으로 원하는 정확도까지 유리수로 근사할 수 있다. 예를 들어 $x_1 = 2$에서

출발하여 $x_{n+1} = \tfrac{1}{2}\left(x_n + 2/x_n\right)$을 되풀이하면

$$2, \quad \frac{3}{2}, \quad \frac{17}{12}, \quad \frac{577}{408} = 1.4142156\cdots$$

을 얻고, 넷째 항은 이미 $\sqrt{2} = 1.4142135\cdots$와 소수점 아래 다섯 자리까지 일치한다. 또한 무한히 이어지는 소수라는 이유만으로 무리수가 되는 것도 아니다. $1/3 = 0.333\cdots$은 무한소수이지만 유리수이다. 유리수와 무리수를 가르는 기준은 소수 전개가 어느 자리부터 주기적으로 반복되는지이다. 유리수의 소수 전개는 유한하거나 순환하고, 무리수의 소수 전개는 순환하지 않는 무한소수이다(제1권 제4장).

주의 (무리수의 사칙연산). 유리수 r와 무리수 x의 합 $r+x$는 무리수이다. $r+x=s$가 유리수라면 $x = s - r$도 유리수가 되기 때문이다. 같은 이유로 $r \neq 0$이면 rx와 x/r도 무리수이다. 그러나 무리수끼리의 합과 곱은 유리수일 수 있다. $\sqrt{2} + (-\sqrt{2}) = 0$, $\sqrt{2}\cdot\sqrt{2} = 2$가 그 예이다. 따라서 무리수의 집합은 덧셈과 곱셈에 대해 닫혀 있지 않다.

역사 (통약 불가능성). 정사각형의 한 변과 대각선을 공통의 단위로 잴 수 없다는 사실은 고대 그리스의 피타고라스 학파에서 발견된 것으로 전해진다. Euclid의 『원론』 제10권은 이처럼 통약 불가능한 크기를 체계적으로 분류한다. 무리수를 포함한 실수 전체를 유리수로부터 엄밀하게 구성하는 일은 19세기 후반에 이루어졌다.

6.2 상계, 상한, 최댓값

정의 6.3 실수의 집합 S에 대하여 모든 $x \in S$가 $x \le M$을 만족하면 실수 M을 S의 **상계**(*upper bound*)라고 하고, 상계가 존재하는 집합을 **위로 유계**라고 한다. 상계 가운데 가장 작은 것을 **상한**(*supremum*) 또는 **최소상계**라 하고 $\sup S$로 쓴다. $m \in S$가 S의 모든 원소 이상이면 m을 S의 **최댓값**이라 하고 $\max S$로 쓴다.

부등호의 방향을 바꾸면 아래쪽 개념을 얻는다. 모든 $x \in S$가 $x \ge M$을 만족하면 M을 **하계**(*lower bound*)라고 하고, 하계가 존재하는 집합을 **아래로 유계**라고 한다. 하계 가운데 가장 큰 것이 **하한**(*infimum*) 또는 **최대하계** $\inf S$이고, S의 모든 원소 이하인 S의 원소가 **최솟값** $\min S$이다. 위로도 아래로도 유계인 집합을 **유계**라고 한다.

상한은 집합 안에 있을 필요가 없지만, 최댓값은 반드시 집합 안에 있어야 한다. 예를 들어 열린구간 $(0,1)$의 상한은 1이지만 최댓값은 없다. 닫힌구간 $[0,1]$은 상한과 최댓값이 모두 1이다. 상계는 $1, 2, 100$처럼 여러 개일 수 있어도 상한은 존재한다면 유일하다. s와 s'이 모두 상한이면 둘 다 상계이므로 최소성에서 $s \le s'$과 $s' \le s$가 함께 성립하기 때문이다. 최댓값 m이 존재하면 m은 상계이고, 어떤 상계 u도 $m \in S$에서 $m \le u$를 만족하므로 $\sup S = \max S$이다.

명제 6.4 실수 s가 $s = \sup S$일 필요충분조건은 다음 두 조건이 함께 성립하는 것이다.

(1) 모든 $x \in S$에 대하여 $x \le s$이다.

(2) 모든 $\varepsilon > 0$에 대하여 $s - \varepsilon < x$인 $x \in S$가 존재한다.

증명. $s = \sup S$라 하자. s는 상계이므로 첫째 조건이 성립한다. $\varepsilon > 0$이면 $s - \varepsilon$는 s보다 작은 수이므로 상계일 수 없다. 따라서 $s - \varepsilon < x$인 원소 $x \in S$가 존재한다.

역으로 두 조건이 성립한다고 하자. 첫째 조건에서 s는 상계이다. $u < s$인 상계 u가 있다고 가정하고 둘째 조건에 $\varepsilon = s - u > 0$을 대입하면 $u = s - \varepsilon < x$인 $x \in S$가 존재하며, 이는 u가 상계라는 가정에 모순이다. 따라서 s보다 작은 상계는 없고 s는 최소상계이다. □

둘째 조건을 상한의 **근접 성질**이라고 부른다. 상한 바로 아래에는 아무리 좁은 폭을 잡아도 집합의 원소가 들어 있다는 뜻이다.

> **예제 6.5** $S = \{1 - 1/n : n \in \mathbb{N}_{>0}\}$의 상한은 1이다. 모든 항이 1보다 작으므로 1은 상계이다. 임의의 $\varepsilon > 0$에 대해 $n > 1/\varepsilon$인 양의 정수 n을 택하면 $1/n < \varepsilon$이므로 $1 - 1/n > 1 - \varepsilon$이다. 그러한 n이 존재한다는 사실은 아르키메데스 성질(정리 6.6)이 보장한다. 따라서 명제 6.4에 의해 $\sup S = 1$이다. 그러나 어떤 항도 1과 같지 않으므로 최댓값은 없다(그림 6.1). 한편 첫 항 0은 S의 최솟값이자 하한이다.

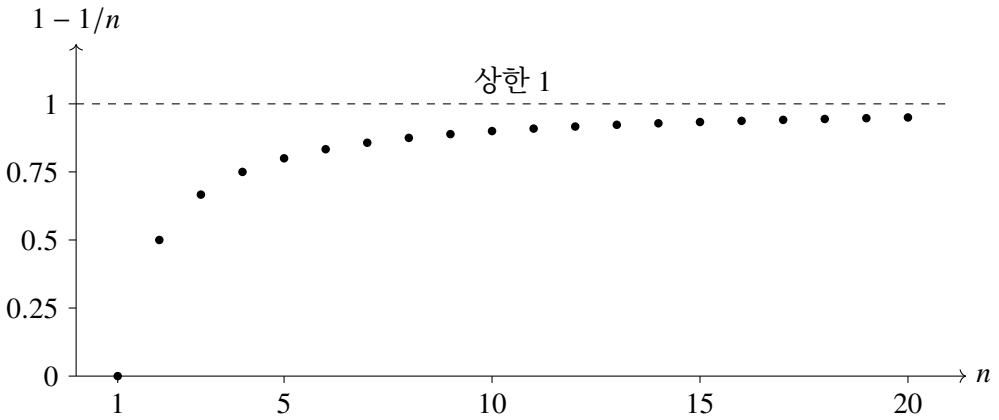

그림 6.1 수열 $1 - 1/n$의 항은 상한 1에 한없이 가까워지지만 어떤 항도 1에 도달하지 않는다. 증가수열의 상한과 최댓값은 다를 수 있다.

참고 (하한과 상한의 관계). $-S = \{-x : x \in S\}$로 놓으면 M이 S의 하계인 것과 $-M$이 $-S$의 상계인 것은 같다. 따라서

$$\inf S = -\sup(-S)$$

이고, 상한에 관한 모든 진술은 부호를 바꾸어 하한에 관한 진술로 옮겨진다. 특히 $t = \inf S$일 필요충분조건은 모든 $x \in S$에 대하여 $t \le x$이고, 모든 $\varepsilon > 0$에 대하여 $x < t + \varepsilon$인 $x \in S$가 존재하는 것이다.

6.3 완비성 공리

실수의 **완비성**(*completeness*)은 다음과 같이 진술한다. 이 진술을 **완비성 공리** 또는 **상한 공리**라고 한다.

> 공집합이 아니고 위로 유계인 실수의 부분집합은 모두 실수인 상한을 갖는다.

앞 절의 참고에 따라, 공집합이 아니고 아래로 유계인 실수의 부분집합은 모두 실수인 하한을 갖는다는 진술도 이와 동치이다.

이 명제는 유리수에서는 성립하지 않는다. 예를 들어 $S = \{q \in \mathbb{Q} : q \geq 0,\ q^2 < 2\}$를 유리수 안에서만 생각하면 상한이 될 유리수가 없다. 실수에서는 그 틈이 $\sqrt{2}$로 채워진다. 이 두 사실은 다음 계산으로 확인된다.

유도 (제곱이 2인 양의 실수의 존재). $T = \{x \in \mathbb{R} : x \geq 0,\ x^2 < 2\}$라 하자. $1 \in T$이므로 T는 공집합이 아니다. $x > 2$이면 $x^2 > 4$이므로 T의 모든 원소는 2 이하이고, T는 위로 유계이다. 완비성 공리에 의해 $s = \sup T$가 존재하며 $1 \leq s \leq 2$이다. $s^2 = 2$임을 보인다.

$s^2 < 2$라고 가정하고 $h = (2 - s^2)/5$로 놓으면 $0 < h \leq 1/5$이다. $s \leq 2$와 $h^2 < h$를 쓰면

$$(s+h)^2 = s^2 + 2sh + h^2 < s^2 + 4h + h = s^2 + 5h = 2$$

이므로 $s + h \in T$이다. 이는 s가 T의 상계라는 사실에 모순이다.

$s^2 > 2$라고 가정하고 $h = (s^2 - 2)/(2s) > 0$으로 놓으면 $s - h = (s^2 + 2)/(2s) > 0$이고

$$(s-h)^2 = s^2 - 2sh + h^2 > s^2 - 2sh = 2$$

이다. 모든 $x \in T$에 대해 $x^2 < 2 < (s-h)^2$이고 $x \geq 0$, $s - h > 0$이므로 $x < s - h$이다. 그러면 $s - h$가 s보다 작은 상계가 되어 s의 최소성에 모순이다. 따라서 $s^2 = 2$이고, 이 s가 $\sqrt{2}$이다.

같은 계산은 유리수 안에서도 그대로 진행된다. s가 유리수이면 위의 h도 유리수이기 때문이다. 그러므로 S가 유리수인 최소상계 s를 갖는다면 $s^2 = 2$여야 하는데, 이는 정리 6.1에 모순이다.

완비성은 "실수는 소수를 끝까지 쓴 것"이라는 표현보다 정확한 구조를 준다. 실수는 사칙연산과 순서가 서로 어울리는 체, 곧 순서체(*ordered field*)이고, 여기에 더하여 상한 성질을 만족한다. 유리수도 순서체이므로 실수를 유리수와 구별하는 성질은 완비성 하나이다. 데데킨트 절단(*Dedekind cut*)이나 유리수 코시 수열의 동치류를 이용하면 이러한 대상을 유리수로부터 실제로 구성할 수 있다. 두 구성은 겉모양이 달라도 순서와 연산을 보존하는 동형을 통해 같은 실수체를 준다. 일반적으로 완비 순서체는 동형인 것을 같게 보면 하나뿐이다. 구성의 세부와 동형의 의미는 제5권 제4장에서 다룬다.

흔한 오류. 완비성을 "모든 부분집합에 상한이 있다"로 줄이면 틀린 진술이 된다. $\mathbb{R}$ 자체는 위로 유계가 아니므로 실수인 상한을 갖지 않는다. 공집합을 제외하는 조건도 필요하다. 공집합에 대해서는 모든 실수가 상계이므로 가장 작은 상계가 없기 때문이다. 확장실수 $\mathbb{R} \cup \{-\infty, +\infty\}$를 사용하면 $\sup \mathbb{R} = +\infty$, $\sup \emptyset = -\infty$와 같은 별도의 약속으로 이 예외를 표현할 수 있지만, 그때에는 $\infty - \infty$가 정의되지 않는 등 연산 규칙도 달라진다.

참고 (완비성의 동치 표현). 순서체에서 상한 공리는 다음 진술 각각과 동치이다. 위로 유계인 증가수열은 수렴한다(정리 6.11). 아르키메데스 성질이 성립하고 모든 코시 수열이 수렴한다(정리 6.6, 정의 6.12). 이 장은 상한 공리를 출발점으로 삼아 나머지를 정리로 증명한다.

역사 (실수의 엄밀한 구성). R. Dedekind는 1872년의 저서 『연속성과 무리수』(*Stetigkeit und irrationale Zahlen*)에서 유리수의 절단으로 실수를 정의하였고, 같은 해 G. Cantor는 유리수의 코시 수열을 이용한 구성을 발표하였다. 두 구성 모두 실수의 연속성을 기하학적 직관이 아니라 유리수의 산술만으로 설명한다.

6.4 아르키메데스 성질과 조밀성

정리 6.6 모든 실수 x에 대하여 $x < n$을 만족하는 자연수 n이 존재한다. 따라서 모든 $\varepsilon > 0$에 대해 $0 < 1/n < \varepsilon$인 양의 정수 n이 존재한다.

증명. 첫째 진술이 거짓이라면 어떤 실수 x가 모든 자연수 n에 대해 $n \le x$를 만족하므로 자연수 집합 $\mathbb{N}$이 위로 유계이다. $\mathbb{N}$은 공집합이 아니므로 완비성 공리에 의해 상한 $s = \sup \mathbb{N}$이 존재한다. 상한의 근접 성질(명제 6.4에서 $\varepsilon = 1$)로 $s - 1 < n$인 자연수 n이 있다. 그러면 자연수 $n + 1$이 s보다 커서 s가 상계라는 사실에 모순이다.

둘째 진술은 첫째 진술을 $x = 1/\varepsilon$에 적용하여 $n > 1/\varepsilon > 0$인 자연수 n을 택하면 얻어진다. 이때 $n \ge 1$이고 $0 < 1/n < \varepsilon$이다. □

정리 6.6의 성질을 **아르키메데스 성질**(*Archimedean property*)이라고 한다. 양의 실수 a, b에 대하여 $na > b$인 자연수 n이 존재한다는 진술과 같으며($x = b/a$로 놓는다), 아무리 작은 양의 길이도 충분히 여러 번 이어 붙이면 주어진 길이를 넘는다는 뜻이다. 실수에는 모든 $1/n$보다 작은 양수, 곧 무한소가 없다.

정리 6.7 $a < b$인 두 실수 사이에는 유리수가 존재한다.

증명. 정리 6.6에 의해 $1/n < b - a$인 양의 정수 n을 택할 수 있다. 정수 m을 $na < m \le na + 1$이 되게 택하면

$$a < \frac{m}{n} \le a + \frac{1}{n} < b$$

이므로 m/n이 구하는 유리수이다.

그러한 정수 m이 존재함을 보인다. 정리 6.6에 의해 $na < l$인 자연수 l과 $-na < k$인 자연수 k가 있다. na보다 큰 정수의 집합은 l을 포함하므로 공집합이 아니고, 그 원소는 모두 $-k$보다 크다. 아래로 유계인 공집합 아닌 정수 집합에는 가장 작은 원소가 있으므로 그것을 m이라 한다(각 원소에 k를 더하면 양의 정수의 집합이 되므로 제1권 제2장의 정렬 원리를 적용할 수 있다). $m - 1$은 이 집합에 속하지 않으므로 $m - 1 \le na$이고, 따라서 $na < m \le na + 1$이다. 바닥 함수로 쓰면 $m = \lfloor na \rfloor + 1$이다. □

같은 구간 안에는 무리수도 있다. $a < b$이면 $a/\sqrt{2} < b/\sqrt{2}$이므로 정리 6.7에 의해 $a/\sqrt{2} < q < b/\sqrt{2}$인 유리수 q가 있다. $q \neq 0$이면 $q\sqrt{2}$는 무리수이고 $a < q\sqrt{2} < b$이다. $q = 0$이 선택되는 경우는 $a < 0 < b$일 때뿐이며, 이때에는 구간을 $(0, b)$로 줄여 다시 택하면 $q > 0$을 얻는다.

실수의 부분집합 D가 모든 열린구간 $(a, b)(a < b)$와 만날 때 D는 $\mathbb{R}$에서 **조밀하다**(*dense*)고 한다. 위의 논의는 유리수의 집합 $\mathbb{Q}$와 무리수의 집합 $\mathbb{R} \setminus \mathbb{Q}$가 모두 $\mathbb{R}$에서 조밀함을 보여 준다. 구간 (a, b)에서 찾은 유리수 q_1에 대해 다시 (a, q_1)에서 유리수를 찾는 일을 되풀이하면, 서로 다른 두 실수 사이에는 유리수가 무한히 많이 있음을 알 수 있다. 무리수도 마찬가지이다.

6.5 수열의 수렴

실수의 **수열**(*sequence*)은 양의 정수 n마다 실수 a_n을 하나씩 대응시킨 것이며 (a_n)으로 쓴다.

정의 6.8 실수 수열 (a_n)이 실수 L로 **수렴**한다는 것은 모든 $\varepsilon > 0$에 대해 어떤 양의 정수 N이 존재하여 $n \geq N$이면 $|a_n - L| < \varepsilon$이 성립한다는 뜻이다. 이때 L을 수열의 **극한**이라 하고 $a_n \to L$ 또는 $\lim_{n\to\infty} a_n = L$로 쓴다. 어떤 실수로도 수렴하지 않는 수열은 **발산**한다고 한다.

기호로 쓰면 수렴의 정의는

$$\forall \varepsilon > 0 \ \ \exists N \in \mathbb{N}_{>0} \ \ \forall n \geq N : \quad |a_n - L| < \varepsilon \tag{6.1}$$

이다. 양화사의 순서가 중요하다. 먼저 요구 정확도 ε이 주어지고, 그 정확도에 맞추어 N을 택한다. N은 ε에 의존할 수 있지만 그 뒤의 개별 n마다 새로 고르는 값은 아니다. 하나의 N이 그보다 뒤에 있는 모든 항에 대해 한꺼번에 조건을 보장해야 한다. 부등식 $|a_n - L| < \varepsilon$은 $L - \varepsilon < a_n < L + \varepsilon$과 같으므로, 수렴은 어떤 폭의 구간 $(L-\varepsilon, L+\varepsilon)$을 잡아도 유한 개를 뺀 모든 항이 그 안에 든다는 뜻이다. 식 (6.1)을 부정하면 "a_n이 L로 수렴하지 않는다"는 진술을 얻는다. 곧 어떤 $\varepsilon > 0$이 있어서 모든 N에 대해 $|a_n - L| \geq \varepsilon$인 $n \geq N$이 존재한다는 것이다.

예제 6.9 $a_n = 3 + 2/n$이 3으로 수렴함을 보인다. $\varepsilon > 0$이 주어지면 $N > 2/\varepsilon$인 양의 정수 N을 택한다(정리 6.6). $n \geq N$이면

$$|a_n - 3| = \frac{2}{n} \leq \frac{2}{N} < \varepsilon$$

이므로 정의가 충족된다. 예를 들어 오차를 0.001보다 작게 하려면 $2/n < 0.001$, 곧 $n > 2000$이면 충분하고, $N = 2001$로 택할 수 있다.

정리 6.10 수열의 극한은 존재한다면 유일하다.

증명. 수열 (a_n)이 서로 다른 두 극한 L, M을 갖는다고 가정하고 $\varepsilon = |L - M|/3 > 0$으로 놓는다. 정의에 의해 $n \geq N_1$이면 $|a_n - L| < \varepsilon$인 N_1과 $n \geq N_2$이면 $|a_n - M| < \varepsilon$인 N_2가 있다. $n \geq \max(N_1, N_2)$인 n을 하나 택하면 두 부등식이 동시에 성립하므로 삼각부등식에 의해

$$|L - M| \leq |L - a_n| + |a_n - M| < 2\varepsilon = \frac{2}{3}|L - M|$$

이다. $|L - M| > 0$이므로 이는 모순이다. $\square$

참고 (수렴 수열은 유계이다). $a_n \to L$이면 식 (6.1)에서 $\varepsilon = 1$에 대한 N을 택할 때 $n \geq N$인 모든 항이 $|a_n| < |L| + 1$을 만족한다. 따라서 모든 n에 대하여 $|a_n| \leq \max\bigl(|a_1|, \dots, |a_{N-1}|, |L| + 1\bigr)$이다. 역은 성립하지 않는다. $a_n = (-1)^n$은 유계이지만 수렴하지 않는다(연습문제 6.15).

6.6 단조수렴과 코시 조건

모든 n에 대하여 $a_n \leq a_{n+1}$인 수열을 **증가수열**, $a_n \geq a_{n+1}$인 수열을 **감소수열**이라 하고, 둘을 합쳐 **단조수열**이라고 한다. 여기서 증가는 등호를 허용하는 넓은 뜻이다.

정리 6.11 위로 유계인 증가수열은 그 항들의 집합의 상한으로 수렴한다.

증명. 항들의 집합 $\{a_n : n \geq 1\}$은 공집합이 아니고 위로 유계이므로 완비성 공리에 의해 상한 $L = \sup\{a_n : n \geq 1\}$이 존재한다. 임의의 $\varepsilon > 0$에 대해 상한의 근접 성질로 $L - \varepsilon < a_N$인 항 a_N

이 존재한다. 수열이 증가하고 L이 상계이므로 $n \geq N$이면

$$L - \varepsilon < a_N \leq a_n \leq L$$

이다. 따라서 $n \geq N$이면 $|a_n - L| < \varepsilon$이다. □

이 정리를 **단조수렴 정리**(*monotone convergence theorem*)라고 한다. 수열 $(-a_n)$에 적용하면 아래로 유계인 감소수열이 그 항들의 집합의 하한으로 수렴한다는 결과를 얻는다. 이 정리는 극한의 값을 미리 알지 못해도 수렴을 보장한다는 점에서 유용하다. 예제 6.5의 수열 $1 - 1/n$은 위로 유계인 증가수열이고 그 극한은 상한 1이다.

정의 6.12 모든 $\varepsilon > 0$에 대해 어떤 양의 정수 N이 존재하여 $m, n \geq N$이면 $|a_m - a_n| < \varepsilon$이 성립하는 수열 (a_n)을 **코시 수열**(*Cauchy sequence*)이라고 한다.

수렴의 정의는 후보 극한 L과 항을 비교하지만, 코시 조건은 뒤쪽 항들끼리만 비교한다. 따라서 코시 조건은 극한의 값을 모르는 상태에서도 확인할 수 있다. 실수에서는 코시 수열과 수렴 수열이 정확히 일치한다. 수렴 수열이 코시 수열이라는 방향은 삼각부등식으로 바로 보이고, 반대 방향에는 완비성이 필요하다.

유도 (수렴 수열은 코시 수열이다). $a_n \to L$이고 $\varepsilon > 0$이라 하자. $n \geq N$이면 $|a_n - L| < \varepsilon/2$인 N을 택한다. $m, n \geq N$이면

$$|a_m - a_n| \leq |a_m - L| + |L - a_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$$

이다. 이 논증은 완비성을 쓰지 않으므로 유리수 안에서도 성립한다.

유도 (실수의 코시 수열은 수렴한다). (a_n)이 코시 수열이라 하자.

1단계. 유계성. $\varepsilon = 1$에 대한 N_0을 택하면 $n \geq N_0$일 때 $|a_n| < |a_{N_0}| + 1$이므로, 앞 절의 참고와 같은 방법으로 수열이 유계임을 알 수 있다.

2단계. 후보 극한. $b_n = \inf\{a_k : k \geq n\}$으로 놓는다. 수열이 아래로 유계이므로 이 하한은 완비성에 의해 존재한다. n이 커지면 하한을 취하는 집합이 작아지므로 (b_n)은 증가수열이고, $b_n \leq a_n$이며 (a_n)이 유계이므로 (b_n)은 위로 유계이다. 정리 6.11에 의해 $b_n \to L$인 실수 L이 존재한다.

3단계. 수렴. $\varepsilon > 0$이 주어지면 $m, n \geq N$일 때 $|a_m - a_n| < \varepsilon$인 N을 택한다. $k \geq N$이면 $a_N - \varepsilon < a_k < a_N + \varepsilon$이므로, $n \geq N$일 때 $a_N - \varepsilon \leq b_n \leq a_n < a_N + \varepsilon$이고 따라서 $0 \leq a_n - b_n < 2\varepsilon$이다. 또 $n \geq N'$이면 $|b_n - L| < \varepsilon$인 N'이 있다. $n \geq \max(N, N')$이면

$$|a_n - L| \leq |a_n - b_n| + |b_n - L| < 3\varepsilon$$

이다. ε은 임의이므로 $a_n \to L$이다.

유리수 안에서는 반대 방향이 성립하지 않는다. $\sqrt{2}$에 접근하는 유리수 근사 수열은 코시 수열이지만 유리수인 극한을 갖지 않는다.

참고 (극한이 유리수가 아닌 유리수 코시 수열). $x_1 = 2$, $x_{n+1} = \tfrac{1}{2}\left(x_n + 2/x_n\right)$으로 정한 수열의 항은 모두 양의 유리수이다. 직접 계산하면

$$x_{n+1} - \sqrt{2} = \frac{x_n^2 - 2\sqrt{2}\,x_n + 2}{2x_n} = \frac{(x_n - \sqrt{2})^2}{2x_n} \geq 0$$

이므로 모든 항이 $x_n \ge \sqrt{2} > 1$을 만족하고, 오차 $e_n = x_n - \sqrt{2}$는 $0 \le e_{n+1} \le e_n^2/2$를 만족한다. $e_2 = 3/2 - \sqrt{2} < 1/10$이므로 $e_3 < 1/200$, $e_4 < 1/80000$이고, 일반적으로 $n \ge 2$에서 $e_{n+1} \le e_n/20$이다. 이로부터 $n \ge 2$에서 $e_n \le 20^{-(n-2)}/10$이다. $20^k > k$이므로 아르키메데스 성질에 의해 주어진 $\varepsilon > 0$에 대해 충분히 큰 n에서 $e_n < \varepsilon$이 된다. 따라서 $x_n \to \sqrt{2}$이다. 이 수열은 실수에서 수렴하므로 코시 수열이고, 코시 조건은 항들 사이의 부등식일 뿐이므로 유리수 안에서 보아도 코시 수열이다. 그러나 극한 $\sqrt{2}$가 유리수가 아니므로, 극한의 유일성(정리 6.10)에 의해 이 수열은 어떤 유리수로도 수렴하지 않는다.

핵심 수식

$$s = \sup S \iff (\forall x \in S:\ x \le s) \text{ 이고 } (\forall \varepsilon > 0\ \exists x \in S:\ s - \varepsilon < x),$$

$$a_n \to L \iff \forall \varepsilon > 0\ \exists N\ \forall n \ge N:\ |a_n - L| < \varepsilon,$$

$$(a_n)\text{이 코시 수열} \iff \forall \varepsilon > 0\ \exists N\ \forall m, n \ge N:\ |a_m - a_n| < \varepsilon.$$

6.7 문제와 풀이

연습문제 6.13 $\sqrt{12}$가 무리수임을 보여라.

풀이. $3^2 = 9 < 12 < 16 = 4^2$이므로 $3 < \sqrt{12} < 4$이고 $\sqrt{12}$는 정수가 아니다. 곧 12는 완전제곱수가 아니므로 명제 6.2에 의해 $\sqrt{12}$는 유리수가 아니다.

다른 방법으로, $\sqrt{12} = 2\sqrt{3}$이므로 $\sqrt{12}$가 유리수이면 $\sqrt{3} = \sqrt{12}/2$도 유리수이다. $\sqrt{3} = a/b$(a, b는 양의 정수)라 하면 $a^2 = 3b^2$이다. 소인수분해에서 좌변의 소인수 3의 지수는 짝수이고 우변에서는 홀수이므로, 소인수분해의 유일성(제1권 제3장)에 모순이다.

연습문제 6.14 $S = \{2 - 3/n : n \ge 1\}$의 상한, 하한, 최댓값, 최솟값을 구하여라.

풀이. $3/n$이 n에 대해 감소하므로 수열 $2 - 3/n$은 증가하고 첫 항은 -1이다. 따라서 최솟값은 -1이고 하한도 -1이다. 모든 항이 2보다 작으므로 2는 상계이다. 임의의 $\varepsilon > 0$에 대해 $n > 3/\varepsilon$이면 $2 - 3/n > 2 - \varepsilon$이므로 명제 6.4에 의해 상한은 2이다. 어떤 항도 2와 같지 않으므로 최댓값은 없다.

연습문제 6.15 $a_n = (-1)^n$이 수렴하지 않음을 정의 또는 코시 조건으로 보여라.

풀이. 코시 조건을 이용한다. 어떤 N을 잡아도 $m = 2N$, $n = 2N + 1$은 N 이상이고 $|a_m - a_n| = |1 - (-1)| = 2$이다. 따라서 $\varepsilon = 1$에 대한 코시 조건이 성립하지 않는다. 모든 수렴 수열은 코시 수열이므로 이 수열은 수렴하지 않는다.

정의를 직접 써도 된다. $a_n \to L$이라 가정하고 $\varepsilon = 1$에 대한 N을 택하면, N 이상의 짝수 m과 홀수 n에 대해 $|1 - L| < 1$, $|-1 - L| < 1$이다. 삼각부등식으로 $2 = |1 - (-1)| \le |1 - L| + |L + 1| < 2$가 되어 모순이다.

연습문제 6.16 $a_n \to L$이고 모든 n에 대해 $a_n \ge 0$이면 $L \ge 0$임을 보여라.

풀이. $L < 0$이라고 가정하고 $\varepsilon = -L/2 > 0$을 택한다. 충분히 큰 n에서 $|a_n - L| < \varepsilon$이므로 $a_n < L + \varepsilon = L/2 < 0$이 되어 $a_n \ge 0$이라는 가정에 모순이다. 단, 모든 항이 양수라고 해서 극한도

반드시 양수인 것은 아니다. $a_n = 1/n$은 모든 항이 양수이지만 극한은 0이다. 극한으로 넘어갈 때 엄격한 부등호 $>$는 $\geq$로 약해질 수 있다.

연습문제 6.17 $\sqrt{2}+\sqrt{3}$이 무리수임을 보여라.

풀이. $r = \sqrt{2}+\sqrt{3}$이 유리수라고 가정한다. 제곱하면 $r^2 = 5 + 2\sqrt{6}$이므로 $\sqrt{6} = (r^2-5)/2$도 유리수이다. 그런데 $2^2 < 6 < 3^2$이므로 6은 완전제곱수가 아니고, 명제 6.2에 의해 $\sqrt{6}$은 무리수이다. 이는 모순이다.

연습문제 6.18 공집합이 아니고 위로 유계인 실수 집합 A, B에 대하여 $A + B = \{a + b : a \in A,\ b \in B\}$라 할 때 $\sup(A+B) = \sup A + \sup B$임을 보여라.

풀이. $\alpha = \sup A$, $\beta = \sup B$라 하자. 모든 $a \in A$, $b \in B$에 대해 $a + b \leq \alpha + \beta$이므로 $\alpha+\beta$는 $A+B$의 상계이다. $\varepsilon > 0$이 주어지면 상한의 근접 성질로 $\alpha - \varepsilon/2 < a$인 $a \in A$와 $\beta - \varepsilon/2 < b$인 $b \in B$가 있고, 이때 $\alpha+\beta-\varepsilon < a+b$이다. 명제 6.4에 의해 $\sup(A+B) = \alpha+\beta$이다.

참고 (다음 연결). 실수를 유리수로부터 구성하는 방법은 제5권 제4장에서, 함수의 극한과 연속은 제8권 제1장에서, 수열과 급수의 수렴 판정은 제8권 제6장에서 다룬다. 상극한과 실수의 위상적 성질은 제10권 제1장에서 이어진다. 완비성은 실수 지수의 거듭제곱을 정의하는 데에도 쓰인다(제1권 제7장).

제 7 장

거듭제곱, 근호, 지수와 로그

개요 거듭제곱은 같은 수를 되풀이하여 곱하는 연산이고, 근호와 로그는 각각 밑과 지수를 되찾는 역연산이다. 이 장은 지수를 양의 정수에서 정수, 유리수, 실수로 차례로 넓히면서 단계마다 지수 법칙이 유지되기 위해 밑에 어떤 조건이 필요한지를 밝힌다. 근호는 여러 근 가운데 하나를 가리키는 주값의 기호로 정의하고, 로그는 지수함수의 역함수로 정의하여 곱·몫·거듭제곱의 법칙과 밑 변환 공식을 증명한다. 끝으로 로그 방정식과 무리방정식에서 정의역을 먼저 정해야 하는 이유를 예제로 보인다. 선행 지식: 실수의 순서와 분수 계산(제1권 제4장, 제1권 제5장). 실수 지수의 존재에는 실수의 완비성(제1권 제6장)이 쓰이며, 자세한 구성은 제8권에서 보충한다.

7.1 정수 지수와 역원

실수 a와 양의 정수 n에 대해 **거듭제곱**(*power*) a^n은 a를 n번 곱한 값이다. 귀납적으로는 $a^1 = a$, $a^{n+1} = a^n \cdot a$로 정의한다. a를 **밑**, n을 **지수**라고 한다. $a \neq 0$일 때

$$a^0 = 1, \qquad a^{-n} = \frac{1}{a^n}$$

으로 정의하면 모든 정수 m, n과 0이 아닌 실수 a, b에 대하여 **지수 법칙**

$$a^{m+n} = a^m a^n, \qquad (a^m)^n = a^{mn}, \qquad (ab)^n = a^n b^n \tag{7.1}$$

이 성립한다. a^0과 a^{-n}의 정의는 임의로 고른 것이 아니다. 첫째 법칙이 지수 0과 음의 정수에서도 성립하려면 $a^n = a^{0+n} = a^0 a^n$에서 $a^0 = 1$이어야 하고, $a^{-n}a^n = a^0 = 1$에서 a^{-n}은 a^n의 곱셈 역원이어야 한다. 첫째 법칙에서 n을 $-n$으로 바꾸면 $a^m / a^n = a^{m-n}$을 얻으며, 이 식을 쓸 때에는 분모가 0이 아니어야 한다. $a = 0$이면 양의 정수 n에 대해 $0^n = 0$이고, 양의 정수 지수에 한해서는 식 (7.1)이 그대로 성립한다. 그러나 0에는 곱셈 역원이 없으므로 0의 음의 지수 거듭제곱은 정의되지 않는다.

0^0에는 모든 문맥을 관통하는 하나의 약속을 두지 않는다. 다항식과 조합론에서는 빈 곱을 1로 두는 약속과 일관되게 $0^0 = 1$을 사용한다. 다항식 $\sum_{k=0}^{n} c_k x^k$의 $x = 0$에서의 값이 상수항 c_0이 되려면 x^0을 $x = 0$에서도 1로 읽어야 하기 때문이다. 반면 극한에서는 밑과 지수가 모두 0으로 접근한다는 정보만으로 극한값이 정해지지 않으며, 이 현상을 "0^0 꼴의 부정형"이라고 부른다. 예를 들어 $x > 0$이 0으로 갈 때 x^0은 항상 1이고 0^x은 항상 0이며, $(2^{-1/x})^x = 2^{-1}$은 항상 $1/2$이다. 세 식 모두 밑과 지수가 0으로 접근하지만 극한은 서로 다르다. 특정 문맥에서 정한 값과 극한의 불확정성은 서로 다른 문제이다.

> **예제 7.1** $2^{-3} \cdot 2^5 = 2^2 = 4$이고 $(2^{-3})^{-2} = 2^6 = 64$이다. 그러나 $(-2)^{1/2}$은 실수 범위에서 정의되지 않는다. 정수 지수의 법칙을 정수가 아닌 지수로 확장하려면 밑의 범위를 먼저 제한해야 한다.

흔한 오류. -2^2과 $(-2)^2$은 다르다. 거듭제곱은 부호 반전보다 먼저 계산하므로 $-2^2 = -(2^2) = -4$이고 $(-2)^2 = 4$이다. 일반적으로 $(-a)^n$은 n이 짝수이면 a^n, 홀수이면 $-a^n$이다.

7.2 근호의 주값

실수 $x \ge 0$의 **제곱근**(*square root*)은 제곱해서 x가 되는 실수이다. $x > 0$이면 제곱근은 부호가 반대인 두 개가 있지만, 기호 $\sqrt{x}$는 그 가운데 음이 아닌 하나만을 가리킨다. 이처럼 여러 값 가운데 기호가 가리키도록 정한 하나를 **주값**(*principal value*)이라고 한다. 따라서 방정식 $y^2 = 9$의 해는 $y = \pm 3$이지만 $\sqrt{9} = 3$이다. 기호의 값과 방정식의 해집합은 다르다.

양의 정수 n에 대해 $y^n = x$를 만족하는 실수 y를 x의 n**제곱근**이라고 한다. n이 홀수이면 모든 실수 x에 실수 n제곱근이 유일하게 존재하고, 그것을 $\sqrt[n]{x}$로 쓴다. n이 짝수이면 $x < 0$의 실수 n제곱근은 없고, $x \ge 0$에서 기호 $\sqrt[n]{x}$는 음이 아닌 근을 가리킨다. 이때

$$\sqrt[n]{x^n} = \begin{cases} |x|, & n\text{이 짝수}, \\ x, & n\text{이 홀수} \end{cases} \tag{7.2}$$

이다. 특히 $\sqrt{x^2} = |x|$이며, $\sqrt{x^2} = x$는 $x \ge 0$일 때에만 성립한다.

참고 (n제곱근의 존재와 유일성). $0 \le y_1 < y_2$이면 $y_1^n < y_2^n$이므로 음이 아닌 n제곱근은 많아야 하나이다. 존재는 실수의 완비성에서 나온다. $x \ge 0$에 대해 $s = \sup\{t \ge 0 : t^n \le x\}$로 놓으면, $\sqrt{2}$의 존재를 보인 것과 같은 논법으로 $s^n < x$와 $s^n > x$가 모두 모순임을 보일 수 있다(제1권 제6장). n이 홀수이고 $x < 0$이면 $\sqrt[n]{x} = -\sqrt[n]{-x}$이다. 유리수 안에서는 $y^2 = 2$의 해가 없으므로, 근호가 언제나 정의되려면 실수가 필요하다.

근호를 곱이나 합에 나누어 적용하는 계산에도 조건이 붙는다. $a, b \ge 0$이면

$$\sqrt{ab} = \sqrt{a}\,\sqrt{b}, \qquad \sqrt{\frac{a}{b}} = \frac{\sqrt{a}}{\sqrt{b}} \quad (b > 0) \tag{7.3}$$

이다. 실제로 $\sqrt{a}\sqrt{b}$는 음이 아니고 그 제곱이 ab이므로, 음이 아닌 제곱근의 유일성에 의해 $\sqrt{ab}$와 같다. a, b가 모두 음수이면 $ab > 0$이어서 좌변 $\sqrt{ab}$는 정의되지만 우변의 $\sqrt{a}$, $\sqrt{b}$는 실수 범위에서 정의되지 않는다. 이 경우의 올바른 식은 $\sqrt{ab} = \sqrt{-a}\,\sqrt{-b}$이다. 한편 $\sqrt{a+b} = \sqrt{a} + \sqrt{b}$는 일반적으로 거짓이다. $a = b = 1$이 간단한 반례로, 좌변은 $\sqrt{2}$이고 우변은 2이다. $a, b \ge 0$일 때 $(\sqrt{a} + \sqrt{b})^2 = a + b + 2\sqrt{ab} \ge a + b$이므로 일반적으로 성립하는 것은 부등식 $\sqrt{a+b} \le \sqrt{a} + \sqrt{b}$이고, 등호는 $a = 0$ 또는 $b = 0$일 때에만 성립한다.

> **예제 7.2** $\sqrt{50} - \sqrt{8} = 5\sqrt{2} - 2\sqrt{2} = 3\sqrt{2}$이다. 이 과정에서는 $50 = 25 \cdot 2$, $8 = 4 \cdot 2$로 완전제곱인수 25와 4를 분리하고 식 (7.3)을 쓴다. 반면 $\sqrt{x^2 y} = x\sqrt{y}$는 $x \ge 0$, $y \ge 0$이면 성립하지만, $y \ge 0$만 가정하면 정확한 식은 $\sqrt{x^2 y} = |x|\sqrt{y}$이다. 특히 $y > 0$에서는 등식 $\sqrt{x^2 y} = x\sqrt{y}$가 $x \ge 0$일 때에만 성립하고, $y = 0$이면 모든 실수 x에서 양변이 0이다.

7.3 유리 지수와 실수 지수

$a > 0$이고 $m \in \mathbb{Z}$, $n \in \mathbb{N}_{>0}$이면 **유리 지수**의 거듭제곱을

$$a^{m/n} = \sqrt[n]{a^m} = \left(\sqrt[n]{a}\right)^m \tag{7.4}$$

으로 정의한다. 예를 들어 $8^{2/3} = \sqrt[3]{64} = 4$이고 $4^{-3/2} = (\sqrt{4})^{-3} = 1/8$이다. 이 정의는 같은 유리수를 다른 분수로 나타내도 값이 같고, 식 (7.1)의 지수 법칙을 유리 지수에서도 보존한다.

유도 (유리 지수의 정의가 분수 표현에 의존하지 않음). $m/n = m'/n'$, 곧 $mn' = m'n$이라 하고 $u = \sqrt[n]{a^m}$, $v = \sqrt[n']{a^{m'}}$으로 놓는다. u, v는 양수이고

$$u^{nn'} = (u^n)^{n'} = a^{mn'} = a^{m'n} = (v^{n'})^n = v^{nn'}$$

이다. 양수의 nn' 제곱근은 유일하므로 $u = v$이다. 식 (7.4)의 둘째 등호도 같은 방법으로 확인된다. $w = (\sqrt[n]{a})^m$은 양수이고 $w^n = (\sqrt[n]{a})^{mn} = a^m$이기 때문이다.

음의 밑에서는 일부 유리 지수의 실수값을 정의할 수 있지만 일률적인 법칙을 사용하기 어렵다. 예를 들어 $(-8)^{1/3} = -2$라는 실수 세제곱근 해석은 가능하다. 그러나 지수를 $1/3 = 2/6$으로 바꾸어 식 (7.4)의 꼴로 계산하면 $\sqrt[6]{(-8)^2} = \sqrt[6]{64} = 2$가 되어 -2와 다르고, $\left(\sqrt[6]{-8}\right)^2$은 실수 범위에서 정의되지도 않는다. 이 때문에 유리 지수와 실수 지수의 거듭제곱은 양의 밑에서만 정의하는 것이 표준이다.

양의 밑에 대해서는 유리 지수의 값을 연속적으로 확장하여 모든 실수 지수를 정의한다. $a > 1$이면 유리수 $p < q$에 대해 $a^{q-p} > 1$이므로 $a^p < a^q$이고, 실수 x에 대해

$$a^x = \sup\{a^q : q \in \mathbb{Q},\ q \le x\} \tag{7.5}$$

로 정의한다. 이 집합은 공집합이 아니고 위로 유계이므로 완비성 공리에 의해 상한이 존재한다(제1권 제6장). $0 < a < 1$이면 $a^x = (1/a)^{-x}$으로, $a = 1$이면 $1^x = 1$로 정의한다. 예를 들어 $2^{\sqrt{2}}$은 $\sqrt{2} = 1.41421\cdots$의 유리수 근삿값을 지수로 하는 수

$$2^{1.4} = 2.6390\cdots, \quad 2^{1.41} = 2.6573\cdots, \quad 2^{1.414} = 2.6647\cdots$$

의 상한이고, 그 값은 $2.6651\cdots$이다.

이렇게 정의한 **지수함수**(*exponential function*) $x \mapsto a^x$은 $a > 1$이면 증가하고, $0 < a < 1$이면 감소하며, $a = 1$이면 상수함수이다. 모든 실수 x, y와 양수 a, b에 대하여

$$a^{x+y} = a^x a^y, \qquad (a^x)^y = a^{xy}, \qquad (ab)^x = a^x b^x, \qquad a^{-x} = \frac{1}{a^x}, \qquad a^x > 0 \tag{7.6}$$

이 성립한다. 또한 $a \neq 1$이면 $x \mapsto a^x$은 $\mathbb{R}$에서 양의 실수 전체 $(0, \infty)$로 가는 일대일 대응이다. 이러한 연속 확장이 존재하고 지수 법칙을 만족한다는 증명은 실수의 완비성과 극한 이론을 사용한다(제8권 제1장).

> **예제 7.3** $0 < a < 1$일 때 $a^x < a^y$이면 $x > y$이다. 지수 부등식에서 밑이 1보다 작은지 확인하지 않으면 부등호의 방향을 잘못 유지하게 된다. 예를 들어 $(1/2)^x < 1/8 = (1/2)^3$의 해는 $x > 3$이다. 밑이 1보다 큰 $2^x > 8 = 2^3$에서는 부등호의 방향이 그대로 유지되어 같은 해

$x > 3$을 얻는다.

7.4 로그의 정의와 조건

$a > 0$, $a \neq 1$이고 $x > 0$일 때 $a^y = x$를 만족하는 실수 y를 a를 **밑**으로 하는 x의 **로그**(*logarithm*)라 하고 $\log_a x$로 쓴다. x를 **진수**라고 한다. 지수함수 $y \mapsto a^y$이 $\mathbb{R}$에서 $(0,\infty)$로 가는 일대일 대응이므로 그러한 y는 $x > 0$마다 정확히 하나 존재한다. 따라서 로그의 정의역은 $x > 0$이고, 밑의 조건 $a \neq 1$은 $1^y = 1$이 일대일이 아니기 때문에 필요하다. 로그는 지수함수의 역함수이므로

$$a^{\log_a x} = x \quad (x > 0), \qquad \log_a(a^y) = y \quad (y \in \mathbb{R}) \tag{7.7}$$

이다. 특히 $\log_a 1 = 0$, $\log_a a = 1$이다. 예를 들어 $\log_2 8 = 3$, $\log_{10} 0.01 = -2$, $\log_{1/2} 8 = -3$이다. 역함수는 원래 함수의 단조성을 물려받으므로 $\log_a$는 $a > 1$이면 증가하고 $0 < a < 1$이면 감소한다.

실수 범위에서는 $\log_a 0$이나 음수의 로그를 같은 방식으로 정의할 수 없다. 모든 실수 y에 대해 $a^y > 0$이기 때문이다. 복소로그를 도입하면 더 넓은 범위를 다룰 수 있지만, 값이 여럿이 되고 가지를 선택하는 문제가 생기므로 별도의 이론이 된다(제11권 제2장).

명제 7.4 $x, y > 0$, $r \in \mathbb{R}$, $a > 0$, $a \neq 1$이면

$$\log_a(xy) = \log_a x + \log_a y, \qquad \log_a \frac{x}{y} = \log_a x - \log_a y, \qquad \log_a(x^r) = r \log_a x \tag{7.8}$$

이다.

증명. $u = \log_a x$, $v = \log_a y$로 놓으면 $x = a^u$, $y = a^v$이다. 식 (7.6)에 의해 $xy = a^{u+v}$이므로 양변의 로그를 취하면 식 (7.7)에 의해 $\log_a(xy) = u + v$이다. 같은 방식으로 $x/y = a^{u-v}$, $x^r = (a^u)^r = a^{ur}$에서 나머지 두 식을 얻는다. □

흔한 오류. $\log(x+y)$를 $\log x + \log y$로 분리할 수는 없다. 곱의 로그에 대한 법칙을 합에 잘못 적용한 것이다. 예를 들어 밑이 10일 때 $\log_{10}(10+10) = \log_{10} 20$이지만 $\log_{10} 10 + \log_{10} 10 = 2 = \log_{10} 100$이다.

주의 (로그 법칙의 정의역). 식 (7.8)은 $x, y > 0$일 때의 등식이다. x, y가 모두 음수이면 $\log_a(xy)$는 정의되지만 $\log_a x$와 $\log_a y$는 정의되지 않는다. 같은 이유로 $x \neq 0$인 실수에 대한 올바른 식은 $\log_a(x^2) = 2\log_a |x|$이며, $\log_a(x^2) = 2\log_a x$는 $x > 0$에서만 성립한다.

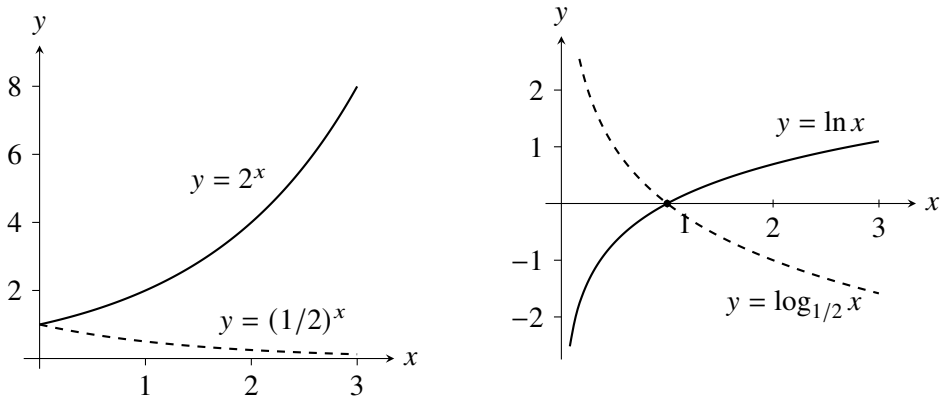

그림 7.1 밑이 1보다 큰지 작은지에 따라 지수함수(왼쪽)와 로그함수(오른쪽)의 단조성이 달라진다. 밑이 1보다 크면 증가하고(실선), 1보다 작으면 감소한다(점선). 모든 로그함수의 그래프는 점 $(1,0)$을 지난다.

7.5 밑 변환과 자연로그

$a, c > 0$, $a, c \neq 1$이고 $x > 0$이면 **밑 변환 공식**

$$\log_a x = \frac{\log_c x}{\log_c a} \tag{7.9}$$

가 성립한다. $y = \log_a x$로 두고 $a^y = x$의 양변에 밑이 c인 로그를 취하면 식 (7.8)의 셋째 법칙에 의해 $y \log_c a = \log_c x$이다. $a \neq 1$이므로 $\log_c a \neq 0$이고, 양변을 $\log_c a$로 나누면 식 (7.9)을 얻는다. 이 공식에서 $x = c$로 놓으면 $\log_a c \cdot \log_c a = 1$이고, 0이 아닌 실수 k에 대하여 $\log_{a^k} x = \frac{1}{k} \log_a x$이다. 따라서 밑이 다른 로그는 서로 상수배이며, 한 가지 밑의 로그만 계산할 수 있으면 다른 모든 밑의 로그를 얻는다.

밑이 e인 로그를 **자연로그**(*natural logarithm*)라 하고 $\ln x$로 쓴다. 밑 변환 공식에 의해

$$\log_a x = \frac{\ln x}{\ln a}, \qquad a^x = e^{x \ln a}$$

이다. 자연로그의 밑 $e = 2.71828\cdots$은 무리수이며 $(1 + 1/n)^n$의 극한으로 정의할 수 있다. 해석학에서는 도함수가 자기 자신과 같은 지수함수 $\exp$의 성질, 또는 적분 $\ln x = \int_1^x \mathrm{d}t/t$를 통해 e와 자연로그를 특징짓는다(제8권 제2장, 제8권 제4장). 이 권의 계산에서는 e의 근삿값보다 로그의 법칙과 정의역이 중요하다.

표기 (밑을 생략한 log). 밑이 10인 로그를 **상용로그**라고 한다. 밑을 적지 않은 $\log x$의 뜻은 분야마다 다르다. 초등 수학과 공학에서는 흔히 상용로그 $\log_{10} x$를, 해석학과 정수론에서는 자연로그 $\ln x$를, 정보 이론과 계산 이론에서는 $\log_2 x$를 가리킨다. 식 (7.9)에 의해 이들은 상수배만큼만 다르지만, 수치를 계산할 때에는 밑을 확인해야 한다.

> **예제 7.5** $2^x = 7$의 실수해는 $x = \log_2 7 = \ln 7 / \ln 2$이다. 이것은 근삿값을 적기 전의 정확한 해이고, 근삿값은 $x \approx 2.807$이다. $2^2 < 7 < 2^3$이고 밑이 1보다 크므로 $2 < x < 3$이라는 범위도 계산기 없이 확인할 수 있다.

역사 (로그의 발명). 로그는 큰 수의 곱셈과 나눗셈을 덧셈과 뺄셈으로 바꾸는 계산 도구로 출발하였다. J. Napier가 1614년에 첫 로그표를 발표하였고, H. Briggs가 밑이 10인 상용로그표를 만들어

천문 계산과 항해에 널리 쓰이게 하였다. 로그를 지수함수의 역함수로 정의하는 오늘날의 관점은 L. Euler의 1748년 저서 『무한해석 입문』(*Introductio in analysin infinitorum*)에서 자리 잡았다.

7.6 로그 방정식에서 정의역을 먼저 정하기

로그나 근호가 들어 있는 방정식은 식이 정의되는 범위를 먼저 정한 뒤에 변형한다. 변형한 식의 정의역이 원래 식의 정의역보다 넓어지면 원래 방정식의 해가 아닌 값이 섞여 들기 때문이다.

> **예제 7.6** $\log_2(x-1)+\log_2(x+1)=3$을 푼다. 두 로그가 모두 정의되려면 $x-1>0$이고 $x+1>0$이어야 하므로 $x>1$이다. 이 범위에서 합을 결합하면 $\log_2(x^2-1)=3$이고, 따라서 $x^2-1=2^3=8$, 곧 $x^2=9$이다. 대수적으로는 $x=\pm 3$이 나오지만 정의역 조건 $x>1$로 $x=3$만 남는다. 실제로 $\log_2 2+\log_2 4=1+2=3$이다.

이 예제에서 음수해는 마지막에 "이상해 보인다"는 이유로 버리는 것이 아니라, 원래 식이 정의되는 범위를 논리적으로 유지함으로써 제거된다. 결합한 식 $\log_2(x^2-1)$은 $x<-1$에서도 정의되므로, $x=-3$은 변형 과정에서 정의역이 넓어져 생긴 값이다. 근호가 있는 식을 제곱하는 계산에서도 비슷한 문제가 생긴다. $A=B$이면 $A^2=B^2$이지만 그 역은 $A=\pm B$까지만 말해 주므로 제곱은 한쪽 방향의 함의이다. 계산의 각 단계가 동치인지 한쪽 함의인지 확인하고, 한쪽 함의를 썼다면 후보를 원래 식에 대입하여 검증한다.

방법 (동치를 유지하는 변형). $a>0$, $a\neq 1$일 때 다음 변형은 동치이다.

$$\begin{aligned}
\log_a f(x)=\log_a g(x) &\iff f(x)=g(x)\ \text{이고}\ f(x)>0,\\
\log_a f(x)=c &\iff f(x)=a^c,\\
\sqrt{f(x)}=g(x) &\iff f(x)=g(x)^2\ \text{이고}\ g(x)\geq 0.
\end{aligned}$$

둘째 줄에서는 $a^c>0$이므로 $f(x)>0$이 자동으로 성립하고, 셋째 줄에서는 $f(x)=g(x)^2\geq 0$이 자동으로 성립한다.

> **예제 7.7** $\sqrt{x+2}=x$에서 좌변이 음이 아니므로 $x\geq 0$이다. 제곱하면 $x+2=x^2$, 곧 $(x-2)(x+1)=0$이므로 후보는 2와 -1이다. $x=-1$은 조건 $x\geq 0$을 어기고, 원래 식에 대입해도 좌변은 1, 우변은 -1이어서 맞지 않는다. $x=2$는 $\sqrt{4}=2$로 원래 식을 만족한다. 따라서 해는 $x=2$이다.

핵심 수식

$$a^{x+y}=a^x a^y,\quad (a^x)^y=a^{xy},\quad (ab)^x=a^x b^x \qquad (a,b>0),$$

$$\sqrt[n]{x^n}=|x|\ \ (n\text{이 짝수}),\qquad \sqrt{ab}=\sqrt{a}\,\sqrt{b} \qquad (a,b\geq 0),$$

$$\log_a(xy)=\log_a x+\log_a y,\quad \log_a(x^r)=r\log_a x \qquad (x,y>0),$$

$$\log_a x=\frac{\log_c x}{\log_c a}=\frac{\ln x}{\ln a} \qquad (a,c>0,\ a,c\neq 1,\ x>0).$$

7.7 문제와 풀이

연습문제 7.8 $\sqrt{(x-3)^2}$을 절댓값 없이 경우를 나누어 나타내어라.

풀이. 식 (7.2)에 의해 $\sqrt{(x-3)^2} = |x-3|$이다. 따라서 $x \geq 3$이면 $x-3$이고, $x < 3$이면 $3-x$이다. 제곱근 기호가 음이 아닌 주값을 가리킨다는 점을 사용한다.

연습문제 7.9 $\log_3(2x-1) = 2$를 풀어라.

풀이. 정의역은 $2x-1 > 0$, 곧 $x > 1/2$이다. 로그의 정의에 의해 $2x-1 = 3^2 = 9$이므로 $x = 5$이며, 이는 정의역 조건을 만족한다.

연습문제 7.10 $\log_{1/2} x > 2$의 해를 구하여라.

풀이. 정의역은 $x > 0$이다. 밑이 1보다 작으므로 $\log_{1/2}$은 감소한다. $2 = \log_{1/2}(1/2)^2 = \log_{1/2}(1/4)$이므로 주어진 부등식은 $x < 1/4$과 같다. 정의역과 합치면 해는 $0 < x < 1/4$이다.

연습문제 7.11 $a, b > 0$일 때 $\sqrt{a} - \sqrt{b} = (a-b)/(\sqrt{a}+\sqrt{b})$를 증명하고, 이 식의 계산상 의미를 설명하여라.

풀이. $(\sqrt{a}-\sqrt{b})(\sqrt{a}+\sqrt{b}) = a-b$이고 $\sqrt{a}+\sqrt{b} > 0$이므로 양변을 $\sqrt{a}+\sqrt{b}$로 나누면 주어진 식을 얻는다.

a와 b가 가까울 때 두 근삿값을 직접 빼면 앞자리의 유효숫자가 상쇄되어 정밀도를 잃을 수 있다. 예를 들어 $a = 1000001$, $b = 1000000$을 유효숫자 일곱 자리로 계산하면 $\sqrt{a} \approx 1000.000$, $\sqrt{b} = 1000.000$이어서 차가 0이 된다. 우변을 쓰면 $1/(1000.000 + 1000.000) = 5.000000 \times 10^{-4}$을 얻고, 참값 $4.99999875\cdots \times 10^{-4}$과의 상대오차는 10^{-6}보다 작다. 우변의 표현은 이런 상황에서 더 안정적인 계산을 주지만, 분자 $a-b$를 정확하게 얻을 수 있는지도 함께 고려해야 한다(제1권 제8장).

연습문제 7.12 $\log_2 3$이 무리수임을 보여라.

풀이. $3 > 1$이므로 $\log_2 3 > 0$이다. $\log_2 3 = p/q$인 양의 정수 p, q가 있다고 가정하면 $2^{p/q} = 3$이고, 양변을 q제곱하면 $2^p = 3^q$이다. 좌변은 짝수이고 우변은 홀수이므로 모순이다. 따라서 $\log_2 3$은 유리수가 아니다.

연습문제 7.13 $\sqrt{x-1} = x-3$을 풀어라.

풀이. 좌변이 음이 아니므로 $x-3 \geq 0$, 곧 $x \geq 3$이어야 한다. 제곱하면 $x-1 = x^2 - 6x + 9$, 곧 $x^2 - 7x + 10 = (x-2)(x-5) = 0$이므로 후보는 2와 5이다. $x = 2$는 조건 $x \geq 3$을 어기며, 대입하면 좌변은 1, 우변은 -1이다. $x = 5$는 $\sqrt{4} = 2 = 5-3$으로 원래 식을 만족한다. 따라서 해는 $x = 5$이다.

참고 (다음 연결). 지수·로그 방정식과 매개변수가 있는 문제는 제2권 제9장에서, 무리방정식은 제2권 제6장에서 체계적으로 다룬다. 지수함수와 로그함수의 그래프와 역함수 관계는 제3권 제1장에서, 미분과 적분은 제8권 제2장와 제8권 제4장에서 다룬다. 복소수 범위의 지수·로그·거듭제곱과 가지의 선택은 제11권 제2장의 주제이다.

제 8 장

근사값, 오차, 수치 표현

개요 근사값의 오차는 참값과 근삿값의 차이를 절대오차와 상대오차로 측정하는 데서 출발하여, 반올림·버림의 오차 상한, 구간 연산으로 오차를 관리하는 방법, 사칙연산에서 오차가 전달되는 식, 이진 부동소수점의 수학적 모형, 상쇄로 인한 유효숫자 손실, 문제의 조건과 알고리즘의 안정성을 구별하는 데까지 이른다. 이 장의 내용은 수치를 직접 계산하거나 측정값을 다루는 모든 응용 수학의 바탕이 된다. 선행 지식: 절댓값과 부등식(제1권 제5장), 자릿수 표현(제1권 제1장)과 로그(제1권 제7장).

8.1 정확한 값과 근삿값

$1/3$, $\sqrt{2}$, π처럼 기호로 지정된 값과 0.333, 1.414, 3.142 같은 유한소수 근삿값은 구별해야 한다. 정확한 식을 가능한 한 오래 유지하면 중간 반올림의 누적을 줄일 수 있다. 다만 어떤 응용에서는 입력 자체가 측정값이므로 처음부터 오차 범위를 포함한 해석이 필요하다.

정의 8.1 (절대오차와 상대오차) 참값 x와 근삿값 $\tilde{x}$에 대한 **절대오차**(*absolute error*)는 $|\tilde{x} - x|$이고, $x \neq 0$일 때 **상대오차**(*relative error*)는

$$\frac{|\tilde{x} - x|}{|x|} \tag{8.1}$$

이다. 상대오차의 분모는 보통 참값의 절댓값으로 정의한다. 실제 문제에서 참값을 모르면 추정값을 분모로 쓰는 대체 기준을 사용할 수도 있지만, 그것은 같은 정의가 아니므로 구분해야 한다.

예제 8.2 1000을 1001로 근사하면 절대오차는 1, 상대오차는 0.001이다. 0.001을 0.002로 근사하면 절대오차는 0.001로 더 작지만 상대오차는 1로 훨씬 크다. “작은 오차”라는 말에는 어떤 척도를 쓰는지 밝혀야 한다.

8.2 반올림과 버림의 오차 상한

십진 소수점 아래 m자리까지 가장 가까운 값으로 반올림하면, 정확히 중간에 있는 경우의 선택 규칙과 무관하게 절대오차는 $\frac{1}{2}10^{-m}$ 이하이다. 소수점 아래의 나머지를 0 방향으로 버리면 절대오차는 10^{-m}보다 작다. 바닥 함수로 아래쪽에 내리는 연산과 0 방향으로 버리는 연산은 음수에서 서로 다르다.

예제 8.3 -1.27을 소수 첫째 자리까지 0 방향으로 버리면 -1.2이고, 0.1 단위로 바닥을 취하면 -1.3이다. 어느 방법을 쓰는지 명시하지 않은 “버림”이라는 표현은 음수에서 모호할 수 있다.

소수점 아래 자릿수와 **유효숫자**(*significant figures*) 수도 다르다. 0.00340은 표기가 의도적으로 마지막 0의 정확성을 표현하는 상황에서 유효숫자 세 자리이다. 그러나 순수한 실수의 값으로

보면 0.0034와 같다. 측정값의 보고 규칙과 수의 수학적 동치를 한 문장 안에서 혼동하지 않아야 한다.

8.3 구간으로 오차를 관리하기

근삿값 하나 대신 참값을 포함하는 구간을 유지하면 부호와 크기를 보장하는 계산을 할 수 있다. $x \in [a, b]$, $y \in [c, d]$이면

$$x + y \in [a + c, b + d], \qquad x - y \in [a - d, b - c] \tag{8.2}$$

이다. 곱은 네 끝점 곱의 최솟값과 최댓값을 이용하여

$$xy \in \big[\min(ac, ad, bc, bd), \max(ac, ad, bc, bd)\big] \tag{8.3}$$

로 둘 수 있다. 나눗셈을 하려면 분모 구간에 0이 포함되지 않는지 확인해야 한다. $0 < c \le d$이면 $1/y \in [1/d, 1/c]$이고 이를 곱셈 규칙과 결합한다.

> **예제 8.4** $x \in [1.9, 2.1]$, $y \in [2.8, 3.2]$이면 $xy \in [5.32, 6.72]$이다. 두 구간이 모두 양수이므로 최소는 두 최솟값의 곱, 최대는 두 최댓값의 곱이다. 부호가 섞인 구간에서는 같은 단순 규칙을 적용할 수 없어 네 곱을 모두 비교해야 한다.

같은 미지수가 여러 번 나타나면 구간 계산이 실제 범위보다 넓어질 수 있다. $x \in [0, 1]$이면 일반 뺄셈 규칙은 $x - x \in [-1, 1]$을 주지만 실제 값은 항상 0이다. 이는 보장된 포함 구간을 얻었다는 것과 최적의 좁은 구간을 얻었다는 것이 다른 문제임을 보여 준다.

8.4 오차의 전달

$\tilde{x} = x + \delta x$, $\tilde{y} = y + \delta y$이면 곱의 오차는 정확히

$$\tilde{x}\tilde{y} - xy = y\,\delta x + x\,\delta y + \delta x\,\delta y$$

이다. 따라서

$$|\tilde{x}\tilde{y} - xy| \le |y||\delta x| + |x||\delta y| + |\delta x||\delta y|. \tag{8.4}$$

마지막 항을 생략하는 것은 오차가 충분히 작다는 가정 아래의 일차 근사이지 항상 정확한 등식이 아니다. 상대오차 형태로는 $x, y \neq 0$일 때 $(1 + \varepsilon_x)(1 + \varepsilon_y) - 1 = \varepsilon_x + \varepsilon_y + \varepsilon_x\varepsilon_y$가 된다.

> **예제 8.5** $x = 20$, $y = 5$의 측정 오차가 각각 $0.1, 0.02$ 이하이면, 식 (8.4)에 의해 곱의 절대오차는 $5 \cdot 0.1 + 20 \cdot 0.02 + 0.1 \cdot 0.02 = 0.902$ 이하이다. 일차항만 사용한 0.9는 매우 가까운 근사이지만 엄밀한 상한으로 쓰려면 이차항을 처리해야 한다.

핵심 수식

$\lvert\tilde{x} - x\rvert, \quad \dfrac{\lvert\tilde{x} - x\rvert}{\lvert x\rvert} \quad (x \neq 0)$	절대오차, 상대오차
$xy \in [\min(ac, ad, bc, bd), \max(ac, ad, bc, bd)]$	구간곱 ($x \in [a, b]$, $y \in [c, d]$)

$\lvert\tilde{x}\tilde{y} - xy\rvert \le \lvert y\rvert\lvert\delta x\rvert + \lvert x\rvert\lvert\delta y\rvert + \lvert\delta x\rvert\lvert\delta y\rvert$	곱의 오차 전달

8.5 이진 부동소수점의 수학적 모형

유한한 저장공간을 사용하는 계산기는 모든 실수를 정확히 저장할 수 없다. 간단한 정규화 모형에서는 부호 s, 유한한 유효숫자열, 정수 지수 e를 사용해

$$(-1)^{s}(1.b_1 b_2 \cdots b_{p-1})_2 \, 2^{e}$$

형태의 수를 나타낸다. 이 식은 원리를 설명하기 위한 모형이며, 실제 **부동소수점**(*floating-point*) 형식에는 지수 범위, 비정규수, 무한대, 비수치값 등에 관한 추가 규칙이 있다(IEEE 754 표준). 같은 지수 구간에서 인접한 표현 가능 수의 간격은 일정하지만, 지수가 커지면 그 간격도 커진다. 따라서 큰 수에 충분히 작은 수를 더하면 반올림 결과가 원래 큰 수와 같을 수 있다. 실수의 정확한 연산에서 성립하는 결합법칙이 유한 정밀도 계산에서는 실패할 수 있는 이유도 여기에 있다.

> **예제 8.6** 십진 유효숫자 세 자리만 저장하고 매번 반올림하는 장난감 모형을 생각하자. $a = 10000$, $b = -10000$, $c = 1$을 선택하면 $b + c = -9999$가 세 자리 반올림으로 -10000이 되어 $a + (b + c) = 0$인 반면 $(a + b) + c = 0 + 1 = 1$이다. 수치 반례를 만들 때도 지정한 정밀도에서 중간값이 실제로 어떻게 반올림되는지 확인해야 한다.

8.6 상쇄와 계산식의 선택

서로 가까운 근삿값의 차를 계산하면 각 값에 있던 작은 절대오차가 결과에 비해 커질 수 있다. 이 현상을 상쇄에 따른 유효숫자 손실, 곧 **파국적 상쇄**(*catastrophic cancellation*)라고 부른다. 상쇄가 일어났다는 이유만으로 결과가 항상 틀린 것은 아니지만, 결과의 상대오차가 나빠질 수 있다.

> **예제 8.7** 큰 양수 x에 대해 $\sqrt{x+1} - \sqrt{x}$를 계산할 때 두 제곱근이 매우 가까워 직접 뺄셈이 불리할 수 있다. 항등식을 이용하면
>
> $$\sqrt{x+1} - \sqrt{x} = \frac{1}{\sqrt{x+1} + \sqrt{x}}$$
>
> 이다. 오른쪽은 가까운 두 수의 뺄셈을 피한다. 다만 $x + 1$ 자체가 저장 과정에서 x와 같아질 정도로 큰 입력이면 입력 표현의 문제도 함께 분석해야 한다. 계산식의 안정성과 입력 정보의 손실은 구별되는 문제이다.

흔한 오류 (상쇄를 피하지 않은 계산식). 두 근삿값이 거의 같을 때 직접 빼는 공식을 그대로 코드로 옮기면, 두 값에 있던 절대오차가 작은 차에 비해 상대적으로 커져 결과의 유효숫자가 크게 줄어든다. 식이 수학적으로 동치라고 해서 유한 정밀도에서도 같은 정확도를 낸다고 가정해서는 안 된다. 상쇄가 일어나는 부분식을 항등식으로 다시 쓸 수 있는지 먼저 확인해야 한다.

8.7 조건과 안정성의 구별

문제의 **조건**(*condition*)은 입력이 조금 바뀔 때 정확한 답이 얼마나 바뀌는지를 말한다. 알고리즘의 **안정성**(*stability*)은 유한 정밀도로 계산한 결과가 그 문제의 정확한 해와 어떤 관계를 갖는지 말한다. 좋은 알고리즘도 정보가 본질적으로 부족한 입력에서 상대적으로 정확한 답을 보장할 수는 없다.

예를 들어 $f(x) = 1/x$에서 x가 0에 가까우면 작은 절대 입력 오차가 큰 절대 출력 오차를 만들 수 있다. 반면 상대오차 관점에서는 $x \neq 0$에서 국소 상대 **조건수**(*condition number*)가 1이라는 다른 진술이 가능하다. 따라서 "나쁜 조건"이라는 평가에도 절대 척도인지 상대 척도인지, 어느 입력 범위인지가 필요하다. 조건수의 미분을 이용한 정의는 수치해석을 다루는 권에서 정식화한다.

8.8 문제와 풀이

> **연습문제 8.8** $\sqrt{2}$를 1.414로 근사할 때 소수 셋째 자리 반올림의 일반 상한만으로 절대오차를 제한하여라.

풀이. 올바르게 반올림했다는 전제 아래 절대오차는 0.0005 이하이다. 실제 오차를 구하려면 더 정확한 $\sqrt{2}$의 값이나 이를 포함하는 구간이 필요하다.

> **연습문제 8.9** $x \in [-2, 3]$, $y \in [1, 4]$일 때 xy의 범위를 구하여라.

풀이. 네 끝점 곱은 $-2, -8, 3, 12$이므로 포함 구간은 $[-8, 12]$이다. 두 끝값이 실제 입력 조합에서 달성되므로 이 경우 정확한 범위이다.

> **연습문제 8.10** $x \in [2, 3]$일 때 일반 구간 규칙으로 구한 $x(1 - x)$의 포함 구간과 실제 범위를 비교하여라.

풀이. $1 - x \in [-2, -1]$이므로 독립적인 구간 곱은 $[-6, -2]$를 준다. 함수 $x - x^2$는 $[2, 3]$에서 감소하고 끝값은 $-2, -6$이므로 이 경우에는 실제 범위와 같다. 같은 미지수가 반복된다고 해서 언제나 과대평가가 엄격하게 발생하는 것은 아니다.

> **연습문제 8.11** 참값이 0일 때 상대오차의 정의를 그대로 사용할 수 없는 이유를 설명하여라.

풀이. 분모 $|x|$가 0이 되어 정의되지 않는다. 이때는 절대오차를 사용하거나 응용에 맞는 다른 기준 척도를 정해야 한다. 기준을 바꾸었다면 이를 명시해야 한다.

참고 (다음 연결). 구간 연산과 오차 전달식은 극한의 ε-논법(제1권 제6장)에서 다루는 부등식 추정과 같은 방식으로 쓰이고, 반올림·버림과 유효숫자는 합동식의 나머지 계산(제9장)에서 정수를 유한 정밀도로 다루는 상황과 대응된다. 부동소수점 산술의 전제가 되는 이진법 자릿수 표현은 제1권 제1장에서 다시 확인할 수 있다.

제 9 장

합동식과 나머지 계산

개요 합동식은 두 정수가 주어진 양의 정수(법)로 나눈 나머지가 같다는 관계를 식으로 다루는 체계이다. 이 장은 합동의 정의와 덧셈·곱셈에 대한 호환성에서 출발하여, 역원이 존재할 조건과 약분이 법을 바꿀 수 있다는 사실, 일차 합동식 $ax \equiv b \pmod{m}$의 해의 개수, 중국인의 나머지 정리의 두 가지 법(서로소인 경우와 일반의 경우), 빠른 거듭제곱 알고리즘, 페르마의 소정리와 그 역이 성립하지 않는 예(위양성)를 차례로 세운다. 선행 지식: 정수의 약수, 최대공약수, 베주 항등식(제1권 제2장).

9.1 합동의 정의

정의 9.1 (합동) 양의 정수 m에 대하여 $m \mid (a-b)$이면 a와 b가 **법**(*modulus*) m에 관해 **합동**(*congruent*)이라고 하고 $a \equiv b \pmod{m}$으로 쓴다.

합동은 두 수가 반드시 같다는 뜻이 아니라, 차이가 m의 배수라는 뜻이다. 나눗셈 알고리즘(제1권 제2장)을 사용하면 두 수를 m으로 나눈 비음수 나머지가 같다는 말과 동치이다. 예를 들어 $17 \equiv 5 \equiv -7 \pmod{12}$이다. 이 세 정수는 서로 다르지만 시계의 12시간 주기처럼 같은 나머지 정보를 갖는다.

합동 관계는 반사성, 대칭성, 추이성을 만족하므로 동치관계이다. 따라서 정수들을 같은 나머지를 갖는 부류로 나눌 수 있다. 법 m에서 대표값은 $0, 1, \dots, m-1$로 선택할 수 있고, 이 부류들의 집합을 $\mathbb{Z}/m\mathbb{Z}$로 쓴다. 이 장에서는 대표 정수로 계산하되, 나중에 몫집합과 몫환의 예로 다시 해석한다(제4권 제7장, 제14권 제4장).

9.2 덧셈과 곱셈의 호환성

명제 9.2 (합동의 연산 호환성) $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$이면 $a+c \equiv b+d \pmod{m}$, $ac \equiv bd \pmod{m}$이다.

증명. $a-b = mu$, $c-d = mv$로 놓으면 합의 차이는 $(a+c)-(b+d) = m(u+v)$이다. 곱의 차이는 $ac - bd = ac - bc + bc - bd = c(a-b) + b(c-d) = m(cu+bv)$이므로 역시 m의 배수이다. $\square$

따라서 거듭제곱, 다항식 계산에서도 중간값을 나머지로 바꾸어도 된다. 이는 매우 큰 정수를 실제로 전부 계산하지 않고도 최종 나머지를 구할 수 있게 한다. 그러나 나눗셈은 별도의 조건이 필요하다.

예제 9.3 $6 \cdot 1 \equiv 6 \cdot 3 \pmod{12}$이지만 $1 \not\equiv 3 \pmod{12}$이다. 양변의 6을 조건 없이 약분하면 틀린 결론이 된다. 실수에서 0이 아닌 수로 나누는 규칙과 합동식에서의 역원 조건은 다르다.

9.3 역원과 약분 조건

정리 9.4 (곱셈 역원의 존재 조건) a가 법 $m \geq 2$에서 곱셈 역원을 가질 필요충분조건은 $\gcd(a, m) = 1$이다.

증명. $ax \equiv 1 \pmod m$이면 $ax + my = 1$인 정수 y가 존재한다. 따라서 a, m의 모든 공약수는 1을 나누므로 최대공약수는 1이다. 역으로 최대공약수가 1이면 베주 항등식 $ax + my = 1$에서 $ax \equiv 1 \pmod m$을 얻는다. □

예제 9.5 법 26에서 7의 **역원**(*multiplicative inverse*)은 15이다. 실제로 $7 \cdot 15 = 105 \equiv 1 \pmod{26}$이다. 유클리드 알고리즘을 역대입하면 $1 = 15 \cdot 7 - 4 \cdot 26$을 얻으므로, 큰 수에서도 역원을 체계적으로 찾을 수 있다.

$ac \equiv bc \pmod m$이고 $\gcd(c, m) = 1$이면 c의 역원을 곱하여 $a \equiv b \pmod m$을 얻는다. 일반적인 c에 대해서는 $d = \gcd(c, m)$이라 할 때 법을 m/d로 줄인 $a \equiv b \pmod{m/d}$가 정확한 결론이다. 약분하면서 법까지 바뀔 수 있다는 점을 기억해야 한다.

9.4 일차 합동식

정리 9.6 (일차 합동식의 해) $ax \equiv b \pmod m$이 해를 가질 필요충분조건은 $d = \gcd(a, m)$이 b를 나누는 것이다. 해가 있으면 법 m에서 서로 다른 해는 정확히 d개이다.

증명. 합동식은 $ax + my = b$인 정수 x, y의 존재와 동치이므로 첫 명제는 디오판토스 방정식의 해 조건이다. $d \mid b$이면 $a' = a/d$, $m' = m/d$, $b' = b/d$로 두어 $a'x \equiv b' \pmod{m'}$로 줄인다. a', m'가 서로소이므로 법 m'에서는 해가 하나이다. 이를 법 m에서 보면 $x_0, x_0 + m', \dots, x_0 + (d-1)m'$의 d개 부류를 얻는다. □

예제 9.7 $6x \equiv 9 \pmod{15}$에서 $d = 3$은 9를 나누므로 해가 있다. $2x \equiv 3 \pmod 5$로 줄이고 2의 역원 3을 곱하면 $x \equiv 4 \pmod 5$이다. 법 15에서 해는 $4, 9, 14$이다. 원식에 대입하면 각각 $24, 54, 84$가 모두 나머지 9를 갖는다.

9.5 중국인의 나머지 정리의 두 법 형태

정리 9.8 (중국인의 나머지 정리, 서로소인 법) 양의 정수 m, n이 서로소이면 임의의 정수 a, b에 대해

$$x \equiv a \pmod m, \qquad x \equiv b \pmod n \tag{9.1}$$

은 법 mn에서 유일한 해를 갖는다.

증명. 베주 항등식 $um + vn = 1$을 택하고 $x = avn + bum$으로 놓는다. 법 m에서는 $vn \equiv 1$이고 $um \equiv 0$이므로 $x \equiv a$이다. 법 n에서도 마찬가지로 $x \equiv b$이다. 두 해의 차이는 m, n으로 모두 나누어지고 두 수가 서로소이므로 mn으로 나누어진다. 따라서 법 mn에서 유일하다. □

역사 (중국인의 나머지 정리의 기원). 서로소인 법에 대한 연립 합동식 문제는 3–5세기경의 중국 수학서 『손자산경』(*Sunzi Suanjing*)에 "몇 개인지 모르는 것을 세는 문제"로 처음 등장한다. 임

의의 법으로 확장한 일반해의 구성법은 1247년 진구소(秦九韶)의 『수서구장』(*Shushu Jiuzhang*)에서 체계적으로 제시되었다.

> **예제 9.9** $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$를 풀자. $x = 2 + 3t$를 두 번째 식에 대입하면 $3t \equiv 1 \pmod 5$이므로 $t \equiv 2 \pmod 5$이다. 따라서 $x \equiv 8 \pmod{15}$이다.

서로소 조건이 없으면 해가 아예 없을 수도 있다. 일반적으로 두 합동식 $x \equiv a \pmod m$, $x \equiv b \pmod n$은 $a \equiv b \pmod{\gcd(m,n)}$일 때 그리고 그때에만 양립하며, 해가 있으면 법 $\operatorname{lcm}(m,n)$에서 유일하다. 예를 들어 $x \equiv 1 \pmod 4$, $x \equiv 2 \pmod 6$은 홀짝 조건이 충돌하여 해가 없다. 법 $2 = \gcd(4,6)$에서 보면 1은 홀수이고 2는 짝수이므로 두 조건을 동시에 만족하는 x는 있을 수 없다.

9.6 빠른 거듭제곱

지수를 이진수로 나타내고 제곱을 반복하면 곱셈 횟수를 줄일 수 있다. 법 m의 계산에서는 매 단계 나머지를 취해 수의 크기도 제한한다. 예를 들어 $13 = 8 + 4 + 1$이므로 $a^{13} = a^8 a^4 a$이고, a^2, a^4, a^8은 연속해서 제곱하여 구한다.

> **예제 9.10** 7^{13}을 11로 나눈 나머지를 구하자.
>
> $$7^2 \equiv 5, \qquad 7^4 \equiv 3, \qquad 7^8 \equiv 9 \pmod{11}.$$
>
> 따라서 $7^{13} \equiv 9 \cdot 3 \cdot 7 = 189 \equiv 2 \pmod{11}$이다. 실제 거듭제곱의 모든 자릿수를 쓸 필요가 없다.

9.7 페르마의 소정리와 적용 한계

> **정리 9.11 (페르마의 소정리)** 소수 p와 $p \nmid a$인 정수 a에 대하여 $a^{p-1} \equiv 1 \pmod p$이다.

증명. 법 p에서 $a, 2a, \dots, (p-1)a$는 모두 0이 아니고 서로 다른 나머지를 갖는다. 두 항의 나머지가 같으면 $a(i-j) \equiv 0$이고 a의 역원을 곱해 $i \equiv j$를 얻으므로, 이는 $1 \le i, j \le p-1$에서 $i = j$를 뜻한다. 따라서 이 나머지들은 $1, \dots, p-1$의 순열이다. 모두 곱하면 $a^{p-1}(p-1)! \equiv (p-1)! \pmod p$이며, 각 인수가 역원을 가지므로 $(p-1)!$을 약분한다. □

역사 (페르마의 소정리). 피에르 드 페르마(Pierre de Fermat)는 1640년 프레니클 드 베시(Frénicle de Bessy)에게 보낸 편지에서 이 정리를 증명 없이 적었다. 최초로 출판된 증명은 1736년경 레온하르트 오일러(Leonhard Euler)의 것이며, 오일러는 이후 1760년에 법이 소수가 아닌 경우로 일반화한 정리도 증명하였다(제15권 제1장).

이 정리는 소수인 경우의 성질이지, 어떤 밑 하나에 대해 합동식이 성립하면 그 법이 소수라는 역명제가 아니다. 예를 들어 $341 = 11 \cdot 31$은 합성수지만 $2^{10} = 1024 \equiv 1 \pmod{341}$이므로 $2^{340} \equiv 1 \pmod{341}$이다. 소수 판정에서 이러한 위양성을 처리하려면 더 정교한 논리가 필요하다.

주의 (페르마 소정리의 역을 쓰는 오류). $a^{n-1} \equiv 1 \pmod n$이 특정한 밑 a 하나에 대해 성립한다고 해서 n이 소수라고 단정할 수 없다. 341은 밑 2에 대해 이 식이 성립하는 합성수이며, 이러한 합성수를 **페르마 유사소수**(*Fermat pseudoprime*)라고 한다. 여러 밑에 대해 검사해도 n과 서로소인

모든 밑에서 속는 카마이클 수가 존재하므로, 이 검사만으로는 소수성을 확정적으로 증명할 수 없다.

핵심 수식

$a \equiv b \pmod{m} \iff m \mid (a-b)$	합동의 정의
$ax \equiv b \pmod{m}$ 의 해 조건: $\gcd(a,m) \mid b$, 해 개수 $\gcd(a,m)$	일차 합동식
$a^{p-1} \equiv 1 \pmod{p}$ (p 소수, $p \nmid a$)	페르마의 소정리

9.8 문제와 풀이

연습문제 9.12 $8x \equiv 6 \pmod{14}$의 모든 해를 법 14에서 구하여라.

풀이. 최대공약수는 2이고 6을 나눈다. $4x \equiv 3 \pmod{7}$로 줄인 뒤 4의 역원 2를 곱하면 $x \equiv 6 \pmod{7}$이다. 따라서 법 14의 해는 $6, 13$이다.

연습문제 9.13 $x \equiv 1 \pmod{4}$, $x \equiv 3 \pmod{7}$의 최소 비음수 해를 구하여라.

풀이. $x = 1+4t$를 대입하면 $4t \equiv 2 \pmod{7}$이다. 역원 2를 곱해 $t \equiv 4 \pmod{7}$을 얻으므로 $x \equiv 17 \pmod{28}$이고 답은 17이다.

연습문제 9.14 3^{100}의 마지막 십진 자릿수를 구하여라.

풀이. 법 10에서 거듭제곱의 나머지는 $3, 9, 7, 1$의 주기를 갖는다. 100은 4의 배수이므로 마지막 자릿수는 1이다. 주기를 실제로 확인하거나 $3^4 \equiv 1 \pmod{10}$을 이용한다.

연습문제 9.15 자연수 a, b에 대해 $a \equiv b \pmod{9}$이면 두 수의 십진 자릿수 합이 법 9에서 같다는 검산 원리를 설명하여라.

풀이. $10 \equiv 1 \pmod{9}$이므로 $n = \sum a_j 10^j \equiv \sum a_j \pmod{9}$이다. 따라서 자릿수 합은 나머지를 보존한다. 하지만 나머지가 일치한다고 수가 같은 것은 아니므로 이 검사는 일부 오류만 검출한다.

참고 (다음 연결). 법 m에서의 역원과 일차 합동식은 제15권 제1장에서 오일러 함수·원시근과 함께 더 깊이 다루고, 합동 관계를 몫집합 $\mathbb{Z}/m\mathbb{Z}$와 몫환으로 재해석하는 일은 제4권 제7장과 제14권 제4장의 주제이다. 페르마의 소정리를 밑이 서로소가 아닌 경우까지 일반화한 오일러 정리도 제15권 제1장에서 다룬다.

제 10 장

복소수의 첫 구조

개요 복소수는 실수의 순서쌍에 특정한 덧셈과 곱셈을 주어 만든 수 체계이며, $i^2 = -1$을 만족하는 원소 i를 덧붙여 모든 원소를 $a + bi$ 꼴로 표현한다. 이 장은 복소수의 대수적 정의와 사칙연산에서 출발하여 켤레와 절댓값의 성질, 복소수에는 실수와 같은 전순서를 줄 수 없다는 사실, 극형식을 이용한 곱셈·거듭제곱·거듭제곱근의 기하학적 해석, 그리고 실수 계수 다항식의 켤레근 성질을 차례로 세운다. 선행 지식: 실수의 체 연산과 이차방정식의 판별식, 평면 좌표, 삼각함수의 덧셈 정리와 기하학적 정의.

10.1 복소수의 정의와 기본 연산

정의 10.1 (복소수) **복소수**(*complex number*)는 실수 순서쌍 (a, b) 전체의 집합에 덧셈과 곱셈을

$$(a, b) + (c, d) = (a + c,\ b + d), \qquad (a, b)(c, d) = (ac - bd,\ ad + bc) \tag{10.1}$$

로 정의하여 얻는 수이다. 실수 a를 $(a, 0)$과 동일시하고 $i = (0, 1)$로 쓰면, 식 (10.1)의 곱셈에서 $i^2 = (0,1)(0,1) = (-1, 0) = -1$이고 $(a, b) = (a, 0) + (b, 0)(0, 1) = a + bi$이다. 따라서 모든 복소수는 $a + bi$ $(a, b \in \mathbb{R})$ 꼴로 유일하게 표현된다. 복소수 전체의 집합을 $\mathbb{C}$로 쓴다.

식 (10.1)로 정의한 연산은 복소수를 "불가능한 제곱근을 가정한 기호"가 아니라, 실수쌍 위에 구체적으로 계산할 수 있는 체(*field*)의 구조로 만들어 준다는 점이 이 구성의 요점이다. 덧셈과 곱셈은 실수와 마찬가지로 결합·교환·분배법칙을 만족하며, 이는 정의를 성분별로 전개하면 바로 확인된다. $a + bi$ 표기를 쓰면 곱셈은

$$(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i$$

이고, $i^2 = -1$만 적용하면 식 (10.1)과 같은 결과를 얻는다. 이후로는 성분 표기 (a, b) 대신 $a + bi$ 표기만 사용한다.

복소수 $z = a + bi$ $(a, b \in \mathbb{R})$의 **실수부**(*real part*)와 **허수부**(*imaginary part*)는 각각

$$\operatorname{Re} z = a, \qquad \operatorname{Im} z = b$$

이다. 허수부는 bi가 아니라 실수 b 자신이라는 표기 관례에 주의한다. 두 복소수 $a + bi$와 $c + di$가 같을 필요충분조건은 $a = c$이고 $b = d$인 것, 곧 실수부와 허수부가 각각 같은 것이다. 이는 $\{1, i\}$가 $\mathbb{R}^2$의 기저를 이룬다는 사실과 같은 내용이다.

예제 10.2 $(2 + 3i)(4 - i) = 8 - 2i + 12i - 3i^2 = 8 + 10i + 3 = 11 + 10i$이다. 실수의 분배법칙처럼 전개한 뒤 $i^2 = -1$을 적용하면 정의와 같은 계산을 얻는다. i의 거듭제곱은 $i, -1, -i, 1$의 네 값을 주기적으로 반복하므로(주기 4), $n = 4q + r$ $(0 \le r < 4)$이면 $i^n = i^r$이다. $2026 = 4 \cdot 506 + 2$이므로 $i^{2026} = i^2 = -1$이다.

10.2 켤레와 절댓값

정의 10.3 (켤레와 절댓값) $z = a + bi$ $(a, b \in \mathbb{R})$의 **켤레**(*complex conjugate*)는 $\overline{z} = a - bi$이고, **절댓값**(*modulus*)은 $|z| = \sqrt{a^2 + b^2}$이다.

명제 10.4 (켤레와 절댓값의 기본 성질) 임의의 $z, w \in \mathbb{C}$에 대하여

$$z\overline{z} = |z|^2, \qquad \overline{z+w} = \overline{z} + \overline{w}, \qquad \overline{zw} = \overline{z}\,\overline{w} \tag{10.2}$$

이다. $z \neq 0$이면 $|z|^2 > 0$이므로

$$\frac{1}{z} = \frac{\overline{z}}{|z|^2} \tag{10.3}$$

이고, 이 식으로 0이 아닌 복소수의 곱셈 역원이 존재함을 확인할 수 있다.

증명. $z = a + bi$, $w = c + di$로 쓰면 $z\overline{z} = (a+bi)(a-bi) = a^2 + b^2 = |z|^2$이다. $\overline{z+w} = \overline{(a+c)+(b+d)i} = (a+c)-(b+d)i = (a-bi)+(c-di) = \overline{z}+\overline{w}$이다. $\overline{zw} = \overline{(ac-bd)+(ad+bc)i} = (ac-bd)-(ad+bc)i$이고, $\overline{z}\,\overline{w} = (a-bi)(c-di) = (ac-bd)-(ad+bc)i$이므로 둘은 같다. 식 (10.3)은 $z\overline{z} = |z|^2 \neq 0$의 양변을 $z\,|z|^2$로 나누면 바로 얻는다. □

예제 10.5 $\dfrac{1+2i}{3-i}$는 분자와 분모에 $3-i$의 켤레 $3+i$를 곱해

$$\frac{1+2i}{3-i} = \frac{(1+2i)(3+i)}{(3-i)(3+i)} = \frac{3+i+6i+2i^2}{9+1} = \frac{1+7i}{10}$$

로 구한다. 분모를 실수로 바꾸는 과정은 단순한 계산 요령이 아니라 식 (10.3)에 담긴 켤레를 이용한 역원 공식 자체이다.

명제 10.6 (절댓값의 곱셈성과 삼각부등식) 임의의 $z, w \in \mathbb{C}$에 대하여

$$|zw| = |z|\,|w| \tag{10.4}$$

이고, 삼각부등식

$$|z+w| \le |z| + |w| \tag{10.5}$$

이 성립한다.

증명. 식 (10.2)에 의해 $|zw|^2 = (zw)\overline{(zw)} = zw\,\overline{z}\,\overline{w} = (z\overline{z})(w\overline{w}) = |z|^2\,|w|^2$이고, 양변이 음이 아니므로 제곱근을 취하면 식 (10.4)을 얻는다.

삼각부등식은 $|z+w|^2$을 직접 전개하여 보인다.

$$|z+w|^2 = (z+w)\overline{(z+w)} = z\overline{z} + z\overline{w} + w\overline{z} + w\overline{w} = |z|^2 + 2\,\mathrm{Re}(z\overline{w}) + |w|^2 .$$

$\mathrm{Re}(z\overline{w}) \le |z\overline{w}| = |z|\,|\overline{w}| = |z|\,|w|$이므로

$$|z+w|^2 \le |z|^2 + 2\,|z|\,|w| + |w|^2 = (|z| + |w|)^2$$

이고, 양변이 음이 아니므로 제곱근을 취하면 식 (10.5)을 얻는다. □

참고. 식 (10.5)은 평면 벡터 (a,b)의 길이에 관한 삼각부등식과 같은 내용이다. 등호는 $z=0$이거나 $w=0$이거나, $z,w\neq 0$이고 $\operatorname{Re}(z\overline{w})=|z|\,|w|$일 때, 곧 $z\overline{w}$가 음이 아닌 실수일 때 성립한다.

역사 (복소수 개념의 형성). Rafael Bombelli는 저서 *L'Algebra*(1572)에서 삼차방정식의 카르다노 공식이 실근을 주는 경우에도 계산 과정에 음수의 제곱근이 나타나는 *casus irreducibilis*를 다루며 이런 양을 형식적으로 계산하는 규칙을 처음으로 체계화했다. Leonhard Euler는 $\sqrt{-1}$을 가리키는 기호 i를 사용했고, Carl Friedrich Gauss는 1831년의 논문에서 "복소수"(독일어 *komplexe Zahl*)라는 용어를 쓰고 평면 좌표에 의한 기하학적 표현을 정착시켰다. 복소수를 평면의 점으로 나타내는 착상 자체는 Caspar Wessel(1799)과 Jean-Robert Argand(1806)가 Gauss보다 먼저 독립적으로 제시했다.

10.3 복소수에는 실수와 같은 순서를 줄 수 없다

명제 10.7 복소수 전체 $\mathbb{C}$에 덧셈 및 양수의 곱셈과 호환되는(곧 체의 순서 공리를 만족하는) 전순서를 확장할 수 없다.

증명. 그러한 순서가 있는 체에서는 모든 비영 원소의 제곱이 양수이다. 실제로 $x>0$이면 양수끼리의 곱이 양수이므로 $x^2>0$이고, $x<0$이면 $-x>0$이므로 $x^2=(-x)^2>0$이다. $i\neq 0$이므로 이 성질을 i에 적용하면 $i^2>0$이어야 한다. 그러나 정의에 의해 $i^2=-1<0$이므로 모순이다. $\square$

따라서 $z<w$라는 표현은 별도의 정의 없이는 실수의 부등식처럼 사용할 수 없다. 대신 $|z|<|w|$처럼 절댓값을 비교하거나 $\operatorname{Re}z<\operatorname{Re}w$처럼 실수부를 비교할 수 있다. 복소해석에서도 부등식의 양변은 보통 실수인 크기나 노름이다.

10.4 극형식과 회전

정의 10.8 (극형식) $z\neq 0$이면 평면 좌표 $(\operatorname{Re}z,\operatorname{Im}z)$를 극좌표로 바꾸어

$$z=r(\cos\theta+i\sin\theta),\qquad r=|z|>0 \tag{10.6}$$

으로 표현할 수 있다. 이를 z의 **극형식**이라 하고, 각 θ를 z의 **편각**(*argument*)이라 한다.

편각 θ는 2π의 정수배만큼 바꾸어도 $\cos,\sin$의 값이 같으므로 같은 복소수를 나타낸다. 따라서 편각은 원래 여러 값을 가지며, 특정한 **주편각**을 선택할 때에는 그 범위(흔히 $(-\pi,\pi]$)를 명시해야 한다.

삼각함수의 덧셈정리 $\cos(\alpha+\beta)=\cos\alpha\cos\beta-\sin\alpha\sin\beta$, $\sin(\alpha+\beta)=\sin\alpha\cos\beta+\cos\alpha\sin\beta$를 사용하면

$$\begin{aligned}&\big(r_1(\cos\alpha+i\sin\alpha)\big)\big(r_2(\cos\beta+i\sin\beta)\big)\\&\quad=r_1r_2\big[(\cos\alpha\cos\beta-\sin\alpha\sin\beta)+i(\sin\alpha\cos\beta+\cos\alpha\sin\beta)\big]\\&\quad=r_1r_2\big(\cos(\alpha+\beta)+i\sin(\alpha+\beta)\big)\end{aligned}\tag{10.7}$$

를 얻는다. 극형식의 곱셈은 길이를 곱하고 각도를 더하는 연산이다. 특히 절댓값이 1인 복소수의 곱셈은 평면의 회전이며, $i=\cos(\pi/2)+i\sin(\pi/2)$를 곱하면 반시계 방향으로 90도 회전한다.

10.5 거듭제곱과 거듭제곱근

정리 10.9 (드무아브르 공식) 정수 n에 대하여

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta) \tag{10.8}$$

이다.

증명. $n \geq 1$에 대해서는 n에 관한 귀납법으로 보인다. $n = 1$이면 양변이 같다. $n = k$에서 식 (10.8)이 성립한다고 가정하면, 식 (10.7)을 $r_1 = r_2 = 1$, $\alpha = k\theta$, $\beta = \theta$에 적용하여

$$\begin{aligned}(\cos\theta + i\sin\theta)^{k+1} &= (\cos\theta + i\sin\theta)^k(\cos\theta + i\sin\theta)\\ &= \big(\cos(k\theta) + i\sin(k\theta)\big)(\cos\theta + i\sin\theta)\\ &= \cos\big((k+1)\theta\big) + i\sin\big((k+1)\theta\big)\end{aligned}$$

을 얻으므로 모든 양의 정수에서 성립한다. $n = 0$이면 양변이 1이다. $n < 0$이면 $n = -m$ $(m > 0)$으로 쓰고 식 (10.3)을 $|z| = 1$인 $z = \cos\theta + i\sin\theta$에 적용하면 $z^{-1} = \overline{z} = \cos\theta - i\sin\theta = \cos(-\theta) + i\sin(-\theta)$이므로, 이미 증명한 양의 정수 경우를 z^{-1}과 지수 m에 적용하여

$$z^n = (z^{-1})^m = \cos(-m\theta) + i\sin(-m\theta) = \cos(n\theta) + i\sin(n\theta)$$

를 얻는다. □

$z = r(\cos\theta + i\sin\theta) \neq 0$의 n**제곱근**은 $n \geq 1$일 때

$$w_k = r^{1/n}\left(\cos\frac{\theta + 2\pi k}{n} + i\sin\frac{\theta + 2\pi k}{n}\right), \qquad k = 0, 1, \dots, n-1 \tag{10.9}$$

이다. 실제로 식 (10.8)에 의해 $w_k^n = r\big(\cos(\theta + 2\pi k) + i\sin(\theta + 2\pi k)\big) = r(\cos\theta + i\sin\theta) = z$이므로 w_k는 모두 z의 n제곱근이다. $k = 0, \dots, n-1$에 대응하는 각 $(\theta + 2\pi k)/n$들의 서로 다른 두 값의 차이는 $2\pi/n$의 0이 아닌 정수배이면서 크기가 2π 미만이므로 2π의 정수배가 될 수 없고, 따라서 $w_0, \dots, w_{n-1}$은 서로 다른 n개의 복소수이다. n차 다항식 $X^n - z$는 복소수 범위에서 서로 다른 근을 최대 n개 가지므로(제2권 제2장) 이들이 n제곱근의 전부이다. 이들은 평면에서 원점이 중심이고 반지름이 $r^{1/n}$인 원 위에 각도 $2\pi/n$ 간격으로 균등하게 배치된다. 원래 편각 θ를 2π의 다른 정수배만큼 바꾼 대표로 택해도, k의 값이 그에 맞추어 순환할 뿐 해들의 집합 전체는 바뀌지 않는다.

예제 10.10 $w^3 = 1$의 해는 $1 = \cos 0 + i\sin 0$, $-\dfrac{1}{2} + \dfrac{\sqrt{3}}{2}i = \cos\dfrac{2\pi}{3} + i\sin\dfrac{2\pi}{3}$, $-\dfrac{1}{2} - \dfrac{\sqrt{3}}{2}i = \cos\dfrac{4\pi}{3} + i\sin\dfrac{4\pi}{3}$이다. 직접 검산하면 $\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)^2 = \frac{1}{4} - \frac{\sqrt{3}}{2}i - \frac{3}{4} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$이고, 이 값에 다시 $-\frac{1}{2} + \frac{\sqrt{3}}{2}i$를 곱하면 $\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = \frac{1}{4} + \frac{3}{4} = 1$이 되어 확인된다. 실수에서는 세제곱근이 1 하나뿐이지만 복소수에서는 서로 다른 세 근을 얻는다. 이 차이는 복소수에서의 방정식 해석에서 중요하다.

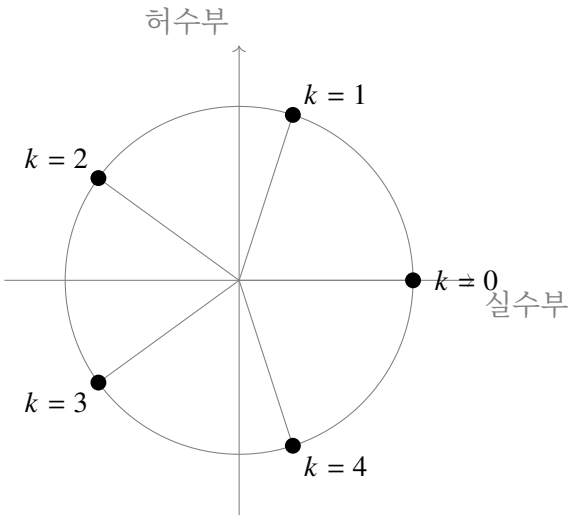

그림 10.1 방정식 $z^5 = 1$의 다섯 근은 단위원 위에 각도 $2\pi/5$ 간격으로 균등하게 배치된다.

10.6 실수 계수 다항식의 켤레근

명제 10.11 실수 계수 다항식 p에 대하여 $p(z) = 0$이면 $p(\overline{z}) = 0$이다.

증명. 실수는 켤레를 취해도 바뀌지 않으므로, p의 계수가 모두 실수이면 식 (10.2)의 켤레가 합과 곱을 보존하는 성질에 의해 $p(\overline{z}) = \overline{p(z)} = \overline{0} = 0$이다. $\square$

실수가 아닌 근은 따라서 켤레 쌍으로 나타난다. 예를 들어 $x^2 - 2x + 5 = 0$의 근은 근의 공식으로 구하면 $x = 1 \pm 2i$이고, 두 일차인수의 곱은

$$(x - 1 - 2i)(x - 1 + 2i) = (x-1)^2 - (2i)^2 = (x-1)^2 + 4 = x^2 - 2x + 5$$

라는 실수 계수 이차식이다. 계수가 복소수이면 켤레근 성질을 그대로 적용할 수 없다. $p(z) = z - i$는 $p(i) = 0$이지만 $p(\overline{i}) = p(-i) = -2i \neq 0$이므로 간단한 반례이다.

10.7 문제와 풀이

연습문제 10.12 $|3 - 4i|$, $\overline{3 - 4i}$, $1/(3 - 4i)$를 구하여라.

풀이. $|3 - 4i| = \sqrt{9 + 16} = 5$, $\overline{3 - 4i} = 3 + 4i$이다. 식 (10.3)에 의해 $1/(3 - 4i) = (3 + 4i)/25$이다. 검산: $(3 - 4i) \cdot \dfrac{3 + 4i}{25} = \dfrac{9 + 16}{25} = 1$이다.

연습문제 10.13 $z^2 = -4$와 $|z| = 2$의 해 집합이 어떻게 다른지 설명하여라.

풀이. 첫 방정식의 해는 $z = \pm 2i$ 두 개이다. 두 번째 식은 원점을 중심으로 반지름이 2인 원 위의 모든 복소수이다. 제곱의 값을 고정하는 조건과 절댓값을 고정하는 조건은 서로 다른 정보이며, 전자가 후자보다 훨씬 강한 제약이다.

연습문제 10.14 복소수 z가 실수일 필요충분조건이 $z = \overline{z}$임을 보여라.

풀이. $z = a + bi$로 쓰면 $z = \bar{z}$는 $a + bi = a - bi$, 곧 $2bi = 0$과 동치이고 이는 $b = 0$과 동치이다. 따라서 $z = \bar{z}$인 경우와 허수부가 0인 경우, 곧 z가 실수인 경우가 정확히 일치한다.

연습문제 10.15 $1 + i$의 네제곱을 대수적 방법과 극형식 방법으로 각각 구하여라.

풀이. 대수적으로는 $(1+i)^2 = 1 + 2i + i^2 = 2i$이므로 $(1+i)^4 = (2i)^2 = -4$이다. 극형식으로는 $|1+i| = \sqrt{2}$, 편각은 $\pi/4$이므로 $1 + i = \sqrt{2}(\cos(\pi/4) + i\sin(\pi/4))$이고, 식 (10.8)에 의해 $(1+i)^4 = (\sqrt{2})^4(\cos\pi + i\sin\pi) = 4(-1+0) = -4$이다. 두 방법의 결과가 일치한다.

제 11 장

유한한 합과 계산 구조

개요 유한합은 유한히 많은 수의 덧셈을 하나의 식으로 묶어 나타내는 표기이다. 이 장은 시그마 기호의 규칙에서 출발하여 등차수열과 등비수열의 합, 망원경 합, 거듭제곱의 합 공식, 계승과 소인수 지수의 계산을 차례로 다룬다. 모든 공식은 유한한 항의 수에 대한 등식이며, 무한급수로 넘어갈 때 추가로 필요한 수렴 조건과는 구별한다. 선행 지식: 거듭제곱, 분배법칙, 기본 부등식.

11.1 시그마 기호와 인덱스

기호 $\sum_{k=a}^{b} u_k$는 $u_a + u_{a+1} + \cdots + u_b$를 줄여 쓴 것이다. 첨자 k는 합 안에서만 쓰이는 **묶인 변수**(*bound variable*)이므로, 다른 기호 j로 일관되게 바꾸어도 값은 같다. 반면 묶인 변수를 합 바깥에서 이미 쓰고 있는 기호와 충돌하게 바꾸면 의미가 달라질 수 있으므로 피해야 한다.

유한합은 다음 선형성을 만족한다.

$$\sum_{k=1}^{n} (a u_k + b v_k) = a \sum_{k=1}^{n} u_k + b \sum_{k=1}^{n} v_k. \tag{11.1}$$

이 선형성은 유한한 분배법칙 $a(x+y) = ax + ay$를 n번 반복하여 얻는다. 일반적으로 합의 곱은 각 항끼리 같은 첨자로 곱한 합과 다르다.

$$\left(\sum_{i=1}^{n} a_i \right) \left(\sum_{j=1}^{m} b_j \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j. \tag{11.2}$$

식 (11.2)의 오른쪽에는 가능한 모든 첨자 쌍 (i, j)에 대응하는 항이 나타난다.

흔한 오류 (교차항 누락). $n = m$일 때 왼쪽 식을 $\sum_i a_i b_i$로 줄여 쓰는 것은 오류이다. 식 (11.2)의 오른쪽에는 $i = j$인 n개의 항뿐 아니라 $i \neq j$인 교차항 $n^2 - n$개도 포함되어 있으며, 이들을 누락하면 일반적으로 다른 값을 얻는다. 예를 들어 $a_i = b_i = 1$ $(i = 1, 2)$이면 왼쪽은 $2 \cdot 2 = 4$이지만 $\sum_i a_i b_i = 1 + 1 = 2$에 불과하다.

11.2 등차수열의 합

초항이 a, 공차가 d인 등차수열의 k번째 항은 $a + (k-1)d$이다.

명제 11.1 (등차수열의 합) 첫 n항의 합은

$$S_n = \frac{n}{2} \{ 2a + (n-1)d \} = \frac{n}{2} (a + a_n) \tag{11.3}$$

이다. 여기서 $a_n = a + (n-1)d$는 n번째 항이다.

증명. 합을 정방향과 역방향으로 나란히 적어 더한다.

$$S_n = a + (a+d) + \cdots + (a+(n-1)d),$$
$$S_n = (a+(n-1)d) + (a+(n-2)d) + \cdots + a.$$

두 식을 같은 자리끼리 더하면 각 쌍의 합이 $2a+(n-1)d$로 모두 같고, 쌍이 n개이므로 $2S_n = n\{2a+(n-1)d\}$이다. 양변을 2로 나누면 식 (11.3)을 얻는다. □

예제 11.2 $7, 11, 15, \ldots$의 첫 20항의 합을 구하자. $a=7$, $d=4$이므로 식 (11.3)에 의해

$$S_{20} = \frac{20}{2}\{2\cdot 7 + 19\cdot 4\} = 10(14+76) = 10\cdot 90 = 900.$$

마지막 항은 $a_{20} = 7+19\cdot 4 = 83$이고, 첫 항과 마지막 항의 평균 $(7+83)/2 = 45$에 항 수 20을 곱해도 900으로 같은 값을 얻는다.

11.3 등비수열의 합과 예외

초항이 a, 공비가 r인 등비수열의 첫 n항의 합은 $S_n = a + ar + \cdots + ar^{n-1}$이다.

명제 11.3 (등비수열의 합) $r \neq 1$이면

$$S_n = a\,\frac{1-r^n}{1-r} \tag{11.4}$$

이다.

증명. $S_n = a + ar + \cdots + ar^{n-1}$의 양변에 r을 곱하면 $rS_n = ar + ar^2 + \cdots + ar^n$이다. 두 식을 빼면 중간 항이 모두 상쇄되어

$$(1-r)S_n = S_n - rS_n = a - ar^n$$

을 얻고, $r \neq 1$이므로 양변을 $1-r$로 나누면 식 (11.4)을 얻는다. □

$r = 1$일 때는 분모를 0으로 만드는 식 (11.4)을 사용하지 말고 $S_n = na$로 따로 계산한다. r이 음수여도 식 (11.4)은 그대로 성립한다.

예제 11.4

$$1 - 2 + 4 - 8 + 16 = \frac{1-(-2)^5}{1-(-2)} = \frac{1-(-32)}{3} = \frac{33}{3} = 11.$$

공비가 음수인 교대 부호의 합에서는 각 항의 크기만 더하면$(1+2+4+8+16=31)$ 전혀 다른 결과를 얻으므로, 부호를 지킨 식 (11.4)을 적용해야 한다.

참고 (무한등비급수로의 확장). 무한 등비급수 $\sum_{k=0}^{\infty} ar^k$로 넘어갈 때에는 추가 조건이 필요하다. $|r|<1$이면 $r^n \to 0$이므로 식 (11.4)에서 극한을 취해 $\sum_{k=0}^{\infty} ar^k = a/(1-r)$을 얻는다. $|r| \geq 1$에서는 $a=0$인 자명한 예외를 제외하면 이 극한이 존재하지 않으므로 같은 공식을 일반적인 수렴 공식으로 사용할 수 없다. 유한합의 항등식 식 (11.4)과 무한급수의 수렴 정리(제8권 제6장)는 서로 다른 종류의 명제이므로 구별해야 한다.

11.4 망원경 합

항들을 전개했을 때 중간 항이 상쇄되는 합을 **망원경 합**(*telescoping sum*)이라 한다. 기본 구조는

$$\sum_{k=1}^{n} (u_k - u_{k+1}) = u_1 - u_{n+1} \tag{11.5}$$

이다. 이는 각 항을 나란히 적으면 $u_2, u_3, \dots, u_n$이 한 번은 $+$ 부호로, 한 번은 $-$ 부호로 나타나 모두 상쇄되기 때문이다. 겉보기에 복잡한 합도 각 항을 차의 형태로 바꿀 수 있는지 찾으면 계산이 단순해진다.

> **예제 11.5** $\dfrac{1}{k(k+1)} = \dfrac{1}{k} - \dfrac{1}{k+1}$이므로 식 (11.5)에 $u_k = 1/k$를 대입하여
>
> $$\sum_{k=1}^{n} \frac{1}{k(k+1)} = 1 - \frac{1}{n+1} = \frac{n}{n+1}$$
>
> 을 얻는다. 유한합을 정확히 구한 뒤 $n \to \infty$로 보내면 무한합은 1이다. 처음부터 무한히 많은 항을 임의로 재배열하지 않고, 이처럼 유한한 부분합으로 논증하는 것이 안전하다.

11.5 제곱과 세제곱의 합

> **명제 11.6** 양의 정수 n에 대하여
>
> $$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}, \qquad \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}, \qquad \sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2 \tag{11.6}$$
>
> 이다.

증명. 첫 식은 $a = d = 1$인 등차수열의 합이므로 식 (11.3)에서 바로 나온다.

둘째 식은 망원경 합과 첫 식을 조합하여 유도한다. 항등식 $(k+1)^3 - k^3 = 3k^2 + 3k + 1$을 $k = 1, \dots, n$에 대해 더하면, 왼쪽은 식 (11.5)에 의해 $(n+1)^3 - 1$이고

$$(n+1)^3 - 1 = 3\sum_{k=1}^{n} k^2 + 3\sum_{k=1}^{n} k + n$$

이다. $(n+1)^3 - 1 = n^3 + 3n^2 + 3n$이고 $3\sum k = 3n(n+1)/2$이므로

$$3\sum_{k=1}^{n} k^2 = n^3 + 3n^2 + 3n - \frac{3n^2+3n}{2} - n = n^3 + \frac{3n^2+n}{2} = \frac{2n^3+3n^2+n}{2} = \frac{n(n+1)(2n+1)}{2}$$

이고, 양변을 3으로 나누면 둘째 식을 얻는다.

셋째 식은 n에 대한 귀납법으로 검증한다. $n = 1$에서 양변은 모두 1이다. n에서 식이 성립한다고 가정하면

$$\left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 = (n+1)^2\left[\frac{n^2}{4} + (n+1)\right] = (n+1)^2 \cdot \frac{n^2+4n+4}{4} = \left(\frac{(n+1)(n+2)}{2}\right)^2$$

이므로 $n+1$에서도 성립한다. 초기값과 귀납 단계가 모두 확인되었으므로 모든 양의 정수 n에 대해 참이다. $\square$

참고. 공식을 검산할 때는 작은 n을 대입하는 일이 유용하지만, 몇 개의 예에서 맞는다는 사실만으로 모든 n에 대한 증명이 되지는 않는다. 귀납 단계나 위와 같은 항등식 유도처럼 모든 n에 적용되는 일반적인 논증이 따로 필요하다.

11.6 곱의 구조와 팩토리얼

양의 정수 n에 대하여 $n! = 1 \cdot 2 \cdots n$이고, 빈 곱의 약속에 따라 $0! = 1$이다. $n!$은 n개의 서로 다른 대상을 일렬로 배열하는 방법의 수와 같다. 첫 자리에 n가지, 둘째 자리에 $n-1$가지, ..., 마지막 자리에 한 가지의 선택이 남기 때문이다.

명제 11.7 (Legendre 공식) 소수 p가 $n!$에 나타나는 지수는

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \tag{11.7}$$

이다. 오른쪽 급수는 $p^k > n$인 항부터 모두 0이므로 사실상 유한합이다.

증명. $1, 2, \ldots, n$ 가운데 p의 배수는 적어도 한 개의 인수 p를 제공하고, 그 개수는 $\lfloor n/p \rfloor$이다. p^2의 배수는 이미 센 p 하나에 더하여 두 번째 p를 추가로 제공하며, 그 개수는 $\lfloor n/p^2 \rfloor$이다. 일반적으로 p^k의 배수는 k번째 p를 추가로 제공한다. 각 층 $\lfloor n/p^k \rfloor$의 개수를 모두 더하면 $1, \ldots, n$에 들어 있는 인수 p의 중복을 정확히 집계하게 되어 식 (11.7)을 얻는다. $\square$

예제 11.8 $100!$의 십진 표현 끝에 붙는 0의 개수는 $10 = 2 \cdot 5$가 몇 번 곱해지는지로 결정되며, 이는 $\min(v_2(100!), v_5(100!))$이다. $v_2(100!) = \lfloor 100/2 \rfloor + \lfloor 100/4 \rfloor + \cdots$가 $v_5(100!)$보다 항상 크므로 5의 지수만 계산하면

$$v_5(100!) = \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{25} \right\rfloor = 20 + 4 = 24$$

를 얻는다.

역사 (거듭제곱 합의 일반 공식). $\sum_{k=1}^{n} k^p$을 n에 관한 차수 $p+1$의 다항식으로 표현하는 일반 공식은 Johann Faulhaber가 17세기 초에 $p = 17$까지 체계적으로 계산했다. 이 다항식의 계수는 이후 Jacob Bernoulli가 도입한 Bernoulli 수로 표현되며, 그 수렴·근사와의 관계는 Taylor 급수의 오차 분석(제8권 제6장)에서 다시 나타난다.

11.7 문제와 풀이

연습문제 11.9 $3 + 8 + 13 + \cdots + 98$의 합을 구하여라.

풀이. 공차가 5, 초항이 3이므로 $98 = 3 + (n-1)5$에서 $n - 1 = 19$, $n = 20$이다. 식 (11.3)에 의해 합은 $20(3+98)/2 = 20 \cdot 101/2 = 1010$이다. 항의 개수를 $98/5$처럼 어림으로 정하지 말고, 초항부터 정확히 센 $n = 20$을 사용해야 한다.

연습문제 11.10 $\sum_{k=1}^{n} (2k-1)$을 구하고 기하학적 의미를 설명하여라.

풀이. 식 (11.1)과 식 (11.6)에 의해 $2\sum_{k=1}^{n} k - n = n(n+1) - n = n^2$이다. 한 변이 $k-1$인 정사각형에 $2k-1$개의 단위 정사각형을 바깥쪽 꺾인 줄 모양(*gnomon*)으로 붙이면 한 변이 k인 정사각형이

된다는 기하학적 해석도 가능하며, 이를 $k = 1, \dots, n$에 대해 반복하면 한 변이 n인 정사각형의 넓이 n^2을 얻는다.

연습문제 11.11 $\sum_{k=1}^{n} \dfrac{1}{(k+1)(k+2)}$을 구하여라.

풀이. 각 항을 $\dfrac{1}{k+1} - \dfrac{1}{k+2}$로 바꾸면 식 (11.5)의 구조와 같아 합은 $\dfrac{1}{2} - \dfrac{1}{n+2} = \dfrac{n}{2(n+2)}$이다. 시작과 끝의 첨자가 한 칸씩 이동했다는 점이 예제 11.5와 다르다.

연습문제 11.12 $25!$이 2로 몇 번 나누어지는지, 그리고 끝의 0은 몇 개인지 구하여라.

풀이. 식 (11.7)에 의해 $v_2(25!) = \lfloor 25/2 \rfloor + \lfloor 25/4 \rfloor + \lfloor 25/8 \rfloor + \lfloor 25/16 \rfloor = 12 + 6 + 3 + 1 = 22$이다. 끝의 0의 개수는 $v_5(25!) = \lfloor 25/5 \rfloor + \lfloor 25/25 \rfloor = 5 + 1 = 6$개이다. 두 질문은 서로 다른 소수에 대한 지수를 묻고 있으므로 같은 답을 가질 이유가 없다.

제1권의 범위와 다음 읽기

제1권은 수의 표현과 연산, 정수의 나눗셈과 약수, 소수와 정수의 구조, 유리수와 실수의 소수 표현, 순서와 절댓값, 무리수와 실수의 완비성, 거듭제곱·근호·지수와 로그, 근사값과 오차, 합동식과 나머지 계산, 복소수, 유한합을 다루었다. 초등적인 계산을 다루면서도 각 결과가 성립하는 조건, 반례, 증명의 구조를 함께 적었다. 장별 분량은 책 전체의 어떤 목표 쪽수에 맞추기 위해서가 아니라 내용의 실제 조판 결과로 정했으며, 같은 설명을 되풀이하여 분량을 채운 쪽은 없다.

다음 권인 제2권은 문자식의 동치 변형, 다항식의 계산과 나눗셈, 인수분해와 유리식, 방정식과 부등식, 함수의 표현을 체계적으로 다룬다. 제4권(증명·명제논리·술어논리)에서는 이 권에서 사용한 수학적 귀납법과 대우·귀류법의 문장 구조를 정식화한다. 제5권(집합·수 체계·수학기초론)에서는 자연수·정수·유리수·실수의 구성을 자세히 설명하고, 제15권(정수론·대수적 정수론)에서는 합동식과 소수의 이론을 더 깊게 확장한다. 제8권(미분·적분·급수)과 제10권(실해석·측도·적분)에서는 완비성, 수렴, 오차의 개념을 함수와 알고리즘의 영역으로 넓힌다.

참고 자료의 사용 방식

본문의 설명과 문제는 이 참고서를 위해 새로 작성했다. 아래 목록은 관련 주제를 더 넓은 교재와 대조해 읽기 위한 안내이며, 이 원고 전체가 해당 기관이나 저자의 검토를 받았다는 뜻은 아니다. 개별 정리의 정확한 가정과 기호 약속은 자료마다 다를 수 있으므로, 독자는 다른 자료를 참고할 때마다 그 자료의 정의를 먼저 확인해야 한다.

- American Institute of Mathematics, Open Textbook Initiative: 수학 분야별 공개 교재를 찾기 위한 편집 목록.
- OpenStax, *Elementary Algebra* 2e: 수와 식, 방정식의 기초를 더 많은 연습문제와 함께 학습하는 자료.
- OpenStax, *Precalculus* 2e: 함수·지수·로그·삼각함수 및 미적분 준비 내용을 다루는 자료.

제 2 권

문자식·방정식·부등식

제2권은 문자로 쓴 식을 변형하여 방정식과 부등식을 푸는 방법과 그 정당성을 다룬다. 제1장은 변수와 매개변수의 구분, 항등식의 의미, 함의와 동치의 구별을 정하여 식의 변형이 해집합을 어떻게 바꾸는지 밝히는 기준을 세운다. 제2–3장은 다항식의 나눗셈 알고리즘, 나머지 정리와 인수 정리, 인수분해와 유리식을 다루고, 제4–6장은 일차방정식과 연립방정식, 이차방정식과 근의 구조, 유리방정식과 무리방정식을 가짜 해와 잃어버린 해의 구분 위에서 풀이한다. 제7–9장은 부호표를 이용한 부등식의 해집합, 부등식의 증명과 최댓값·최솟값, 지수·로그 방정식과 매개변수에 따른 해의 개수로 마무리한다.

제 1 장

문자식과 동치 변형

개요 문자식은 수, 변수, 연산으로 구성된 표현이며, 식에 연산을 적용하는 일은 언제나 그 조건과 보존되는 값을 따져야 하는 변형이다. 이 장은 변수·상수·매개변수의 구분, 식의 자연스러운 정의역과 항등식의 의미에서 출발하여, 등식의 양변에 연산을 적용할 때 해집합이 어떻게 바뀌는지, 그리고 함의와 동치를 어떻게 구별하여 적는지를 다룬다. 선행 지식: 실수의 사칙연산, 분수, 거듭제곱. 이 장의 목표는 문자를 계산하는 규칙 자체가 아니라, 각 변형이 어떤 값을 보존하는지 확인하는 방법이다.

1.1 변수, 상수, 매개변수

변수(*variable*)는 정한 범위에서 값을 받을 수 있는 기호이고, **상수**(*constant*)는 문맥에서 고정한 값이다. **매개변수**(*parameter*)는 한 문제를 풀 때에는 고정하지만, 여러 문제를 비교할 때에는 바꾸는 값이다. 예를 들어 $ax+b=0$에서 x를 미지수로, a, b를 매개변수로 다룰 수 있다. 이 역할은 글자의 모양이 정하는 것이 아니라 문제의 문맥이 정한다.

문자식은 수와 변수, 연산으로 구성된 표현이다. 식과 함수는 밀접하지만 같은 개념은 아니다. 함수는 정의역과 공역, 대응 규칙을 함께 갖춘 대상이다. 식 x^2만으로는 자연수에서 자연수로 가는 함수인지, 실수에서 실수로 가는 함수인지가 정해지지 않는다. 방정식 $x^2=4$는 식 두 개의 값이 같아지는 조건이고, 해집합은 그 조건을 만족하는 정의역의 원소 전체이다.

> **예제 1.1** $x^2=2$의 해집합은 정의역이 $\mathbb{Q}$이면 공집합이고, $\mathbb{R}$이면 $\{-\sqrt{2}, \sqrt{2}\}$이다. $x^2=-1$은 $\mathbb{R}$에서는 해가 없고, $\mathbb{C}$에서는 $\{-i, i\}$를 해집합으로 갖는다(제1권 제10장). 따라서 방정식의 해를 말할 때에는 어떤 수의 범위를 허용하는지도 함께 말해야 한다.

1.2 식의 정의역과 같은 식이라는 말

> **정의 1.2 (자연스러운 정의역)** 주어진 식의 **자연스러운 정의역**은 그 식에 나타나는 모든 연산이 실수에서 정의되는 입력의 집합이다. 분모는 0이 아니어야 하고, 짝수 제곱근 안은 비음수여야 하며, 로그의 진수는 양수여야 한다.

> **예제 1.3** $\sqrt{3-x}/(x-1)$의 정의역은 $(-\infty, 3]\setminus\{1\}$이다. 두 조건 $3-x\ge 0$과 $x-1\neq 0$을 동시에 적용한다. $\log(x-2)+\log(5-x)$의 정의역은 $(2, 5)$이다. 로그의 밑은 별도로 양수이며 1이 아닌 고정값이라고 가정한다.

공통 정의역에서

$$\frac{x^2-1}{x-1}=x+1 \qquad (x\neq 1)$$

은 올바른 등식이다. 그러나 왼쪽 식이 정하는 함수와 오른쪽 식이 정하는 함수를 각각 자연스러운 정의역까지 포함하여 비교하면 서로 다른 함수이다. 오른쪽은 $x=1$에서도 정의되지만 왼쪽은

그렇지 않다. 약분으로 얻은 식을 이용해 극한을 계산할 수는 있어도, 원래 식이 정의되지 않은 값을 그 극한으로 자동으로 정의할 수는 없다.

항등식(*identity*)은 정한 정의역의 모든 값에서 성립하는 등식이다. $(x+1)^2 = x^2 + 2x + 1$은 실수 전체에서 항등식이다. 반면 $x^2 = x$는 모든 실수에서 참이 아니므로 방정식으로 다루며 해는 $0, 1$이다. 두 표현이 몇 개의 입력에서 같은 값을 갖는다는 사실만으로 일반적인 항등식임을 증명할 수는 없다. 다항식에는 차수에 따른 별도의 판정 정리가 있다(제2권 제2장).

1.3 등식에 적용하는 연산

$A = B$이면 같은 식 C를 더하여 $A + C = B + C$로 만들 수 있다. 역으로 $A + C = B + C$에서 C를 빼면 원래 등식을 얻는다. 따라서 정의되는 범위 안에서는 두 조건이 동치이다. $C \neq 0$이 확실하면 $AC = BC$와 $A = B$도 동치이다. 그러나 C가 0일 수 있으면 곱셈은 원래 해를 보존하지만 새로운 해를 만들 수 있다.

> **예제 1.4** $x = 1$의 양변에 $x - 2$를 곱하면 $x(x-2) = x - 2$이다. 정리하면 $(x-1)(x-2) = 0$이므로 새 방정식은 $x = 2$까지 허용한다. 변형은 참인 등식을 참인 등식으로 보내지만, 거꾸로 원래 식을 반드시 복원하지는 못한다.

> **예제 1.5** $x(x-1) = 0$에서 양변을 x로 나누면 $x = 1$만 남아 $x = 0$을 잃는다. 올바른 방법은 $x = 0$과 $x \neq 0$을 나누어 살피거나, 실수에서 곱이 0이면 어느 한 인수가 0이라는 성질을 적용하는 것이다.

> **명제 1.6** 실수값 식 $A(x), B(x)$가 공통 정의역 D에서 정의된다고 하자. f가 두 식의 값이 들어가는 집합에서 단사함수이면
>
> $$A(x) = B(x) \iff f(A(x)) = f(B(x)) \tag{1.1}$$
>
> 이다.

증명. 앞에서 뒤로의 함의는 함수의 정의(같은 입력은 같은 값으로 보낸다)에 따른다. 뒤에서 앞으로의 함의는 같은 함수값을 갖는 두 입력이 같다는 단사성의 정의에 따른다. □

실수 전체에서 세제곱 함수 $x \mapsto x^3$은 단사이므로 등식의 양변을 세제곱하는 것은 식 (1.1)에 의해 동치 변형이다. 제곱 함수는 $1, -1$에서 같은 값 1을 가지므로 단사가 아니다. 다만 양변이 비음수라는 조건이 이미 있으면, 그 범위로 정의역을 제한한 제곱 함수는 단사이므로 제곱도 동치 변형이 된다.

1.4 함의와 동치를 계산에 표시하기

풀이에서 $\Rightarrow$는 앞 조건이 뒤 조건을 보장한다는 뜻이고, $\iff$는 두 조건의 해집합이 같다는 뜻이다. 필요조건만 얻는 단계에는 함의를 사용하고, 마지막에 얻은 후보를 원래 식에 대입하여 검산한다. 모든 단계를 동치로 만들 수 있다면 마지막 후보 검사가 논리적으로는 불필요할 수도 있지만, 계산 과정의 실수를 잡는 검산으로서는 여전히 유용하다.

예제 1.7 $\sqrt{x+2} = x$를 풀자. 자연스러운 정의역의 조건은 $x \geq -2$이지만, 왼쪽이 제곱근이라 비음수이므로 해는 $x \geq 0$이어야 한다. 이 조건 아래에서 양변을 제곱하면 $x+2 = x^2$, 곧 $(x-2)(x+1) = 0$이다. 후보 $2, -1$ 가운데 $x \geq 0$인 2만 남는다. 실제로 $\sqrt{4} = 2$이므로 해는 $x = 2$이다.

흔한 오류. 양변에 같은 연산을 했다는 이유만으로 항상 동치라고 적지 않는다. 정의역, 연산의 단사성, 나눈 값이 0일 가능성을 함께 확인해야 한다.

핵심 (등식을 동치로 바꾸는 조건 요약). 등식 $A = B$에 적용하는 연산이 동치 변형이려면 다음 가운데 하나가 성립해야 한다. (1) 양변에 같은 식 C를 더하거나 뺀다(항상 동치). (2) 양변에 0이 아님이 확실한 C를 곱하거나 나눈다. (3) 양변에 단사함수를 적용한다(식 (1.1)). 이 가운데 어느 것도 아니면, 얻은 해 후보를 반드시 원래 식에 대입해 검산해야 한다.

1.5 문제와 풀이

연습문제 1.8 $\dfrac{x^2-4}{x-2} = x+2$의 해집합을 실수에서 구하여라.

풀이. 원래 식은 $x \neq 2$에서만 정의된다. 그 범위의 모든 값에서 약분이 가능하므로 해집합은 $\mathbb{R} \setminus \{2\}$이다. "모든 실수"라고 쓰면 정의역의 제한을 잊은 것이다.

연습문제 1.9 $ax = a$를 매개변수 $a \in \mathbb{R}$에 따라 풀어라.

풀이. $a = 0$이면 $0 = 0$이므로 모든 실수가 해이다. $a \neq 0$이면 a로 나누어 $x = 1$이다. 처음부터 양변을 a로 나누면 $a = 0$인 첫 경우가 통째로 사라진다.

연습문제 1.10 $\sqrt{x^2} = x$가 항등식이 되는 최대의 실수 정의역을 구하여라.

풀이. 모든 실수에서 $\sqrt{x^2} = |x|$이므로, 이 식이 $x \geq 0$에서만 등식이 참이다. 참이 되는 최대 집합은 $[0, \infty)$이다.

연습문제 1.11 실수 a, b에 대해 $a^3 = b^3$이면 $a = b$임을 인수분해로 증명하여라.

풀이. $a^3 - b^3 = (a-b)(a^2+ab+b^2) = 0$이다. 둘째 인수는 $a^2+ab+b^2 = (a+b/2)^2 + 3b^2/4$로 완전제곱의 합이므로 음수가 아니고, 0이 되려면 $b = 0$과 $a + b/2 = 0$이 동시에 성립해야 하므로 $a = b = 0$일 때뿐이다. 따라서 둘째 인수가 0인 경우에도 $a = b$(둘 다 0)이고, 첫째 인수가 0인 경우에는 바로 $a = b$이므로, 어느 경우든 $a = b$를 얻는다.

연습문제 1.12 $\log(x^2) = 2\log x$를 실수에서 사용할 수 있는 범위를 설명하여라.

풀이. 오른쪽이 정의되려면 $x > 0$이어야 한다. 왼쪽만 보면 $x \neq 0$이면 충분하다. 따라서 주어진 등식의 공통 정의역은 $x > 0$이다. 더 넓은 범위에서는 $\log(x^2) = 2\log|x|$라고 쓰면 $x \neq 0$에서 성립한다.

제 2 장

다항식의 계산과 나눗셈

개요 다항식은 유한합으로 표현되는 문자식이며, 차수·전개 항등식·나눗셈 알고리즘·근의 개수 상한·보간이라는 다섯 가지 기본 결과로 다항식환의 계산 구조를 세울 수 있다. 이 장은 다항식과 차수의 정의에서 출발하여 전개 공식과 다항식 나눗셈 알고리즘, 나머지 정리와 인수 정리, 근의 개수에 대한 상한, 보간의 유일성을 차례로 증명한다. 선행 지식: 분배법칙, 유한합(제1권 제11장), 문자식의 동치(제2권 제1장). 이 장의 계수는 별도 언급이 없으면 실수이다.

2.1 다항식과 차수

정의 2.1 (다항식과 차수) 한 변수 x에 대한 **다항식**(*polynomial*)은 유한합

$$P(x) = a_0 + a_1 x + \cdots + a_n x^n \tag{2.1}$$

의 형태인 식이다. 계수 a_j는 실수이고 지수는 비음수 정수이다. $a_n \neq 0$일 때 최고 지수 n을 **차수**라 하고 $\deg P = n$으로 쓴다. 영다항식의 차수는 여기서는 정의하지 않는다.

$1/x$, $\sqrt{x}$, 2^x는 x에 관한 다항식이 아니다. $\sqrt{2}\,x^2 + \pi$는 실수 계수 다항식이다. "계수가 정수인가"와 "지수가 비음수 정수인가"는 서로 다른 요구이다. 다항식환 $\mathbb{R}[x]$는 다항식 전체와 계수별 덧셈, 분배법칙에 따른 곱셈을 함께 나타내는 기호이다.

명제 2.2 (차수의 덧셈성) 0이 아닌 다항식 P, Q에 대해서

$$\deg(PQ) = \deg P + \deg Q \tag{2.2}$$

이다. $P + Q \neq 0$이면 $\deg(P+Q) \le \max(\deg P, \deg Q)$이지만 등호는 항상 성립하지는 않는다.

증명. P, Q의 최고차항을 각각 $a_m x^m$, $b_n x^n$ $(a_m, b_n \neq 0,\ m = \deg P,\ n = \deg Q)$이라 하면, PQ를 전개했을 때 지수가 $m+n$보다 큰 항은 나오지 않고 지수가 $m+n$인 항의 계수는 $a_m b_n$이다. 실수에서 0이 아닌 두 수의 곱은 0이 아니므로 $a_m b_n \neq 0$이고, 최고차항이 사라지지 않아 $\deg(PQ) = m+n$이다.

$P+Q$를 전개하면 지수가 $\max(m,n)$보다 큰 항은 나올 수 없으므로 $\deg(P+Q) \le \max(m,n)$이다. 그러나 $m = n$이고 최고차항의 계수가 서로 상쇄되면 등호가 깨질 수 있다. 예를 들어 $(x^3 + x) + (-x^3 + 1) = x + 1$이므로 $\deg(P+Q) = 1 < 3 = \max(\deg P, \deg Q)$이다. □

2.2 전개와 항등식

분배법칙을 반복하면 다음 전개 항등식을 얻는다.

$$(a+b)^2 = a^2 + 2ab + b^2, \tag{2.3}$$

$$(a-b)^2 = a^2 - 2ab + b^2,$$

$$(a+b)(a-b) = a^2 - b^2, \tag{2.4}$$

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3. \tag{2.5}$$

이 공식은 실수와 복소수에서 성립한다. 행렬처럼 곱셈이 교환하지 않는 상황에서는 $(A+B)^2 = A^2 + AB + BA + B^2$이고, 추가로 $AB = BA$가 있어야 비로소 $AB+BA = 2AB$로 정리하여 식 (2.3)과 같은 꼴을 얻을 수 있다.

예제 2.3 $(2x-3)(x^2+x+4)$를 전개하면

$$2x^3 + 2x^2 + 8x - 3x^2 - 3x - 12 = 2x^3 - x^2 + 5x - 12$$

이다. $x=0$을 대입하면 상수항 -12를, $x=1$을 대입하면 전체 값 $2-1+5-12=-6$을 검산할 수 있다. 몇 개의 대입 검산이 전개의 증명을 대신하는 것은 아니지만, 부호 오류를 찾는 데 유용하다.

2.3 다항식 나눗셈 알고리즘

정리 2.4 (다항식 나눗셈 알고리즘) 다항식 P, D에서 $D \neq 0$이면 유일한 다항식 Q, R이 존재하여

$$P = DQ + R \tag{2.6}$$

이고, $R = 0$이거나 $\deg R < \deg D$이다.

증명. 존재. $P = 0$이면 $Q = R = 0$으로 자명하다. $\deg P \geq \deg D$이면 P의 최고차항을 없애는 단항식 배수를 D에 곱해 P에서 뺀다. 그 결과로 얻은 새 다항식의 차수는 엄격히 감소하므로, 이 과정을 유한 번 반복하면 $\deg D$보다 낮은 차수의 나머지를 얻는다.

유일성. $DQ + R = DQ' + R'$이라 하자. $Q \neq Q'$이면 $D(Q-Q') = R' - R$에서 왼쪽의 차수는 식 (2.2)에 의해 적어도 $\deg D$인데, 오른쪽은 영다항식이거나 차수가 $\deg D$보다 작으므로 모순이다. 따라서 $Q = Q'$이고 $R = R'$이다. □

실수 계수라는 조건 덕분에 최고차항 계수로 나눌 수 있다. 정수 계수 다항식만 허용하면, 예를 들어 x를 $2x+1$로 나눌 때 같은 형태의 나눗셈 알고리즘이 정수 계수 안에서는 성립하지 않는다. 일반대수학에서는 계수의 구조(체인가, 정역인가)를 먼저 확인하는 이유가 여기에 있다(제14권 제5장).

예제 2.5 $P = x^3 - 2x^2 + 4x - 5$를 $D = x - 2$로 나누면

$$P = (x-2)(x^2+4) + 3$$

이다. 최고차항부터 차례로 없애면 몫은 x^2+4, 나머지는 3이다. 나머지에 x가 남지 않는 이유는 나누는 다항식의 차수가 1이기 때문이다.

예제 2.6 $x^4 + 1$을 $x^2 + 1$로 나누면

$$x^4 + 1 = (x^2+1)(x^2-1) + 2$$

이다. 정수의 나눗셈과 달리 나머지가 양수일 필요는 없다. 다항식의 나머지 조건은 크기의 비교가 아니라 차수의 비교이다.

2.4 나머지 정리와 인수 정리

정리 2.7 (나머지 정리와 인수 정리) P를 $x-a$로 나눈 나머지는 $P(a)$이다. 따라서 $P(a)=0$일 필요충분조건은 $x-a$가 P의 인수라는 것이다.

증명. 나눗셈 알고리즘(정리 2.4)에 의해 $P(x)=(x-a)Q(x)+r$이고 $\deg(x-a)=1$이므로 r는 상수이다. $x=a$를 대입하면 $P(a)=r$이다. 따라서 $r=0$인 것과 $P(a)=0$인 것은 같은 조건이고, $r=0$은 정확히 $x-a$가 P를 나누어떨어지게 한다는 뜻이다. □

예제 2.8 $P(x)=x^3-4x^2+x+6$이면 $P(2)=8-16+2+6=0$이다. 따라서 $x-2$로 나눌 수 있고, 몫을 나눗셈 알고리즘으로 구하면

$$P(x)=(x-2)(x^2-2x-3)=(x-2)(x-3)(x+1)$$

이다. 이 결과를 전개하면 원래의 세 계수와 상수항을 모두 확인할 수 있다.

역사 (조립제법). 나머지 정리를 이용해 $P(x)$를 $x-a$로 나누는 계산은 조립제법(*synthetic division*)으로 간단히 수행할 수 있다. 이 절차는 이탈리아의 Paolo Ruffini가 1804년에, 영국의 William George Horner가 1819년에 독립적으로 체계화했으며, 일반적인 다항식의 근을 수치적으로 근사하는 Horner 방법과 같은 계산 구조를 공유한다.

정리 2.9 (근의 개수 상한) 실수 또는 복소수 계수의 n차 영이 아닌 다항식은 서로 다른 근을 최대 n개 갖는다.

증명. n에 관한 귀납법으로 보인다. $n=0$이면 P는 0이 아닌 상수이므로 근이 없다. $n\geq 1$에서 근 a가 없으면 근이 0개이므로 상한을 만족한다. 근 a가 있으면 인수 정리(정리 2.7)에 의해 $P=(x-a)Q$이고 Q의 차수는 $n-1$이다. a와 다른 근은 모두 $x-a\neq 0$이므로 Q의 근이고, 귀납 가정에 의해 Q는 서로 다른 근을 최대 $n-1$개 가지므로 P는 a를 더해 최대 n개의 서로 다른 근을 갖는다. □

이 정리는 실근이 반드시 존재한다고 말하지 않는다. x^2+1은 실근이 없다. 복소수 범위에서는 모든 양의 차수의 다항식이 적어도 한 개의 근을 갖는다는 대수학의 기본정리(*fundamental theorem of algebra*)가 별도로 필요하며, 이 정리는 복소해석의 도구로 증명한다(제11권 제4장).

2.5 항등식 판정과 보간의 첫 예

차수가 n 이하인 두 다항식이 서로 다른 $n+1$개의 값에서 같으면 두 다항식은 같다. 두 다항식의 차를 취하면 차수가 n 이하인 다항식이 $n+1$개의 근을 가지게 되므로, 정리 2.9에 의해 그 차는 영다항식이어야 하기 때문이다. 이 판정은 비교하는 두 표현이 다항식이고 차수의 상계가 알려졌을 때에만 적용할 수 있다.

예제 2.10 이차 이하 다항식 P가 $P(0)=1$, $P(1)=3$, $P(2)=9$를 만족한다고 하자. $P=ax^2+bx+c$로 쓰면 $c=1$, $a+b=2$, $4a+2b=8$이므로 연립하여 $a=2$, $b=0$이다. 따라서 $P=2x^2+1$이다. 같은 세 값을 만족하는 더 고차인 다항식은 $2x^2+1+x(x-1)(x-2)Q(x)$처럼 무수히 많다. 차수를 이차 이하로 제한하는 조건이 유일성을 만든다.

2.6 문제와 풀이

연습문제 2.11 x^3+2x^2-5x+1을 $x+3$으로 나눈 나머지를 구하여라.

풀이. $x=-3$을 대입하여 $-27+18+15+1=7$이다. $x+3=x-(-3)$이므로 3이 아니라 -3을 대입해야 한다.

연습문제 2.12 x^4-1을 실수의 일차 또는 이차 인수로 분해하여라.

풀이. $x^4-1=(x^2-1)(x^2+1)=(x-1)(x+1)(x^2+1)$이다. 마지막 인수는 실근이 없으므로 실수 일차 인수로 더 나눌 수 없다.

연습문제 2.13 서로 다른 실수 a, b에 대해 $P(a)=P(b)=0$이면 $(x-a)(x-b)$가 P를 나눔을 보여라.

풀이. 인수 정리에 의해 $P=(x-a)Q$로 쓸 수 있다. $0=P(b)=(b-a)Q(b)$이고 $b-a\neq 0$이므로 $Q(b)=0$이다. Q에 인수 정리를 다시 적용하면 $Q=(x-b)R$이므로 $P=(x-a)(x-b)R$이다.

연습문제 2.14 $P(x)=x^2+ax+b$가 $P(1)=0$, $P(3)=0$을 만족할 때 a, b를 구하여라.

풀이. 최고차항 계수가 1인 이차식이고 서로 다른 두 근이 $1, 3$이므로 $P=(x-1)(x-3)=x^2-4x+3$이다. 따라서 $a=-4$, $b=3$이다.

연습문제 2.15 정수 전체에서 같은 값을 갖는 두 실수 계수 다항식이 같음을 증명하여라.

풀이. 두 다항식의 차를 D라 하자. D가 영다항식이 아니면 정리 2.9에 의해 D는 자신의 차수보다 많은 서로 다른 근을 가질 수 없다. 모든 정수에서 $D=0$이라는 조건은 무한히 많은 서로 다른 근을 주므로, 어떤 유한한 차수와도 모순이다. 따라서 D는 영다항식이고 두 다항식은 같다.

제 3 장

인수분해와 유리식

개요 인수분해는 다항식을 더 낮은 차수 다항식의 곱으로 나타내는 일이며, 어떤 계수의 범위를 허용하느냐에 따라 같은 다항식의 분해 결과가 달라진다. 이 장은 인수분해의 범위를 명확히 하는 일에서 출발하여 공통 인수·묶음·치환, 세제곱과 고차의 기본 공식, 유리근 정리, 유리식의 약분·통분, 부분분수의 첫 단계를 차례로 다룬다. 선행 지식: 다항식과 나머지 정리(제2권 제2장), 실수의 분수 계산.

3.1 어떤 범위에서 인수분해하는가

인수분해는 다항식을 더 낮은 차수 다항식의 곱으로 나타내는 일이다. 가능한 인수의 계수 범위가 결과를 바꾼다.

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$$

는 실수 계수 분해이지만 유리수 계수의 일차 인수분해는 아니다. $x^2 + 1$은 실수 계수에서 일차 인수로 분해되지 않지만 복소수 계수에서는 $(x - i)(x + i)$이다. 이후 어떤 다항식이 정한 계수 범위에서 **기약**(*irreducible*)이라는 말은, 그 범위에서 비상수 다항식의 곱으로 더 나눌 수 없다는 뜻으로 쓴다. 계수 범위를 체로 고정하면 다항식환에서도 정수의 소인수분해에 대응하는 유일 인수분해가 성립한다(제14권 제5장).

3.2 공통 인수, 묶음, 치환

가장 먼저 모든 항의 공통 인수를 살핀다. 다음으로 두 항씩 묶거나 같은 부분식을 하나의 변수로 바꾸면 구조가 드러난다. 각 방법의 정당성은 분배법칙이다.

> **예제 3.1** $6x^3 - 9x^2 = 3x^2(2x - 3)$이다. $x^3 + 2x^2 + 3x + 6 = x^2(x + 2) + 3(x + 2) = (x + 2)(x^2 + 3)$이다. 두 번째 예에서는 첫 두 항과 마지막 두 항에서 같은 괄호 $(x + 2)$를 만든다.

> **예제 3.2** $x^4 - 5x^2 + 4$에 $u = x^2$을 쓰면 $u^2 - 5u + 4 = (u - 1)(u - 4)$이다. 따라서
>
> $$x^4 - 5x^2 + 4 = (x^2 - 1)(x^2 - 4) = (x - 1)(x + 1)(x - 2)(x + 2)$$
>
> 이다. 치환한 변수를 되돌릴 때 $u = x^2 \geq 0$ 같은 제약도 함께 되돌려야 한다. 인수분해 자체에는 문제가 없지만, 방정식 풀이에서는 음의 u가 가짜 후보가 될 수 있다.

3.3 세제곱과 고차의 기본 공식

$$a^3 - b^3 = (a-b)(a^2 + ab + b^2), \tag{3.1}$$

$$a^3 + b^3 = (a+b)(a^2 - ab + b^2). \tag{3.2}$$

더 일반적으로 양의 정수 n에 대해

$$a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^{n-1-k}b^k \tag{3.3}$$

이다. 오른쪽을 전개하면 중간 항이 상쇄되어 첫 항 a^n과 마지막 항 $-b^n$만 남는다. n이 홀수이면 $a^n + b^n$에 b 대신 $-b$를 넣어 비슷한 공식 $a^n + b^n = (a+b)\sum_{k=0}^{n-1}(-1)^k a^{n-1-k}b^k$를 얻는다.

예제 3.3 $x^6 - 1 = (x^3-1)(x^3+1)$에서 식 (3.1), (3.2)을 적용하면

$$x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$$

이다. 두 이차식 $x^2 \pm x + 1$의 판별식은 모두 $1 - 4 = -3$이므로 실수 일차 인수로 더 나뉘지 않는다. 복소수에서는 여섯 개의 단위근 $e^{2\pi i k/6}$ $(k = 0, \dots, 5)$과 연결된다(제1권 제10장).

3.4 유리근 정리

정리 3.4 (유리근 정리) 정수 계수 다항식 $P(x) = a_n x^n + \cdots + a_0$에서 $a_n \neq 0$이라 하자. 기약분수 p/q가 근이고 $q > 0$이면 $p \mid a_0$, $q \mid a_n$이다.

증명. $P(p/q) = 0$에 q^n을 곱하면

$$a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_0 q^n = 0.$$

모든 항에서 마지막 항을 제외하면 p가 공통 인수이므로 $p \mid a_0 q^n$이다. $\gcd(p,q) = 1$이므로 $\gcd(p, q^n) = 1$이고, 따라서 $p \mid a_0$이다. 같은 방식으로 첫 항을 제외한 나머지를 보면 $q \mid a_n p^n$이고 $\gcd(q, p^n) = 1$이므로 $q \mid a_n$이다. $p = 0$인 경우에는 근 조건이 $a_0 = 0$을 뜻하며, 모든 정수가 0을 나눈다는 약수의 정의와 호환된다. □

예제 3.5 $2x^3 - 3x^2 - 8x + 12$의 유리근 후보는 기약형으로 분자가 12의 약수, 분모가 2의 약수인 수들이다. $P(2) = 16 - 12 - 16 + 12 = 0$을 확인하여 $x - 2$로 나누면

$$P(x) = (x-2)(2x^2 + x - 6) = (x-2)(2x-3)(x+2)$$

이다. 유리근 정리는 후보를 제한할 뿐, 후보 모두가 실제로 근이라고 말하지는 않는다.

최고차항 계수가 1인 정수 계수 다항식의 유리근은 정수여야 한다. 이를 사용하면 $x^2 - 2$가 유리근을 갖지 않음을 빠르게 보일 수 있다. 가능한 정수 후보 $\pm 1, \pm 2$ 가운데 어느 것도 근이 아니기 때문이다. 고차식은 유리근이 없어도 유리수 계수의 더 낮은 차수 인수끼리 나뉠 수 있으므로, "유리근 없음"과 "기약"은 일반적으로 동치가 아니다.

3.5 유리식의 약분과 통분

정의 3.6 (유리식) 두 다항식 P, Q에서 $Q \neq 0$일 때 P/Q를 **유리식**(*rational expression*)이라 한다. 실수 함수로 평가할 때는 $Q(x) = 0$인 점을 정의역에서 제외한다.

예제 3.7

$$\frac{x^2 - 9}{x^2 - x - 6} = \frac{(x-3)(x+3)}{(x-3)(x+2)} = \frac{x+3}{x+2}, \qquad x \neq 3, -2.$$

약분 뒤에도 원래 식을 나타낼 때는 두 제외값을 모두 유지한다. $x = 3$은 약분된 식에서는 계산할 수 있지만, 원래 분모는 $x = 3$에서 0이다.

예제 3.8

$$\frac{1}{x-1} - \frac{2}{x+1} = \frac{(x+1) - 2(x-1)}{(x-1)(x+1)} = \frac{3 - x}{x^2 - 1}, \qquad x \neq \pm 1.$$

두 번째 분자의 괄호를 빠뜨리면 상수항이 달라진다. 통분은 분모를 같게 만드는 연산이고, 분자의 항을 그대로 더하는 규칙이 아니다.

흔한 오류. $(a+b)/(a+c)$에서 a를 지워 b/c라고 쓰면 안 된다. 약분할 수 있는 것은 전체 분자와 전체 분모에 공통으로 곱해진 인수뿐이다. a가 분자와 분모에 더해진 항이라는 사실은 약분의 근거가 되지 않는다.

3.6 부분분수의 첫 단계

서로 다른 실수 a, b에 대해 분모가 $(x-a)(x-b)$인 낮은 차수 유리식은 단순한 분수의 합으로 분해할 수 있다. 이는 적분, 수열의 합, 라플라스 변환에서 유용하다.

예제 3.9

$$\frac{3x + 1}{(x-1)(x+2)} = \frac{A}{x-1} + \frac{B}{x+2}$$

라고 두면 통분하여 $3x + 1 = A(x+2) + B(x-1)$이다. $x = 1$에서 $4 = 3A$, $x = -2$에서 $-5 = -3B$이므로 $A = 4/3$, $B = 5/3$이다. 여기서 $x = 1, -2$를 대입하는 것은 분모를 제거한 다항식 항등식에 대입하는 것이므로 정당하다. 원래 유리식의 정의역에는 여전히 포함되지 않는다.

분자의 차수가 분모 이상이면 먼저 다항식 나눗셈(정리 2.4)을 한다. 중복 인수 $(x-a)^m$에는 $1/(x-a), \dots, 1/(x-a)^m$ 항이 필요하며, 실수에서 기약인 이차 인수에는 일차식 분자를 사용한다. 이 일반 형태의 증명은 다항식의 서로소 분해와 연립일차방정식으로 연결된다.

3.7 문제와 풀이

연습문제 3.10 $x^4 + 4$를 실수 계수 이차식의 곱으로 분해하여라.

풀이. $x^4 + 4 = (x^2 + 2)^2 - (2x)^2 = (x^2 - 2x + 2)(x^2 + 2x + 2)$이다. 항을 더했다가 빼서 완전제곱의 차 꼴을 만든다(Sophie Germain 항등식).

연습문제 3.11 $x^4 + 2x^2 + 1$은 유리근이 없지만 유리수 계수에서 기약이 아님을 설명하여라.

풀이. $x^4+2x^2+1=(x^2+1)^2$이고 실수근조차 없다. 유리근이 없다는 사실은 일차 인수가 없다는 뜻이지 모든 비상수 인수가 없다는 뜻이 아니다.

연습문제 3.12 $\dfrac{x^2-1}{x^2+2x+1}$을 정리하고 원래 정의역을 써라.

풀이. $(x-1)(x+1)/(x+1)^2=(x-1)/(x+1)$이고 $x\neq -1$이다. 약분 전후의 정의역이 이 예에서는 같다.

연습문제 3.13 $1/[x(x+1)]$의 부분분수를 구하고 $\sum_{k=1}^{n} 1/[k(k+1)]$을 계산하여라.

풀이. $1/[x(x+1)]=1/x-1/(x+1)$이다. 따라서 합은

$$\left(1-\frac{1}{2}\right)+\left(\frac{1}{2}-\frac{1}{3}\right)+\cdots+\left(\frac{1}{n}-\frac{1}{n+1}\right)=\frac{n}{n+1}$$

이다.

연습문제 3.14 x^3-2가 유리수 계수에서 기약임을 보여라.

풀이. 세제곱 다항식이 비상수인 두 다항식의 곱으로 나뉜다면, 차수가 $3=1+2$로 쪼개지는 방법은 1과 2뿐이므로 어느 인수는 반드시 일차이고, 유리근이 생긴다. 유리근 정리(정리 3.4)의 후보 $\pm 1, \pm 2$는 어느 것도 x^3-2의 근이 아니다. 따라서 기약이다. 이 논법의 “일차 인수가 존재한다” 부분은 차수가 3이기 때문에 성립하는 것으로, 일반적인 사차 이상에서는 비상수 인수 두 개의 차수가 모두 2 이상일 수 있어 성립하지 않는다.

제 4 장

일차방정식과 연립방정식

개요 이 장은 미지수가 일차로 나타나는 방정식과 그 연립계를 다룬다. 일차방정식 $ax = b$의 해집합을 매개변수 a, b의 값에 따라 분류하고, 분모에 상수가 있는 방정식과 두세 미지수의 연립일차방정식의 풀이법을 제시한다. 행렬식을 이용한 해의 공식과 소거법이 해집합을 보존하는 이유를 증명하며, 문장으로 주어진 조건을 방정식으로 옮기는 과정을 다룬다. 선행 지식: 등식의 동치 변형, 분수 계산. 연립방정식의 일반적인 구조는 선형대수 권에서 행렬과 벡터공간의 언어로 확장한다(제7권 제1장).

4.1 일차방정식의 세 경우

일차방정식(*linear equation*)은 미지수가 일차로 나타나는 방정식이다. 가장 기본적인 꼴은 $ax = b$이다. 실수 매개변수 a, b를 허용하면 해집합은 다음 세 가지로 나뉜다.

$$\{x : ax = b\} = \begin{cases} \{b/a\}, & a \neq 0, \\ \mathbb{R}, & a = 0,\ b = 0, \\ \varnothing, & a = 0,\ b \neq 0. \end{cases}$$

"일차방정식은 해가 하나"라는 말은 실제로 미지수의 계수가 0이 아니라는 조건을 전제한다. 매개변수가 있는 문제에서는 이 조건부터 확인한다.

> **예제 4.1** $3(2x - 1) - 4(x + 2) = 7$을 풀면 $6x - 3 - 4x - 8 = 7$, $2x = 18$, $x = 9$이다. 원래 식의 왼쪽은 $3 \cdot 17 - 4 \cdot 11 = 7$이므로 검산된다.

> **예제 4.2** $(a - 2)x = a^2 - 4$에서는 $a \neq 2$이면 $x = a + 2$이다. $a = 2$이면 양변이 0이라 모든 실수가 해이다. 인수 $a - 2$를 약분한 공식 $x = a + 2$는 $a = 2$일 때의 전체 해집합을 나타내지 못한다.

4.2 분수가 있는 일차방정식

분모가 상수이면 공통분모로 양변을 곱해 분수를 없앨 수 있다. 공통분모는 0이 아니므로 이 변형은 동치이다. 분모가 미지수에 따라 달라지면 분모가 0이 되는 값을 먼저 제외해야 한다.

> **예제 4.3**
> $$\frac{x - 1}{3} - \frac{x + 2}{4} = 1$$
> 에서 양변에 12를 곱하면 $4(x-1) - 3(x+2) = 12$이다. 따라서 $x - 10 = 12$, $x = 22$이다. 대입하면 $7 - 6 = 1$이다.

4.3 두 미지수의 연립일차방정식

연립방정식(*system of equations*)은 두 조건

$$ax + by = e, \qquad cx + dy = f$$

을 동시에 만족하는 순서쌍 (x, y)를 찾는 문제이다. 각 일차식에서 a, b(또는 c, d)가 모두 0은 아니면 그 식은 평면의 직선을 나타낸다. 두 직선이 한 점에서 만나면 유일한 해가 있고, 평행하면서 서로 다르면 해가 없으며, 같은 직선이면 무한히 많은 해를 갖는다. 계수가 전부 0인 등식은 직선을 나타내지 않으므로 따로 다룬다.

> **정리 4.4 (두 미지수 연립일차방정식의 해)** $\Delta = ad - bc \neq 0$이면 연립방정식 $ax + by = e,\ cx + dy = f$의 유일한 해는
>
> $$x = \frac{ed - bf}{\Delta}, \qquad y = \frac{af - ec}{\Delta} \tag{4.1}$$
>
> 이다.

증명. 첫 식에 d, 둘째 식에 b를 곱하여 빼면 $\Delta x = ed - bf$이다. 첫 식에 c, 둘째 식에 a를 곱하여 빼면 $-\Delta y = ec - af$이다. $\Delta \neq 0$이므로 해가 있다면 식 (4.1)의 형태뿐이다. 이 값을 두 식에 대입하면 각각 e, f가 되어 실제 해임도 확인된다. □

핵심 수식

$$x = \frac{ed - bf}{\Delta}, \qquad y = \frac{af - ec}{\Delta}, \qquad \Delta = ad - bc. \tag{4.2}$$

역사 (Cramer 공식). 행렬식으로 두 미지수 연립일차방정식의 해를 나타내는 식 (4.1)는 Gabriel Cramer가 1750년에 발표하였고, 오늘날 **Cramer 공식**(*Cramer's rule*)이라고 부른다. 미지수가 많아지면 이 공식은 각 분자·분모가 행렬식이 되는 형태로 일반화된다(제7권 제6장).

이 공식은 작은 계수에서는 편리하지만, 많은 미지수에서는 소거법이 더 체계적이다. 또한 $\Delta = 0$이라는 사실만으로 해가 없다고 결론 내릴 수는 없다. 무수히 많은 해가 있을 수도 있다.

> **예제 4.5** $2x + 3y = 7,\ 4x - y = 7$에서 둘째 식을 이용하면 $y = 4x - 7$이다. 첫 식에 대입하여 $14x - 21 = 7,\ x = 2,\ y = 1$을 얻는다. $\Delta = 2(-1) - 3\cdot 4 = -14$이고 공식으로도 같은 값이 나온다.

> **예제 4.6** $2x + 4y = 6$과 $x + 2y = 3$은 같은 조건이므로 해는 $(x, y) = (3 - 2t, t),\ t \in \mathbb{R}$이다. 둘째 식을 $x + 2y = 4$로 바꾸면 첫 식의 절반과 충돌하므로 해가 없다. 두 경우 모두 계수행렬의 행렬식은 0이다.

4.4 소거법이 해집합을 보존하는 이유

연립방정식에서 한 식을 0이 아닌 상수배로 바꾸거나, 한 식에 다른 식의 배수를 더하거나, 식의 순서를 바꾸어도 해집합은 같다. 각 연산에는 원래 식으로 돌아가는 역연산이 있기 때문이다. 단순히 새 식이 원래 식들에서 따라온다는 것만으로는 동치가 충분히 설명되지 않으며, 역방향도 성립해야 한다.

예제 4.7

$$x + y + z = 6, \qquad 2x - y + z = 3, \qquad x + 2y - z = 2$$

를 풀자. 둘째 식에서 첫 식의 두 배를 빼면 $-3y - z = -9$이다. 셋째 식에서 첫 식을 빼면 $y - 2z = -4$이다. 앞 식을 $3y + z = 9$로 쓰고 $z = 9 - 3y$를 대입하면 $7y = 14$이다. 따라서 $y = 2$, $z = 3$, $x = 1$이다. 원래 세 식은 각각 $6, 3, 2$가 되어 모두 만족한다.

자유변수가 생기면 해를 매개변수로 나타낸다. 모순식 $0 = 1$이 생기면 해가 없으며, 항등식 $0 = 0$은 새 제약을 주지 않는다. 일반적인 해의 개수와 자유도는 계수행렬의 **계수**(*rank*)와 **영공간**(*null space*)의 차원으로 설명되며, 이는 선형사상의 핵과 상의 차원 정리로 정식화된다(제7권 제4장).

4.5 문장으로 된 조건을 식으로 옮기기

미지수의 단위와 의미를 먼저 정하고, 각 문장이 무엇의 합 또는 차를 나타내는지 구별한다. 계산 뒤에는 원래 상황에서 허용되는 범위를 확인한다. 실수해가 존재해도 물건의 개수처럼 비음수 정수여야 하는 상황에서는 답이 아닐 수 있다.

예제 4.8 어떤 혼합물 200 g의 성분 농도가 12%이다. 농도 20%인 혼합물을 몇 g 더해야 전체가 15%가 되는가? 더하는 질량을 x g이라 하면 성분량 보존으로

$$0.12 \cdot 200 + 0.20x = 0.15(200 + x)$$

이다. 따라서 $0.05x = 6$, $x = 120$ g이다. 농도 자체를 단순히 더하지 않고 성분의 질량을 더해야 한다. 실제로 성분 48 g을 총 320 g으로 나누면 15%이다.

4.6 문제와 풀이

연습문제 4.9 $2(x - 3) = 2x + 1$을 풀어라.

풀이. $-6 = 1$이라는 모순으로 정리되므로 해가 없다. x가 사라졌다고 해서 언제나 모든 수가 해인 것은 아니다.

연습문제 4.10 $kx + 2y = 1,\ 2x + ky = 1$을 실수 k에 따라 분류하여라.

풀이. 계수행렬의 행렬식은 $k^2 - 4$이다. $k \neq \pm 2$이면 두 식을 빼서 $(k - 2)(x - y) = 0$, 즉 $x = y$이고 $x = y = 1/(k + 2)$이다. $k = 2$이면 두 식이 같아져 $x + y = 1/2$인 무한히 많은 해를 갖는다. $k = -2$이면 두 식의 왼쪽이 서로 반대인데 오른쪽은 모두 1이므로 해가 없다.

연습문제 4.11 $x + y = 3,\ 2x + 2y = 6,\ 3x + 3y = 10$의 해를 구하여라.

풀이. 앞 두 식은 양립하지만 셋째 식은 첫 식의 세 배가 되어야 할 9와 충돌한다. 따라서 전체 연립방정식은 해가 없다. 일부 식의 양립만으로 전체의 양립을 판단할 수 없다.

연습문제 4.12 $x + y + z = 1,\ x - y + z = 3$의 해를 매개변수로 나타내라.

풀이. 두 식을 빼면 $2y = -2$이므로 $y = -1$이다. 따라서 $x + z = 2$이고 $(x, y, z) = (2 - t, -1, t)$, $t \in \mathbb{R}$이다.

연습문제 4.13 총 거리 180 km를 일정한 속력으로 갈 때 속력을 15 km/h 높이면 시간이 1시간 줄어든다고 하자. 방정식을 세우고 허용되는 해를 구하여라.

풀이. 원래 속력을 $v > 0$이라 하면 $180/v - 180/(v+15) = 1$이다. 정리하면 $v^2 + 15v - 2700 = 0 = (v-45)(v+60)$이다. 상황에 맞는 해는 $v = 45\,\text{km/h}$이다. 음의 후보 -60은 물리적 속력으로 허용되지 않는다.

제 5 장

이차방정식과 근의 구조

개요 이 장은 완전제곱의 변형에서 출발하여 이차방정식 $ax^2+bx+c=0$의 근의 공식과 판별식, 근과 계수의 관계, 중근과 중복도, 치환으로 풀리는 방정식, 그리고 수치 계산에서 근의 공식이 겪는 정확도 문제를 다룬다. 선행 지식: 인수분해, 제곱근, 복소수의 기본. 이 장에서는 실근과 복소근을 구분한다.

5.1 완전제곱 만들기

x^2+px에 $(p/2)^2$을 더하면 $(x+p/2)^2$이 된다. 식의 값을 유지하려면 같은 양을 빼야 한다.

$$x^2+px+q=\left(x+\frac{p}{2}\right)^2+q-\frac{p^2}{4}. \tag{5.1}$$

이 변형은 이차방정식의 근, 이차함수의 꼭짓점, 최솟값을 한꺼번에 설명한다.

> **예제 5.1** $x^2-6x+5=0$은 $(x-3)^2=4$이므로 $x=1,5$이다. $x^2-6x+11=0$은 $(x-3)^2=-2$이므로 실근은 없고 복소근은 $3\pm i\sqrt{2}$이다.

5.2 근의 공식과 판별식

> **정리 5.2 (근의 공식)** $a,b,c\in\mathbb{R}$, $a\neq 0$일 때 $ax^2+bx+c=0$의 복소근은
>
> $$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a} \tag{5.2}$$
>
> 이다. **판별식**(*discriminant*) $D=b^2-4ac$가 양수이면 서로 다른 두 실근, 0이면 **중근**, 음수이면 서로 켤레인 비실수 두 근을 갖는다.

증명. 양변을 a로 나누어 완전제곱을 만들면

$$\left(x+\frac{b}{2a}\right)^2=\frac{b^2-4ac}{4a^2}$$

이다. 또는 분모의 절댓값 문제를 피하여 $(2ax+b)^2=D$로 쓸 수 있다. $2ax+b=\pm\sqrt{D}$를 풀면 식 (5.2)가 된다. D의 부호에 따라 제곱근의 성질을 적용한다. $\square$

핵심 수식

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a},\qquad D=b^2-4ac, \tag{5.3}$$

$$\alpha+\beta=-\frac{b}{a},\qquad \alpha\beta=\frac{c}{a}. \tag{5.4}$$

예제 5.3 $2x^2 - 3x - 2 = 0$에서 $D = 9 + 16 = 25$이므로 $x = (3 \pm 5)/4$이고 근은 $2, -1/2$이다. 인수분해 $(2x+1)(x-2) = 0$과 일치한다.

예제 5.4 $x^2 + 2tx + 1 = 0$이 실근을 가질 필요충분조건은 $4t^2 - 4 \geq 0$, 즉 $t \leq -1$ 또는 $t \geq 1$이다. 중근은 $t = \pm 1$에서 생긴다. 매개변수 조건을 구할 때도 x의 정의역이 실수인지 확인한다.

5.3 근과 계수의 관계

정리 5.5 (근과 계수의 관계) $ax^2 + bx + c$의 두 복소근을 중복도까지 세어 α, β라 하면

$$\alpha + \beta = -\frac{b}{a}, \qquad \alpha\beta = \frac{c}{a}$$

이다.

증명. $a(x-\alpha)(x-\beta) = ax^2 - a(\alpha+\beta)x + a\alpha\beta$의 계수를 비교한다. 근의 공식으로도 두 관계를 직접 확인할 수 있다. $\square$

역사 (비에트의 공식). 근과 계수의 관계는 프랑스의 수학자 François Viète가 16세기 말에 처음 체계적으로 다루었으며, 오늘날에도 **Vieta 공식**(*Vieta's formulas*)이라고 부른다.

예제 5.6 $x^2 - 5x + 3 = 0$의 근을 실제로 구하지 않고 $\alpha^2 + \beta^2$을 계산하면

$$(\alpha+\beta)^2 - 2\alpha\beta = 25 - 6 = 19.$$

또한 $\alpha\beta = 3 \neq 0$이므로 $1/\alpha + 1/\beta = 5/3$이다. 역수는 근이 0이 아님을 확인한 뒤 사용한다.

예제 5.7 합이 s, 곱이 p인 두 실수를 찾으려면 $z^2 - sz + p = 0$의 근을 찾으면 된다. 그런 두 실수가 존재할 필요충분조건은 $s^2 - 4p \geq 0$이다. 합 4, 곱 5는 판별식 -4 때문에 실수에서 실현되지 않는다.

5.4 중근과 중복도

다항식 P가 $(x-a)^m$으로 나누어지고 $(x-a)^{m+1}$로는 나누어지지 않을 때 a를 **중복도**(*multiplicity*) m인 근이라 한다. 서로 다른 해의 개수를 셀 때 중근은 한 개의 값이지만, 대수학의 기본정리에서 차수만큼 근을 센다는 말은 중복도를 포함한다.

참고 (중복도와 도함수). 다항식 P가 a에서 중복도 $m \geq 2$인 근을 가지면 $P(x) = (x-a)^m Q(x)$, $Q(a) \neq 0$으로 쓸 수 있고, $P'(x) = m(x-a)^{m-1}Q(x) + (x-a)^m Q'(x)$이므로 $P'(a) = 0$이다. 반대로 $m = 1$이면 $P'(a) = Q(a) \neq 0$이다. 따라서 a가 P와 P'의 공통근일 필요충분조건에 가까운 성질로 중근 여부를 판정할 수 있으며, 이 생각은 미분과 적분 권의 중근 판정법으로 이어진다(제8권 제2장).

예제 5.8 $P = (x-1)^2(x+2)$의 서로 다른 근은 $1, -2$ 두 개이고, 중복도를 세면 세 개이다. 실수축에서 짝수 중복도 근을 지날 때 인수의 부호가 바뀌지 않고, 홀수 중복도 근에서는 바뀐다. 이 성질은 다항부등식의 부호표를 만드는 데 사용한다.

5.5 치환으로 풀리는 방정식

예제 5.9 $x^4 - 5x^2 + 4 = 0$에서 $u = x^2$으로 두면 $u = 1, 4$이다. 둘 다 비음수이므로 $x = \pm 1, \pm 2$이다. 반면 $x^4 + x^2 - 2 = 0$에서는 $u = 1, -2$이고 실수해는 $u = 1$에서 나온 $x = \pm 1$뿐이다.

예제 5.10 $x + 1/x = 3$은 $x \neq 0$에서 $x^2 - 3x + 1 = 0$과 동치이다. 따라서 $x = (3 \pm \sqrt{5})/2$이다. 두 근의 곱은 1이므로 서로 역수이다. 실수 $x \neq 0$에 대해 $x + 1/x$가 $(-2, 2)$에 들어갈 수 없다는 사실도 제곱 또는 산술기하평균 부등식으로 설명할 수 있다.

5.6 수치 계산에서의 주의

근의 공식은 정확한 대수적 공식이지만 유한 자릿수 계산에서는 큰 두 수의 차 때문에 정확도가 떨어질 수 있다. 예를 들어 $x^2 - 10^8 x + 1 = 0$의 작은 근을

$$\frac{10^8 - \sqrt{10^{16} - 4}}{2}$$

로 계산하면 가까운 수의 차를 취한다. 유리화하면 같은 근은

$$\frac{2}{10^8 + \sqrt{10^{16} - 4}}$$

이므로 작은 차를 직접 계산하지 않는다. 두 근의 곱이 1이라는 관계를 이용해 큰 근을 구한 뒤 역수를 취해도 된다. 대수적 동치와 수치적 안정성은 별개의 성질이다.

5.7 문제와 풀이

연습문제 5.11 $3x^2 + 6x + 7 = 0$의 복소근을 구하여라.

풀이. $3(x+1)^2 + 4 = 0$이므로 $x = -1 \pm 2i/\sqrt{3}$이다. 근의 합은 -2, 곱은 $1 + 4/3 = 7/3$으로 검산된다.

연습문제 5.12 $x^2 - (m+1)x + m = 0$의 근과 중근 조건을 구하여라.

풀이. $(x-1)(x-m) = 0$이므로 근은 $1, m$이다. 중근일 필요충분조건은 $m = 1$이다. 판별식은 $(m-1)^2$이다.

연습문제 5.13 $x^2 - 3x - 1 = 0$의 두 근에 대해 $\alpha^3 + \beta^3$을 구하여라.

풀이. $\alpha + \beta = 3$, $\alpha\beta = -1$이다. 따라서 $\alpha^3 + \beta^3 = (\alpha+\beta)^3 - 3\alpha\beta(\alpha+\beta) = 27 + 9 = 36$이다.

연습문제 5.14 $x^2 + bx + c$가 모든 실수에서 양수일 필요충분조건을 구하여라.

풀이. $(x + b/2)^2 + c - b^2/4$의 최솟값이 $c - b^2/4$이다. 따라서 $c > b^2/4$가 필요충분하다. "비음수"라면 등호를 포함해 $c \geq b^2/4$이다.

연습문제 5.15 $x^2 + 1/x^2 = 7$을 실수에서 풀어라.

풀이. $x \neq 0$이고 $(x + 1/x)^2 = 9$이다. 따라서 $x + 1/x = 3$ 또는 -3이다. 각각 이차식을 풀어 $x = (3 \pm \sqrt{5})/2$와 $x = (-3 \pm \sqrt{5})/2$ 네 해를 얻는다.

제 6 장

유리방정식과 무리방정식

개요 이 장은 분모나 근호 안에 미지수가 있는 방정식을 다룬다. **유리방정식**(*rational equation*)에서는 분모가 0이 되는 값을 배제한 뒤 공통분모를 곱하는 절차를, **무리방정식**(*radical equation*)에서는 제곱이 만드는 가짜 해와 나눗셈이 버리는 잃어버린 해를 구분하는 방법을 제시한다. 절댓값 방정식은 거리의 관점에서 다룬다. 선행 지식: 정의역, 인수분해, 제곱근, 일차·이차방정식.

6.1 분모 제거의 정확한 순서

유리방정식은 미지수가 분모에 들어갈 수 있는 방정식이다. 모든 분모가 0이 아닌 범위를 먼저 기록하고, 그 범위에서 공통분모를 곱한다. 이때 곱하는 값은 범위 안에서 0이 아니므로 변형이 동치이다. 얻어진 다항방정식의 근 중 제외값을 제거한다.

예제 6.1 $1/(x-1) + 1/(x+1) = 1$에서 $x \neq \pm 1$이다. 양변에 $x^2 - 1$을 곱하면 $2x = x^2 - 1$이고 $x = 1 \pm \sqrt{2}$이다. 두 값 모두 제외값이 아니므로 둘 다 해이다.

예제 6.2

$$\frac{x}{x-1} = \frac{1}{x-1}$$

에서 $x \neq 1$이다. 분모를 곱하면 $x = 1$이지만 허용 범위를 벗어나므로 해가 없다. 분모를 없앤 식만 보고 1을 답으로 적으면 원래 식의 정의역을 잃는다.

6.2 가짜 해와 잃어버린 해

곱하거나 제곱하는 단계는 필요조건을 만들 수 있고, 나누는 단계는 해를 버릴 수 있다. 이를 구분해 관리하면 풀이 전체의 논리 방향이 분명해진다. 계산 끝에서 대입만 한다고 해서 이미 버린 해가 자동으로 복구되지는 않는다. 따라서 나누기 전에는 그 인수가 0인 경우를 먼저 보존해야 한다.

예제 6.3

$$\frac{x^2 - 1}{x - 1} = 2$$

의 허용 범위는 $x \neq 1$이다. 약분하면 $x + 1 = 2$에서 $x = 1$이 나오지만 제외값이므로 해가 없다. 반면 분모가 없는 $x^2 - 1 = 2(x-1)$은 $(x-1)^2 = 0$이라 $x = 1$을 해로 갖는다. 두 식은 허용 범위가 다르다.

6.3 제곱근 하나가 있는 방정식

명제 6.4 (제곱근 방정식의 동치 조건) 실수값 식 A, B에 대해 $\sqrt{A} = B$는

$$A \geq 0, \qquad B \geq 0, \qquad A = B^2$$

와 동치이다. 사실 마지막 두 조건이면 $A \geq 0$은 자동으로 따른다.

증명. 원래 식이 참이면 제곱근의 정의에 의해 두 부호 조건과 제곱 등식이 성립한다. 역으로 $A = B^2$, $B \geq 0$이면 $\sqrt{A} = \sqrt{B^2} = |B| = B$이다. □

예제 6.5 $\sqrt{2x+3} = x$는 $x \geq 0$, $2x+3 = x^2$과 동치이다. 이차식 $(x-3)(x+1) = 0$의 후보 중 $x = 3$만 비음수이므로 해이다.

예제 6.6 $\sqrt{x+4} = x - 2$는 $x \geq 2$를 요구한다. 제곱하면 $x + 4 = x^2 - 4x + 4$, 즉 $x(x-5) = 0$이다. 0은 부호 조건을 만족하지 않으며 해는 5이다. 실제로 $\sqrt{9} = 3$이다.

6.4 제곱근 둘과 반복 제곱

먼저 한 제곱근을 고립시키거나, 합의 부호를 이용하여 한 번 제곱한 식을 단순하게 만든다. 다시 제곱할 때에도 양변의 부호 조건을 추적한다. 여러 번 제곱하면 후보가 많아질 수 있으므로 마지막에 원래 식에 대입하는 검증이 특히 중요하다.

예제 6.7 $\sqrt{x+1} + \sqrt{x-2} = 3$을 풀자. 정의역은 $x \geq 2$이다. 두 변을 제곱하면

$$2x - 1 + 2\sqrt{(x+1)(x-2)} = 9,$$

즉 $\sqrt{(x+1)(x-2)} = 5 - x$이다. 따라서 추가로 $x \leq 5$가 필요하다. 다시 제곱하면 $x^2 - x - 2 = x^2 - 10x + 25$, $x = 3$이다. 원래 식에서 $2 + 1 = 3$이므로 해이다.

예제 6.8 $\sqrt{x+1} - \sqrt{x-2} = 3$은 해가 없다. $x \geq 2$에서 왼쪽은

$$\frac{3}{\sqrt{x+1} + \sqrt{x-2}} \leq \frac{3}{\sqrt{3}} = \sqrt{3} < 3$$

이기 때문이다. 무조건 여러 번 제곱하기 전에 범위와 크기를 살피면 더 짧게 해결할 수 있다.

방법 (무리방정식을 푸는 절차).

1단계. 근호 안 식(진수)이 비음수라는 조건과, 등식 양변의 부호 조건을 먼저 적는다.

2단계. 제곱근을 하나만 남기도록 식을 정리한 뒤 양변을 제곱한다.

3단계. 제곱근이 남아 있으면 다시 고립시켜 제곱하고, 그때마다 부호 조건을 추적한다.

4단계. 얻은 다항방정식을 풀고, 처음에 적은 모든 조건과 원래 식에 후보를 대입해 검증한다.

6.5 절댓값 방정식과 거리

절댓값 $|x-a|$는 실수축에서 x와 a 사이의 거리이다. $c<0$이면 $|x-a|=c$는 해가 없고, $c=0$이면 $x=a$, $c>0$이면 $x=a\pm c$이다. 절댓값이 여러 개이면 부호가 바뀌는 지점을 기준으로 구간을 나눈다.

예제 6.9 $|x-1|=2x+1$에서 오른쪽은 비음수여야 하므로 $x\ge -1/2$이다. $x\ge 1$이면 $x-1=2x+1$에서 $x=-2$로 구간에 속하지 않는다. $-1/2\le x<1$이면 $1-x=2x+1$이므로 $x=0$이다. 따라서 유일한 해는 0이다.

예제 6.10 $|x-1|+|x-4|=5$를 풀자. $x<1$이면 $5-2x=5$에서 $x=0$이다. $1\le x\le 4$에서는 합이 3으로 일정하여 해가 없다. $x>4$이면 $2x-5=5$에서 $x=5$이다. 거리 관점에서 구간 $[1,4]$ 안의 거리 합은 항상 두 끝점 사이 거리 3이다.

6.6 문제와 풀이

연습문제 6.11

$$\frac{2}{x-2}=\frac{3}{x+1}$$

을 풀어라.

풀이. $x\neq 2,-1$에서 $2(x+1)=3(x-2)$, 따라서 $x=8$이다. 두 분모는 각각 $6,9$이고 양쪽 모두 $1/3$이다.

연습문제 6.12 $\sqrt{3x+4}=x+2$를 풀어라.

풀이. 제곱하면 $3x+4=x^2+4x+4$이므로 $x(x+1)=0$이다. 후보 $0,-1$은 모두 $x+2\ge 0$과 진수 조건을 만족한다. 실제로 $\sqrt{4}=2$, $\sqrt{1}=1$이므로 둘 다 해이다.

연습문제 6.13 $\sqrt{x}=x-2$를 풀어라.

풀이. $x\ge 2$에서 $x=x^2-4x+4$이고 $(x-1)(x-4)=0$이다. 따라서 해는 4뿐이다. 1은 제곱 후에 생긴 후보이다.

연습문제 6.14 $|2x-3|=|x+1|$을 풀어라.

풀이. 두 변이 비음수이므로 제곱이 동치이다. $(2x-3)^2=(x+1)^2$을 제곱의 차로 분해하면 $(x-4)(3x-2)=0$이다. 따라서 $x=4,2/3$이다.

연습문제 6.15 $\sqrt{x+9}-\sqrt{x}=1$을 풀어라.

풀이. $x\ge 0$에서 첫 제곱근을 고립시켜 $\sqrt{x+9}=1+\sqrt{x}$로 쓴다. 두 변이 비음수이므로 제곱하면 $9=1+2\sqrt{x}$, 따라서 $\sqrt{x}=4$, $x=16$이다. 원래 식은 $5-4=1$이다.

참고 (다음 연결). 방정식의 동치 변형은 논리학의 추론 규칙과 연결된다. 알고리즘으로 해를 구할 때에도 입력의 정의역, 역연산의 존재, 해의 보존을 명시해야 한다.

제 7 장

부등식의 해집합과 부호표

개요 이 장은 부등식의 양변에 수를 더하거나 곱할 때 부등호가 보존되거나 뒤집히는 규칙에서 출발하여, 연립부등식의 교집합·합집합, 인수분해된 다항식과 유리식의 **부호표**(*sign chart*), 절댓값 부등식을 다룬다. 선행 지식: 실수의 순서, 구간 표기, 인수분해.

7.1 부등호를 보존하거나 뒤집는 연산

실수 $a < b$에 같은 실수 c를 더하면 $a + c < b + c$이다. 양수 c를 곱하면 $ac < bc$이고, 음수 c를 곱하면 $ac > bc$이다. 음수를 곱할 때 부등호가 뒤집히는 이유는 양수 $b - a$에 음수 c를 곱하면 $c(b - a) < 0$이 되기 때문이다.

역수를 취할 때는 부호를 확인한다. $0 < a < b$이면 $1/a > 1/b$이고, $a < b < 0$일 때도 $1/a > 1/b$이다. 그러나 $a < 0 < b$이면 $1/a < 1/b$로 원래 방향이 유지된다. 따라서 "역수면 항상 뒤집는다"는 규칙은 같은 부호인 두 수에 한정된다.

> **예제 7.1** $3 - 2x < 7$에서 $-2x < 4$를 얻고 음수 -2로 나누면 $x > -2$이다. 해집합은 $(-2, \infty)$이다. 경계값 -2는 원래 식에서 등호를 만들므로 엄격한 부등식의 해에 포함되지 않는다.

> **예제 7.2** $ax < 1$을 매개변수 a에 따라 풀면 $a > 0$에서 $x < 1/a$, $a < 0$에서 $x > 1/a$, $a = 0$에서 모든 실수가 해이다. 상수항이 바뀌어 $ax < -1$이면 $a = 0$에서 해가 없어진다.

7.2 연립부등식과 합집합

두 조건을 모두 만족해야 하면 해집합의 교집합을 취한다. 둘 중 하나라도 만족하면 되면 합집합을 취한다. $-1 < x \le 3$은 $x > -1$과 $x \le 3$의 교집합이며 $(-1, 3]$이다. $x < -1$ 또는 $x > 3$은 $(-\infty, -1) \cup (3, \infty)$이다.

> **예제 7.3** $2x - 1 \ge 3$, $3x + 2 < 14$를 동시에 풀면 $x \ge 2$, $x < 4$이므로 해는 $[2, 4)$이다. 두 경계에서 등호를 허용하는지가 각각 다르다.

7.3 곱의 부호와 이차부등식

0이 아닌 두 실수의 곱은 두 수의 부호가 같을 때 양수이고 다를 때 음수이다. 인수분해한 식에서 각 인수의 부호가 바뀌는 점을 찾고 그 사이 구간의 부호를 조사한다.

> **예제 7.4** $(x - 1)(x + 2) > 0$의 경계는 $-2, 1$이다. $x < -2$에서는 두 인수가 음수이므로 곱이 양수, $-2 < x < 1$에서는 서로 다른 부호이므로 음수, $x > 1$에서는 둘 다 양수이다. 따라서 해는 $(-\infty, -2) \cup (1, \infty)$이다.

명제 7.5 $a > 0$이고 $\alpha < \beta$이면 $a(x-\alpha)(x-\beta)$는 두 근 바깥에서 양수이고 두 근 사이에서 음수이다. $a < 0$이면 부호가 반대이다.

근이 없는 이차식에서는 판별식과 최고차항의 부호를 사용한다. $a > 0$, $D < 0$이면 모든 실수에서 양수이다. $a > 0$, $D = 0$이면 중근에서만 0이고 나머지에서 양수이다. 완전제곱을 만들면 이 사실을 직접 확인할 수 있다.

예제 7.6 $-2x^2 + 4x - 5 < 0$은 모든 실수에서 참이다. 식을 $-2(x-1)^2 - 3$으로 쓰면 항상 -3 이하이다. 근이 없다는 이유만으로 부등식에 해가 없다고 판단하면 안 된다.

7.4 고차식의 부호와 중복도

실수 인수분해가 알려졌으면 각 실근에서 부호가 바뀌는지 확인한다. $(x-a)^m$은 m이 홀수일 때 a를 지날 때 부호가 바뀌고, m이 짝수일 때 바뀌지 않는다. 실근이 없는 이차 인수는 부호가 일정하다.

예제 7.7 $(x-1)^2(x+2)(x-3) \le 0$에서 제곱 인수는 $x \neq 1$에서 양수이다. 나머지 곱은 $[-2, 3]$에서 비양수이다. $x = 1$도 이 구간 안에 있고 전체 식을 0으로 만든다. 따라서 해집합은 $[-2, 3]$이다. 반면 > 0이면 $(-\infty, -2) \cup (3, \infty)$이다.

예제 7.8 $(x-1)^2(x+2) > 0$이면 $x + 2 > 0$이면서 $x \neq 1$이어야 한다. 해는 $(-2, 1) \cup (1, \infty)$이다. 짝수 중복도 근은 부호를 바꾸지는 않지만 엄격한 부등식에서는 제외되는 구멍을 만들 수 있다.

7.5 유리부등식의 분모

미지수를 포함한 분모의 부호를 모른 채 양변에 분모를 곱하면 부등호 방향을 결정할 수 없다. 한 쪽으로 모두 옮겨 단일 분수로 만든 뒤, 분자와 분모의 0점으로 구간을 나누는 방법이 안전하다. 분모의 0점은 등호를 허용하는 부등식에서도 해가 아니다.

예제 7.9

$$\frac{x+1}{x-2} \ge 0$$

의 경계는 $-1, 2$이다. $x < -1$에서는 음수끼리 나누어 양수, $-1 < x < 2$에서는 양수를 음수로 나누어 음수, $x > 2$에서는 양수이다. 분자 0점 -1은 포함하고 분모 0점 2는 제외하여

$$(-\infty, -1] \cup (2, \infty)$$

를 얻는다.

예제 7.10 $1/x > 1$은 $x \neq 0$에서 $(1-x)/x > 0$이다. 해는 $0 < x < 1$이다. 처음부터 양변에 x를 곱해 $1 > x$라고 쓰면 음수 x까지 잘못 포함한다.

분모의 제곱을 곱하는 방법도 가능하다. $Q(x) \neq 0$인 범위에서 $Q(x)^2 > 0$이므로 $P(x)/Q(x) > 0$과 $P(x)Q(x) > 0$은 동치이다. 단 원래 제외값을 끝까지 보존한다.

방법 (부호표를 이용한 부등식 풀이).

1단계. 모든 항을 한쪽으로 모아 인수분해한다. 분수식이면 분자와 분모를 각각 인수분해한다.

2단계. 각 인수가 0이 되는 점(분수식이면 분모가 0이 되는 점도 포함)을 실수축 위에 표시한다.

3단계. 각 구간에서 대표값을 넣어 전체 식의 부호를 정하거나, 각 인수의 중복도의 홀짝으로 부호가 바뀌는지 판단한다.

4단계. 부등식의 등호 포함 여부에 따라 경계점의 포함을 결정하고, 분모가 0인 점은 항상 제외한다.

7.6 절댓값 부등식

$r > 0$일 때

$$|x-a| < r \iff a-r < x < a+r, \tag{7.1}$$

$$|x-a| > r \iff x < a-r \text{ 또는 } x > a+r. \tag{7.2}$$

이는 거리가 r보다 가까운지 먼지를 표현한다. $r = 0$ 또는 음수인 경우를 같은 공식에 무심코 넣지 않는다. 예를 들어 $|x-a| < 0$의 해는 없고 $|x-a| \geq 0$은 모든 실수에서 참이다.

핵심 수식

$$|x-a| < r \iff a-r < x < a+r, \qquad r > 0, \tag{7.3}$$

$$|x-a| > r \iff x < a-r \text{ 또는 } x > a+r, \qquad r > 0. \tag{7.4}$$

예제 7.11 $|2x-3| \leq 5$는 $-5 \leq 2x-3 \leq 5$와 동치이므로 $-1 \leq x \leq 4$이다. $|x-1| < x+1$에서는 오른쪽이 양수여야 하고, 제곱 비교로 $(x-1)^2 < (x+1)^2$에서 $x > 0$을 얻는다. 이 범위에서 오른쪽은 실제 양수이므로 해집합은 $(0, \infty)$이다.

7.7 문제와 풀이

연습문제 7.12 $x^2 - 5x + 6 \leq 0$을 풀어라.

풀이. $(x-2)(x-3) \leq 0$이므로 해는 $[2, 3]$이다.

연습문제 7.13

$$\frac{x-1}{(x+2)^2} > 0$$

을 풀어라.

풀이. $x \neq -2$에서 분모는 양수이므로 $x - 1 > 0$이어야 한다. 해는 $(1, \infty)$이고 제외값 -2는 이 범위 밖이다.

연습문제 7.14

$$\frac{x^2-1}{x-1} \leq 0$$

을 풀어라.

풀이. 원래 정의역은 $x \neq 1$이다. 약분 뒤 $x+1 \le 0$이므로 $x \le -1$이다. 이 범위에 제외값이 없으므로 해는 $(-\infty, -1]$이다.

연습문제 7.15 $|x-2| + |x+1| \le 3$을 풀어라.

풀이. 삼각부등식에 의해 왼쪽은 항상 3 이상이다. $-1 \le x \le 2$에서 $(2-x)+(x+1)=3$이고, 구간 밖에서는 더 크다. 따라서 해는 $[-1, 2]$이다.

연습문제 7.16 $x^2 + 2ax + a + 2 > 0$이 모든 실수 x에 대해 성립할 a를 구하여라.

풀이. 최솟값은 $a + 2 - a^2$이다. 이것이 양수여야 하므로 $(a-2)(a+1) < 0$, 즉 $-1 < a < 2$이다. 끝점에서는 중근이 생겨 엄격한 양수 조건을 만족하지 않는다.

제 8 장

부등식의 증명과 최댓값·최솟값

개요 이 장은 상계와 최댓값을 구분하는 데서 출발하여, 제곱의 비음수성을 이용한 부등식 증명, 산술평균–기하평균 부등식, 코시–슈바르츠 부등식과 그 분수 꼴(따름정리), 조건이 있는 최적화 문제를 다룬다. 선행 지식: 제곱의 비음수성, 실수의 순서, 절댓값. 최적값의 존재와 단순 상계를 구분한다.

8.1 상계와 실제 최댓값

모든 허용 입력에서 $f(x) \le M$이면 M은 값들의 **상계**(*upper bound*)이다. 어떤 허용 입력 x_0에서 $f(x_0) = M$까지 성립하면 M은 **최댓값**(*maximum*)이다. 따라서 최댓값 증명은 부등식과 등호 달성이라는 두 부분으로 구성된다. 열린 구간에서는 상한은 있어도 최댓값이 없을 수 있다.

> **예제 8.1** $0 < x < 1$에서 $f(x) = x$는 항상 $f(x) < 1$이고 상한은 1이지만 최댓값은 없다. $0 \le x \le 1$로 바꾸면 $x = 1$에서 최댓값 1을 갖는다. 허용 범위의 끝점이 포함되는지 확인해야 한다.

8.2 제곱의 합으로 바꾸기

> **명제 8.2** 실수 a, b에 대해 $a^2 + b^2 \ge 2ab$이며 등호는 $a = b$일 때만 성립한다.

증명. $a^2 + b^2 - 2ab = (a - b)^2 \ge 0$이다. 제곱이 0일 필요충분조건은 $a - b = 0$이다. □

> **예제 8.3** 실수 x에 대해 $x^2 - 6x + 13 = (x - 3)^2 + 4 \ge 4$이다. 등호는 $x = 3$에서 성립하므로 최솟값은 4이다. 정의역을 $x > 4$로 바꾸면 값은 5보다 크고 하한은 5이지만 최솟값은 없다.

> **예제 8.4** $a + b + c = 0$이면 $a^2 + b^2 + c^2 = -2(ab + bc + ca)$이다. 왼쪽이 비음수이므로 $ab + bc + ca \le 0$이다. 등호는 세 수가 모두 0일 때만 성립한다. 조건식을 제곱하여 유용한 관계를 얻은 예이다.

8.3 산술평균과 기하평균

> **정리 8.5 (산술기하평균 부등식, 두 변수)** $a, b \ge 0$이면
>
> $$\sqrt{ab} \le \frac{a + b}{2},$$
>
> 이며 등호는 $a = b$일 때만 성립한다.

증명. $(\sqrt{a} - \sqrt{b})^2 \ge 0$을 전개한다. □

예제 8.6 $x, y > 0$, $x + y = 10$이면 $xy \le 25$이고 등호는 $x = y = 5$에서 성립한다. 따라서 넓이 xy인 직사각형의 둘레가 20으로 고정되면 정사각형이 최대 넓이를 갖는다. 양수 조건과 둘레를 절반으로 나눈 합의 조건을 정확히 구분한다.

예제 8.7 $x > 0$에서 $x + 9/x \ge 2\sqrt{9} = 6$이며 등호는 $x = 9/x$, 즉 $x = 3$에서 성립한다. $x < 0$까지 허용하면 이 부등식은 같은 방향으로 성립하지 않는다. 적용할 두 항이 비음수인지 먼저 확인한다.

일반적인 n개 비음수에 대한 산술기하평균 부등식은

$$\left(\prod_{j=1}^{n} a_j\right)^{1/n} \le \frac{1}{n}\sum_{j=1}^{n} a_j \tag{8.1}$$

이다. 양수인 경우에는 로그함수의 오목성과 옌센 부등식으로 증명할 수 있다. 이 경로는 미분과 볼록성을 사용하므로 여기서는 두 변수의 완전한 증명과 구별한다. 0인 항이 있는 경우는 양수 근사 또는 직접적인 비음수성으로 처리한다. 모든 a_j가 같을 때, 그리고 그때만 등호이다.

핵심 수식

$$\sqrt{ab} \le \frac{a+b}{2}, \qquad a, b \ge 0, \tag{8.2}$$

$$\left(\prod_{j=1}^{n} a_j\right)^{1/n} \le \frac{1}{n}\sum_{j=1}^{n} a_j, \qquad a_j \ge 0, \tag{8.3}$$

$$\left(\sum_{j=1}^{n} a_j b_j\right)^2 \le \left(\sum_{j=1}^{n} a_j^2\right)\left(\sum_{j=1}^{n} b_j^2\right). \tag{8.4}$$

8.4 코시–슈바르츠 부등식

정리 8.8 (Cauchy–Schwarz 부등식) 실수 $a_1, \dots, a_n, b_1, \dots, b_n$에 대해

$$\left(\sum_{j=1}^{n} a_j b_j\right)^2 \le \left(\sum_{j=1}^{n} a_j^2\right)\left(\sum_{j=1}^{n} b_j^2\right). \tag{8.5}$$

등호는 두 벡터 (a_j)와 (b_j)가 선형종속일 때만 성립한다. 여기에는 한 벡터가 영벡터인 경우도 포함한다.

증명. $\sum b_j^2 = 0$이면 모든 $b_j = 0$이라 자명하다. 그렇지 않으면 모든 실수 t에 대해

$$0 \le \sum (a_j - t b_j)^2 = A - 2Bt + Ct^2,$$

여기서 $A = \sum a_j^2$, $B = \sum a_j b_j$, $C = \sum b_j^2 > 0$이다. $t = B/C$를 대입하면 $A - B^2/C \ge 0$으로 원하는 결과를 얻는다. 등호일 때에는 제곱합의 모든 항이 0이므로 $a_j = (B/C) b_j$이다. □

역사 (세 이름의 부등식). 식 (8.5)는 Augustin-Louis Cauchy가 1821년에 유한 합의 형태로, Viktor Bunyakovsky가 1859년에 적분 형태로, Hermann Schwarz가 1888년에 다시 적분 형태로 독립적

으로 다루었다. 그래서 적분형을 가리킬 때에는 Cauchy–Bunyakovsky–Schwarz 부등식이라고도 부른다.

> **예제 8.9** $x^2+y^2=1$이면 $|3x+4y|\le 5$이다. 일차식 $3x+4y$의 최댓값 5는 $(x,y)=(3/5,4/5)$에서, 최솟값 -5는 반대 점에서 달성된다. 절댓값의 상계를 구한 뒤 원래 일차식의 최댓값과 최솟값을 따로 확인한다.

> **예제 8.10** $u,v,w>0$이면
> $$(u+v+w)\left(\frac{1}{u}+\frac{1}{v}+\frac{1}{w}\right)\ge 9.$$
> 코시–슈바르츠에서 두 벡터를 $(\sqrt{u},\sqrt{v},\sqrt{w})$와 $(1/\sqrt{u},1/\sqrt{v},1/\sqrt{w})$로 택한다. 등호 조건은 $u=v=w$이다.

8.5 분수 꼴의 코시–슈바르츠

> **따름정리 8.11 (Engel 형태)** $b_j>0$이고 $a_j\in\mathbb{R}$이면
> $$\sum_{j=1}^{n}\frac{a_j^2}{b_j}\ge\frac{\left(\sum_{j=1}^{n}a_j\right)^2}{\sum_{j=1}^{n}b_j}.$$
> 등호는 모든 a_j/b_j가 같을 때만 성립한다.

증명. 두 벡터 $a_j/\sqrt{b_j}$와 $\sqrt{b_j}$에 코시–슈바르츠를 적용하고 양수 $\sum b_j$로 나눈다. □

> **예제 8.12** $a,b,c>0$일 때
> $$\frac{a^2}{b+c}+\frac{b^2}{c+a}+\frac{c^2}{a+b}\ge\frac{a+b+c}{2}.$$
> 분모의 합이 $2(a+b+c)$이므로 바로 따른다. 등호 조건 $a/(b+c)=b/(c+a)=c/(a+b)$은 양수 조건 아래에서 $a=b=c$와 동치이다.

8.6 단조성과 조건의 활용

식의 최댓값을 구할 때 모든 변수를 독립적으로 최대화하면 제약 조건을 어길 수 있다. 먼저 조건을 사용해 변수를 줄이거나, 등호가 동시에 성립할 수 있는 부등식을 선택한다.

> **예제 8.13** $x,y\ge 0$, $x+y=1$일 때 $x^2+y^2=1-2xy\le 1$이고 끝점 $(1,0),(0,1)$에서 최댓값 1이다. 반면 $xy\le 1/4$이므로 최솟값은 $1/2$이고 $x=y=1/2$에서 달성한다. 같은 제약에서 곱의 최대와 제곱합의 최대는 서로 다른 위치에서 생긴다.

흔한 오류. 부등식의 등호 조건을 무시하면 도달할 수 없는 상계를 최댓값이라고 부를 수 있다. 여러 부등식을 이어 쓸 때에는 모든 등호 조건이 동시에 가능한지 확인한다.

8.7 문제와 풀이

연습문제 8.14 $x>0$에서 $2x+8/x$의 최솟값을 구하여라.

풀이. 두 양수의 곱은 16이므로 합은 8 이상이다. 등호 조건 $2x=8/x$에서 $x=2$이며 최솟값은 8이다.

연습문제 8.15 $x^2+y^2=4$에서 $x-\sqrt{3}y$의 범위를 구하여라.

풀이. 코시–슈바르츠로 절댓값은 $\sqrt{1+3}\sqrt{4}=4$ 이하이다. $(x,y)=(1,-\sqrt{3})$에서 4, 반대 점에서 -4이다. 원 위를 연속적으로 움직이면 중간 값도 얻으므로 범위는 $[-4,4]$이다.

연습문제 8.16 $a,b,c\in\mathbb{R}$에 대해 $a^2+b^2+c^2\ge ab+bc+ca$를 증명하여라.

풀이. 차이는 $[(a-b)^2+(b-c)^2+(c-a)^2]/2$이다. 비음수이며 등호는 $a=b=c$에서만 성립한다.

연습문제 8.17 $a,b>0$, $a+b=1$에서 $1/a+1/b$의 최솟값을 구하여라.

풀이. $1/a+1/b=(a+b)/(ab)=1/(ab)$이고 $ab\le 1/4$이므로 합은 4 이상이다. 등호는 $a=b=1/2$에서 성립한다.

연습문제 8.18 $0<x<2$에서 $x(2-x)$의 최대와 최소를 설명하여라.

풀이. $x(2-x)=1-(x-1)^2$이므로 $x=1$에서 최댓값 1이다. 값은 항상 양수이고 $x\to 0^+$에서 0으로 접근하므로 하한은 0이다. 끝점이 제외되어 최솟값은 없다.

제 9 장

지수·로그 방정식과 매개변수

개요 이 장은 지수함수와 로그함수의 단사성에서 출발하여 지수방정식·로그방정식의 동치 변형, 로그 부등식에서 밑의 크기에 따른 부등호 방향, 지수함수와 다항식의 성장 비교, 매개변수에 따라 해의 개수가 바뀌는 문제를 다룬다. 선행 지식: 지수와 로그의 정의, 정의역, 단조함수, 이차방정식.

9.1 같은 밑으로 바꾸는 원리

$a>0,\ a\neq 1$일 때 실수 지수함수 $x\mapsto a^x$는 단사이다. 따라서 $a^u=a^v$와 $u=v$는 동치이다. $a>1$이면 증가함수이고 $0<a<1$이면 감소함수라는 점은 부등식의 방향을 결정한다.

예제 9.1 $2^{x+1}=8^{x-1}$은 $2^{x+1}=2^{3x-3}$이므로 $x+1=3x-3$, $x=2$이다. 두 변은 각각 8이다.

예제 9.2 $(1/3)^{2x-1}\geq (1/3)^{x+2}$에서 밑이 1보다 작으므로 $2x-1\leq x+2$이다. 해는 $x\leq 3$이다.

지수가 변수라는 이유만으로 다항식 기법을 버릴 필요는 없다. $a^{2x}=(a^x)^2$처럼 같은 지수 표현이 반복되면 새 변수로 치환한다. 단 새 변수는 양수라는 제약이 있다.

예제 9.3 $4^x-5\cdot 2^x+4=0$에서 $t=2^x>0$라 하면 $(t-1)(t-4)=0$이다. 따라서 $t=1,4$, 즉 $x=0,2$이다.

9.2 로그 방정식과 진수 조건

$a>0,\ a\neq 1$에서 $\log_a u=\log_a v$는 $u,v>0$라는 정의역 안에서 $u=v$와 동치이다. 로그의 덧셈을 곱으로 합치는 법칙도 원래 각 진수가 양수라는 조건을 유지해야 한다.

핵심 수식

$$a^u=a^v \iff u=v, \qquad a>0,\ a\neq 1, \tag{9.1}$$

$$\log_a u=\log_a v \iff u=v, \qquad a>0,\ a\neq 1,\ u,v>0. \tag{9.2}$$

예제 9.4 $\log_2(x-1)+\log_2(x+2)=2$에서 원래 정의역은 $x>1$이다. 로그를 합치면 $(x-1)(x+2)=4$이고 $x^2+x-6=0$이다. 후보 $2,-3$ 중 2만 원래 정의역에 있으므로 해는 2이다. 곱의 양수 조건만 사용하면 -3을 잘못 포함할 수 있다.

예제 9.5 $\log_x 16=4$의 밑 조건은 $x>0,\ x\neq 1$이다. 정의로 $x^4=16$이고 양의 해는 $x=2$이다. 음의 후보 -2는 실수 로그의 밑으로 허용되지 않는다.

흔한 오류. 로그의 합을 진수의 곱으로 바꾸거나 반대로 바꿀 때, 바뀌기 전과 후의 정의역이 서로 다를 수 있다. 더 넓어진 쪽(곱)의 양수 조건만 확인하면 원래 식에서는 정의되지 않는 해를 잘못 포함하게 된다. 로그를 합치거나 나누기 전의 원래 정의역을 끝까지 보존해야 한다.

9.3 로그 부등식

밑이 1보다 크면 로그는 증가하고, 0과 1 사이이면 감소한다. 진수의 양수 조건을 먼저 구한 다음 부등호의 방향을 바꾸거나 유지한다.

예제 9.6 $\log_{1/2}(x-1) > -2$에서 $x > 1$이다. 감소함수이므로 $0 < x-1 < (1/2)^{-2} = 4$이고 해는 $1 < x < 5$이다.

예제 9.7 $\log_2(x^2 - 3x) > 1$은 $x^2 - 3x > 2$와 동치이다. 오른쪽 조건이 진수의 양수성도 보장한다. 이차식의 근이 $(3 \pm \sqrt{17})/2$이므로 해는 그 두 근 바깥의 열린 구간이다.

9.4 지수 성장의 비교와 정확한 의미

$a > 1$인 지수함수 a^x와 다항식의 성장 비교는 극한의 정리이다. 유한한 작은 x에서는 다항식이 더 클 수 있고, 결국 지수함수가 커진다는 말과 모든 x에서 크다는 말은 다르다. 예를 들어 $2^x > x^2$는 $x = 3$에서 거짓이고 $x = 4$에서 등호이며 정수 $x \geq 5$에서는 참이다.

명제 9.8 모든 정수 $n \geq 5$에 대해 $2^n > n^2$이다.

증명. $n = 5$에서 $32 > 25$이다. $2^n > n^2$라고 가정하면 $2^{n+1} > 2n^2$이다. $n \geq 3$이면 $2n^2 - (n+1)^2 = n^2 - 2n - 1 > 0$이므로 $2^{n+1} > (n+1)^2$이다. 수학적 귀납법으로 결론을 얻는다. $\square$

이 증명은 정수 입력에 대한 명제이며, 모든 실수 입력이나 임의 차수 다항식의 극한 비교를 자동으로 증명한 것은 아니다. 더 일반적인 비교는 미적분 권에서 다룬다(제8권 제3장).

9.5 매개변수 문제의 경계 찾기

매개변수가 바뀌면 해의 개수가 바뀔 수 있다. 그 변화는 정의역 경계, 중근, 계수가 0이 되는 지점, 단조성의 변화에서 자주 일어난다. 각각의 경우를 나누어 해집합이 어떻게 달라지는지 조사한다.

예제 9.9 $2^{2x} - a \cdot 2^x + 1 = 0$의 실수해 개수를 구하자. $t = 2^x > 0$로 두면 $t^2 - at + 1 = 0$이다. 두 근의 곱은 1이고 합은 a이다. $a > 2$이면 서로 다른 양의 두 근이 있어 서로 다른 실수해 두 개, $a = 2$이면 $t = 1$의 중근으로 $x = 0$ 하나이다. $a < 2$에서는 양의 근이 없다. 특히 $a \leq -2$에서 생기는 실근은 음수여서 치환의 범위 밖이다.

예제 9.10 $|x| = a - x$를 a에 따라 풀자. $x \geq 0$에서는 $x = a - x$이므로 $x = a/2$이며 $a \geq 0$일 때 가능하다. $x < 0$에서는 $-x = a - x$이므로 $a = 0$이어야 한다. 따라서 $a > 0$이면 해가 $a/2$ 하나, $a = 0$이면 모든 $x \leq 0$, $a < 0$이면 해가 없다. 경계 매개변수에서 해가 갑자기 무한히 많아질 수도 있다.

9.6 문제와 풀이

연습문제 9.11 $9^x - 10 \cdot 3^x + 9 = 0$을 풀어라.

풀이. $t = 3^x > 0$라 하면 $(t-1)(t-9) = 0$이다. 따라서 $x = 0, 2$이다.

연습문제 9.12 $\log_3(x+2) - \log_3 x = 1$을 풀어라.

풀이. 정의역은 $x > 0$이다. $(x+2)/x = 3$이므로 $x = 1$이다. 로그의 차는 진수의 차가 아니라 비의 로그이다.

연습문제 9.13 $\log_{1/2}(2x+1) \le 1$을 풀어라.

풀이. 정의역 $2x+1 > 0$에서 감소성을 적용하면 $2x+1 \ge 1/2$이다. 따라서 $x \ge -1/4$이고 이 조건은 정의역도 보장한다.

연습문제 9.14 $x^2 - 2ax + a = 0$이 서로 다른 양의 실근 두 개를 가질 조건을 구하여라.

풀이. 판별식 $4a(a-1) > 0$, 근의 합 $2a > 0$, 곱 $a > 0$을 동시에 요구한다. 따라서 $a > 1$이다. 판별식 조건만 쓰면 $a < 0$도 포함되어 잘못된다.

연습문제 9.15 $2^x + 2^{-x} \ge 2$를 증명하고 등호 조건을 구하여라.

풀이. 두 항은 양수이며 곱이 1이므로 산술기하평균 부등식으로 합은 2 이상이다. 등호는 $2^x = 2^{-x}$, 즉 $x = 0$에서만 성립한다.

제 3 권

함수 · 삼각법 · 초등기하

제3권은 함수의 언어를 정하고 이를 좌표, 삼각함수, 초등기하, 이차곡선에 적용하는 권이다. 제1장은 함수와 그래프, 단사·전사와 역함수, 합성, 대칭성과 그래프의 변환을 정리하여 이후 모든 장의 공통 언어를 마련한다. 제2장은 좌표와 벡터, 직선과 거리를 다루고, 제3장은 도와 라디안, 단위원으로 정의한 삼각함수와 덧셈정리를 세운다. 제4장은 삼각형의 합동과 닮음, 사인법칙과 코사인법칙, 헤론 공식, 원의 기하를 증명하고, 제5장은 초점과 준선으로 정의한 이차곡선과 극좌표로 권을 마친다.

제 1 장

함수와 그래프의 언어

개요 **함수**(*function*) $f : A \to B$는 집합 A의 각 원소에 집합 B의 원소를 정확히 하나씩 대응시키는 규칙이다. 이 장은 함수의 정의에서 출발하여 그래프, 단사·전사·역함수, 합성, 증가·감소와 대칭성(짝함수·홀함수), 평행이동과 확대·반사까지 함수를 다루는 데 필요한 기본 언어를 정리한다. 정의가 허용하는 것과 금지하는 것을 분명히 구분하는 것이 이 장의 목표이며, 이 언어는 이후 삼각함수(제3권 제3장)와 이차곡선(제3권 제5장)을 다룰 때 그대로 쓰인다. 선행 지식: 집합의 원소, 실수의 구간, 문자식.

1.1 함수는 입력마다 출력을 하나 정한다

정의 1.1 (함수) 집합 A에서 집합 B로 가는 함수 $f : A \to B$는 각 $x \in A$에 정확히 하나의 원소 $f(x) \in B$를 대응시키는 규칙이다. A는 **정의역**(*domain*), B는 **공역**(*codomain*)이며, 실제 출력들의 집합

$$f(A) = \{ f(x) : x \in A \}$$

은 **치역**(*range*)이다.

하나의 입력에 두 출력을 동시에 대응시키는 관계는 이 정의의 함수가 아니다. 그러나 서로 다른 두 입력이 같은 출력을 갖는 것은 허용한다. 함수가 **단사**라는 조건은 이런 중복까지 금지하는 추가 조건이며, §1.3에서 정식으로 다룬다.

역사 (함수 개념의 일반화). "입력마다 출력을 하나 정하는 임의의 대응"이라는 현대적 함수 정의는 특정한 식으로 주어질 필요가 없다는 점에서 초기의 "공식으로 표시되는 양" 개념보다 훨씬 넓다. 19세기에 Peter Gustav Lejeune Dirichlet가 푸리에 급수를 연구하면서 이런 임의의 대응으로서의 함수 개념을 명확히 사용하였고, 이후 집합과 순서쌍의 언어로 다시 정식화되었다(제5권 제1장).

예제 1.2 $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$의 공역은 $\mathbb{R}$이고 치역은 $[0, \infty)$이다. 같은 규칙을 $g : [0, \infty) \to [0, \infty)$에 적용하면 정의역과 공역이 달라지므로 다른 함수이다. f는 단사가 아니지만 g는 단사이다.

예제 1.3 방정식 $x^2 + y^2 = 1$로 정해진 전체 원은 y를 x의 함수로 표현하지 못한다. $x = 0$일 때 $y = 1, -1$ 두 값이 나오기 때문이다. 위쪽 반원만 택하면 $y = \sqrt{1 - x^2}$, $-1 \le x \le 1$이라는 함수가 된다.

1.2 함수의 그래프와 좌표

함수 $f : A \to \mathbb{R}$, $A \subseteq \mathbb{R}$의 **그래프**(*graph*)는 평면의 점집합 $\{(x, f(x)) : x \in A\}$이다. 세로선 $x = a$가 그래프와 만나는 점이 최대 하나라는 사실은 함수의 출력 유일성을 나타낸다. 그 세로선이 아예 만나지 않는다면 a가 정의역 밖일 수 있다.

그래프와 가로축의 교점은 $f(x) = 0$의 해이고, 세로축의 교점은 0이 정의역에 있을 때 $(0, f(0))$이다. 그래프를 그릴 때는 정의역의 제외점, 경계의 포함 여부, 대칭, 부호, 증가·감소를 함께 표시한다. 몇 개의 점만 연결하면 그 사이에서 일어나는 급격한 변화나 불연속을 놓칠 수 있다.

> **예제 1.4** $f(x) = (x^2 - 1)/(x - 1)$의 그래프는 직선 $y = x + 1$에서 $(1, 2)$를 뺀 것이다. 약분한 식으로 직선을 그리더라도 빠진 점을 빈 원으로 표시해야 원래 정의역을 표현한다(그림 1.1).

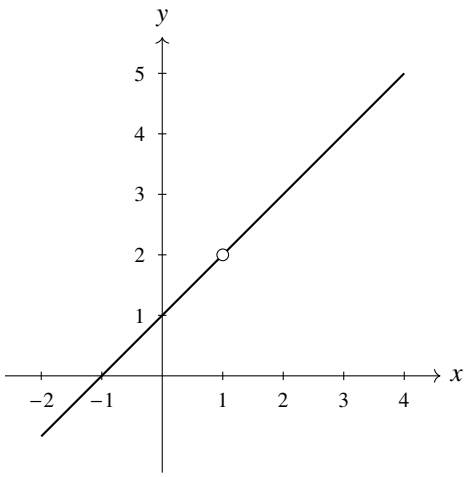

그림 1.1 $f(x) = (x^2 - 1)/(x - 1)$의 그래프. 약분한 직선 $y = x + 1$에서 제외점 $(1, 2)$만 비어 있다.

1.3 일대일, 위로, 역함수

> **정의 1.5 (단사, 전사, 전단사)** $f : A \to B$가 **단사**(*injective*)라는 것은 $f(x) = f(y)$이면 $x = y$라는 뜻이다. **전사**(*surjective*)라는 것은 모든 $b \in B$에 대해 $f(a) = b$인 $a \in A$가 존재한다는 뜻이다. 둘 다 만족하면 **전단사**(*bijective*)라 한다.

> **정리 1.6 (역함수의 존재)** $f : A \to B$가 양쪽 **역함수**(*inverse function*) $f^{-1} : B \to A$를 가질 필요충분조건은 전단사인 것이다.

증명. 역함수가 있으면 $f(x) = f(y)$에 역함수를 적용해 $x = y$를 얻고, 모든 $b \in B$는 $b = f(f^{-1}(b))$로 표현된다. 역으로 전사이면 각 b의 원상이 존재하고 단사이면 그것이 유일하다. 그 유일한 원상을 $f^{-1}(b)$로 정하면 두 합성이 항등함수이다. $\square$

> **예제 1.7** $f(x) = 2x - 3$을 $\mathbb{R} \to \mathbb{R}$로 보면 역함수는 $f^{-1}(y) = (y + 3)/2$이다. x^2를 $\mathbb{R} \to [0, \infty)$로 보면 전사이지만 단사가 아니므로 역함수가 없다. 정의역을 $[0, \infty)$로 제한하면 역함수 $\sqrt{y}$를 얻는다.

흔한 오류 (역함수 표기와 원상). $f^{-1}(x)$는 역함수 값이며 일반적으로 $1/f(x)$가 아니다. 집합 S의 **원상**(*preimage*) $f^{-1}(S)$라는 표기는 역함수가 존재하지 않아도 사용할 수 있는데, 이는 $\{x : f(x) \in S\}$를 뜻한다.

1.4 합성과 정의역

$f : A \to B$, $g : B \to C$이면 **합성함수**(*composition*) $g \circ f$는 $(g \circ f)(x) = g(f(x))$로 정의된다. 실제 식이 자연스러운 정의역으로만 주어졌다면 x가 f의 정의역에 있고 $f(x)$가 g의 정의역에 들어가는지 확인한다. 일반적으로 합성의 순서는 바꿀 수 없다.

> **예제 1.8** $f(x) = x + 1$, $g(x) = x^2$이면 $(g \circ f)(x) = (x+1)^2$이고 $(f \circ g)(x) = x^2 + 1$이다. $x = 1$에서 각각 $4, 2$이므로 서로 다른 함수이다.

> **예제 1.9** $f(x) = \sqrt{x}$, $g(x) = 1/(x-1)$이면 $g \circ f$의 정의역은 $x \geq 0$, $x \neq 1$이다. $f \circ g$의 정의역은 $1/(x-1) \geq 0$, $x \neq 1$로부터 $x > 1$이다. 두 합성은 식뿐 아니라 정의역도 다르다.

> **명제 1.10 (합성의 결합법칙)** 정의역과 공역이 맞는 함수들의 합성은 결합법칙을 만족한다: $h \circ (g \circ f) = (h \circ g) \circ f$.

증명. 각 입력 x에 대해 $((h \circ g) \circ f)(x) = h(g(f(x))) = (h \circ (g \circ f))(x)$이다. □

1.5 증가, 감소, 짝함수와 홀함수

함수가 구간에서 증가한다는 말은 여기서는 $x < y$일 때 $f(x) < f(y)$라는 엄격한 의미로 사용한다. $f(x) \leq f(y)$만 요구하면 비감소라 한다. 감소와 비증가도 같은 방식으로 구별한다. 엄격한 단조함수는 단사이지만, 임의의 집합에서 단사인 함수가 항상 단조인 것은 아니다.

정의역이 원점에 대해 대칭일 때 $f(-x) = f(x)$이면 **짝함수**(*even function*), $f(-x) = -f(x)$이면 **홀함수**(*odd function*)이다. 짝함수의 그래프는 세로축 대칭이고 홀함수의 그래프는 원점 대칭이다. $x^2, |x|$는 짝함수, x^3, x는 홀함수이다. 영함수는 둘 다 해당한다.

> **예제 1.11 (짝함수와 홀함수로의 분해)** 대칭 정의역의 임의 함수 f는
>
> $$f(x) = \frac{f(x) + f(-x)}{2} + \frac{f(x) - f(-x)}{2} \tag{1.1}$$
>
> 로 짝함수 부분과 홀함수 부분의 합으로 분해된다. 첫 항에 $-x$를 대입하면 같고 둘째 항에는 부호가 바뀐다.

1.6 평행이동과 확대·반사

$y = f(x - h) + k$의 그래프는 $y = f(x)$를 오른쪽으로 h, 위로 k만큼 옮긴 것이다. $x - h$의 부호가 이동 방향과 반대로 보이는 이유는 새 입력 x가 원래 입력 $x - h$에 대응하기 때문이다. $y = a f(x)$는 세로방향 배율 $|a|$와 $a < 0$일 때의 가로축 반사를, $y = f(bx)$는 $b \neq 0$에서 가로방향 배율 $1/|b|$와 $b < 0$일 때의 세로축 반사를 나타낸다.

예제 1.12 $y = -2(x-3)^2 + 1$은 $y = x^2$을 오른쪽으로 3, 위로 1 옮기고, 꼭짓점 기준 세로 크기를 두 배로 하여 아래로 열린 포물선이다. 꼭짓점은 $(3, 1)$이고 최댓값은 1이다. 변환의 순서를 달리 설명할 때는 어느 축이나 어느 점을 기준으로 확대하는지 명시해야 한다.

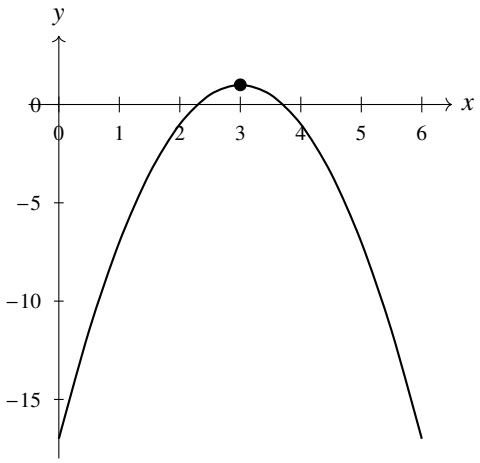

그림 1.2 $y = -2(x-3)^2 + 1$. 꼭짓점 $(3, 1)$이 변환의 기준점이다.

1.7 문제와 풀이

연습문제 1.13 $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^3$이 전단사임을 설명하고 역함수를 써라.

풀이. 세제곱은 엄격히 증가하므로 단사이며, 모든 실수 y에는 유일한 실수 세제곱근이 있으므로 전사이다. 역함수는 $f^{-1}(y) = \sqrt[3]{y}$이다.

연습문제 1.14 $f(x) = 1/x$에 대해 $f \circ f$를 구하고 정의역을 써라.

풀이. $x \neq 0$이면 $f(x) \neq 0$이고 $f(f(x)) = x$이다. 정의역은 $\mathbb{R} \setminus \{0\}$이며 실수 전체의 항등함수와는 정의역이 다르다.

연습문제 1.15 $f(x) = x^2 + 2x$의 짝함수 부분과 홀함수 부분을 구하여라.

풀이. $f(-x) = x^2 - 2x$이므로 각각 x^2와 $2x$이다.

연습문제 1.16 $f(x) = \sqrt{4 - x^2}$의 정의역과 치역을 구하여라.

풀이. $4 - x^2 \geq 0$이므로 정의역은 $[-2, 2]$이다. 출력은 0부터 2까지이며 각 값이 실제로 얻어지므로 치역은 $[0, 2]$이다.

연습문제 1.17 $f(x) = x^2$의 정의역을 $(-\infty, 0]$로 제한하고 공역을 $[0, \infty)$로 정할 때 역함수를 구하여라.

풀이. 이 범위에서 제곱은 엄격히 감소하며 전사이다. 원상은 비양수여야 하므로 $f^{-1}(y) = -\sqrt{y}$이다.

제 2 장

좌표, 직선, 거리

개요 평면에 **좌표계**(*coordinate system*)를 고정하면 점을 순서쌍으로, 변위를 벡터로 나타낼 수 있다. 이 장은 점과 벡터의 구분에서 출발하여 벡터의 내적과 수직성, 직선의 매개변수·법선 표현, 점과 직선 사이의 거리, 내분점과 무게중심, 그리고 좌표 변환이 거리를 보존하는 조건을 차례로 다룬다. 평면은 유클리드 평면이다. 선행 지식: 피타고라스 정리의 기본 형태, 일차방정식, 제곱근.

역사 (좌표기하의 시작). 점을 수의 순서쌍으로 나타내어 기하 문제를 대수적으로 다루는 방법은 17세기에 René Descartes가 *La Géométrie*(1637)에서 체계화하였다. 이 때문에 직교좌표를 데카르트 좌표라고도 부른다.

2.1 점과 벡터를 구분하기

좌표평면의 **점**은 위치를 나타내고, **벡터**(*vector*)는 변위를 나타낸다. 점 $P=(x_1,y_1)$에서 $Q=(x_2,y_2)$로 가는 변위는 $\overrightarrow{PQ}=(x_2-x_1,y_2-y_1)$이다. 원점을 정하면 점과 그 위치벡터를 같은 좌표쌍으로 표현할 수 있지만 역할은 구분하는 편이 좋다.

정의 2.1 (내적과 길이) 벡터 $\mathbf{u}=(u_1,u_2)$, $\mathbf{v}=(v_1,v_2)$에 대해 **내적**(*inner product*)과 길이를

$$\mathbf{u}\cdot\mathbf{v}=u_1v_1+u_2v_2, \qquad \|\mathbf{u}\|=\sqrt{u_1^2+u_2^2} \tag{2.1}$$

로 정의한다. 점 사이의 거리는 $d(P,Q)=\left\|\overrightarrow{PQ}\right\|$이다.

예제 2.2 $P=(-1,2)$, $Q=(3,-1)$이면 변위는 $(4,-3)$이고 거리는 5이다. 두 점의 중점은 $(1,1/2)$이다. 중점의 좌표는 두 위치벡터의 평균으로 얻는다.

2.2 내적과 수직성

0이 아닌 두 벡터 사이의 각을 $\theta\in[0,\pi]$라 하면

$$\mathbf{u}\cdot\mathbf{v}=\|\mathbf{u}\|\,\|\mathbf{v}\|\cos\theta.$$

이 식에서 코사인은 뒤 삼각함수 장의 단위원 정의를 따른다(제3권 제3장). $\mathbf{u}$ 방향을 첫 좌표축으로 잡으면 $\mathbf{u}=(\|\mathbf{u}\|,0)$이고 $\mathbf{v}$의 첫 좌표는 $\|\mathbf{v}\|\cos\theta$이다. 둘째 좌표는 어느 반평면에 놓이는지에 따라 $\pm\|\mathbf{v}\|\sin\theta$가 되지만, $\mathbf{u}$와의 내적에는 영향을 주지 않으므로 위 식을 얻는다. 직교 정규 좌표축 사이의 회전은 내적을 보존한다. 실제 회전행렬 R에 대해 $R^{\mathsf T}R=I$를 성분으로 확인하면 $(R\mathbf{u})\cdot(R\mathbf{v})=\mathbf{u}\cdot\mathbf{v}$이다. 이 유도는 코사인법칙을 전제하지 않는다. 특히 두 벡터가 **수직**일 필요충분조건은 내적이 0인 것이다. 영벡터에는 방향각을 정하지 않지만 모든 벡터와 내적은 0이다.

예제 2.3 $(2,3)$과 $(3,-2)$의 내적은 $6-6=0$이다. 따라서 이 두 방향을 갖는 직선들은 수직이다. 두 기울기의 곱이 -1이라는 규칙은 두 기울기가 모두 정의될 때의 특수한 표현이다. 수직선과 수평선에는 내적 방식이 더 보편적이다.

2.3 직선의 여러 표현

한 점 P_0와 0이 아닌 방향벡터 $\mathbf{v}$가 정해지면 직선은

$$P(t) = P_0 + t\mathbf{v}, \qquad t \in \mathbb{R} \tag{2.2}$$

로 표현된다. 법선벡터 $\mathbf{n} = (a,b) \neq (0,0)$를 사용하면 같은 직선을

$$ax + by + c = 0 \tag{2.3}$$

으로 쓸 수 있다. 방향벡터와 법선벡터는 수직이다.

예제 2.4 점 $(1,2)$를 지나고 방향 $(3,-1)$을 갖는 직선은 $(x,y) = (1+3t, 2-t)$이다. 법선 $(1,3)$을 사용하면 $(x-1)+3(y-2)=0$, 즉 $x+3y-7=0$이다.

$y = mx + b$는 수직선이 아닌 직선의 표현이다. m은 가로변화에 대한 세로변화의 비이고, b는 세로축 절편이다. 수직선은 $x = a$로 나타내며 유한한 기울기를 갖지 않는다.

2.4 점과 직선 사이의 거리

정리 2.5 점 $P = (x_0, y_0)$와 직선 $ax + by + c = 0$ 사이의 거리는

$$d = \frac{|ax_0 + by_0 + c|}{\sqrt{a^2 + b^2}}, \qquad (a,b) \neq (0,0) \tag{2.4}$$

이다.

증명. 직선 위의 점 Q를 하나 잡고 단위 법선 $\mathbf{n} = (a,b)/\sqrt{a^2+b^2}$를 택한다. 변위 $P - Q$의 법선 성분의 절댓값은 $|(P-Q)\cdot\mathbf{n}|$이다. 직선 위에서 이동하는 성분은 $\mathbf{n}$과 내적이 0이므로 이 값은 Q에 무관하고, 수선의 발에서 실제 최소거리로 달성된다. $aQ_x + bQ_y = -c$를 대입하면 공식이다. $\square$

예제 2.6 $(2,1)$과 $3x+4y-5=0$ 사이의 거리는 $|6+4-5|/5 = 1$이다. 수선의 발은

$$(2,1) - \frac{5}{25}(3,4) = (7/5, 1/5)$$

이며 실제로 $3(7/5)+4(1/5)-5=0$이다.

2.5 내분점과 무게중심

선분 AB 위의 점 P가 $AP : PB = m : n$을 만족하고 $m, n > 0$이면

$$P = \frac{nA + mB}{m+n}. \tag{2.5}$$

A에서 B 쪽으로 전체 길이의 $m/(m+n)$만큼 가므로 $A + [m/(m+n)](B-A)$를 정리한 것이다. A에 곱하는 계수는 맞은편 길이의 비 n이라는 점을 주의한다.

예제 2.7 $A=(0,0)$, $B=(6,3)$에서 $AP:PB=2:1$이면 $P=(4,2)$이다. A에서 전체 변위의 $2/3$만큼 움직였다.

삼각형의 세 중선은 **무게중심**(*centroid*) $G=(A+B+C)/3$에서 만난다. BC의 중점이 $M=(B+C)/2$이면 $G=A+(2/3)(M-A)$이므로 $AG:GM=2:1$이다. 다른 꼭짓점에서도 같은 식이 성립하므로 세 중선의 공통 교점임을 알 수 있다.

2.6 좌표 변환과 거리 보존

평행이동은 모든 점에 같은 벡터를 더하므로 점 사이의 변위와 거리를 보존한다. 회전과 반사도 내적을 보존한다. 하지만 가로와 세로를 서로 다른 비율로 늘이면 일반적으로 각도와 거리는 보존되지 않는다. 그림을 편하게 바꾸는 변환이 문제의 조건을 보존하는지 확인해야 한다.

예제 2.8 직각삼각형의 두 직각변을 각각 길이 a, b에서 모두 1로 바꾸는 비등방 확대는 직각을 이 특정 배치에서는 유지할 수 있지만, 일반적인 각도와 두 변의 길이비를 보존하지 않는다. 유사변환은 모든 방향에 같은 양의 배율을 사용하여 각도와 길이비를 보존한다.

2.7 문제와 풀이

연습문제 2.9 $(1,-2)$와 $(5,1)$을 지나는 직선의 방정식을 구하여라.

풀이. 방향벡터는 $(4,3)$이고 법선은 $(3,-4)$이다. 따라서 $3(x-1)-4(y+2)=0$, 즉 $3x-4y-11=0$이다.

연습문제 2.10 점 $(0,0)$에서 $2x-y+3=0$까지의 거리와 수선의 발을 구하여라.

풀이. 거리는 $3/\sqrt{5}$이다. 법선 방향으로 $-(3/5)(2,-1)$만큼 이동한 $(-6/5,3/5)$가 수선의 발이고 직선에 대입하면 0이다.

연습문제 2.11 $A=(0,0)$, $B=(6,0)$, $C=(0,3)$인 삼각형의 무게중심을 구하여라.

풀이. 세 좌표의 평균으로 $G=(2,1)$이다. 예를 들어 BC의 중점 $(3,3/2)$까지 가는 중선의 $2/3$ 지점이다.

연습문제 2.12 두 점 $A=(-1,0)$, $B=(1,0)$까지 거리가 같은 점들의 집합을 구하여라.

풀이. $(x+1)^2+y^2=(x-1)^2+y^2$에서 $4x=0$이다. 따라서 자취는 선분 AB의 수직이등분선인 $x=0$이다.

연습문제 2.13 $\mathbf{u}=(1,2)$, $\mathbf{v}=(2,4)$가 같은 방향임을 보이고, 수직일 수 없는 이유를 내적으로 설명하여라.

풀이. $\mathbf{v}=2\mathbf{u}$이고 배율이 양수이므로 같은 방향이다. 내적은 $10\neq 0$이다. 평행성과 수직성은 서로 다른 조건이다.

제 3 장

각도와 삼각함수

개요 삼각함수는 각 θ에 단위원 위의 점의 좌표 $(\cos\theta, \sin\theta)$와 그 비 $\tan\theta = \sin\theta/\cos\theta$를 대응시키는 주기함수이다. 이 장은 각의 두 단위인 도와 라디안을 정하고, 단위원으로 사인·코사인·탄젠트를 모든 실수 각에 대하여 정의한 다음, 피타고라스 항등식과 덧셈정리, 두 배 각 공식과 반각 공식을 유도한다. 이어서 주기성을 이용하여 삼각방정식의 해를 빠짐없이 적는 방법과, 정의역을 제한하여 얻는 역삼각함수의 주값을 다룬다. 선행 지식: 원, 직각삼각형, 함수, 실수의 사칙연산. 미적분을 사용할 때 각도는 라디안으로 나타낸다.

3.1 도와 라디안

도(*degree*)는 한 바퀴의 회전을 360등분한 각을 1°로 삼는 각의 단위이다. **라디안**(*radian*)은 반지름이 $r > 0$인 원에서 중심각이 잘라내는 호의 길이 s를 반지름으로 나눈 비

$$\theta = \frac{s}{r} \tag{3.1}$$

로 각을 재는 단위이다. 중심각이 같은 부채꼴은 서로 닮음이어서 호의 길이가 반지름에 비례하므로, 이 비는 원의 크기에 의존하지 않고 각만으로 정해진다. 원의 둘레가 $2\pi r$이므로 한 바퀴는 2π 라디안이다. 따라서 두 단위는

$$180^\circ = \pi \text{ 라디안}, \qquad \theta_{\text{rad}} = \frac{\pi}{180}\,\theta_{\text{deg}} \tag{3.2}$$

로 환산된다. 여기서 θ_{deg}와 θ_{rad}는 같은 각을 도와 라디안으로 잰 수치이다. 1 라디안은 $180^\circ/\pi \approx 57.2958^\circ$이고 1°는 약 0.0174533 라디안이다.

라디안은 길이끼리의 비여서 무차원이지만, 수치가 어느 각도 단위를 뜻하는지 표시하는 관례는 유용하다. $\sin 30$과 $\sin 30^\circ$는 서로 다른 입력이다. 앞의 것은 30 라디안의 사인으로 약 -0.988이고, 뒤의 것은 $1/2$이다. 도 기호가 없으면 라디안을 기본으로 한다.

각을 라디안으로 재면 식 (3.1)에서 호의 길이와 부채꼴의 넓이가 곧바로 나온다. 반지름 r, 중심각 θ $(0 \le \theta \le 2\pi)$인 부채꼴의 호의 길이 s와 넓이 A는

$$s = r\theta, \qquad A = \frac{1}{2}r^2\theta \tag{3.3}$$

이다. 넓이 공식은 전체 원의 넓이 πr^2에 각의 비 $\theta/(2\pi)$를 곱하여 얻는다. 두 식은 θ가 라디안일 때에만 이 모양이며, 도 단위에서는 $s = \pi r\theta_{\text{deg}}/180$처럼 환산 인자가 붙는다.

> **예제 3.1** $60^\circ = \pi/3$ 라디안이다. 반지름 6인 원에서 이 각이 만드는 호의 길이는 $s = 6\cdot(\pi/3) = 2\pi$이고 부채꼴 넓이는 $\frac{1}{2}r^2\theta = \frac{1}{2}\cdot 36\cdot\frac{\pi}{3} = 6\pi$이다. 같은 넓이는 원 전체의 넓이 36π의 $60/360 = 1/6$로도 얻는다.

참고 (미적분에서 라디안을 쓰는 이유). θ를 라디안으로 재면 $\theta \to 0$일 때 $\sin\theta/\theta \to 1$이고, 그 결과 사인의 도함수가 상수 인자 없이 코사인이 된다. 도 단위로 재면 같은 극한이 $\pi/180$이 되어

모든 미분 공식에 이 인자가 따라붙는다. 극한과 도함수의 계산은 제8권 제1장과 제8권 제2장에서 다룬다.

역사 (도와 라디안). 한 바퀴를 360으로 나누는 방식은 고대 바빌로니아의 육십진법 천문 계산에서 비롯하여 그리스 천문학을 거쳐 전해졌다. 호의 길이와 반지름의 비로 각을 재는 방법은 18세기에 이미 쓰였으나, 라디안이라는 이름은 1873년 James Thomson이 Belfast의 Queen's College 시험 문제에 쓴 것이 인쇄물에 나타난 첫 사례이다.

3.2 단위원에서 정의하기

단위원(*unit circle*) $x^2+y^2=1$ 위에서 양의 가로축 위의 점 $(1,0)$을 원점을 중심으로 반시계방향으로 각 θ만큼 회전한 점의 좌표를 $(\cos\theta, \sin\theta)$로 정의한다. 가로좌표를 주는 함수가 **코사인**(*cosine*), 세로좌표를 주는 함수가 **사인**(*sine*)이다. 음의 각은 시계방향 회전이다. 여러 바퀴를 허용하므로 두 함수는 모든 실수에서 정의되며, 한 바퀴를 더 돌면 같은 점으로 돌아오므로 **주기**(*period*) 2π를 갖는다.

$$\cos(\theta+2\pi)=\cos\theta, \qquad \sin(\theta+2\pi)=\sin\theta. \tag{3.4}$$

회전한 점이 다시 $(1,0)$이 되는 것은 θ가 2π의 정수배일 때뿐이므로, 2π보다 작은 양의 주기는 없다.

두 좌표의 부호는 점이 놓인 사분면으로 정해진다. 제1사분면에서는 사인과 코사인이 모두 양수이고, 제2사분면에서는 사인만, 제4사분면에서는 코사인만 양수이며, 제3사분면에서는 둘 다 음수이다.

명제 3.2 모든 실수 θ에 대하여

$$\cos^2\theta+\sin^2\theta=1, \qquad |\sin\theta|\le 1, \quad |\cos\theta|\le 1 \tag{3.5}$$

이다. 또한 $\cos(-\theta)=\cos\theta$, $\sin(-\theta)=-\sin\theta$이다.

증명. 첫 등식은 정의한 점 $(\cos\theta,\sin\theta)$가 단위원 $x^2+y^2=1$ 위에 있다는 사실 그대로이다. 두 제곱이 음이 아니고 합이 1이므로 각각 1 이하이고, 여기서 두 부등식이 따른다. 각의 부호를 바꾸면 회전 방향이 반대가 되어 점이 가로축에 대한 반사점으로 옮겨지므로, 가로좌표는 같고 세로좌표는 부호가 바뀐다. □

식 (3.5)의 첫 등식을 **피타고라스 항등식**이라고 한다. $\cos^2\theta$는 $(\cos\theta)^2$을 뜻하는 표기이며 $\cos(\theta^2)$과 다르다. 명제의 둘째 문장은 코사인이 짝함수, 사인이 홀함수임을 말한다.

참고 (단위원의 대칭에서 나오는 관계). 명제 3.2의 증명과 같은 방식으로 단위원의 다른 대칭도 항등식으로 옮길 수 있다. 반 바퀴 회전은 점 (x,y)를 $(-x,-y)$로 옮기고, 세로축에 대한 반사는 각 θ의 점을 각 $\pi-\theta$의 점 $(-x,y)$로 옮기며, 직선 $y=x$에 대한 반사는 각 θ의 점을 각 $\pi/2-\theta$의

점 (y, x)로 옮긴다. 따라서

$$\cos(\theta+\pi) = -\cos\theta, \qquad \sin(\theta+\pi) = -\sin\theta,$$
$$\cos(\pi-\theta) = -\cos\theta, \qquad \sin(\pi-\theta) = \sin\theta,$$
$$\cos\left(\frac{\pi}{2}-\theta\right) = \sin\theta, \qquad \sin\left(\frac{\pi}{2}-\theta\right) = \cos\theta$$

가 모든 실수 θ에 대하여 성립한다. 둘째 줄은 삼각방정식에서 사인값이 같은 두 번째 각을 찾을 때 쓰인다.

예제 3.3 한 변의 길이가 2인 정삼각형을 반으로 나눈 직각삼각형은 변의 길이가 1, $\sqrt{3}$, 2이므로 $\sin(\pi/6) = 1/2$, $\cos(\pi/6) = \sqrt{3}/2$이다. 직각을 낀 두 변의 길이가 1인 직각이등변삼각형은 빗변이 $\sqrt{2}$이므로 $\sin(\pi/4) = \cos(\pi/4) = 1/\sqrt{2}$이다. 이러한 특수각의 값은 삼각형의 변의 비로 설명할 수 있다. 표 3.1에 제1사분면의 값을 모았다.

표 3.1 특수각의 삼각함수 값

θ (라디안)	0	$\pi/6$	$\pi/4$	$\pi/3$	$\pi/2$
θ (도)	0°	30°	45°	60°	90°
$\sin\theta$	0	$1/2$	$\sqrt{2}/2$	$\sqrt{3}/2$	1
$\cos\theta$	1	$\sqrt{3}/2$	$\sqrt{2}/2$	$1/2$	0
$\tan\theta$	0	$\sqrt{3}/3$	1	$\sqrt{3}$	정의되지 않음

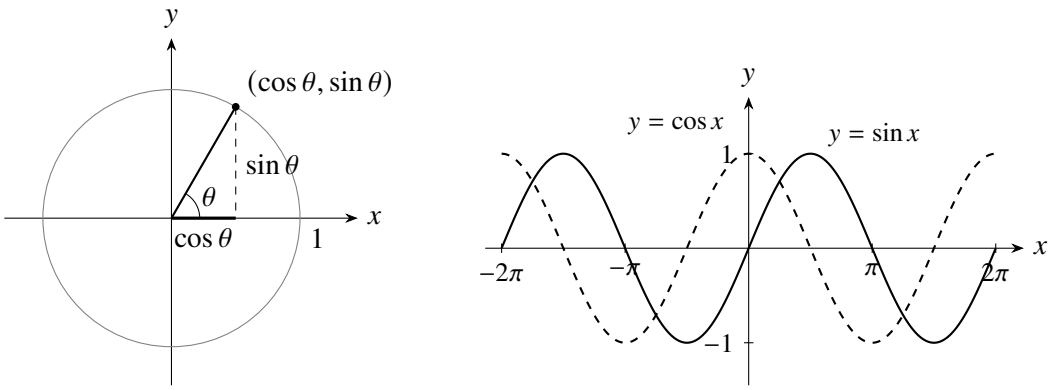

그림 3.1 단위원 위의 점의 두 좌표가 사인과 코사인을 정한다(왼쪽). 두 함수의 그래프는 주기가 2π로 같고 시작 위치만 다르다(오른쪽; 실선은 사인, 점선은 코사인이고 가로축은 라디안이다).

그림 3.1의 두 그래프는 모양이 같고 가로 방향으로 $\pi/2$만큼 어긋나 있다. 이는 위 참고의 셋째 줄과 코사인이 짝함수라는 사실에서 얻는 $\cos(x-\pi/2) = \sin x$를 그림으로 나타낸 것이다.

3.3 탄젠트와 정의되지 않는 각

정의 3.4 $\cos\theta \neq 0$일 때 **탄젠트**(*tangent*)를 $\tan\theta = \sin\theta/\cos\theta$로 정의한다. 따라서 정의역에서 $\theta = \pi/2 + k\pi$, $k \in \mathbb{Z}$를 제외한다.

제외되는 각은 단위원 위의 점이 세로축 위에 놓이는 각이다. $\tan\theta$는 원점과 점 $(\cos\theta, \sin\theta)$를 잇는 직선의 기울기이며, 세로축 방향의 직선에는 기울기가 없다는 사실과 맞아떨어진다.

탄젠트의 주기는 π이다. 반 바퀴를 더 돌면 $\sin(\theta+\pi) = -\sin\theta$, $\cos(\theta+\pi) = -\cos\theta$로 분자와 분모의 부호가 함께 바뀌어 비가 그대로이기 때문이다. 직각삼각형의 예각에서는 사인이 맞은편 변/빗변, 코사인이 이웃변/빗변, 탄젠트가 맞은편 변/이웃변이 된다. 빗변의 길이가 h인 직각삼각형을 $1/h$배로 줄여 빗변을 단위원의 반지름에 겹치면 두 정의가 일치함을 알 수 있다. 단위원 정의는 이 비율을 둔각, 음의 각, 여러 바퀴까지 확장한다.

$$1 + \tan^2\theta = \frac{1}{\cos^2\theta} \qquad (\cos\theta \neq 0). \tag{3.6}$$

이 식은 피타고라스 항등식 (3.5)을 $\cos^2\theta$로 나눈 결과이며, 나눗셈이 가능한 각에서만 성립하므로 분모가 0이 되는 각은 처음부터 포함하지 않는다.

표기 (나머지 세 삼각함수). 분모가 0이 아닌 각에서 **시컨트** $\sec\theta = 1/\cos\theta$, **코시컨트** $\csc\theta = 1/\sin\theta$, **코탄젠트** $\cot\theta = \cos\theta/\sin\theta$를 정의한다. 식 (3.6)은 $1+\tan^2\theta = \sec^2\theta$로 쓸 수 있고, 피타고라스 항등식을 $\sin^2\theta$로 나누면 $1+\cot^2\theta = \csc^2\theta$ $(\sin\theta \neq 0)$를 얻는다.

3.4 덧셈정리

정리 3.5 모든 실수 α, β에 대하여

$$\cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta, \tag{3.7}$$

$$\sin(\alpha+\beta) = \sin\alpha\cos\beta + \cos\alpha\sin\beta \tag{3.8}$$

이다.

증명. 원점을 중심으로 각 α만큼 회전하면 가로 단위벡터 $(1,0)$은 $(\cos\alpha, \sin\alpha)$로 옮겨진다. 세로 단위벡터 $(0,1)$은 $(1,0)$을 $\pi/2$만큼 회전한 것이므로, $(\cos\alpha, \sin\alpha)$를 $\pi/2$만큼 회전한 $(-\sin\alpha, \cos\alpha)$로 옮겨진다. 여기서 점 (x,y)를 $\pi/2$만큼 회전하면 $(-y,x)$가 된다는 사실을 썼다.

회전은 선형이다. 곧 벡터의 합과 실수배를 보존한다. 따라서 $(\cos\beta, \sin\beta) = \cos\beta\,(1,0) + \sin\beta\,(0,1)$의 회전상은 옮겨진 두 벡터에 각각 $\cos\beta$, $\sin\beta$를 곱한 합

$$\cos\beta\,(\cos\alpha, \sin\alpha) + \sin\beta\,(-\sin\alpha, \cos\alpha) = (\cos\alpha\cos\beta - \sin\alpha\sin\beta,\ \sin\alpha\cos\beta + \cos\alpha\sin\beta)$$

이다. 한편 각 β의 점을 α만큼 더 회전한 점은 각 $\alpha+\beta$에 해당하므로 그 좌표는 $(\cos(\alpha+\beta), \sin(\alpha+\beta))$이다. 두 좌표를 비교하면 공식이다. 이 증명은 유클리드 회전의 선형성과 각의 합성 성질을 사용한다. □

참고 (뺄셈 공식). 정리 3.5에서 β를 $-\beta$로 바꾸고 명제 3.2의 $\cos(-\beta)=\cos\beta$, $\sin(-\beta)=-\sin\beta$를 쓰면

$$\cos(\alpha-\beta)=\cos\alpha\cos\beta+\sin\alpha\sin\beta, \qquad \sin(\alpha-\beta)=\sin\alpha\cos\beta-\cos\alpha\sin\beta$$

를 얻는다. 첫 식에 $\beta=\alpha$를 넣으면 $1=\cos^2\alpha+\sin^2\alpha$로 피타고라스 항등식이 다시 나온다.

예제 3.6 $5\pi/12=\pi/4+\pi/6$이므로

$$\sin\frac{5\pi}{12}=\sin\frac{\pi}{4}\cos\frac{\pi}{6}+\cos\frac{\pi}{4}\sin\frac{\pi}{6}=\frac{\sqrt{2}}{2}\cdot\frac{\sqrt{3}}{2}+\frac{\sqrt{2}}{2}\cdot\frac{1}{2}=\frac{\sqrt{6}+\sqrt{2}}{4}\approx 0.966$$

이다. 두 사인을 더한 $\sin(\pi/4)+\sin(\pi/6)=(\sqrt{2}+1)/2\approx 1.207$과는 다르다. 뒤의 값은 1보다 크므로 어떤 각의 사인도 될 수 없다.

분모가 정의되는 경우 덧셈정리에서

$$\tan(\alpha+\beta)=\frac{\tan\alpha+\tan\beta}{1-\tan\alpha\tan\beta} \tag{3.9}$$

를 얻는다. 식 (3.8)를 식 (3.7)로 나눈 다음 분자와 분모를 $\cos\alpha\cos\beta$로 나누면 된다. 오른쪽을 사용할 때 $\cos\alpha$, $\cos\beta$가 0이 아니고 분모도 0이 아니어야 한다. $1-\tan\alpha\tan\beta=\cos(\alpha+\beta)/(\cos\alpha\cos\beta)$이므로 분모가 0이 아니라는 조건은 $\tan(\alpha+\beta)$가 정의된다는 조건과 같다. 사인·코사인 덧셈정리에는 이런 제외가 없다.

참고 (사인과 코사인의 합성). 둘 다 0은 아닌 실수 a, b에 대하여 $R=\sqrt{a^2+b^2}$으로 놓으면 점 $(a/R, b/R)$가 단위원 위에 있으므로 $\cos\varphi=a/R$, $\sin\varphi=b/R$인 각 φ가 있다. 식 (3.8)에 의하여

$$a\sin x+b\cos x=R(\sin x\cos\varphi+\cos x\sin\varphi)=R\sin(x+\varphi)$$

이다. 따라서 $a\sin x+b\cos x$의 값의 범위는 $[-R, R]$이고, 주기가 같은 사인과 코사인의 합은 진폭과 시작 위치만 바뀐 사인 하나로 쓸 수 있다.

역사 (덧셈정리의 기원). 2세기 Ptolemy의 『알마게스트』에는 원의 현의 길이를 각에 따라 적은 표가 실려 있다. 그 표는 두 호의 합과 차에 대한 현의 길이를 구하는 명제를 써서 만들어졌고, 이 명제들은 오늘날의 사인·코사인 덧셈정리와 내용이 같다.

3.5 두 배 각과 반각

덧셈정리에 $\beta=\alpha$를 넣고 각을 θ로 쓰면 **두 배 각 공식**

$$\sin 2\theta=2\sin\theta\cos\theta, \tag{3.10}$$

$$\cos 2\theta=\cos^2\theta-\sin^2\theta=1-2\sin^2\theta=2\cos^2\theta-1 \tag{3.11}$$

을 얻는다. 식 (3.11)의 뒤 두 표현은 피타고라스 항등식으로 $\cos^2\theta$ 또는 $\sin^2\theta$를 소거한 것이다. 같은 방법으로 식 (3.9)에서 $\tan 2\theta=2\tan\theta/(1-\tan^2\theta)$를 얻으며, 이 식은 $\tan\theta$와 $\tan 2\theta$가 모두 정의될 때 성립한다.

식 (3.11)에서 θ를 $\theta/2$로 바꾸어 정리하면 **반각 공식**

$$\sin^2\frac{\theta}{2}=\frac{1-\cos\theta}{2},\qquad \cos^2\frac{\theta}{2}=\frac{1+\cos\theta}{2} \tag{3.12}$$

이 나온다. 제곱을 제거할 때에는 반각 $\theta/2$가 어느 사분면에 있는지에 따라 부호를 선택한다.

> **예제 3.7** $\pi/12$는 제1사분면의 각이어서 $\sin(\pi/12)>0$이므로 반각 공식을 이용하면
>
> $$\sin\frac{\pi}{12}=\sqrt{\frac{1-\cos(\pi/6)}{2}}=\sqrt{\frac{2-\sqrt{3}}{4}}=\frac{\sqrt{6}-\sqrt{2}}{4}$$
>
> 이다. 마지막 등호는 $(\sqrt{6}-\sqrt{2})^2=8-4\sqrt{3}=4(2-\sqrt{3})$에서 $\sqrt{2-\sqrt{3}}=(\sqrt{6}-\sqrt{2})/2$이기 때문이다. 뺄셈 공식으로 계산한 $\sin(\pi/4-\pi/6)=\frac{\sqrt{2}}{2}\cdot\frac{\sqrt{3}}{2}-\frac{\sqrt{2}}{2}\cdot\frac{1}{2}$도 같은 값을 준다.

흔한 오류. 음의 각에 같은 양의 제곱근을 무조건 적용하면 부호가 틀릴 수 있다. 식 (3.12)에서 제곱근을 취하여 얻는 것은 $|\sin(\theta/2)|=\sqrt{(1-\cos\theta)/2}$이다. 예를 들어 $\theta=-\pi/6$이면 $\cos\theta$는 $\theta=\pi/6$일 때와 같지만 $\sin(-\pi/12)=-(\sqrt{6}-\sqrt{2})/4$로 음수이다.

핵심 수식

$$\cos^2\theta+\sin^2\theta=1,\qquad 1+\tan^2\theta=\frac{1}{\cos^2\theta},$$

$$\cos(\alpha\pm\beta)=\cos\alpha\cos\beta\mp\sin\alpha\sin\beta,\qquad \sin(\alpha\pm\beta)=\sin\alpha\cos\beta\pm\cos\alpha\sin\beta,$$

$$\sin 2\theta=2\sin\theta\cos\theta,\qquad \cos 2\theta=1-2\sin^2\theta=2\cos^2\theta-1.$$

3.6 삼각방정식의 모든 해

주기함수의 방정식은 한 주기 안의 해를 찾은 뒤 주기를 더하여 전체 해를 나타낸다. 역삼각함수 하나를 계산하는 것과 모든 각을 찾는 것은 다르다. 역삼각함수는 해 가운데 하나만 주며, 나머지는 단위원의 대칭과 주기에서 나온다.

방법 (기본 방정식의 일반해). 단위원에서 세로좌표가 같은 점은 세로축에 대하여 대칭인 두 점이고, 가로좌표가 같은 점은 가로축에 대하여 대칭인 두 점이다. 따라서 실수 α에 대하여 다음이 성립한다. 여기서 k는 임의의 정수이다.

$$\sin x=\sin\alpha \iff x=\alpha+2k\pi \ \text{또는}\ x=\pi-\alpha+2k\pi,$$

$$\cos x=\cos\alpha \iff x=\alpha+2k\pi \ \text{또는}\ x=-\alpha+2k\pi,$$

$$\tan x=\tan\alpha \iff x=\alpha+k\pi \qquad (\cos\alpha\neq 0).$$

> **예제 3.8** $\sin x=1/2$의 모든 실수해는
>
> $$x=\frac{\pi}{6}+2k\pi \quad\text{또는}\quad x=\frac{5\pi}{6}+2k\pi,\qquad k\in\mathbb{Z}$$
>
> 이다. 사인이 양수인 두 사분면, 곧 제1사분면과 제2사분면의 각을 모두 포함해야 한다. $\cos x=0$의 모든 해는 $x=\pi/2+k\pi$이다. 한 주기 안의 두 해 $\pi/2$와 $3\pi/2$가 π 간격이어서 한 식으로 묶인다.

예제 3.9 $\sin 2x = \sin x$에서 두 배 각 공식을 쓰면 $\sin x\,(2\cos x - 1) = 0$이다. 따라서 $\sin x = 0$ 또는 $\cos x = 1/2$이고, 해는 $x = k\pi$ 또는 $x = \pm\pi/3 + 2k\pi$ $(k \in \mathbb{Z})$이다. 양변을 $\sin x$로 먼저 나누면 첫 해족을 잃는다.

검산. 예제 3.9는 일반해 공식으로도 풀 수 있다. $\sin 2x = \sin x$는 $2x = x + 2k\pi$ 또는 $2x = \pi - x + 2k\pi$, 곧 $x = 2k\pi$ 또는 $x = \pi/3 + 2k\pi/3$와 같다. 둘째 해족은 2π를 주기로 $\pi/3$, π, $5\pi/3$를 되풀이하므로, 두 해족을 합하면 위에서 구한 $x = k\pi$, $x = \pm\pi/3 + 2k\pi$와 같은 집합이다.

3.7 역삼각함수의 주값

사인 함수는 실수 전체에서 단사가 아니므로 역함수를 만들려면 정의역을 제한한다. 관례적으로

$$\arcsin : [-1,1] \to \left[-\frac{\pi}{2}, \frac{\pi}{2}\right], \qquad \arccos : [-1,1] \to [0,\pi], \qquad \arctan : \mathbb{R} \to \left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \tag{3.13}$$

를 사용한다. 이 구간들이 **주값**(*principal value*)의 범위이다. 사인은 $[-\pi/2, \pi/2]$에서 증가하면서 $[-1,1]$의 모든 값을 한 번씩 취하고, 코사인은 $[0,\pi]$에서 감소하면서 $[-1,1]$의 모든 값을 한 번씩 취하며, 탄젠트는 $(-\pi/2, \pi/2)$에서 증가하면서 모든 실수 값을 한 번씩 취한다. 세 **역삼각함수**는 각 함수를 이 구간으로 제한한 것의 역함수이다(함수의 제한과 역함수는 제3권 제1장).

예제 3.10 $\arcsin(\sin(5\pi/6)) = \arcsin(1/2) = \pi/6$이다. 따라서 $\arcsin(\sin x) = x$는 모든 실수에서 성립하지 않고 $x \in [-\pi/2, \pi/2]$에서 성립한다.

참고 (역삼각함수의 기본 관계). 반대 순서의 합성 $\sin(\arcsin y) = y$는 모든 $y \in [-1,1]$에서 성립한다. 또 $\theta = \arcsin y$이면 $\pi/2 - \theta \in [0,\pi]$이고 $\cos(\pi/2 - \theta) = \sin\theta = y$이므로

$$\arcsin y + \arccos y = \frac{\pi}{2} \qquad (-1 \le y \le 1)$$

이다. $|c| \le 1$일 때 $\sin x = c$의 모든 해는 $x = \arcsin c + 2k\pi$ 또는 $x = \pi - \arcsin c + 2k\pi$ $(k \in \mathbb{Z})$이다.

주의 (표기 $\sin^{-1}$). $\arcsin y$를 $\sin^{-1} y$로 쓰기도 한다. 이때 -1은 역함수를 뜻하며 역수 $1/\sin y$가 아니다. 반면 $\sin^2 y$는 $(\sin y)^2$을 뜻하므로 두 표기의 지수는 뜻이 다르다.

3.8 문제와 풀이

연습문제 3.11 반지름 4인 원에서 135°에 해당하는 호의 길이와 부채꼴 넓이를 구하여라.

풀이. 각은 $135 \cdot \pi/180 = 3\pi/4$ 라디안이다. 호의 길이는 $4 \cdot (3\pi/4) = 3\pi$, 넓이는 $\frac{1}{2} \cdot 16 \cdot \frac{3\pi}{4} = 6\pi$이다.

연습문제 3.12 $\cos x = -1/2$의 모든 실수해를 구하여라.

풀이. $x = 2\pi/3 + 2k\pi$ 또는 $x = 4\pi/3 + 2k\pi$, $k \in \mathbb{Z}$이다. 코사인이 음수인 제2사분면과 제3사분면의 각이며, 둘째 해족은 $x = -2\pi/3 + 2k\pi$로 써도 같다.

연습문제 3.13 $\tan x = 1$의 모든 해를 쓰고 사인 방정식과 주기를 비교하여라.

풀이. $x = \pi/4 + k\pi$, $k \in \mathbb{Z}$이다. 탄젠트는 반 바퀴 회전하면 분자와 분모의 부호가 함께 바뀌어 같은 값을 갖는다. 따라서 주기가 π이고 해족이 하나이다. 사인 방정식은 주기가 2π이고 한 주기 안에 해가 일반적으로 두 개이므로 해족이 둘이다.

연습문제 3.14 $\sin x + \cos x$의 범위와 최댓값을 달성하는 각을 구하여라.

풀이. 덧셈정리로 $\sqrt{2}\sin(x+\pi/4) = \sqrt{2}\left(\sin x\cos\frac{\pi}{4} + \cos x\sin\frac{\pi}{4}\right) = \sin x + \cos x$이다. 범위는 $[-\sqrt{2}, \sqrt{2}]$이고 최댓값 $\sqrt{2}$는 $x+\pi/4 = \pi/2 + 2k\pi$, 곧 $x = \pi/4 + 2k\pi$ $(k \in \mathbb{Z})$에서 달성된다. 최솟값 $-\sqrt{2}$는 $x = 5\pi/4 + 2k\pi$에서 달성된다.

연습문제 3.15 $\arccos(\cos(5\pi/3))$을 구하여라.

풀이. $\cos(5\pi/3) = \cos(2\pi - \pi/3) = \cos(\pi/3) = 1/2$이고, $[0, \pi]$에서 이 값을 갖는 각은 $\pi/3$이다. 따라서 답은 $\pi/3$이며 $5\pi/3$이 아니다.

연습문제 3.16 모든 실수 θ에 대하여 $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$임을 보이고, 이를 이용하여 $x = \cos(\pi/9)$가 방정식 $8x^3 - 6x - 1 = 0$의 해임을 보여라.

풀이. $3\theta = 2\theta + \theta$에 덧셈정리와 두 배 각 공식을 쓰면

$$\cos 3\theta = \cos 2\theta\cos\theta - \sin 2\theta\sin\theta = (2\cos^2\theta - 1)\cos\theta - 2\sin^2\theta\cos\theta$$
$$= (2\cos^2\theta - 1)\cos\theta - 2(1-\cos^2\theta)\cos\theta = 4\cos^3\theta - 3\cos\theta$$

이다. $\theta = \pi/9$를 넣으면 왼쪽은 $\cos(\pi/3) = 1/2$이므로 $4x^3 - 3x = 1/2$, 곧 $8x^3 - 6x - 1 = 0$이다.

참고 (다음 연결). 이 장의 공식은 제3권 제4장에서 코사인법칙과 사인법칙으로 삼각형의 변과 각을 계산하는 데 쓰이고, 제3권 제5장에서 극좌표 $x = r\cos\theta$, $y = r\sin\theta$의 바탕이 된다. 복소지수함수와의 관계 $e^{i\theta} = \cos\theta + i\sin\theta$는 제11권 제2장에서 다룬다.

제 4 장

삼각형과 원의 기하

개요 삼각형과 원의 기하는 유클리드 평면에서 삼각형의 변·각·넓이와 원의 접선·현·호 사이의 관계를 다루는 초등기하의 중심 부분이다. 이 장은 내각의 합과 삼각부등식, 합동과 닮음의 판정을 정리하고, 코사인법칙과 사인법칙, 넓이 공식과 헤론 공식을 증명한다. 이어서 원의 방정식과 접선의 방정식, 원주각의 성질과 원에 내접한 사각형, 점의 멱을 다룬다. 선행 지식: 유클리드 평면의 평행선과 각, 피타고라스 정리, 삼각함수(제3권 제3장). 쌍곡기하와 구면기하에는 같은 공식이 그대로 적용되지 않는다.

표기. 이 장에서 삼각형 ABC의 꼭짓점 A, B, C에서의 내각의 크기를 같은 글자 A, B, C로 쓰고, 그 맞은편 변 BC, CA, AB의 길이를 각각 a, b, c로 쓴다. 삼각형의 넓이는 K로 쓴다.

4.1 삼각형의 기본 제약

삼각형의 내각의 합은 π 라디안이다. 한 꼭짓점을 지나 맞은편 변에 평행한 직선을 그으면 다른 두 내각이 엇각으로 옮겨지고 세 각이 평각을 이룬다. 이 증명은 평행선에서 엇각이 같다는 유클리드 평행선 성질을 사용한다. 이 성질이 성립하지 않는 구면에서는 삼각형의 내각의 합이 π보다 크고, 쌍곡평면에서는 π보다 작다.

양의 세 수 a, b, c가 퇴화하지 않은 삼각형의 변이 될 필요충분조건은

$$a + b > c, \qquad b + c > a, \qquad c + a > b \tag{4.1}$$

이다. 이 조건을 **삼각부등식**(*triangle inequality*)이라고 한다. 등호가 성립하면 세 점이 한 직선에 놓이는 퇴화 경우이다. 가장 긴 변만 알면 그 변이 나머지 두 변의 합보다 작은지 확인하면 충분하다. 예를 들어 c가 가장 길면 $a \le c < b + c$, $b \le c < c + a$이므로 나머지 두 부등식은 저절로 성립한다.

참고 (삼각부등식이 필요충분조건인 이유). 필요성은 두 점을 잇는 가장 짧은 길이 선분이라는 사실에서 나온다. 충분성은 코사인법칙(정리 4.3)으로 확인할 수 있다. 식 (4.1)은 $|a - b| < c < a + b$와 같고, 각 변을 제곱하여 정리하면

$$-1 < \frac{a^2 + b^2 - c^2}{2ab} < 1$$

이 된다. 따라서 이 값을 코사인으로 갖는 각 $C \in (0, \pi)$가 하나 있고, 길이 a, b인 두 변이 각 C를 끼도록 삼각형을 그리면 셋째 변의 길이는 코사인법칙에 의하여 c이다.

> **예제 4.1** $2, 3, 6$은 $2 + 3 < 6$ 때문에 삼각형을 만들지 못한다. $2, 3, 5$는 $2 + 3 = 5$이므로 퇴화하고, $2, 3, 4$는 $2 + 3 > 4$이므로 삼각형을 이룬다. 변 길이 조건을 확인하지 않고 넓이 공식을 대입하면 음수의 제곱근 같은 모순이 나타날 수 있다. 실제로 $2, 3, 6$을 헤론 공식(정리 4.7)에 넣으면 $s = 11/2$이고 근호 안의 값이 $\frac{11}{2} \cdot \frac{7}{2} \cdot \frac{5}{2} \cdot \left(-\frac{1}{2}\right) = -\frac{385}{16}$으로 음수이다.

4.2 합동과 닮음

두 도형이 **합동**(*congruent*)이라는 것은 거리와 각을 보존하는 평면의 **등거리변환**(*isometry*), 곧 평행이동·회전·반사와 그 합성으로 한 도형을 다른 도형에 겹칠 수 있다는 뜻이다. 삼각형의 대표적 합동 판정은 다음 세 가지이다.

- 세 변이 각각 같다(SSS).
- 두 변과 그 끼인각이 각각 같다(SAS).
- 대응하는 두 각과 한 변이 각각 같다(ASA, AAS).

두 변과 끼이지 않은 각(SSA)은 일반적으로 합동을 결정하지 않는다. 주어진 각이 직각인 경우, 곧 직각삼각형의 빗변과 다른 한 변이 각각 같은 경우에는 피타고라스 정리로 셋째 변이 정해지므로 합동이 결정된다. SSA에서 생기는 두 가지 가능성은 사인법칙을 다루는 절에서 계산으로 확인한다.

두 도형이 **닮음**(*similar*)이라는 것은 공통 배율의 확대·축소와 등거리변환으로 한 도형을 다른 도형으로 옮길 수 있다는 뜻이다. 닮은 도형에서는 대응각이 같고 대응변의 비가 일정하다. 길이 배율이 $k>0$이면 넓이 배율은 k^2이고 입체의 부피 배율은 k^3이다. 삼각형에서는 두 각이 각각 같으면 내각의 합이 π이므로 나머지 각도 같아져 닮음을 얻는다(AA). 세 변의 비가 같은 경우와, 두 변의 비가 같고 그 끼인각이 같은 경우에도 두 삼각형은 닮음이다.

> **예제 4.2** 닮은 두 삼각형의 변 길이 비가 $2:3$이면 넓이 비는 $2^2:3^2=4:9$이다. 넓이 비를 길이 비와 같다고 놓으면 단위의 차원을 놓친다. 넓이는 길이의 제곱의 차원을 가지므로 배율도 제곱으로 바뀐다.

4.3 코사인법칙

> **정리 4.3** 삼각형에서 각 C에 마주 보는 변을 c, 나머지 두 변을 a, b라 하면
>
> $$c^2 = a^2 + b^2 - 2ab\cos C \tag{4.2}$$
>
> 이다.

증명. 꼭짓점 C를 원점에 놓고 두 이웃 꼭짓점 B, A의 위치벡터를 $\mathbf{u}, \mathbf{v}$라 하자. $\|\mathbf{u}\| = a$, $\|\mathbf{v}\| = b$이고 두 벡터가 이루는 각이 C이므로 $\mathbf{u}\cdot\mathbf{v} = ab\cos C$이다. 따라서

$$c^2 = \|\mathbf{u}-\mathbf{v}\|^2 = \|\mathbf{u}\|^2 + \|\mathbf{v}\|^2 - 2\,\mathbf{u}\cdot\mathbf{v} = a^2 + b^2 - 2ab\cos C$$

이다. 좌표로 쓰면 $B=(a,0)$, $A=(b\cos C, b\sin C)$로 놓을 수 있고, $c^2 = (b\cos C - a)^2 + (b\sin C)^2 = a^2 + b^2(\cos^2 C + \sin^2 C) - 2ab\cos C$로 같은 식을 얻는다. $\square$

$C=\pi/2$이면 코사인이 0이므로 피타고라스 정리를 얻는다. 코사인법칙은 예각·직각·둔각을 같은 식으로 다룬다. 식 (4.2)을 코사인에 대하여 풀면

$$\cos C = \frac{a^2 + b^2 - c^2}{2ab} \tag{4.3}$$

이므로 세 변에서 세 각을 구할 수 있다. 코사인은 $(0,\pi)$에서 단사이므로 각은 유일하게 정해지며, $c^2 < a^2+b^2$이면 C는 예각, $c^2 = a^2+b^2$이면 직각, $c^2 > a^2+b^2$이면 둔각이다.

> **예제 4.4** 두 변이 $5, 7$이고 끼인각이 60°이면 맞은편 변의 제곱은 $25+49-2\cdot 5\cdot 7\cdot \frac{1}{2} = 39$이므로 길이는 $\sqrt{39}\approx 6.245$이다.

4.4 넓이와 사인법칙

변 a, b와 끼인각 C에 대하여 넓이 K는

$$K = \frac{1}{2}ab\sin C \tag{4.4}$$

이다. 변 a를 밑변으로 놓으면 높이가 다른 변의 길이 b에 $\sin C$를 곱한 값이기 때문이다. C가 둔각이면 높이의 발이 밑변의 연장선 위에 놓이고 높이는 $b\sin(\pi-C)$인데, $\sin(\pi-C)=\sin C$이므로 높이의 길이를 동일한 사인으로 표현할 수 있다.

> **정리 4.5** 변 a, b, c의 맞은편 각을 A, B, C라 하면
>
> $$\frac{a}{\sin A} = \frac{b}{\sin B} = \frac{c}{\sin C} \tag{4.5}$$
>
> 이다.

증명. 같은 넓이를 식 (4.4)의 세 가지 방식으로 나타내면 $2K = bc\sin A = ca\sin B = ab\sin C$이다. 이를 양수 abc로 나누면 $\sin A/a = \sin B/b = \sin C/c$이다. 삼각형이 퇴화하지 않으므로 세 각은 $(0,\pi)$에 있고 세 사인은 양수이다. 따라서 역수를 취할 수 있다. □

> **예제 4.6** $A = 30^\circ$, $B = 45^\circ$, $a = 2$이면 $b = 2\sin 45^\circ/\sin 30^\circ = 2\sqrt{2}$이고 $C = 180^\circ - 30^\circ - 45^\circ = 105^\circ$이다. 이미 두 각을 알 때는 남은 각이 유일하다. 남은 변은 $c = 2\sin 105^\circ/\sin 30^\circ = 4\cdot\frac{\sqrt{6}+\sqrt{2}}{4} = \sqrt{6}+\sqrt{2}\approx 3.864$이다.

SSA 정보에서는 $\sin B$만 결정될 수 있어 B와 $\pi-B$의 두 후보가 남는다. 두 후보가 모두 삼각형의 내각의 합과 변 조건을 만족하면 서로 다른 두 삼각형이 생긴다. 역삼각함수의 주값만 반환하는 계산기를 그대로 쓰면 이 모호성을 놓칠 수 있다.

참고 (SSA에서 삼각형의 개수). 예각 A와 변 a, b가 주어지면 사인법칙에서 $\sin B = b\sin A/a$이다. $a < b\sin A$이면 이 값이 1보다 커서 삼각형이 없고, $a = b\sin A$이면 B가 직각인 삼각형 하나가 있다. $b\sin A < a < b$이면 예각 B와 둔각 $\pi-B$가 모두 가능하여 삼각형이 둘이고, $a \ge b$이면 $B \le A$이어야 하므로 삼각형이 하나이다. 예를 들어 $A = 30^\circ$, $a = 5$, $b = 8$이면 $\sin B = 0.8$이고 $B \approx 53.13^\circ$ 또는 $B \approx 126.87^\circ$이다. 각 경우 $C \approx 96.87^\circ$, $c \approx 9.928$ 또는 $C \approx 23.13^\circ$, $c \approx 3.928$이다. 같은 두 값은 코사인법칙 $a^2 = b^2+c^2-2bc\cos A$를 c의 이차방정식 $c^2 - 8\sqrt{3}\,c + 39 = 0$으로 풀어 $c = 4\sqrt{3}\pm 3$으로도 얻는다.

4.5 헤론 공식과 그 조건

정리 4.7 세 변이 a, b, c인 삼각형의 반둘레를 $s = (a+b+c)/2$라 하면 넓이는

$$K = \sqrt{s(s-a)(s-b)(s-c)} \tag{4.6}$$

이다.

증명. $K = \tfrac{1}{2}ab\sin C$에서 $16K^2 = 4a^2b^2\sin^2 C = 4a^2b^2 - (2ab\cos C)^2$이다. 코사인법칙으로 $2ab\cos C = a^2+b^2-c^2$을 대입하고 제곱의 차를 두 번 인수분해하면

$$\begin{aligned} 16K^2 &= 4a^2b^2 - (a^2+b^2-c^2)^2 \\ &= \bigl(2ab + a^2 + b^2 - c^2\bigr)\bigl(2ab - a^2 - b^2 + c^2\bigr) \\ &= \bigl((a+b)^2 - c^2\bigr)\bigl(c^2 - (a-b)^2\bigr) \\ &= (a+b+c)(a+b-c)(c+a-b)(c-a+b) \\ &= 16\,s(s-a)(s-b)(s-c) \end{aligned}$$

이다. 마지막 줄에서 $a+b+c = 2s$, $a+b-c = 2(s-c)$, $c+a-b = 2(s-b)$, $c-a+b = 2(s-a)$를 썼다. 넓이는 양수이므로 양의 제곱근을 택한다. □

참고 (근호 안이 양수일 조건). 양수 a, b, c에 대하여 $s > 0$이고, 세 인수 $s-a$, $s-b$, $s-c$ 가운데 어느 둘의 합도 양수이다. 예를 들어 $(s-a)+(s-b) = c > 0$이다. 따라서 세 인수 가운데 0 이하인 것은 많아야 하나이고, 근호 안의 값이 양수인 것은 세 인수가 모두 양수인 것과 같다. 이것은 삼각부등식 (4.1)과 같은 조건이다. 헤론 공식은 삼각형을 이루는 세 변에 대해서만 뜻이 있으며, 근호 안이 0이면 퇴화한 경우, 음수이면 삼각형이 없는 경우이다.

예제 4.8 변이 $13, 14, 15$이면 $s = 21$이고 $K = \sqrt{21\cdot 8\cdot 7\cdot 6} = \sqrt{7056} = 84$이다. 밑변 14에 대한 높이는 $2K/14 = 12$이다. 이 높이는 삼각형을 변의 길이가 $5, 12, 13$과 $9, 12, 15$인 두 직각삼각형으로 나누며, 밑변의 두 조각의 합이 $5+9 = 14$로 맞는다.

역사 (헤론 공식). 이 공식은 1세기 Alexandria의 Heron이 쓴 『측량술』(*Metrica*)에 증명과 함께 실려 있다. 코사인법칙에 해당하는 명제는 그보다 앞서 Euclid의 『원론』 제2권에 둔각삼각형과 예각삼각형의 경우로 나뉘어 넓이의 말로 서술되어 있다.

4.6 원의 방정식과 접선

중심 (a, b), 반지름 $r > 0$인 원은 중심에서 거리가 r인 점 (x, y)의 집합이므로 그 방정식은

$$(x-a)^2 + (y-b)^2 = r^2 \tag{4.7}$$

이다. 원 위 점 (x_0, y_0)에서의 **접선**은 그 점을 지나고 반지름 벡터 $(x_0-a,\ y_0-b)$에 수직인 직선이므로

$$(x_0-a)(x-a) + (y_0-b)(y-b) = r^2 \tag{4.8}$$

으로 쓸 수 있다. 미분을 사용하지 않아도 직선의 법선 표현으로 얻을 수 있다.

유도 (접선의 방정식). 점 (x_0, y_0)을 지나고 벡터 $(x_0 - a,\ y_0 - b)$에 수직인 직선은 $(x_0 - a)(x - x_0) + (y_0 - b)(y - y_0) = 0$이다. 여기에 $x - x_0 = (x - a) - (x_0 - a)$, $y - y_0 = (y - b) - (y_0 - b)$를 넣으면

$$(x_0 - a)(x - a) + (y_0 - b)(y - b) = (x_0 - a)^2 + (y_0 - b)^2 = r^2$$

이 되어 식 (4.8)을 얻는다. 마지막 등호는 (x_0, y_0)이 원 위의 점이라는 조건이다. 이 직선이 원과 한 점에서만 만난다는 것은 피타고라스 정리에서 나온다. 직선 위의 다른 점 Q와 접점 T, 중심 O는 T에서 직각인 삼각형을 이루므로 $OQ^2 = r^2 + TQ^2 > r^2$이고, Q는 원의 바깥에 있다.

> **예제 4.9** $x^2 + y^2 = 25$ 위의 점 $(3, 4)$에서 접선은 $3x + 4y = 25$이다. 중심 $(0, 0)$에서 이 직선까지의 거리는 $25/\sqrt{3^2 + 4^2} = 25/5 = 5$로 반지름과 같아 접선임을 다시 확인할 수 있다.

4.7 원주각과 원에 내접한 사각형

원 위의 두 점 A, B가 정하는 호에 대하여, 중심 O에서 그 호를 바라보는 각을 **중심각**, 그 호 위에 있지 않은 원 위의 점 P에서 바라보는 각 $\angle APB$를 **원주각**(*inscribed angle*)이라고 한다. 같은 호를 바라보는 원주각은 중심각의 절반이다.

$$\angle APB = \frac{1}{2}\angle AOB. \tag{4.9}$$

중심과 원주 위 점들을 연결해 이등변삼각형의 밑각을 비교하면 증명할 수 있으며, 중심이 각의 내부 또는 외부에 있는 배치에 따라 각을 더하거나 빼면 된다. 호가 어느 쪽인지 함께 지정해야 보각을 혼동하지 않는다. 점 P를 포함하지 않는 호가 반원보다 크면 그 중심각은 π보다 크고 원주각은 둔각이다.

유도 (원주각 정리). P를 지나는 지름의 다른 끝점을 Q라 하자(그림 4.1). 삼각형 OPA는 $OP = OA$인 이등변삼각형이므로 두 밑각 $\angle OPA$와 $\angle OAP$가 같고, 꼭짓점 O에서의 외각 $\angle AOQ$는 이 두 각의 합이다. 따라서 $\angle APQ = \frac{1}{2}\angle AOQ$이다. 같은 이유로 $\angle QPB = \frac{1}{2}\angle QOB$이다.

1단계. 중심이 각의 변 위에 있는 경우, 곧 $B = Q$인 경우에는 위의 식이 곧 결론이다.

2단계. 중심이 각의 내부에 있으면 $\angle APB = \angle APQ + \angle QPB = \frac{1}{2}(\angle AOQ + \angle QOB) = \frac{1}{2}\angle AOB$이다.

3단계. 중심이 각의 외부에 있으면 두 각의 차를 취하여 $\angle APB = |\angle QPB - \angle QPA| = \frac{1}{2}|\angle QOB - \angle QOA| = \frac{1}{2}\angle AOB$이다.

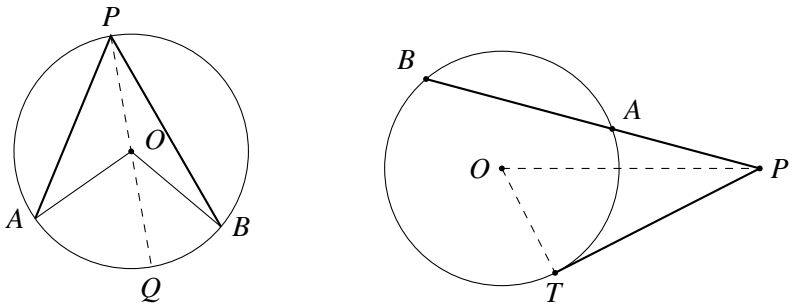

그림 4.1 원주각 $\angle APB$는 중심각 $\angle AOB$의 절반이다(왼쪽; 점선은 P를 지나는 지름). 원 밖의 점 P에서 그은 할선과 접선에 대하여 $PA \cdot PB = PT^2 = OP^2 - r^2$이다(오른쪽).

따라서 지름을 바라보는 원주각은 직각이다. 지름에 대한 중심각이 평각 π이기 때문이다. 한 원에 네 꼭짓점이 놓이는 볼록사각형에서는 마주 보는 두 내각의 합이 π이다. 두 각이 바라보는 호의 합이 한 바퀴 2π이기 때문이다. 역으로 마주 보는 두 내각의 합이 π인 볼록사각형은 한 원에 내접한다.

> **예제 4.10** 볼록사각형이 원에 내접하고 한 내각이 70°이면 맞은편 내각은 110°이다. 이웃각의 합이 반드시 180°라는 뜻은 아니다. 나머지 두 내각은 합이 180°라는 것만 정해지며, 예를 들어 60°와 120°일 수 있다.

참고 (외접원과 내접원의 반지름). 삼각형 ABC의 외접원의 반지름을 R라 하면 변 BC는 원주각 A가 바라보는 현이고 그 중심각은 $2A$이다. 중심에서 현에 내린 수선이 중심각을 이등분하므로 현의 길이는 $a = 2R\sin A$이다. 따라서 사인법칙의 공통값은 외접원의 지름이다.

$$\frac{a}{\sin A} = \frac{b}{\sin B} = \frac{c}{\sin C} = 2R, \qquad K = \frac{1}{2}bc\sin A = \frac{abc}{4R}.$$

내접원의 중심과 세 꼭짓점을 이으면 삼각형이 높이가 내접원의 반지름 r인 세 삼각형으로 나뉘므로 $K = \frac{1}{2}r(a+b+c) = rs$이다.

4.8 점의 멱

중심 O, 반지름 r인 원에 대한 점 P의 **멱**(*power of a point*)은 수 $OP^2 - r^2$이다. 멱은 P가 원 밖에 있으면 양수, 원 위에 있으면 0, 원 안에 있으면 음수이다. 다음 정리는 P를 지나는 직선이 원과 만나는 두 점까지의 부호 있는 거리의 곱이 직선의 방향과 무관하게 멱과 같음을 말한다.

> **정리 4.11** 중심 O, 반지름 r인 원과 점 P를 잡는다. P를 지나고 원과 만나는 직선에 단위방향벡터 $\mathbf{u}$를 정하고 교점을 $P + t_1\mathbf{u}$, $P + t_2\mathbf{u}$로 나타내면
>
> $$t_1 t_2 = \|P - O\|^2 - r^2 \tag{4.10}$$
>
> 이다. 여기서 t_j는 방향을 포함하는 부호 있는 길이이고, 직선이 원에 접하면 $t_1 = t_2$로 본다.

증명. 직선 위의 점 $P + t\mathbf{u}$가 원 위에 있을 조건 $\|P - O + t\mathbf{u}\|^2 = r^2$를 전개하면 $\|\mathbf{u}\| = 1$이므로

$$t^2 + 2\,\mathbf{u}\cdot(P-O)\,t + \|P-O\|^2 - r^2 = 0$$

이다. 직선이 원과 만나므로 이 이차방정식은 실근 t_1, t_2를 가지며, 접하는 경우는 중근이다. 두 근의 곱을 근과 계수의 관계로 읽으면 결론이다. □

외부 점에서 한 방향으로 원을 가로지르면 t_1, t_2의 부호가 같으므로 보통의 양의 길이로 $PA \cdot PB$가 일정하다. 접선의 경우 두 교점이 합쳐져 접선 길이의 제곱 PT^2이 그 값이다(그림 4.1의 오른쪽). 내부 점에서는 두 교점의 매개변수 부호가 반대이므로 부호 있는 곱은 음수이다. 이때 길이의 곱은 $PA \cdot PB = r^2 - OP^2$이며, 원 안의 한 점을 지나는 모든 현에서 두 조각의 길이의 곱이 같다.

> **예제 4.12** 원의 반지름이 3이고 외부 점에서 중심까지 거리가 5이면 접선 길이의 제곱은 $25 - 9 = 16$이므로 접선 길이는 4이다. 다른 할선의 두 양의 교점 거리도 곱이 16이어야 한다. 중심을 지나는 할선에서는 두 거리가 $5 - 3 = 2$와 $5 + 3 = 8$이고 곱이 16이다.

역사 (원에 관한 명제와 멱이라는 이름). 원주각이 중심각의 절반이라는 명제와, 한 점을 지나는 현 또는 할선의 두 조각으로 만든 직사각형의 넓이가 일정하다는 명제는 Euclid의 『원론』 제3권에 실려 있다. 이 일정한 값에 멱(*Potenz*)이라는 이름을 붙인 사람은 Jakob Steiner이며 1826년의 일이다.

핵심 수식

$$c^2 = a^2 + b^2 - 2ab\cos C, \qquad \frac{a}{\sin A} = \frac{b}{\sin B} = \frac{c}{\sin C} = 2R,$$

$$K = \frac{1}{2}ab\sin C = \sqrt{s(s-a)(s-b)(s-c)}, \quad s = \frac{a+b+c}{2},$$

$$(x_0 - a)(x - a) + (y_0 - b)(y - b) = r^2, \qquad PA \cdot PB = PT^2 = OP^2 - r^2 \quad (P\text{가 원 밖의 점}).$$

4.9 문제와 풀이

연습문제 4.13 변 길이가 $4, 5, 7$인 삼각형에서 가장 큰 각의 코사인을 구하여라.

풀이. 가장 긴 변 7의 맞은편 각 C가 가장 크다. 식 (4.3)에서 $\cos C = (16+25-49)/(2\cdot 4\cdot 5) = -1/5$이므로 둔각이다. 각의 크기는 약 101.5°이다.

연습문제 4.14 두 변이 $6, 8$이고 끼인각이 30°인 삼각형의 넓이를 구하여라.

풀이. $K = \tfrac{1}{2}\cdot 6 \cdot 8 \cdot \tfrac{1}{2} = 12$이다. 세 번째 변을 먼저 구할 필요가 없다.

연습문제 4.15 중심 $(1, -2)$, 반지름 5인 원의 점 $(4, 2)$에서 접선을 구하여라.

풀이. $(4-1)^2 + (2+2)^2 = 25$이므로 점 $(4,2)$는 원 위에 있다. 반지름 벡터는 $(3, 4)$이므로 식 (4.8)에서 $3(x-1) + 4(y+2) = 25$, 즉 $3x + 4y = 20$이다.

연습문제 4.16 외부 점 P에서 원을 지나는 한 할선의 두 교점까지 거리가 $3, 12$이다. 접선 길이와 다른 할선의 가까운 교점 거리가 4일 때 먼 교점 거리를 구하여라.

풀이. 점의 멱은 $3 \cdot 12 = 36$이므로 접선 길이는 6이다. 다른 두 거리의 곱도 36이므로 먼 거리는 $36/4 = 9$이다.

연습문제 4.17 변이 $5, 5, 6$인 삼각형의 넓이를 두 방법으로 구하여라.

풀이. 이등변삼각형이므로 꼭짓점에서 밑변 6에 내린 수선이 밑변을 반으로 나눈다. 높이는 $\sqrt{25 - 9} = 4$이고 넓이는 $\tfrac{1}{2}\cdot 6 \cdot 4 = 12$이다. 헤론 공식에서는 $s = 8$이므로 $\sqrt{8\cdot 3\cdot 3\cdot 2} = \sqrt{144} = 12$이다.

연습문제 4.18 변이 $13, 14, 15$인 삼각형의 외접원의 반지름 R와 내접원의 반지름 r를 구하여라.

풀이. 예제 4.8에서 $K = 84$, $s = 21$이다. $K = abc/(4R)$에서 $R = 13\cdot 14\cdot 15/(4\cdot 84) = 2730/336 = 65/8$이고, $K = rs$에서 $r = 84/21 = 4$이다. 검산으로, 길이 13인 변의 맞은편 각을 A라 하면 $84 = \tfrac{1}{2}\cdot 14 \cdot 15\sin A$에서 $\sin A = 4/5$이고 $13/\sin A = 65/4 = 2R$이다.

제 5 장

이차곡선과 극좌표

개요 이차곡선(*conic section*)은 두 변수 x, y의 이차방정식으로 정해지는 평면곡선이며, 퇴화하지 않은 것은 포물선·타원·쌍곡선 가운데 하나이다. 이 장은 세 곡선을 초점과 준선까지의 거리로 정의하고, 그 정의에서 표준형 방정식을 유도하며, 역으로 표준형 위의 점이 거리 조건을 만족함을 확인한다. 이어서 평행이동과 퇴화 경우, 일반 이차식의 판별식에 따른 분류, 매개변수 표현을 다루고, 극좌표를 정의하여 한 점이 여러 좌표를 갖는 까닭과 직교좌표와의 변환을 정리한다. 마지막으로 이심률을 써서 세 곡선을 하나의 조건으로 묶고, 초점을 극으로 하는 극방정식을 유도한다. 이차곡선은 대수식과 기하적 자취를 연결하는 첫 본보기이다. 선행 지식: 거리 공식과 직선(제3권 제2장), 완전제곱(제2권 제5장), 삼각함수(제3권 제3장).

5.1 포물선: 한 점과 한 직선까지 같은 거리

정의 5.1 고정된 점과, 그 점을 지나지 않는 고정된 직선까지의 거리가 같은 평면의 점들의 집합을 **포물선**(*parabola*)이라 한다. 이때 고정된 점을 **초점**(*focus*), 고정된 직선을 **준선**(*directrix*)이라 한다.

초점을 $(0, p)$, 준선을 $y = -p$로 놓고 $p \neq 0$이라 하자. 점 (x, y)에서 준선까지의 거리는 $|y + p|$이므로 거리 등식은

$$\sqrt{x^2 + (y - p)^2} = |y + p|$$

이다. 두 변이 모두 음이 아니므로 이 등식은 양변을 제곱한 식 $x^2 + y^2 - 2py + p^2 = y^2 + 2py + p^2$과 동치이고, 정리하면

$$x^2 = 4py \tag{5.1}$$

이다. 초점을 지나 준선에 수직인 직선을 포물선의 **축**(*axis*), 축과 포물선의 교점을 **꼭짓점**(*vertex*)이라 한다. 식 (5.1)에서 꼭짓점은 원점이고 축은 세로축이며, 곡선은 축에 대하여 대칭이다. $p > 0$이면 위로, $p < 0$이면 아래로 열린다. 꼭짓점에서 초점까지의 거리 $|p|$를 초점 거리라 한다.

초점이 준선 위에 있는 경우는 정의에서 제외한다. $p = 0$이면 거리 등식이 $\sqrt{x^2 + y^2} = |y|$, 곧 $x = 0$이 되어 자취가 곡선이 아니라 준선에 수직인 직선이 되기 때문이다.

예제 5.2 $x^2 = 8y$는 $4p = 8$에서 $p = 2$이므로 초점은 $(0, 2)$, 준선은 $y = -2$이다. 꼭짓점을 (h, k)로 옮긴 $(x - h)^2 = 4p(y - k)$에서는 초점이 $(h, k + p)$, 준선이 $y = k - p$이다. 좌표의 역할을 바꾼 $y^2 = 4px$는 초점이 $(p, 0)$, 준선이 $x = -p$이며 $p > 0$이면 오른쪽으로 열린다.

이차함수의 그래프 $y = ax^2 + bx + c$ $(a \neq 0)$는 완전제곱으로 꼭짓점 형태

$$y = a\left(x + \frac{b}{2a}\right)^2 + c - \frac{b^2}{4a}$$

로 바꿀 수 있다. 이것은 $(x-h)^2 = 4p(y-k)$에서 $h = -b/(2a)$, $k = c - b^2/(4a)$, $4p = 1/a$로 둔 것이므로, 계수 a와 초점 거리 p는

$$a = \frac{1}{4p}$$

로 연결된다. 예를 들어 $y = 2x^2 - 4x + 5 = 2(x-1)^2 + 3$은 꼭짓점이 $(1, 3)$이고 $p = 1/8$이므로 초점은 $(1, 25/8)$, 준선은 $y = 23/8$이다.

$|a|$가 클수록 초점이 꼭짓점에 가깝고 그래프가 좁게 그려진다. 그러나 좁아 보이는 정도는 좌표축의 표시 배율에 따라 달라지므로, 두 포물선을 비교할 때에는 p의 수치와 축의 단위를 함께 보아야 한다. 실제로 $x^2 = 4py$에 $x = 4pX$, $y = 4pY$를 대입하면 $Y = X^2$이 되므로, 모든 포물선은 $y = x^2$을 $4|p|$배로 확대하거나 축소한 것과 합동이다. 곧 포물선은 모두 서로 닮은 도형이다.

5.2 타원: 두 초점까지 거리의 합

> **정의 5.3** 서로 다른 두 고정된 점까지의 거리의 합이 일정하고, 그 합이 두 점 사이의 거리보다 큰 평면의 점들의 집합을 **타원**(*ellipse*)이라 한다. 두 고정된 점을 타원의 초점이라 한다. 두 초점이 일치하는 경우의 자취인 원은 이 정의의 자연스러운 확장으로 다룰 수 있다.

초점이 $(\pm c, 0)$이고 거리의 합이 $2a$라 하자. 정의에 따라 $a > c > 0$이고, 원까지 포함하면 $a > c \geq 0$이다. $b > 0$을 $b^2 = a^2 - c^2$으로 정하면 타원의 방정식은

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 \tag{5.2}$$

이다. a는 **긴 반지름**(*semi-major axis*), b는 **짧은 반지름**(*semi-minor axis*), c는 중심에서 초점까지의 거리이다. 두 초점의 중점인 원점이 타원의 **중심**이고, 축과 만나는 네 점 $(\pm a, 0)$, $(0, \pm b)$가 꼭짓점이다. 길이 $2a$인 선분을 장축, 길이 $2b$인 선분을 단축이라 한다. $c = 0$이면 $a = b$이고 식 (5.2)는 반지름 a인 원이다.

초점 거리와 두 반지름의 관계는

$$c^2 = a^2 - b^2 \tag{5.3}$$

이다. 꼭짓점 $(0, b)$에서 각 초점까지의 거리가 $\sqrt{b^2 + c^2} = a$이므로, 이 식은 두 변이 b, c이고 빗변이 a인 직각삼각형의 피타고라스 정리이다. 빗변은 c가 아니라 a이며, 이 모양을 $c^2 = a^2 + b^2$으로 바꾸어 쓰면 쌍곡선의 관계식이 된다.

자취에서 방정식을 얻는 계산. 점 (x, y)에서 두 초점 $(c, 0)$, $(-c, 0)$까지의 거리를 각각

$$r_+ = \sqrt{(x-c)^2 + y^2}, \qquad r_- = \sqrt{(x+c)^2 + y^2}$$

라 하자. 먼저 $r_+ + r_- = 2a$라 가정한다. 제곱의 차는 $r_-^2 - r_+^2 = 4cx$이고 $r_-^2 - r_+^2 = (r_- - r_+)(r_- + r_+)$이므로 $r_- - r_+ = 2cx/a$이다. 이 식과 $r_- + r_+ = 2a$를 더하고 빼면

$$r_- = a + \frac{cx}{a}, \qquad r_+ = a - \frac{cx}{a} \tag{5.4}$$

이다. 첫 식을 제곱하면 $x^2 + 2cx + c^2 + y^2 = a^2 + 2cx + c^2x^2/a^2$이고, 정리하면 $(a^2 - c^2)x^2/a^2 + y^2 = a^2 - c^2$, 곧

$$\frac{x^2}{a^2} + \frac{y^2}{a^2 - c^2} = 1$$

이다.

역으로 점 (x, y)가 이 방정식을 만족한다고 하자. $y^2 = b^2(1 - x^2/a^2)$을 대입하면

$$(x \pm c)^2 + y^2 = \frac{c^2 x^2}{a^2} \pm 2cx + a^2 = \left(a \pm \frac{cx}{a}\right)^2$$

이다. 타원 위에서는 $|x| \le a$이므로 $a \pm cx/a \ge a - c > 0$이다. 따라서 양의 제곱근을 취하면 식 (5.4)이 복원되고, 두 거리의 합은 $r_+ + r_- = 2a$이다. □

> **예제 5.4** $x^2/25 + y^2/9 = 1$에서는 $a = 5$, $b = 3$, $c = \sqrt{25 - 9} = 4$이다. 초점은 $(\pm 4, 0)$이고 두 초점까지 거리의 합은 10이다. 꼭짓점 $(0, 3)$에서는 두 거리가 각각 $\sqrt{16 + 9} = 5$이고, 꼭짓점 $(5, 0)$에서는 1과 9이므로 합이 10임이 실제로 확인된다.

참고 (거리의 합에 붙은 조건). 삼각부등식에 의해 평면의 모든 점에서 $r_+ + r_- \ge 2c$이고, 등호는 두 초점을 잇는 선분 위의 점에서만 성립한다. 따라서 거리의 합이 $2c$와 같으면 자취는 그 선분이고, $2c$보다 작으면 공집합이다. 정의 5.3에서 합이 초점 사이 거리보다 크다고 요구하는 까닭이 이것이다.

참고 (세로로 긴 타원). 초점이 세로축 위의 $(0, \pm c)$에 있고 거리의 합이 $2a$이면 방정식은 $x^2/b^2 + y^2/a^2 = 1$이다. 표준형에서 초점은 언제나 분모가 큰 쪽의 축 위에 놓이며, 식 (5.3)는 그대로 성립한다.

5.3 쌍곡선: 거리 차의 절댓값

두 초점 $(\pm c, 0)$까지의 거리의 차의 절댓값이 $2a$로 일정하고 $0 < a < c$인 점들의 자취를 **쌍곡선**(*hyperbola*)이라 한다. $b > 0$을 $b^2 = c^2 - a^2$으로 정하면 쌍곡선의 방정식은

$$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1 \tag{5.5}$$

이다. 이 식에서 $x^2 \ge a^2$이므로 곡선은 $x \ge a$인 부분과 $x \le -a$인 부분, 두 가지(*branch*)로 나뉜다. 꼭짓점은 $(\pm a, 0)$, 초점은 $(\pm c, 0)$이다. 타원과 달리

$$c^2 = a^2 + b^2 \tag{5.6}$$

이다. 두 직선

$$y = \pm \frac{b}{a} x \tag{5.7}$$

를 쌍곡선의 **점근선**(*asymptote*)이라 한다.

유도 (쌍곡선의 방정식). 타원에서와 같이 $r_\pm = \sqrt{(x \mp c)^2 + y^2}$으로 두고 $r_- - r_+ = \pm 2a$라 하자. $r_-^2 - r_+^2 = 4cx$이므로 $r_- + r_+ = \pm 2cx/a$이고, 두 식을 더하면 $r_- = \pm(a + cx/a)$이다. 제곱하면 부호와 관계없이 타원의 경우와 같은 식 $x^2/a^2 + y^2/(a^2 - c^2) = 1$을 얻는데, 이번에는 $a^2 - c^2 = -b^2 < 0$이므로 식 (5.5)가 된다. 역으로 식 (5.5) 위의 점에서는 $y^2 = b^2(x^2/a^2 - 1)$을 대입하여 $r_\pm^2 = (cx/a \mp a)^2$을 얻는다. $x \ge a$이면 $cx/a \ge c > a$이므로 $r_- = cx/a + a$, $r_+ = cx/a - a$이고 $r_- - r_+ = 2a$이다. $x \le -a$이면 $r_- = -cx/a - a$, $r_+ = -cx/a + a$이고 $r_- - r_+ = -2a$이다. 두 경우 모두 거리 차의 절댓값이 $2a$이다.

예제 5.5 $x^2/9 - y^2/16 = 1$이면 $a = 3$, $b = 4$, $c = \sqrt{9+16} = 5$이다. 초점은 $(\pm 5, 0)$, 점근선은 $y = \pm 4x/3$이다. 점근선의 기울기를 $3/4$으로 뒤집어 쓰지 않으려면 원래 식의 최고차 부분을 0으로 둔 $x^2/9 - y^2/16 = 0$, 곧 $y^2 = 16x^2/9$에서 직접 구한다.

점근선은 "곡선과 만나지 않는 직선"으로 정의되는 것이 아니다. 여기에서는 $x \to \pm\infty$일 때 해당 가지와 직선 사이의 세로 방향 차가 0으로 간다는 뜻이다. 오른쪽 가지의 위쪽 절반 $y = (b/a)\sqrt{x^2 - a^2}$ $(x \ge a)$에 대하여

$$\frac{b}{a}x - \frac{b}{a}\sqrt{x^2 - a^2} = \frac{b}{a}\cdot\frac{a^2}{x + \sqrt{x^2 - a^2}} = \frac{ab}{x + \sqrt{x^2 - a^2}}$$

이고, 이 값은 양수이면서 $x \to \infty$일 때 0으로 간다. 나머지 세 부분은 대칭으로 같은 결론을 얻는다. 쌍곡선은 점근선과 만나지 않지만 이것은 쌍곡선의 성질이지 점근선의 정의가 아니다. 예를 들어 $y = (\sin x)/x$의 그래프는 점근선 $y = 0$과 무한히 여러 번 교차한다. 극한의 엄밀한 정의는 제8권 제1장에서 다룬다.

참고 (거리 차에 붙은 조건과 세로 방향 쌍곡선). 삼각부등식에 의해 $|r_- - r_+| \le 2c$이므로 $a > c$이면 자취는 공집합이다. $a = c$이면 자취는 두 초점에서 바깥쪽으로 뻗는 두 반직선이고, $a = 0$이면 두 초점을 잇는 선분의 수직이등분선이다. 초점이 세로축 위의 $(0, \pm c)$에 있으면 방정식은 $y^2/a^2 - x^2/b^2 = 1$이고, 꼭짓점은 $(0, \pm a)$, 점근선은 $y = \pm(a/b)x$이다. 표준형에서 초점과 꼭짓점은 부호가 양인 항의 축 위에 놓인다.

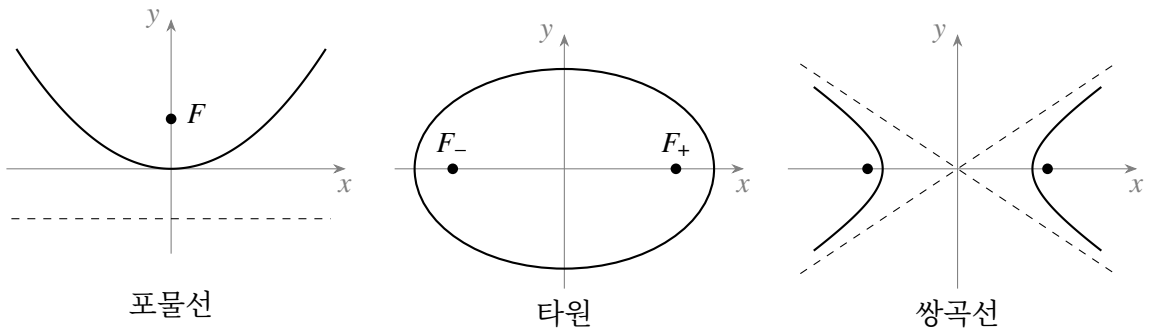

그림 5.1 세 이차곡선의 예. 왼쪽부터 포물선 $x^2 = 4y$, 타원 $x^2/9 + y^2/4 = 1$, 쌍곡선 $4x^2/9 - y^2 = 1$이다. 검은 점은 초점이고, 포물선 아래의 수평 점선은 준선 $y = -1$, 쌍곡선의 두 점선은 점근선 $y = \pm 2x/3$이다.

표준형

포물선	$x^2 = 4py$,	초점 $(0, p)$, 준선 $y = -p$,
타원	$\dfrac{x^2}{a^2} + \dfrac{y^2}{b^2} = 1$,	초점 $(\pm c, 0)$, $c^2 = a^2 - b^2$,
쌍곡선	$\dfrac{x^2}{a^2} - \dfrac{y^2}{b^2} = 1$,	초점 $(\pm c, 0)$, $c^2 = a^2 + b^2$, 점근선 $y = \pm\dfrac{b}{a}x$.

역사. 이차곡선은 고대 그리스에서 원뿔을 평면으로 자른 단면으로 연구되었고, 원뿔곡선이라는 이름이 여기서 나왔다. Perga의 Apollonius는 기원전 200년 무렵의 저술 『원뿔곡선론』에서 이 곡선들을 체계적으로 다루었으며, 타원·포물선·쌍곡선이라는 이름도 그에게서 비롯한다. Kepler는 1609년 『신천문학』에서 행성의 궤도가 태양을 한 초점으로 하는 타원임을 밝혔다.

5.4 평행이동과 퇴화 경우

이차식에 일차항이 있으면 완전제곱으로 중심이나 꼭짓점을 옮긴다. 이때 완전제곱 뒤의 우변이 양수인지, 0인지, 음수인지를 확인해야 한다. 이를 확인하지 않고 좌변의 모양만으로 판정하면 한 점이나 공집합을 타원이라고 잘못 부르게 된다. 예를 들어 $A, C > 0$일 때 $Ax^2+Cy^2+Dx+Ey+F = 0$은

$$A\left(x+\frac{D}{2A}\right)^2 + C\left(y+\frac{E}{2C}\right)^2 = G, \qquad G = \frac{D^2}{4A}+\frac{E^2}{4C}-F$$

와 같고, $G > 0$이면 타원, $G = 0$이면 한 점, $G < 0$이면 공집합이다.

> **예제 5.6** $x^2 + 4y^2 - 2x + 8y + 1 = 0$은 $(x-1)^2 - 1 + 4(y+1)^2 - 4 + 1 = 0$, 곧
>
> $$(x-1)^2 + 4(y+1)^2 = 4$$
>
> 이고, 양변을 4로 나누면 $(x-1)^2/4 + (y+1)^2 = 1$이다. 중심은 $(1, -1)$이고 반지름은 가로 2, 세로 1이다. $c = \sqrt{4-1} = \sqrt{3}$이므로 초점은 $(1 \pm \sqrt{3}, -1)$이다.

> **예제 5.7** $x^2 + y^2 = 0$의 실수 자취는 원점 하나이고, $x^2 + y^2 = -1$의 실수 자취는 공집합이다. $x^2 - y^2 = 0$은 $(x-y)(x+y) = 0$이므로 두 직선 $y = \pm x$의 합집합이다. 이들은 모두 이차식으로 표현되지만 타원이나 쌍곡선이 아니다. 이처럼 이차방정식의 자취가 점, 직선, 공집합이 되는 경우를 **퇴화**(*degenerate*) 경우라 한다.

일반적인 이차방정식

$$Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0 \qquad (A,\ B,\ C \text{ 가운데 적어도 하나는 0이 아니다}) \tag{5.8}$$

에서는 좌표축을 회전하여 교차항 Bxy를 없앤 다음 완전제곱을 한다. 축을 각 φ만큼 회전한 좌표 (u, v)를

$$x = u\cos\varphi - v\sin\varphi, \qquad y = u\sin\varphi + v\cos\varphi$$

로 도입하면 이차 부분은 $A'u^2 + B'uv + C'v^2$으로 바뀌고, 삼각함수의 배각 공식으로 정리하면

$$B' = B\cos 2\varphi - (A-C)\sin 2\varphi$$

이다. 따라서 $B \neq 0$일 때 $\cot 2\varphi = (A-C)/B$인 φ를 택하면 교차항이 사라진다. 이 회전에서 $A' + C' = A + C$와 $B'^2 - 4A'C' = B^2 - 4AC$가 성립한다. 곧 **판별식**(*discriminant*) $B^2 - 4AC$는 좌표축의 회전으로 바뀌지 않는다.

$B^2 - 4AC$의 부호는 곡선의 유형을 판단하는 중요한 정보이다. 그러나 표 5.1가 보이듯이 퇴화 여부와 실수 점의 존재까지 그것 하나로 결정하지는 못한다.

표 5.1 판별식에 따른 이차방정식 (5.8)의 실수 자취

$B^2 - 4AC$	퇴화하지 않은 경우	퇴화 경우와 그 예
음수	타원(원 포함)	한 점 $(x^2 + y^2 = 0)$, 공집합 $(x^2 + y^2 = -1)$
0	포물선	평행한 두 직선 $(x^2 = 1)$, 한 직선 $(x^2 = 0)$, 공집합 $(x^2 = -1)$
양수	쌍곡선	만나는 두 직선 $(x^2 - y^2 = 0)$

교차항을 없애는 문제는 선형대수에서 이차형식의 대각화로 다룬다. 식 (5.8)의 이차 부분은 대칭행렬로

$$Ax^2 + Bxy + Cy^2 = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

와 같이 쓸 수 있고, 교차항을 없앤 뒤의 계수 A', C'은 이 행렬의 두 고유값이다. 행렬식이 $AC - B^2/4$이므로 판별식이 음수이면 두 고유값의 부호가 같고, 양수이면 다르며, 0이면 한 고유값이 0이다. 대칭행렬의 고유값과 직교 대각화(제7권 제7장, 제7권 제8장)가 기하 문제에 쓰이는 대표적인 연결이다.

참고 (교차항만 있는 쌍곡선). $xy = 1$은 $A = C = 0$, $B = 1$이므로 판별식이 $1 > 0$이고 $\cot 2\varphi = 0$에서 $\varphi = \pi/4$이다. $x = (u - v)/\sqrt{2}$, $y = (u + v)/\sqrt{2}$를 대입하면 $xy = (u^2 - v^2)/2$이므로 방정식은 $u^2/2 - v^2/2 = 1$이다. 곧 $a = b = \sqrt{2}$, $c = 2$인 쌍곡선이고, 초점은 $(u, v) = (\pm 2, 0)$, 원래 좌표로 $\pm(\sqrt{2}, \sqrt{2})$이다. 점근선 $v = \pm u$는 원래 좌표의 두 좌표축 $x = 0$, $y = 0$이다.

5.5 매개변수 표현

타원 (5.2)는

$$x = a\cos t, \qquad y = b\sin t, \qquad 0 \le t < 2\pi \tag{5.9}$$

로 표현할 수 있다. 대입하면 $\cos^2 t + \sin^2 t = 1$에 의해 타원의 방정식을 만족한다. 역으로 타원 위의 점 (x, y)에 대해서는 점 $(x/a, y/b)$가 단위원 위에 있으므로 $\cos t = x/a$, $\sin t = y/b$인 t가 $0 \le t < 2\pi$에서 꼭 하나 있다. 따라서 이 표현은 타원의 모든 점을 한 번씩 얻는다.

매개변수 t는 일반적으로 원점에서 그 점을 향하는 방향각 θ와 같지 않다. $\cos t \neq 0$일 때 두 각은

$$\tan\theta = \frac{y}{x} = \frac{b}{a}\tan t$$

로 연결되며, 원인 경우 $a = b$에서만 모든 점에서 두 각이 일치한다. $a \neq b$이면 네 꼭짓점에서만 일치한다.

> **예제 5.8** $x = 3\cos t$, $y = 2\sin t$에서 $t = \pi/4$이면 점은 $(3/\sqrt{2}, \sqrt{2})$이다. 원점과 이 점을 잇는 직선의 기울기는 $\sqrt{2}\cdot\sqrt{2}/3 = 2/3$이므로 원점에서 본 방향각의 탄젠트는 $2/3$이다. 이것은 매개변수 $t = \pi/4$의 탄젠트 1과 다르다.

포물선 $x^2 = 4py$는

$$(x, y) = (2pt,\ pt^2), \qquad t \in \mathbb{R}$$

로 매개화할 수 있다. $(2pt)^2 = 4p\cdot pt^2$이고 $t = x/(2p)$가 점마다 하나로 정해지기 때문이다. 쌍곡선 $x^2/a^2 - y^2/b^2 = 1$의 오른쪽 가지는

$$(x, y) = (a\cosh t,\ b\sinh t), \qquad t \in \mathbb{R}$$

로 매개화할 수 있다. 여기서 **쌍곡선함수**(*hyperbolic function*)는

$$\cosh t = \frac{e^t + e^{-t}}{2}, \qquad \sinh t = \frac{e^t - e^{-t}}{2}$$

이며, 이 표현은 항등식

$$\cosh^2 t - \sinh^2 t = \frac{(e^t + e^{-t})^2 - (e^t - e^{-t})^2}{4} = 1$$

을 사용한다. $\cosh t \geq 1$이므로 $x \geq a$인 가지만 얻으며, 왼쪽 가지는 $(-a\cosh t,\ b\sinh t)$이다. sinh가 $\mathbb{R}$에서 $\mathbb{R}$로 가는 증가하는 일대일 대응이므로 $y = b\sinh t$에서 t가 하나로 정해지고, 가지의 각 점은 한 번씩 얻어진다.

5.6 극좌표와 같은 점의 여러 표현

평면의 점을 원점에서의 거리 $r \geq 0$과, 양의 x축에서 반시계 방향으로 잰 방향각 θ로 나타낸 순서쌍 (r, θ)를 그 점의 **극좌표**(*polar coordinates*)라 한다. 이때 원점을 극(*pole*)이라 한다. 직교좌표와의 관계는

$$x = r\cos\theta, \qquad y = r\sin\theta \tag{5.10}$$

이다. 반지름은 $r = \sqrt{x^2 + y^2}$으로 정해진다. 원점이 아닌 점에서 방향각은 $\cos\theta = x/r$, $\sin\theta = y/r$로 정해지며 2π의 정수배만큼의 차이를 제외하면 유일하다. 원점에서는 $r = 0$이고 모든 θ가 같은 점을 나타낸다. 음의 r까지 허용하는 관례에서는 식 (5.10)를 그대로 정의로 쓰며, 이때 (r, θ)와 $(-r, \theta+\pi)$도 같은 점이다. 직교좌표와 달리 극좌표는 한 점에 여러 좌표가 대응하므로, 극방정식의 자취를 구할 때 한 점의 좌표 가운데 하나라도 방정식을 만족하면 그 점은 자취에 속한다.

> **예제 5.9** 직교좌표 $(-1, \sqrt{3})$의 반지름은 $\sqrt{1+3} = 2$이고 방향각의 한 선택은 $2\pi/3$이다. 단순히 $\arctan(y/x)$만 계산하면 $\arctan(-\sqrt{3}) = -\pi/3$을 얻어 제2사분면의 점을 제4사분면의 방향으로 잘못 읽게 된다. 두 좌표의 부호를 함께 사용하여 사분면을 판정해야 한다.

방법 (방향각의 계산). arctan의 값은 $(-\pi/2, \pi/2)$에 있으므로 $x > 0$인 점의 방향만 나타낼 수 있다. 원점이 아닌 점 (x, y)의 방향각은 다음과 같이 택한다.

$$\theta = \begin{cases} \arctan(y/x), & x > 0, \\ \arctan(y/x) + \pi, & x < 0, \\ \pi/2, & x = 0,\ y > 0, \\ -\pi/2, & x = 0,\ y < 0. \end{cases}$$

예제 5.9에서는 $x < 0$이므로 $\theta = -\pi/3 + \pi = 2\pi/3$이다.

> **예제 5.10** $r = 2a\cos\theta$에서 $r \geq 0$, $a > 0$이라 하자. 양변에 r을 곱하면 $r^2 = 2ar\cos\theta$, 곧 $x^2 + y^2 = 2ax$이다. 따라서 자취는 원 $(x-a)^2 + y^2 = a^2$에 포함된다. 역으로 이 원 위의 원점이 아닌 점에서는 $2ax = x^2 + y^2 > 0$이므로 $\cos\theta > 0$이고, $r^2 = 2ar\cos\theta$를 $r > 0$으로 나누어 $r = 2a\cos\theta$를 얻는다. 원점은 $\theta = \pi/2$에서 $r = 0$으로 얻어진다. 그러므로 자취는 중심 $(a, 0)$, 반지름 a인 원 전체이며, 각의 허용 범위는 $r \geq 0$에 맞추어 $\cos\theta \geq 0$이다. r을 곱하는 변형은 $r = 0$인 점을 새로 들여올 수 있으므로, 원점이 원래 자취에 속하는지를 이와 같이 따로 확인한다.

극좌표는 복소수의 극형식(제1권 제10장)과 같은 내용이며, 중적분의 변수변환(제9권 제5장)에서 다시 쓰인다.

5.7 이심률과 초점을 극으로 하는 방정식

타원과 쌍곡선에서 비

$$e = \frac{c}{a} \tag{5.11}$$

를 **이심률**(*eccentricity*)이라 한다. 타원에서는 $0 \le e < 1$이고 $e = 0$이 원이며, 쌍곡선에서는 $e > 1$이다. 이 절의 e는 이심률이며 자연상수가 아니다.

식 (5.4)을 이심률로 다시 쓰면 $e > 0$인 타원 위의 점 (x, y)에서 초점 $(c, 0)$까지의 거리는

$$r_+ = a - ex = e\left(\frac{a}{e} - x\right)$$

이다. $x \le a < a/e$이므로 괄호 안은 점에서 직선 $x = a/e$까지의 거리이다. 쌍곡선에서도 $r_+ = |ex - a| = e\,|x - a/e|$이다. 곧 타원과 쌍곡선 위의 점에서는 초점까지의 거리가 직선 $x = a/e$까지의 거리의 e배이다. 이 직선을 초점 $(c, 0)$에 대응하는 준선이라 한다. 포물선은 정의 5.1에 의해 이 비가 1인 곡선이다. 따라서 세 곡선은 하나의 조건으로 묶인다.

점 F와 F를 지나지 않는 직선 L, 양수 e에 대하여 F까지의 거리가 L까지의 거리의 e배인 점의 자취는 $e < 1$이면 타원, $e = 1$이면 포물선, $e > 1$이면 쌍곡선이다. 이를 확인하려면 F를 원점에, L을 직선 $x = d$ $(d > 0)$에 놓는다. 조건 $\sqrt{x^2 + y^2} = e\,|d - x|$를 제곱하면

$$(1 - e^2)x^2 + 2e^2 d\,x + y^2 = e^2 d^2$$

이다. 판별식은 $-4(1 - e^2)$이므로 표 5.1의 세 유형이 $e < 1$, $e = 1$, $e > 1$에 차례로 대응한다. $e = 1$이면 $y^2 = -2d(x - d/2)$인 포물선이다. $e \ne 1$이면 완전제곱으로

$$(1 - e^2)\left(x + \frac{e^2 d}{1 - e^2}\right)^2 + y^2 = \frac{e^2 d^2}{1 - e^2}$$

을 얻고, $d > 0$이므로 우변이 0이 아니며 그 부호가 x의 제곱항의 계수와 같다. 따라서 어느 경우에도 퇴화하지 않는다.

같은 배치에서 극좌표를 쓰면 방정식이 간단해진다. F와 같은 쪽$(x < d)$에 있는 점에서는 $r = e(d - r\cos\theta)$이므로

$$r = \frac{\ell}{1 + e\cos\theta}, \qquad \ell = ed \tag{5.12}$$

이다. $e \le 1$이면 $x \ge d$인 점에서 $r \ge x > e(x - d)$이므로 자취 전체가 $x < d$에 있고, 식 (5.12)이 곡선 전체를 나타낸다. $e > 1$이면 이 식은 $1 + e\cos\theta > 0$인 각에서 F에 가까운 가지를 나타내며, 다른 가지는 $x > d$에서 $r = \ell/(e\cos\theta - 1)$로 주어진다. 상수 ℓ은 $\theta = \pi/2$일 때의 r, 곧 초점을 지나고 축에 수직인 현의 길이의 절반이며 반통경(*semi-latus rectum*)이라 한다. 타원과 쌍곡선에서는 $d = |a/e - c|$이므로 $\ell = a\left|1 - e^2\right| = b^2/a$이고, 포물선 $x^2 = 4py$에서는 $\ell = 2\,|p|$이다. 표 5.2에 세 곡선의 값을 모았다.

표 5.2 이심률로 본 세 이차곡선

곡선	이심률	표준형	초점	준선	반통경 ℓ
타원	$0 < e < 1$	$x^2/a^2 + y^2/b^2 = 1$	$(\pm c, 0)$	$x = \pm a/e$	b^2/a
포물선	$e = 1$	$x^2 = 4py$	$(0, p)$	$y = -p$	$2\,\lvert p\rvert$
쌍곡선	$e > 1$	$x^2/a^2 - y^2/b^2 = 1$	$(\pm c, 0)$	$x = \pm a/e$	b^2/a

타원의 경우 식 (5.12)에서 초점까지의 거리는 $\theta = 0$에서 최솟값 $\ell/(1+e) = a(1-e)$, $\theta = \pi$에서 최댓값 $\ell/(1-e) = a(1+e)$를 갖고 두 값의 합은 $2a$이다. 행성의 궤도는 태양을 한 초점으로 하는 타원이므로 이 두 값이 근일점 거리와 원일점 거리이다. 지구 궤도는 $a \approx 1.496 \times 10^8\,\text{km}$, $e \approx 0.0167$이므로 근일점 거리는 약 $1.471 \times 10^8\,\text{km}$, 원일점 거리는 약 $1.521 \times 10^8\,\text{km}$이고, 두 거리의 비는 $(1-e)/(1+e) \approx 0.967$이다.

극좌표

$$x = r\cos\theta, \quad y = r\sin\theta, \quad r = \sqrt{x^2+y^2},$$

$$r = \frac{\ell}{1 + e\cos\theta} \qquad (\text{초점이 극인 이차곡선, } e\text{는 이심률, } \ell\text{은 반통경}).$$

5.8 문제와 풀이

연습문제 5.11 $(y-1)^2 = 12(x+2)$의 초점과 준선을 구하여라.

풀이. $(y-k)^2 = 4p(x-h)$ 꼴이므로 꼭짓점은 $(-2, 1)$이고 오른쪽으로 열린다. $4p = 12$이므로 $p = 3$이다. 초점은 꼭짓점에서 오른쪽으로 3만큼 간 $(1, 1)$이고, 준선은 왼쪽으로 3만큼 간 $x = -5$이다. 검산으로 곡선 위의 점 $(1, 7)$을 보면 초점까지의 거리와 준선까지의 거리가 모두 6이다.

연습문제 5.12 $x^2/16 + y^2/7 = 1$의 초점과 거리의 합을 구하여라.

풀이. $a = 4$, $b = \sqrt{7}$, $c = \sqrt{16-7} = 3$이다. 초점은 $(\pm 3, 0)$이고 거리의 합은 $2a = 8$이다.

연습문제 5.13 $y^2/9 - x^2/16 = 1$의 꼭짓점과 점근선을 구하여라.

풀이. 부호가 양인 항이 y^2이므로 세로축 방향 쌍곡선이고 꼭짓점은 $(0, \pm 3)$이다. 최고차 부분을 0으로 두면 $y^2/9 = x^2/16$이므로 점근선은 $y = \pm 3x/4$이다.

연습문제 5.14 $x^2 + y^2 + 4x - 6y + 13 = 0$의 실수 자취를 구하여라.

풀이. 완전제곱을 하면 $(x+2)^2 - 4 + (y-3)^2 - 9 + 13 = 0$, 곧 $(x+2)^2 + (y-3)^2 = 0$이므로 자취는 점 $(-2, 3)$ 하나이다. 반지름이 양수인 원이 아니다.

연습문제 5.15 극좌표 $r = 3$, $\theta = 7\pi/6$인 점의 직교좌표를 구하여라.

풀이. $7\pi/6$은 제3사분면의 각이므로 두 좌표는 모두 음수이다. $\cos(7\pi/6) = -\sqrt{3}/2$, $\sin(7\pi/6) = -1/2$이므로 $(x, y) = (-3\sqrt{3}/2,\ -3/2)$이다.

연습문제 5.16 $4x^2 - 9y^2 - 16x - 18y - 29 = 0$이 나타내는 곡선의 중심, 초점, 점근선을 구하여라.

풀이. $4(x^2 - 4x) - 9(y^2 + 2y) = 29$에서 완전제곱을 하면 $4(x-2)^2 - 16 - 9(y+1)^2 + 9 = 29$, 곧 $4(x-2)^2 - 9(y+1)^2 = 36$이다. 양변을 36으로 나누면

$$\frac{(x-2)^2}{9} - \frac{(y+1)^2}{4} = 1$$

이므로 중심이 $(2, -1)$이고 $a = 3$, $b = 2$, $c = \sqrt{13}$인 쌍곡선이다. 초점은 $(2 \pm \sqrt{13}, -1)$이고 점근선은 $y + 1 = \pm\frac{2}{3}(x-2)$이다. 우변이 0이었다면 자취는 이 두 직선의 합집합이 된다.

연습문제 5.17 극방정식 $r = \dfrac{6}{2 + \cos\theta}$ $(r \ge 0)$이 나타내는 곡선의 직교좌표 방정식을 구하고, 이심률과 두 초점을 구하여라.

풀이. $r = 3/(1 + \tfrac{1}{2}\cos\theta)$이므로 식 (5.12)에서 $e = 1/2$, $\ell = 3$인 타원이다. 직접 변환하면 $2r + r\cos\theta = 6$에서 $2r = 6 - x$이고, 제곱하여 $4(x^2 + y^2) = (6 - x)^2$, 곧 $3x^2 + 12x + 4y^2 = 36$이다. 완전제곱을 하면

$$\frac{(x + 2)^2}{16} + \frac{y^2}{12} = 1$$

이다. 이 타원 위에서는 $x \le 2$이므로 $6 - x > 0$이고, 제곱으로 새로 들어온 점은 없다. $a = 4$, $b = 2\sqrt{3}$, $c = 2$이므로 $e = c/a = 1/2$, $\ell = b^2/a = 3$으로 일치한다. 중심이 $(-2, 0)$이므로 초점은 $(0, 0)$과 $(-4, 0)$이고, 한 초점이 극에 놓인다.

5.9 제3권의 범위와 다음 읽기

제3권은 함수와 그래프의 언어(제1장), 좌표와 직선과 거리(제2장), 각도와 삼각함수(제3장), 삼각형과 원의 기하(제4장), 이차곡선과 극좌표(제5장)를 다루었다. 함수의 극한과 미분·적분은 제8권에서 이어지고, 회전과 이차형식의 일반적인 구조는 제7권 선형대수에서 이어진다. 기하의 공리적 기초, 비유클리드 기하, 사영기하의 상세한 전개는 이 총서의 현재 수록 범위에 들어 있지 않다.

기초 연습 문제와 추가 그림을 위한 자료로 OpenStax의 *Precalculus* 2e를 참고할 수 있다. 제3권의 본문은 그 자료와 독립적으로 작성한 한국어 원고이며, 추가 자료를 사용하는 경우에는 해당 판의 이용 조건을 따로 확인해야 한다.

제 4 권

증명 · 명제논리 · 술어논리

제4권은 수학적 증명을 쓰고 검토하는 데 필요한 논리의 언어와 증명의 기법을 정리한 권이다. 제1–3장은 진술과 양화사, 진리표에서 논리적 귀결까지의 명제논리, 직접증명 · 대우 · 귀류법과 반례의 설계를 다루고, 제4–5장은 술어논리의 구문과 의미, 자연연역과 시퀀트로 증명 자체를 형식적 대상으로 다룬다. 제6–9장은 귀납법과 재귀적 정의, 관계와 몫집합, 함수와 섬유, 부분순서와 Zorn 보조정리를 통해 이후 모든 권에서 쓰는 집합론적 도구를 갖춘다. 제10–12장은 유한 SAT의 정규형과 해결법, 유한 조건과 무한 조건의 차이를 보이는 콤팩트성, 그럴듯한 풀이의 오류를 찾는 증명 교정 실습으로 마무리한다.

제 1 장

수학적 진술과 양화사의 언어

개요 이 장은 수학적 문장을 정확히 읽고 쓰는 데 필요한 최소한의 논리 언어, 곧 **진술**(*statement*), 연결사, **전칭**(*universal*)·**존재**(*existential*) **양화사**(*quantifier*), 그리고 유일성의 표현을 정리한다. 기호화 자체를 목표로 삼지 않고, 무엇을 대상으로 말하는지, 어떤 조건을 이미 가정했는지, 무엇을 새로 주장하는지를 구별하는 것이 목표이다. 이후 해석학의 극한, 대수학의 준동형, 확률론의 독립성을 읽을 때 같은 문장 구조를 알아보는 데 이 장의 언어가 그대로 쓰인다. 선행 지식: 정수와 실수의 기본 연산, 등식과 부등식의 뜻. 이 권에서는 별도 표시가 없으면 고전논리를 사용하고, $\mathbb{N} = \{0, 1, 2, \dots\}$로 둔다.

수학에서 문장을 이해한다는 것은 기호를 읽는 일보다 넓다. 무엇을 대상으로 말하는지, 어떤 조건을 이미 가정했는지, 무엇을 새로 주장하는지를 구별해야 한다. 예를 들어 "제곱이 양수이다"라는 말만으로는 참과 거짓을 판단할 수 없다. 실수 x에 관한 말이라면 $x = 0$이라는 예외가 있고, 복소수라면 "양수"라는 표현에 쓰는 순서부터 정해야 한다. 수식은 그 수식이 놓인 문맥과 함께 읽는다.

1.1 진술, 열린 식, 수학적 문맥

정의 1.1 (진술과 열린 식) 문맥이 정해졌을 때 참 또는 거짓을 주장하는 문장을 **진술**이라 부른다. 변수의 값에 따라 참과 거짓이 달라지는 식은 **열린 식**(*open formula*)으로 다룬다. 예를 들어 실수 변수 x에 관한 $x^2 = 4$는 열린 식이고, $2^2 = 4$와 $\exists x \in \mathbb{R}\,(x^2 = 4)$는 진술이다.

"열린 식은 아무 의미가 없다"는 뜻이 아니다. 열린 식은 값을 대입하거나 변수를 양화하면 진술을 만든다. 또한 "x를 고정된 양의 실수라 하자"라고 선언한 문맥에서는 $x > 0$을 가정으로 사용할 수 있다. 이때 x가 모든 실수일 때도 양수라는 주장을 한 것은 아니다.

예제 1.2 다음 네 식은 같은 모양의 등호를 포함하지만 역할이 다르다.

$$x^2 = 1, \qquad (x-1)(x+1) = x^2 - 1, \qquad f(x) := x^2 - 1, \qquad x = 1.$$

첫 식은 미지수를 정하는 조건이다. 둘째 식은 모든 실수 x에 대해 성립하는 항등식이다. 셋째 식은 함수의 정의이며, 기호 $:=$는 오른쪽 식으로 왼쪽을 정한다는 뜻이다. 넷째 식은 앞의 방정식의 한 해를 지정할 수도 있고, 증명 중의 가정일 수도 있다. 기호의 모양만으로 역할을 결정할 수 없으므로 앞뒤의 선언을 읽어야 한다.

수학적 문맥을 적을 때는 대상의 종류를 먼저 밝힌다. "n은 정수이고 x는 실수이다"라는 선언은 $n \mid x$ 같은 식이 정수 나눗셈의 약수 관계(제1권 제2장)로는 허용되지 않음을 알려 준다. 정의역이 없는 함수를 말하거나, 서로 다른 공간의 원소를 더하는 오류도 같은 종류이다. 계산을 시작하기 전에 각 기호의 역할을 확인하면 많은 오류를 피할 수 있다.

주의 ("명제"라는 말의 두 쓰임). 이 권에서는 "명제"라는 말을 논리적으로 참과 거짓을 논하는 진술에도 쓰고, 증명할 만한 수학적 결과의 이름에도 쓴다. "명제논리의 명제 변수"와 "다음 명제를 증명한다"는 표현은 문맥으로 구별한다. 참인지 아직 모르는 진술도 진술이며, 참인 것만을 **명제**라고 부르는 것은 아니다.

1.2 연결사와 조건문의 방향

진술 P, Q에 대해 $\neg P$는 부정, $P \wedge Q$는 **논리곱**(*conjunction*), $P \vee Q$는 **논리합**(*disjunction*)을 나타낸다. 이때 $P \vee Q$는 둘 중 적어도 하나가 참이라는 뜻이므로 둘 다 참인 경우를 포함한다. 정확히 하나만 참이라는 배타적 논리합은

$$(P \vee Q) \wedge \neg(P \wedge Q)$$

로 따로 쓴다. 일상 언어의 "또는"이 어느 뜻인지 모호할 때는 문장을 풀어 쓰는 편이 낫다.

조건문(*conditional*) $P \to Q$는 P가 참이고 Q가 거짓인 경우에만 거짓이다. 이를 "P이면 Q이다"라고 읽는다. 조건문은 원인과 결과의 시간 순서를 정의하지 않는다. "n이 4의 배수이면 n은 짝수이다"는 수의 성질 사이의 포함 관계를 표현한다.

> **정의 1.3 (충분조건과 필요조건)** $P \to Q$가 성립할 때 P를 Q의 **충분조건**(*sufficient condition*), Q를 P의 **필요조건**(*necessary condition*)이라 한다. 두 방향 $P \to Q$와 $Q \to P$가 모두 성립하면 P와 Q는 **동치**(*equivalent*)이고 $P \leftrightarrow Q$로 쓴다.

> **예제 1.4** 정수 n에 대해 "n이 4의 배수"는 "n이 짝수"의 충분조건이다. 짝수 6은 4의 배수가 아니므로 충분조건을 필요조건으로 바꾸면 틀린다. 반면 "n이 짝수"와 "n^2이 짝수"는 동치이다. 뒤의 동치를 증명하려면 두 방향을 각각 다루어야 한다.

일상 문장의 "P일 때에만 Q"는 $Q \to P$이다. "신청한 사람만 입장할 수 있다"는 입장한 사람이 신청했다는 조건이지, 신청자 전원이 실제 입장했다는 주장이 아니다. "Q이기 위해서는 P가 필요하다"도 $Q \to P$이다. 언어를 기호로 바꿀 때는 먼저 조건을 만족하는 대상의 집합이 어느 쪽에 포함되는지 생각하면 방향을 확인할 수 있다.

흔한 오류 (후건 긍정). 결론을 보고 가정을 추론하는 것은 일반적으로 허용되지 않는다. $P \to Q$와 Q로부터 P를 얻는 추론은 **후건 긍정의 오류**(*affirming the consequent*)이다. 정수 6이 짝수라는 사실은 6이 4의 배수임을 보장하지 않는다.

1.3 전칭과 존재: 대상을 고르는 권한

역사 (양화사 기호의 역사). 문장 속의 "모든"과 "어떤"을 엄밀한 기호로 처음 다룬 것은 1879년 Gottlob Frege의 *Begriffsschrift*이다. 현재 쓰는 존재 양화사 기호 ∃는 1897년 Giuseppe Peano가 도입하였고, 전칭 양화사 기호 ∀는 1935년 Gerhard Gentzen이 이를 본떠 도입하였다.

> **정의 1.5 (전칭 양화사와 존재 양화사)** 대상들의 집합 D와 성질 $P(x)$에 대해
>
> $$\forall x \in D\, P(x) \qquad \text{및} \qquad \exists x \in D\, P(x)$$

는 각각 D의 모든 원소가 P를 만족한다는 뜻과, 적어도 한 원소가 P를 만족한다는 뜻이다. 존재를 확인해 주는 원소를 **증인**(*witness*)이라고 부른다.

전칭 명제를 증명할 때는 특별한 성질을 갖지 않는 임의의 원소를 고른다. x를 임의로 잡았다는 말은 아무 이유 없이 $x = 0$으로 바꾸어도 된다는 뜻이 아니다. 오히려 x가 D에 속한다는 정보 이외의 특수한 성질을 사용하지 않겠다는 약속이다.

존재 명제를 증명할 때는 적절한 증인을 선택해 성질을 확인하면 된다. 실수의 명제 $\exists x\,(x^2 = x)$에는 $x = 0$도 $x = 1$도 증인이다. 증인이 여러 개일 수 있으므로 존재를 증명한 것만으로 유일성을 얻지는 못한다.

예제 1.6

$$\forall x \in \mathbb{R}\, \exists y \in \mathbb{R}\, (y > x)$$

를 증명하자. 임의의 x가 주어지면 $y = x + 1$로 둔다. 실수 1이 양수이므로 $x + 1 > x$이다. 선택한 y는 앞서 주어진 x에 의존해도 된다. 이 증명은 어떤 하나의 y가 모든 x보다 크다는 말은 하지 않는다.

반대로

$$\exists y \in \mathbb{R}\, \forall x \in \mathbb{R}\, (y > x)$$

는 거짓이다. 그런 y가 있다면 전칭 문장에서 $x = y$를 대입하여 $y > y$를 얻기 때문이다. 양화사의 순서를 바꾸면 대상을 고르는 순서가 바뀐다. 앞에서 고른 증인은 뒤에 등장하는 임의의 변수에 의존할 수 없다.

명제 1.7 D, E를 집합, $R(x, y)$를 관계라 하자. 다음 함의는 항상 성립한다.

$$\big(\exists y \in E\, \forall x \in D\, R(x, y)\big) \;\longrightarrow\; \big(\forall x \in D\, \exists y \in E\, R(x, y)\big). \tag{1.1}$$

역방향은 일반적으로 성립하지 않는다.

증명. 왼쪽이 참이면 모든 x에 대해 쓸 수 있는 하나의 증인 $y_0 \in E$가 있다. 임의의 $x \in D$에 대해 같은 y_0를 증인으로 선택하면 오른쪽이 성립한다. 역방향의 반례는 $D = E = \mathbb{R}$, $R(x, y)$를 $y > x$로 둔 앞의 예이다. □

같은 종류의 양화사는 서로 바꿀 수 있다. 예를 들어 $\forall x \forall y\, R(x, y)$와 $\forall y \forall x\, R(x, y)$는 같은 뜻이다. 존재 양화사 두 개도 서로 바꿀 수 있다. 그러나 전칭과 존재가 섞이면 일반적으로 바꿀 수 없다. 이 차이는 균등수렴과 점별수렴처럼 더 높은 수준의 수학에서도 그대로 나타난다(제10권 제2장).

1.4 범위 제한, 빈 집합, 문장 부정

범위가 제한된 양화는 보통 다음의 약속으로 해석한다.

$$\forall x \in A\, P(x) \quad \text{는} \quad \forall x\, (x \in A \to P(x)), \tag{1.2}$$

$$\exists x \in A\, P(x) \quad \text{는} \quad \exists x\, (x \in A \wedge P(x)). \tag{1.3}$$

전칭에서 조건문을 쓰고 존재에서 논리곱을 쓰는 이유가 중요하다. A 밖의 원소는 전칭 주장을 위반하지 않아야 하므로 조건문을 쓴다. 존재의 증인은 실제로 A 안에 있어야 하므로 논리곱을 쓴다.

예제 1.8 “모든 양의 실수의 제곱은 양수”는

$$\forall x \in \mathbb{R}\,(x > 0 \to x^2 > 0)$$

이다. 이를 $\forall x \in \mathbb{R}\,(x > 0 \land x^2 > 0)$로 바꾸면 모든 실수가 양수라는 잘못된 주장까지 포함한다. “양수인 해가 있다”를 $\exists x \in \mathbb{R}\,(x > 0 \to f(x) = 0)$으로 쓰는 것도 틀리다. $x = 0$이면 앞부분이 거짓이므로 함수에 해가 없어도 이 조건문은 참이 될 수 있다.

명제 1.9 (양화사의 드 모르간 법칙) 고전 논리에서 다음 동치가 성립한다.

$$\neg\forall x \in D\, P(x) \leftrightarrow \exists x \in D\, \neg P(x), \tag{1.4}$$

$$\neg\exists x \in D\, P(x) \leftrightarrow \forall x \in D\, \neg P(x). \tag{1.5}$$

증명. 첫 동치에서 “모든 원소가 만족한다”가 거짓이라는 것은 만족하지 않는 원소가 적어도 하나 있다는 뜻이다. 둘째 동치에서 만족하는 원소가 하나도 없다는 것은 어느 원소를 골라도 만족하지 않는다는 뜻이다. 이 설명은 뒤에서 정의할 고전적 만족 관계의 양화사 절을 직접 풀어 쓴 것이다. □

부정은 문장 전체에 적용한 뒤 한 단계씩 안으로 이동시킨다. 예를 들어

$$\neg\big[\forall x \in \mathbb{R}\,\exists y \in \mathbb{R}\,(x + y = 0)\big] \leftrightarrow \exists x \in \mathbb{R}\,\forall y \in \mathbb{R}\,(x + y \neq 0).$$

이때 등호만 부등호로 바꾸고 양화사는 그대로 두면 다른 문장이 된다.

빈 집합에서는 $\forall x \in \varnothing\, P(x)$가 참이고 $\exists x \in \varnothing\, P(x)$는 거짓이다. 첫 문장을 위반하는 원소가 전혀 없기 때문이다. 이 현상을 **공허한 참**(*vacuous truth*)이라고 부른다. 공집합의 모든 원소가 양수라는 말과 공집합에 양수가 있다는 말은 모순되지 않는다. 전자는 참이고 후자는 거짓이다.

1.5 유일성, 함수의 성질, 의존 관계

정의 1.10 (유일한 존재) $P(x)$를 만족하는 원소가 정확히 하나 있다는 주장은

$$\exists! x \in D\, P(x) \quad :\Longleftrightarrow \quad \exists x \in D\,\big(P(x) \land \forall y \in D\,(P(y) \to y = x)\big) \tag{1.6}$$

로 정의한다.

유일성(*uniqueness*) 부분만 따로 쓰면

$$\forall x, y \in D\,\big((P(x) \land P(y)) \to x = y\big)$$

이다. 이것은 해가 전혀 없을 때도 참이다. 따라서 “해가 있다면 하나뿐”과 “해가 정확히 하나 있다”를 구별해야 한다.

예제 1.11 방정식 $ax = b$를 실수에서 생각하자. $a \neq 0$이면 $x = b/a$가 해이고, 두 해 x, y에 대해 $ax = ay$에서 $x = y$이므로 해가 유일하다. $a = 0, b \neq 0$이면 해가 없고, $a = b = 0$이면 모든 실수가 해이다. "일차방정식의 해는 유일하다"에는 최고차 계수 $a \neq 0$이라는 가정이 숨어 있다.

함수 $f : A \to B$의 단사성과 전사성(제3권 제1장)은 양화사의 좋은 연습 대상이다.

$$f\text{가 단사} \iff \forall x, y \in A\,(f(x) = f(y) \to x = y), \tag{1.7}$$

$$f\text{가 전사} \iff \forall b \in B\,\exists a \in A\,(f(a) = b). \tag{1.8}$$

단사의 부정은 서로 다른 두 입력이 같은 값을 갖는다는 것이고, 전사의 부정은 도달하지 못하는 출력이 있다는 것이다.

$$\neg\mathrm{Inj}(f) \iff \exists x, y \in A\,(x \neq y \wedge f(x) = f(y)), \qquad \neg\mathrm{Surj}(f) \iff \exists b \in B\,\forall a \in A\,(f(a) \neq b).$$

여기서 공역 B는 부수적인 정보가 아니다. $f(x) = x^2$를 $\mathbb{R} \to \mathbb{R}$로 보면 전사가 아니지만, 같은 대응을 $\mathbb{R} \to [0, \infty)$로 보면 전사이다.

1.6 연습문제와 해설

연습문제 1.12 정수 n에 대한 "n이 6의 배수일 때에만 n이 3의 배수이다"를 조건문으로 쓰고 참인지 판정하라.

풀이. 문장 그대로 쓰면 $3 \mid n \to 6 \mid n$이다. $n = 3$이 반례이므로 거짓이다. 참인 문장은 "n이 6의 배수이면 n이 3의 배수이다"이고, 이는 $6 \mid n \to 3 \mid n$이다. 일상 표현이 의도와 다르게 읽힐 수 있으므로 필요한 경우 조건문의 두 절을 명시한다.

연습문제 1.13 다음 문장의 참과 거짓을 판정하고, 거짓이면 부정을 써라.

$$\text{(가) } \forall n \in \mathbb{Z}\,\exists m \in \mathbb{Z}\,(m > n), \qquad \text{(나) } \exists m \in \mathbb{Z}\,\forall n \in \mathbb{Z}\,(m > n).$$

풀이. (가)는 $m = n + 1$을 택하면 참이다. (나)는 $n = m$을 대입하면 모순이므로 거짓이다. (나)의 부정은 $\forall m \in \mathbb{Z}\,\exists n \in \mathbb{Z}\,(m \leq n)$이며, $n = m$이 증인이다. 원문에서 $>$를 부정했으므로 $\leq$가 나타난다.

연습문제 1.14 실수 수열 (a_n)과 실수 L에 관한 다음 진술의 부정을 정확히 써라.

$$\forall \varepsilon > 0\,\exists N \in \mathbb{N}\,\forall n \in \mathbb{N}\,(n \geq N \to |a_n - L| < \varepsilon).$$

풀이. 부정은

$$\exists \varepsilon > 0\,\forall N \in \mathbb{N}\,\exists n \in \mathbb{N}\,(n \geq N \wedge |a_n - L| \geq \varepsilon)$$

이다. 조건문 $A \to B$의 부정이 $A \wedge \neg B$라는 점을 사용했다. 단 "충분히 큰 어떤 n에서 오차가 크다"는 표현은 N을 아무리 크게 잡아도 다시 반례가 존재한다는 뜻을 놓치므로 부족하다.

연습문제 1.15 집합 D에 대해 $\forall x \in D\,P(x)$로부터 $\exists x \in D\,P(x)$를 추론하려면 어떤 추가 가정이 필요한가?

풀이. $D \neq \varnothing$가 필요하다. 이때 $d \in D$를 하나 잡으면 전칭 명제로부터 $P(d)$를 얻고 존재를 결론낸다. $D = \varnothing$이면 전칭 명제는 참이지만 존재 명제는 거짓이다. 통상 일차논리의 전체 정의역은 비어 있지 않게 정하지만, 그 안에서 조건으로 잘라 낸 집합 D는 비어 있을 수 있다.

> **연습문제 1.16** “모든 사람은 누군가를 신뢰한다”와 “누군가를 모든 사람이 신뢰한다”를 구별하라. 두 번째가 거짓이고 첫 번째가 참인 유한 예를 만들라.

풀이. 관계 $T(x,y)$를 x가 y를 신뢰함으로 두면 각각 $\forall x \exists y\, T(x,y)$와 $\exists y \forall x\, T(x,y)$이다. 사람이 두 명 a, b이고 각자가 자기 자신만 신뢰한다고 하자. 그러면 각 사람에게 증인이 있으나 두 사람이 공통으로 신뢰하는 한 사람은 없다. 반례의 정의역과 관계 전체를 명시했으므로 모호한 사례가 아니다.

다음 장(제4권 제2장)에서는 이러한 문장의 연결사 구조를 진리값으로 계산한다. 이후 술어논리(제4권 제4장)에서는 대상과 양화사의 의미를 별도의 구조로 엄밀히 정의한다.

제 2 장

명제논리: 진리표에서 논리적 귀결까지

개요 **명제논리**(*propositional logic*)는 문장의 내부 대상 구조를 제쳐 두고, 문장들이 부정·논리곱·논리합·조건문·쌍조건문 같은 연결사로 결합되는 방식만으로 타당한 추론을 분석하는 논리 체계이다. 이 장은 논리식의 구문을 재귀적으로 정의하고, 각 논리식에 참·거짓의 값을 주는 평가와 진리표를 도입한 뒤, 타당성·충족가능성·논리적 귀결을 정의한다. 이어서 모든 논리식이 논리합 정규형(DNF)과 논리곱 정규형(CNF)으로 바꿀 수 있음을 증명하고, 절 형태의 식에서 모순을 기계적으로 확인하는 해결 규칙을 다룬다. "7은 소수이다"와 "비가 온다"는 내용이 다르지만 각각을 명제 변수에 대응시키면 같은 논리 형식을 가질 수 있다는 점이 이 장의 추상화가 의도하는 것이다. 이 추상화는 내용상의 진리를 발견하는 방법이 아니라, 내용이 무엇이든 보존되는 추론의 틀을 찾는 방법이다. 선행 지식: 제4권 제1장의 수학적 진술과 연결사. 이 장의 의미론은 참과 거짓 두 진리값만을 쓰는 고전 명제논리이다.

2.1 구문: 어떤 문자열이 식인가

정의 2.1 (논리식) **명제 변수**(*propositional variable*) $p_0, p_1, p_2, \dots$ 를 정한다. **논리식**(*well-formed formula*)은 다음 규칙으로 유한 번 구성되는 식이다.

(1) 모든 명제 변수와 상수 $\bot, \top$는 논리식이다.

(2) φ가 논리식이면 $\neg\varphi$도 논리식이다.

(3) φ, ψ가 논리식이면 $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$, $(\varphi \to \psi)$, $(\varphi \leftrightarrow \psi)$도 논리식이다.

이 규칙으로 얻지 않은 문자열은 논리식으로 인정하지 않는다. $\neg$를 **부정**, $\wedge$를 **논리곱**, $\vee$를 **논리합**, $\to$를 **조건문**, $\leftrightarrow$를 **쌍조건문**이라 하고, 이들을 통틀어 **연결사**(*connective*)라 한다.

괄호는 단순한 장식이 아니라 식의 구조를 결정한다. $p \vee (q \wedge r)$와 $(p \vee q) \wedge r$는 다른 식이다. 일상적인 표기에서는 $\neg, \wedge, \vee, \to, \leftrightarrow$ 순서로 결합력이 약해지는 약속을 쓰기도 하지만, 혼동할 수 있는 곳에서는 괄호를 남겨 둔다. 특히 조건문을 연달아 쓸 때는 결합 방향을 명시해야 한다. 연습문제 2.17는 괄호를 생략했을 때 결합 방향이 바뀌면 값도 달라질 수 있음을 보인다.

예제 2.2 $\neg(p \wedge q) \to r$의 가장 바깥 연결사는 $\to$이다. 왼쪽 부분식은 $\neg(p \wedge q)$, 오른쪽 부분식은 r이다. 왼쪽 식의 가장 바깥 연결사는 $\neg$이고 그 내부는 $p \wedge q$이다. 따라서 계산 순서는 p, q의 값, 그 논리곱, 논리곱의 부정, 마지막 조건문의 순서로 정해진다.

정의 2.3 (논리식의 복잡도) 논리식의 **복잡도** c를

$$c(p_i) = c(\bot) = c(\top) = 0, \qquad c(\neg\varphi) = c(\varphi) + 1, \qquad c(\varphi \circ \psi) = c(\varphi) + c(\psi) + 1 \tag{2.1}$$

로 정의한다. 여기서 $\circ$는 $\wedge, \vee, \to, \leftrightarrow$ 중 하나의 이항 연결사이다.

식 (2.1)에서 각 부분식은 전체 식보다 복잡도가 작다. 따라서 복잡도가 작은 부분식에 대해 정의한 값을 조합하여 전체 식의 값을 정의할 수 있다. 이 방식이 **귀납적 정의**와 **구조적 귀납**의 출발점이며, 뒤의 정리 2.12 의 증명에서도 암묵적으로 쓰인다(진리표의 각 행은 복잡도와 무관하게 전체 식을 한 번에 평가하지만, 평가 자체가 부분식의 값을 먼저 정해 조합하는 절차이다).

2.2 평가와 진리표

정의 2.4 (평가) **평가**(*valuation*) v는 각 명제 변수에 0 또는 1을 지정하는 함수이다. 0은 거짓, 1은 참을 나타낸다. 평가는 다음 표에 따라 모든 논리식으로 유일하게 확장되며, $v(\bot) = 0$, $v(\top) = 1$로 둔다.

표 2.1 이항 연결사의 진리표

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \to q$	$p \leftrightarrow q$
1	1	0	1	1	1	1
1	0	0	0	1	0	0
0	1	1	0	1	1	0
0	0	1	0	0	1	1

조건문의 마지막 두 행이 낯설 수 있다. 조건문을 “전제가 참인 경우에 결론이 거짓인 반례가 없다”고 읽으면 자연스럽다. p가 거짓이면 그 평가는 반례가 아니므로 $p \to q$는 참이 된다. 이 정의를 인과관계나 관련성의 정도를 수치화한 것으로 해석해서는 안 된다.

예제 2.5 $(p \to q) \wedge (q \to p)$의 진리값은 p, q가 같은 값을 가질 때만 1이다. 따라서 이 식은 $p \leftrightarrow q$와 모든 평가에서 같은 값을 갖는다. 이 계산은 쌍조건문이 두 조건문의 논리곱이라는 설명을 진리표로 확인해 준다.

명제 변수가 n개이면 가능한 평가는 2^n개이다. 진리표는 유한한 식의 모든 경우를 빠짐없이 검사하는 방법이다. 다만 n이 커지면 행의 수가 지수적으로 늘어난다. “결정하는 절차가 있다”와 “큰 입력에서 빠르게 계산된다”는 서로 다른 주장이며, 이 구별은 정규형을 다루는 §2.4에서 다시 나온다.

2.3 타당성, 충족가능성, 논리적 귀결

정의 2.6 (타당성과 충족가능성) 논리식 φ가 모든 평가에서 참이면 **타당하다**(*valid*)고 하고 $\models \varphi$로 쓴다. 적어도 한 평가에서 참이면 **충족가능하다**(*satisfiable*)고 한다. 어떤 평가에서도 참이 아니면 **충족불가능하다**(*unsatisfiable*)고 한다. 두 식이 모든 평가에서 같은 값을 가지면 **논리적으로 동치**(*logically equivalent*)라 하고 $\varphi \equiv \psi$로 쓴다.

$\varphi \leftrightarrow \psi$는 논리식 안의 연결사로 만든 하나의 논리식이고, $\varphi \equiv \psi$는 두 식의 진리값 관계를 말하는 바깥 수준의 표기이다. 둘은 밀접하게 연결되어 있지만 문법적 역할이 다르다. 정의 2.1의

구문 규칙에서 $\equiv$는 메타언어의 기호이지 논리식을 구성하는 연결사가 아니다. 정확히

$$\varphi \equiv \psi \iff \models (\varphi \leftrightarrow \psi) \tag{2.2}$$

가 성립한다.

정의 2.7 (논리적 귀결) 논리식의 집합 Γ가 주어졌다고 하자. Γ의 모든 식을 참으로 만드는 평가가 φ도 참으로 만들 때 $\Gamma \models \varphi$라 쓰고, φ가 Γ의 **논리적 귀결**(*logical consequence*)이라고 한다. Γ를 모두 참으로 만들지만 φ를 거짓으로 만드는 평가를 이 귀결 주장에 대한 **반평가**(*countermodel*)라 한다.

명제 2.8 유한 전제 $\gamma_1, \dots, \gamma_n$에 대해

$$\{\gamma_1, \dots, \gamma_n\} \models \varphi \iff \models \big((\gamma_1 \wedge \cdots \wedge \gamma_n) \to \varphi\big). \tag{2.3}$$

전제가 없으면 왼쪽은 $\models \varphi$라는 뜻이다.

증명. 식 (2.3)의 오른쪽 조건문이 거짓이 되는 평가는, 모든 γ_i를 참으로 만들고 φ를 거짓으로 만드는 평가와 정확히 같다. 따라서 그러한 평가가 존재하지 않는다는 두 주장은 동치이다. □

예제 2.9 $\{p \to q,\ p\} \models q$이다. 두 전제가 모두 참이면 $p = 1$이고 $p \to q = 1$이어야 하므로 $q = 1$이다. 반면 $\{p \to q,\ q\} \not\models p$이다. $p = 0, q = 1$이 두 전제를 참으로, 결론을 거짓으로 만드는 반평가이다.

명제 2.10 $\Gamma \models \varphi$일 필요충분조건은 $\Gamma \cup \{\neg\varphi\}$가 충족불가능하다는 것이다.

증명. $\Gamma \cup \{\neg\varphi\}$를 만족하는 평가는 Γ를 만족하면서 φ를 거짓으로 만드는 평가이다. 이것은 정의 2.7 의 반평가와 정확히 같은 대상이다. 따라서 $\Gamma \cup \{\neg\varphi\}$를 만족하는 평가가 하나도 없다는 것과 $\Gamma \models \varphi$는 동치이다. □

명제 2.10은 타당성 문제를 반례 탐색 문제로 바꾼다. 결론을 부정하여 전제에 더한 뒤, 모든 조건을 함께 만족하는 평가가 있는지 찾으면 된다. 반례를 하나 찾으면 귀결은 거짓이다. 반면 반례 탐색이 실패했다는 보고만으로는 충분하지 않고, 모든 경우가 배제되었다는 근거가 있어야 한다. §2.5의 해결 규칙은 바로 이 "모든 경우가 배제되었다"는 근거를 짧은 절차로 제시하는 방법이다.

2.4 동치 변형과 정규형

다음 법칙은 각 변수의 모든 진리값을 표 2.1에 대입하여 확인할 수 있다.

$$\neg\neg p \equiv p, \tag{2.4}$$

$$p \to q \equiv \neg p \vee q, \tag{2.5}$$

$$\neg(p \wedge q) \equiv \neg p \vee \neg q, \tag{2.6}$$

$$\neg(p \vee q) \equiv \neg p \wedge \neg q, \tag{2.7}$$

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r), \tag{2.8}$$

$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r). \tag{2.9}$$

식 (2.6), (2.7)는 드모르간 법칙(*De Morgan's laws*)이라 하며, 부정이 안으로 들어갈 때 연결사가 바뀐다는 뜻이다. 식 (2.8), (2.9)는 분배법칙이다. 산술의 분배법칙과 비슷하지만, 논리에서는 논리곱이 논리합에 분배되고 논리합도 논리곱에 분배된다는 두 방향의 법칙이 모두 성립한다는 점이 다르다.

정의 2.11 (리터럴과 정규형) 변수 또는 변수의 부정을 **리터럴**(*literal*)이라 한다. 리터럴들의 논리곱을 여러 개 논리합으로 연결한 식을 **논리합 정규형**(DNF, *disjunctive normal form*), 리터럴들의 논리합을 여러 개 논리곱으로 연결한 식을 **논리곱 정규형**(CNF, *conjunctive normal form*)이라 한다. CNF에서 논리합으로만 이루어진 각 부분을 **절**(*clause*)이라 한다.

정리 2.12 (정규형의 존재) 유한 개의 명제 변수에 의존하는 모든 논리식은 어떤 DNF 및 어떤 CNF와 논리적으로 동치이다. 항상 거짓인 경우와 항상 참인 경우에는 상수 $\bot, \top$를 그 정규형으로 허용한다.

증명. φ를 참으로 만드는 진리표의 각 행을 생각하자. 그 행에서 값이 1인 변수는 그대로, 값이 0인 변수는 부정하여 모두 논리곱으로 연결한다. 이 논리곱은 정확히 그 행에서만 참이다. φ가 참인 모든 행에 대해 이렇게 만든 논리곱을 논리합으로 연결하면, 그 결과는 φ와 같은 진리표를 갖는다. 참인 행이 하나도 없으면(φ가 항상 거짓이면) $\bot$를 쓴다. 이것이 DNF이다.

CNF는 거짓인 각 행을 정확히 배제하는 절을 만든다. 그 행에서 값이 0인 변수는 그대로, 값이 1인 변수는 부정하여 논리합으로 연결한다. 이 절은 그 행에서만 거짓이고 다른 모든 행에서는 참이다. φ가 거짓인 모든 행의 절을 논리곱으로 연결하면, 그 논리곱은 정확히 φ가 거짓인 행들을 배제하여 φ가 참인 행만 남긴다. 거짓인 행이 하나도 없으면 $\top$를 쓴다. □

예제 2.13 p와 q가 서로 다른 값을 가질 때만 참인 식은 DNF로

$$(p \wedge \neg q) \vee (\neg p \wedge q)$$

이고, CNF로 $(p \vee q) \wedge (\neg p \vee \neg q)$이다. 전자는 참인 두 행($p=1, q=0$과 $p=0, q=1$)을 직접 열거하고, 후자는 둘 다 거짓인 행과 둘 다 참인 행을 배제한다.

정규형이 존재한다는 사실은 변환 후의 길이가 짧다는 뜻이 아니다. 정리 2.12의 증명을 그대로 따르면 최대 2^n개의 행에 해당하는 항이나 절을 만들어야 한다. 따라서 실제 계산에서는 식의 구조를 보존하는 다른 표현이나 보조 변수를 도입하는 변환(이른바 **Tseitin 변환**)을 활용할 수 있다. 보조 변수를 넣은 변환이 원래 변수에 대해 논리적으로 동치인지, 아니면 단지 충족가능성만 보존하는지는 구별해야 한다. 뒤의 §2.5의 해결 규칙은 CNF, 곧 절의 모음에 대해 작동하므로 임의의 식을 해결 규칙으로 다루려면 먼저 CNF로(또는 충족가능성을 보존하는 절 형태로) 바꾸어야 한다.

2.5 해결 규칙과 모순의 인증

절 $C \vee p$와 $D \vee \neg p$로부터 절 $C \vee D$를 얻는 규칙을 **해결 규칙**(*resolution rule*)이라 한다. 여기서 C, D는 다른 리터럴들의 논리합이며 비어 있을 수도 있다. 리터럴이 하나도 없는 **빈 절**은 $\bot$를 뜻한다.

명제 2.14 (해결 규칙의 건전성) 해결 규칙은 건전하다. 즉,

$$\{C \vee p,\ D \vee \neg p\} \models C \vee D.$$

증명. 전제 두 절이 모두 참이라고 하자. p가 참이면 $\neg p$가 거짓이므로 둘째 절에서 D가 참이어야 한다. p가 거짓이면 첫째 절에서 C가 참이어야 한다. 어느 경우든 $C \vee D$는 참이다. □

예제 2.15 절 집합

$$\{\, p \vee q,\ \neg p \vee r,\ \neg q,\ \neg r \,\}$$

은 충족불가능하다. 첫째 절과 $\neg q$를 해결하면 p를 얻는다. p와 $\neg p \vee r$를 해결하면 r을 얻는다. r과 $\neg r$을 해결하면 빈 절을 얻는다. 명제 2.14에 의해 모든 단계가 전제의 논리적 귀결을 보존하므로, 전제를 만족하는 평가가 있다면 마지막의 거짓인 빈 절도 만족해야 한다는 모순에 이른다. 따라서 그런 평가는 없다.

이 예는 "모순인 것 같다"는 판단을 검산 가능한 짧은 인증으로 바꾼다. 다만 어떤 해결 순서를 시도했는데 빈 절을 얻지 못했다는 것만으로 절 집합이 충족가능하다고 결론 내릴 수는 없다. 모든 해결 가능한 쌍을 체계적으로 시도하는 완전한 탐색 절차를 정하고, 그 절차가 빈 절을 못 찾으면 실제로 충족가능함을 보장한다는 사실(해결의 완전성)은 별도로 증명해야 하는 성질이다.

2.6 연습문제와 해설

연습문제 2.16 $p \to (q \to p)$가 타당함을 진리표의 여덟 행을 쓰지 않고 설명하라.

풀이. $p = 0$이면 바깥 조건문은 전제가 거짓이므로 참이다. $p = 1$이면 안쪽 $q \to p$의 결론이 참이므로 안쪽 조건문이 참이고, 따라서 바깥 조건문도 참이다. q의 두 값을 따로 적을 필요 없이 두 경우에 모두 포함했다. 빠뜨린 평가가 없으므로 타당성이 증명되었다.

연습문제 2.17 $(p \to q) \to r$와 $p \to (q \to r)$가 동치인지 판정하라.

풀이. 동치가 아니다. $p = 0, q = 0, r = 0$이면 $p \to q = 1$이므로 첫 식은 $1 \to 0 = 0$이다. 둘째 식은 바깥 전제가 $p = 0$이므로 참이다. 이 예는 연속한 조건문에서 괄호를 생략할 때 결합 방향을 정해야 하는 이유를 보여 준다.

연습문제 2.18 $\{p \vee q,\ p \to r,\ q \to r\} \models r$임을 증명하라.

풀이. 첫 전제가 참이면 p 또는 q가 참이다. p가 참인 경우 둘째 전제에서 r을 얻고, q가 참인 경우 셋째 전제에서 r을 얻는다. 두 경우를 모두 처리했으므로 r은 어느 경우에도 참이다. $p \vee q$에서 곧바로 p를 선택한 것이 아니라, 어느 쪽이 참이어도 같은 결론이 나온다는 점이 핵심이다.

연습문제 2.19 $\neg(p \to q) \vee r$를 CNF로 바꾸라.

풀이. 식 (2.5)에 의해 먼저 $\neg(p \to q) \equiv p \wedge \neg q$이다. 분배법칙 (2.9)로

$$(p \wedge \neg q) \vee r \equiv (p \vee r) \wedge (\neg q \vee r)$$

를 얻는다. 각 괄호는 리터럴들의 논리합이고 전체는 그 논리곱이므로 이것이 CNF이다.

연습문제 2.20 충족불가능한 전제 집합 Γ에서는 임의의 φ에 대해 $\Gamma \models \varphi$임을 설명하라. 이것이 φ 자체가 타당하다는 뜻인지도 답하라.

풀이. Γ의 모든 전제를 참으로 만드는 평가가 없으므로, 전제를 참으로 만들고 결론을 거짓으로 만드는 반평가도 없다. 따라서 정의 2.7에 의해 $\Gamma \models \varphi$가 성립한다. 하지만 φ 자체는 타당할 필요가 없다. 예를 들어 $\{p, \neg p\} \models q$이지만 $q = 0$인 평가가 있으므로 $\not\models q$이다. 전제의 모순은 그 자체로 유용한 사실을 보장하는 출발점이 아니다.

연습문제 2.21 절 집합 $\{p \vee q,\ \neg p \vee q,\ p \vee \neg q,\ \neg p \vee \neg q\}$에서 해결 규칙으로 빈 절을 유도하라.

풀이. 앞의 두 절에서 p를 해결하면 $q \vee q$, 곧 q가 된다. 뒤의 두 절에서 p를 해결하면 $\neg q \vee \neg q$, 곧 $\neg q$가 된다. 두 결과 $q, \neg q$를 해결하면 빈 절이다. 처음 네 절은 진리표의 네 행을 각각 하나씩 배제하므로, 모든 행이 배제되어 직접 보아도 충족불가능함을 알 수 있다. 해결 규칙을 이용한 풀이와 직접 관찰한 풀이가 같은 결론을 독립적으로 확인해 준다.

진리표는 문장 형식의 타당성을 유한한 절차로 검사한다. 다음 장(제4권 제3장)에서는 실제 수학적 대상의 정의와 성질을 사용하여 증명을 구성하고, 그 안에서 이 장에서 다룬 어떤 논리 형식이 실제로 쓰이는지 확인한다.

역사. 진리표를 체계적으로 조직하는 방법은 1920년대 초 Emil Post와 Ludwig Wittgenstein이 독립적으로 제시하였다. 이들의 작업은 명제논리의 식이 유한 번의 기계적 검사로 타당성을 판정할 수 있다는 사실, 곧 명제논리의 결정가능성을 보여 주는 초기 사례가 되었다.

제 3 장

증명 방법과 반례의 설계

개요 이 장은 수학적 증명을 구성하는 표준 기법인 직접증명, 대우, 귀류법, 경우분석, 동치의 양방향 증명, 존재·유일성·잘 정의됨의 논증, 집합과 함수에 관한 증명을 차례로 다루고, 반례의 설계와 증명을 스스로 검산하는 절차로 마무리한다. 각 기법은 증명할 명제의 가장 바깥 논리 구조(전칭, 조건문, 논리곱, 존재)에 대응하는 표준적인 절차로 제시된다. 선행 지식: 제4권 제1장의 조건문과 전칭·존재 양화사, 제4권 제2장의 명제논리의 기본 법칙. 이 장에서 정수의 나눗셈 $a \mid b$는 어떤 $k \in \mathbb{Z}$에 대해 $b = ak$임을 뜻한다 (제1권 제2장).

좋은 증명은 결론이 참이라는 확신을 전달하는 데 그치지 않는다. 어떤 가정이 어느 단계에서 필요한지 추적할 수 있어야 하고, 같은 생각을 다른 문제에 적용할 수 있게 해야 한다. 한편 모든 계산을 가장 작은 논리 규칙으로 해체할 필요는 없다. 독자에게 이미 알려진 결과는 명확히 인용하고, 새로 넘어야 하는 핵심 단계를 자세히 설명하는 것이 효율적이다.

증명할 식을 보았을 때 먼저 문장의 가장 바깥 구조를 확인한다. 전칭이면 임의의 대상을 잡고, 조건문이면 가정을 받아들이고, 논리곱이면 두 주장을 각각 보이며, 존재이면 증인을 찾는다. 이 원칙은 증명의 모든 창의적 아이디어를 대신하지는 않지만, 무엇을 얻어야 하는지와 현재 무엇을 사용할 수 있는지를 정리해 준다.

3.1 직접증명과 정의의 사용

명제 3.1 정수 a, b, c에 대해 $a \mid b$이고 $b \mid c$이면 $a \mid c$이다.

증명. 가정에서 정수 k, ℓ이 존재하여 $b = ak$, $c = b\ell$이다. 따라서 $c = (ak)\ell = a(k\ell)$이고 $k\ell \in \mathbb{Z}$이다. 정수 나눗셈의 정의에 따라 $a \mid c$이다. □

이 증명은 a, b가 0이 아니라고 가정하지 않았다. 나눗셈 기호 $a \mid b$를 분수 b/a로 해석하지 않고 존재식 $b = ak$로 풀었기 때문이다. 정의에서 허용한 경우는 증명에서도 그대로 유지된다.

명제 3.2 실수 x, y가 $0 \le x \le y$를 만족하면 $x^2 \le y^2$이다.

증명. $y^2 - x^2 = (y - x)(y + x)$이고, $y - x \ge 0$과 $y + x \ge 0$이므로 두 인수가 모두 음이 아니다. 음이 아닌 두 수의 곱은 음이 아니므로 $y^2 - x^2 \ge 0$, 즉 $x^2 \le y^2$이다. □

흔한 오류. $x \le y$라는 가정만으로는 제곱해도 순서가 보존된다고 말할 수 없다. $x = -2, y = -1$이면 $x \le y$이지만 $x^2 = 4 > 1 = y^2$이다. 명제 3.2에서 $x \ge 0$이라는 조건이 실제로 쓰였다. 식에 같은 연산을 적용할 때는 그 연산이 현재 범위에서 동치나 부등호의 방향을 보존하는지 먼저 확인해야 한다.

예제 3.3 (식의 변형과 논리 방향) 실수 방정식 $\sqrt{x + 2} = x$를 풀자. 제곱근의 값은 음이 아니므

> 로 모든 해는 $x \geq 0$을 만족한다. 양변을 제곱하면 $x+2 = x^2$, 즉
>
> $$(x-2)(x+1) = 0$$
>
> 이다. 후보는 $x = 2, -1$이고 $x \geq 0$에 맞는 것은 2만 남는다. 원식에 대입하면 $\sqrt{2+2} = 2$이므로 실제 해임을 확인한다. 제곱한 식만 풀고 $x = -1$까지 답에 넣는 것은, 제곱이 만드는 필요조건을 원식의 충분조건으로 오인한 오류이다.

등식의 연속된 계산에서는 각 등호가 참이어야 한다. 부등식이나 조건식의 연속 변형에서는 화살표가 한쪽 방향(함의)인지 양방향(동치)인지 표시해야 한다. 예제 3.3처럼 "원식이면 변형식"만 보장되는 단계가 있으면, 마지막에 후보를 원식에 대입하여 확인하는 절차가 반드시 필요하다.

3.2 대우와 귀류법

고전 논리에서 $P \to Q$는 $\neg Q \to \neg P$와 동치이다(식 (2.5)와 드모르간 법칙으로 확인된다). 후자를 원래 조건문의 **대우**(*contrapositive*)라 한다. 반면 $Q \to P$는 **역**(*converse*)이며, 원래 조건문과 일반적으로 동치가 아니다.

명제 3.4 정수 n의 제곱이 짝수이면 n은 짝수이다.

증명. 대우를 증명한다. n이 홀수이면 어떤 $k \in \mathbb{Z}$에 대해 $n = 2k+1$이다. 그러면

$$n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

이므로 n^2도 홀수이다. 따라서 n^2이 짝수인 경우 n은 홀수일 수 없고, 정수의 짝홀 분류에 의해 n은 짝수이다. □

대우가 편리한 경우는 결론의 부정이 구체적인 정보를 줄 때이다. 예를 들어 "단사이면 서로 다른 입력은 서로 다른 값을 갖는다"는 정의의 대우를 읽은 것이다. "어떤 성질이 없다"는 부정만으로 증명을 시작하면 다루기 어려운 문제에서, 반대 방향의 긍정적인 구조를 대신 활용할 수 있다.

증명 과정에서 결론을 부정하여 모순을 이끌어 내는 방법을 **귀류법**(*proof by contradiction*)이라 한다. 다음 정리는 귀류법의 표준 예이다.

정리 3.5 $\sqrt{2}$는 유리수가 아니다.

증명. 반대로 $\sqrt{2} = a/b$라고 하자. 여기서 a, b는 서로소인 양의 정수이고 $b \neq 0$이다. 양변을 제곱하면 $a^2 = 2b^2$이므로 a^2이 짝수이다. 명제 3.4에 의해 $a = 2k$인 정수 k가 존재한다. 대입하면 $4k^2 = 2b^2$, 즉 $b^2 = 2k^2$이므로 b도 짝수이다. a, b가 모두 2의 배수라는 것은 a, b를 서로소로 택했다는 가정과 모순된다. 따라서 처음의 유리수 가정이 거짓이다. □

이 증명에서 "서로소인 분수로 택한다"는 단계는 장식이 아니다. 단순히 a, b가 모두 짝수라는 사실만으로는 임의의 분수 표현과 모순되지 않는다. 모든 유리수를 기약분수로 고를 수 있다는 정수의 성질이 증명에서 실제로 사용되었다.

주의 (부정의 두 쓰임). P를 부정해서 모순을 얻는 방식과, P를 가정해서 모순을 얻어 $\neg P$를 증명하는 방식은 구별해야 한다. 후자는 부정의 기본 도입 규칙이다. 전자, 곧 $\neg\neg P$로부터 P를

얻는 단계에는 고전 논리의 이중부정 제거 원리가 쓰인다. 직관주의 논리처럼 이중부정 제거를 일반적으로 허용하지 않는 체계를 다룰 때는 이 차이를 다시 살펴야 한다.

3.3 경우분석과 동치의 두 방향

경우분석(*proof by cases*)은 가능한 경우들이 전체를 덮는다는 사실과, 각 경우에서 결론이 성립한다는 사실을 함께 요구한다. 서로 겹치는 경우를 쓰는 것은 논리적으로 문제가 없지만, 빠진 경우가 있어서는 안 된다.

명제 3.6 모든 정수 n에 대해 $n(n+1)$은 짝수이다.

증명. n이 짝수이면 어떤 $k \in \mathbb{Z}$에 대해 $n = 2k$이므로 $n(n+1) = 2k(n+1)$이다. n이 홀수이면 $n+1$이 짝수이므로 역시 곱은 짝수이다. 모든 정수는 짝수 또는 홀수이므로 두 경우가 전체를 덮는다. □

명제 3.7 실수 x, y에 대해 $|x+y| \le |x| + |y|$이다.

증명. $-|x| \le x \le |x|$이고 $-|y| \le y \le |y|$이므로 두 부등식을 변끼리 더하면

$$-(|x|+|y|) \le x+y \le |x|+|y|.$$

$t \ge 0$일 때 $-t \le z \le t$와 $|z| \le t$가 동치라는 절댓값의 성질을 적용하면 $|x+y| \le |x|+|y|$를 얻는다. □

이 명제는 x, y의 부호를 네 가지로 나누어도 증명할 수 있다. 그러나 모든 경우를 한 번에 다루는 부등식 $-|x| \le x \le |x|$를 쓰면 계산이 짧고 구조가 드러난다. 증명 방법을 선택하는 기준은 결과에 붙은 익숙한 이름이 아니라, 현재 가정에서 바로 얻을 수 있는 정보이다.

명제 3.8 실수 a, b에 대해 $a^2 = b^2$일 필요충분조건은 $a = b$ 또는 $a = -b$이다.

증명. 먼저 $a^2 = b^2$이면 $(a-b)(a+b) = 0$이다. 실수에서 두 수의 곱이 0이면 적어도 하나가 0이므로 $a = b$ 또는 $a = -b$이다. 반대로 $a = b$이면 제곱이 같고, $a = -b$이어도 $a^2 = (-b)^2 = b^2$이다. 두 방향이 모두 성립했다. □

동치의 한 방향만 증명하고 끝내는 실수는 흔하다. 두 방향의 난이도가 매우 다르면 쉬운 방향을 한 문장으로 적어도 되지만, 어느 방향을 처리했는지는 반드시 남겨야 한다. 서로 다른 조건 세 개 A, B, C의 동치를 보이려면, 서로 다른 두 조건 사이의 여섯 개의 함의를 모두 보이는 대신 $A \to B \to C \to A$라는 순환 하나만 증명해도 충분하다.

3.4 존재, 유일성, 잘 정의됨

존재를 보이는 가장 직접적인 방법은 대상을 만들고 그것이 원하는 성질을 만족함을 검사하는 것이다. 그러나 대상의 구체적인 수치나 닫힌 형태를 주지 않는 존재 증명도 있다. 중간값정리를 이용한 방정식의 해의 존재, 유한 집합에서의 최댓값의 존재가 그 예이다. 어느 경우든 사용한 정리의 가정을 확인해야 한다.

정리 3.9 (정수의 나눗셈 알고리즘) 정수 a와 양의 정수 b에 대해

$$a = bq + r, \qquad 0 \le r < b$$

를 만족하는 정수 q, r가 유일하게 존재한다.

증명. $S = \{a - bk : k \in \mathbb{Z},\ a - bk \ge 0\}$이라 하자. 충분히 작은 정수 k를 택하면 $a - bk \ge 0$이므로 S는 비어 있지 않다. 예를 들어 $k = -|a|$이면 $b \ge 1$이므로 $a - bk = a + b|a| \ge a + |a| \ge 0$이다. 자연수의 정렬성에 의해 S에는 최소 원소 r가 있다. 정의에 따라 $r = a - bq$인 정수 q가 존재한다. $r \ge b$이면 $r - b = a - b(q+1)$도 S의 원소이면서 r보다 작으므로 r의 최소성에 모순이다. 따라서 $0 \le r < b$이고 존재가 증명되었다.

다른 표현 $a = bq' + r'$, $0 \le r' < b$가 있다고 하자. 그러면 $b(q - q') = r' - r$이고 $|r' - r| < b$이다. $q - q'$가 0이 아닌 정수이면 $|b(q - q')| \ge b$이므로 모순이다. 따라서 $q = q'$이고, 그로부터 $r = r'$이다. □

존재와 유일성의 논리는 분리되어 있다. 정리 3.9의 증명에서 첫 부분은 정렬성에 의한 최소 원소를 택해 조건을 만족하는 해를 만들고, 둘째 부분은 조건을 만족하는 임의의 두 해를 비교하여 같음을 보인다. 정수 a가 음수여도 증명은 그대로 작동하며, $b > 0$이라는 조건은 나머지의 범위와 최소성 논증에 쓰인다.

정의 3.10 (잘 정의됨) 어떤 대상을 표현하는 방식이 여러 개일 때, 그 표현에 공식을 적용한 결과가 표현의 선택에 무관하면 그 공식은 **잘 정의되어**(*well-defined*) 있다고 말한다.

예제 3.11 법 $m \ge 1$을 고정한 정수의 합동류 $[a]$에서 $[a] + [b] = [a+b]$로 덧셈을 정의하려 한다. $a \equiv a' \pmod m$, $b \equiv b' \pmod m$이면 $m \mid (a-a')$와 $m \mid (b-b')$이므로 $m \mid \big((a+b)-(a'+b')\big)$이다. 따라서 $[a+b] = [a'+b']$여서 이 덧셈은 대표원의 선택에 무관하다. 즉 잘 정의되어 있다. 반면 $[a] \mapsto a$를 정수로 보내는 규칙은, 같은 합동류의 서로 다른 대표 a, a'가 서로 다른 정수를 주므로 잘 정의되지 않는다.

3.5 집합과 함수에 대한 증명

집합의 등식 $A = B$는 양방향 포함 $A \subseteq B$와 $B \subseteq A$로 증명할 수 있다. 또는 임의의 x에 대해 $x \in A \leftrightarrow x \in B$를 보일 수도 있다. 집합의 원소를 하나씩 확인하는 이 방법은 집합이 무한해도 그대로 적용된다. 여기서 "임의의 원소"는 특정한 원소 하나를 검사한다는 말과는 다르다.

명제 3.12 함수 $f : X \to Y$와 부분집합 $A, B \subseteq Y$에 대해

$$f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B).$$

여기서 $f^{-1}(A) = \{x \in X : f(x) \in A\}$는 역상이며, 역함수의 존재를 뜻하지 않는다.

증명. 임의의 $x \in X$에 대해

$$\begin{aligned} x \in f^{-1}(A \cap B) &\iff f(x) \in A \cap B \\ &\iff f(x) \in A \land f(x) \in B \end{aligned}$$

$$\iff x \in f^{-1}(A) \cap f^{-1}(B).$$

따라서 두 집합은 같은 원소를 가지므로 서로 같다. □

명제 3.13 함수 $f : X \to Y$, $g : Y \to Z$를 생각하자. 합성 $g \circ f$가 단사이면 f는 단사이다. 합성 $g \circ f$가 전사이면 g는 전사이다.

증명. 첫 주장에서는 $f(x_1) = f(x_2)$라 하자. 양변에 g를 적용하면 $(g \circ f)(x_1) = (g \circ f)(x_2)$이므로 합성의 단사성에 의해 $x_1 = x_2$이다.

둘째 주장에서는 임의의 $z \in Z$를 잡는다. 합성의 전사성으로 $(g \circ f)(x) = z$인 $x \in X$가 있다. $y = f(x) \in Y$를 택하면 $g(y) = z$이므로 g가 전사이다. □

첫 주장으로부터 g도 단사라고 결론 내릴 수는 없다. g는 $f(X)$ 밖에서 서로 다른 원소를 같은 값으로 보낼 수 있다. 예를 들어 $X = \{0\}$, $Y = \{0, 1\}$, $Z = \{0\}$에서 $f(0) = 0$, $g(0) = g(1) = 0$으로 두면 합성은 단사이지만 g는 단사가 아니다.

3.6 반례와 증명 검산

정의 3.14 (반례) 전칭 명제 "모든 x에 대해 $P(x)$이면 $Q(x)$이다"에 대한 **반례**(*counterexample*)는 $P(x)$를 만족하면서 $Q(x)$는 만족하지 않는 대상 x이다. 가정 P에서 제외된 대상을 가져오면 반례가 아니다. 존재 명제 "어떤 x에 대해 $R(x)$이다"를 반박하려면 증인 후보 하나가 R을 만족하지 않는다는 사실로는 부족하고, 가능한 모든 증인이 R을 만족하지 않음을 보여야 한다.

방법 (증명 검산의 순서). 다음 순서로 검산하면 증명의 약한 지점을 찾기 쉽다.

(1) 명제의 정의역과 예외를 확인한다.

(2) 각 단계가 앞의 가정에서 따라오는지, 나눗셈이나 제곱에서 허용 조건을 확인했는지 살핀다.

(3) 증인이 뒤에 나오는 임의의 변수에 몰래 의존하지 않는지, 증명하려는 명제를 중간에 다시 사용하지 않았는지(순환 논증이 아닌지) 확인한다.

예제 3.15 (숨은 0으로 나누기) $a = b \neq 0$에서 $a^2 = ab$를 얻고, 양변에서 b^2을 빼면 $(a-b)(a+b) = b(a-b)$이다. 여기서 $a-b$를 약분하면 $a+b = b$, 따라서 $2 = 1$이라는 잘못된 결론이 나온다. 문제는 $a - b = 0$이므로 약분이 허용되지 않는다는 것이다. 모순된 결론은 첫 가정이 틀렸다는 뜻이 아니라, 추론 단계 중 하나(여기서는 0에 의한 나눗셈)가 잘못되었을 수 있음을 뜻한다.

예제 3.16 (결론을 가정한 계산) 증명하려는 부등식에서 출발해 참인 식 $0 \le (x-y)^2$을 얻었다고 하자. 모든 변형이 양방향 동치라면 거꾸로 읽어 증명을 완성할 수 있다. 하지만 일부 단계가 한 방향 함의에 불과하다면, 이 계산은 "주장하면 참인 식이 따라온다"는 사실만 보인 것이다. 참인 결론을 얻었다는 이유만으로 출발점이 참이라고 결론 내릴 수 없다.

역사. $\sqrt{2}$의 무리수성(정리 3.5)을 귀류법으로 증명하는 방법은 고대 그리스의 산술에서 이미 알려져 있었고, Euclid의 『원론』 제10권에 비슷한 형태의 증명이 실려 있다. 이는 유리수가 아닌 수의 존재를 엄밀한 증명으로 확립한 가장 이른 예로 꼽힌다.

3.7 연습문제와 해설

연습문제 3.17 정수 a, b에 대해 a, b가 홀수이면 ab가 홀수임을 증명하라.

풀이. $a = 2k+1, b = 2\ell+1$인 정수 k, ℓ을 택하면

$$ab = 2(2k\ell + k + \ell) + 1.$$

괄호 안이 정수이므로 홀수의 정의를 만족한다. a, b가 양수라는 가정은 쓰이지 않았으므로 음의 홀수에도 성립한다.

연습문제 3.18 $a, b, c \in \mathbb{R}$일 때 $ab = ac \to b = c$가 항상 참인지 판정하고, 참이 되도록 가정을 보완하라.

풀이. $a = 0, b = 1, c = 2$가 반례이다. $a \neq 0$을 추가하면 $a(b-c) = 0$에서 $b - c = 0$을 얻거나, 양변을 a로 나누어 증명할 수 있다. 다른 대수 구조에서는 $a \neq 0$이어도 약분이 불가능할 수 있으므로, 여기서는 실수라는 범위도 실제로 사용되었다.

연습문제 3.19 모든 유리수 r와 무리수 x에 대해 $r + x$가 무리수임을 증명하라. 곱 rx에도 같은 결론이 성립하는지 답하라.

풀이. $r+x$가 유리수라면 $x = (r+x) - r$도 유리수여서 x가 무리수라는 가정과 모순이다. 곱은 $r = 0$이면 $rx = 0$이므로 일반적으로는 거짓이다. $r \neq 0$일 때는 rx가 유리수라는 가정에서 $x = (rx)/r$이 유리수라는 모순을 얻으므로 무리수이다.

연습문제 3.20 함수 $f : X \to Y$와 $A, B \subseteq X$에 대해 $f(A \cap B) \subseteq f(A) \cap f(B)$를 보이고, 등식이 실패하는 예를 들라.

풀이. $y \in f(A \cap B)$이면 $x \in A \cap B$이면서 $f(x) = y$인 x가 존재한다. 같은 x가 $y \in f(A)$와 $y \in f(B)$의 증인이므로 포함이 성립한다. 등식의 반례로 $X = \{0, 1\}$, $Y = \{0\}$, 상수함수 f, $A = \{0\}$, $B = \{1\}$을 택한다. 왼쪽은 $f(\varnothing) = \varnothing$이고 오른쪽은 $\{0\}$이다. 오른쪽 두 존재문의 증인이 서로 같아야 할 이유가 없다는 것이 실패의 원인이다.

연습문제 3.21 정수 $a = -17, b = 5$에 대해 나눗셈 알고리즘의 q, r를 구하고, $q = -3, r = -2$가 왜 요구 조건을 만족하지 않는지 설명하라.

풀이. $-17 = 5(-4) + 3$이므로 $q = -4, r = 3$이다. $-17 = 5(-3) - 2$도 등식으로는 맞지만 $0 \le r < 5$라는 나머지의 범위 조건을 위반한다. 정리 3.9의 유일성은 모든 가능한 정수 표현이 유일하다는 주장이 아니라, 정해진 범위를 만족하는 표현이 유일하다는 주장이다.

연습문제 3.22 집합 A, B, C에 대해 $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$를 증명하라.

풀이. 임의의 x에 대해 왼쪽의 소속 조건은

$$x \in A \wedge \neg(x \in B \vee x \in C) \iff x \in A \wedge x \notin B \wedge x \notin C.$$

오른쪽의 소속 조건도 동일하다. 드모르간 법칙(식 (2.7))을 집합의 소속 진술에 적용한 것이다. 집합이 유한하다는 가정은 필요하지 않다.

앞의 증명에서 사용한 “임의의 원소”, “증인을 택한다”, “대입한다”를 엄밀히 해석하려면 변수와 구조의 의미가 필요하다. 다음 장(제4권 제4장)에서는 술어논리의 구문과 의미론으로 그 언어를 만든다.

제 4 장

술어논리의 구문, 의미, 치환

개요 술어논리(*predicate logic*), 곧 일차논리(*first-order logic*)는 대상·함수·관계·양화사를 명시적인 기호로 다루어 "모든 정수는 어떤 정수의 후속수이다"와 같은 문장의 내부 구조를 드러내는 논리 체계이다. 명제논리는 이런 문장 전체를 쪼갤 수 없는 하나의 기호 p로 취급하지만, 술어논리는 대상을 가리키는 항과 대상 사이의 관계를 주장하는 원자식을 구별하고 양화사로 "모든"과 "어떤"을 표현한다. 이 장은 일차 언어와 그 언어로 만들어지는 항·논리식의 구문을 정하고(4.1절), 자유변수와 속박변수를 구별하며(4.2절), 언어를 실제로 해석하는 구조와 할당을 도입하고(4.3절), 만족 관계 $\mathcal{M}, s \models \varphi$로 의미론을 완성한 뒤(4.4절), 항을 변수에 대입하는 치환이 포획을 피해야 하는 이유와 그 의미론적 정당화인 치환 보조정리를 다룬다(4.5절). 이 장에서 다루는 일차논리는 동일성 기호를 논리 기호로 포함하며, 구조의 정의역은 항상 비어 있지 않다고 가정한다. 함수 기호는 정의역 전체에서 값이 정해지는 전함수로만 해석한다. 선행 지식: 명제논리, 함수와 관계의 기본 개념.

4.1 언어, 항, 원자식

정의 4.1 (일차 언어) **일차 언어**(*first-order language*) L은 상수 기호의 모임, 각 양의 정수 n에 대한 n항 함수 기호의 모임, 각 양의 정수 n에 대한 n항 관계 기호의 모임을 지정하여 얻는다. 변수 $x_0, x_1, \dots$와 논리 기호 $(\neg, \wedge, \vee, \to, \forall, \exists$ 및 괄호)는 모든 언어가 공통으로 사용하며 L의 지정에 포함되지 않는다. 동일성 기호 $=$는 임의의 기호가 아니라 실제 동일성을 나타내는 논리 기호로 취급하며, 모든 구조에서 항상 같은 뜻으로 해석된다.

예제 4.2 군을 표현하는 언어는 상수 e, 이항 함수 기호 $\cdot$, 단항 함수 기호 $^{-1}$을 가질 수 있다. 순서를 표현하는 언어는 이항 관계 기호 $<$ 하나만 가질 수 있다. 산술의 언어는 상수 0, 단항 함수 기호 S(후속자), 이항 함수 기호 $+, \times$를 포함할 수 있다. 집합론의 언어는 보통 이항 관계 기호 $\in$ 하나만 가지며, 상수나 함수 기호를 전혀 쓰지 않고도 모든 집합론적 대상을 $\in$에 대한 논리식으로 기술한다. 어떤 기호를 기본으로 두고 어떤 기호를 약어로 정의하는지는 언어를 고정할 때 미리 정해 둔다.

정의 4.3 (항과 원자식) 언어 L의 **항**(*term*)은 다음 규칙으로 유한 번 만들어지는 식이다. 변수와 상수 기호는 항이고, n항 함수 기호 f와 항 $t_1, \dots, t_n$에 대하여 $f(t_1, \dots, t_n)$은 항이다. **원자식**(*atomic formula*)은 $t = u$ 꼴이거나, n항 관계 기호 R과 항 $t_1, \dots, t_n$에 대한 $R(t_1, \dots, t_n)$ 꼴의 식이다. **논리식**(*formula*)은 원자식에 연결사 $\neg, \wedge, \vee, \to$와 양화사 $\forall x, \exists x$를 유한 번 적용하여 만든다.

항은 대상을 지칭하고 논리식은 성질을 주장한다는 점에서 역할이 다르다. $x + y$는 항이지만 $x + y = z$는 논리식이다. $R(x)$가 논리식이라고 해서 $f(R(x))$가 자동으로 허용되는 것은 아니다. f의 입력 자리에는 대상을 가리키는 항이 와야 하는데 $R(x)$는 대상이 아니라 주장이기 때문이다.

이러한 문법 검사(어떤 기호열이 항이고 어떤 기호열이 논리식인지 가리는 일)는 참·거짓을 따지는 의미론보다 앞서 이루어지는 순수한 구문적 절차이다.

흔한 오류 (항과 논리식의 혼동). 항과 논리식을 자리에 맞지 않게 섞어 쓰는 오류는 겉보기에 그럴듯한 기호열을 만들어낸다. 언어가 전함수만 허용한다는 규약 아래, 부분적으로만 정의되는 연산(예: 실수 나눗셈)을 항으로 직접 쓰려면 별도의 총체화 규약을 정하거나, 나눗셈 자체를 조건이 붙은 관계(곱셈)로 바꾸어 표현해야 한다. 이 점은 §4.3에서 다시 다룬다.

4.2 자유변수와 양화 범위

정의 4.4 (자유변수) 논리식 φ의 **자유변수**(*free variable*) 집합을 $\mathrm{FV}(\varphi)$로 쓴다. 원자식의 자유변수는 그 안에 나타난 변수들이고, 다음이 성립한다.

$$\begin{aligned} \mathrm{FV}(\neg\varphi) &= \mathrm{FV}(\varphi), \\ \mathrm{FV}(\varphi \circ \psi) &= \mathrm{FV}(\varphi) \cup \mathrm{FV}(\psi), \qquad \circ \in \{\wedge, \vee, \to\}, \\ \mathrm{FV}(\forall x\, \varphi) &= \mathrm{FV}(\exists x\, \varphi) = \mathrm{FV}(\varphi) \setminus \{x\}. \end{aligned} \tag{4.1}$$

자유변수가 없는 논리식을 **문장**(*sentence*)이라 한다. x가 φ에서 자유변수가 아닌 자리에 나타나면 그 출현은 **속박**(*bound*)되어 있다고 한다.

같은 변수 기호가 한 식 안에서 자유로운 출현과 속박된 출현을 동시에 가질 수 있다. 예를 들어

$$P(x) \wedge \forall x\, Q(x, y)$$

에서 첫 x는 자유롭고 Q 안의 x는 속박되어 있다. 식 (4.1)을 그대로 적용하면 전체 자유변수는 x, y이다. 표기를 $P(x) \wedge \forall z\, Q(z, y)$로 바꾸면 이러한 역할이 더 잘 드러난다.

예제 4.5 $\forall x\,(R(x,y) \to \exists y\, R(y,x))$의 바깥 x는 뒤의 두 원자식 안에서 모두 속박되어 있다. 첫 $R(x,y)$의 y는 자유롭지만 둘째 $R(y,x)$의 y는 안쪽 존재 양화사에 속박된다. 따라서 전체 자유변수 집합은 $\{y\}$이다. 안쪽 변수를 z로 바꿔 $\forall x\,(R(x,y) \to \exists z\, R(z,x))$로 쓰면 더 읽기 쉽다.

참고 (알파 이름변경). 속박변수의 이름을 다른 자유변수나 바깥 속박변수와 충돌하지 않게 바꾸는 것을 **알파 이름변경**(*alpha renaming*)이라 부른다. $\forall x\, P(x)$와 $\forall z\, P(z)$는 같은 의미를 가진다. 그러나 $\forall x\, R(x,z)$를 $\forall z\, R(z,z)$로 바꾸면 원래 자유롭던 z가 새 양화사에 속박되므로 허용되는 이름변경이 아니다. 알파 이름변경이 허용되려면 새 이름이 그 식의 다른 자유변수나 속박변수와 겹치지 않아야 한다.

4.3 구조와 항의 값

정의 4.6 (구조와 할당) 언어 L의 **구조**(*structure*) $\mathcal{M}$은 비어 있지 않은 집합 M(**정의역**)과 다음 해석으로 이루어진다. 각 상수 c에는 원소 $c^{\mathcal{M}} \in M$을, 각 n항 함수 기호 f에는 함수 $f^{\mathcal{M}} : M^n \to M$을, 각 n항 관계 기호 R에는 부분집합 $R^{\mathcal{M}} \subseteq M^n$을 지정한다. **할당**(*assignment*) s는 각 변수에 M의 원소를 지정하는 함수 $s : \{x_0, x_1, \dots\} \to M$이다. 항 t의 값 $t^{\mathcal{M}}[s]$는 다음과

같이 항의 구성에 대한 재귀로 정의한다.

$$x^{\mathcal{M}}[s] = s(x), \qquad c^{\mathcal{M}}[s] = c^{\mathcal{M}}, \qquad f(t_1,\dots,t_n)^{\mathcal{M}}[s] = f^{\mathcal{M}}\big(t_1^{\mathcal{M}}[s],\dots,t_n^{\mathcal{M}}[s]\big). \tag{4.2}$$

언어에 있는 $+$ 기호 자체가 반드시 보통 덧셈을 뜻하는 것은 아니다. 산술의 표준 구조를 택했을 때에만 그 해석이 보통 덧셈이 된다. 같은 언어를 다른 구조에서 전혀 다르게 해석할 수 있다는 점이 **모형론** (*model theory*)의 출발점이다.

예제 4.7 언어 $\{0, S\}$를 자연수에서 $0^{\mathcal{N}} = 0$, $S^{\mathcal{N}}(n) = n+1$로 해석하자. $s(x) = 3$이면 $S(S(x))^{\mathcal{N}}[s] = 5$이다. 한편 정의역 $M = \{0,1\}$에서 $0^{\mathcal{M}} = 0$, $S^{\mathcal{M}}(0) = 1$, $S^{\mathcal{M}}(1) = 0$으로 해석하면 $S(S(x))^{\mathcal{M}}[s] = s(x)$이다. 같은 항이 다른 구조에서 다른 함수를 표현한다.

참고 (전함수 규약과 부분연산). 함수 기호가 전함수로 해석된다는 규약은 부분적으로만 정의되는 연산을 사용할 때 주의를 요구한다. 실수에서 나눗셈은 분모가 0인 경우 통상의 의미로 정의되지 않는다. 이를 일차언어의 전역 이항 함수로 쓰려면 0으로 나눈 값을 임의로 지정하는 별도의 총체화 규약을 정하거나, $y \neq 0$이라는 조건 아래 곱셈 관계 $yz = x$로 나눗셈 $x/y = z$를 표현해야 한다. 뒤의 방법은 함수 기호 대신 관계 기호를 쓰므로 전함수 요구를 피해 간다.

4.4 만족 관계와 논리적 귀결

정의 4.8 (만족 관계) 구조 $\mathcal{M}$에서 할당 s에 대해 논리식 φ가 참임을 $\mathcal{M}, s \models \varphi$로 쓰고 다음으로 정의한다. 할당 s에서 변수 x의 값만 a로 바꾼 할당을 $s[x \mapsto a]$로 쓴다.

$$\begin{aligned}
\mathcal{M}, s \models t = u &\iff t^{\mathcal{M}}[s] = u^{\mathcal{M}}[s],\\
\mathcal{M}, s \models R(t_1,\dots,t_n) &\iff \big(t_1^{\mathcal{M}}[s],\dots,t_n^{\mathcal{M}}[s]\big) \in R^{\mathcal{M}},\\
\mathcal{M}, s \models \neg\varphi &\iff \mathcal{M}, s \not\models \varphi,\\
\mathcal{M}, s \models \varphi \wedge \psi &\iff \mathcal{M}, s \models \varphi \text{ 이고 } \mathcal{M}, s \models \psi,\\
\mathcal{M}, s \models \forall x\,\varphi &\iff \text{모든 } a \in M \text{에 대해 } \mathcal{M}, s[x \mapsto a] \models \varphi,\\
\mathcal{M}, s \models \exists x\,\varphi &\iff \text{어떤 } a \in M \text{에 대해 } \mathcal{M}, s[x \mapsto a] \models \varphi.
\end{aligned} \tag{4.3}$$

나머지 연결사 $\vee, \rightarrow$는 명제논리와 같은 진리표로 해석한다.

보조정리 4.9 (자유변수에 대한 일치) 두 할당 s, s'가 φ의 모든 자유변수에서 같은 값을 주면

$$\mathcal{M}, s \models \varphi \iff \mathcal{M}, s' \models \varphi.$$

따라서 문장의 참·거짓은 할당의 선택에 의존하지 않는다.

증명. 먼저 항의 값이 그 항에 나타난 변수의 값에만 의존함을 항의 구성에 대한 귀납으로 보인다. 변수와 상수의 경우는 식 (4.2)에서 바로 확인되고, 함수 적용의 경우는 귀납 가정을 각 t_i에 적용하면 된다. 이 사실이 만족 관계의 원자식 경우를 준다. 연결사의 경우에는 구성 부분식에 대한 귀납 가정을 적용한다. $\varphi = \forall x\,\psi$인 경우, 임의의 $a \in M$에 대해 $s[x \mapsto a]$와 $s'[x \mapsto a]$는 ψ의 모든 자유변수에서 같은 값을 준다. x에서는 둘 다 a이고, ψ의 나머지 자유변수(모두 φ의 자유변

수이기도 하다)에서는 가정에 의해 같기 때문이다. 따라서 귀납 가정으로 ψ의 참값이 같고, 모든 a에 대해 비교하면 전칭식의 참값도 같다. 존재 양화사의 경우도 같은 방식으로 처리한다. □

문장 σ에 대해서는 $\mathcal{M} \models \sigma$라고 쓸 수 있다. 문장들의 집합 T의 모든 원소가 $\mathcal{M}$에서 참이면 $\mathcal{M}$을 T의 **모형**(*model*)이라 한다. $T \models \sigma$는 T의 모든 모형이 σ를 만족한다는 뜻이며, 이를 **논리적 귀결**(*logical consequence*)이라 부른다. 특정 구조 하나에서의 참과 그 언어의 모든 구조에서 성립하는 타당성은 서로 다른 개념이므로 혼동하지 않아야 한다.

예제 4.10 언어 $\{<\}$의 문장 $\forall x \exists y\,(x < y)$는 통상의 순서를 가진 $\mathbb{N}$과 $\mathbb{Z}$에서 참이다. 하지만 통상의 순서를 제한한 집합 $\{0, 1\}$에서는 $x = 1$의 증인이 없어 거짓이다. 따라서 이 문장은 논리적으로 타당한 문장이 아니다. 어떤 구조가 이 문장을 만족하려면 무한성이나 비유계성에 관한 실질적인 정보가 필요하다.

4.5 포획 없는 치환과 치환 보조정리

φ에서 변수 x의 자유로운 출현을 모두 항 t로 바꾼 식을 $\varphi[t/x]$로 쓴다. 이 치환이 뜻대로 작동하려면 t에 들어 있는 변수가 치환 결과에서 새로운 양화사에 **포획**(*capture*)되지 않아야 한다. 충돌이 생기면 먼저 그 양화사의 속박변수 이름을 식에 나타나지 않는 새 이름으로 바꾼 뒤 치환을 수행한다. 이렇게 수행한 치환을 **포획 없는 치환**(*capture-avoiding substitution*)이라 한다.

예제 4.11 $\varphi = \exists y\,(x < y)$에서 x에 y를 대입하려 한다. 기계적으로 바꾸어 $\exists y\,(y < y)$를 얻으면 원래 자유로웠던 증인의 입력값 y가 양화사에 포획되어 식의 뜻이 바뀐다. 먼저 φ를 $\exists z\,(x < z)$로 이름변경한 뒤

$$\varphi[y/x] = \exists z\,(y < z)$$

로 바꿔야 한다. 실수에서 잘못 치환한 식 $\exists y\,(y < y)$는 거짓이고 올바르게 치환한 식은 모든 y에서 참이므로 둘의 차이가 분명하다.

속박된 출현은 치환하지 않는다. $(P(x) \wedge \forall x\, Q(x))[t/x]$에서는 첫 $P(x)$만 $P(t)$로 바뀌고, 뒤의 전칭식은 x가 이미 그 안에서 속박되어 있으므로 그대로 둔다. 변수 이름만 기계적으로 검색하여 모두 바꾸는 작업은 이러한 수학적 치환과 같지 않다.

정리 4.12 (치환 보조정리) 치환 $\varphi[t/x]$를 포획 없이 수행했다고 하자. 임의의 구조 $\mathcal{M}$과 할당 s에 대해

$$\mathcal{M}, s \models \varphi[t/x] \iff \mathcal{M}, s[x \mapsto t^{\mathcal{M}}[s]] \models \varphi. \tag{4.4}$$

즉, 식에 항을 대입하여 평가하는 것과 원래 식에서 해당 변수에 그 항의 값을 배정하는 것은 일치한다.

증명. 항의 치환에 대해서도 같은 형태의 값 등식 $r[t/x]^{\mathcal{M}}[s] = r^{\mathcal{M}}[s[x \mapsto t^{\mathcal{M}}[s]]]$이 성립하며, 항의 구성에 대한 귀납으로 증명된다. 그 결과를 사용하면 원자식의 경우가 바로 따라온다. 연결사의 경우에는 각 부분식에 귀납 가정을 적용하면 된다.

양화사 단계가 핵심이다. $\varphi = \forall y\,\psi$이고 $y \neq x$라 하자. 포획 없는 치환의 가정에 따라 필요하면 이름변경하여 y가 t에 나타나지 않게 해 둔다. 그러면 임의의 $a \in M$에 대해 $t^{\mathcal{M}}[s[y \mapsto a]] = t^{\mathcal{M}}[s]$이고, 서로 다른 변수 x, y에 대한 값 변경은 이 상황에서 순서를 교환할 수 있다. 따라서 귀납

가정을 ψ에 적용하면 각 $a \in M$에 대해

$$\mathcal{M}, s[y \mapsto a] \models \psi[t/x] \iff \mathcal{M}, s[x \mapsto t^{\mathcal{M}}[s]][y \mapsto a] \models \psi$$

이다. 모든 a에 대해 양쪽을 비교하면 전칭식의 등가성이 나온다. $y = x$인 경우에는 치환이 그 양화사 내부의 x의 출현을 바꾸지 않으며, 전칭식의 참값은 애초에 x에 배정된 값과 무관하므로 결론이 바로 성립한다. 존재 양화사의 경우도 같은 방식으로 처리한다. □

이 정리는 대입 규칙이 왜 의미론적으로 올바른지를 설명한다. $\forall x\, P(x)$에서 $P(t)$를 얻을 수 있는 것은 모든 원소에 대해 참인 성질이 항 t의 값에서도 참이기 때문이다. 변수 포획을 허용하면 식 (4.4)의 좌변과 우변이 더 이상 같은 뜻을 갖지 않게 되어 이러한 의미론적 설명이 깨진다.

역사. 현대적인 양화사 표기 $\forall, \exists$와 자유변수·속박변수의 엄밀한 구별은 Gottlob Frege가 1879년 저작 *Begriffsschrift*에서 처음 체계적으로 제시했으며, Charles Sanders Peirce도 1880년대에 독립적으로 양화사 표기를 발전시켰다. 구조와 만족 관계를 통한 형식 의미론은 20세기에 들어 Alfred Tarski가 정식화했다.

4.6 연습문제와 해설

> **연습문제 4.13** $\exists x\,(R(x,y) \wedge \forall y\, S(x,y,z))$의 자유변수를 구하고, 혼동을 줄이도록 속박변수를 다시 쓰라.

풀이. 자유변수는 y, z이다. 첫 $R(x,y)$의 y는 자유롭고, $S(x,y,z)$의 y는 속박되어 있다. 예를 들어 $\exists u\,(R(u,y) \wedge \forall v\, S(u,v,z))$로 쓰면 각 출현의 역할이 분명하다. 자유로운 y까지 v로 바꾸면 다른 뜻의 식이 된다.

> **연습문제 4.14** $M = \{a, b\}$, $R^{\mathcal{M}} = \{(a,b), (b,a)\}$인 구조에서 $\forall x \exists y\, R(x,y)$와 $\exists y \forall x\, R(x,y)$의 값을 구하라.

풀이. 첫 식은 참이다. $x = a$이면 $y = b$, $x = b$이면 $y = a$를 택한다. 둘째 식은 거짓이다. $y = a$를 택하면 $R(a,a)$가 거짓이고, $y = b$를 택하면 $R(b,b)$가 거짓이므로 가능한 두 증인이 모두 실패한다.

> **연습문제 4.15** 언어가 동일성만 포함할 때, 정확히 두 원소를 갖는 구조를 표현하는 문장을 쓰라.

풀이. 다음 문장이 가능하다.

$$\exists x \exists y\, \big(x \neq y \wedge \forall z\,(z = x \vee z = y)\big).$$

$x \neq y$는 적어도 두 원소를 보장하고, 전칭식은 모든 원소가 이 둘 중 하나임을 말하여 많아야 두 원소임을 보장한다. 한쪽 조건만 쓰면 정확한 크기를 지정하지 못한다.

> **연습문제 4.16** $\varphi = \forall y\,(R(x,y) \vee P(z))$에서 x를 항 $f(y)$로 포획 없이 치환하라.

풀이. 먼저 속박된 y를 새 변수 u로 바꾼다. 결과는

$$\forall u\,(R(f(y),u) \vee P(z))$$

이다. 여기서 y는 여전히 자유롭다. 이름변경 없이 $\forall y\,(R(f(y),y)\lor P(z))$로 쓰면 입력항 $f(y)$의 자유변수 y가 포획되어 의미가 바뀐다.

연습문제 4.17 $\forall x\,(P(x)\lor Q(x))$에서 $(\forall x\,P(x))\lor(\forall x\,Q(x))$가 따라오는지 판정하라.

풀이. 일반적으로 따라오지 않는다. 정의역 $\{0,1\}$에서 P는 0에서만, Q는 1에서만 참이라고 하자. 모든 원소에서 둘 중 하나는 참이지만, P가 모든 원소에서 참인 것도 아니고 Q가 모든 원소에서 참인 것도 아니다. 반대 방향의 함의 $(\forall x\,P(x))\lor(\forall x\,Q(x))\to\forall x\,(P(x)\lor Q(x))$는 참이다.

연습문제 4.18 y가 φ에 자유롭게 나타나지 않을 때 φ와 $\forall y\,\varphi$가 이 장의 의미론에서 동치임을 설명하라.

풀이. 보조정리 4.9에 의해 y의 할당을 바꾸어도 φ의 참값은 변하지 않는다. 따라서 φ가 참이면 모든 y값에서 참이므로 $\forall y\,\varphi$가 참이다. 반대로 정의역이 비어 있지 않으므로 원소를 하나 택하면 $\forall y\,\varphi$의 참으로부터 그 원소에서 φ가 참임을 얻고, 다시 보조정리로 임의의 할당에서 φ가 참임을 얻는다. 정의역이 비어도 되는 다른 체계에서는 $\forall y\,\varphi$가 공허하게 참일 수 있어 이 역방향이 깨지므로 주의해야 한다.

다음 연결. 이 장의 의미론은 무엇이 참인지를 정한다. 다음 장의 증명 규칙은 어떤 기호적 단계를 정당하게 사용할 수 있는지 정한다. 건전성은 이 두 층이 맞물린다는 주장이다.

제 5 장

자연연역과 시퀀트의 첫걸음

개요 **자연연역**(*natural deduction*)은 “가정하자”, “두 경우를 나누자”, “임의의 원소를 택하자”처럼 수학자가 실제로 증명에서 수행하는 조작을 명시적인 추론 규칙으로 옮긴 증명 체계이다. 이 장은 전제 집합 Γ 아래 φ를 유도할 수 있다는 증명 판단 $\Gamma \vdash \varphi$를 정의하고(5.1절), 각 논리 연결사의 도입·제거 규칙을 세우며(5.2절), 배중률처럼 고전논리에서만 성립하는 규칙의 위치를 밝히고(5.3절), 양화사 규칙과 그에 딸린 고유변수 조건을 다룬다(5.4절). 이어 같은 추론을 반대 방향—결론에서 전제로—으로 읽는 시퀀트 계산의 언어를 소개하고(5.5절), 마지막으로 이 장에서 제시한 규칙들이 실제로 참을 보존한다는 건전성 정리를 증명한다(5.6절). 이 장에서는 부정을 $\neg\varphi := \varphi \to \bot$로 읽을 수 있는 자연연역을 사용하며, 고전적 규칙을 추가하는 위치는 따로 표시한다. 규칙을 외우는 것보다 증명의 각 단계에서 현재 어떤 가정에 의존하고 있는지를 정확히 기록하는 일이 중요하다. 잠시 도입한 가정을 해제하지 않은 채 결론에서 지워 버리면, 참인 추론처럼 보이는 오류를 만들 수 있다. 선행 지식: 명제논리의 의미론, 술어논리의 변수와 치환.

5.1 판단과 가정의 관리

> **정의 5.1 (증명 판단과 의미론적 귀결)** $\Gamma \vdash \varphi$는 전제 집합 Γ에 속한 가정들을 사용하여 이 장의 규칙에 따라 φ를 유도할 수 있다는 **증명 판단**(*provability judgment*)이다. $\Gamma \models \varphi$는 Γ의 모든 해석에서 참을 보존한다는 **의미론적 귀결**(*semantic consequence*)이다. 두 표기는 정의가 서로 다르며, 둘이 같은 범위를 가리킨다는 것은 그 자체로 증명이 필요한 사실(건전성·완전성)이다.

가정 규칙(*assumption rule*)은 $\varphi \in \Gamma$이면 $\Gamma \vdash \varphi$라는 것이다. 모든 증명은 유한한 단계로 이루어진다. Γ가 무한 집합이어도 개별 증명에서 실제로 사용하는 가정은 유한 개뿐이다. 이 사실만으로 의미론의 콤팩트성(제4권 제11장)까지 증명한 것은 아니다. 증명론적 귀결과 의미론적 귀결을 연결하는 메타정리(건전성, 완전성)가 별도로 필요하다.

조건문을 증명할 때는 가정을 임시로 묶음 안으로 들여왔다가 해제하고 나온다. 다음 표의 들여쓰기는 가정의 사용 범위를 보여준다.

표 5.1 가정의 도입과 해제: $p \to (q \to p)$의 유도

단계	내용	이유
1	p	임시 가정
2	q	임시 가정
3	p	1에서
4	$q \to p$	2의 가정을 해제
5	$p \to (q \to p)$	1의 가정을 해제

3에서는 p라는 바깥 가정이 여전히 사용 중이므로 들여쓰기가 2와 같다. 4의 결론 $q \to p$는 p에 의존하지만 더 이상 q에는 의존하지 않으므로 들여쓰기가 한 단계 줄어든다. 5에서는 둘 다 해제되므로 전제가 없는 정리 $\vdash p \to (q \to p)$를 얻는다. 가정 해제는 그 가정이 참임을 증명하는 절차가 아니라, 그 가정 아래 얻은 결론을 조건문으로 묶어 가정에 대한 의존성을 없애는 절차이다.

5.2 연결사의 도입과 제거

도입 규칙(*introduction rule*)은 특정 연결사를 가진 결론을 어떻게 만드는지 알려 준다. **제거 규칙**(*elimination rule*)은 이미 얻은 연결사 식에서 무엇을 꺼내 쓸 수 있는지 알려 준다. 전제 집합을 하나로 통일하여 적으면 논리곱의 핵심 규칙은 다음과 같다.

$$\frac{\Gamma \vdash \varphi \qquad \Gamma \vdash \psi}{\Gamma \vdash \varphi \wedge \psi}\ (\wedge I), \qquad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \varphi}\ (\wedge E_1), \qquad \frac{\Gamma \vdash \varphi \wedge \psi}{\Gamma \vdash \psi}\ (\wedge E_2).$$

조건문의 규칙은

$$\frac{\Gamma, \varphi \vdash \psi}{\Gamma \vdash \varphi \to \psi}\ (\to I), \qquad \frac{\Gamma \vdash \varphi \to \psi \qquad \Gamma \vdash \varphi}{\Gamma \vdash \psi}\ (\to E).$$

쉼표 Γ, φ는 $\Gamma \cup \{\varphi\}$의 약어이다. $\to I$에서는 φ라는 임시 가정의 의존성이 해제된다. $\to E$는 **전건긍정**(*modus ponens*), 곧 모두스 포넨스이다.

논리합은 한쪽 증거만으로 도입할 수 있다.

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \varphi \vee \psi}\ (\vee I_1), \qquad \frac{\Gamma \vdash \psi}{\Gamma \vdash \varphi \vee \psi}\ (\vee I_2).$$

하지만 제거할 때는 어느 쪽이 참인지 모르므로 두 갈래가 모두 같은 결론을 주어야 한다.

$$\frac{\Gamma \vdash \varphi \vee \psi \qquad \Gamma, \varphi \vdash \chi \qquad \Gamma, \psi \vdash \chi}{\Gamma \vdash \chi}\ (\vee E).$$

$\varphi \vee \psi$에서 φ를 곧바로 꺼내는 규칙은 없다. $\varphi = 0, \psi = 1$(거짓, 참)이면 그러한 규칙은 참인 전제를 거짓인 결론으로 보내기 때문이다.

거짓 상수 $\bot$에서 임의의 결론을 얻는 규칙은

$$\frac{\Gamma \vdash \bot}{\Gamma \vdash \varphi}\ (\bot E)$$

이다. $\neg\varphi = \varphi \to \bot$로 읽으면 부정 도입은 φ를 가정하여 $\bot$을 유도한 뒤 가정을 해제하는 것이고, φ와 $\neg\varphi$에서 $\bot$을 얻는 것은 조건문 제거($\to E$)의 한 경우이다.

예제 5.2 (가정을 기록한 조건문의 합성) $(p \to q) \land (q \to r)$에서 $p \to r$를 유도하자. 전제의 논리곱을 제거하여 $p \to q$, $q \to r$를 얻는다. 이제 p를 임시로 가정한다. $p \to q$와 p에서 q를 얻고($\to E$), 이어 $q \to r$와 q에서 r를 얻는다($\to E$). p 가정을 해제하면($\to I$) $p \to r$이다. 처음 전제까지 해제하면 전제 없는 정리

$$\vdash \big((p \to q) \land (q \to r)\big) \to (p \to r)$$

를 얻는다.

검산. 예제 5.2의 결론은 명제 p, q, r에 대한 진리표 여덟 줄을 모두 확인해도 거짓이 되는 줄이 없으므로 항진식이다. 이는 유도가 건전성 정리(정리 5.9)와 들어맞는다는 간단한 점검이다.

5.3 고전 규칙과 부정의 역할

앞의 연결사 규칙은 **직관주의 논리**(*intuitionistic logic*)에서도 그대로 사용된다. 고전 논리를 얻는 한 방법은 다음의 **고전적 귀류 규칙**(*classical reductio rule*)을 추가하는 것이다.

$$\frac{\Gamma, \neg\varphi \vdash \bot}{\Gamma \vdash \varphi} \quad \text{(고전적 귀류 규칙).}$$

부정 도입과 모양이 닮았지만 결론이 $\neg\neg\varphi$가 아니라 φ라는 점이 다르다. 고전적 이중부정 제거를 별도 규칙으로 두어도 같은 목적을 달성할 수 있다.

예제 5.3 (배중률의 고전적 유도) $\neg(p \lor \neg p)$를 가정한다. 그 아래 p를 추가로 가정하면 논리합 도입($\lor I_1$)으로 $p \lor \neg p$를 만들 수 있어 바깥 가정과 모순이다. 따라서 p 가정을 해제하여($\to I$, 곧 부정 도입) $\neg p$를 얻는다. 이번에는 이 $\neg p$에서 논리합 도입($\lor I_2$)으로 $p \lor \neg p$를 다시 얻어, 처음 가정 $\neg(p \lor \neg p)$와 모순을 얻는다. 처음 가정을 고전적 귀류 규칙으로 해제하면 $\vdash p \lor \neg p$이다.

이 과정에서 배중률을 증명했다고 해서, 어떤 계산 문제 P에 대해 언제나 P 또는 $\neg P$의 구체적인 증명을 찾아 주는 알고리즘을 얻은 것은 아니다. 고전 명제의 타당성과, 그 증거를 실제로 계산하는 절차는 서로 다른 층의 주장이다.

예제 5.4 (구성적인 한 방향과 고전적인 역방향) $\neg p \lor \neg q$에서 $\neg(p \land q)$는 고전적 규칙 없이 유도할 수 있다. $p \land q$를 가정하고, $\neg p$인 경우에는 p와 모순, $\neg q$인 경우에는 q와 모순을 얻는다. 두 경우 모두 모순이므로 논리합 제거($\lor E$)로 합쳐 $\bot$을 얻고, $p \land q$ 가정을 해제하면($\to I$) $\neg(p \land q)$이다. 역방향 $\neg(p \land q) \to (\neg p \lor \neg q)$는 고전 논리에서는 타당하지만, 이 일반 형태는 직관주의 규칙만으로는 얻지 못한다.

검산. 드모르간의 두 방향 $\neg(p \land q) \leftrightarrow (\neg p \lor \neg q)$은 진리표로 확인하면 p, q의 네 조합에서 모두 성립하는 고전적 항진 동치이다. 예제 5.4이 보여 주는 것은 두 방향의 증명론적 난이도가 다르다는 점이지, 어느 한쪽이 의미론적으로 더 약하다는 점이 아니다. 논리 체계를 밝혀야 하는 이유가 여기에 있다.

5.4 양화사 규칙과 고유변수 조건

전칭 제거와 존재 도입은 치환을 사용한다. 아래에서 모든 치환은 포획 없이(제4권 제4장) 수행한다.

$$\frac{\Gamma \vdash \forall x\, \varphi}{\Gamma \vdash \varphi[t/x]}\ (\forall E), \qquad \frac{\Gamma \vdash \varphi[t/x]}{\Gamma \vdash \exists x\, \varphi}\ (\exists I).$$

첫 규칙은 모든 대상에 대해 참인 성질을 특정 항의 값에 적용한다. 둘째 규칙은 특정 증인의 성질로부터 존재를 결론 내린다. 항 t에 자유변수가 있어도, 현재 할당에서 그 항이 나타내는 대상을 증인으로 사용하는 것이다.

전칭 도입은 임의성을 요구한다.

$$\frac{\Gamma \vdash \varphi}{\Gamma \vdash \forall x\, \varphi}\ (\forall I), \qquad x \notin \mathrm{FV}(\Gamma).$$

여기서 $\mathrm{FV}(\Gamma)$는 사용 중인 가정들의 자유변수 집합의 합집합이다. 가정에 x의 특수한 성질이 남아 있다면 x에 관한 결론을 모든 대상으로 일반화할 수 없다. 이 조건을 만족하지 않는 단계를 허용하면 $P(x) \vdash \forall x\, P(x)$ 같은 잘못된 유도를 허용하게 된다.

존재 제거는 증인에 잠시 이름을 붙여 사용하되, 결론이 그 이름에 의존하지 않게 한다.

$$\frac{\Gamma \vdash \exists x\, \varphi \qquad \Gamma, \varphi[y/x] \vdash \psi}{\Gamma \vdash \psi}\ (\exists E), \qquad y \notin \mathrm{FV}(\Gamma, \psi, \exists x\, \varphi).$$

여기서 y는 $\Gamma, \psi, \exists x\, \varphi$에 자유롭게 나타나지 않는 새 변수로 택한다. 필요하면 기존 속박변수도 이름변경한다. 이러한 변수를 **고유변수**(*eigenvariable*)라고 부른다. 새 변수는 "어떤 증인"을 대표하지만, 그 증인이 특정한 원소라고 가정할 권한을 주지는 않는다.

> **예제 5.5 (존재 추론의 올바른 사용)** $\forall x\,(P(x) \to Q(x))$와 $\exists x\, P(x)$로부터 $\exists x\, Q(x)$를 유도하자. 새 변수 a에 대해 $P(a)$를 임시로 가정한다. 전칭 제거로 $P(a) \to Q(a)$를 얻고 조건문 제거로 $Q(a)$를 얻는다. 존재 도입으로 $\exists x\, Q(x)$를 얻는다. 최종 결론에는 a가 자유롭게 나타나지 않으므로 존재 제거로 $P(a)$의 임시 가정을 해제할 수 있다.

> **예제 5.6 (서로 다른 존재 증인)** $\exists x\, P(x)$와 $\exists x\, Q(x)$에서 $\exists x\,(P(x) \wedge Q(x))$를 일반적으로 유도할 수 없다. P의 증인을 a, Q의 증인을 b로 각각 새로 잡아야 하며 둘이 같다고 보장할 정보가 없다. 정의역 $\{0, 1\}$에서 P는 0만, Q는 1만 만족하게 하면 두 전제는 참이고 결론은 거짓이다.

동일성에는 $t = t$라는 반사성과, 동일한 대상을 서로 대체하는 규칙이 있다. 예를 들어 $s = t$와 $P(s)$에서 $P(t)$를 얻는다. 이때 $P(s)$가 구체적으로 어떤 식의 어느 자유로운 자리에 s를 넣은 것인지 정하고, 대체 과정에서도 포획을 피한다. 동일성을 단순한 이름의 철자 일치와 혼동해서는 안 된다.

5.5 시퀀트로 읽는 증명의 상태

> **정의 5.7 (고전적 시퀀트)** 고전적인 다중 결론 **시퀀트**(*sequent*) $\Gamma \Rightarrow \Delta$는 왼쪽 식들이 모두 참이면 오른쪽 식들 중 적어도 하나가 참이어야 한다는 주장을 표현한다. 여기서 유한한 Γ, Δ를 생각한다. 오른쪽이 비어 있으면 왼쪽 전제들이 함께 참일 수 없다는 뜻이다.

이 절의 $\Rightarrow$는 시퀀트의 양쪽을 구분하는 기호이며, 논리식 안의 연결사 $\rightarrow$와는 다르다. 또한 이 절은 시퀀트 계산의 규칙이 전체 증명 체계 안에서 어떤 역할을 하는지 소개하는 데 그치며, 시퀀트 계산 자체의 완전성이나 컷 제거 정리를 증명하는 절은 아니다.

대표적인 규칙은 오른쪽 논리곱과 왼쪽 논리합이다.

$$\frac{\Gamma \Rightarrow \Delta, A \qquad \Gamma \Rightarrow \Delta, B}{\Gamma \Rightarrow \Delta, A \wedge B}\ (\wedge R), \qquad \frac{\Gamma, A \Rightarrow \Delta \qquad \Gamma, B \Rightarrow \Delta}{\Gamma, A \vee B \Rightarrow \Delta}\ (\vee L).$$

첫 규칙은, 오른쪽의 나머지 결론 Δ가 모두 거짓인 경우를 생각하면 위의 두 전제가 각각 A와 B를 강제하므로 논리곱 $A \wedge B$도 참이라는 뜻이다. 둘째 규칙은 왼쪽의 논리합이 어느 쪽으로 참이 되든 같은 오른쪽 결론을 얻어야 한다는 경우분석이다.

> **예제 5.8** $A \wedge B \Rightarrow B \wedge A$를 뒤에서 앞으로 분해하면, 오른쪽 논리곱 때문에 $A \wedge B \Rightarrow B$와 $A \wedge B \Rightarrow A$라는 두 목표가 생긴다. 왼쪽 논리곱을 풀면 각각 $A, B \Rightarrow B$와 $A, B \Rightarrow A$가 된다. 두 목표는 모두 가정에 결론이 그대로 들어 있는 초기 시퀀트로 닫힌다. 이 과정은 자연연역의 논리곱 제거와 도입을 다른 방향으로 조직한 것과 같다.

시퀀트를 뒤에서 앞으로 읽으면 증명 탐색의 작업 목록이 된다. 지금 증명할 결론이 논리곱이면 두 목표로 나누고, 사용 가능한 가정이 논리합이면 경우를 나눈다. 어떤 규칙을 뒤로 적용해도 되는지, 그리고 탐색이 언제 끝나는지는 논리 체계와 규칙에 따라 별도로 분석해야 한다.

5.6 건전성: 규칙은 참을 보존하는가

> **정리 5.9 (자연연역의 건전성)** 위에서 제시한 고전 자연연역 규칙으로 $\Gamma \vdash \varphi$를 유도했다면 $\Gamma \models \varphi$이다. 명제논리에서는 진리값 평가를, 일차논리에서는 구조와 할당을 해석 대상으로 삼는다.

증명. 유도의 높이에 대한 귀납을 사용한다. 가정에서 시작한 단계는 전제들이 모두 참이라는 조건으로 바로 성립한다. 논리곱 도입·제거와 조건문 제거는 진리표에서 직접 참을 보존한다. 조건문 도입에서는 Γ가 참인 해석을 고정한다. φ가 거짓이면 $\varphi \rightarrow \psi$는 참이고, φ가 참이면 위의 부분 유도에 대한 귀납 가정으로 ψ가 참이므로 역시 조건문이 참이다. 논리합 제거는 참인 논리합의 어느 한쪽이 참임을 이용하여 해당 부분 유도에 귀납 가정을 적용한다. $\bot E$에서는 $\bot$이 참인 해석이 없으므로 반례가 없다. 고전적 귀류 규칙에서는 결론 φ가 거짓이라고 하면 $\neg\varphi$가 참이므로 부분 유도에 의해 $\bot$이 참이어야 하는 모순을 얻는다.

양화사 제거와 존재 도입은 치환 보조정리(제4권 제4장)로 정당화된다. 전칭 도입에서는 x가 Γ에 자유롭게 나타나지 않으므로 x의 값을 어떤 $a \in M$으로 바꾸어도 전제들은 참이다. 귀납 가정에 따라 바뀐 할당마다 φ가 참이므로 $\forall x\,\varphi$가 참이다.

존재 제거에서는 $\exists x\,\varphi$의 증인 $a \in M$을 고른다. 새 변수 y의 값을 a로 정하면 추가 가정 $\varphi[y/x]$가 참이고, 기존 Γ의 참값은 바뀌지 않는다. 부분 유도에 귀납 가정을 적용하여 ψ를 얻는다. y가 ψ에 자유롭게 나타나지 않으므로 원래 할당에서도 ψ는 참이다. 동일성 규칙은 같은 원소를 함수와 관계에 대입해도 값과 참값이 유지된다는 해석의 정의에서 바로 성립한다. 모든 가능한 마지막 규칙을 처리했으므로 전체 유도에 결론이 적용된다. $\square$

건전성의 실용적인 결과는, 반모형을 찾으면 유도 가능성을 부정할 수 있다는 것이다. 전제들이 참인데 결론이 거짓인 구조를 찾았다면, 건전한 규칙으로는 그 결론을 증명할 수 없다. 하지만 반모형을 아직 찾지 못했다는 사실만으로 증명이 존재한다고 말할 수는 없다. 역방향인 완전성은 별도의 정리이다.

역사. 자연연역(직관주의 변형 **NJ**와 고전 변형 **NK**)과 시퀀트 계산(직관주의 변형 **LJ**와 고전 변형 **LK**)은 모두 Gerhard Gentzen이 1935년 논문 *Untersuchungen über das logische Schließen*에서 도입했다. 같은 논문에서 시퀀트 계산의 컷 제거 정리(*Hauptsatz*)도 함께 증명되었다.

5.7 연습문제와 해설

연습문제 5.10 $p \wedge (q \vee r)$에서 $(p \wedge q) \vee (p \wedge r)$를 자연연역으로 유도하라.

풀이. 전제에서 p와 $q \vee r$를 꺼낸다($\wedge E_1, \wedge E_2$). q를 가정한 갈래에서는 $p \wedge q$를 만들고 왼쪽 논리합 도입($\vee I_1$)으로 목표를 얻는다. r를 가정한 갈래에서는 $p \wedge r$를 만들고 오른쪽 논리합 도입($\vee I_2$)으로 같은 목표를 얻는다. 두 갈래의 임시 가정을 논리합 제거($\vee E$)로 해제하면 결론이 나온다.

연습문제 5.11 $p \to q$와 $\neg q$에서 $\neg p$를 유도할 때 고전적 귀류 규칙이 필요한지 설명하라.

풀이. 필요하지 않다. p를 가정하면 $p \to q$에서 q를 얻고($\to E$) $\neg q = q \to \bot$과 함께 모순 $\bot$을 얻는다($\to E$). p 가정을 조건문 도입으로 해제하면 $p \to \bot$, 즉 $\neg p$이다. 이것은 부정 도입이지 이중부정 제거가 아니다.

연습문제 5.12 $P(a)$를 가정한 뒤 $\forall x\, P(x)$를 결론 내린 유도에서 무엇이 잘못되었는가?

풀이. a를 변수로 쓴다면 그 변수가 해제되지 않은 가정 $P(a)$에 자유롭게 나타나므로 전칭 도입의 고유변수 조건을 위반한다. a를 상수로 쓴다면 그 상수가 가리키는 특정 대상의 성질만 확인했을 뿐이므로 여전히 모든 대상에 대한 일반화가 허용되지 않는다. 두 원소를 가진 구조에서 P가 한 원소에서만 참인 반모형을 만들 수 있다.

연습문제 5.13 $\exists x \forall y\, R(x,y)$에서 $\forall y \exists x\, R(x,y)$를 유도하는 증명을 설명하라.

풀이. 존재 증인을 새 변수 a로 택하여 $\forall y\, R(a,y)$를 가정한다. 임의의 변수 b에 대해 전칭 제거로 $R(a,b)$를, 존재 도입으로 $\exists x\, R(x,b)$를 얻는다. b는 남은 가정에 자유롭게 나타나지 않으므로 전칭 도입으로 $\forall y \exists x\, R(x,y)$를 얻는다. 이 결론에는 a가 자유롭게 나타나지 않으므로 처음 증인 가정을 존재 제거로 해제한다.

연습문제 5.14 존재 제거의 결론에서 증인 변수를 자유롭게 남겨도 된다고 허용하면 어떤 오류가 생기는지 예를 들라.

풀이. $\exists x\, P(x)$에서 새 변수 a로 $P(a)$를 가정하고, 바로 $P(a)$를 결론으로 남긴 채 가정을 해제할 수 있게 된다고 하자. 그러면 어떤 원소가 P를 만족한다는 사실만으로 자유변수 a의 임의의 값이 P를 만족한다고 주장하게 된다. P가 두 원소 중 하나에서만 참인 구조에서 a를 다른 원소에 할당하면 전제는 참이고 결론은 거짓이다.

연습문제 5.15 시퀀트 $A, B \Rightarrow A \wedge B$와 $A \Rightarrow A \vee B$를 이 절의 의미로 해석하고 참을 보존하는 이유를 말하라.

풀이. 첫 시퀀트는 두 전제가 모두 참이면 두 전제의 논리곱이 참이라는 주장이다. 둘째는 A가 참이면 적어도 A가 참이므로 논리합이 참이라는 주장이다. 어느 시퀀트도 $A \vee B \Rightarrow A$를 정당화하지 않는다. 오른쪽이 여러 식일 때도 그 의미는 “모두”가 아니라 “적어도 하나”라는 점을 기억한다.

다음 연결. 건전성의 증명 자체에서 유도의 높이에 대한 귀납을 사용했다. 다음 장에서는 이러한 메타 수준의 귀납을, 수열·알고리즘·논리식의 구조에 대한 귀납과 함께 정리한다.

제 6 장

귀납법과 재귀적 정의

개요 수학적 귀납법(*mathematical induction*)은 자연수 전체에 걸친 명제를 시작점의 확인과 단계적 연결의 증명이라는 두 단계로 정당화하는 증명 방법이고, 재귀적 정의(*recursive definition*)는 그 쌍대로 앞선 값에서 다음 값을 정해 함수나 수열을 구성하는 방법이다. 유한 개의 사례를 확인하는 것과 모든 자연수에서 명제가 성립함을 증명하는 것은 다른 일이며, 귀납법은 사례가 많이 들어맞는다는 경험적 관찰이 아니라 시작점에서 출발해 한 단계씩 전진하는 논리적 연결을 증명하는 방법이다. 이 장은 보통 귀납법에서 출발하여 강한 귀납법과 자연수의 정렬성이 귀납법과 동치임을 보이고, 자연수 재귀 정리로 재귀적 정의가 실제로 유일한 함수를 결정함을 증명한다. 이어 논리식이나 나무처럼 생성 규칙을 가진 대상에 대한 구조적 귀납, 재귀 알고리즘의 부분 정확성과 전체 정확성의 구별, 귀납 가정을 강화하는 전략을 차례로 다룬다. 이 장에서 자연수 집합 $\mathbb{N}$은 0을 포함하며, 시작값이 1인 명제는 그 적용 범위를 별도로 명시한다. 선행 지식: 자연수의 순서와 기본 연산, 함수, 증명의 기본 구조(제4권 제5장).

6.1 보통 귀납법과 시작점

정리 6.1 (수학적 귀납법) 자연수 n에 관한 성질 $P(n)$이 다음 두 조건을 만족하면 모든 $n \in \mathbb{N}$에 대해 $P(n)$이 성립한다.

(1) $P(0)$이 성립한다.

(2) 임의의 $n \in \mathbb{N}$에 대해 $P(n)$이면 $P(n+1)$이다.

이 정리는 여기서는 자연수의 기본 원리로 사용한다. 집합론에서 자연수를 구성하는 단계에서는 $\mathbb{N}$의 최소 귀납적 집합 성질로부터 이를 증명할 수 있다(제5권 제3장). 지금 전제로 사용하는 자연수의 성질과 나중에 그 성질을 구성에서 도출하는 작업을 혼동하지 않는다.

참고 (귀납 가정). 정리 6.1의 두 번째 조건을 보이는 증명 안에서, 고정된 n에 대해 $P(n)$이 성립한다고 두는 가정을 **귀납 가정**(*induction hypothesis*)이라고 한다. 귀납 가정은 증명하려는 전체 명제 "모든 n에서 $P(n)$"을 다시 가정하는 것이 아니라, 조건문 $P(n) \to P(n+1)$을 증명하는 동안 고정된 하나의 n에 대해서만 임시로 사용하는 가정이다.

예제 6.2 (등차합) 모든 $n \in \mathbb{N}$에 대해

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

이다.

증명. $n = 0$에서 왼쪽은 빈 합 0이고 오른쪽도 0이다. n에서 성립한다고 가정하면

$$\sum_{k=1}^{n+1} k = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2}$$

이므로 다음 단계에서도 성립한다. □

시작값이 n_0이면 $P(n_0)$와 $P(n) \to P(n+1)$을 모든 $n \ge n_0$에서 보이면 된다. 시작점은 실제 주장 범위에 포함되어야 한다. 시작점만 성립하고 연결 단계가 끊기거나, 연결 단계만 성립하고 출발할 참인 사례가 없으면 결론을 얻을 수 없다.

> **예제 6.3 (거짓 명제를 유지하는 연결)** $P(n)$을 "$n \ge n+1$"로 두면 $P(n)$은 모든 n에서 거짓이다. 따라서 조건문 $P(n) \to P(n+1)$ 자체는 모든 n에서 참이다. 그러나 $P(0)$이 거짓이므로 귀납법의 가정을 만족하지 않는다. 귀납 단계만 증명했다고 해서 전체 명제가 참이 되는 것은 아니다.

6.2 부등식의 귀납과 가정 사용

> **명제 6.4 (베르누이 부등식)** 실수 $x \ge -1$과 자연수 n에 대해
>
> $$(1+x)^n \ge 1 + nx \tag{6.1}$$
>
> 이다.

증명. $x \ge -1$을 고정하고 n에 관해 귀납한다. $n = 0$에서는 양변이 1이다. 귀납 가정에 $1 + x \ge 0$을 곱하면 부등호 방향이 유지되어

$$(1+x)^{n+1} \ge (1+nx)(1+x) = 1 + (n+1)x + nx^2 \ge 1 + (n+1)x$$

이다. 마지막 단계에서는 $n \ge 0$과 $x^2 \ge 0$을 사용했다. □

이 증명에서는 귀납 가정의 오른쪽 $1+nx$가 양수일 필요는 없다. 부등호를 유지하려면 곱하는 수 $1+x$가 음이 아니면 충분하다. 어떤 가정을 정확히 어느 연산에 사용하는지 구별하면 불필요하게 강한 조건을 추가하지 않게 된다.

> **명제 6.5** 모든 정수 $n \ge 4$에 대해 $2^n \ge n^2$이다.

증명. $n = 4$에서 $16 = 16$이다. $n \ge 4$에서 성립한다고 가정하면 $2^{n+1} \ge 2n^2$이다. 이제

$$2n^2 - (n+1)^2 = n^2 - 2n - 1 = (n-1)^2 - 2 \ge 7 > 0$$

이므로 $2^{n+1} \ge (n+1)^2$이다. □

귀납 증명에서는 목표식을 귀납 가정과 비교해 무엇이 더 필요한지 찾는다. 위의 증명에서는 $2^{n+1} = 2 \cdot 2^n$을 이용한 뒤, 남은 목표가 $2n^2 \ge (n+1)^2$임을 드러냈다. 모든 부등식을 처음부터 전개하는 것보다 연결 지점을 먼저 찾는 것이 효과적이다.

6.3 강한 귀납법과 정렬성

> **정리 6.6 (강한 귀납법)** 각 $n \in \mathbb{N}$에 대해 "모든 $k < n$에서 $P(k)$가 성립하면 $P(n)$이 성립한다"를 증명했다고 하자. 그러면 모든 $n \in \mathbb{N}$에서 $P(n)$이 성립한다.

증명. $Q(n)$을 "모든 $k < n$에 대해 $P(k)$"로 둔다. $Q(0)$은 빈 범위의 전칭 명제이므로 참이다. $Q(n)$을 가정하면 주어진 조건으로 $P(n)$을 얻으므로 $Q(n+1)$이다. 보통 귀납법으로 모든 $Q(n)$이 참이고, 특히 $Q(n+1)$에서 $P(n)$을 얻는다. □

강한 귀납법(*strong induction*)은 더 강한 결론을 내는 별개의 신비한 원리가 아니다. 귀납 가정을 묶어 사용하는 보통 귀납법이다. 다음 단계를 증명하는 데 바로 앞의 경우만이 아니라 더 작은 여러 경우가 필요할 때 편리하다.

정리 6.7 모든 정수 $n \geq 2$는 유한 개의 소수의 곱으로 표현된다.

증명. $n \geq 2$에 대해 강한 귀납을 사용한다. n이 소수이면 한 개의 소수로 이루어진 곱이므로 끝난다. n이 소수가 아니면 $n = ab$, $2 \leq a < n$, $2 \leq b < n$인 정수 a, b가 있다. 귀납 가정으로 a, b는 각각 소수들의 유한 곱이므로 두 곱을 이어 붙이면 n의 소수 곱 표현을 얻는다. 가장 작은 경우 $n = 2$는 소수인 갈래에서 처리된다. □

흔한 오류. 이 증명은 소인수분해의 존재만 보인다. 소수 인자들의 순서를 제외한 유일성은 별도 정리이며, 보통 소수가 곱을 나누면 한 인자를 나눈다는 보조정리를 이용해 증명한다(제1권 제3장).

정리 6.8 (자연수의 정렬성) 자연수의 비어 있지 않은 모든 부분집합에는 최소 원소가 있다. 통상의 자연수 순서 성질을 전제하면 이 원리와 귀납법은 서로 도출할 수 있다.

증명. 귀납법을 가정하고, 비어 있지 않지만 최소 원소가 없는 집합 $S \subseteq \mathbb{N}$이 있다고 하자. $0 \notin S$이다. $0, \dots, n$이 모두 S 밖에 있으면 $n+1$도 S에 있을 수 없다. 있다면 앞에 S의 원소가 없으므로 최소 원소가 되기 때문이다. 귀납법에 따라 모든 자연수가 S 밖에 있으므로 S가 비어 있지 않다는 가정과 모순된다.

반대로 정렬성을 가정하고 귀납법의 두 조건을 만족하는 P가 모든 자연수에서 성립하지 않는다고 하자. 반례 집합에 최소 원소 m이 있다. $P(0)$이 참이므로 $m \neq 0$이고, m이 최소 반례이므로 m보다 작은 자연수는 모두 P를 만족하며 특히 자연수 $m-1$에서 P가 참이다. 귀납 단계로 $P(m)$을 얻어 모순이다. □

6.4 재귀적 정의의 존재와 유일성

정리 6.9 (자연수 재귀 정리) 집합 X, 원소 $a \in X$, 함수 $F : \mathbb{N} \times X \to X$가 주어졌다고 하자. 다음 조건을 만족하는 함수 $u : \mathbb{N} \to X$가 유일하게 존재한다.

$$u(0) = a, \qquad u(n+1) = F(n, u(n)). \tag{6.2}$$

증명. 유한한 초기 구간에서 값을 차례로 정한다. 먼저 $u_0 : \{0\} \to X$를 $u_0(0) = a$로 둔다. u_n이 $0, \dots, n$에서 정의되어 있으면 기존 값을 그대로 두고 $n+1$에서 $F(n, u_n(n))$을 추가해 u_{n+1}을 만든다. F가 함수이므로 추가할 값은 정확히 하나이다. 각 단계는 앞 단계를 확장하므로 서로 겹치는 부분에서 값이 일치한다. 이 유한 함수들의 그래프를 모두 합치면 정의역이 $\mathbb{N}$인 함수 u가 되며 요구된 재귀식을 만족한다.

유일성을 보이기 위해 다른 함수 v도 같은 조건을 만족한다고 하자. $u(0) = v(0) = a$이다. $u(n) = v(n)$이면 $u(n+1) = F(n, u(n)) = F(n, v(n)) = v(n+1)$이다. 귀납법으로 모든 n에서 같으므로 $u = v$이다. □

첫 부분의 유한 초기 함수들을 집합으로 모으는 과정은 통상의 집합론 안에서 수행한다. 이 권에서는 그 배경을 전제한다. 재귀식만 적었다고 해서 어떤 상황에서도 자동으로 대상을 정의하는 것은 아니다. 앞의 값에서 다음 값으로 가는 연산이 존재하고 유일해야 하며, 서로 충돌하는 조건을 동시에 주어서는 안 된다.

예제 6.10 $u(0) = 1$, $u(n+1) = 2u(n)$은 재귀 정리에 의해 유일한 수열을 정의한다. 귀납법으로 $u(n) = 2^n$임을 확인할 수 있다. 반면 "$u(n+1)^2 = u(n)$"만으로 다음 값을 정하면 실수 범위에서 양수의 제곱근 부호가 둘이라 유일하지 않을 수 있다. $u(n+1) \geq 0$ 같은 추가 조건이 필요하다. "$u(0) = 1$이고 $u(0) = 2$"는 시작점부터 충돌하여 존재하지 않는다.

두 개 이상의 이전 값을 쓰는 점화식은 상태 공간을 키워 일차 재귀로 바꿀 수 있다. **피보나치 수열**(*Fibonacci sequence*)은

$$F_0 = 0, \qquad F_1 = 1, \qquad F_{n+2} = F_{n+1} + F_n \tag{6.3}$$

으로 정의한다. 쌍 (F_n, F_{n+1})를 하나의 상태로 보면 전이 함수는 $(a, b) \mapsto (b, a+b)$이다. 따라서 앞의 재귀 정리를 $X = \mathbb{N}^2$에 적용할 수 있다.

명제 6.11 피보나치 수열에 대해 모든 $n \in \mathbb{N}$에서

$$\sum_{k=0}^{n} F_k = F_{n+2} - 1$$

이다.

증명. $n = 0$이면 $F_0 = 0 = F_2 - 1$이다. n에서 성립한다고 가정하면

$$\sum_{k=0}^{n+1} F_k = F_{n+2} - 1 + F_{n+1} = F_{n+3} - 1$$

이므로 다음 단계에서도 성립한다. □

6.5 구조적 귀납: 식과 나무

자연수에서의 귀납은 "작은 수에서 큰 수"로 이동한다. 논리식이나 나무에서는 "구성 부분에서 전체"로 이동한다. 이를 **구조적 귀납**(*structural induction*)이라고 하며, 대상의 생성 규칙에 맞추어 기초 경우와 각 생성자 경우를 확인한다.

정의 6.12 변수와 상수로 시작하고 단항 부정 및 이항 연결사로 구성한 논리식에 대해, $a(\varphi)$를 원자 또는 상수의 출현 횟수, $b(\varphi)$를 이항 연결사의 출현 횟수라 하자. 같은 변수가 여러 번 나타나면 각 출현을 따로 센다.

명제 6.13 모든 이러한 논리식에 대해 $a(\varphi) = b(\varphi) + 1$이다. 단항 부정의 개수는 이 등식에 영향을 주지 않는다.

증명. 원자식 또는 상수 하나에서는 $a = 1, b = 0$이다. $\varphi = \neg\psi$이면 두 개수는 ψ와 같으므로 귀납 가정으로 성립한다. $\varphi = (\psi \circ \chi)$이면

$$a(\varphi) = a(\psi) + a(\chi), \qquad b(\varphi) = b(\psi) + b(\chi) + 1.$$

귀납 가정 $a(\psi) = b(\psi) + 1$, $a(\chi) = b(\chi) + 1$을 대입하면 $a(\varphi) = b(\varphi) + 1$이다. 모든 생성 규칙을 처리했으므로 증명이 끝난다. □

> **예제 6.14** $\neg(p \wedge q) \to (p \vee r)$에는 원자 출현이 4개이고 이항 연결사가 3개이다. 서로 다른 변수는 p, q, r의 3개이지만, 명제 6.13에서 세는 것은 변수 종류가 아니라 출현 횟수이다. 수식의 길이나 나무의 잎 수를 셀 때 이 차이를 분명히 해야 한다.

구조적 귀납은 유한 구문에서 성립한다. 무한한 나무나 순환하는 그래프를 같은 규칙으로 다루려면 추가 원리가 필요하다. “모든 부분에서 참이면 전체에서 참”이라는 말만으로 순환적인 대상을 정당화할 수는 없다.

6.6 종료와 정확성을 분리한 알고리즘 증명

재귀 프로그램이나 반복 절차를 검증할 때는 두 질문을 나눈다. 첫째는 종료할 때 답이 맞는가이고, 둘째는 모든 허용 입력에서 실제 종료하는가이다. 첫째만 보인 것을 **부분 정확성**(*partial correctness*), 종료까지 보인 것을 **전체 정확성**(*total correctness*)이라고 부른다.

> **예제 6.15 (유클리드 알고리즘)** 입력은 정수 $a \geq 0$, $b > 0$이다. 현재 쌍 (a, b)에서 나눗셈 알고리즘으로 $a = bq + r$, $0 \leq r < b$를 구한다. $r = 0$이면 b를 출력한다. $r > 0$이면 (a, b)를 (b, r)로 바꾸고 반복한다.

명제 6.16 이 알고리즘은 종료하고, 양의 최대공약수를 출력한다.

증명. 양의 공약수의 집합이 단계마다 보존됨을 먼저 보인다. $a = bq + r$이면 양의 정수 d에 대해

$$d \mid a \text{ 및 } d \mid b \quad \Longleftrightarrow \quad d \mid b \text{ 및 } d \mid r.$$

왼쪽이면 $r = a - bq$를 나누고, 오른쪽이면 $a = bq + r$를 나누기 때문이다. 따라서 마지막 단계에서 나머지가 0이면 공약수들은 b의 양의 약수들과 같고 그중 가장 큰 수는 b이다.

종료하지 않는다고 가정하면 각 반복에서 둘째 성분이 양의 정수이면서 이전보다 엄격히 작아진다. 이렇게 무한히 감소하는 자연수열은 존재할 수 없다. 실제로 그 값들의 집합에는 최소 원소가 있어야 하는데 그 다음 값이 더 작아 모순이다. 따라서 유한 단계 후 종료하며, 보존된 공약수 성질에 의해 출력은 원래 입력의 최대공약수이다. □

이 예에서 공약수 집합의 보존은 **불변식**(*invariant*), 둘째 성분의 감소는 **종료 척도**(*termination measure*)이다. 불변식만으로 종료가 보장되지는 않고, 감소하는 양을 찾았어도 그 양이 아래로 무한히 내려갈 수 없는 범위에 있어야 한다. 실수 $1, 1/2, 1/4, \ldots$는 엄격히 감소하지만 무한히 이어진다.

6.7 매개변수를 강화하는 귀납

처음 주어진 목표를 그대로 귀납 가정으로 쓰면 다음 단계에 필요한 정보가 부족할 때가 있다. 이때 목표를 더 강한 명제로 바꾸어 증명하는 전략이 유용하다. 더 강한 명제가 증명하기 더 어려울 것처럼 보이지만, 귀납 단계에서 더 풍부한 가정을 사용할 수 있다는 이점이 있다.

예제 6.17 (기록을 함께 보존하는 수열) 피보나치 수열에서 $F_n \le 2^n$만 보여도 되지만, 재귀는 F_{n+1}과 F_n을 함께 쓴다. $P(n)$을

$$F_n \le 2^n \quad \text{및} \quad F_{n+1} \le 2^{n+1}$$

이라는 두 주장으로 두면 다음 단계의 첫 주장은 현재 둘째 주장이고, 다음 둘째 주장은

$$F_{n+2} = F_{n+1} + F_n \le 2^{n+1} + 2^n \le 2^{n+2}$$

에서 나온다. 시작점 $n = 0$도 즉시 확인된다. 상태를 묶는 생각은 재귀 정의에서 쌍을 사용한 것과 같다.

강화는 필요 없이 복잡한 목표를 붙이는 작업이 아니다. 다음 단계에서 실제 필요한 정보가 무엇인지 역으로 추적해 넣는다. 알고리즘의 불변식을 찾거나 구조적 귀납에서 보조 명제를 동시에 증명하는 경우에도 같은 전략을 쓴다.

6.8 연습문제와 해설

연습문제 6.18 모든 $n \in \mathbb{N}$에 대해 $\sum_{k=1}^{n} (2k-1) = n^2$임을 귀납법으로 증명하라.

풀이. $n = 0$에서 빈 합은 0이다. n에서 성립하면 다음 합은 $n^2 + (2(n+1)-1) = n^2 + 2n + 1 = (n+1)^2$이다. 새로 더해지는 항을 $2n-1$로 잘못 쓰지 않도록 합의 상한이 $n+1$이라는 점을 확인한다.

연습문제 6.19 귀납 단계가 $P(n) \to P(n+2)$뿐일 때 $P(0)$만으로 모든 자연수의 P를 결론 내릴 수 있는가? 필요한 시작 조건을 설명하라.

풀이. $P(0)$만으로는 짝수 경우만 연결된다. $P(n)$을 "n은 짝수"로 잡으면 단계와 $P(0)$은 참이지만 홀수 경우는 거짓이다. 모든 자연수에 대해 주장하려면 $P(0)$과 $P(1)$을 모두 확인하면 충분하다. 두 갈래에서 각각 두 칸씩 이동한다.

연습문제 6.20 $u(0) = 3$, $u(n+1) = u(n) + 2$인 수열의 닫힌 식을 구하고 증명하라.

풀이. $u(n) = 2n + 3$이다. $n = 0$에서 맞고, $u(n) = 2n + 3$이면 $u(n+1) = 2n + 5 = 2(n+1) + 3$이다. 재귀 정리로 수열의 존재와 유일성이 확보되고, 귀납법으로 그 수열이 제시한 닫힌 식과 같음을 확인한다. 닫힌 식을 추측한 것과 그 추측을 검증한 것은 별도의 단계이다.

연습문제 6.21 양의 정수만으로 이루어진 무한히 엄격한 감소 수열이 없음을 정렬성으로 증명하라. 실수에서는 어떤 반례가 있는가?

풀이. 그런 자연수열 (a_n)이 있다면 값들의 비어 있지 않은 집합에 최소 원소 a_m이 있다. 하지만 $a_{m+1} < a_m$이므로 모순이다. 실수에서는 $a_n = 2^{-n}$이 양수이며 무한히 엄격히 감소한다. 따라서 "계속 감소한다"만으로 종료를 주장하면 범위 조건을 빠뜨린 것이다.

연습문제 6.22 잎 하나 또는 두 나무를 새 뿌리 아래 붙이는 규칙으로 만든 유한 완전 이진나무에서 잎 수가 내부 꼭짓점 수보다 하나 많음을 증명하라.

풀이. 잎 하나에서는 잎 수 1, 내부 꼭짓점 수 0이다. 두 나무에서 각각 $L_1 = I_1 + 1$, $L_2 = I_2 + 1$이라 하자. 새 나무의 잎 수는 $L_1 + L_2$, 내부 꼭짓점 수는 $I_1 + I_2 + 1$이므로 차이는 1이다. 여기서 완전 이진나무는 각 내부 꼭짓점의 자식이 정확히 둘인 나무라는 뜻으로 사용했다.

연습문제 6.23 "모든 유한 집합의 원소는 같은 색이다"라는 다음 귀납 논증의 오류를 찾으라. 한 원소 집합에서는 참이다. $n+1$개 원소에서 첫 원소를 뺀 n개와 마지막 원소를 뺀 n개는 각각 같은 색이고, 두 부분집합이 겹치므로 전체가 같은 색이라는 논증이다.

풀이. $n = 1$에서 $n+1 = 2$로 넘어갈 때 두 부분집합의 교집합이 비어 있다. 공통 원소의 색으로 두 집단의 색을 연결할 수 없다. 귀납 단계의 논리가 $n \geq 2$에서만 작동하므로 시작점 1과 연결되지 않는다. 귀납 가정 자체를 반복해서 말하는 것보다 각 단계의 실제 연결을 검사해야 한다.

연습문제 6.24 유클리드 알고리즘으로 $\gcd(252, 105)$를 구하고 각 나머지의 범위를 확인하라.

풀이. $252 = 2 \cdot 105 + 42$, $105 = 2 \cdot 42 + 21$, $42 = 2 \cdot 21 + 0$이다. 나머지들은 각각 $0 \leq 42 < 105$, $0 \leq 21 < 42$, $0 \leq 0 < 21$을 만족한다. 마지막 양의 나누는 수가 21이므로 최대공약수는 21이다. 중간 나머지 중 아무것이나 답으로 택하는 것이 아니라, 나머지가 0이 되는 단계의 나누는 수를 출력한다.

연습문제 6.25 논리식에서 부정의 개수 u, 이항 연결사의 개수 b, 원자 출현의 개수 a를 셀 때 전체 구문 나무 꼭짓점 수를 b, u만으로 표현하라.

풀이. 전체 수는 $a + b + u$이다. 앞에서 증명한 $a = b + 1$을 대입하면 $2b + u + 1$이다. 원자 종류가 아니라 원자 출현을 세므로 같은 변수가 여러 위치에 쓰인 경우도 올바르게 계산한다. 이 등식은 수식 구문 분석 결과를 검사하는 간단한 불변식으로도 쓸 수 있다.

다음 장에서는 관계와 동치류를 사용하여 몫집합을 구성한다(제4권 제7장).

제 7 장

관계, 분할, 몫집합

개요 이항관계는 두 집합의 원소 사이의 대응을 순서쌍의 집합으로 기록한 것이고, 그 가운데 반사성·대칭성·추이성을 모두 만족하는 동치관계는 서로 "같다고 볼" 원소들을 하나의 부류로 묶는 관계이다. 같은 나머지를 갖는 정수, 같은 방향을 가리키는 벡터, 서로 도달할 수 있는 그래프의 꼭짓점은 모두 관계로 표현할 수 있다. 이 장은 관계의 역·합성과 그 성질에서 출발하여, 동치관계의 동치류가 바탕집합의 분할과 정확히 대응함을 증명하고, 몫집합과 표준 몫사상, 몫집합 위에 함수를 내려보내는 보편 성질을 세운다. 이어 임의의 관계를 포함하는 가장 작은 동치관계(생성되는 동치관계)와 두 동치관계 사이의 세분 관계를 다룬다. 이 장의 목표는 "같다고 생각한다"는 말을 실제 집합과 함수의 구성으로 바꾸는 것이다. 선행 지식: 집합의 포함과 연산, 전칭·존재 양화, 함수와 순서쌍의 기본 개념. 집합의 등식은 원소가 정확히 같다는 뜻으로 사용한다.

7.1 관계의 형식과 연산

정의 7.1 집합 X에서 집합 Y로의 **이항관계**(*binary relation*)는 부분집합 $R \subseteq X \times Y$이다. $(x,y) \in R$를 xRy로 줄여 쓴다. $X = Y$이면 X 위의 관계라 한다. **역관계**와 **합성**은

$$R^{-1} = \{(y,x) : (x,y) \in R\}, \qquad S \circ R = \{(x,z) : \exists y \in Y\ (xRy \wedge ySz)\}$$

로 정의한다. 합성에서 $R \subseteq X \times Y$, $S \subseteq Y \times Z$이다.

관계의 합성은 중간 증인이 존재하는지 묻는다. R을 "직접 기차로 이동할 수 있다", S를 "직접 버스로 이동할 수 있다"로 해석하면 $S \circ R$는 기차를 탄 뒤 버스로 이동할 수 있음을 뜻한다. 화살표를 읽는 실제 순서와 합성 기호의 오른쪽부터 적용하는 순서를 구별한다.

명제 7.2 관계의 합성은 결합법칙을 만족한다. 즉, 적절한 집합 사이의 관계 R, S, T에 대해

$$T \circ (S \circ R) = (T \circ S) \circ R.$$

증명. (x,w)가 왼쪽에 속할 조건을 풀면, 어떤 z에 대해 $(x,z) \in S \circ R$이고 zTw이다. 이는 어떤 y, z에 대해 xRy, ySz, zTw라는 뜻이다. 같은 두 증인을 먼저 y에 관해 묶으면 오른쪽의 소속 조건이 된다. 모든 시작점과 끝점에 대해 조건이 같으므로 관계가 같다. □

대각관계 $\Delta_X = \{(x,x) : x \in X\}$는 항등원 역할을 한다. $R \subseteq X \times Y$이면 $R \circ \Delta_X = R = \Delta_Y \circ R$이다. 또한 $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$이다. 역관계를 취하면 이동 방향이 뒤집히므로 합성 순서도 뒤집힌다. 관계는 함수보다 넓은 개념이어서 한 입력에 출력이 없거나 여러 개 있어도 허용한다.

예제 7.3 $X = \{1,2,3\}$에서 $R = \{(1,2),(2,3)\}$라 하자. $R \circ R = \{(1,3)\}$이고 $R^{-1} = \{(2,1),(3,2)\}$이다. $R \cup R^{-1}$는 대칭적인 연결을 나타내지만, $(1,3)$이 없으므로 추이적이지 않다. 역관계를 더하는 것만으로 모든 경로의 연결이 포함되지는 않는다.

7.2 관계의 성질과 독립적인 검사

정의 7.4 X 위의 관계 R에 대해 다음과 같이 정의한다.

$$\begin{aligned} \text{반사적:}\quad & \forall x \in X\,(xRx),\\ \text{대칭적:}\quad & \forall x,y \in X\,(xRy \to yRx),\\ \text{반대칭적:}\quad & \forall x,y \in X\,((xRy \wedge yRx) \to x = y),\\ \text{추이적:}\quad & \forall x,y,z \in X\,((xRy \wedge yRz) \to xRz). \end{aligned}$$

반사성, **대칭성**, **반대칭성**, **추이성**은 서로의 부정이 아니다. 대각관계는 둘 다 만족한다. 서로 다른 두 원소만 양방향으로 연결한 관계는 대칭적이지만 반대칭적이지 않고, 엄격한 대소관계는 대칭적이지 않지만 반대칭 조건을 만족한다. "대칭이 아니면 반대칭"이라는 이분법은 성립하지 않는다.

반사성은 전체 바탕 집합에 관한 성질이다. 예를 들어 $R = \{(0,0)\}$는 $\{0\}$ 위에서는 반사적이지만 $\{0,1\}$ 위에서는 반사적이지 않다. 관계의 순서쌍 목록만 적고 바탕 집합을 생략하면 이런 성질의 판정이 모호해질 수 있다.

예제 7.5 실수에서 xRy를 $|x-y|<1$로 정의하자. 이 관계는 반사적이고 대칭적이다. 하지만 $0R(3/4)$와 $(3/4)R(3/2)$가 성립하면서 $0R(3/2)$는 성립하지 않으므로 추이적이지 않다. "아주 가깝다"를 반복하면 누적된 거리는 커질 수 있다. 근접성과 동치성을 같은 방식으로 다루면 안 되는 이유이다.

명제 7.6 R가 대칭적이고 추이적이며 모든 $x \in X$에 대해 xRy인 $y \in X$가 존재하면 R는 반사적이다.

증명. 임의의 x에 대해 xRy인 y를 고른다. 대칭성으로 yRx이고, 두 관계를 추이성으로 연결하면 xRx이다. 모든 x에 대해 성립한다. □

주의. 존재 조건을 빼면 명제 7.6는 거짓이다. 공관계는 대칭적이고 추이적이지만, 비어 있지 않은 집합 위에서는 반사적이지 않다. 성질을 결합할 때 누락된 원소가 있는지 확인하는 것이 간단하면서도 유용한 반례 탐색법이다.

7.3 동치류와 분할의 대응

정의 7.7 반사적·대칭적·추이적인 관계를 **동치관계**(*equivalence relation*)라 하고 보통 $\sim$로 쓴다. $x \in X$의 **동치류**(*equivalence class*)는

$$[x] = \{y \in X : y \sim x\}$$

이다. X의 **분할**(*partition*)은 공집합이 아닌 부분집합들의 모임 $\mathcal{P}$로서, 그 합집합이 X이고 서로 다른 두 원소가 서로소인 것이다. $X = \emptyset$의 분할은 빈 모임으로 허용한다.

정리 7.8 동치관계의 동치류들은 X의 분할을 이룬다. 특히

$$x \sim y \iff [x] = [y], \qquad [x] \cap [y] \neq \emptyset \implies [x] = [y]. \tag{7.1}$$

반대로 분할이 주어지면 "같은 부분집합에 속한다"는 관계가 동치관계이고 그 동치류가 원래 분할의 원소들이다.

증명. 반사성으로 $x \in [x]$이므로 각 동치류는 비어 있지 않고 모든 원소가 어느 동치류에 속한다. $x \sim y$이고 $z \in [x]$이면 $z \sim x \sim y$이므로 $z \in [y]$이다. 대칭성을 사용해 역포함도 얻어 $[x] = [y]$이다. 반대로 $[x] = [y]$이면 $x \in [x] = [y]$이므로 $x \sim y$이다.

$z \in [x] \cap [y]$가 있다면 $z \sim x$, $z \sim y$이다. 대칭성과 추이성으로 $x \sim y$이므로 두 류가 같다. 따라서 서로 다른 류는 서로소이다.

이제 분할 $\mathcal{P}$를 주고 $x \sim y$를 x, y가 같은 분할 원소에 속함으로 정의하자. 모든 x가 한 분할 원소에 속하므로 반사적이고, 정의가 두 원소에 대해 대칭적이다. x, y를 포함하는 분할 원소와 y, z를 포함하는 분할 원소는 y에서 만나므로 같은 부분집합이다. 따라서 x, z도 함께 들어 있어 추이성이 성립한다. 각 동치류는 해당 원소가 속한 분할 원소와 정확히 같다. □

이 대응은 관계와 집합 모임이라는 두 표현이 같은 정보를 담는다는 뜻이다. 증명할 때는 관계 표현이 편하고, 결과를 나누어 볼 때는 분할 표현이 편할 수 있다. 동치류 $[x]$를 대표원 x와 혼동하지 않는다. $[x]$는 보통 여러 원소를 포함하는 집합이다.

예제 7.9 (정수의 나머지) $m \geq 1$을 고정하고 $a \sim b$를 $m \mid (a - b)$로 정의하면 동치관계이다. 나눗셈 알고리즘에 의해 각 정수는 $0, \dots, m-1$ 중 정확히 하나와 동치이므로 분할은 m개의 류로 이루어진다. "대표원을 $0, \dots, m-1$로 정한다"는 말은 다른 정수가 사라진다는 뜻이 아니라 각 류를 표시할 표준 이름을 고른다는 뜻이다.

7.4 생성되는 동치관계

주어진 관계 R 자체는 동치관계가 아닐 수 있다. 그래도 R의 모든 연결을 유지하면서 동치관계가 되도록 필요한 연결을 추가할 수 있다.

명제 7.10 X 위에서 R를 포함하는 모든 동치관계의 교집합은 R를 포함하는 가장 작은 동치관계이다.

증명. 전체 관계 $X \times X$가 동치관계이므로 교집합을 취할 대상이 적어도 하나 있다. 반사성, 대칭성, 추이성은 각 관계에서 성립하면 교집합에서도 성립한다. 예를 들어 교집합에서 $x \sim y$, $y \sim z$이면 모든 구성 관계에 두 순서쌍이 들어 있으므로 모든 관계의 추이성으로 (x, z)도 들어 있다. 따라서 교집합은 동치관계이다. 정의상 R를 포함하고, 다른 어떤 후보에도 포함되므로 가장 작다. □

더 구체적으로는 R의 연결을 양방향으로 사용한 유한 경로로 설명할 수 있다. $x \approx y$를 $x = y$이거나, 어떤 유한열 $x = x_0, x_1, \dots, x_n = y$의 이웃한 두 원소마다 $x_i R x_{i+1}$ 또는 $x_{i+1} R x_i$가 성립함으로 정의한다. 길이 0인 경로가 반사성을, 경로 뒤집기가 대칭성을, 경로 이어 붙이기가 추이성을 준다. R를 포함하는 모든 동치관계는 이러한 유한 경로의 두 끝점을 동치로 만들어야 하므로 $\approx$가 바로 가장 작은 동치관계이다.

예제 7.11 $X = \{a, b, c, d, e\}$에서 $R = \{(a,b), (c,b), (d,e)\}$이면 생성되는 동치관계의 류는 $\{a, b, c\}$와 $\{d, e\}$이다. 처음 목록에 (a, c)가 없었어도 a, b, c를 연결하는 경로가 있기 때문에 같은 류가 된다. 집합의 크기가 유한하면 연결 성분을 구하는 문제로 바뀐다.

주의. 동치관계의 합집합은 일반적으로 동치관계가 아니다. 각각의 관계 안에서 가능한 연결을 섞어 새 경로를 만들면 그 끝점을 잇는 쌍이 합집합에 없을 수 있다. 관계들의 합집합으로부터 동치관계를 만들고 싶다면 다시 동치관계 생성을 수행해야 한다.

7.5 몫집합과 함수가 내려가는 조건

정의 7.12 동치관계 $\sim$에 대한 **몫집합**(*quotient set*)은 동치류들의 집합

$$X/{\sim} = \{[x] : x \in X\}$$

이다. 함수 $q : X \to X/{\sim}$, $q(x) = [x]$를 **표준 몫사상**(*canonical quotient map*)이라 한다. 모든 동치류는 어떤 x에서 나오므로 q는 전사이다.

정리 7.13 (몫집합의 보편 성질) 함수 $f : X \to Y$에 대해 다음 두 조건은 동치이다.

(1) $x \sim x'$이면 $f(x) = f(x')$이다.

(2) $f = \bar{f} \circ q$를 만족하는 함수 $\bar{f} : X/{\sim} \to Y$가 유일하게 존재한다.

증명. 첫 조건이 성립하면 $\bar{f}([x]) = f(x)$로 정의한다. 같은 동치류의 다른 대표를 택해도 첫 조건 때문에 값이 같으므로 잘 정의된다. 모든 x에 대해 $\bar{f}(q(x)) = f(x)$이다. 다른 함수 h도 같은 합성 조건을 만족하면 각 동치류 $[x]$에서 $h([x]) = f(x) = \bar{f}([x])$이므로 유일하다.

반대로 $f = \bar{f} \circ q$이면 $x \sim x'$일 때 $q(x) = q(x')$이고 따라서 $f(x) = \bar{f}(q(x)) = \bar{f}(q(x')) = f(x')$이다. □

이 정리는 대표원을 실제로 하나씩 선택하지 않고도 몫집합 위의 함수를 정의하는 기준을 준다. 모든 대표가 같은 값을 준다는 사실이 더 중요하다. 대표원 하나를 임의로 골랐다는 말은 그 값이 선택에 무관하다는 증명을 대신하지 못한다.

예제 7.14 정수의 m에 대한 합동류에서 $[a] \mapsto [a^2]$는 잘 정의된다. $a \sim a'$, 곧 $m \mid (a - a')$이면 $a^2 - a'^2 = (a - a')(a + a')$도 m의 배수이기 때문이다. 하지만 $[a] \mapsto a^2$를 정수값 함수로 정의하면 보통 실패한다. $a = 0$과 $a = m$은 같은 류인데 제곱은 0과 m^2로 다르다. 출력이 정수인지 합동류인지에 따라 결론이 달라진다.

7.6 동치관계의 세분과 정보의 손실

두 동치관계 $\sim_1, \sim_2$에 대해 $\sim_1 \subseteq \sim_2$이면 첫 관계의 류가 둘째 관계의 류보다 더 잘게 나뉜다. 같은 것으로 취급하는 쌍을 늘리면 구분할 수 있는 정보는 줄어든다. 이때

$$\pi : X/{\sim_1} \longrightarrow X/{\sim_2}, \qquad \pi([x]_1) = [x]_2$$

가 잘 정의된 전사이다. $[x]_1 = [y]_1$이면 $x \sim_1 y$이고 따라서 $x \sim_2 y$이므로 잘 정의된다.

예제 7.15 정수에서 법 6의 합동은 법 3의 합동을 함의한다. 따라서 여섯 개의 나머지 류를 세 개의 나머지 류로 보내는 함수가 있다. $[0]_6, [3]_6$은 모두 $[0]_3$로, $[1]_6, [4]_6$은 $[1]_3$로, $[2]_6, [5]_6$은 $[2]_3$로 간다. 반대로 법 3의 류 하나만 알아서는 법 6의 류를 유일하게 복원할 수 없다.

7.7 연습문제와 해설

연습문제 7.16 $\mathbb{Z}$에서 aRb를 $a-b$가 짝수임으로 정의하라. 동치관계의 세 조건을 검사하고 몫집합을 적으라.

풀이. $a-a=0$은 짝수이므로 반사적이다. $a-b=2k$이면 $b-a=2(-k)$이므로 대칭적이다. $a-b=2k$, $b-c=2\ell$이면 $a-c=2(k+\ell)$이므로 추이적이다. 몫집합은 짝수 전체의 류와 홀수 전체의 류라는 두 원소를 가진다. 원래 집합은 무한하지만 몫집합은 유한하다.

연습문제 7.17 $X=\{1,2,3\}$에서 두 분할 $\{\{1,2\},\{3\}\}$와 $\{\{1\},\{2,3\}\}$가 주는 동치관계의 합집합이 추이적이지 않음을 보이라.

풀이. 합집합에는 $1\sim 2$와 $2\sim 3$이 있지만 $1\sim 3$은 어느 관계에도 없다. 따라서 추이성이 실패한다. 합집합이 생성하는 동치관계는 세 원소를 모두 하나의 류로 묶는다.

연습문제 7.18 임의의 함수 $f: X\to Y$에 대해 $x\sim x'$를 $f(x)=f(x')$로 정의하면 동치관계임을 보이라. 그 동치류를 함수의 관점에서 설명하라.

풀이. 등호의 반사성·대칭성·추이성을 그대로 적용하면 된다. x의 류는 $f^{-1}(\{f(x)\})$, 즉 x와 같은 출력값을 갖는 입력들의 집합이다. 이것을 해당 출력 위의 **섬유**(*fiber*)라고 부른다. 다음 장에서는 이 몫집합과 함수의 상이 자연스럽게 일대일 대응함을 보인다.

연습문제 7.19 $\mathbb{R}$에서 $x\sim y$를 $x-y\in\mathbb{Z}$로 정의하자. 각 동치류에 $[0,1)$의 원소가 정확히 하나 있음을 보이라. 정수부분의 존재를 사용해도 된다.

풀이. 정수 n을 $n\le x<n+1$이 되도록 잡으면 $r=x-n\in[0,1)$이고 $x\sim r$이다. $r,s\in[0,1)$가 동치이면 $r-s$는 정수이면서 $-1<r-s<1$이므로 $r-s=0$이다. 따라서 대표는 유일하다. 반닫힌 구간을 쓴 이유는 0과 1이 같은 류인데 두 대표를 동시에 허용하지 않기 위해서이다.

연습문제 7.20 동치관계 $\sim$에서 "각 류의 원소 개수가 같다"가 항상 성립하는지 판정하라.

풀이. 성립하지 않는다. $X=\{a,b,c\}$를 $\{a\}$와 $\{b,c\}$로 분할하면 크기가 1과 2인 동치류를 얻는다. 합동류나 군의 특정 몫에서 류들의 크기가 같아지는 현상에는 추가 대수 구조가 사용된다(제14권 제2장). 동치관계의 정의만으로는 보장되지 않는다.

연습문제 7.21 $R\subseteq X\times X$의 역관계를 다시 취하면 R가 됨을 보이고, R가 대칭일 필요충분조건을 역관계로 표현하라.

풀이. $(x,y)\in (R^{-1})^{-1}$일 조건은 $(y,x)\in R^{-1}$이고 이는 $(x,y)\in R$와 같다. 따라서 두 번 뒤집으면 원래 관계이다. 대칭성은 $R\subseteq R^{-1}$와 같고, 역을 취하면 반대 포함도 얻으므로 $R=R^{-1}$와 동치이다.

다음 장에서는 함수의 섬유, 상, 역함수와 집합의 크기 비교를 이 동치류의 관점으로 정리한다(제4권 제8장).

제 8 장

함수, 섬유, 역함수와 크기 비교

개요 이 장은 함수를 그래프·상·섬유로 분석하여 단사성과 전사성을 섬유의 크기로 특징짓고(8.1–8.2절), 몫집합을 통한 함수의 표준분해를 세운다(8.3절). 이어 왼쪽 역·오른쪽 역의 존재와 선택공리의 관계를 밝히고(8.4절), 유한집합에서는 비둘기집 원리로 단사·전사·전단사가 일치함을 보인 뒤(8.5절), 두 단사로부터 전단사를 구성하는 슈뢰더-베른슈타인 정리(8.6절)와 멱집합이 항상 더 크다는 칸토어의 대각선 논증(8.7절)으로 무한집합의 크기 비교를 마무리한다. 이 장에서는 모든 함수가 정의역 전체에서 정의된 것으로 한다. 선행 지식: 함수의 정의역·공역, 단사·전사, 집합의 상과 역상, 동치관계와 몫집합(제4권 제7장).

함수는 입력마다 출력을 하나 정하지만, 서로 다른 입력을 같은 출력으로 보낼 수 있고 공역의 일부를 전혀 방문하지 않을 수도 있다. 이 두 현상이 각각 단사성(*injectivity*)과 전사성(*surjectivity*)이 실패하는 방식이다. 함수를 섬유와 상으로 나누어 보면 어떤 정보가 합쳐지고 어떤 출력이 빠져 있는지가 드러난다.

8.1 그래프, 상, 섬유

정의 8.1 (그래프, 상, 섬유) 함수 $f : X \to Y$의 **그래프**(*graph*)는 $\{(x, f(x)) : x \in X\}$이다. 함수의 **상**(*image*)은 $f(X) = \{f(x) : x \in X\}$이고, $y \in Y$ 위의 **섬유**(*fiber*)는 $f^{-1}(\{y\})$이다. $A \subseteq X$에 대한 상과 $B \subseteq Y$에 대한 **역상**(*preimage*)은 각각

$$f(A) = \{f(x) : x \in A\}, \qquad f^{-1}(B) = \{x \in X : f(x) \in B\}$$

이다.

그래프와 함께 정의역·공역을 지정하여 함수를 논한다. 같은 대응식이라도 공역을 바꾸면 전사성이 바뀔 수 있다. 반면 단사성은 정의역 안의 두 입력을 비교하므로 공역을 상을 포함하는 더 큰 집합으로 바꿔도 변하지 않는다.

주의 (역상 기호의 쓰임). $f^{-1}(B)$는 f가 단사도 전사도 아니어도 항상 뜻이 있는 집합이다. 역함수 $f^{-1} : Y \to X$는 f가 전단사일 때에만 정의되는 함수이고, $f^{-1}(B)$는 그런 역함수의 존재와 무관하게 정의되는 집합이다. 같은 기호가 두 가지 다른 대상(집합의 역상과 함수로서의 역함수)을 가리키므로 문맥으로 구별해야 한다.

명제 8.2 f가 **단사**(*injective*)일 필요충분조건은 모든 섬유가 원소를 많아야 하나 갖는 것이다. f가 **전사**(*surjective*)일 필요충분조건은 모든 섬유가 비어 있지 않은 것이다. 따라서 f가 **전단사**(*bijective*)일 필요충분조건은 모든 섬유가 정확히 한 원소를 갖는 것이다.

각 문장은 단사·전사의 정의를 출력값별로 다시 묶은 것이다. 섬유를 그리거나 계산하면 함수의 성질을 빠르게 파악할 수 있다.

예제 8.3 $f:\mathbb{R}\to[0,\infty)$, $f(x)=x^2$의 0 위 섬유는 $\{0\}$이고 $y>0$ 위 섬유는 $\{-\sqrt{y},\sqrt{y}\}$이다. 따라서 전사이지만 단사는 아니다. 정의역을 $[0,\infty)$로 제한하면 모든 섬유가 하나의 원소가 되므로 전단사가 된다. 함수의 역을 정의할 때 왜 가지 또는 부호를 정해야 하는지 보여 주는 예이다.

8.2 상과 역상의 정밀한 법칙

정리 8.4 함수 $f:X\to Y$, 부분집합 $A\subseteq X$, $B\subseteq Y$에 대해

$$f(A)\subseteq B \iff A\subseteq f^{-1}(B) \tag{8.1}$$

이다. 또한

$$A\subseteq f^{-1}(f(A)), \tag{8.2}$$

$$f(f^{-1}(B))=B\cap f(X). \tag{8.3}$$

증명. 식 (8.1)의 동치는 A의 모든 원소 x가 $f(x)\in B$를 만족한다는 조건을 양쪽에서 읽은 것이다. $x\in A$이면 $f(x)\in f(A)$이므로 식 (8.2)의 포함이 성립한다. 식 (8.3)의 왼쪽 원소 y는 어떤 x의 출력이면서 $y\in B$이다. 이는 $y\in f(X)\cap B$와 정확히 같다. □

명제 8.5 모든 $A\subseteq X$에 대해 $f^{-1}(f(A))=A$일 필요충분조건은 f가 단사인 것이다. 모든 $B\subseteq Y$에 대해 $f(f^{-1}(B))=B$일 필요충분조건은 f가 전사인 것이다.

증명. 단사이면 $x\in f^{-1}(f(A))$에서 $f(x)=f(a)$인 $a\in A$를 얻고 단사성으로 $x=a\in A$이다. 역으로 등식이 모든 A에 성립하고 $f(x)=f(x')$이면 $A=\{x\}$에 대해 $x'\in f^{-1}(f(A))=\{x\}$이므로 $x'=x$이다.

전사성에 관한 방향은 식 (8.3)에서 따라온다. 모든 B에 대해 등식이면 특히 $B=Y$에서 $f(X)=Y$이다. □

역상은 임의의 합집합과 교집합을 보존하며 여집합도 공역과 정의역을 맞추어 보존한다.

$$f^{-1}(Y\setminus B)=X\setminus f^{-1}(B). \tag{8.4}$$

반면 상은 합집합을 보존하지만 교집합에 대해서는 일반적으로 포함만 보장한다. 상의 교집합 등식이 깨지는 원인은 서로 다른 입력이 같은 출력으로 합쳐질 수 있다는 데 있다.

예제 8.6 $f:\mathbb{R}\to\mathbb{R}$, $f(x)=x^2$에서 $A=[-1,0]$, $B=[0,1]$로 두면 $f(A)=[0,1]=f(B)$이므로 $f(A)\cap f(B)=[0,1]$이다. 그러나 $A\cap B=\{0\}$이므로 $f(A\cap B)=\{0\}\subsetneq f(A)\cap f(B)$이다. $-1\in A$와 $1\in B$가 같은 출력 1로 합쳐지는 것이 등식이 깨지는 원인이다.

예제 8.7 $f:\mathbb{Z}\to\mathbb{Z}$, $f(n)=2n$에서 B를 홀수 집합으로 두면 $f^{-1}(B)=\emptyset$이다. 따라서 $f(f^{-1}(B))=\emptyset\neq B$이다. 역상 기호가 "무조건 이전 상태를 복원한다"는 뜻이 아님을 보여 준다. 공역에 있는 모든 원소가 실제 출력은 아니다.

핵심 수식

$$f(A)\subseteq B \iff A\subseteq f^{-1}(B), \qquad A\subseteq f^{-1}(f(A)),$$
$$f(f^{-1}(B)) = B\cap f(X), \qquad f^{-1}(Y\setminus B) = X\setminus f^{-1}(B).$$

8.3 몫과 상을 통한 함수의 분해

정리 8.8 $f:X\to Y$에 대해 $x\sim x'$를 $f(x)=f(x')$로 정의하자. 그러면

$$\hat{f}: X/{\sim} \longrightarrow f(X), \qquad \hat{f}([x]) = f(x) \tag{8.5}$$

는 전단사이다. 따라서 f는 몫사상, 전단사, 포함함수의 합성으로 분해된다.

증명. 같은 동치류이면 출력값이 같다는 정의 때문에 잘 정의된다. $\hat{f}([x])=\hat{f}([x'])$이면 $f(x)=f(x')$, 즉 $x\sim x'$여서 두 류가 같으므로 단사이다. $f(X)$의 원소는 어떤 $f(x)$이므로 전사이다. 포함함수 $i:f(X)\hookrightarrow Y$를 쓰면 모든 x에서 $f(x)=i(\hat{f}(q(x)))$이다. □

이 분해는 함수를 세 단계로 구별한다. 몫사상은 같은 결과를 내는 입력을 하나로 묶고, 중간 전단사는 그 묶음에 출력 이름을 붙이며, 포함함수는 실제 출력들을 원래 공역 안에 놓는다. 대수학의 동형정리 (제14권 제2장)에서는 여기에 연산 보존이라는 추가 구조가 붙는다.

예제 8.9 정수 함수 $f(n)=n \bmod 3$을 공역 $\mathbb{Z}$의 함수로 생각하자. 첫 단계는 정수들을 세 합동류로 묶는다. 둘째 단계는 세 류를 $0,1,2$에 대응시킨다. 셋째 단계는 $\{0,1,2\}$를 $\mathbb{Z}$에 포함시킨다. 단사 실패와 전사 실패가 서로 다른 단계에 분리되어 있다.

8.4 왼쪽 역과 오른쪽 역, 그리고 선택

정의 8.10 (왼쪽 역과 오른쪽 역) $f:X\to Y$에 대해 $\ell:Y\to X$가 $\ell\circ f=\mathrm{id}_X$를 만족하면 **왼쪽 역**(*left inverse*), $r:Y\to X$가 $f\circ r=\mathrm{id}_Y$를 만족하면 **오른쪽 역**(*right inverse*)이라 한다. 두 등식을 동시에 만족하면 **역함수**이다.

명제 8.11 왼쪽 역이 있는 함수는 단사이고, 오른쪽 역이 있는 함수는 전사이다. 왼쪽 역과 오른쪽 역이 모두 있으면 두 역은 서로 같으며 역함수가 된다.

증명. $f(x)=f(x')$에 왼쪽 역 ℓ을 적용하면 $x=x'$이다. 오른쪽 역 r가 있으면 임의의 y에 대해 $f(r(y))=y$이므로 전사이다. 두 역이 모두 있으면

$$\ell = \ell\circ \mathrm{id}_Y = \ell\circ(f\circ r) = (\ell\circ f)\circ r = r.$$

따라서 같은 함수가 두 역 조건을 만족한다. □

$X\neq\emptyset$이고 f가 단사이면 왼쪽 역을 만들 수 있다. $x_0\in X$를 하나 고정하고, $y\in f(X)$에는 유일한 원상을, $y\notin f(X)$에는 x_0를 대응시킨다. 같은 섬유 안에서 여러 후보 중 하나를 골라야 하는 문제가 없으므로 선택공리(*axiom of choice*)를 쓰지 않는다. $X=\emptyset, Y\neq\emptyset$인 유일한 함수는 단사지만 $Y\to X$인 함수가 없으므로 왼쪽 역도 없다. 빈 집합 예외를 생략하면 역명제가 틀린다.

전사의 오른쪽 역은 각 비어 있지 않은 섬유에서 대표를 하나 고르는 함수이다. 공역이 유한하면 유한 번의 선택으로 만들 수 있다. 임의의 집합 사이의 모든 전사에 오른쪽 역이 있다는 주장은 집합론에서 선택공리와 동치이다. 이 장에서는 이 일반 주장을 무조건적인 기본 사실로 숨겨 쓰지 않는다.

명제 8.12 선택공리를 가정하면 모든 전사는 오른쪽 역을 가진다. 반대로 모든 전사가 오른쪽 역을 가진다고 가정하면 비어 있지 않은 집합들의 임의의 집합족에 선택함수가 존재한다.

증명. 첫 방향은 전사 $f : X \to Y$의 비어 있지 않은 섬유 $f^{-1}(\{y\})$에서 하나씩 고르면 된다. 고른 원소를 $r(y)$라 하면 $f(r(y)) = y$이다.

역으로 집합족 $(A_i)_{i \in I}$의 모든 A_i가 비어 있지 않다고 하자. 서로 겹칠 수 있으므로 표지를 붙인 합집합 $D = \{(i, a) : i \in I,\ a \in A_i\}$를 만든다. 사영 $p : D \to I$, $p(i, a) = i$는 전사이다. 오른쪽 역 r가 있으면 $r(i) = (i, a_i)$이고 $a_i \in A_i$이므로 $i \mapsto a_i$가 선택함수이다. I가 빈 경우에는 빈 함수가 선택함수이다. □

8.5 유한 집합과 무한 집합의 차이

유한 집합 사이의 함수는 원소의 개수를 세는 것만으로 단사성과 전사성이 갈라지는 경계를 알 수 있다. 이 경계를 정하는 사실이 다음 비둘기집 원리(*pigeonhole principle*)이다.

정리 8.13 (유한 비둘기집 원리) 원소가 $n+1$개인 집합에서 원소가 n개인 집합으로 가는 함수는 단사일 수 없다. 따라서 같은 유한 원소 수를 가진 두 집합 사이에서는 단사, 전사, 전단사가 서로 동치이다.

증명. 첫 주장은 n에 관한 귀납으로 보인다. $n = 0$에서는 비어 있지 않은 정의역에서 공집합으로 가는 함수 자체가 없다. $n \geq 1$이라 하고 단사 함수가 있다고 가정하자. 정의역 원소 하나와 그 출력 하나를 제거하면 나머지 n개 원소의 출력은 제거한 출력과 다르므로, n개 원소에서 $n-1$개 원소로 가는 단사 함수가 남는다. 귀납 가정과 모순이다.

크기가 같은 두 유한 집합에서 단사인데 전사가 아니면 출력 하나를 사용하지 않아 더 작은 공역으로 단사 함수가 생기므로 불가능하다. 전사인데 단사가 아니면 같은 출력으로 가는 입력 둘 중 하나를 제거해도 전사가 유지된다. 이는 더 작은 유한 정의역으로 더 큰 공역을 모두 채운다는 뜻이며, 각 출력의 원상을 유한 번 골라 반대 방향의 단사를 만들면 첫 주장에 모순된다. □

예제 8.14 무한 집합에서는 두 성질이 갈라진다. $s : \mathbb{N} \to \mathbb{N}$, $s(n) = n+1$은 단사지만 0을 출력하지 않아 전사가 아니다. $t(0) = 0$, $t(n+1) = n$으로 정한 $t : \mathbb{N} \to \mathbb{N}$은 전사지만 $t(0) = t(1) = 0$이므로 단사가 아니다. 실제로 $t \circ s = \mathrm{id}_{\mathbb{N}}$이지만 $s \circ t \neq \mathrm{id}_{\mathbb{N}}$이다.

무한 집합의 크기는 원소를 세어 끝내는 방식 대신 전단사의 존재로 비교한다. 같은 크기를 "서로 전단사가 존재한다"로 정의하면 진부분집합과도 같은 크기일 수 있다. 자연수 전체와 짝수 자연수 사이에는 $n \mapsto 2n$이라는 전단사가 있다.

8.6 두 단사에서 전단사로

두 집합 사이에 서로 다른 방향의 단사가 각각 있으면, 선택을 전혀 쓰지 않는 명시적인 구성만으로 전단사를 얻을 수 있다.

정리 8.15 (슈뢰더-베른슈타인) 단사 함수 $f : X \to Y$와 $g : Y \to X$가 모두 존재하면 X와 Y 사이에 전단사가 존재한다. 이 결과의 아래 구성에는 선택공리가 필요하지 않다.

증명. $X_0 = X \setminus g(Y)$로 두고 재귀적으로 $X_{n+1} = g(f(X_n))$를 정한다. $A = \bigcup_{n \in \mathbb{N}} X_n$이라 하자. $X \setminus A$는 X_0와 만나지 않으므로 $g(Y)$에 포함된다. g가 단사이므로 $x \in X \setminus A$에는 유일한 g의 원상이 있다. 다음과 같이 정의한다.

$$h(x) = \begin{cases} f(x), & x \in A, \\ g^{-1}(x), & x \notin A. \end{cases} \tag{8.6}$$

여기서 g^{-1}는 $g(Y)$ 위에서만 사용하는 역함수이다.

A 안에서는 f의 단사성으로, $X \setminus A$ 안에서는 g의 역의 단사성으로 충돌이 없다. 서로 다른 영역의 $a \in A$, $x \notin A$가 같은 값으로 가면 $f(a) = g^{-1}(x)$여서 $x = g(f(a)) \in A$가 되므로 모순이다. 따라서 h는 단사이다.

임의의 $y \in Y$를 잡는다. $g(y) \notin A$이면 $h(g(y)) = y$이다. $g(y) \in A$이면 $g(y)$는 X_0에 속할 수 없으므로 어떤 n에 대해 $g(y) \in X_{n+1} = g(f(X_n))$이다. 따라서 어떤 $a \in X_n$에 대해 $g(y) = g(f(a))$이고, g의 단사성으로 $y = f(a) = h(a)$이다. 두 경우 모두 원상이 있으므로 h는 전사이다. □

증명의 핵심은 모든 점에 같은 방향의 함수를 적용하지 않고, g의 상 밖에서 시작해 번갈아 이동하는 부분에서는 f를 사용하며 나머지에서는 g의 역을 사용하는 것이다. 역을 쓸 수 있는 부분과 서로 다른 영역의 충돌이 없다는 점을 모두 검사해야 한다.

역사. 이 정리는 Georg Cantor가 1880년대에 추측하였고, Richard Dedekind가 독립적으로 증명을 남겼으며, Felix Bernstein이 1897년에 증명을 완성하였다. Ernst Schröder도 비슷한 시기에 증명을 발표하였으나 그 증명에는 결함이 있었다. 관례상 슈뢰더-베른슈타인 정리라 부르지만 베른슈타인-칸토어 정리로도 불린다.

8.7 대각선 논증과 크기의 엄격한 증가

임의의 집합은 자신의 멱집합보다 반드시 작다. 이 칸토어의 정리(*Cantor's theorem*)는 다음과 같은 대각선 논증으로 증명된다.

정리 8.16 (칸토어) 임의의 집합 X에서 멱집합 $\mathcal{P}(X)$으로 가는 전사 함수는 존재하지 않는다.

증명. 전사 $f : X \to \mathcal{P}(X)$가 있다고 가정하고 $D = \{x \in X : x \notin f(x)\}$를 만든다. $D \subseteq X$이므로 전사성에 의해 $f(d) = D$인 $d \in X$가 있다. 정의에서 $d \in D$일 필요충분조건은 $d \notin f(d) = D$이다. 참과 거짓 어느 쪽도 일관되지 않으므로 모순이다. □

X에서 $\mathcal{P}(X)$로는 $x \mapsto \{x\}$라는 단사가 있다. 따라서 멱집합은 원래 집합보다 더 큰 크기를 갖는다. **대각선 논증**(*diagonal argument*)에서 D는 막연히 "빠진 집합"이라고 선언한 것이 아니다. 어떤 후보 $f(x)$와도 원소 x의 포함 여부에서 다르게 되도록 명시적으로 구성했다.

8.8 연습문제와 해설

연습문제 8.17 $f : X \to Y$가 단사일 때 모든 $A, B \subseteq X$에 대해 $f(A \cap B) = f(A) \cap f(B)$임을 보이라.

풀이. 왼쪽이 오른쪽에 포함되는 것은 일반적으로 성립한다. 오른쪽의 y를 잡으면 $a \in A$, $b \in B$가 있어 $f(a) = y = f(b)$이다. 단사성으로 $a = b$이므로 같은 원소가 $A \cap B$에 속하고 $y \in f(A \cap B)$이다. 두 증인을 같은 원소로 만들 수 있는 조건이 단사성이다.

연습문제 8.18 함수 $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^3$이 전단사임을 설명하고 역함수를 쓰라. 실수의 세제곱근 존재를 사용해도 된다.

풀이. 세제곱 함수는 실수에서 엄격히 증가하므로 단사이다. 임의의 $y \in \mathbb{R}$에 대해 유일한 실수 세제곱근 $x = \sqrt[3]{y}$가 있어 $f(x) = y$이므로 전사이다. 역은 $f^{-1}(y) = \sqrt[3]{y}$이다. 짝수 거듭제곱의 부호 문제와 달리 정의역을 양수로 제한할 필요가 없다.

연습문제 8.19 $X = \{a\}$, $Y = \{0, 1\}$이고 $f(a) = 0$이라 하자. 왼쪽 역은 존재하는가? 오른쪽 역은 존재하는가?

풀이. $\ell(0) = \ell(1) = a$로 두면 $\ell(f(a)) = a$이므로 왼쪽 역이다. 오른쪽 역은 없다. f가 1을 출력하지 않으므로 어떤 $r(1)$을 선택해도 $f(r(1)) = 1$을 만족할 수 없다.

연습문제 8.20 $\mathbb{N}$과 $\mathbb{Z}$ 사이의 전단사를 하나 구성하라.

풀이. $h(0) = 0$, $h(2k-1) = k$, $h(2k) = -k$를 $k \geq 1$에서 정의한다. 0, 양수, 음수라는 서로 다른 출력 영역을 사용하므로 영역 사이 충돌이 없다. 각 영역 안에서도 입력이 유일하며 모든 정수를 방문한다. 따라서 전단사이다. 서로 다른 세 경우가 모든 자연수를 덮는지도 확인했다.

연습문제 8.21 $\mathcal{P}(\mathbb{N})$의 원소를 $A_0, A_1, A_2, \ldots$로 전부 나열할 수 있다는 주장에 대각선 반례를 만들라.

풀이. $D = \{n \in \mathbb{N} : n \notin A_n\}$로 둔다. 모든 k에 대해 k의 포함 여부가 D와 A_k에서 다르므로 $D \neq A_k$이다. 따라서 목록이 어떤 것이든 빠진 부분집합이 있다. 목록의 처음 몇 항을 모르더라도 목록 전체를 매개변수로 반례를 정의할 수 있다.

연습문제 8.22 $X \neq \emptyset$이고 $f : X \to Y$가 단사일 때 만든 왼쪽 역이 유일할 필요가 없는 이유와 예를 제시하라.

풀이. 왼쪽 역 조건은 $f(X)$에서의 값만 정한다. $X = \{a, b\}$, $Y = \{0, 1, 2\}$, $f(a) = 0$, $f(b) = 1$로 두면 $\ell(0) = a$, $\ell(1) = b$는 강제되지만 $\ell(2)$는 a 또는 b로 정할 수 있다. 원래 함수가 전단사라면 남는 공역 원소가 없어 역함수가 유일해진다.

함수의 크기 비교와 대표 선택은 집합의 순서 구조 및 선택 원리와 연결된다. 다음 장은 부분순서에서 무엇을 비교할 수 있고 어떤 최대성 주장이 추가 공리를 요구하는지 구별한다.

제 9 장

부분순서, 정렬, 최대성 원리

개요 이 장은 반사성·반대칭성·추이성을 만족하는 관계로 부분순서를 정의하고 준순서와의 관계를 밝히며(9.1절), 상계와 극대원소·최대원소를 구별한다(9.2절). 이어 최소상계와 격자 구조를 도입하고 분배법칙이 일반적으로 성립하지 않음을 보인 뒤(9.3절), 사슬·정렬순서와 순서를 보존하는 함수의 두 층위(순서보존과 순서매장)를 정리한다(9.4절). 마지막으로 선택공리와 동치인 조른 보조정리의 정확한 적용 조건을 밝히고(9.5절), 그 대표적 응용으로 벡터공간의 선형독립 집합을 기저로 확장한다(9.6절). 이 장의 조른 보조정리 응용에서는 선택공리를 가정한다고 명시한다. 선행 지식: 관계의 반사성·반대칭성·추이성, 집합의 포함관계, 귀납법과 자연수의 정렬성(제4권 제6장).

크기 비교가 항상 두 대상을 한 줄로 세우는 것은 아니다. 두 부분집합 중 어느 것도 다른 쪽에 포함되지 않을 수 있고, 두 양의 정수 중 어느 것도 다른 쪽을 나누지 않을 수 있다. 부분순서는 이런 비교 불가능성을 허용한다. 그 안에서 "더 큰 것이 없다"와 "모든 것보다 크다"는 다른 성질이며, 둘을 구별해야 최대성 원리를 올바르게 적용할 수 있다.

9.1 부분순서와 전순서

정의 9.1 (부분순서와 전순서) 집합 P 위의 반사적·반대칭적·추이적 관계 $\preceq$를 **부분순서**(*partial order*)라 하고 $(P, \preceq)$를 **부분순서 집합**(*partially ordered set*, 약칭 poset)이라 한다. 모든 $x, y \in P$에 대해 $x \preceq y$ 또는 $y \preceq x$이면 **전순서**(*total order*)이다. $x \prec y$는 $x \preceq y$이면서 $x \neq y$임을 뜻한다.

예제 9.2 $\mathcal{P}(X)$ 위의 포함관계는 부분순서이다. $X = \{a, b\}$이면 $\{a\}$와 $\{b\}$는 비교할 수 없으므로 전순서가 아니다. 양의 정수 위의 나눗셈 관계 $a \preceq b \iff a \mid b$도 부분순서이다. 모든 정수로 범위를 넓히면 $2 \mid -2$이고 $-2 \mid 2$인데 $2 \neq -2$이므로 반대칭성이 깨진다. 바탕 집합의 양수 조건이 중요하다.

$\mathbb{R}^2$의 좌표별 순서 $(x_1, x_2) \preceq (y_1, y_2)$를 두 좌표의 부등식이 모두 성립함으로 정의하면 부분순서이다. $(0, 1)$과 $(1, 0)$은 비교할 수 없다. 사전식 순서는 첫 좌표를 먼저 비교하고 첫 좌표가 같을 때 둘째 좌표를 비교하므로 전순서이다. 같은 집합에 서로 다른 순서를 줄 수 있다.

정의 9.3 (준순서) 반사적이고 추이적이지만 반대칭성을 요구하지 않는 관계를 전순서와 구별하여 **준순서**(*preorder*)라 한다. 이 권에서 준순서는 모든 쌍이 비교 가능하다는 뜻이 아니다.

명제 9.4 준순서 $\preceq$에서 $x \sim y$를 $x \preceq y$이고 $y \preceq x$임으로 정의하면 동치관계이다 (제4권 제7장). 몫집합에 $[x] \le [y]$를 $x \preceq y$로 정의하면 잘 정의된 부분순서가 된다.

증명. 동치관계의 반사성과 대칭성은 정의에서 바로 나온다. $x \sim y$, $y \sim z$이면 원래 관계의 추이성으로 $x \preceq z$와 $z \preceq x$이므로 추이성도 성립한다. 대표를 $x' \sim x$, $y' \sim y$로 바꾸어도 $x' \preceq x \preceq y \preceq y'$

이므로 $x' \preceq y'$이다. 역방향도 같으므로 몫의 순서는 잘 정의된다. 반사성·추이성은 내려가고, 두 류가 서로 작거나 같으면 대표가 동치이므로 같은 류여서 반대칭성이 성립한다. □

준순서에서 구별되지 않는 원소를 먼저 하나로 묶으면 실제 부분순서를 얻는다. 이는 동치관계와 순서 구조가 따로 있는 주제가 아니라 서로를 정리하는 도구임을 보여 준다.

9.2 극대, 최대, 상계

정의 9.5 (상계, 최대원소, 극대원소) 부분순서 집합 P의 부분집합 A에 대해 $u \in P$가 모든 $a \in A$에 대해 $a \le u$를 만족시키면 **상계**(*upper bound*)라 한다. $m \in A$가 A의 상계이면 **최대원소**(*maximum element*)라 한다. A에 $m \in A$보다 엄격히 큰 원소가 없으면 m은 **극대원소**(*maximal element*)이다. **하계**(*lower bound*)·**최소원소**(*minimum element*)·**극소원소** (*minimal element*)는 순서를 뒤집어 정의한다.

최대원소는 모든 원소와 비교되어 그 위에 있어야 하지만, 극대원소는 자신보다 위인 원소가 없으면 된다. 비교 불가능한 다른 극대원소가 여러 개 있을 수 있다. 최대원소가 있으면 반대칭성 때문에 유일하다. 극대원소가 유일하다는 것만으로 무한한 부분순서 집합의 최대원소라고 결론낼 수는 없다.

예제 9.6 집합족 $A = \{\{1\}, \{2\}, \{1,3\}\}$를 포함순서로 보자. 극대원소는 $\{2\}$와 $\{1,3\}$이다. 둘이 비교 불가능하므로 최대원소는 없다. $\{1,2,3\}$은 바탕 부분순서 집합 $\mathcal{P}(\{1,2,3\})$ 안에서 A의 상계이지만 A의 원소가 아니므로 A의 최대원소는 아니다.

명제 9.7 유한하고 비어 있지 않은 부분순서 집합에는 극대원소가 존재한다. 더 강하게, 각 원소 x 위에 어떤 극대원소 m이 있어 $x \le m$이다.

증명. x가 극대이면 끝난다. 아니라면 $x < x_1$인 원소를 고른다. x_1도 극대가 아니면 더 큰 원소를 고른다. 엄격한 증가 사슬에서는 앞선 원소로 돌아갈 수 없고, 원소 수가 유한하므로 이 과정은 유한 단계 후 멈춘다. 멈춘 원소는 극대이며 추이성에 의해 x보다 크거나 같다. □

따름정리 9.8 유한한 비어 있지 않은 부분순서 집합에서 극대원소가 하나뿐이면 그것이 최대원소이다.

각 원소 위에 극대원소가 있는데 후보가 하나뿐이므로 모든 원소가 그 아래에 있다. 유한성은 증명의 증가 과정이 멈추는 데 사용되었다.

9.3 최소상계와 격자

정의 9.9 (최소상계와 하한) $A \subseteq P$의 상계들 중 가장 작은 원소를 **최소상계**(*least upper bound*) 또는 **상한**(*supremum*) $\sup A$라 한다. 하계들 중 가장 큰 원소를 **하한**(*infimum*) $\inf A$라 한다. 존재하면 각각 유일하지만 A에 속할 필요는 없다.

실수의 열린 구간 $(0,1)$은 상한 1을 가지지만 최대원소는 없다. 양의 정수의 나눗셈 순서에서 $\{2,3\}$의 상한은 최소공배수 6이고 하한은 최대공약수 1이다(제1권 제2장). 여기서 “최소”는 수치적으로 작다는 말 이전에 주어진 나눗셈 순서에 관한 말이다.

정의 9.10 (격자와 완비격자) 모든 두 원소가 상한과 하한을 가지는 부분순서 집합을 **격자**(*lattice*)라 한다. 두 원소의 상한을 $x \vee y$, 하한을 $x \wedge y$로 쓴다. 모든 부분집합이 상한과 하한을 가지면 **완비격자**(*complete lattice*)라 한다. 빈 부분집합도 포함하므로 완비격자에는 최소원소와 최대원소가 있다.

예제 9.11 $\mathcal{P}(X)$는 완비격자이다. 임의의 집합족의 상한은 합집합, 하한은 교집합이다. 빈 집합족의 합집합은 $\emptyset$, X의 부분집합들로 보는 빈 교집합은 X이다. 따라서 빈 집합족의 상한은 최소원소, 하한은 최대원소가 된다. 빈 교집합에서 바탕 집합 X를 밝히는 이유가 여기에 있다.

격자라는 조건만으로 모든 분배법칙이 성립하지는 않는다. 예를 들어 최소원소 0, 최대원소 1, 서로 비교 불가능한 세 원소 a, b, c가 있고 각각 0 위와 1 아래에 놓인 다섯 원소 격자를 생각하자. 서로 다른 중간 원소의 상한은 1, 하한은 0이다. 그러면

$$a \wedge (b \vee c) = a, \qquad (a \wedge b) \vee (a \wedge c) = 0$$

이므로 분배법칙이 실패한다. 집합 연산에서 보았던 성질을 추상적인 격자 전체에 그대로 옮기지 않는다.

9.4 사슬, 정렬, 두 종류의 순서 보존

정의 9.12 (사슬, 반사슬, 정렬순서) 부분순서 집합의 부분집합 C가 제한된 순서에서 전순서이면 **사슬**(*chain*)이라 한다. 서로 다른 두 원소가 비교 불가능한 부분집합은 **반사슬**(*antichain*)이라 한다. 전순서가 그 모든 비어 있지 않은 부분집합에 최소원소를 주면 **정렬순서**(*well-order*)이다.

통상의 $\mathbb{N}$은 정렬되어 있지만 $\mathbb{Z}$는 전체 집합에 최소원소가 없으므로 정렬되어 있지 않다. $[0,1]$도 전체 집합의 최소원소 0은 있지만 부분집합 $(0,1]$에 최소원소가 없어 통상의 순서에서 정렬되어 있지 않다. 전체의 최소원소 하나만 확인하는 것으로 정렬성을 증명할 수 없다.

예제 9.13 $\mathbb{N} \times \mathbb{N}$의 사전식 순서는 정렬순서이다. 비어 있지 않은 부분집합 A에서 등장하는 첫 좌표의 집합은 최솟값 m을 가진다. 첫 좌표가 m인 원소들의 둘째 좌표 중 최솟값 n을 택하면 (m, n)이 A의 최소원소이다. 반면 순서를 뒤집어 첫 좌표에서 무한히 감소할 수 있게 만들면 정렬성이 사라질 수 있다.

정의 9.14 (순서보존, 순서매장, 순서동형) 부분순서 집합 사이의 함수 $f : P \to Q$가 $x \le y$이면 $f(x) \le f(y)$를 만족하면 **순서보존** (*order-preserving*)이라 한다. 양방향

$$x \le y \iff f(x) \le f(y)$$

를 만족하면 **순서매장**(*order embedding*)이라 한다. 전단사이며 자신과 역함수가 모두 순서보존이면 **순서동형**(*order isomorphism*)이다.

순서매장은 자동으로 단사이다. $f(x) = f(y)$이면 양방향 비교가 성립하므로 원래 원소도 $x \le y$와 $y \le x$를 만족하고 반대칭성으로 같다. 하지만 단사인 순서보존 함수라고 해서 비교 불가능한 두 원소의 출력도 비교 불가능하다는 보장은 없다.

9.5 조른 보조정리의 정확한 경계

비어 있지 않은 부분순서 집합에서 모든 사슬이 상계를 가지면 그 집합 전체의 상계를 넘어 극대원소까지 존재한다는 것이 다음 조른 보조정리(*Zorn's lemma*)이다. 이는 선택공리(제4권 제8장)와 동치인 원리이며, 가정할 때마다 그 사실을 명시한다.

> **정리 9.15 (조른 보조정리: 선택공리를 가정)** 비어 있지 않은 부분순서 집합 P에서 모든 사슬이 P 안의 상계를 가지면 P에는 극대원소가 존재한다.

이 정리는 표준 집합론 ZF 위에서 선택공리 및 모든 집합을 정렬할 수 있다는 정리와 동치이다. 여기서는 그 동치 전체를 증명하지 않고, 사용 시 선택공리를 가정한 원리로 표시한다. 정렬 가능성은 기존에 주어진 실수의 대소관계가 정렬순서라는 뜻이 아니다. 그 집합에 어떤 다른 정렬순서를 줄 수 있다는 뜻이다.

조른 보조정리를 적용할 때 확인할 것은 다음 세 가지이다. 후보들을 이루는 집합과 순서를 정확히 정하고, 후보가 하나 이상 있음을 보이며, 임의의 사슬에서 후보 집합 안에 남는 상계를 만든다. 상계가 사슬 안에 있을 필요는 없지만 후보 집합 P 밖에 있어서는 안 된다. 결론은 극대원소이며 최대원소가 아니다.

역사. Max Zorn은 1935년에 이 보조정리를 발표하였다. 같은 뜻의 원리를 Felix Hausdorff는 1914년에 극대 사슬의 존재(Hausdorff 최대성 원리)라는 형태로 먼저 제시하였고, Ernst Zermelo는 1904년과 1908년에 선택공리로부터 정렬정리를 증명하였다. 세 결과는 모두 ZF 위에서 선택공리와 동치이다.

> **예제 9.16 (조건이 실패하는 표준 사례)** P를 $\mathbb{N}$의 유한 부분집합들의 집합으로 두고 포함순서를 주자. 각 유한 사슬에는 그중 가장 큰 집합이라는 상계가 있다. 그러나 $C = \{\{0, \dots, n\} : n \in \mathbb{N}\}$라는 무한 사슬에는 유한한 상계가 없다. 따라서 조른의 가정을 만족하지 않는다. 실제로 임의의 유한 집합에 새로운 자연수를 하나 추가할 수 있어 극대원소도 없다.

9.6 선형독립 집합을 기저로 확장하기

이 절은 조른 보조정리의 대표적인 응용을 보인다. 벡터공간의 정의와 유한 선형결합을 알고 있는 독자를 위한 연결 예제이며, 선형대수 권(제7권 제3장)에서 다시 활용한다.

> **정리 9.17 (선택공리를 가정한 기저 확장)** 체 K 위의 벡터공간 V에서 선형독립 집합 S가 주어지면 S를 포함하는 기저가 존재한다.

증명. P를 S를 포함하는 모든 선형독립 부분집합의 모임으로 두고 포함순서를 준다. $S \in P$이므로 비어 있지 않다. 비어 있지 않은 사슬 $C \subseteq P$에 대해 $U = \bigcup_{A \in C} A$라 하자. U는 S를 포함한다. U에서 서로 다른 유한 개의 벡터를 고르면 각각을 담는 사슬 원소들이 있고, 유한 개의 사슬 원소 중 가장 큰 하나가 그 벡터들을 모두 담는다. 그 집합이 선형독립이므로 해당 벡터들의 영벡터 선형결합은 자명한 것뿐이다. 따라서 U도 선형독립이고 P 안의 상계이다. 빈 사슬에는 S가 상계이다.

조른 보조정리로 극대 원소 $B \in P$를 얻는다. B가 V를 생성하지 않는다면 $v \notin \operatorname{span}(B)$인 벡터 v가 있다. $B \cup \{v\}$의 유한 선형결합이 0이고 v의 계수가 0이 아니면, 식을 풀어 $v \in \operatorname{span}(B)$를

얻어 모순이다. 그 계수가 0이면 B의 선형독립성으로 나머지 계수도 모두 0이다. 따라서 $B \cup \{v\}$가 더 큰 선형독립 집합이 되어 극대성과 모순된다. 그러므로 B는 V를 생성하고 기저이다. $\square$

사슬의 합집합에서 선형독립성이 보존되는 핵심 이유는 선형독립 조건이 유한 개 벡터의 관계만 검사한다는 데 있다. 임의의 부분집합족의 합집합이 선형독립이라는 말은 아니다. 서로 비교되지 않는 두 선형독립 집합을 합치면 선형종속이 생길 수 있다.

9.7 연습문제와 해설

연습문제 9.18 양의 정수의 나눗셈 순서에서 부분집합 $A = \{2, 3, 6, 10\}$의 극대원소와 최대원소를 구하라.

풀이. 6과 10은 A 안의 더 큰 배수가 없으므로 극대원소이다. 2는 $6, 10$을 나누고 3은 6을 나누므로 극대가 아니다. 6과 10은 서로 나누지 못하므로 모든 원소 위에 있는 최대원소는 없다. 수치적으로 가장 큰 10을 최대원소라고 부르면 순서를 바꾼 셈이다.

연습문제 9.19 극대원소가 하나뿐이지만 최대원소가 없는 무한 부분순서 집합을 구성하라.

풀이. 통상의 순서를 가진 $\mathbb{N}$에 새 원소 a를 추가하고 a가 자신 이외의 모든 자연수와 비교 불가능하도록 한다. 각 자연수는 더 큰 자연수를 가지므로 극대가 아니고 a만 극대이다. 하지만 a는 자연수들의 상계가 아니므로 최대원소는 아니다. 유한성 없이 유일한 극대성을 최대성으로 바꿀 수 없음을 보여 준다.

연습문제 9.20 두 원소 반사슬에서 두 원소 전순서로 가는 전단사가 순서보존이지만 역은 순서보존이 아닌 예를 쓰라.

풀이. $P = \{a, b\}$에서는 서로 다른 두 원소를 비교하지 않고, $Q = \{0, 1\}$에서는 $0 < 1$로 둔다. $f(a) = 0$, $f(b) = 1$은 P의 같은 원소 비교만 보존하면 되므로 순서보존이다. 역이 순서보존이면 $0 \le 1$에서 $a \le b$를 얻어야 하지만 P에는 그런 비교가 없다.

연습문제 9.21 $\mathcal{P}(X)$에서 어떤 집합족의 최소상계가 합집합인 이유를 상계의 두 조건으로 증명하라.

풀이. 각 구성 집합은 합집합에 포함되므로 합집합은 상계이다. 다른 상계 B는 각 구성 집합을 포함하므로 그 원소 전체인 합집합도 포함한다. 따라서 합집합은 모든 상계보다 작거나 같아 최소상계이다. 단지 상계 하나를 찾는 것과 최소성을 증명하는 것을 분리했다.

연습문제 9.22 조른 보조정리로 기저를 만들 때 모든 후보 선형독립 집합의 합집합을 곧바로 택하지 않는 이유를 설명하라.

풀이. 모든 후보가 서로 포함 비교되는 것은 아니다. 예를 들어 한 차원 공간에서 영벡터가 아닌 v에 대해 $\{v\}$와 $\{2v\}$는 체의 특성 및 $2 \neq 0$을 가정하면 각각 선형독립이지만 그 합집합은 종속이다. 구체적으로 실수 벡터공간을 택하면 $2v - 1 \cdot (2v) = 0$이라는 비자명 관계가 있다. 사슬에서는 유한 벡터들이 하나의 독립 집합 안에 들어간다는 조건이 이 문제를 막는다.

연습문제 9.23 준순서 $x \preceq y \iff |x| \le |y|$를 $\mathbb{R}$ 위에 주자. 동치류와 몫의 부분순서를 설명하라.

풀이. $x \sim y$일 조건은 $|x| = |y|$이다. 0의 류는 $\{0\}$이고 $r > 0$에 대한 류는 $\{-r, r\}$이다. 각 류를 공통 절댓값으로 보내면 몫은 통상의 순서를 가진 $[0, \infty)$와 순서동형이다. 원래 관계에서 두 부호를 구별하지 못하는 점이 몫에서 제거된다.

순서와 최대성에서는 무한 집합과 선택 원리가 드러났다. 다음 장은 다시 유한한 논리식으로 돌아가, 모든 경우를 실제로 제거할 수 있다는 의미의 완전성을 알고리즘 수준에서 증명한다.

제 10 장

정규형, 해결법, 유한 SAT의 완전성

개요 **SAT**(충족가능성 문제, *satisfiability problem*)는 주어진 유한 명제논리식을 참으로 만드는 평가가 있는지 묻는 결정 문제이다. 이 장은 식을 절 집합으로 표현하는 약속을 정하고, 변수 수에 따라 지수적으로 커지는 직접 분배법칙 전개 대신 보조 변수를 쓰는 정의적 변환이 선형 크기의 CNF를 만든다는 사실을 증명한다(10.1–10.2절). 이어 부분 평가에 의한 절 집합의 단순화(10.3절)와, 한 변수에 관한 모든 해결 결과를 모아 그 변수를 완전히 제거하면서 충족가능성을 보존하는 변수 제거(10.4절)를 다룬다. 변수 개수에 대한 귀납으로 변수 제거를 반복하면 유한 절 집합의 해결 반박 완전성(10.5절)을 얻고, 이와 별도로 단위 전파와 분기를 결합한 탐색의 건전성·완전성·종료(10.6절)를 증명한다. 마지막으로 그래프 색칠을 CNF로 부호화하는 표준 예(10.7절)를 다룬다. 선행 지식: 명제논리의 평가와 충족가능성, CNF와 DNF, 해결 규칙의 건전성과 정규형의 존재(제4권 제2장). 그 정규형 존재 증명은 이미 아는 것으로 하고, 여기서는 표현의 크기, 변수 제거, 탐색의 완전성을 다룬다. 진리표는 항상 SAT의 답을 주지만, 변수가 많은 식에서는 2^n 개의 행을 모두 쓰기가 현실적이지 않다. 종료하는 탐색과 참을 보존하는 추론이 결합되면 완전한 결정 절차를 얻는다.

10.1 절을 집합으로 기록하기

정의 10.1 (반대 리터럴과 절) 리터럴 p의 **반대 리터럴**은 $\neg p$이고, $\neg p$의 반대 리터럴은 p이다. 절은 유한 리터럴 집합으로 기록하고 그 원소들의 논리합으로 해석한다. 절 집합 S는 각 절의 논리곱으로 해석한다. 빈 절 $\varnothing$은 거짓이고, 절이 하나도 없는 빈 절 집합은 참이다.

참고 (두 층의 빈 기호). 표현상 같은 $\varnothing$이라도 "절 한 개"와 "절들의 집합"이라는 층이 다르다. 충족불가능한 입력 $\{\varnothing\}$과 모든 평가가 만족하는 입력 $\varnothing$을 구별해야 한다. 중복 리터럴을 제거해도 논리합 값은 바뀌지 않으므로 절을 집합으로 기록할 수 있다.

정의 10.2 (항진 절과 포섭) 한 절이 어떤 변수 p와 $\neg p$를 모두 포함하면 **항진 절**(*tautological clause*)이라 한다. 모든 평가가 그 절을 만족하므로 CNF에서 항진 절을 제거해도 논리적 동치가 유지된다. 절 $C \subseteq D$이면 C가 D를 포함관계상 **포섭**(*subsumption*)한다고 표현하며, C와 D가 함께 있을 때 D를 제거할 수 있다.

작은 절은 더 강한 조건이다. 예를 들어 $\{p\}$를 만족하면 $\{p, q\}$도 만족하므로 둘의 논리곱은 $\{p\}$만 남겨도 된다. 리터럴이 많을수록 만족시킬 방법이 많아진다. 집합의 포함 방향과 논리 조건의 강약 방향이 반대라는 점에 주의한다.

예제 10.3 $S = \{\{p, \neg p, q\}, \{p, q\}, \{p\}, \{\neg p, r\}\}$에서 첫 항진 절을 제거하고, $\{p\}$에 포섭되는 $\{p, q\}$를 제거하면 $\{\{p\}, \{\neg p, r\}\}$만 남는다. 이는 $p \wedge r$와 동치이다. 첫 두 제거는 모든 평가에서 동치를 보존하며, 마지막은 p가 강제되는 점을 사용했다.

10.2 직접 CNF 변환의 크기와 보조 변수

식

$$\Phi_n = (a_1 \wedge b_1) \vee \cdots \vee (a_n \wedge b_n)$$

에 분배법칙을 기계적으로 적용하면 각 쌍에서 하나씩 리터럴을 택한 2^n 개의 절이 나타난다. 원래 식은 쌍의 개수에 비례하는 길이인데 전개 후에는 훨씬 커질 수 있다. 이 사실은 특정 전개 방식의 크기에 관한 설명이며, 모든 표현 방식을 금지하는 결과가 아니다.

새 변수를 사용하여 부분식의 값을 기록하면 전개를 피할 수 있다. 새 변수 z가 $a \wedge b$의 값을 나타내게 하려면 동치 $z \leftrightarrow (a \wedge b)$를 다음 세 절로 표현한다.

$$(\neg z \vee a) \wedge (\neg z \vee b) \wedge (z \vee \neg a \vee \neg b). \tag{10.1}$$

앞의 두 절은 $z \to a \wedge b$, 마지막 절은 $a \wedge b \to z$를 표현한다. 어느 한 방향을 빼면 부분식 값과 새 변수 값이 어긋날 수 있다.

논리합과 부정의 대응도 고정 길이의 절들로 표현한다.

$$z \leftrightarrow (a \vee b) \;\rightsquigarrow\; (z \vee \neg a) \wedge (z \vee \neg b) \wedge (\neg z \vee a \vee b),$$

$$z \leftrightarrow \neg a \;\rightsquigarrow\; (\neg z \vee \neg a) \wedge (z \vee a).$$

$\rightsquigarrow$는 이 절에서 오른쪽 CNF로 기록한다는 표시이며 새로운 논리 연결사는 아니다. 조건문 등 다른 연결사는 기본 연결사로 바꾸거나 별도의 고정 크기 정의 절을 사용할 수 있다. 식의 각 부분식마다 식 (10.1)과 같은 꼴의 절을 붙여 전체 식의 충족가능성을 보존하는 절 집합을 얻는 방법을 **정의적 CNF 변환**(*definitional CNF transformation*)이라 한다.

> **정리 10.4 (정의적 CNF 변환)** 각 부분식에 새로운 변수를 배정하고 해당 연결사의 동치를 위와 같은 절들로 기록하라. 전체 식을 나타내는 변수 z_Φ의 단위절도 추가하라. 얻은 절 집합 S_Φ는 원래 식 Φ와 충족가능성이 같다. 원래 변수의 각 평가에는 모든 정의 절을 만족하는 새 변수 값의 확장이 정확히 하나 있으며, 그 확장이 z_Φ를 참으로 만들 필요충분조건은 원래 평가가 Φ를 참으로 만드는 것이다.

증명. 원래 변수의 값을 고정하면 부분식의 구문 나무를 아래에서 위로 계산하여 각 새 변수에 해당 부분식 값을 배정할 수 있다. 각 동치의 정의 절을 만족하며, 반대로 정의 절은 새 변수의 값을 연결사의 진리표 값으로 강제하므로 다른 확장은 없다. 맨 위의 값도 Φ의 값과 같으므로 그 값이 참이라는 단위절을 추가하면 정확히 원래 식의 만족 평가만 남는다. 유한 구문 나무의 각 연결사에 고정 개수의 절을 쓰므로 결과 절 수는 연결사 수에 비례한다. □

새 변수가 생겼으므로 S_Φ와 Φ가 같은 변수 집합의 모든 평가에서 동치라고 말하면 부정확하다. 정확한 관계는 새 변수들을 존재적으로 잊었을 때 원래 식과 동치라는 것이다. 원래 변수만 보고 만족하는 평가를 복원할 수 있고, 새 변수 값은 정의로 결정된다.

> **예제 10.5** $\Phi = (p \wedge q) \vee \neg r$에 $a \leftrightarrow (p \wedge q)$, $b \leftrightarrow \neg r$, $c \leftrightarrow (a \vee b)$를 도입하고 c를 참으로 강제한다. $p = q = 0, r = 0$이면 $a = 0, b = 1, c = 1$로 유일하게 확장되어 식을 만족한다. $p = 1, q = 0, r = 1$이면 $a = b = c = 0$이 강제되므로 마지막 단위절을 만족하지 못한다. 원래 식의 두 평가 결과와 일치한다.

10.3 부분 평가와 안전한 단순화

부분 평가(*partial assignment*)는 일부 변수에만 진리값을 준다. 절 집합 S에 부분 평가 α를 적용할 때, 이미 참인 리터럴을 포함한 절은 제거하고, 나머지 절에서는 거짓으로 정해진 리터럴을 제거한다. 결과를 $S \restriction \alpha$로 쓰자.

> **명제 10.6 (부분 평가에 의한 안전한 단순화)** α를 확장하는 전체 평가 v에 대해 v가 S를 만족할 필요충분조건은 미정 변수에 대한 v의 값들이 $S \restriction \alpha$를 만족하는 것이다.

증명. 이미 참인 리터럴이 있는 절은 모든 확장에서 참이므로 지워도 된다. 그런 리터럴이 없는 절에서는 이미 거짓인 리터럴이 그 절을 만족시키는 데 기여하지 않는다. 따라서 남은 리터럴 중 하나가 참이어야 한다는 조건만 남는다. 모든 절에 적용하면 결론이다. $\square$

> **정의 10.7 (단위절, 단위 전파, 순수 리터럴)** 한 리터럴만 있는 절을 **단위절**(*unit clause*)이라 한다. $\{p\}$가 있으면 모든 만족 평가는 $p = 1$을 가져야 하고, $\{\neg p\}$가 있으면 $p = 0$이어야 한다. 이 값을 배정하고 식을 단순화하는 과정을 **단위 전파**(*unit propagation*)라 한다. 어떤 변수가 한쪽 부호로만 나타나면 그 리터럴을 **순수 리터럴**(*pure literal*)이라 한다.

그 부호를 참으로 두면 해당 리터럴을 가진 절들은 모두 만족하고, 반대 부호가 없으므로 다른 절을 어렵게 만들지 않는다. 따라서 순수 리터럴을 참으로 배정해도 충족가능성을 보존한다. 그러나 모든 원래 만족 평가가 그 값을 갖는다는 뜻은 아니다. 단위절과 순수 리터럴의 논리적 강제력은 다르다.

> **예제 10.8** $S = \{\{p, q\}, \{\neg q, r\}\}$에서 p는 순수하지만 반드시 참일 필요는 없다. $p = 0, q = 1, r = 1$도 만족 평가이다. 반면 단위절 $\{p\}$가 추가되면 모든 만족 평가에서 $p = 1$이어야 한다. 순수 리터럴 처리는 적어도 한 해를 보존하는 탐색 전략이며, 단위 전파는 현재 남은 모든 해에 공통인 값을 사용한다.

10.4 변수 제거 보조정리

표기 (해결 규칙의 표기). 두 절 $C \cup \{p\}$와 $D \cup \{\neg p\}$ (단, $p, \neg p \notin C \cup D$)로부터 **해결 결과**(*resolvent*) $C \cup D$를 이끌어 내는 추론을 **해결 규칙**(*resolution rule*)이라 한다. 그 건전성—원래 두 절을 만족하는 모든 평가는 해결 결과도 만족한다는 사실—은 앞서 증명하였다(제4권 제2장). 이 절에서는 한 변수에 관한 모든 해결 결과를 한꺼번에 모아 그 변수를 식에서 완전히 지운다.

항진 절을 제거한 유한 절 집합 S에서 변수 p를 고르자. p를 포함한 절을 $\{p\} \cup C_i$, $\neg p$를 포함한 절을 $\{\neg p\} \cup D_j$로 쓰고, 어느 쪽도 포함하지 않는 절들의 집합을 S_0라 하자. C_i, D_j에는 p나 $\neg p$가 없다. 다음 절 집합을 만든다.

$$E_p(S) = S_0 \cup \{\, C_i \cup D_j : \text{모든 } i, j \,\}. \tag{10.2}$$

만들어진 항진 절은 다시 지워도 된다. 한 부호의 절이 하나도 없으면 그에 따른 해결 결과도 없다.

> **보조정리 10.9 (충족가능성을 보존하는 변수 제거)** p 이외 변수들의 평가 v가 $E_p(S)$를 만족할 필요충분조건은 v에 적절한 p 값을 더하여 S를 만족시킬 수 있다는 것이다.

증명. S를 만족하는 확장이 있으면 S_0의 모든 절과 모든 해결 결과 $C_i \cup D_j$가 참이다. 이는 해결 규칙의 건전성에 의해 성립한다.

역으로 v가 $E_p(S)$를 만족한다고 하자. 모든 C_i가 이미 참이면 $p = 0$으로 둔다. 양의 p 절은 C_i 덕분에 참이고, 음의 p 절은 $\neg p$ 덕분에 참이다. 어떤 C_{i_0}가 거짓이면 $p = 1$로 둔다. 모든 j에 대해 해결 결과 $C_{i_0} \cup D_j$가 참이므로 D_j는 참이어야 한다. 따라서 양의 p 절은 p 덕분에 참이고, 음의 p 절은 D_j 덕분에 참이다. S_0는 어느 경우든 이미 참이다. 이로써 만족 확장이 존재한다. □

해결 결과를 모으는 일은 단순히 결과 몇 개를 추가하는 데 그치지 않는다. 원래 변수 p에 관한 모든 양·음의 절을 함께 고려하면 p를 잊은 뒤 남는 조건을 정확히 기술한다. 임의의 일부 해결 결과만 남기고 원래 절을 지우면 이 등가성이 깨질 수 있다.

예제 10.10 $S = \{\{p, q\}, \{\neg p, r\}, \{\neg p, s\}, \{\neg q\}\}$에서 p를 제거하면

$$E_p(S) = \{\{q, r\}, \{q, s\}, \{\neg q\}\}.$$

$\neg q$ 때문에 $q = 0$이고, 따라서 $r = s = 1$이어야 한다. 양의 p 절의 나머지 q가 거짓이므로 원래 S로 돌아갈 때 $p = 1$로 확장한다. 이 예는 축소 문제를 푼 뒤 제거한 변수의 값을 복원하는 방법도 보여 준다.

10.5 유한 해결법의 완전성

정리 10.11 (유한 절 집합의 해결 반박 완전성) 유한 절 집합 S가 충족불가능할 필요충분조건은 해결 규칙을 유한 번 적용하여 빈 절을 유도할 수 있다는 것이다. 항진 절 제거와 중복 제거는 허용한다.

증명. 빈 절이 유도되면 해결 규칙의 건전성에 의해 원래 절들의 모든 만족 평가가 빈 절도 만족해야 한다. 빈 절은 항상 거짓이므로 만족 평가는 없다.

역방향은 S에 나타나는 변수 개수에 대한 귀납으로 증명한다. 변수가 없으면 가능한 비항진 절은 빈 절뿐이다. 절 집합이 비어 있으면 만족되므로, 충족불가능한 경우에는 이미 빈 절이 들어 있다. 변수가 하나 이상이면 p를 골라 $E_p(S)$를 만든다. 변수 제거 보조정리(보조정리 10.9)로 S와 $E_p(S)$의 충족가능성이 같으므로 후자도 충족불가능하다. p가 사라졌으므로 변수 개수가 줄었다. 귀납 가정에 의해 $E_p(S)$에서 빈 절로 가는 유한 해결 유도가 있다. $E_p(S)$의 각 초기 절은 원래 S_0의 절이거나 S의 두 절을 한 번 해결한 결과이다. 따라서 그 초기 절들을 먼저 S에서 유도한 뒤 귀납 가정의 유도를 이어 붙이면 S에서 빈 절을 얻는다. □

이 정리는 “어떤 해결 순서를 택해도 금방 빈 절이 나온다”는 뜻이 아니다. 불필요한 절을 계속 만들거나 일부 변수를 처리하지 않는 전략은 비효율적일 수 있다. 증명은 적절한 유한 유도가 존재함을 보장하며, 변수 제거 절차는 그 유도를 얻는 한 방법을 제시한다. 생성되는 절의 수가 크게 늘어날 수 있으므로 완전성과 계산 효율성은 구별한다.

역사 (해결법, DPLL, NP-완전성의 역사). Davis와 Putnam은 1960년에 변수 제거에 기반한 결정 절차를 제시했고, Davis, Putnam, Logemann, Loveland는 1962년에 변수 제거 대신 단위 전파와 분기를 결합하여 기억 공간을 크게 줄인 탐색 절차를 내놓았다. 오늘날 이를 흔히 DPLL 알고리

즘이라 부른다. 절들 사이의 해결 규칙에 기반한 반박 완전성은 J. A. Robinson이 1965년에 단일화와 함께 일차논리까지 확장하여 증명하였다. 부분식마다 새 변수를 두어 식의 크기를 선형으로 유지하는 정의적 CNF 변환은 G. S. Tseitin이 1968년에 발표하였다. SAT를 해결하는 결정 절차가 존재한다는 사실(완전성)과 그 절차가 효율적인가는 별개의 질문이다. Cook은 1971년에, Levin은 독립적으로 1973년에 SAT가 NP-완전임을 증명하여, 이 문제를 계산 복잡도 이론의 중심에 놓았다.

10.6 분기 탐색의 건전성, 완전성, 종료

미정 변수 p를 고르면 모든 전체 평가는 $p = 0$ 또는 $p = 1$ 중 한 경우에 속한다. 따라서

$$S\text{가 충족가능} \iff S \restriction (p = 0) \text{ 또는 } S \restriction (p = 1)\text{이 충족가능.} \tag{10.3}$$

이 등가성을 바탕으로 단위 전파와 분기를 결합한 기본 DPLL 탐색을 다음과 같이 설명할 수 있다.

1단계. 현재 절 집합에 빈 절이 있으면 현재 갈래를 실패로 닫는다.

2단계. 남은 절이 없으면 현재 부분 평가를 해로 받아들인다.

3단계. 단위절이 있으면 단위 전파(정의 10.7)를 수행한다.

4단계. 그 밖에는 미정 변수를 하나 골라 $p = 0$과 $p = 1$ 두 값을 각각 탐색한다.

> **명제 10.12 (분기 탐색의 종료와 완전성)** 유한 변수에 대한 위 탐색이 매 분기마다 미정 변수를 하나 배정하고 두 갈래를 빠뜨리지 않으면 종료하며, 해가 존재할 때 그리고 그때에만 만족 평가를 반환한다.

증명. 한 경로에서 분기할 때마다 미정 변수 수가 줄어드므로 경로 길이는 변수 수를 넘지 않는다. 각 노드의 자식 수가 많아야 둘이므로 전체 나무가 유한하다. 단순화 보조정리(명제 10.6)와 두 값 분기의 등가성(식 (10.3)) 때문에 어떤 해도 두 갈래 모두에서 사라지지 않는다. 남은 절이 없는 갈래의 부분 평가는 미정 변수를 임의로 채워도 원래 절들을 만족한다. 반대로 빈 절이 있는 갈래는 만족 확장이 없으므로 버려도 된다. 유한 탐색의 모든 갈래가 실패할 때 정확히 해가 없다. □

> **예제 10.13** $S = \{\{p, q\}, \{p, \neg q\}, \{\neg p, r\}, \{\neg p, \neg r\}\}$를 보자. $p = 0$이면 앞의 두 절이 q와 $\neg q$가 되어 모순이다. $p = 1$이면 뒤의 두 절이 r와 $\neg r$가 되어 모순이다. 두 갈래가 모두 닫히므로 충족불가능하다. 해결법으로는 앞의 두 절에서 p, 뒤의 두 절에서 $\neg p$를 얻은 뒤 빈 절을 얻는다. 같은 불가능성을 탐색 나무와 증명 인증으로 각각 표현한 것이다.

10.7 조건을 SAT로 옮기는 예: 그래프 색칠

표기 (그래프와 색칠의 표기). 유한 **그래프**(*graph*) $G = (V, E)$는 **꼭짓점**(*vertex*) 집합 V와, 두 꼭짓점을 잇는 **변**(*edge*) 집합 E로 이루어진다. 양의 정수 k에 대해 G의 k **색칠**(k-*coloring*)은 각 꼭짓점에 $\{1, \dots, k\}$ 가운데 색을 하나씩 배정하여, 변으로 이어진 두 꼭짓점이 항상 다른 색을 갖게 하는 함수이다. 꼭짓점 부분집합 $W \subseteq V$가 정하는 **유도부분그래프**(*induced subgraph*)는 W를 꼭짓점 집합으로, 양 끝점이 모두 W에 있는 E의 변만을 변 집합으로 갖는 그래프이다.

유한 그래프의 꼭짓점 v와 색 $i \in \{1, \dots, k\}$에 대해 변수 $x_{v,i}$를 "v가 색 i를 갖는다"로 읽자. 꼭짓점마다 적어도 한 색을 요구하는 절은

$$x_{v,1} \vee \cdots \vee x_{v,k}$$

이다. 많아야 한 색은 모든 $i < j$에 대한 $\neg x_{v,i} \vee \neg x_{v,j}$로 표현한다. 변 $\{u, v\}$의 두 끝점이 같은 색 i를 쓰지 못하게 하려면 $\neg x_{u,i} \vee \neg x_{v,i}$를 넣는다.

이 CNF의 만족 평가는 정확히 올바른 k색칠에 대응한다. "적어도 하나"와 "많아야 하나"를 모두 넣어야 정확히 한 색이 된다. 문제를 논리식으로 옮길 때는 해를 만족 평가로 보내는 방향과 만족 평가를 해로 되돌리는 방향을 모두 확인해야 한다.

> **예제 10.14** 삼각형의 두 색칠은 불가능하다. 첫 꼭짓점의 색을 정하면 이웃한 두 꼭짓점은 모두 다른 색이어야 하므로 서로 같은 색을 갖게 되는데, 그 둘도 변으로 연결되어 있다. 세 색이면 세 꼭짓점에 서로 다른 색을 주면 된다. 이는 논리식 작성이 끝난 뒤 원래 문제의 간단한 구조로 결과를 검산하는 예이다.

10.8 연습문제와 해설

> **연습문제 10.15** 빈 절 집합과 빈 절을 포함한 절 집합의 만족 평가를 각각 설명하라.

풀이. 빈 절 집합은 요구할 조건이 없으므로 모든 평가가 만족한다. 빈 절을 하나라도 포함하면 그 절을 만족하는 평가가 없으므로 전체가 충족불가능하다. 알고리즘에서 "할 일이 남아 있지 않음"과 "현재 조건이 불가능함"을 서로 다른 종료 상태로 기록해야 한다.

> **연습문제 10.16** $z \leftrightarrow (p \wedge q)$의 세 정의 절 중 $(z \vee \neg p \vee \neg q)$를 빼면 어떤 잘못된 평가가 허용되는가?

풀이. $p = q = 1, z = 0$이면 남은 두 절 $\neg z \vee p$, $\neg z \vee q$는 모두 참이다. 하지만 $p \wedge q = 1$과 $z = 0$은 같지 않다. 빠진 절이 참인 두 입력에서 출력 변수를 참으로 강제하는 역방향을 담당한다.

> **연습문제 10.17** $S = \{\{p, a\}, \{p, b\}, \{\neg p, c\}\}$에서 p를 제거한 절 집합을 쓰라. $a = 0, b = 1, c = 1$인 평가를 원래 변수들로 확장하라.

풀이. 제거 결과는 $\{\{a, c\}, \{b, c\}\}$이다. 주어진 평가는 두 절을 만족한다. $a = 0$인 첫 양의 절을 만족하려면 $p = 1$이어야 하며, 그러면 다른 양의 절은 자동으로 참이고 음의 절은 $c = 1$ 덕분에 참이다.

> **연습문제 10.18** 순수 리터럴 처리를 "모든 해에서 반드시 그 부호가 참이다"라고 설명하면 왜 틀리는지 한 절 예를 들라.

풀이. 절 $p \vee q$에서 p는 순수 리터럴이지만 $p = 0, q = 1$도 해이다. $p = 1$로 두는 것은 다른 해가 있더라도 적어도 하나의 해를 남긴다는 선택이지, 논리적 귀결 $S \models p$를 주장하는 것이 아니다.

> **연습문제 10.19** 세 변수 p, q, r의 "정확히 하나가 참"을 CNF로 쓰고, 각 종류의 절이 필요한 이유를 설명하라.

풀이. $(p \vee q \vee r) \wedge (\neg p \vee \neg q) \wedge (\neg p \vee \neg r) \wedge (\neg q \vee \neg r)$이다. 첫 절은 모두 거짓인 평가를 배제한다. 나머지는 두 개 이상 참인 평가를 배제한다. 세 변수가 모두 참인 경우도 임의의 쌍에 대한 금지 절을 위반하므로 별도 삼중 금지 절은 필요하지 않다.

> **연습문제 10.20** 유한 해결 완전성 정리가 일반 일차논리의 모든 문제를 같은 유한 절차로 결정한다는 결론을 주지 않는 이유를 설명하라.

풀이. 여기서는 입력에 나타난 명제 변수의 개수가 유한하고, 제거할 때마다 그 수가 줄어든다는 귀납을 사용했다. 일차논리에는 대상 변수, 양화사, 함수항과 구조의 해석이 있어 단순히 같은 유한 변수 제거 논증을 적용할 수 없다. 명제 변수와 일차논리의 대상 변수를 이름이 비슷하다는 이유로 같은 계산 대상으로 보아서는 안 된다.

다음 연결. 유한 SAT에서는 실제로 모든 후보를 유한하게 다룬다. 제4권 제11장의 콤팩트성은 무한한 조건 모음에 대해 유한 부분마다 해가 있다는 사실이 어떤 전역적 존재를 보장하는지 설명한다.

제 11 장

유한 조건과 무한 조건: 콤팩트성의 의미

개요 조건이 유한 개이면 모두 함께 놓고 해를 찾을 수 있다. 조건이 무한 개일 때 "아무리 많은 유한 조건을 가져와도 해가 있다"는 사실은 전체의 해를 보장할까? 어떤 종류의 조건과 어떤 해 공간을 사용하는지에 따라 답이 다르다. **콤팩트성**(*compactness*)은 이 질문에 정확한 가정을 붙여 답하는 정리이다. 이 장은 가산 명제언어의 콤팩트성(11.3절)을 이진 나무의 경로 보조정리(11.2절)로부터 직접 증명하고, 모순의 유한 지지(11.4절)와 무한 그래프의 유한 색칠(11.5절)에 응용한다. 일반 일차논리의 콤팩트성은 증명을 뒤의 모형론 권으로 미루고, 그 정확한 진술과 자주 저지르는 오적용만을 구별하여 소개한다(11.6절). 선행 지식: 명제논리의 충족가능성, 제4권 제10장의 유한 SAT와 해결법, 유한열과 수학적 귀납법.

11.1 유한 충족가능성의 양화사

정의 11.1 (유한 충족가능성) 논리식들의 집합 Γ가 **유한 충족가능**(*finitely satisfiable*)하다는 것은 모든 유한 부분집합 $\Gamma_0 \subseteq \Gamma$가 만족 평가를 갖는다는 뜻이다. 그 구조는

$$\forall \Gamma_0 \subseteq \Gamma \ (\text{유한}) \quad \exists v \quad v \models \Gamma_0 \tag{11.1}$$

이다. 전체 충족가능성은 $\exists v \, \forall \varphi \in \Gamma \, (v \models \varphi)$이다.

유한 충족가능성에서는 부분집합마다 서로 다른 평가를 써도 된다. 전체 충족가능성에서는 하나의 평가가 모든 조건을 동시에 만족해야 한다. 단순히 양화사의 순서를 바꾼 것만으로 결론을 얻을 수 없으며, 사용하는 논리의 특별한 성질이 필요하다.

각 식을 따로 만족시킬 수 있다는 조건은 훨씬 약하다. p도 만족가능하고 $\neg p$도 만족가능하지만 두 식을 함께 만족시킬 수는 없다. 유한 충족가능성은 한 개짜리 부분집합만이 아니라 두 개, 세 개, 그리고 임의의 유한 개를 함께 검사한다.

예제 11.2 변수 $p_0, p_1, \ldots$에 대해 $\Gamma = \{p_n : n \in \mathbb{N}\}$이라 하자. 모든 변수를 참으로 두면 전체를 만족하므로 유한 충족가능하다. 한편 각 유한 부분집합의 해를 찾을 때 그 밖의 변수를 모두 거짓으로 두는 식으로 선택하면, 부분집합이 달라질 때 평가도 달라진다. 이 서로 다른 해들을 아무 설명 없이 하나의 함수로 합칠 수는 없다. 공통 전역 해의 존재와 임의로 고른 부분 해들의 일치 여부는 다른 질문이다.

11.2 유한 분기 나무의 무한 경로

정의 11.3 (이진 나무와 무한 경로) 유한한 0, 1 수열들의 집합을 $\{0,1\}^{<\mathbb{N}}$로 쓴다. 그 부분집합 T가 어떤 수열을 포함할 때 그 수열의 모든 초기 부분수열도 포함하면 **이진 나무**(*binary tree*)라 한다. 길이 n인 수열을 **깊이 n**의 꼭짓점이라 한다. 무한열 $b_0, b_1, \ldots$의 모든 유한 초기 부분이 T에 속하면 그 열을 **무한 경로**(*infinite path*)라 한다.

보조정리 11.4 (이진 나무의 경로 보조정리) 이진 나무 T에 임의로 깊은 꼭짓점이 있으면 T에는 무한 경로가 있다.

증명. 어떤 꼭짓점 아래로 길이를 제한 없이 늘려 갈 수 있으면 그 꼭짓점을 계속 확장 가능한 꼭짓점이라 부르자. 빈 수열은 가정에 의해 계속 확장 가능하다. 계속 확장 가능한 꼭짓점의 두 자식 모두에서 가능한 추가 길이가 유계이면 그 두 상한 중 큰 것으로 부모 아래 길이도 제한된다. 따라서 적어도 한 자식은 계속 확장 가능하다.

각 단계에서 0을 붙인 자식이 계속 확장 가능하면 그쪽을 택하고, 그렇지 않으면 1을 붙인 자식을 택한다. 앞의 관찰 때문에 둘 중 한쪽이 항상 존재한다. 자연수 재귀로 무한열을 만들면 모든 초기 부분이 T에 속한다. 이것이 원하는 무한 경로이다. □

이 증명은 경로의 존재를 보이지만, 임의로 주어진 나무에서 "이 자식은 제한 없이 확장 가능한가"를 유한 시간에 판정하는 알고리즘을 제공한 것은 아니다. 수학적으로 대상을 정의할 수 있다는 말과 유한 절차로 계산할 수 있다는 말은 구별한다.

유한 분기가 핵심이다. 뿌리 아래에 길이 $1, 2, 3, \ldots$인 유한 사슬을 각각 하나씩 붙이면 전체에는 임의로 깊은 꼭짓점이 있지만 무한 경로는 없다. 뿌리의 자식 수가 무한하기 때문이다. 경로 보조정리를 사용할 때 전체 나무가 무한하다는 사실만 확인해서는 부족하다.

역사 (König의 나무 보조정리). 보조정리 11.4는 *König's lemma*라 불리는 일반적 사실의 이진 나무 경우이다. Dénes König은 1927년에, 각 꼭짓점의 자식 수가 유한한(이진 나무를 포함하는) 무한 나무에는 반드시 무한 경로가 있음을 증명하였다. 뿌리의 자식 수가 무한할 수 있는 나무에서는 위의 반례처럼 결론이 깨진다.

11.3 가산 명제논리의 콤팩트성

정리 11.5 (가산 명제논리의 콤팩트성) 명제 변수들이 $p_0, p_1, p_2, \ldots$인 언어에서 논리식 집합 Γ는 충족가능할 필요충분조건이 유한 충족가능한 것이다.

증명. 전체를 만족하는 평가는 모든 부분집합도 만족하므로 한 방향은 즉시 성립한다. 역방향을 보이자. 논리식은 가산한 기호의 유한열로 쓰이므로 가능한 논리식들의 집합도 가산하다. 따라서 Γ를 $\varphi_0, \varphi_1, \ldots$로 나열할 수 있다. Γ가 유한하면 항진식을 반복하여 무한 목록으로 만들어도 된다. 빈 경우는 아무 평가나 택하면 된다. 이 나열이 계산 가능한 나열이라고 가정할 필요는 없다.

길이 n인 이진열 s를 변수 $p_0, \ldots, p_{n-1}$의 부분 평가로 읽는다. 나무 T에는 다음 조건을 만족하는 s를 넣는다. $i < n$이고 φ_i의 모든 변수가 앞의 n개 변수 중에 있으면 s가 φ_i를 참으로 만들어야 한다. 더 짧은 초기 부분에서는 검사할 식의 목록과 사용 가능한 변수 모두 줄어드므로, T는 초기 부분에 닫힌 이진 나무이다.

유한 충족가능성에 의해 $\varphi_0, \dots, \varphi_{n-1}$을 동시에 만족하는 전체 평가가 있다. 이를 앞의 n개 변수로 제한하면 깊이 n의 T 꼭짓점을 얻는다. 따라서 임의로 깊은 꼭짓점이 있고, 경로 보조정리(보조정리 11.4)로 무한 경로 $b_0, b_1, \dots$가 존재한다. $v(p_j) = b_j$로 정하자.

임의의 $\varphi_i \in \Gamma$를 잡는다. 이 식에는 유한 개의 변수만 있으므로 $n > i$이고 그 모든 변수가 $p_0, \dots, p_{n-1}$에 포함되도록 n을 충분히 크게 잡을 수 있다. 경로의 길이 n인 초기 부분은 T에 속하므로 φ_i를 참으로 만든다. 전체 평가 v도 그 변수들에서 값이 같으므로 φ_i를 만족한다. 모든 i에 성립하므로 $v \models \Gamma$이다. □

이 증명에서 각 논리식이 유한 개 변수에만 의존한다는 점과 평가의 각 자리가 두 선택지만 갖는다는 점이 함께 쓰였다. 무한한 논리곱을 하나의 식으로 허용하는 다른 논리로 옮기면 같은 증명이 자동으로 성립하지 않는다.

임의의 크기의 명제변수 집합에 대한 일반 콤팩트성은 선택 원리와 연결된다. 여기서는 자연수로 번호를 매긴 가산 경우를 실제로 증명했으며, 더 일반적인 명제를 같은 증명으로 처리했다고 주장하지 않는다.

11.4 유한한 모순 증거와 귀결의 유한 지지

따름정리 11.6 (콤팩트성의 대우) 위 가산 언어에서 Γ가 충족불가능하면 어떤 유한 부분집합 $\Gamma_0 \subseteq \Gamma$가 이미 충족불가능하다.

이는 정리 11.5의 대우이다. 전체 무한 조건이 실패했다면 실패 원인은 유한한 조건들 안에서 드러난다. 어떤 유한 부분집합인지를 효과적으로 찾아 주는 절차를 언제나 가진다는 말은 아니다. 특히 Γ의 원소들을 어떻게 제시받는지도 계산 문제에서 중요하다.

따름정리 11.7 (귀결의 유한 지지) $\Gamma \models \psi$이면 어떤 유한 부분집합 $\Gamma_0 \subseteq \Gamma$에 대해 $\Gamma_0 \models \psi$이다.

증명. $\Gamma \cup \{\neg\psi\}$는 충족불가능하다. 따라서 따름정리 11.6에 의해 충족불가능한 유한 부분집합 F가 있다. $\Gamma_0 = F \cap \Gamma$로 두면 $\Gamma_0 \cup \{\neg\psi\}$는 F를 포함하므로 역시 충족불가능하다. 따라서 $\Gamma_0 \models \psi$이다. □

앞 묶음(제4권 제10장)에서 유한한 증명은 유한 개 가정만 사용한다는 구문적 관찰을 했다. 여기서는 모든 평가에 대한 의미론적 귀결도 유한 개 전제로 지지된다는 사실을 얻었다. 두 진술이 닮은 것은 우연이 아니지만, 그 연결을 정리로 만들려면 건전성·완전성 같은 메타정리가 필요하다. 이 장의 가산 명제논리 결과는 나무를 사용하여 직접 증명했다.

예제 11.8 $\Gamma = \{p_0,\ p_0 \to p_1,\ p_1 \to p_2, \dots\}$이면 각 고정된 k에 대해 $\Gamma \models p_k$이다. 실제로 p_0부터 $p_{k-1} \to p_k$까지 유한 부분만 있으면 충분하다. 하지만 하나의 동일한 유한 부분집합이 모든 p_k를 동시에 함의해야 한다는 결론은 나오지 않는다. 결론 p_k에 따라 필요한 유한 부분이 달라질 수 있다.

11.5 응용: 무한 그래프의 유한 색칠 조건

정리 11.9 (무한 그래프의 유한 색칠) 꼭짓점 집합이 유한 또는 가산인 그래프 G와 양의 정수 k를 고정하자. 모든 유한 유도부분그래프가 k색칠 가능하면 전체 그래프도 k색칠 가능하다.

증명. 각 꼭짓점 v와 색 $i \in \{1, \dots, k\}$에 변수 $x_{v,i}$를 두고, 꼭짓점마다 정확히 한 색을 쓰며 변의 양 끝점은 다른 색을 쓴다는 절들을 만든다(제4권 제10장의 그래프 색칠 부호화와 같다). 꼭짓점이 가산이고 k가 유한하므로 변수와 절은 가산하다.

임의의 유한 절 모음을 고르면 그 안에 등장하는 꼭짓점은 유한 개뿐이다. 그 꼭짓점들이 만드는 유도부분그래프를 올바르게 k색칠할 수 있다는 가정에 의해 해당 절들을 모두 만족시키는 변수 값을 정할 수 있다. 목록에 없는 변수는 임의로 채우면 되므로 모든 유한 절 모음이 충족가능하다. 명제논리의 콤팩트성(정리 11.5)으로 전체 절을 만족하는 평가가 있고, 그 평가를 색칠로 읽으면 전체 그래프의 k색칠을 얻는다. □

개별 유한 부분그래프의 색칠을 미리 골라 놓으면 서로 겹치는 꼭짓점에서 다른 색을 줄 수 있다. 증명은 그 임의의 색칠들을 그대로 합친 것이 아니라, 전체 조건에 맞는 일관된 선택이 존재함을 보였다. 유한 국소 해와 전역 해 사이의 일관성을 확보하는 것이 콤팩트성의 역할이다.

k를 하나의 고정된 수로 두는 조건도 중요하다. "모든 유한 부분그래프가 어떤 유한 수의 색으로 색칠된다"는 말은 모든 그래프에 너무 쉽게 성립한다. 가산 무한 완전그래프(complete graph)는 각 유한 부분이 유한 색칠 가능하지만 전체를 고정된 유한 k개 색으로 칠할 수 없다.

역사 (드브라윈–에르되시 정리). 정리 11.9과 그 비가산 경우(선택공리 전체보다 약한 선택 원리, 곧 불리언 소아이디얼 정리에 기대는 형태)는 N. G. de Bruijn과 P. Erdős가 1951년에 증명하였으며, 흔히 *de Bruijn–Erdős theorem*이라 부른다. 여기서 증명한 가산 꼭짓점의 경우는 그래프를 명제논리로 부호화하고 가산 콤팩트성만 사용하면 충분하다.

11.6 일차논리로 확장할 때의 정확한 진술

정리 11.10 (일차논리 콤팩트성; 증명은 모형론 권으로 이관) 동일한 일차언어의 문장 집합 T에서 모든 유한 부분집합이 모형을 가지면 T 전체도 모형을 가진다. 정의역은 비어 있지 않은 임의의 집합을 허용하며, 유한 모형으로 제한하지 않는다.

이 정리는 앞의 이진 평가 나무를 그대로 사용한 결과가 아니다. 명제논리와 달리 대상, 함수, 관계의 해석을 함께 만들어야 한다. 제6권 모형론·증명론·계산가능성에서는 적절한 증명 체계의 완전성 또는 구조의 구성 방법을 통해 증명한다. 지금은 정리의 내용과 잘못 적용되는 지점을 구별한다.

예제 11.11 (유한 모형만으로 제한하면 실패) 각 $n \geq 1$에 대해 "서로 다른 원소가 적어도 n개 존재한다"는 문장

$$\sigma_n := \exists x_1 \cdots \exists x_n \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j$$

을 만든다. $n = 1$에서 빈 논리곱은 참으로 해석한다. 이 문장들의 유한 부분집합은 가장 큰 요구 수만큼의 유한 집합에서 만족된다. 그러나 전체 문장들을 만족하는 유한 집합은 없다. 무한

> 집합은 모두를 만족하므로 일반 콤팩트성과 충돌하지 않는다. “모형이 있다”를 “유한 모형이 있다”로 바꾸면 정리가 달라진다.

> **예제 11.12 (고정된 구조에서의 증인 존재와 다름)** 실수 x에 대한 조건 $x > 0, x > 1, x > 2, \dots$는 어떤 유한 개를 택해도 실수 해가 있다. 하지만 모든 자연수보다 큰 실수는 없다. 일차논리 콤팩트성은 이러한 조건에 맞는 원소가 반드시 원래의 통상적 실수 구조 안에 있다고 보장하지 않는다. 언어와 문장 집합을 정한 뒤 모든 모형을 허용하는 정리이다. 고정된 해 공간 안에서 유한 교차 성질을 전역 해로 바꾸려면 그 공간의 별도 조건이 필요하다.

해석학의 콤팩트 집합에서는 닫힌 부분집합들의 유한 교차 성질이 전체 교차의 비어 있지 않음을 보장한다. 여기서 닫힘과 콤팩트한 바탕 공간이 핵심이다. 실수 전체의 닫힌 반직선 $[n, \infty)$들은 유한 교차가 비어 있지 않지만 전체 교차는 비어 있다. “콤팩트성”이라는 이름만 보고 필요한 공간 가정을 생략해서는 안 된다.

11.7 연습문제와 해설

> **연습문제 11.13** 조건 $\Gamma = \{p_n \vee p_{n+1} : n \in \mathbb{N}\} \cup \{\neg p_{2n} : n \in \mathbb{N}\}$의 전체 만족 평가를 직접 구성하라.

풀이. 짝수 번호 변수는 거짓, 홀수 번호 변수는 참으로 둔다. 서로 이웃한 두 번호 중 하나는 홀수이므로 각 논리합이 참이고, 짝수 변수의 부정도 참이다. 이 경우에는 콤팩트성을 불러오기 전에 명시적인 해를 만들 수 있다. 존재 정리는 항상 가장 짧은 증명 방법인 것은 아니다.

> **연습문제 11.14** 위 조건에 $\neg p_1$을 추가하면 어떤 유한 부분이 이미 모순을 만드는가?

풀이. $\{p_0 \vee p_1,\ \neg p_0,\ \neg p_1\}$만으로 충족불가능하다. 전체 무한 목록을 확인할 필요가 없다. 이 세 절에서 단위 전파 또는 두 번의 해결로 빈 절을 얻을 수 있다.

> **연습문제 11.15** 이진 나무에 “모든 자연수 n에 대해 깊이 n의 꼭짓점이 있다”는 조건 대신 “꼭짓점이 무한히 많다”만 주어도 이 장의 보조정리를 적용할 수 있는가?

풀이. 이진 나무에서는 가능하다. 깊이가 N 이하라면 꼭짓점 수는 많아야 $1 + 2 + \cdots + 2^N$으로 유한하다. 따라서 무한히 많은 꼭짓점이 있으면 깊이가 제한되지 않는다. 임의의 무한 분기 나무에서는 깊이 1에 무한히 많은 자식을 둘 수 있으므로 같은 추론이 성립하지 않는다.

> **연습문제 11.16** 모든 유한 부분그래프가 두 색으로 칠해진다는 조건에서, 각 변만 두 색으로 칠해진다는 조건으로 약화하면 충분한가?

풀이. 충분하지 않다. 삼각형의 각 변만 보면 두 꼭짓점에 서로 다른 두 색을 줄 수 있지만 세 변을 함께 보면 두 색칠이 불가능하다. 유한 부분의 크기를 2로 제한한 검사는 모든 유한 부분을 검사한 것과 다르다.

> **연습문제 11.17** 가산 명제논리에서 $\Gamma \models \psi$이고 Γ가 무한할 때, 유한 지지 따름정리가 보장하는 것과 보장하지 않는 것을 구별하라.

풀이. 보장하는 것은 어떤 유한 $\Gamma_0 \subseteq \Gamma$만으로도 ψ가 따라온다는 존재이다. 임의로 고른 처음 열 개 전제가 충분하다는 뜻도 아니고, Γ가 임의의 방식으로 주어졌을 때 그 부분집합을 계산할 수 있다는 뜻도 아니다. 또한 서로 다른 모든 결론에 같은 Γ_0를 사용할 수 있다는 주장도 아니다.

> **연습문제 11.18** 닫힌구간 $[0, 1/n]$의 전체 교차와 열린구간 $(0, 1/n)$의 전체 교차를 구하라. 각각의 유한 교차는 어떤가?

풀이. $n \geq 1$에 대해 닫힌구간들의 전체 교차는 $\{0\}$이고 열린구간들의 전체 교차는 공집합이다. 유한 교차는 가장 작은 구간과 같아서 두 경우 모두 비어 있지 않다. 열린 경우에는 0이 제외되며 어떤 양수도 모든 $1/n$보다 작을 수 없다. 바탕 $[0, 1]$의 콤팩트성을 쓸 때 부분집합의 닫힘 조건이 필요한 이유를 보여 준다.

다음 연결. 앞 장들의 결과를 실제로 적용할 때는 조건을 읽는 작은 차이가 결론을 바꾼다. 제4권 제12장에서는 오류가 있는 풀이를 고쳐 쓰고, 반례의 크기와 가정의 역할을 체계적으로 점검한다.

제 12 장

증명 교정 실습과 반례 설계

개요 이 장은 이 권에서 익힌 양화사의 언어, 증명 방법, 관계와 함수, 순서와 콤팩트성을 실제 증명 읽기에 적용하는 열한 개의 연습문제를 모은다. 각 연습문제는 그럴듯하게 들리는 하나의 풀이를 제시하고, 그 풀이가 무너지는 지점을 밝힌 뒤 올바른 명제와 증명 또는 반례로 바로잡는다. 다루는 오류의 유형은 양화사의 순서를 뒤바꾸는 오류, "유일하다"가 존재까지 포함하는지를 혼동하는 오류, 몫집합의 대표원에 의존하는 표기를 잘 정의된 함수로 착각하는 오류, 함수 합성을 수처럼 약분하는 오류, 집합의 크기와 순서형을 혼동하는 오류, 충족가능성만으로 논리적 동치를 대신하는 오류, 탐색의 한 갈래만 보고 전체의 불가능성을 단정하는 오류, 특정 분모로 나눈 공식의 적용 범위를 놓치는 오류, 유한한 기술의 개수에 관한 사실을 무한 대상 전체로 확대하는 오류, 선택공리가 필요한 경우와 필요하지 않은 경우를 가르지 못하는 오류이다. 마지막 절은 이런 검토를 기록으로 남기는 방법과, 이 권에서 증명한 결과의 사용 범위를 정리한다. 선행 지식: 이 권 제1장(양화사의 언어)과 제2장(명제논리), 제6장(귀납법), 제7장(관계·분할·몫집합), 제8장(함수·섬유·역함수와 크기 비교), 제9장(부분순서·정렬·최대성), 제10장(정규형과 해결법), 제11장(콤팩트성).

이 장의 여러 반례는 다음 두 문장의 방향을 혼동하는 데서 생긴다.

핵심 수식

$$\exists y\, \forall x\, P(x,y) \implies \forall x\, \exists y\, P(x,y)$$

역은 일반적으로 성립하지 않는다. 왼쪽은 모든 경우에 공통으로 통하는 하나의 증인을 요구하고, 오른쪽은 경우마다 다른 증인을 허용한다.

12.1 의존 관계: 하나의 시점을 모두에게 쓸 수 있는가

연습문제 12.1 (점별 조건과 공통 조건) $k, n \in \mathbb{N}$에 대해

$$a_n(k) = \begin{cases} 1, & n \le k, \\ 0, & n > k \end{cases}$$

로 둔다. 다음 풀이를 검토하고 두 양화 문장의 참과 거짓을 판정하라.

"각 k에서 충분히 큰 n이면 $a_n(k) = 0$이다. 따라서 충분히 큰 하나의 N을 골라 모든 k와 모든 $n \ge N$에서 $a_n(k) = 0$으로 만들 수 있다."

풀이. 첫 주장은

$$\forall k \in \mathbb{N}\, \exists N \in \mathbb{N}\, \forall n \ge N\ (a_n(k) = 0)$$

이며 참이다. 주어진 k에 대해 $N = k+1$로 두면 된다. 둘째 주장은

$$\exists N \in \mathbb{N}\, \forall k \in \mathbb{N}\, \forall n \geq N\ (a_n(k) = 0)$$

이며 거짓이다. 임의의 후보 N에 대해 $k = N$, $n = N$으로 두면 $a_N(N) = 1$이다. 첫 증인 N이 k에 의존한다는 점을 지우면 잘못된 강화가 된다.

수정된 결론. k의 범위를 유한 집합 $\{0, \dots, K\}$로 제한하면 $N = K+1$이 모든 k에 공통으로 통한다. 따라서 문제는 각 개별 증인의 존재가 아니라 증인들을 하나의 상한으로 묶을 수 있는지에 있다. 함수열의 점별수렴과 균등수렴을 가르는 것도 같은 양화 구조이다(제10권 제2장).

12.2 존재와 유일성: 관계가 정말 함수인가

> **연습문제 12.2 (양쪽의 정확히 하나)** 관계 $R \subseteq X \times Y$가 다음을 만족한다고 하자.
>
> $$\forall x \in X\ \exists! y \in Y\ R(x,y), \qquad \forall y \in Y\ \exists! x \in X\ R(x,y).$$
>
> 이 관계가 전단사 함수의 그래프임을 증명하라. 두 문장에서 유일성을 모두 빼면 같은 결론이 남는지도 판정하라.

풀이. 첫 조건은 각 입력에 정확히 하나의 출력을 주므로 함수 $f : X \to Y$를 정의한다. 둘째 조건의 존재 부분으로 모든 y에 원상이 있으므로 전사이다. 둘째 조건의 유일성 부분으로 같은 출력에 서로 다른 두 입력이 갈 수 없으므로 단사이다.

유일성을 빼면 일반 관계일 뿐이다. $X = Y = \{0,1\}$, $R = X \times Y$로 두면 모든 입력에 관련된 출력이 있고 모든 출력에 관련된 입력이 있지만, 한 입력에 출력이 두 개이므로 함수의 그래프가 아니다. 유일성의 위치에 따라 보장되는 성질이 다르다. 첫 유일성은 함수로서의 단일값, 둘째 유일성은 단사성이다.

빈 집합 검사. $X = Y = \emptyset$이면 두 조건은 공허하게 참이고 빈 함수는 전단사이다. 한쪽만 비면 비어 있지 않은 쪽의 전칭 대상에 필요한 존재 조건이 실패한다. 따라서 정확한 문장은 빈 경우에도 일관되게 작동한다.

12.3 대표원 의존성: 좌표 하나로 몫을 표시할 때

> **연습문제 12.3 (직선 방향의 잘못된 좌표)** $X = \mathbb{R}^2 \setminus \{(0,0)\}$에서 $u \sim v$를 어떤 $c \in \mathbb{R} \setminus \{0\}$에 대해 $v = cu$임으로 정의한다. "각 류를 기울기 y/x에 대응시키면 $X/\!\sim$는 $\mathbb{R}$과 전단사이다"라는 풀이를 검사하고, 자연스러운 올바른 표기를 제시하라.

풀이. 먼저 관계는 동치관계이다. 상수 1이 반사성을, $1/c$가 대칭성을, 두 배율의 곱이 추이성을 준다. $x \neq 0$인 벡터들의 류에서는 y/x가 대표를 바꾸어도 같으므로 좋은 좌표이다. 그러나 수직 방향의 류는 모든 대표가 첫 좌표 0을 가져 그 식이 정의되지 않는다.

각 류는 정확히 하나의 $(1,t)$, $t \in \mathbb{R}$ 또는 $(0,1)$로 표시할 수 있다. 첫 좌표가 0이 아니면 $1/x$배 하여 $(1, y/x)$로 만들고, 첫 좌표가 0이면 둘째 좌표가 0이 아니므로 $(0,1)$로 만든다. 서로 다른 두 $(1,t)$가 같은 류이면 첫 좌표에서 배율이 1이어야 하므로 t도 같고, 수직 류는 그들과 다르다.

따라서 자연스러운 매개 집합은 $\mathbb{R}$에 수직 방향을 뜻하는 원소 하나를 더한 집합이며, 이는 실수 사영직선에 해당한다.

검토 범위. 원래 제시한 기울기 함수가 전단사가 아니라는 사실을 보였을 뿐, 이 몫집합과 $\mathbb{R}$ 사이에 다른 방식의 전단사가 전혀 없다고 결론 내린 것은 아니다. 실제로 무한 집합의 크기 비교에서는 원소 하나를 더해도 같은 크기일 수 있다(제4권 제8장). 특정 공식의 실패와 임의의 함수 존재 불가능성을 구별한다.

12.4 합성 등식: 멱등함수의 숨은 가정

> **연습문제 12.4 (멱등함수의 약분)** 함수 $f : X \to X$가 $f \circ f = f$를 만족한다고 하자. "양변의 f를 약분하면 $f = \mathrm{id}_X$이다"라는 주장을 검토하라. 단사 또는 전사라는 가정을 각각 추가하면 무엇이 되는가?

풀이. 일반적으로 함수 합성을 약분할 수 없다. $X = \{0, 1\}$에서 $f(0) = f(1) = 0$인 상수함수는 $f(f(x)) = f(x)$를 만족하지만 항등함수가 아니다.

f가 단사이면 각 x에서 $f(f(x)) = f(x)$에 단사성을 적용하여 $f(x) = x$를 얻는다. f가 전사이면 임의의 $y \in X$에 대해 $f(x) = y$인 x를 잡고 $f(y) = f(f(x)) = f(x) = y$를 얻는다. 따라서 어느 가정을 추가해도 항등함수라는 결론이 참이다. 두 증명은 같은 "약분"이라는 말로 묶을 수 있지만 실제 논리는 다르다.

구조적 해석. 가정 없이도 f는 자신의 상에서는 항등으로 작용한다. 실제로 $y = f(x)$이면 $f(y) = y$이다. 그러므로 **멱등함수**(*idempotent function*)는 입력들을 상 안의 고정점으로 모으는 함수로 볼 수 있다. 잘못된 전체 결론에서 참인 부분 결론을 분리하는 예이다.

12.5 기수와 순서형: 같은 수의 원소, 다른 순서

> **연습문제 12.5** $\mathbb{N} \times \mathbb{N}$에 사전식 순서를 주자. 다음 두 주장을 각각 판단하라.
> (1) $\mathbb{N} \times \mathbb{N}$과 $\mathbb{N}$은 전단사로 대응한다.
> (2) 이 사전식 순서와 자연수의 통상 순서는 순서동형이다.

풀이. 첫 주장은 참이다. $s = m + n$인 대각선을 순서대로 나열하는 함수

$$\pi(m, n) = \frac{(m+n)(m+n+1)}{2} + n$$

를 쓴다. 고정된 s에서 $n = 0, \dots, s$가 변하면 값은 $s(s+1)/2$부터 $(s+1)(s+2)/2 - 1$까지 연속한 정수 구간을 한 번씩 방문한다. 이 구간들이 자연수를 겹치지 않게 덮으므로 전단사이다.

둘째 주장은 거짓이다. 사전식 순서에서 $(1, 0)$보다 작은 원소로 $(0, 0), (0, 1), (0, 2), \dots$가 모두 있어 무한히 많다. 자연수 N보다 작은 자연수는 $0, \dots, N-1$의 유한 개이다. 순서동형은 한 원소보다 작은 원소들의 집합을 서로 전단사로 대응시켜야 하므로 이런 차이를 보존할 수 없다.

수정된 이해. 원소 수의 같음은 집합으로서의 대응이고, 순서형의 같음은 순서까지 보존하는 대응이다. 더 많은 구조를 보존하도록 요구하면 가능한 함수가 줄어든다. 기수와 순서수를 다른 불변량으로 다루는 이론은 이후 권에서 정리한다(제5권 제5장).

12.6 집합 연산: 여집합을 보존하는 상의 조건

> **연습문제 12.6** $f : X \to Y$에 대해 모든 $A \subseteq X$에서
>
> $$f(X \setminus A) = Y \setminus f(A)$$
>
> 가 성립할 필요충분조건은 f가 전단사임을 증명하라.

풀이. f가 전단사라고 하자. $y = f(x)$이고 $x \notin A$이면 단사성 때문에 y는 A의 다른 원소에서 나올 수 없으므로 $y \notin f(A)$이다. 따라서 왼쪽이 오른쪽에 포함된다. 반대로 $y \notin f(A)$이면 전사성으로 원상 x가 있으며 이 x는 A에 있을 수 없다. 따라서 오른쪽이 왼쪽에 포함된다.

이제 모든 A에서 등식을 가정한다. $A = \emptyset$을 대입하면 $f(X) = Y$이므로 전사이다. 단사가 아니면 서로 다른 x, x'에 대해 $f(x) = f(x')$이다. $A = \{x\}$로 두면 $x' \in X \setminus A$이므로 공통 출력은 왼쪽에 속하지만 동시에 $f(A)$에 속해 오른쪽에는 속할 수 없다. 등식에 모순이므로 단사이다.

검토 기준. 충분성을 보일 때 단사성과 전사성이 각각 어느 포함에 쓰였는지 확인했다. 필요성을 보일 때는 특수한 부분집합 $\emptyset, \{x\}$만으로 두 성질을 끌어냈다. 모든 부분집합에 대한 가정을 사용할 때 가장 단순한 부분집합부터 대입해 보는 전략이 효과적이다.

12.7 논리식 대체: 충족가능성이 같으면 바꿔도 되는가

> **연습문제 12.7** 두 식 φ, ψ가 둘 다 충족가능하므로 어떤 더 큰 식 안에서도 서로 바꿔 넣어도 된다는 주장을 반박하라. 올바른 대체 기준을 설명하라.

풀이. $\varphi = p$, $\psi = q$를 택하면 둘 다 충족가능하다. 그러나 $\varphi \wedge \neg p = p \wedge \neg p$는 충족불가능하고, $\psi \wedge \neg p = q \wedge \neg p$는 $q = 1, p = 0$에서 만족된다. 단지 해가 하나라도 존재한다는 여부가 같다고 해서 다른 조건과 결합한 뒤에도 같은 동작을 하는 것은 아니다.

모든 평가에서 진리값이 같은 논리적 동치라면 연결사로 만든 문맥 안에서 대체해도 값이 보존된다. 이는 문맥의 구성에 대한 귀납으로 증명한다. 대체하는 작은 식의 값이 같고, 각 연결사의 출력은 입력 진리값에만 의존하기 때문이다.

정의적 CNF와의 연결. 새 변수를 사용하는 변환은 이 반례를 무시하는 예외가 아니다. 정의 절들이 새 변수 값을 원래 부분식에 정확히 묶고, 새 변수들을 존재적으로 제거했을 때 원래 조건이 복원됨을 따로 증명했다(제4권 제10장). 새 변수의 이름은 바깥 문맥의 기존 변수와 겹치지 않아야 한다. 그렇지 않으면 원래 없던 의존 조건을 만들 수 있다.

12.8 알고리즘의 결론: 탐색 실패와 불가능성

> **연습문제 12.8** 한 SAT 프로그램이 변수 $p = 0$인 갈래를 모두 검사하여 해가 없음을 확인했다. 따라서 입력 전체가 충족불가능하다고 보고했다. 빠진 검사를 밝히고, 구체적인 입력에서 오류를 드러내라.

풀이. $p=1$인 갈래가 빠졌다. 입력 $S=\{\{p\}\}$이면 $p=0$인 갈래는 빈 절이 되어 실패하지만 $p=1$이면 모든 절이 만족된다. 한 갈래에서 해가 없다는 것은 해당 부분 평가를 확장하는 해가 없다는 뜻이지 전체 해의 부재가 아니다.

올바른 불가능성 보고에는 모든 경우를 덮는 탐색 또는 건전한 반박 인증이 필요하다. 유한 SAT에서는 두 갈래를 모두 탐색하고 미정 변수 수가 줄어든다는 종료 논증을 함께 주면 완전한 결정을 얻는다(제4권 제10장). 반대로 시간 제한 때문에 종료한 탐색은 그 시간 안에 해를 못 찾았다는 사실만 보고해야 한다.

구체적인 인증. $\{\{p,q\},\{p,\neg q\},\{\neg p\}\}$에서는 $p=0$이 마지막 절(리터럴 하나뿐인 절, *unit clause*)에 의해 강제되고, 앞의 두 절이 q, $\neg q$가 된다. 이 경우에는 다른 갈래가 해가 될 가능성을 단위절이 이미 배제했다. 따라서 모든 p값을 별도 순회하지 않아도 논리적 근거를 기록하면 완전한 결론이 가능하다.

12.9 귀납 검토: 목표의 매개변수 범위를 고정하기

> **연습문제 12.9** 실수 r와 자연수 n에 대해
>
> $$1+r+\cdots+r^{n}=\frac{r^{n+1}-1}{r-1}$$
>
> 이라는 공식을 모든 r에서 증명하려는 풀이를 검토하고, 정확한 정리와 증명을 쓰라.

풀이. 오른쪽은 $r=1$에서 정의되지 않는다. 올바른 식은

$$\sum_{k=0}^{n} r^{k}=\begin{cases}(r^{n+1}-1)/(r-1), & r\neq 1,\\ n+1, & r=1\end{cases}$$

이다.

$r\neq 1$을 고정하고 $S=\sum_{k=0}^{n} r^{k}$라 두면 $rS-S=r^{n+1}-1$이다. $r-1\neq 0$이므로 나누어 첫 식을 얻는다. $r=1$이면 합에 1이 $n+1$개 있으므로 둘째 식이다.

나눗셈 없는 식.

$$(r-1)\sum_{k=0}^{n} r^{k}=r^{n+1}-1$$

은 $r=1$을 포함한 모든 실수에서 참이다. 다만 $r=1$에서 양변이 0이 되어 합의 값을 결정해 주지 않는다. 항상 참인 곱셈 항등식과 특정 분모로 나눈 공식의 적용 범위를 구별해야 한다.

12.10 유한 기술과 무한 대상

> **연습문제 12.10** “모든 수학적 대상을 유한 문자열로 정의할 수 있으므로 모든 실수는 가산하게 나열된다”라는 논증을 검토하라. 실제로 유한 문자열의 수가 가산하다는 사실이 무엇을 보장하는지 설명하라.

풀이. 가산한 기호들의 유한 문자열 전체는 가산하다. 따라서 고정된 가산 언어와 고정된 의미 해석 아래에서, 매개변수 없이 각 유한 문자열이 많아야 하나의 대상을 유일하게 지정하도록 한

경우 그렇게 지정되는 대상들의 집합은 많아야 가산하다. 그러나 모든 실수가 그런 유한 정의를 갖는다는 첫 주장은 보장되지 않는다.

수학은 개별 원소를 하나씩 이름 붙이지 않고도 집합 전체를 대상으로 논할 수 있다. 특히 자연수 부분집합 전체는 대각선 논증으로 가산 목록에 담을 수 없다(제5권 제5장). 따라서 유한한 정의의 개수에 관한 계산을 모든 대상의 개수로 옮기려면 모든 대상을 그렇게 지정할 수 있다는 추가 가정이 필요한데, 그 가정이 바로 실패한다.

매개변수 주의. 임의의 실수 a를 매개변수로 허용하면 "$x = a$"는 a를 지정한다. 하지만 이 경우 기호 바깥에서 허용한 매개변수 자체가 이미 많은 대상을 공급하므로, 매개변수 없는 가산 문자열 수 논증을 그대로 사용할 수 없다. 언어의 기호 수와 허용 매개변수 범위를 함께 고정해야 한다.

12.11 혼합 문제: 지역 정보에서 전역 함수를 만들기

> **연습문제 12.11** 집합 X, Y와 관계 $R \subseteq X \times Y$가 $\forall x \in X\ \exists! y \in Y\ R(x,y)$를 만족한다고 하자. "각 x에 대해 하나씩 y를 골라야 하므로 반드시 선택공리가 필요하다"는 주장을 검토하라. 유일성이 없는 경우와 비교하라.

풀이. 유일성이 있으면 후보 사이에서 비결정적인 선택을 할 필요가 없다. 관계 R 자체가 이미 각 x를 정확히 하나의 y와 연결하므로 함수의 그래프이다. 정의역 전체에서 존재하고 단일값이라는 함수 조건을 그대로 만족한다. 통상의 ZF 집합론에서는 이처럼 유일하게 지정된 값들로 함수를 만드는 데 선택공리가 필요하지 않다.

유일성이 없으면 관계의 각 섬유에서 하나의 원소만 남기는 선택이 필요하다. 임의의 비어 있지 않은 집합족에 대해 그런 선택을 할 수 있다는 일반 주장은 선택공리이다. 다만 유한 가족이거나 각 섬유에 명시적인 최소원소 규칙이 있는 경우처럼 구체적 선택이 가능한 상황도 많다. 어떤 증명이 선택공리를 쓴다고 말하려면 실제로 어떤 가족에서 무엇을 골랐는지 밝혀야 한다.

몫집합과의 비교. 함수 $\bar{f}([x]) = f(x)$가 모든 대표에서 같은 값을 준다는 조건으로 잘 정의되는 경우도 유일한 값의 지정이다. 반면 각 동치류에서 대표원 그 자체를 하나씩 골라 모으는 일은 다른 문제이다. 몫집합이 존재한다는 사실만으로 대표계의 선택이 언제나 자동으로 따라오지는 않는다. 선택공리의 정확한 지위는 다음 권에서 공리로 다룬다(제5권 제6장).

12.12 검토 기록을 남기는 방법

실제 정오표에는 원래 주장, 실패한 조건, 반례 또는 올바른 증명, 수정된 문장을 함께 기록하면 다시 검토하기 쉽다. 예를 들어 "f를 약분했다"는 지적만 남기기보다 "왼쪽 합성 약분에는 단사성이 필요하며, 상수함수가 반례이다. 단사성을 가정하면 각 x에 적용해 결론을 얻는다"라고 적는 식이 구체적이다. 오류의 위치와 수정의 범위가 분명해진다.

검토가 끝났다는 말도 범위를 가져야 한다. 유한 예를 계산한 것, 일반 증명을 확인한 것, 알고리즘이 모든 입력에서 종료함을 증명한 것은 서로 다른 수준의 결과이다. 이 권에서 증명한 유한 해결 완전성(제4권 제10장)과 가산 명제논리 콤팩트성(제4권 제11장)은 그 이름에 적힌

범위에서만 사용한다. 일차논리의 일반 정리, 공리적 집합론의 독립성, 불완전성의 조건은 이후 권에서 따로 정리한다(제5권 제6장).

제 5 권

집합·수 체계·수학기초론

제5권은 집합론을 언어와 공리의 수준에서 세우고, 그 위에서 수 체계를 구성하며 수학기초론의 주요 결과가 말하는 범위를 정확히 밝힌 권이다. 제1장은 원소 관계와 부분집합을 정한 뒤 무제한 내포 원리가 Russell 역설로 무너지는 이유를 보이고, 제2장은 이를 피하는 ZFC의 공리를 하나씩 제시한다. 제3–4장은 자연수 집합 ω에서 정수와 유리수를 동치류로 구성하고, Dedekind 절단으로 실수체를 구성한다. 제5장은 가산성, Cantor의 대각선 논증, 기수와 서수를 다루고, 제6장은 선택공리, 독립성, 불완전성이 각각 정확히 무엇을 주장하는지를 정리한다.

제 1 장

집합을 말하는 언어와 역설의 경계

개요 이 장은 집합론의 가장 기본적인 언어, 곧 원소 관계와 부분집합 관계를 고정한다. 임의의 조건으로 집합을 만들 수 있다는 순진한 생각, 곧 무제한 내포 원리가 러셀 역설을 통해 모순에 이름을 보인 뒤, 그 모순을 피하는 분리 공리꼴과 클래스라는 보조 개념을 도입한다. 쿠라토프스키의 순서쌍 구성과 함수의 집합론적 정의로 장을 마무리하며, 새 대상을 구성할 때 확인할 세 가지 질문(재료의 존재, 구성 연산의 정당화, 대표원 선택과 무관함)을 제시한다. 선행 지식: 명제논리와 술어논리(제4권 제2장, 제4권 제4장), 함수와 동치관계(제4권 제7장, 제4권 제8장). 이 책에서 자연수에는 0을 포함한다. 이 권에서는 선택공리를 별도로 표시할 때를 제외하고 ZF 집합론을 기본 배경으로 삼는다.

1.1 원소라는 말과 부분집합이라는 말

집합을 이용한 수학의 장점은 서로 다른 대상을 한 언어로 다룰 수 있다는 데 있다. 수열은 함수이고, 함수는 순서쌍의 집합이며, 순서쌍 자체도 집합으로 표현할 수 있다. 그러나 표현할 수 있다는 사실과 어떤 조건으로도 집합을 만들 수 있다는 주장은 다르다. 이 장의 목적은 사용할 수 있는 표기와 존재가 보장되는 대상을 구별하는 것이다.

집합론의 기본 **원소 관계**(*membership relation*)는 $x \in A$이다. 이것은 "x가 A의 원소이다"라는 뜻이며, x가 A보다 작다거나 x가 A의 일부를 물리적으로 차지한다는 뜻이 아니다. **부분집합**(*subset*) 관계는 다음과 같이 정의한다.

$$A \subseteq B \iff \forall x\,(x \in A \to x \in B). \tag{1.1}$$

왼쪽은 두 집합 사이의 포함 관계이고, 오른쪽은 원소 관계만으로 쓴 정의이다. $A \subsetneq B$는 $A \subseteq B$와 $A \neq B$를 함께 뜻한다. 같은 원소를 가지는 두 집합은 같은 집합이라는 원리를 **외연성**(*extensionality*)이라고 한다.

> **예제 1.1** $A = \{\emptyset, \{\emptyset\}\}$라고 하자. $\emptyset \in A$, $\emptyset \subseteq A$, $\{\emptyset\} \in A$, $\{\emptyset\} \subseteq A$는 모두 참이다. 하지만 이 네 문장은 서로 다른 이유로 참이다. 특히 $\emptyset \subseteq A$는 공집합의 원소가 하나도 없어서 포함 조건을 위반할 수 없기 때문에 참이다. $\emptyset \in A$는 실제로 A의 원소 목록에 공집합이 들어 있기 때문에 참이다.

명제 1.2 모든 집합 A에 대해 $\emptyset \subseteq A$이다. 또한 $A \subseteq \emptyset$이면 $A = \emptyset$이다.

증명. 첫 문장의 부정은 어떤 x가 $\emptyset$의 원소이면서 A의 원소가 아니라는 것이다. 공집합에는 원소가 없으므로 불가능하다. 두 번째 문장에서 $x \in A$라면 포함 관계에 의해 $x \in \emptyset$이어야 한다. 따라서 A도 원소가 없으며 외연성으로 공집합과 같다. □

집합의 중복 표기나 나열 순서는 원소를 바꾸지 않는다. 따라서 $\{a, a, b\} = \{b, a\}$이다. 반면 순서를 기억하는 자료가 필요하면 집합 자체가 아닌 별도의 부호화를 써야 한다. 뒤에서 도입할

순서쌍 (a, b)가 그 예이다. 이 구별은 확률의 표본공간, 함수의 그래프, 대수 구조의 정의에서 계속 사용된다.

1.2 조건을 적는 것과 집합이 존재하는 것

조건 $\varphi(x)$를 만족하는 대상을 모은다는 표기

$$\{x : \varphi(x)\}$$

는 편리하다. 그러나 이 표기만으로 하나의 집합이 존재한다고 결론 내릴 수는 없다. 이를 아무 제한 없이 허용하는 원리를 **무제한 내포 원리**(*unrestricted comprehension*)라고 부르면, 그 원리는 다음 형태이다.

$$\exists B \, \forall x \, \big(x \in B \iff \varphi(x) \big).$$

여기서 모든 조건 φ에 이 원리를 적용하는 것은 모순을 일으킨다.

> **정리 1.3 (러셀 역설)** 모든 집합 x에 대하여 $x \in R$과 $x \notin x$가 동치인 집합 R은 존재하지 않는다.

증명. 그러한 R이 있다고 가정하고 정의의 x 자리에 R을 넣으면

$$R \in R \iff R \notin R$$

을 얻는다. $R \in R$이면 오른쪽에 의해 $R \notin R$이고, $R \notin R$이면 오른쪽에서 왼쪽으로의 함의에 의해 $R \in R$이다. 두 경우 모두 모순이다. $\square$

이 논증은 매우 특정한 금지 사항을 보여 준다. “자기 자신을 원소로 갖지 않는 모든 집합”이라는 조건이 문법적으로 작성 가능하더라도, 그 조건의 모든 해를 하나의 집합으로 모으는 것은 허용되지 않는다. 논리의 잘못을 보여 주는 증명이 아니라, 존재 원리를 너무 강하게 잡았을 때 생기는 문제를 보여 주는 증명이다.

1.3 분리: 이미 있는 집합 안에서 고르기

ZF의 **분리 공리꼴**(*axiom schema of separation*)은 이미 주어진 집합 A에 대해

$$\{x \in A : \varphi(x)\}$$

가 존재함을 보장한다. 무제한 내포와 달리 후보 전체가 A 안으로 제한되어 있다. 이 제한은 장식이 아니라 모순을 피하는 핵심이다.

> **명제 1.4** 주어진 집합 A에 대해
>
> $$R_A = \{x \in A : x \notin x\}$$
>
> 를 만들 수 있다. 이 집합은 A의 부분집합이지만 A의 원소는 아니다.

증명. 분리에 의해 R_A가 존재하며 정의상 $R_A \subseteq A$이다. 만일 $R_A \in A$라면 분리식에 $x = R_A$를 넣어

$$R_A \in R_A \iff (R_A \in A \text{ 그리고 } R_A \notin R_A) \iff R_A \notin R_A$$

를 얻으므로 모순이다. 따라서 $R_A \notin A$이다. □

따름정리 1.5 모든 집합을 원소로 갖는 보편 집합은 존재하지 않는다.

증명. U가 모든 집합을 원소로 갖는다면 R_U도 집합이므로 $R_U \in U$이다. 바로 앞 명제는 $R_U \notin U$를 주므로 모순이다. □

흔한 오류. $R_A \subseteq A$로부터 $R_A \in A$를 결론 내리면 안 된다. 러셀 역설을 제한된 분리식에 그대로 적용할 때 흔히 이 두 기호가 혼동된다.

집합의 여집합도 기준 집합을 정해서 사용한다. $A \subseteq U$일 때 $U \setminus A$는 존재하지만, "모든 집합 가운데 A에 속하지 않는 것들"을 하나의 집합으로 만들 수는 없다. 확률에서는 표본공간, 위상에서는 연구 중인 공간, 논리에서는 논의 영역이 이 기준 집합의 역할을 한다.

1.4 클래스는 집합의 다른 이름이 아니다

집합론의 문장 $\varphi(x)$로 대상을 기술할 때 그 대상을 통틀어 **클래스**(*class*)라고 부를 수 있다. 이 권에서 클래스라는 표현은 우선 설명을 위한 약칭이다. ZF의 변수는 집합을 가리키며, 모든 클래스를 별도의 대상으로 양화하는 것은 아니다.

정의 1.6 어떤 조건을 만족하는 집합들의 모임이 하나의 집합으로 나타낼 수 없을 때 그것을 **진클래스**(*proper class*)라고 부른다. 모든 집합의 클래스 V가 대표적인 예이다.

"$x \in V$"는 이 문맥에서 "x가 집합이다"라는 설명을 줄인 말로 읽는다. V 자체가 ZF의 집합 변수에 들어갈 수 있다는 주장은 아니다. 진클래스의 집합을 만들거나 진클래스를 함수의 통상적인 정의역으로 넣으려면 클래스 이론 또는 별도의 약속이 필요하다. 클래스 크기의 함수를 말할 때도 실제로는 모든 집합 입력에 하나의 집합 출력을 지정하는 정의 가능한 관계를 뜻하는 경우가 많다.

예제 1.7 "모든 군의 모임"은 통상 하나의 집합으로 취급하지 않는다. 반면 주어진 집합 X 위에서 정의되는 모든 이항 연산의 모임은 함수 집합 $X^{X \times X}$ 안에 들어가므로 집합으로 다룰 수 있다. 대상의 크기를 먼저 제한하면 많은 모임을 안전하게 집합으로 만들 수 있다.

공리적 집합론은 매번 모든 대상을 원시적인 집합 표기로 전개하라는 요구가 아니다. 필요한 모임이 집합으로 형성될 수 있는 이유를 확보한 다음, 실제 계산에서는 익숙한 수와 함수 표기를 쓰는 것이 보통이다. 중요한 것은 축약을 풀었을 때 어떤 공리와 어떤 논리 규칙이 사용되는지 추적할 수 있다는 점이다.

1.5 순서쌍과 구조의 부호화

순서쌍(*ordered pair*)에는 다음 한 가지 성질이 필요하다.

$$(a, b) = (c, d) \iff a = c \text{ 그리고 } b = d.$$

이 성질을 만족하는 집합 부호화로 Kuratowski의 정의를 사용할 수 있다.

$$(a, b) := \{\{a\}, \{a, b\}\}.$$

순서쌍이 어떤 물리적 모양을 가져야 한다는 뜻이 아니다. 수학에 필요한 구별을 보존하면 목적에 충분하다.

명제 1.8 위의 정의는 순서쌍의 필요한 성질을 만족한다.

증명. $P = (a, b)$에 대해 $\bigcap P = \{a\}$이고 $\bigcup P = \{a, b\}$이다. 따라서 P가 주어지면 첫 성분 a가 결정된다. 합집합이 $\{a\}$이면 두 번째 성분도 a이다. 합집합에 a 이외의 원소가 있으면 그 유일한 원소가 b이다. 그러므로 두 순서쌍이 같으면 두 성분이 각각 같다. 반대 방향은 정의에 같은 성분을 대입하면 바로 얻는다. □

관계는 곱집합의 부분집합으로, 함수는 각 입력에 정확히 하나의 출력을 대응시키는 관계로 정의한다. 정의역과 공역을 함께 지정한 함수 $f : X \to Y$를 다룰 때 그래프만으로는 공역이 복원되지 않을 수 있으므로 X, Y도 자료에 포함한다고 약속한다. 예를 들어 같은 그래프 $\{(0, 0)\}$가 $\{0\} \to \{0\}$에서는 전사 함수이고 $\{0\} \to \{0, 1\}$에서는 전사 함수가 아니다.

1.6 구성과 증명에서 확인할 세 가지

새 대상을 도입할 때는 다음 세 질문을 순서대로 확인하면 좋다.

(1) 재료가 되는 대상은 이미 집합인가.

(2) 그 재료를 모으는 연산은 어떤 공리로 정당화되는가.

(3) 같은 대상을 다른 대표자로 나타낼 때 연산이나 관계가 달라지지 않는가.

첫 두 질문은 존재 문제이고 마지막 질문은 잘 정의됨의 문제이다.

이후의 정수와 유리수 구성은 이 세 질문이 동시에 등장하는 사례이다(제5권 제3장). 정수 -3을 단순히 새로운 기호로 선언하는 대신 자연수 쌍의 동치류로 만들 수 있다. 그때 쌍 전체가 집합인 이유, 동치류 전체가 집합인 이유, 덧셈이 대표자 선택에 의존하지 않는 이유가 각각 필요하다. 이런 기초 작업을 마치면 일상적인 대수 계산은 그 위에서 진행된다.

1.7 연습문제와 해설

연습문제 1.9 $A = \{\emptyset\}$일 때 A의 원소 수와 $\mathcal{P}(A)$의 원소 수를 구하고, 두 집합을 나열하라.

풀이. A에는 원소 $\emptyset$ 하나가 있다. 부분집합은 $\emptyset$과 $\{\emptyset\}$ 두 개이므로 $\mathcal{P}(A) = \{\emptyset, \{\emptyset\}\}$이다. 원소가 없는 집합과 그 집합을 원소로 갖는 집합을 구별해야 한다.

연습문제 1.10 "$A \in B$이고 $B \in C$이면 $A \in C$이다"가 일반적으로 거짓임을 보이라.

풀이. $A = \emptyset$, $B = \{\emptyset\}$, $C = \{\{\emptyset\}\}$로 놓는다. $A \in B$와 $B \in C$는 참이다. 하지만 C의 유일한 원소는 $B \neq A$이므로 $A \notin C$이다. 원소 관계는 일반적으로 추이적이지 않다.

연습문제 1.11 $A \subseteq B$와 $B \subseteq A$에서 $A = B$가 나오는 이유를 원소의 양방향 포함으로 설명하라.

풀이. 임의의 x에 대해 두 포함 관계는 $x \in A \Rightarrow x \in B$와 $x \in B \Rightarrow x \in A$를 준다. 따라서 두 집합은 정확히 같은 원소를 가지며 외연성으로 같다. 여기에는 원소를 유한하게 나열할 수 있다는 가정이 없다.

연습문제 1.12 $R_A \subseteq A$이지만 $R_A \notin A$라는 결과가 모순이 아닌 이유를 설명하라.

풀이. 부분집합의 모든 원소가 A에 들어 있다는 말과 부분집합 자체가 A의 원소라는 말은 다르다. 예컨대 $A = \emptyset$이면 $R_A = \emptyset$이고 $\emptyset \subseteq \emptyset$이지만 $\emptyset \notin \emptyset$이다.

연습문제 1.13 순서쌍을 $\{a, b\}$로 정의할 수 없는 이유와, Kuratowski 정의에서 $a = b$인 경우를 설명하라.

풀이. $a \neq b$여도 $\{a, b\} = \{b, a\}$이므로 순서 정보가 사라진다. Kuratowski 정의는 $a = b$일 때 $(a, a) = \{\{a\}\}$가 된다. 바깥 집합의 원소 수가 한 개로 줄어들어도 첫 성분과 두 번째 성분이 모두 a라는 정보가 복원되므로 문제가 없다.

연습문제 1.14 “이 조건으로 정의했으므로 그 집합이 존재한다”라는 논증을 고쳐 써라.

풀이. 우선 조건을 만족할 후보를 포함하는 기존 집합 U를 찾아야 한다. 그다음 $\{x \in U : \varphi(x)\}$를 분리 공리꼴로 구성한다. 적절한 U가 확보되지 않았다면 이 논증만으로 존재를 결론 내릴 수 없다. 다른 존재 공리를 쓰는 구성이 가능한지 검토해야 한다.

제 2 장

ZFC 공리: 존재를 허용하는 정확한 규칙

개요 이 장은 ZFC의 공리를 하나씩 제시하여, 제1장에서 금지한 무제한 내포 대신 어떤 정확한 규칙으로 집합의 존재가 보장되는지를 밝힌다(제5권 제1장). 외연성·공집합·짝·합집합·멱집합·분리 공리꼴·무한·치환 공리꼴·정칙성·선택의 열 가지 원리를 차례로 진술하고, 각 공리가 실제로 어떤 구성(곱집합, 교집합, 자연수 집합, 몫집합 등)을 정당화하는지 예제로 보인다. 선행 지식: 집합, 포함 관계, 분리와 무제한 내포의 차이(제5권 제1장). 공리의 변수는 모두 집합을 나타낸다. $\forall x \in A$와 $\exists x \in A$는 **제한된 양화사**(*bounded quantifier*)의 약칭이다.

2.1 공리와 공리꼴의 차이

ZFC는 일차논리의 언어에서 집합의 원소 관계를 다루는 이론이다. 논리적 등호를 제외한 기본 비논리 기호는 $\in$ 하나로 잡을 수 있다. $\emptyset, \subseteq, \mathcal{P}, \cup$ 등의 표기는 존재와 유일성을 확인한 뒤 추가하는 약칭이다.

분리와 치환은 각각 한 문장이 아니라 무한히 많은 문장을 생성하는 **공리꼴**(*axiom schema*)이다. 일차논리 공식 φ를 하나 정할 때마다 하나의 공리가 생긴다. 여기서 공식은 유한한 문자열이며, 임의의 외부적 성질이나 진리 술어를 자유롭게 넣을 수 있다는 뜻이 아니다. 집합 매개변수는 허용되지만 변수 포획을 피해야 한다.

아래에서는 읽기 쉬운 표준적 형태를 사용한다. 공집합 공리를 다른 공리에서 유도하는 등 공리 목록을 조금 다르게 제시하는 문헌도 있다. 그 차이는 같은 이론을 다른 방식으로 공리화하는 차이일 수 있으므로, 공리의 개수만으로 이론의 강도를 비교하면 안 된다.

2.2 외연성, 공집합, 짝, 합집합

외연성 공리는 집합의 동일성을 결정한다.

$$\forall A\, \forall B\, \big[\forall x\, (x \in A \leftrightarrow x \in B) \rightarrow A = B\big]. \tag{2.1}$$

공집합(*empty set*) 공리는 원소가 없는 집합을 준다.

$$\exists E\, \forall x\, (x \notin E).$$

외연성에 의해 그런 집합은 유일하므로 $\emptyset$라고 쓴다.

짝 공리는 주어진 두 집합을 원소로 갖는 집합을 준다.

$$\forall a\, \forall b\, \exists C\, \forall x\, \big(x \in C \leftrightarrow (x = a \vee x = b)\big).$$

$a = b$를 허용하므로 한원소집합 $\{a\}$도 존재한다. 짝 공리와 합집합 공리를 반복하면 임의의 고정된 유한 목록을 집합으로 모을 수 있다. 그러나 "각 유한 목록을 만들 수 있다"는 말만으로 모든 자연수를 동시에 담는 무한 집합의 존재가 나오지는 않는다.

합집합 공리는 집합족 A의 원소들의 원소를 한 단계 모은다.

$$\forall A\, \exists U\, \forall x\, \big(x \in U \leftrightarrow \exists y\, (y \in A \wedge x \in y)\big).$$

이 U를 $\bigcup A$라고 쓴다. 두 집합의 합집합은 $A \cup B = \bigcup\{A, B\}$로 정의한다. $\bigcup \emptyset = \emptyset$이며, 합집합을 취한다고 기존 집합 자체가 자동으로 원소가 되는 것은 아니다.

> **예제 2.1** $A = \{\{1,2\},\{2,3\}\}$이면 $\bigcup A = \{1,2,3\}$이다. A의 원소는 집합 $\{1,2\}$와 $\{2,3\}$이고, $\bigcup A$의 원소는 수 $1, 2, 3$이다. 이 예에서 숫자는 이미 구성된 집합 부호화의 약칭으로 이해한다.

2.3 멱집합과 분리 공리꼴

멱집합 공리는 한 집합의 모든 부분집합을 한 집합으로 모은다.

$$\forall A\, \exists P\, \forall x\, \big[x \in P \leftrightarrow \forall y\, (y \in x \to y \in A)\big].$$

이 P를 $\mathcal{P}(A)$라고 한다. 여기서 "모든"은 해당 집합론의 우주 안에 존재하는 모든 부분집합을 뜻한다. 모형론에서 어떤 모형의 내부 멱집합과 외부에서 보는 부분집합 전체를 구별해야 하는 문제는 별도로 다룬다.

공식 $\varphi(x, p_1, \dots, p_k)$를 고정하면 분리 공리꼴의 한 사례는

$$\forall A\, \forall p_1 \cdots \forall p_k\, \exists B\, \forall x\, \big[x \in B \leftrightarrow (x \in A \wedge \varphi(x, p_1, \dots, p_k))\big]$$

이다. 새 집합 변수 B가 φ에 자유롭게 등장하지 않도록 이름을 고른다. A는 분리할 범위를 주고, φ는 그 범위 안에서의 판정 조건을 준다. 공식 안에 A 자체를 매개변수로 넣는 것도 가능하다.

> **예제 2.2 (곱집합의 존재)** Kuratowski 순서쌍 (x, y)는 $x \in X$, $y \in Y$이면
>
> $$(x, y) \in \mathcal{P}\big(\mathcal{P}(X \cup Y)\big)$$
>
> 를 만족한다. 따라서 이 멱집합에서 $x \in X$, $y \in Y$인 순서쌍만 분리하면 $X \times Y$가 얻어진다. 곱집합을 만들기 위해 선택공리를 쓸 필요가 없다. 이후 $X \to Y$인 함수 그래프 전체의 모임은 $\mathcal{P}(X \times Y)$의 부분집합이므로, 함수 집합 역시 분리로 얻어진다.

> **예제 2.3 (교집합과 공집합족)** $\mathcal{A} \neq \emptyset$인 집합족에서 $A_0 \in \mathcal{A}$ 하나를 고르면
>
> $$\bigcap \mathcal{A} = \{x \in A_0 : \forall A \in \mathcal{A}\, (x \in A)\}$$
>
> 로 교집합을 구성할 수 있다. 하나의 존재하는 원소를 증명 안에서 고르는 일은 무한히 많은 선택을 동시에 요구하는 선택공리와 다르다. $\mathcal{A} = \emptyset$에는 이 정의를 그대로 쓸 수 없다. 기준 집합 U가 지정된 상대적 교집합이라면 $\bigcap \emptyset = U$라고 약속할 수 있으나, 기준 없이 모든 집합의 공통 원소를 모으는 것은 보편 집합을 요구한다.

2.4 무한 공리와 최소의 귀납적 집합

후속자(*successor*) 연산을 $S(x) = x \cup \{x\}$로 쓰자. 무한 공리는 다음과 같다.

$$\exists I\, \big[\emptyset \in I \wedge \forall x\, (x \in I \to S(x) \in I)\big].$$

$\emptyset$를 포함하고 후속자에 대해 닫힌 집합을 **귀납적 집합**(*inductive set*)이라고 부른다. 공리는 어떤 귀납적 집합이 존재함을 말할 뿐, 그 집합이 필요한 원소만 포함한다고 말하지는 않는다. 다음 장에서는 분리를 이용하여 모든 귀납적 집합에 공통으로 들어가는 최소 부분을 추출한다. 이것이 자연수 집합 ω이다(제5권 제3장).

무한 공리는 “아무리 큰 유한 수를 주어도 그보다 큰 수를 쓸 수 있다”라는 비형식적 말보다 강한 집합 존재 주장이다. 어떤 대상을 하나씩 유한 번 만드는 과정과, 그 모든 단계를 하나의 집합 안에서 동시에 다루는 일은 구별된다.

2.5 치환 공리꼴: 함수적 대응의 상을 모으기

공식 $\varphi(x, y, \mathbf{p})$가 집합 A의 각 원소에 정확히 하나의 집합 y를 대응시킨다고 하자. **치환**(*replacement*)은 그 출력 전체가 집합임을 보장한다. 정확한 한 형태는

$$\forall A\, \forall \mathbf{p}\, \Big[\forall x \in A\, \exists! y\, \varphi(x, y, \mathbf{p}) \\ \rightarrow \exists B\, \forall y\, \big(y \in B \leftrightarrow \exists x \in A\, \varphi(x, y, \mathbf{p}) \big) \Big]. \tag{2.2}$$

벡터 기호 $\mathbf{p}$는 유한한 매개변수 목록의 약칭이다. 여기서도 B는 φ에 자유롭게 나타나지 않도록 한다.

분리는 이미 주어진 집합 안에서 원소를 골라낸다. 치환은 주어진 집합의 각 원소를 따라 새 출력을 모으며, 출력이 미리 제시된 하나의 집합 안에 있다는 가정을 요구하지 않는다. 다만 입력마다 정확히 하나의 출력이 있다는 점이 중요하다. 출력 후보가 여러 개일 때 하나씩 선택하여 모으는 원리와는 다르다.

> **예제 2.4** 이미 그래프가 집합인 함수 $f : A \to B$의 상 $f(A)$는 B에서 분리하여 만들 수 있다. 치환의 추가 역할은 그래프나 공역의 집합 존재를 아직 확보하지 않은 정의 가능한 대응에도 적용된다는 것이다. 예컨대 각 자연수 n에 대해 X에서 멱집합 연산을 n번 반복한 집합 $\mathcal{P}^n(X)$를 유일하게 지정했다면, 치환은 $\{\mathcal{P}^n(X) : n \in \omega\}$를 한 집합으로 모을 수 있게 한다. 이 예는 역할을 설명하며, 치환이 다른 공리에서 독립이라는 사실의 증명은 아니다.

> **명제 2.5** 치환은 이미 집합인 정의역에서 유일하게 정해진 출력을 모으는 데 선택공리를 요구하지 않는다.

증명. 각 $x \in A$에 유일한 y가 존재한다면 공식 자체가 어떤 y를 써야 하는지 결정한다. 치환으로 모든 순서쌍 (x, y)의 모임을 만들면 함수의 그래프가 된다. 서로 다른 후보 중 하나를 추가로 정하는 단계가 없으므로 선택공리의 가정을 사용하지 않는다. □

2.6 정칙성과 선택: 서로 다른 역할

정칙성 공리, 또는 기초 공리는

$$\forall A\, \big[A \neq \emptyset \rightarrow \exists a \in A\, (a \cap A = \emptyset) \big]$$

이다. 모든 공집합 아닌 집합 안에서, 그 집합의 다른 원소를 자기 원소로 포함하지 않는 원소 하나를 찾을 수 있다는 뜻이다.

명제 2.6 정칙성 아래에서는 $x \in x$인 집합이 없다. 더 일반적으로 유한한 원소 관계의 순환도 없다.

증명. $x \in x$라면 $A = \{x\}$의 유일한 원소 x에 대해 $x \cap A$가 x를 포함하므로 정칙성에 어긋난다. 유한 순환 $x_0 \in x_1 \in \cdots \in x_{n-1} \in x_0$이 있다면 $A = \{x_0, \dots, x_{n-1}\}$의 각 원소는 순환의 바로 앞 원소를 자기 원소로 포함한다. 따라서 어느 $a \in A$도 $a \cap A = \emptyset$를 만족하지 못한다. □

정칙성은 집합의 포함 사슬을 모두 금지하지 않는다. $\emptyset \subsetneq \{\emptyset\} \subsetneq \{\emptyset, \{\emptyset\}\} \subsetneq \cdots$ 같은 증가 사슬은 자연수 구성의 일부이다. 원소 관계와 포함 관계, 감소와 증가를 각각 구별해야 한다.

선택공리의 한 형태는 다음과 같다.

$$\forall \mathcal{A} \left[\emptyset \notin \mathcal{A} \to \exists f \left(\mathrm{dom}(f) = \mathcal{A} \wedge \forall A \in \mathcal{A} \, (f(A) \in A) \right) \right].$$

여기서 f는 함수라는 조건이 포함된 약칭으로 읽는다. ZF에 이 공리를 추가한 이론이 ZFC이다. 정칙성은 원소 관계의 모양을 제한하고, 선택은 집합족 전체에서 동시 선택 함수의 존재를 보장한다. 두 공리는 이름이 비슷한 일상적 단어를 사용하더라도 역할이 전혀 다르다.

2.7 공리를 사용하는 짧은 구성 지도

보통의 수학에서는 한 대상에 공리가 하나만 쓰이지 않는다. 예를 들어 몫집합 $X/\!\sim$을 만들 때 각 동치류는 X에서 분리하고, 동치류 전체는 $\mathcal{P}(X)$에서 다시 분리할 수 있다(제4권 제7장). 대표자를 골라야만 몫집합이 존재하는 것은 아니다. 반대로 모든 동치류에서 대표자 하나를 골라 하나의 횡단집합을 만드는 문제에는 추가 선택이 필요할 수 있다.

자연수에는 무한과 분리가 중요하고, 순서쌍과 유한 자료에는 짝과 합집합이 중요하며, 함수 공간에는 멱집합과 분리가 중요하다. 더 긴 초한 재귀와 누적 계층에서는 치환의 역할이 드러난다. 이것은 각 공리의 사용 위치를 추적하는 지도이지, 나머지 공리가 어떤 경우에도 필요하지 않다는 독립성 주장으로 읽어서는 안 된다.

2.8 연습문제와 해설

연습문제 2.7 멱집합과 분리를 이용하여 X 위의 모든 동치관계의 모임이 집합임을 설명하라.

풀이. 모든 관계는 $\mathcal{P}(X \times X)$의 원소이다. 그중 반사성, 대칭성, 추이성을 만족하는 관계만 일차논리 공식으로 분리하면 된다. 관계가 매우 많다는 것은 집합의 존재를 막지 않는다. 먼저 그것들을 담을 집합을 확보했기 때문이다.

연습문제 2.8 $\mathcal{P}(\emptyset)$, $\bigcup\{A\}$, $\bigcup\{\emptyset, A\}$를 구하라.

풀이. 각각 $\{\emptyset\}$, A, A이다. 마지막 두 식은 합집합의 원소가 원래 집합족 원소들의 원소라는 정의에서 나온다. $\mathcal{P}(\emptyset)$는 공집합 자체를 한 원소로 포함하므로 공집합이 아니다.

연습문제 2.9 "모든 $x \in A$에 어떤 y가 존재한다"에서 곧바로 치환으로 선택 함수를 얻을 수 없는 이유를 설명하라.

풀이. 치환 공리꼴은 출력의 유일성을 요구한다. 후보가 여러 개이면 먼저 어느 출력을 대응시킬 것인지 정하는 함수적 공식을 확보해야 한다. 모든 후보에 최소 원소를 주는 순서가 이미 있으면

해결할 수 있지만, 그런 구조 없이 임의의 공집합 아닌 집합족을 다룰 때는 선택공리의 문제가 된다.

연습문제 2.10 정칙성이 ω의 존재와 충돌하지 않는 이유를 설명하라.

풀이. 폰 노이만 자연수 구성에서 $0 = \emptyset$이고 $0 \in \omega$이다. 따라서 $0 \cap \omega = \emptyset$여서 ω 자체는 정칙성의 요구를 만족한다. 정칙성은 모든 집합이 유한해야 한다고 말하지 않는다.

연습문제 2.11 $X/\sim$의 존재와 각 동치류에서 대표자 하나씩 고르는 일의 차이를 설명하라.

풀이. 몫집합은 $\mathcal{P}(X)$에서 동치류인 부분집합들을 분리하여 얻는다. 이 과정에서 대표자를 동시에 지정하지 않는다. 대표자 함수 $s : X/\sim \to X$를 요구하면 각 C에 대해 $s(C) \in C$여야 하므로 집합족에 대한 선택 문제이다. 특별한 순서나 명시적 규칙이 있으면 ZF에서도 가능하지만, 일반적인 존재 주장은 선택 원리와 관련된다.

연습문제 2.12 분리 공리꼴에 매개변수를 허용하는 것이 왜 유용한지 교집합을 예로 설명하라.

풀이. $A \cap B = \{x \in A : x \in B\}$를 만들 때 판정 공식은 매개변수 B를 사용한다. 모든 매개변수에 대해 공리 문장을 보편 양화하므로 특정 B를 새 상수 기호로 추가할 필요가 없다. 매개변수 허용은 임의의 외부 성질을 허용한다는 뜻이 아니다.

제 3 장

자연수에서 정수와 유리수까지

개요 이 장은 ZF 공리 위에서 자연수 집합 ω를 구성하고, 이로부터 정수 $\mathbb{Z}$와 유리수 $\mathbb{Q}$를 동치류의 몫집합으로 차례로 구성한다. 자연수의 뺄셈이 모든 쌍에서 가능하지 않다는 결함을 자연수 쌍의 동치류(차이의 기록)로 고치면 정수를 얻고, 정수의 나눗셈이 모든 쌍에서 가능하지 않다는 결함을 같은 방식으로 고치면 유리수를 얻는다. 각 단계에서 연산과 순서가 동치류 대표자의 선택과 무관하게 잘 정의됨을 확인하고, 자연수가 정수 속에, 정수가 유리수 속에 연산과 순서를 보존한 채 매장됨을 보인다. 장은 유리수의 조밀성을 증명하고 완비성의 결여를 지적하는 것으로 끝나며, 이 결여는 다음 장의 실수 구성으로 이어진다. 선행 지식: 귀납법과 재귀적 정의(제4권 제6장), 동치관계와 몫집합(제4권 제7장), ZF 공리의 역할(제5권 제2장). 이 장의 구성에는 선택공리가 필요하지 않다.

3.1 자연수를 집합으로 나타내기

폰 노이만(*von Neumann*) 방식에서는 각 자연수를 그보다 작은 모든 자연수의 집합으로 나타낸다. 처음 몇 항은

$$0 = \varnothing,$$
$$1 = \{0\} = \{\varnothing\},$$
$$2 = \{0, 1\},$$
$$3 = \{0, 1, 2\}$$

이고, **후속자**(*successor*)는

$$S(n) = n \cup \{n\} \tag{3.1}$$

이다. 이 부호화에서 $m < n$은 $m \in n$에 대응한다. 자연수의 산술적 성질을 만들기 위해 집합의 우연한 그림을 이용하는 것은 아니며, 필요한 순서와 후속자 관계가 이 표현에 정확히 반영된다.

역사 (자연수의 두 집합론적 부호화). 폰 노이만의 부호화(1923)는 n을 그보다 작은 자연수 전체의 집합 $\{0, \dots, n-1\}$로 나타내어 $m < n \iff m \in n$을 얻고, 원소의 개수가 그대로 n이 되는 장점이 있다. 이보다 앞선 체르멜로(*Zermelo*)의 부호화는 $0 = \varnothing$, $S(n) = \{n\}$으로 두어 $1 = \{\varnothing\}$, $2 = \{\{\varnothing\}\}$, …를 얻는다. 두 부호화 모두 귀납법과 후속자 연산의 공리적 성질을 만족시키므로 집합론적으로 동등하게 쓸 수 있지만, 폰 노이만 부호화는 순서를 원소 관계로, 크기를 원소 개수로 동시에 표현한다는 점에서 이후 서수와 기수의 이론(제5권 제5장)과 바로 연결된다.

무한 공리로 귀납적 집합 I 하나를 확보하고, I의 귀납적 부분집합 전체를

$$\mathcal{I} = \{J \in \mathcal{P}(I) : 0 \in J \wedge \forall x \in J\ S(x) \in J\}$$

로 둔다. $I \in \mathcal{I}$ 이므로 이 집합족은 공집합이 아니다. 따라서

$$\omega = \bigcap \mathcal{I}$$

가 존재한다. 이것이 자연수 집합이다.

정리 3.1 (최소 귀납적 집합) ω는 귀납적이며 모든 귀납적 집합 K에 포함된다. 따라서 처음에 고른 I에 의존하지 않는다.

증명. 각 $J \in \mathcal{I}$가 0을 포함하므로 $0 \in \omega$이다. $n \in \omega$이면 모든 $J \in \mathcal{I}$가 n을 포함하고 후속자에 닫혀 있으므로 $S(n) \in \omega$이다. 이제 임의의 귀납적 집합 K를 잡으면 $I \cap K$도 귀납적이고 I의 부분집합이다. 따라서 $\omega \subseteq I \cap K \subseteq K$이다. 서로 다른 출발 집합에서 구성한 두 최소 귀납적 집합은 서로 포함하므로 같다. $\square$

정리 3.2 (자연수 귀납 원리) $A \subseteq \omega$가 $0 \in A$와 $n \in A \Rightarrow S(n) \in A$를 만족하면 $A = \omega$이다.

증명. 가정에 의해 A가 귀납적이므로 최소성에서 $\omega \subseteq A$이다. 처음에 $A \subseteq \omega$였으므로 두 집합이 같다. $\square$

공식 $P(n)$에 대해 분리로 $A = \{n \in \omega : P(n)\}$를 만들면 정리 3.2이 익숙한 수학적 귀납법을 준다. 집합론 안에서 얻은 이 원리와 일차 산술의 귀납 공리꼴은 서로 연결되어 있지만, 일차 산술의 모든 모형이 표준 자연수와 동형이라는 결론은 나오지 않는다. 비표준 모형에 관한 문제를 건너뛰어 범위를 넓히면 안 된다.

3.2 후속자, 순서, 재귀적 연산

이 구성에서 0은 어떤 자연수의 후속자도 아니고, 서로 다른 자연수는 서로 다른 후속자를 갖는다. 자연수는 원소 관계로 정렬되며, 각 n은 정확히 $0, \dots, n-1$을 원소로 갖는다. 이런 기본 성질은 귀납법으로 확인할 수 있다. 특히 $n \in n$은 성립하지 않고 $S(n)$의 가장 큰 원소는 n이다.

참고 (자연수 재귀 정리). 집합 X, 원소 $a_0 \in X$, 함수 $g : X \to X$가 주어지면

$$f(0) = a_0, \qquad f(S(n)) = g(f(n))$$

를 만족하는 함수 $f : \omega \to X$가 유일하게 존재한다(제4권 제6장). 시작값과 다음 값을 만드는 규칙만으로 자연수 전체 위의 함수가 완전히 정해진다는 것이 이 정리의 내용이며, 아래의 덧셈과 곱셈은 이 정리를 n번째 좌표에 적용하여 얻는다.

고정된 a에 대해 덧셈과 곱셈을 다음과 같이 정의한다.

$$a + 0 = a, \qquad a + S(b) = S(a + b), \qquad\qquad a \cdot 0 = 0, \qquad a \cdot S(b) = a \cdot b + a. \tag{3.2}$$

여기에서 덧셈의 교환법칙은 정의에 포함되어 있지 않다. 정의를 토대로 증명해야 한다. 예를 들어 $0 + a = a$를 먼저 귀납법으로 보이고, $S(a) + b = S(a + b)$를 보인 다음 $a + b = b + a$를 b에 대한 귀납법으로 얻는다. 결합법칙과 분배법칙도 같은 방식으로 정당화한다.

명제 3.3 (덧셈의 소거) 자연수 a, b, c에 대해 $a + c = b + c$이면 $a = b$이다.

증명. c에 대해 귀납한다. $c = 0$이면 가정 자체가 $a = b$이다. $c = S(d)$일 때 가정은 $S(a+d) = S(b+d)$이다. 후속자의 단사성으로 $a+d = b+d$이고, 귀납 가정으로 $a = b$이다. □

정의 3.4 자연수에서 $a \le b$는 어떤 $k \in \omega$에 대해 $b = a + k$라는 뜻으로도 정의할 수 있다. 이 관계는 폰 노이만 표현에서의 포함 관계 $a \subseteq b$와 일치한다.

자연수의 뺄셈은 모든 쌍에서 가능하지 않다. $a \le b$일 때만 $a + k = b$인 자연수 k가 존재하며, 소거법칙(명제 3.3)으로 이 k가 유일하다. 정수의 구성은 이 제한을 풀기 위해 "차이"를 새로운 대상으로 도입하는 과정이다.

3.3 정수는 자연수 쌍의 차이를 기록한다

자연수 쌍 (a, b)를 형식적인 차이 $a - b$로 생각하자. 아직 음수를 구성하지 않았으므로 다음 정의에는 뺄셈을 사용하지 않는다.

$$(a, b) \sim (c, d) \iff a + d = b + c. \tag{3.3}$$

이 관계는 동치관계이다. 반사성과 대칭성은 덧셈의 성질에서 바로 나온다. 추이성은 소거법칙을 사용한다.

추이성의 증명. $a + d = b + c$와 $c + f = d + e$라고 하자. 두 등식을 더하고 항을 재배열하면

$$a + d + c + f = b + c + d + e$$

이다. 양변에서 $c + d$를 소거하여 $a + f = b + e$를 얻는다. 따라서 $(a, b) \sim (e, f)$이다. □

정의 3.5 **정수** 집합을 $\mathbb{Z} = (\omega \times \omega)/\!\sim$로 정의한다. 쌍 (a, b)의 **동치류**를 $[a, b]$라고 쓴다. 다음 연산을 도입한다.

$$[a,b] + [c,d] = [a+c,\ b+d], \qquad -[a,b] = [b,a], \qquad [a,b]\,[c,d] = [ac+bd,\ ad+bc]. \tag{3.4}$$

영원소(*zero element*)는 $[0, 0]$이고 **단위원**(*unit element*)은 $[1, 0]$이다.

이 정의가 정수 위의 연산이 되려면 대표자를 바꾸어도 결과의 동치류가 같아야 한다. 예컨대 $[5, 2] = [4, 1]$인데 이 두 표기 때문에 곱셈 결과가 달라지면 정의에 실패한 것이다.

명제 3.6 (곱셈의 대표자 독립성) 식 (3.4)의 곱셈은 동치류에서 잘 정의된다.

증명. 먼저 첫 인자만 바꾸자. $(a, b) \sim (a', b')$이면 $a + b' = b + a'$이다. 두 곱의 동치 여부를 확인할 식은

$$(ac + bd) + (a'd + b'c) = (ad + bc) + (a'c + b'd)$$

이다. 왼쪽은 $(a+b')c + (b+a')d$이고, 오른쪽은 $(b+a')c + (a+b')d$이므로 가정으로 같다. 자연수 곱셈의 교환법칙에 의해 두 번째 인자의 변경도 같은 논증으로 처리된다. 두 인자를 차례로 바꾸면 일반적인 대표자 변경에 대한 결과를 얻는다. □

덧셈과 음수 연산의 잘 정의됨도 같은 식으로 확인한다. 그 뒤 정수의 결합법칙, 교환법칙, 분배법칙은 자연수 계산을 대표자에 적용하여 얻는다. 중요한 순서는 잘 정의됨을 먼저 확보하고, 그다음 동치류를 하나의 수처럼 계산하는 것이다.

3.4 정수의 순서와 자연수의 포함

자연수를 정수로 보내는 **매장**(*embedding*)은

$$\iota_{\mathbb{NZ}}(n) = [n, 0] \tag{3.5}$$

이다. $[n,0] = [m,0]$이면 $n = m$이므로 단사이고, 덧셈과 곱셈을 보존한다. 따라서 이 상을 원래 자연수와 동일시하여 사용할 수 있다. 엄밀한 부호화에서는 다른 집합일 수 있지만, 연산과 순서가 보존된다는 점이 수학적으로 중요하다.

정수의 순서를

$$[a,b] \le [c,d] \iff a + d \le c + b \tag{3.6}$$

로 정한다. 이 관계도 대표자 선택과 무관하다. 예를 들어 $a + b' = b + a'$와 $c + d' = d + c'$를 이용하여 양변에 공통 항을 더한 뒤 자연수 순서의 소거법칙을 적용하면 대표자를 바꾼 부등식과 동치임을 얻는다.

명제 3.7 (**정수의 표준형**) 모든 정수는 $[n,0]$ 또는 $[0,n]$ 꼴로 나타난다. $n > 0$인 두 꼴이 같은 정수가 되는 일은 없다.

증명. $[a,b]$에서 $a \ge b$이면 $a = b + n$인 자연수 n이 존재하여 $[a,b] = [n,0]$이다. $b \ge a$이면 같은 방식으로 $[a,b] = [0,n]$이다. 두 양의 크기 $n, m > 0$에 대해 $[n,0] = [0,m]$이면 $n + m = 0$이어야 하므로 불가능하다. □

이 표준형은 정수의 부호와 절댓값을 준다. 또한 $xy = 0$이면 $x = 0$ 또는 $y = 0$이라는 사실을 자연수의 곱에 대한 성질로부터 얻는다. 따라서 정수는 **영인자**(*zero divisor*)가 없는 가환환, 즉 **정역**(*integral domain*)이다. 이 성질은 다음 유리수 구성에서 분모를 소거할 때 필요하다.

예제 3.8 $[1,4]$는 정수 -3, $[5,2]$는 3을 나타낸다. 곱의 정의로

$$[1,4]\,[5,2] = [5 + 8,\ 2 + 20] = [13, 22] = [0, 9]$$

이므로 결과는 -9이다. 부호 규칙을 외부에서 강제로 붙인 것이 아니라 쌍의 연산이 그 규칙을 구현한다.

3.5 유리수: 정수의 비를 동치류로 만들기

이제 분모를 양의 자연수로 제한하자. $\mathbb{N}_{>0} = \omega \setminus \{0\}$에 대해

$$(a,b) \approx (c,d) \iff ad = bc, \qquad a, c \in \mathbb{Z}, \quad b, d \in \mathbb{N}_{>0} \tag{3.7}$$

로 정의한다. 양의 분모를 사용하는 이유는 부등식의 방향을 일관되게 다루기 위해서이다. 모든 영 아닌 정수 분모를 허용해도 다른 동치인 구성을 만들 수 있다.

명제 3.9 $\approx$는 동치관계이다.

증명. 반사성과 대칭성은 자명하다. $ad = bc$이고 $cf = de$이면 첫 등식에 f를, 두 번째 등식에 b를 곱하여

$$adf = bcf = bde$$

를 얻는다. $d \neq 0$이고 정수에 영인자가 없으므로 d를 소거하여 $af = be$를 얻는다. 따라서 추이성이 성립한다. □

유리수 집합은 이 몫집합이며, 동치류 $[(a,b)]$를 a/b로 쓴다. 연산과 순서는

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \qquad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}, \qquad -\frac{a}{b} = \frac{-a}{b}, \qquad \frac{a}{b} \le \frac{c}{d} \iff ad \le bc \tag{3.8}$$

이다. $bd > 0$이므로 연산 결과의 분모도 허용된 범위에 있다.

명제 3.10 (유리수 덧셈의 잘 정의됨) $a/b = a'/b'$이면 임의의 c/d에 대해 $(a/b)+(c/d) = (a'/b')+(c/d)$이다.

증명. 가정은 $ab' = a'b$이다. 두 합의 동치 여부를 교차 곱으로 확인하면

$$(ad+bc)b'd = ab'd^2 + bb'cd, \qquad (a'd+b'c)bd = a'bd^2 + bb'cd$$

이므로 두 값이 같다. 두 번째 인자 변경도 같은 논증으로 처리된다. □

$a \neq 0$일 때 a/b의 **역수**(*multiplicative inverse*)는 $a > 0$이면 b/a이고, $a < 0$이면 $(-b)/(-a)$이다. 두 경우 모두 분모가 양수이다. 이 구성으로 덧셈과 곱셈, 순서가 서로 호환되는 **순서체**(*ordered field*) $\mathbb{Q}$를 얻는다. 체의 항등식은 정수의 분배법칙과 교차 곱 계산으로 검증할 수 있다. 여기서는 모든 항등식을 하나씩 반복하기보다 대표자 독립성과 영 아닌 분모의 역할을 드러내는 계산을 제시했다.

3.6 수 체계의 확장은 구조를 보존한다

정수의 유리수 안으로의 매장은 $n \mapsto n/1$이다. 이 대응은 단사이고 연산과 순서를 보존한다. 이후 $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$라고 쓰는 것은 이 매장들을 통해 구조를 동일시한다는 관례이다. 각 단계의 원래 집합 부호화가 문자 그대로 부분집합일 필요는 없다.

명제 3.11 (유리수의 조밀성) $a, b \in \mathbb{Q}$이고 $a < b$이면 $a < c < b$인 유리수 c가 존재한다.

증명. $c = (a+b)/2$로 놓으면 $c - a = (b-a)/2 > 0$이고 $b - c = (b-a)/2 > 0$이다. □

조밀하다(*dense*)는 것은 두 수 사이에 또 다른 수가 있다는 뜻이다. 모든 빈틈이 메워져 있다는 **완비성**(*completeness*)과는 다르다. 유리수에는 $x^2 = 2$의 해가 없고, 그 해가 있어야 할 경계에서 위로 유계인 집합이 유리수 상한을 갖지 못하는 현상이 생긴다. 다음 장(제5권 제4장)의 실수 구성은 바로 그 문제를 해결한다.

3.7 해설이 있는 연습문제

연습문제 3.12 정수 구성에서 $(2,5)$, $(7,10)$, $(0,3)$이 같은 동치류인지 확인하라.

풀이. $2+10 = 5+7 = 12$이고 $2+3 = 5+0 = 5$이다. 따라서 세 쌍은 모두 같은 정수 -3을 나타낸다. 음수가 아직 도입되지 않은 단계에서도 동치 여부는 자연수 덧셈만으로 확인할 수 있다.

연습문제 3.13 정수 덧셈과 음수 연산이 잘 정의됨을 직접 확인하라.

풀이. $a+b' = b+a'$이면 $(a+c)+(b'+d) = (b+d)+(a'+c)$이므로 $[a+c, b+d] = [a'+c, b'+d]$이다. 음수에서는 $b + a' = a + b'$가 그대로 필요한 동치 조건이다. 두 번째 덧셈 인자의 변경은 같은 방식으로 처리한다.

연습문제 3.14 정수 $[a, b]$에서 $[a, b] + [b, a] = 0$임을 정의로 보여라.

풀이. 합은 $[a + b,\ a + b]$이다. $(a + b, a + b) \sim (0, 0)$은 $(a + b) + 0 = (a + b) + 0$이므로 성립한다. 역원은 쌍의 성분을 바꾸는 것으로 구현된다.

연습문제 3.15 유리수 구성에서 분모 0을 허용하면서 같은 교차 곱 관계를 쓰면 어떤 문제가 생기는가.

풀이. $(1, 1) \approx (0, 0)$이고 $(0, 0) \approx (2, 1)$이지만 $(1, 1) \not\approx (2, 1)$이다. 따라서 추이성이 깨져 동치 관계조차 되지 않는다. 분모를 영 아닌 값으로 제한하는 것은 나눗셈 기호의 관습에 그치지 않고 몫집합 구성의 논리적 조건이다.

연습문제 3.16 $-3/4$의 역수를 양의 분모로 표현하고 곱을 확인하라.

풀이. 역수는 $-4/3$이다. 곱은 $12/12 = 1$이며 두 분모는 모두 양수이다. 무심코 $4/(-3)$만 적어도 같은 수를 뜻하지만, 이 장의 대표자 집합에서는 양의 분모 표기로 바꾸어야 한다.

연습문제 3.17 “유리수는 조밀하므로 자연수보다 원소가 더 많다”라는 논증의 문제를 설명하라.

풀이. 조밀성은 순서의 성질이고 원소 수 비교는 전단사의 존재 문제이다. 자연수와 유리수 사이에는 전단사가 있으며 둘 다 가산 무한이다(제5권 제5장). 같은 크기의 집합에 서로 다른 순서 구조를 줄 수 있으므로 순서의 빈틈 모양만으로 기수를 비교할 수 없다.

연습문제 3.18 $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$를 서로 다른 집합으로 구성했는데도 $2 + 3 = 5$를 같은 식으로 쓸 수 있는 이유를 설명하라.

풀이. 매장 $n \mapsto [n, 0]$, $z \mapsto z/1$이 덧셈을 보존하기 때문이다. 자연수에서 계산한 뒤 매장한 값과 먼저 매장한 뒤 계산한 값이 일치한다. 단순한 표기 일치가 아니라 연산 보존이 이 관례를 정당화한다.

제 4 장

데데킨트 절단으로 실수를 구성하기

개요 이 장은 유리수의 부분집합인 데데킨트 절단(*Dedekind cut*)을 이용하여 실수체 $\mathbb{R}$을 구성한다. 유리수는 조밀하지만 위로 유계인 공집합 아닌 부분집합이 항상 유리수 최소 상계를 갖지는 않는다. 절단은 이 빈틈의 "왼쪽 전체"를 그대로 하나의 새 수로 삼는 구성으로, 극한이나 무한소수 전개를 먼저 전제하지 않고 유리수의 부분집합만으로 실수를 정의한다. 절단의 포함 관계가 순서를, 절단족의 합집합이 상한을 주고, 절단의 덧셈·곱셈·음수·역수를 정의한 뒤 그 결과가 완비 순서체임을 요약한다. 마지막으로 $\sqrt{2}$에 대응하는 절단을 구체적으로 구성하여 그것이 어떤 유리수의 절단도 아님을 증명한다. 선행 지식: 유리수의 순서체 성질과 조밀성(제5권 제3장), 상계와 최소 상계의 뜻. 수열의 극한이나 무한소수를 실수의 정의로 미리 사용하지 않는다.

4.1 채울 빈틈을 먼저 정확히 정하기

유리수 집합은 조밀하지만, 위로 유계인 공집합 아닌 부분집합이 항상 유리수 최소 상계를 갖지는 않는다. 예컨대 음의 유리수 전부와 제곱이 2보다 작은 음이 아닌 유리수를 모은 집합의 경계는 유리수가 아니다. 경계가 있어야 한다는 그림만으로 새 수를 만들지 않고, 경계의 왼쪽에 있는 유리수 집합 자체를 새 수로 삼는 것이 절단 구성이다.

정의 4.1 (아래쪽 데데킨트 절단) $A \subseteq \mathbb{Q}$가 다음 세 조건을 만족하면 **절단**(*cut*)이라고 한다.

(1) $A \neq \varnothing$이고 $A \neq \mathbb{Q}$이다.

(2) $a \in A$이고 $q < a$이면 $q \in A$이다.

(3) $a \in A$이면 $a < b$인 $b \in A$가 존재한다.

절단 전체의 집합을 $\mathbb{R}$로 정의한다. 이는 $\mathcal{P}(\mathbb{Q})$에서 위 조건을 만족하는 부분집합들을 분리한 집합이다.

두 번째 조건은 아래로 닫혀 있음을, 세 번째 조건은 최대 원소가 없음을 뜻한다. 어떤 정의에서는 위쪽 부분까지 함께 기록하지만, 아래쪽 집합의 여집합으로 위쪽을 복원할 수 있으므로 정보가 중복된다. 이 장에서는 경계가 유리수여도 아래쪽 부분에 경계 자체를 넣지 않는 관례를 고정한다.

예제 4.2 유리수 r에 대해

$$\widehat{r} = \{q \in \mathbb{Q} : q < r\} \tag{4.1}$$

는 절단이다. 공집합도 전체도 아니고, 아래로 닫혀 있으며, $q < r$이면 $(q + r)/2$가 그 사이에 있으므로 최대 원소가 없다. 반면 $\{q \in \mathbb{Q} : q \le r\}$는 최대 원소 r을 가지므로 이 장의 절단이 아니다.

4.2 포함 관계가 실수의 순서가 된다

절단에 $A \le B \iff A \subseteq B$로 순서를 준다. 이 순서는 전순서이다. 사실 $A \not\subseteq B$이면 $a \in A \setminus B$를 고를 수 있다. 임의의 $b \in B$는 $b < a$여야 한다. $b \ge a$라면 $b = a$이거나 B의 아래 닫힘에 의해 $a \in B$가 되어 모순이기 때문이다. 그러므로 $b \in A$이고 $B \subseteq A$이다.

유리수 매장 $r \mapsto \widehat{r}$는 순서를 정확히 보존한다. $r < s$이면 $r \in \widehat{s} \setminus \widehat{r}$이므로 $\widehat{r} \subsetneq \widehat{s}$이다. 반대로 포함 관계가 성립하면 유리수의 순서 때문에 $r \le s$이다. 이제 유리수를 해당 절단과 동일시할 수 있지만, 구성 과정의 증명에서는 필요에 따라 모자를 유지한다.

> **명제 4.3 (유리수의 실수 안에서의 조밀성)** $A \subsetneq B$인 절단 사이에는 $A \subsetneq \widehat{r} \subsetneq B$인 유리수 r이 존재한다.

증명. $b \in B \setminus A$를 고른다. B에는 최대 원소가 없으므로 $b < r$인 $r \in B$가 있다. $b \notin A$이므로 모든 $a \in A$에 대해 $a < b < r$이고, 따라서 $A \subseteq \widehat{r}$이다. $b \in \widehat{r} \setminus A$이므로 첫 포함은 진포함이다. $r \in B$와 아래 닫힘으로 $\widehat{r} \subseteq B$이고, $r \notin \widehat{r}$이므로 두 번째 포함도 진포함이다. □

> **명제 4.4 (정수 상계)** 각 절단 A보다 큰 자연수 절단 $\widehat{n}$이 존재한다.

증명. $A \neq \mathbb{Q}$이므로 $r \notin A$인 유리수를 하나 고른다. 유리수의 분수 표현을 이용하면 $r < n$인 자연수 n을 찾을 수 있다. 모든 $a \in A$는 $a < r < n$이므로 $A \subseteq \widehat{n}$이고, $r \in \widehat{n} \setminus A$이므로 진포함이다. □

4.3 최소 상계가 합집합으로 나타나는 이유

> **정리 4.5 (절단의 완비성)** $\mathcal{S} \subseteq \mathbb{R}$가 공집합이 아니고 위로 유계이면 최소 상계가 존재한다. 구체적으로
>
> $$\sup \mathcal{S} = \bigcup_{A \in \mathcal{S}} A \tag{4.2}$$
>
> 이다.

증명. $U = \bigcup \mathcal{S}$라 하자. $\mathcal{S} \neq \varnothing$이고 그 원소인 절단은 공집합이 아니므로 $U \neq \varnothing$이다. 상계인 절단 B를 고르면 모든 $A \in \mathcal{S}$에 대해 $A \subseteq B$이므로 $U \subseteq B \neq \mathbb{Q}$이다.

$x \in U$이면 어떤 $A \in \mathcal{S}$에 $x \in A$이다. $q < x$이면 A의 아래 닫힘으로 $q \in A \subseteq U$이다. 또한 $x < y$인 $y \in A$가 있으므로 U에도 최대 원소가 없다. 따라서 U는 절단이다.

각 $A \in \mathcal{S}$가 U에 포함되므로 U는 상계이다. 다른 상계 C는 모든 A를 포함하므로 그 합집합 U도 포함한다. 즉 $U \le C$이므로 U가 최소 상계이다. □

이 증명은 유계성과 공집합이 아니라는 조건이 어디서 쓰이는지를 보여 준다. 유계성은 합집합이 $\mathbb{Q}$ 전체가 되는 일을 막고, 공집합이 아니라는 조건은 합집합이 빈 집합이 되는 일을 막는다. 상한이라는 대상은 존재 조건이 빠진 채 아무 집합에나 붙일 수 있는 기호가 아니다.

> **예제 4.6** $\{\widehat{n} : n \in \mathbb{N}\}$은 위로 유계가 아니며, 그 합집합은 $\mathbb{Q}$이다. 따라서 이 집합족의 합집합은 절단이 아니다. 완비성 정리가 이 사례에 적용되지 않는 이유는 실수 구성이 실패해서가 아니라 유계성 가정이 빠졌기 때문이다.

4.4 절단의 덧셈과 영원소

두 절단의 덧셈을 유리수 합들의 집합으로 정의한다.

$$A + B = \{a + b : a \in A,\ b \in B\}. \tag{4.3}$$

이 집합은 절단이다. 비어 있지 않은 것은 두 절단에 원소가 있기 때문이다. $\alpha \notin A, \beta \notin B$를 고르면 모든 $a \in A, b \in B$에 대해 $a < \alpha, b < \beta$여서 $a+b < \alpha+\beta$이므로 전체 유리수 집합이 되지 않는다.

아래 닫힘을 확인하려면 $q < a+b$일 때 $a' = q - b < a$를 사용한다. 그러면 $a' \in A$이고 $q = a' + b$이다. 최대 원소가 없다는 성질은 a보다 큰 $a' \in A$를 골라 $a + b < a' + b$로 확인한다. 덧셈의 교환법칙과 결합법칙은 유리수 합의 해당 법칙을 원소 수준에서 적용하면 된다.

명제 4.7 $0_{\mathbb{R}} = \widehat{0}$는 덧셈의 영원소이다. 또한 $\widehat{r} + \widehat{s} = \widehat{r+s}$이다.

증명. $a \in A, b < 0$이면 $a + b < a$이므로 $a + b \in A$이다. 따라서 $A + \widehat{0} \subseteq A$이다. 반대로 $x \in A$이면 $x < a$인 $a \in A$를 고를 수 있고 $b = x - a < 0$으로 두면 $x = a + b \in A + \widehat{0}$이다.

유리수 매장에 대해서는 $a < r, b < s$이면 $a + b < r + s$이므로 한쪽 포함이 성립한다. $q < r + s$가 주어지면 $\delta = (r + s - q)/2 > 0$으로 놓고 $a = r - \delta, b = s - \delta$로 두면 $a < r, b < s, a + b = q$이므로 반대 포함도 성립한다. □

4.5 음수에서 경계 하나를 주의해야 한다

단순히 $\{-a : a \in A\}$를 만들면 위로 닫힌 집합이 되어 절단이 되지 않는다. 여집합의 부호를 뒤집되 최대 원소가 생기지 않도록 다음과 같이 정의한다.

$$-A = \{q \in \mathbb{Q} : \exists r \in \mathbb{Q} \setminus A\ (q < -r)\}. \tag{4.4}$$

이 집합은 비어 있지 않고 아래로 닫혀 있으며, $q < -r$ 사이에 다른 유리수를 넣어 최대 원소가 없음을 알 수 있다. $a \in A$를 하나 고르면 모든 $r \notin A$에 대해 $a < r$이므로 $-a$는 위 집합의 원소가 될 수 없다. 따라서 진부분집합 조건도 만족한다.

보조정리 4.8 (경계의 유리수 근사) 절단 A와 양의 유리수 ε에 대해 $a \in A, r \notin A, r - a = \varepsilon$인 유리수 a, r가 존재한다.

증명. $a_0 \in A$를 고르고, A의 유리수 상계 u를 고른다. 충분히 큰 자연수 N에 대해 $a_0 + N\varepsilon > u$이므로 $a_0 + N\varepsilon \notin A$이다. 그러한 양의 자연수 가운데 최소인 n을 고르면 $a = a_0 + (n-1)\varepsilon \in A$이고 $r = a_0 + n\varepsilon \notin A$이다. □

정리 4.9 $A + (-A) = \widehat{0}$이다.

증명. $a \in A$이고 $b \in -A$이면 어떤 $r \notin A$에 대해 $b < -r$이다. $a < r$이므로 $a + b < 0$이다. 따라서 $A + (-A) \subseteq \widehat{0}$이다.

반대로 $t < 0$인 유리수를 잡자. $\varepsilon = -t/2 > 0$으로 놓고 보조정리 4.8에서 $a \in A, r \notin A, r - a = \varepsilon$을 얻는다. $b = t - a$로 두면

$$b + r = t + (r - a) = t + \varepsilon = t/2 < 0$$

이므로 $b < -r$이고 $b \in -A$이다. 따라서 $t = a + b \in A + (-A)$이다. □

흔한 오류. 경계가 유리수인 경우를 확인하지 않은 채 여집합과 부호 반전을 조합하면 닫힌 끝점이 생길 수 있다. 식 (4.4)의 엄격한 부등호 $q < -r$는 이 끝점을 제거한다.

4.6 곱셈과 역수의 구성

먼저 $A, B \geq \widehat{0}$인 절단에 대해

$$AB = \{q \in \mathbb{Q} : q < 0 \text{ 또는 } \exists a \in A\ \exists b \in B\ (a > 0 \wedge b > 0 \wedge q < ab)\} \tag{4.5}$$

로 정의한다. 이 정의는 두 절단 가운데 하나가 $\widehat{0}$일 때 곱이 정확히 $\widehat{0}$이 되게 한다. 두 절단이 양수이면 양의 원소 a, b를 고를 수 있어 곱도 양수이다. 양의 유리수 상계 α, β를 고르면 $\alpha\beta$가 상계가 되고, 엄격한 부등호 때문에 최대 원소가 생기지 않는다.

일반적인 부호에 대해서는 절댓값을 양의 절단으로 바꾼 뒤 부호 규칙으로 확장한다.

$$AB = \begin{cases} -((-A)B), & A < 0 \leq B, \\ -(A(-B)), & B < 0 \leq A, \\ (-A)(-B), & A < 0,\ B < 0. \end{cases} \tag{4.6}$$

이미 두 수가 음이 아닌 경우의 정의가 있으므로 이 경우 나눔은 겹치지 않는다. 표기 0은 여기서 $\widehat{0}$을 뜻한다.

양의 절단 A의 역수는

$$A^{-1} = \{q \in \mathbb{Q} : \exists r \in \mathbb{Q}\ (r > 0 \wedge r \notin A \wedge q < 1/r)\} \tag{4.7}$$

로 정의할 수 있다. 이 집합은 음의 유리수와 0을 모두 포함한다. A 안의 양의 유리수 a를 하나 잡으면 $1/a$가 상계이고, 양의 유리수 $r \notin A$를 하나 잡으면 $1/(2r)$가 원소이므로 양수 절단이다. 음의 A에는 $A^{-1} = -((-A)^{-1})$로 확장한다. 영원소에는 곱셈의 역수가 없다.

> **명제 4.10 (실수체 구성의 결과)** 위 덧셈, 곱셈, 순서를 가진 절단 집합은 완비 순서체이다. 유리수 매장은 두 연산과 순서를 보존한다.

증명의 핵심. 순서와 완비성, 덧셈과 덧셈 역원은 앞에서 증명했다. 곱셈은 양의 유리수 근사를 이용하여 각 포함을 확인한다. 예를 들어 $q < ab$를 만족하는 양의 $a \in A$, $b \in B$가 있으면 그 곱보다 조금 작은 유리수들을 사용해 결합법칙의 중간 곱에 필요한 원소를 만들 수 있다. 반대 포함은 증명 순서를 바꾸면 된다. 분배법칙도 $a(b + c) = ab + ac$와 절단 안에서 더 큰 근삿값을 고를 수 있다는 성질을 사용한다. 역수 법칙은 경계 근사를 점점 좁혀 AA^{-1}에 속하는 유리수가 정확히 1보다 작은 것들임을 보인다. 이 문단은 나머지 체 공리의 검증 경로를 요약하며, 모든 경우의 원소별 포함 증명을 전개한 것은 아니다. □

> **따름정리 4.11 (아르키메데스 성질)** 이 결과를 얻은 뒤에는 통상의 체 계산을 사용할 수 있다. 특히 $x > 0$이면 충분히 큰 자연수 n에 대해 $nx > 1$이다.

증명. 명제 4.4에서 자연수가 위로 유계가 아님을 보였으므로 $n > 1/x$를 고르면 된다. □

4.7 유리수가 아닌 절단의 실제 예

예제 4.12 (유리수가 아닌 절단) 다음 집합을 보자.

$$D = \{q \in \mathbb{Q} : q < 0 \text{ 또는 } q^2 < 2\}. \tag{4.8}$$

$1 \in D$이고 $2 \notin D$이므로 공집합도 전체도 아니다. 아래로 닫힌 것도 직접 확인할 수 있다. 최대 원소가 없다는 조건을 확인해 보자. $q < 0$이면 $0 \in D$가 더 큰 원소이다. $q \geq 0$, $q^2 < 2$이면

$$\varepsilon = \frac{1}{2}\min\left(1,\ \frac{2 - q^2}{2q + 1}\right) > 0$$

로 놓는다. $\varepsilon \leq 1$이므로

$$(q + \varepsilon)^2 - q^2 = 2q\varepsilon + \varepsilon^2 \leq (2q + 1)\varepsilon < 2 - q^2.$$

따라서 $q + \varepsilon \in D$이고 D는 절단이다.

명제 4.13 D는 어떤 유리수 r에 대해서도 $\widehat{r}$와 같지 않다.

증명. $D = \widehat{r}$라고 가정하면 $1 \in D$이므로 $r > 1$이다. $r^2 < 2$이면 $r \in D$가 되어 $r \notin \widehat{r}$와 모순이다. $r^2 > 2$이면 충분히 작은 양의 유리수 δ에 대해 $0 < r - \delta < r$이고 $(r - \delta)^2 > 2$가 된다. 예컨대 $\delta < \min(r, (r^2 - 2)/(2r))$이면 된다. 이때 $r - \delta$는 $\widehat{r}$에는 속하지만 D에는 속하지 않아 모순이다. 남은 가능성은 $r^2 = 2$이다. $r = a/b$를 서로소인 양의 정수로 표현하면 $a^2 = 2b^2$에서 a가 짝수이고, $a = 2c$를 대입하면 b도 짝수이다. 서로소 조건과 모순이다. 따라서 세 경우 모두 불가능하다. □

실수체에서 이 양의 절단이 $\sqrt{2}$이다. 중요한 점은 "무리수는 무한히 긴 소수"라는 설명보다 먼저, 유리수만을 사용한 명확한 집합 정의로 이 대상을 만들었다는 것이다. 무한소수와 코시 수열에 의한 표현은 이후 이 실수체와 연결할 수 있는 또 다른 표현 방식이다.

역사 (데데킨트의 절단). 데데킨트(*Richard Dedekind*)는 1872년의 소책자 「연속성과 무리수」(*Stetigkeit und irrationale Zahlen*)에서 절단에 의한 실수 구성을 발표하였다. 비슷한 시기에 칸토어(*Cantor*)와 메레(*Méray*)는 유리수 코시 수열의 동치류로 실수를 구성하는 방법을 내놓았다. 두 구성은 서로 다른 대상(유리수의 부분집합과 유리수열의 동치류)에서 출발하지만, 완비 순서체로서 동형인 같은 구조를 낳는다는 점에서 실수의 본질이 특정 구성법에 있지 않음을 보여 준다.

4.8 해설이 있는 연습문제

연습문제 4.14 $\bigcap_{n \geq 1} \widehat{1/n}$이 절단인지 판정하라.

풀이. 이 교집합은 $\{q \in \mathbb{Q} : q \leq 0\}$이다. $q \leq 0$이면 모든 $1/n$보다 작고, $q > 0$이면 충분히 큰 n에 대해 $1/n \leq q$여서 교집합에 속하지 않는다. 이 집합에는 최대 원소 0이 있으므로 절단이 아니다. 절단의 임의 교집합이 언제나 절단이라는 주장은 거짓이다.

연습문제 4.15 $-\widehat{r} = \widehat{-r}$임을 정의로 보여라.

풀이. $s \notin \widehat{r}$는 $s \geq r$라는 뜻이다. $q < -s$이면 $q < -r$이다. 반대로 $q < -r$이면 $s = r \notin \widehat{r}$를 선택하여 음수 절단의 조건을 만족시킨다. 따라서 두 집합이 같다.

연습문제 4.16 왜 덧셈의 영원소 증명에 최대 원소가 없다는 조건이 필요한가.

풀이. $x \in A$를 $a + b$로 표현하면서 $b < 0$을 만들려면 $x < a$인 $a \in A$가 필요하다. 만일 최대 원소 x가 있다면 이 단계가 막힌다. 절단의 끝점 관례는 연산의 항등식에도 영향을 준다.

연습문제 4.17 $\mathcal{S}$가 공집합 아닌 아래로 유계인 실수 집합일 때 최소 상계 성질로 최대 하계를 얻는 방법을 설명하라.

풀이. $-\mathcal{S} = \{-x : x \in \mathcal{S}\}$는 공집합이 아니고 위로 유계이다. $u = \sup(-\mathcal{S})$를 잡으면 $-u$가 $\mathcal{S}$의 최대 하계이다. 부호를 바꾸면 부등호가 뒤집히므로 하계 조건과 최대성 모두 상계 조건과 최소성에서 따라온다.

연습문제 4.18 $0 < A < B$이면 역수의 순서가 어떻게 바뀌는지 설명하라.

풀이. 체와 순서의 호환성을 사용하면 $B - A > 0$이고 $AB > 0$이므로 $1/A - 1/B = (B-A)/(AB) > 0$이다. 따라서 $0 < B^{-1} < A^{-1}$이다. 분모의 양수 조건을 확인하지 않고 부등식 양변에 역수를 취하면 안 된다.

연습문제 4.19 실수의 정의에 이미 실수인 경계값 α를 넣어 $\{q : q < \alpha\}$라고만 쓰는 설명이 불충분한 이유를 말하라.

풀이. 실수 α를 아직 구성하지 않았는데 이를 정의에 사용하면 순환적이다. 절단 구성은 유리수의 부분집합 가운데 세 조건을 만족하는 모든 집합을 먼저 모은다. 구성 후에는 각 절단을 그 경계값처럼 읽을 수 있으므로 그런 표기가 정당해진다.

연습문제 4.20 완비성 증명에서 선택공리로 각 절단의 원소를 동시에 하나씩 골랐는지 확인하라.

풀이. 그렇지 않다. 합집합은 집합족 자체에서 직접 구성된다. 비어 있지 않음을 보일 때 절단 하나와 그 원소 하나를 고르고, 특정 $x \in U$에 대한 성질을 보일 때 이를 포함하는 절단 하나를 사용했을 뿐이다. 집합족 전체에 대한 선택 함수를 만들지 않았다.

제 5 장

가산성, 대각선, 기수와 서수의 입문

개요 이 장은 집합의 크기를 전단사·단사로 비교하는 방법을 정비하고, 자연수·정수·유리수가 가산이라는 사실과 실수·멱집합이 비가산이라는 사실을 증명한다. 칸토어의 대각선 논증을 멱집합에 적용하여 임의의 집합이 자신의 멱집합보다 진정으로 작다는 사실(정리 5.5)을 보이고, 이를 변형하여 실수의 비가산성을 소수 표현의 중복 문제 없이 증명한다. 이어서 서수를 추이적이고 $\in$으로 정렬된 집합으로 도입하여, 같은 기수를 갖는 집합도 서로 다른 순서형을 가질 수 있음을 밝히고, 다음 장에서 다룰 선택공리와 연속체 가설을 읽는 데 필요한 최소한의 어휘($\aleph_0$, $\aleph_1$, CH)를 준비한다. 선행 지식: 단사·전사·전단사, 슈뢰더–베른슈타인 정리(제4권 제8장), 실수의 최소상계 성질(제5권 제4장), 정렬 원리(제4권 제6장). 가산 합집합에 관한 결과에서는 선택공리의 사용 여부를 그때그때 밝힌다.

5.1 크기를 비교한다는 말의 정확한 뜻

두 집합의 크기를 비교하는 가장 기본적인 도구는 전단사이다. 두 집합 A, B 사이에 전단사가 있으면 두 집합은 같은 크기, 또는 같은 **기수**(*cardinality*)를 갖는다고 말하고 $|A| = |B|$로 쓴다. 단사 함수 $A \to B$가 존재하면 $|A| \le |B|$라고 쓴다. 양방향 단사, 곧 $|A| \le |B|$이고 $|B| \le |A|$이면 전단사가 있다는 슈뢰더–베른슈타인 정리(제4권 제8장)는 선택공리 없이 성립한다. 따라서 이 크기 비교는 적절한 반대칭성을 갖는다.

> **정의 5.1 (유한·가산·비가산)** 집합이 어떤 자연수 $n = \{0, \dots, n-1\}$과 전단사이면 **유한**이라고 한다. $\mathbb{N}$과 전단사이면 **가산 무한**(*countably infinite*)이라고 한다. 유한 또는 가산 무한인 집합을 **가산**(*countable*)이라고 부른다. 가산이 아닌 집합은 **비가산**(*uncountable*)이다.

참고 (용어의 관례). 문헌에 따라 "가산"이라는 말을 가산 무한의 뜻으로만 쓰기도 한다. 이 권에서는 유한 집합과 공집합도 가산에 포함한다. 따라서 가산 집합을 자연수로 나열한다고 말할 때, 공집합의 예외와 유한 집합에서의 반복을 명시해야 한다.

> **명제 5.2** 공집합 아닌 집합 A가 가산일 필요충분조건은 전사 함수 $e : \mathbb{N} \to A$가 존재하는 것이다.

증명. A가 가산 무한이면 전단사를 쓰면 된다. A가 공집합 아닌 유한 집합이면 원소를 유한하게 나열한 뒤 같은 목록을 반복하면 전사를 얻는다.

반대로 전사 e가 있으면 각 $a \in A$에 대해

$$m(a) = \min\{n \in \mathbb{N} : e(n) = a\}$$

를 정의한다. e가 전사이므로 이 집합은 공집합이 아니고, 자연수의 공집합 아닌 부분집합에는 가장 작은 원소가 있다는 정렬 원리(제4권 제6장)에 의해 최소 원소가 유일하게 존재하므로 선택공리가 필요하지 않다. 서로 다른 원소는 서로 다른 최소 지표를 가지므로 $m : A \to \mathbb{N}$은 단사이다.

$m(A)$가 유한이면 A도 유한이고, 무한이면 $m(A)$의 원소를 작은 것부터 차례로 나열하여 $\mathbb{N}$과 전단사를 만든다. 따라서 A는 가산이다. □

5.2 유리수를 셀 수 있는 이유

정수는 $0, 1, -1, 2, -2, \dots$로 나열할 수 있으므로 가산이다. 자연수의 순서쌍은 합 $m+n$이 같은 대각선을 차례로 훑어 나열할 수 있다.

유도 (대각선 나열의 명시적 공식). 합이 $k = m+n$인 쌍 (m,n)은 $k+1$개 있다. k가 작은 대각선부터, 각 대각선 안에서는 n이 커지는 순서로 나열하면 합이 k보다 작은 쌍은 $1+2+\cdots+k = k(k+1)/2$개 앞서 나오므로, 쌍 (m,n)의 지표는

$$\pi(m,n) = \frac{(m+n)(m+n+1)}{2} + n \tag{5.1}$$

이다. π는 $\mathbb{N}\times\mathbb{N}$에서 $\mathbb{N}$으로의 전단사이며 **칸토어 짝짓기 함수**(*Cantor pairing function*)라고 부른다. 이 공식으로 "대각선을 따라 나열한다"는 서술을 구체적인 전단사로 바꿀 수 있다.

식 (5.1)과 $\mathbb{Z}$의 가산성을 합성하면 $\mathbb{Z}\times\mathbb{N}_{>0}$도 가산이다. 이 집합에서 $\mathbb{Q}$로 가는 전사

$$(a,b) \longmapsto \frac{a}{b}$$

가 있으므로, 명제 5.2에 의해 유리수는 가산이다. 같은 유리수가 여러 번 나타나도 전사라는 사실에는 문제가 없고, 최소 등장 지표를 사용하면 중복 없는 나열을 얻는다.

> **예제 5.3** 분모가 1인 모든 유리수를 먼저 끝낸 다음 분모가 2인 것을 시작하려는 방식은 나열에 실패한다. 첫 단계 자체가 무한하기 때문이다. 대각선 나열은 모든 쌍 (a,b)가 유한한 지표에서 등장하도록 탐색 범위를 늘린다. "각 행이 가산이다"라는 설명만으로 전체 나열의 순서가 자동으로 정해지는 것은 아니다.

참고 (순서의 조밀성과 기수는 별개). 순서의 조밀성과 기수는 별개이다. $\mathbb{Q}$와 $\mathbb{N}$의 기수는 같지만, $\mathbb{N}$의 두 연속 원소 사이에는 자연수가 없고 $\mathbb{Q}$의 서로 다른 두 원소 사이에는 유리수가 있다. 한 집합을 다른 집합에 대응시키는 전단사가 순서를 보존할 필요는 없다.

5.3 가산 합집합에 숨은 자료와 선택

각 $n \in \mathbb{N}$에 대해 공집합 아닌 가산 집합 A_n이 있고, 전사 $e_n : \mathbb{N} \to A_n$들이 이미 하나의 함수족으로 주어졌다고 하자. 그러면

$$(n,k) \longmapsto e_n(k)$$

는 $\mathbb{N}^2$에서 $\bigcup_n A_n$으로의 전사이다. 명제 5.2에 의해 합집합은 가산이다. 이 증명은 나열들이 이미 주어졌다는 자료를 사용한다.

하지만 "각 A_n은 가산이다"라는 문장만 있을 때에는 각 집합에 대해 어떤 나열이 존재한다는 사실과, 모든 n에 대해 나열을 동시에 고른 함수족이 존재한다는 사실을 구별해야 한다. ZFC에서는 선택공리로 이 함수족을 확보하여 가산 합집합 정리를 얻는다(선택공리의 정확한 쓰임은

제5권 제6장에서 다룬다). ZF만을 배경으로 할 때에는 일반적인 정리를 추가 논증 없이 사용하면 안 된다. 이 장에서는 필요한 나열을 명시적으로 제공하거나 선택 가정을 표시한다.

> **예제 5.4** $A_n = \{0, 1, \dots, n\}$이면 $e_n(k)$를 k를 $n+1$로 나눈 나머지로 정할 수 있다. 모든 나열을 하나의 식으로 지정했으므로 선택공리가 필요 없다. 반면 구조가 전혀 주어지지 않은 가산 집합족에는 이런 공식이 자동으로 생기지 않는다.

5.4 대각선은 목록에서 빠진 대상을 만든다

> **정리 5.5 (칸토어)** 임의의 집합 X에서 멱집합 $\mathcal{P}(X)$로의 전사 함수는 존재하지 않는다. 특히 $|X| < |\mathcal{P}(X)|$이다.

증명. $f : X \to \mathcal{P}(X)$가 전사라고 가정하고

$$D = \{x \in X : x \notin f(x)\}$$

를 분리로 만든다. 전사성에 의해 $f(d) = D$인 $d \in X$가 있다. 그러면

$$d \in D \iff d \notin f(d) \iff d \notin D$$

이므로 모순이다. 한편 $x \mapsto \{x\}$는 X에서 $\mathcal{P}(X)$로의 단사이므로 $|X| \le |\mathcal{P}(X)|$이고, 전사가 없으므로 등호는 성립하지 않아 크기는 엄격히 증가한다. $\square$

역사 (대각선 논증의 계보). 칸토어는 1874년에 구간 축소법으로 실수의 비가산성을 먼저 증명했고, 1891년 논문에서 지금의 대각선 논증을 발표했다. 정리 5.5의 증명에서 집합 D를 만드는 방식은 러셀 역설($\{x : x \notin x\}$)과 모양이 비슷하지만, D는 기존 집합 X 안에서 분리했으므로 정당한 집합이다. 모순의 원인은 분리의 존재가 아니라, 모든 부분집합을 빠짐없이 나열한다는 전사성 가정에 있다.

> **따름정리 5.6** 무한 이진 수열 전체 $\{0,1\}^{\mathbb{N}}$는 비가산이다.

증명. 각 부분집합 $A \subseteq \mathbb{N}$에 특성 함수 χ_A를 대응시키면 $\mathcal{P}(\mathbb{N})$과 $\{0,1\}^{\mathbb{N}}$ 사이의 전단사를 얻는다. 칸토어 정리에 의해 $\mathcal{P}(\mathbb{N})$는 가산일 수 없다. $\square$

5.5 실수의 비가산성을 끝점 문제 없이 보이기

소수 전개를 사용한 대각선 논증에서는 $0.4999\ldots = 0.5000\ldots$ 같은 중복 표현을 주의해야 한다. 여기서는 삼진 자리 $0, 2$만 쓰고 직접 부등식으로 단사성을 보인다.

각 $A \subseteq \mathbb{N}$에 대해 유리수 부분합

$$s_m(A) = \sum_{n=0}^{m-1} \frac{2\chi_A(n)}{3^{n+1}}, \qquad s_0(A) = 0 \tag{5.2}$$

을 정의하고 $x_A = \sup\{s_m(A) : m \in \mathbb{N}\}$로 둔다. 부분합은 증가하고 1 이하이므로 실수의 완비성(제5권 제4장)에 의해 $x_A \in [0,1]$이 존재한다. 여기서는 무한급수라는 대상을 별도로 가정하지 않고 상한으로 값을 정의했다.

명제 5.7 사상 $A \mapsto x_A$는 $\mathcal{P}(\mathbb{N})$에서 $[0,1]$로의 단사이다.

증명. $A \neq B$이면 두 특성 함수가 처음으로 달라지는 지표 k가 있다. 필요하면 이름을 바꾸어 $k \in A \setminus B$라 하자. $n < k$인 모든 n에서 $\chi_A(n) = \chi_B(n)$이므로, 이 공통 앞부분의 합을 S라 쓰면

$$s_{k+1}(A) = S + \frac{2}{3^{k+1}}, \qquad s_{k+1}(B) = S.$$

부분합이 증가하므로 $x_A \geq S + 2/3^{k+1}$이다. 한편 k 이후 모든 자리에 2를 넣은 경우의 부분합이 가장 크므로, 기하급수 공식에 의해

$$x_B \leq S + \sum_{n=k+1}^{\infty} \frac{2}{3^{n+1}} = S + \frac{1}{3^{k+1}}$$

이다. 두 부등식을 빼면

$$x_A - x_B \geq \left(S + \frac{2}{3^{k+1}}\right) - \left(S + \frac{1}{3^{k+1}}\right) = \frac{1}{3^{k+1}} > 0$$

이므로 $x_A \neq x_B$이다. □

칸토어 정리와 이 단사성으로 $\mathbb{R}$는 비가산이다. 반대 방향으로, 실수는 유리수의 절단이므로 $\mathbb{R} \subseteq \mathcal{P}(\mathbb{Q})$이다. $\mathbb{Q}$가 $\mathbb{N}$과 전단사이므로 $\mathcal{P}(\mathbb{Q})$와 $\mathcal{P}(\mathbb{N})$도 전단사이다. 양방향 단사와 슈뢰더–베른슈타인 정리를 합치면

$$|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| = 2^{\aleph_0} \tag{5.3}$$

를 얻는다. $2^{\aleph_0}$는 이 단계에서 지수 함수의 실숫값이 아니라, 자연수 집합에서 두 원소 집합으로 가는 함수들의 기수이다.

5.6 서수는 크기가 아니라 순서형을 기록한다

같은 기수의 집합에도 서로 다른 정렬 순서를 줄 수 있다. 자연수를 통상 순서로 나열한 뒤 맨 끝에 새 원소 하나를 붙이면 여전히 가산이지만 가장 큰 원소가 생긴다. 이 차이를 기록하려면 기수와 다른 불변량이 필요하다.

정의 5.8 (추이적 집합과 서수) 집합 T가 **추이적**(*transitive*)이라는 것은 $x \in T$이면 $x \subseteq T$라는 뜻이다. 동치로 $\bigcup T \subseteq T$이다. **서수**(*ordinal*)는 추이적인 집합이며 원소 관계 $\in$에 의해 엄격하게 정렬되는 집합이다.

각 폰 노이만 자연수와 ω는 서수이다. 서수의 기본 정리에 따르면 두 서수는 서로 같거나 한쪽이 다른 쪽의 원소이고, 서수의 원소 역시 서수이다. 각 정렬 집합은 유일한 서수와 순서 동형이다. 이 결과들의 일반적 증명에는 초한 재귀와 정렬 순서 비교가 사용되므로, 여기서는 서수의 정의와 처음 사례들을 중심으로 다룬다.

서수 α의 **후속자**는 $\alpha + 1 = \alpha \cup \{\alpha\}$이다. 따라서

$$\omega + 1 = \{0, 1, 2, \ldots, \omega\}$$

에는 가장 큰 원소 ω가 있다. ω에는 가장 큰 원소가 없으므로 두 순서형은 다르다. 하지만 원소 수는 같다. 구체적으로 ω라는 마지막 원소를 0에, 각 자연수 n을 $n+1$에 보내면 집합으로서는 전단사가 된다.

예제 5.9 (서수 덧셈의 비가환성) 서수 덧셈 $\alpha+\beta$는 α 모양의 정렬 뒤에 β 모양의 정렬을 이어 붙인 순서형이다. 따라서 $1+\omega=\omega$이지만 $\omega+1\neq\omega$이다. 첫 식은 처음의 한 원소와 그 뒤의 자연수 나열을 모두 자연수처럼 다시 번호 붙일 수 있어서 성립한다. 두 번째 식에서는 마지막 원소가 존재한다는 순서 성질이 다르다. 기수 덧셈과 서수 덧셈에 같은 기호를 쓸 때 문맥을 확인해야 한다.

5.7 기수와 연속체 가설을 읽는 데 필요한 최소 배경

정렬 가능한 집합의 기수는 그 집합과 전단사인 서수들 가운데 가장 작은 서수로 나타낼 수 있다. 선택공리를 가정하면 모든 집합이 정렬 가능하므로(제5권 제6장) 모든 집합에 이 표현을 사용할 수 있다. $\aleph_0$는 가장 작은 무한 기수이며 ω로 나타난다. $\aleph_1$은 그다음 무한 기수, 즉 가장 작은 비가산 서수의 기수이다.

$\omega+1$은 ω보다 큰 서수이지만 여전히 가산이므로 $\aleph_1$이 아니다. “다음 서수”와 “다음 기수”는 서로 다르다. 또한 칸토어 정리는 $2^{\aleph_0}>\aleph_0$만 말하며, 그 값이 즉시 다음 기수인지는 결정하지 않는다.

정의 5.10 (연속체 가설) **연속체 가설**(*continuum hypothesis*, CH)는

$$2^{\aleph_0}=\aleph_1$$

이라는 명제이다. ZFC에서는 자연수와 실수의 크기 사이에 중간 기수가 없다는 진술과 동치이다.

명제 5.11 (부랄리포르티 역설) 모든 서수의 모임은 집합이 아니다.

증명. 모든 서수의 집합 O가 있다고 가정하자. 서수 집합의 합집합도 서수라는 성질에 의해 $\alpha=\bigcup O$가 서수이다. 그러면 $\alpha+1\in O$이고, 따라서 $\alpha+1\subseteq\bigcup O=\alpha$이다. 그런데 $\alpha\in\alpha+1$이므로 $\alpha\in\alpha$가 되어 정렬의 비반사성에 모순이다. □

역사 (부랄리포르티 역설). 이 모순은 체사레 부랄리포르티(Cesare Burali-Forti)가 1897년에 처음 지적했으며, 러셀 역설(1901년경)보다 먼저 집합과 진클래스를 구별할 필요성을 보여 준 사례이다. 서수의 크기 자체를 한꺼번에 모두 모으는 데에도 이 구별이 필요하다.

5.8 해설이 있는 연습문제

연습문제 5.12 유한한 이진 문자열 전체가 가산이지만 무한 이진 수열 전체는 비가산인 이유를 비교하라.

풀이. 길이 n인 문자열은 2^n개이고, 길이순으로 나열한 뒤 각 길이 안에서 사전식으로 나열하면 전체가 가산이다. 무한 수열은 어느 유한 길이 목록에도 속하지 않는다. 자연수로 나열했다고 가정하면 n번째 수열의 n번째 자리와 다른 값을 택한 수열이 모든 목록 원소와 달라져 모순이다.

연습문제 5.13 가산 집합의 부분집합이 가산임을 선택공리 없이 설명하라.

풀이. 원래 집합을 $\mathbb{N}$에 단사로 보내면 부분집합도 $\mathbb{N}$에 단사로 보내진다. 그 상이 유한이면 유한이고, 무한이면 최소 원소를 차례로 고르는 재귀로 증가 나열을 만든다. 여기서 매 단계 최소 원소가 유일하므로 임의의 선택을 요구하지 않는다.

> **연습문제 5.14** $\mathbb{N} \cup \{*\}$와 $\mathbb{N}$ 사이의 전단사를 쓰고, 이것이 $\omega + 1$과 ω의 순서 동형이 되지 않는 이유를 설명하라.

풀이. $f(*) = 0$, $f(n) = n + 1$로 둔다. 이는 전단사이다. 하지만 $*$를 마지막 원소로 둔 순서에서는 모든 $n < *$인데, 상에서는 모든 $f(n) > f(*)$이다. 따라서 순서를 보존하지 않는다. 가장 큰 원소의 존재 여부만 비교해도 순서 동형이 불가능함을 알 수 있다.

> **연습문제 5.15** $A \subseteq \mathbb{N}$의 삼진 부호화에서 첫 차이가 $k = 2$이면 두 실숫값 사이의 거리에 어떤 하한을 얻는가.

풀이. 명제 5.7의 증명에서 보였듯이 거리는 적어도 $1/3^3 = 1/27$이다. 첫 번째로 다른 자리의 차이는 $2/27$이고, 뒤의 모든 자리로 상쇄할 수 있는 양은 최대 $1/27$이다. 따라서 중복 표현 때문에 단사성이 깨지지 않는다.

> **연습문제 5.16** "무한 집합의 진부분집합은 항상 더 작다"에 반례를 들고, 유한 집합과의 차이를 설명하라.

풀이. 짝수 자연수 집합 $2\mathbb{N}$은 $\mathbb{N}$의 진부분집합이지만 $n \mapsto 2n$으로 전단사이다. 유한 집합에서는 비둘기집 원리에 의해 진부분집합과 원래 집합 사이에 전단사가 없다. 유한 직관을 무한 기수에 그대로 적용하면 안 된다.

> **연습문제 5.17** "$\omega + 1 > \omega$이므로 $|\omega + 1| > |\omega|$이다"라는 추론을 고쳐라.

풀이. 앞의 부등식은 서수의 순서 비교이고 뒤의 부등식은 기수 비교이다. 실제로 두 기수는 같다. 서로 다른 정렬 순서형이 같은 원소 수를 가질 수 있으므로, 서수의 엄격한 증가가 항상 기수의 엄격한 증가를 뜻하지는 않는다.

> **연습문제 5.18** 나열 e_n들이 이미 주어진 가산 집합족과, 각 집합의 가산성만 알려진 집합족을 증명에서 구별해야 하는 이유를 쓰라.

풀이. 전자는 $(n, k) \mapsto e_n(k)$라는 하나의 전사를 곧바로 쓸 수 있다. 후자는 모든 n에 대응하는 나열을 동시에 모을 수 있는지 먼저 확인해야 한다. ZFC에서는 선택공리가 이를 보장하지만, ZF만의 증명이라고 주장하려면 해당 선택을 없애거나 필요한 약한 선택 가정을 명시해야 한다.

제 6 장

선택공리, 독립성, 불완전성의 정확한 범위

개요 이 장은 집합론과 증명론에서 가장 자주 오해되는 세 낱말—선택, 독립성, 불완전성—을 정확한 진술로 정리한다. 먼저 선택공리를 유한한 경우의 당연한 선택과 구별하고, 정렬 정리·초른 보조정리와의 동치 관계, 전사 함수의 오른쪽 역함수 존재와의 동치 관계를 보인다. 이어서 일관성·구문적 완전성·건전성·의미론적 완전성을 서로 다른 개념으로 구분하고, 한 문장이 "어떤 이론으로부터" 독립이라는 말의 정확한 뜻과 그 증명법(두 모형을 만드는 방법)을 제시한다. 마지막으로 괴델–로서의 제1·제2 불완전성 정리를 계산 가능하게 열거되는 공리계라는 조건과 함께 진술하고, 정리가 실제로 말하는 바와 흔히 오해되는 바를 구별한다. 선행 지식: 공리에서의 형식적 증명($\vdash$)과 모형에서의 참($\models$)의 구별, 가산성(제5권 제5장), ZF와 ZFC의 공리 체계(제5권 제2장). 이 장은 고급 독립성 정리와 불완전성 정리의 정확한 진술과 사용 범위를 소개할 뿐이며, 강제법이나 산술화의 전체 증명은 전개하지 않는다.

6.1 유한한 선택과 무한한 동시 선택

공집합 아닌 집합 A가 존재한다면 증명에서 $a \in A$ 하나를 잡을 수 있다. 이는 존재 양화사의 사용이다. 서로 다른 집합마다 원소 하나를 고른 결과를 동시에 하나의 함수로 모으는 일은 이보다 더 강한 요구가 될 수 있다.

명제 6.1 (유한 선택은 ZF에서 가능하다) 공집합 아닌 집합의 유한 목록 $A_0, \dots, A_{n-1}$에 대해 $a_i \in A_i$인 유한열 $(a_0, \dots, a_{n-1})$이 존재한다.

증명. n에 대해 귀납한다. $n = 0$이면 빈 함수가 조건을 만족한다. 길이 n인 선택 함수가 존재한다고 하자. $A_n \neq \emptyset$이므로 $a_n \in A_n$ 하나를 잡고 기존 함수에 쌍 (n, a_n)을 추가하면 길이 $n+1$인 선택 함수가 된다. 추가되는 정의역 원소가 새 원소이므로 함수 조건이 보존된다. $\square$

이 귀납법은 각 유한 길이마다 선택 함수가 존재함을 보인다. 하지만 그 선택 함수들이 서로 호환되도록 무한히 한 줄로 이어진다는 결론까지 자동으로 주지는 않는다. "모든 n에 대해 길이 n의 자료가 존재한다"와 "모든 길이의 자료를 동시에 일관되게 가진 무한 대상이 존재한다"는 서로 다른 문장이다.

예제 6.2 (최소 원소가 있으면 선택을 정의할 수 있다) $\mathcal{A}$가 공집합 아닌 자연수 부분집합들의 집합족이면 $f(A) = \min A$는 명시적인 선택 함수이다. 반면 공집합 아닌 실수 부분집합마다 최솟값을 택하겠다는 규칙은 작동하지 않는다. 열린 구간 $(0, 1)$에는 최솟값이 없다. 정의하려는 선택 규칙이 실제로 모든 입력에 값을 주는지 먼저 확인해야 한다.

6.2 선택공리의 동치 형식을 사용할 때

선택공리(*axiom of choice*, AC)는 정렬 정리 및 초른 보조정리와 ZF 위에서 동치이다. **정렬 정리**는 모든 집합에 어떤 정렬 순서를 줄 수 있다는 뜻이다. 그 순서가 원래의 크기 순서나 자연스러운 순서와 같다는 뜻은 아니다. **초른 보조정리**는 공집합 아닌 부분순서집합에서 모든 사슬에 상계가 있으면 극대 원소가 존재한다는 진술이다. 이 동치들의 전체 증명은 고급 집합론에서 다룬다.

선형대수(제7권 제3장)에서 선형독립 집합을 기저로 확장하는 일은 유한차원에서는 소거법으로 끝나지만, 일반 벡터공간에서는 초른 보조정리를 가정하여 논증할 수 있다. 그 증명은 기저 존재를 정당화하지만 구체적 벡터 공간의 기저를 계산하는 알고리즘을 자동으로 주지는 않는다. 존재와 계산 가능성은 서로 다른 성질이다. 유한차원 공간에서 소거법으로 기저를 구하는 상황과 일반 벡터 공간에서 선택을 사용하여 존재를 보이는 상황을 구별해야 한다.

> **명제 6.3 (전사 함수의 오른쪽 역함수와 선택)** 모든 전사 함수에 오른쪽 역함수가 존재한다는 원리는 ZF 위에서 선택공리와 동치이다.

논증의 구조. 전사 $p : X \to Y$의 각 섬유 $p^{-1}(\{y\})$는 공집합이 아니다. 선택공리로 각 섬유에서 $s(y)$를 고르면 $p \circ s = \mathrm{id}_Y$이다.

반대로 집합족 $(A_i)_{i \in I}$에 대해 서로소 합집합

$$X = \{(i, a) : i \in I,\ a \in A_i\}$$

에서 지표로 가는 사영 $p(i,a) = i$를 사용한다. 각 $A_i \neq \emptyset$이면 p가 전사이고, 오른쪽 역함수 $s(i) = (i, a_i)$가 선택 함수 $i \mapsto a_i$를 준다. 원소가 겹치는 집합족에서도 지표를 쌍에 넣었으므로 어떤 집합에서 선택했는지 정보가 보존된다. $\square$

선택공리를 쓰는 증명에서는 어떤 집합족에서 무엇을 고르는지 적어 두면 가정의 사용이 명확해진다. 모든 존재 양화사를 선택공리로 설명하는 것도, 모든 무한 선택을 당연하다고 생략하는 것도 피해야 한다.

6.3 일관성, 완전성, 건전성의 서로 다른 대상

이론 T는 주어진 언어의 문장들의 집합으로 생각한다. $T \vdash \varphi$는 T의 공리를 전제로 하는 유한한 형식적 증명이 존재한다는 뜻이다. $M \models T$는 구조 M이 T의 모든 공리를 만족한다는 뜻이다.

> **정의 6.4 (일관성과 구문적 완전성)** 고전논리에서 이론 T가 **일관적**(*consistent*)이라는 것은 $T \nvdash \bot$이라는 뜻이다. 동치로 어떤 문장과 그 부정을 동시에 증명하지 않는다. T가 **구문적으로 완전**하다는 것은 그 언어의 모든 문장 φ에 대해 $T \vdash \varphi$ 또는 $T \vdash \neg\varphi$가 성립한다는 뜻이다.

논리 체계의 **건전성**(*soundness*)은

$$T \vdash \varphi \implies T \models \varphi$$

이고, 논리 체계의 **의미론적 완전성**(*semantic completeness*)은 반대 방향

$$T \models \varphi \implies T \vdash \varphi$$

이다. 여기서 $T \models \varphi$는 T의 모든 모형에서 φ가 참이라는 뜻이다. 일차논리의 완전성 정리와 산술 이론의 불완전성 정리는 "완전성"이라는 단어를 서로 다른 대상에 사용한다.

> **예제 6.5** 선형순서의 공리만으로는 최소 원소가 존재하는지 결정하지 못한다. 자연수의 통상 순서는 최소 원소를 가지고 정수의 통상 순서는 가지지 않으며, 둘 다 선형순서 공리의 모형이다. 따라서 공리에서 최소 원소의 존재도 부재도 증명되지 않는다. 하지만 이것은 일차논리의 증명 규칙이 의미론적으로 불완전하다는 뜻이 아니다. 공리 자체가 허용한 모형들이 해당 성질에 관해 서로 다르다는 뜻이다.

일관성과 특정한 의도된 구조에서의 참도 다르다. 산술의 의도된 구조는 통상적인 자연수 구조 $\mathbb{N}$이다. 이론이 일관적이라는 가정만으로 그 이론의 모든 정리가 표준 자연수에서 참이라고 결론 내릴 수는 없다. 표준 구조에 대한 건전성은 일관성보다 강한 요구이다.

6.4 독립성은 기준 이론을 함께 말해야 한다

> **정의 6.6 (독립성)** 문장 φ가 이론 T로부터 **독립**이라는 것은
>
> $$T \nvdash \varphi \quad \text{그리고} \quad T \nvdash \neg\varphi$$
>
> 라는 뜻이다. 따라서 "φ는 독립이다"라는 말에는 어느 이론을 기준으로 하는지 반드시 포함되어야 한다.

> **명제 6.7** 고전논리에서 φ가 T로부터 독립일 필요충분조건은 $T \cup \{\varphi\}$와 $T \cup \{\neg\varphi\}$가 둘 다 일관적인 것이다.

증명. $T \cup \{\varphi\}$가 모순을 증명하면 연역 정리에 의해 $T \vdash \varphi \to \bot$, 즉 $T \vdash \neg\varphi$이다. 반대로 $T \vdash \neg\varphi$이면 φ를 추가했을 때 모순이 생긴다. 따라서 첫 확장의 일관성은 $T \nvdash \neg\varphi$와 동치이다.

$\neg\varphi$를 추가한 경우에도 같은 논증을 적용한다. 이 경우 확장의 비일관성은 $T \vdash \neg\neg\varphi$와 동치이며, 고전논리의 이중부정 제거로 $T \vdash \varphi$와 동치이다. 두 조건을 함께 모으면 원하는 결과를 얻는다. $\square$

독립성을 보이는 대표적인 방법은 서로 반대되는 문장을 만족하는 두 모형을 만드는 것이다. $M \models T + \varphi$이고 $N \models T + \neg\varphi$이면 건전성에 의해 T가 어느 한쪽을 증명할 수 없다. 단, 집합론처럼 강한 이론의 모형을 만들 때는 그 모형의 존재를 무엇에서 출발해 보장했는지가 핵심이 된다.

> **예제 6.8 (단순한 독립성의 완전한 증명)** 언어가 $<$ 하나인 선형순서 이론 L을 생각하고
>
> $$\mu = \exists x \, \forall y \, \neg(y < x)$$
>
> 라 하자. $(\mathbb{N}, <) \models L + \mu$이고 $(\mathbb{Z}, <) \models L + \neg\mu$이다. $L \vdash \mu$라면 정수 모형에서도 μ가 참이어야 하므로 모순이고, $L \vdash \neg\mu$라면 자연수 모형에서 모순이다. 따라서 μ는 L로부터 독립이다. 이 사례는 괴델의 불완전성 정리를 사용하지 않는다.

6.5 상대적 일관성과 연속체 가설

$\mathrm{Con}(T)$는 우선 바깥 수학에서 "이론 T는 일관적이다"라는 메타수학적 진술을 나타내는 표기로 사용하자. 상대적 일관성 정리는 보통

$$\mathrm{Con}(T) \implies \mathrm{Con}(S)$$

꼴이다. 이는 T의 일관성을 전제로 S의 일관성을 비교하는 것이며, 전제를 없애고 두 이론의 절대적 일관성이 증명되었다는 뜻은 아니다.

고전적인 결과에 따르면 ZFC가 일관적이면 ZFC에 CH를 추가한 이론과 ¬CH를 추가한 이론이 모두 일관적이다. 전자는 괴델의 구성 가능성 방법(1938–1940년), 후자는 코언의 강제법(1963년)과 관련된다. 따라서 ZFC가 일관적이라는 전제 아래 CH는 ZFC로부터 독립이다. 이 권에서는 이 결과의 정확한 의미를 사용하며 두 방법의 기술적 증명을 수행하지 않는다.

독립성은 CH와 그 부정이 하나의 같은 모형에서 동시에 참이라는 말이 아니다. 고전논리의 각 모형에서는 해당 문장에 하나의 진릿값이 정해진다. 기준 공리만으로 가능한 모형들 전체에 공통인 한쪽 진릿값을 강제하지 못한다는 뜻이다. 더 강한 공리를 추가해 질문을 다시 연구할 수 있지만, 그 추가 공리의 정당성과 일관성 강도는 별도의 문제이다.

흔한 오류. 독립성이 증명된 명제와 아직 증명이나 반례를 찾지 못한 명제를 구별해야 한다. "현재 모른다"는 연구 상태이고, "T에서 독립이다"는 특정 증명 체계에 관한 수학적 결론이다.

6.6 효과적으로 공리화된다는 조건

불완전성 정리에서 이론의 공리를 효과적으로 다룰 수 있다는 조건은 중요하다. 여기서는 공리들의 괴델 번호를 알고리즘으로 차례로 나열할 수 있는 이론을 **계산 가능하게 열거되는 공리계**를 가진 이론이라고 부른다. 공리 집합이 유한할 필요는 없다. ZFC의 공리꼴처럼 무한하지만 문법적으로 생성할 수 있는 목록도 이에 해당한다.

이런 공리계에서 정리들도 알고리즘으로 열거할 수 있다. 점점 더 많은 공리를 읽고, 유한한 길이의 모든 가능한 증명 시도를 점점 늘리며 검사하면 된다. 열거 가능한 공리에 대한 사용 근거를 증명 자료에 함께 기록하는 식으로 형식화할 수 있다. 이 사실은 "주어진 문장이 정리인지 항상 유한 시간 안에 판정할 수 있다"는 것과 다르다. 증명이 없으면 단순 탐색은 끝나지 않을 수 있다.

> **명제 6.9** 계산 가능하게 열거되는 공리계를 가진 일관적이고 구문적으로 완전한 이론의 정리 여부는 알고리즘으로 판정할 수 있다.

증명. 입력 문장 φ에 대해 T의 정리들을 차례로 열거하면서 φ와 $\neg\varphi$가 나타나는지 동시에 확인한다. 완전성에 의해 둘 중 하나는 언젠가 등장하므로 절차가 멈춘다. 일관성에 의해 둘 다 정리일 수 없으므로, φ가 먼저 나오면 정리라고, $\neg\varphi$가 나오면 정리가 아니라고 올바르게 답한다. □

전제 가운데 완전성을 빼면 이 절차는 두 문장을 모두 기다리다가 끝나지 않을 수 있다. 일관성을 빼면 부정의 증명을 발견했다고 원래 문장이 증명되지 않는다고 판단할 수 없다. 정리의 조건은 알고리즘의 각 단계가 왜 작동하는지와 직접 연결된다.

6.7 제1 불완전성 정리: 충분조건을 분명히 적기

다음은 이해하기 쉬운 충분조건을 사용한 진술이다. 가능한 가장 약한 가정까지 제시하려는 것은 아니다. PA는 덧셈과 곱셈을 포함하는 일차 페아노 산술을 뜻한다.

> **정리 6.10 (괴델–로서 불완전성 정리의 한 형태)** 산술 언어의 이론 T가 PA를 포함하고, 계산 가능하게 열거되는 공리계를 가지며, 일관적이라고 하자. 그러면 어떤 산술 문장 ρ에 대해
>
> $$T \nvdash \rho \quad \text{그리고} \quad T \nvdash \neg\rho$$
>
> 가 성립한다.

이 결론은 하나의 문장과 그 부정을 동시에 증명한다는 뜻이 아니다. 오히려 일관성을 유지하는 대신 모든 문장을 공리로 결정할 수 없다는 뜻이다. 고정된 이론의 정리 집합에는 포함되지 않는 문장이 남는다. 그런 문장을 새 공리로 추가하더라도 새로운 이론이 같은 효과성과 일관성 조건을 만족하면 다시 같은 형태의 한계가 적용된다.

방법 (증명의 개요). 증명의 큰 흐름은 유한한 공식과 증명을 자연수로 부호화하고, 그 부호에 관한 관계를 산술 안에서 표현한 다음, 자신의 증명 가능성과 연결되는 문장을 만드는 것이다. 로서의 개선은 보통의 일관성만으로 양쪽의 비증명성을 얻도록 논증을 정교하게 만든다. “이 문장은 거짓이다”라는 자연어 역설을 단순히 옮겨 적는 것이 전체 증명은 아니다. 치환의 부호화, 표현 가능성, 대각선 보조정리가 실제로 필요하다.

이 정리로부터 모든 수학 명제가 증명 불가능하다는 결론은 나오지 않는다. 대부분의 익숙한 정리는 공리에서 증명되며, 이 정리는 어떤 문장들은 남는다는 존재 주장이다. 또한 특정한 미해결 문제가 곧바로 해당 이론에서 독립이라는 결론도 나오지 않는다. 그 문제의 독립성에는 별도 논증이 필요하다.

6.8 제2 불완전성 정리와 일관성 문장의 표준화

이제 증명 관계를 산술 안에 표현한 표준 술어를 Prov_T라고 하자. $\ulcorner \varphi \urcorner$는 문장 φ의 괴델 번호를 나타내는 산술의 수 표기이다. 통상의 일관성 문장은

$$\mathrm{Con}_T := \neg\,\mathrm{Prov}_T(\ulcorner 0 = 1 \urcorner)$$

이다. 이는 “$0 = 1$의 T-증명은 없다”를 산술 문장으로 표현한다.

> **정리 6.11 (제2 불완전성 정리의 표준적 형태)** T가 일관적이고 계산 가능하게 열거되는 공리계를 가진 PA의 확장이라고 하자. 통상의 산술화에 따른 증명 가능성 술어와 일관성 문장을 사용하면
>
> $$T \nvdash \mathrm{Con}_T$$
>
> 이다.

여기서 “통상의”라는 조건은 수사적 장식이 아니다. 표준 증명 가능성 술어는 증명의 결합과 자기 증명 가능성에 관한 도출 조건을 만족한다. 단지 바깥에서 같은 대상을 가리킨다는 이유만

으로 임의의 다른 공식에 제2 정리의 결론을 옮기면 안 된다. 또한 정리의 결론은 위의 비증명성 한 방향이다. 일관성만을 가정한 이 진술에서 $T \nvdash \neg \mathrm{Con}_T$까지 자동으로 붙이면 안 된다.

주의. 더 강한 이론 S가 약한 이론 T의 일관성을 증명하는 것은 이 정리와 양립한다. 제2 정리는 모든 일관성 증명을 금지하는 것이 아니라, 정해진 효과적 이론이 자기 표준 일관성 문장을 내부에서 증명하는 데 한계를 준다는 것이다. 외부의 논증이 어느 이론에서 형식화되는지까지 구별해야 한다.

6.9 가정을 빼면 어떤 다른 사례가 가능한가

표준 자연수에서 참인 모든 산술 문장의 집합 $\mathrm{Th}(\mathbb{N})$을 생각하자. 이것은 일관적이고 구문적으로 완전하다. 그러나 계산 가능하게 열거되는 공리계로 모두 제시할 수 없다. 만일 가능하다면 제1 불완전성 정리의 조건을 만족하면서 완전하여 모순이 되기 때문이다. 참인 문장 전체를 그냥 공리로 택하겠다는 제안은 효과성 조건을 포기한다.

유한한 명제 변수에 대한 진리표 판정은 모든 입력 공식에 대해 끝나는 알고리즘이다. 이것은 불완전성 정리와 충돌하지 않는다. 충분한 자연수 산술을 표현하는 이론이라는 조건이 빠져 있기 때문이다. 한편 비일관적인 고전 이론은 폭발 원리로 모든 문장을 증명하므로 구문적으로는 완전하지만, 일관성 조건을 만족하지 않는다.

이런 사례들은 정리의 가정을 확인하는 실용적인 검사 도구이다. 어떤 체계에 불완전성을 적용하려면 그 체계가 충분한 산술을 포함하는지, 효과적으로 공리화되는지, 일관성을 어떤 전제로 놓는지 각각 확인해야 한다. “규칙이 있다” 거나 “매우 복잡하다” 는 말만으로 적용할 수 없다.

6.10 모형의 안과 밖을 혼동하지 않기

집합론의 모형 M이 어떤 집합을 가산이라고 판단한다는 것은 M 안에 적절한 전단사가 존재한다는 뜻이다. 바깥에서 M의 원소들을 나열하는 함수가 존재한다는 사실과는 다를 수 있다. 특히 바깥에서 가산인 모형 안에서도 그 모형이 실수 집합으로 보는 대상은 내부적으로 비가산일 수 있다. 바깥의 나열 함수가 모형 안에 들어 있지 않으면 내부의 가산성을 증명하는 함수가 되지 못한다.

참고 (스콜렘 역설). 이 현상을 **스콜렘 역설**(*Skolem's paradox*)이라고 부른다. 1922년 토랄프 스콜렘(Thoralf Skolem)은 뢰벤하임–스콜렘 정리에 의해 ZFC에 가산 모형이 있다면, 그 모형 안에서도 “실수 전체는 비가산이다” 라는 문장이 참으로 판정된다는 사실을 지적했다. 역설이라는 이름과 달리 논리적 모순은 아니다. 가산성이라는 술어를 모형 안에서 양화되는 함수들로 해석하는지, 모형 바깥의 함수까지 포함해 해석하는지가 다르기 때문이다.

이 설명은 가산 모형이 언제나 존재한다고 아무 전제 없이 선언하는 것이 아니다. 관련 일차 논리 정리의 가정과 출발 모형의 존재를 먼저 확인해야 한다. 핵심은 양화하는 함수들의 범위가 내부와 외부에서 달라질 수 있다는 점이다. 같은 단어 “모든 부분집합” , “모든 증명” , “가산” 을 사용하더라도 어느 구조에서 해석하는지 명시해야 한다.

6.11 해설이 있는 연습문제

연습문제 6.12 공집합 아닌 정수 부분집합들의 집합족에서 “최소 정수를 고르자”는 규칙이 선택 함수가 되지 못하는 반례와, 이를 고치는 명시적 규칙을 제시하라.

풀이. $\mathbb{Z}$ 자체에는 최소 정수가 없다. 대신 $0, 1, -1, 2, -2, \dots$ 라는 고정된 나열에서 처음 나타나는 원소를 고르면 된다. 각 부분집합의 등장 지표들은 공집합 아닌 자연수 집합이므로 최소 지표가 유일하다. 원래 크기 순서의 최솟값과 고정한 정렬 순서의 최솟값은 다르다.

연습문제 6.13 이론 T에 모형이 하나 있다는 사실에서 일관성을 얻는 논증을 쓰라.

풀이. $M \models T$라고 하자. 만일 $T \vdash \bot$이면 건전성에 의해 $M \models \bot$이어야 한다. 모순 문장은 어떤 구조에서도 참이 아니므로 불가능하다. 이 논증은 모형의 존재를 정당화하는 바깥 수학과 논리의 건전성을 사용한다.

연습문제 6.14 CH의 독립성을 “ZFC가 CH도 증명하고 그 부정도 증명한다”라고 설명한 문장을 바로잡아라.

풀이. 일관성을 가정하면 ZFC는 CH도 그 부정도 증명하지 못한다는 뜻이다. 양쪽을 모두 증명한다면 독립성이 아니라 비일관성이 된다. 서로 다른 확장 이론 또는 모형에서 반대되는 문장이 성립할 수 있다는 설명과, 하나의 이론이 양쪽을 증명한다는 설명은 정반대이다.

연습문제 6.15 일차논리의 완전성 정리와 PA의 불완전성이 모순되지 않는 이유를 한 문장씩 설명하라.

풀이. 전자는 PA의 모든 모형에서 참인 문장은 PA로부터 형식적으로 증명된다는 뜻이다. 후자는 PA가 모든 산술 문장의 한쪽 진릿값을 결정하지 못한다는 뜻이다. 결정되지 않는 문장은 PA의 서로 다른 모형에서 다른 진릿값을 가질 수 있으므로 두 진술은 양립한다.

연습문제 6.16 T의 정리를 계속 열거했는데 지금까지 φ가 나오지 않았다는 사실만으로 $T \nvdash \varphi$를 결론 내릴 수 있는가.

풀이. 없다. 더 늦게 등장할 수 있다. 유한 시간 동안의 탐색 실패는 전체 증명의 부재와 다르다. 판정 알고리즘을 주장하려면 모든 입력에서 멈춘다는 논증이 필요하며, 앞의 명제 6.9에서는 일관성과 완전성이 그 논증을 제공했다.

연습문제 6.17 제2 불완전성 정리가 강한 이론에서 약한 이론의 일관성을 증명하는 것을 금지하는지 설명하라.

풀이. 금지하지 않는다. 정리의 대상은 주어진 이론의 자기 일관성 문장이다. $S \vdash \mathrm{Con}_T$는 $T \vdash \mathrm{Con}_T$와 다른 주장이다. 대신 S 자체의 일관성을 무엇으로 뒷받침하는지는 다시 별도의 문제로 남는다.

연습문제 6.18 괴델–로서 정리를 적용하면서 “일관적이다” 대신 “공리가 유한 개이다”만 적어도 되는지 판단하라.

풀이. 안 된다. 유한 공리계는 효과적으로 열거된다는 조건을 충족하지만 일관성을 보장하지 않는다. 예를 들어 φ와 $\neg\varphi$를 함께 공리로 두면 유한하더라도 비일관적이다. 효과성과 일관성은 서로 다른 조건이다.

> **연습문제 6.19** 어떤 명제가 아직 해결되지 않았다는 기사만으로 ZFC에서 독립이라고 표기하면 안 되는 이유를 설명하라.

풀이. 미해결은 현재 알려진 증명과 반례의 상태를 말한다. 독립성은 특정 이론에서 어느 쪽도 증명되지 않는다는 메타수학적 정리이다. 이를 주장하려면 모형 구성이나 상대적 일관성 증명 등 별도 근거가 필요하다. 연구 상태를 갱신할 때에는 발표 시점과 검증 여부도 확인해야 한다.

정확한 정리 조건을 확인할 자료

이 원고의 설명과 예제는 독립적으로 작성했다. 공리적 집합론과 CH의 상대적 일관성 진술은 Open Logic Project의 *Set Theory: An Open Introduction*에서, 불완전성 정리의 도출 조건은 *Incompleteness and Computability* 제5장에서 더 자세히 확인할 수 있다. 두 자료는 전체 증명으로 넘어가기 위한 참고문헌이며, 이 장이 강제법이나 불완전성의 기술적 증명 전체를 수행했다는 뜻은 아니다.

- https://st.openlogicproject.org/settheory-screen.pdf
- https://ic.openlogicproject.org/ic-screen.pdf

다음 연결. 이후의 기초론에서는 초한 귀납과 재귀, 순서수 산술, 모형론, 계산 가능성, 증명론을 따로 전개한다. 이 묶음에서 사용한 고급 결과의 정확한 전제를 유지하면서 증명의 내부 구조를 확장한다.

제 7 권

선형대수

제7권은 벡터와 행렬로 여러 양 사이의 일차적 관계를 분석하는 선형대수를 다룬다. 제1장은 연립일차방정식을 Gauss 소거법으로 푸는 계산에서 출발하고, 제2–4장은 벡터공간과 부분공간, 선형독립·기저·차원, 선형사상의 핵과 상 및 차원 정리로 이 계산의 구조를 추상화한다. 제5장은 기저를 고정하여 선형사상을 행렬로 나타내는 방법과 기저변환을, 제6장은 부피와 가역성을 판정하는 행렬식을 다룬다. 제7–8장은 고유값과 대각화, 내적·직교·최소제곱과 스펙트럼 정리, 특이값 분해를 차례로 증명하여 이후 해석학과 확률·통계의 여러 권에서 쓰는 도구를 완성한다.

제 1 장

연립일차방정식과 소거법

개요 선형대수(*linear algebra*)는 여러 양 사이의 일차적 관계를 벡터와 행렬로 정리하고, 해집합을 바꾸지 않는 조직적인 연산으로 분석하는 수학의 한 분야이다. 이 장은 연립일차방정식을 계수행렬과 상수항으로 묶어 $Ax = b$ 꼴로 표현하고, 기본 행 연산으로 확대행렬을 행 사다리꼴로 바꾸는 Gauss 소거법을 세운다. 이어서 피벗과 자유변수를 통해 해의 존재성과 자유도를 판정하는 일반 정리(정리 1.13)를 증명하고, 정확한 산술과 부동소수점 계산의 차이를 짚는다. 이 권에서는 특별한 언급이 없는 한 실수체 $\mathbb{R}$ 또는 복소수체 $\mathbb{C}$ 위에서 계산하며, 두 경우에 공통으로 성립하는 명제는 체(*field*) $\mathbb{F}$라는 기호로 서술한다. 선행 지식: 일차방정식과 분수 계산, 함수의 기본 개념이며, 행렬과 벡터는 이 장에서 처음 정의한다.

주의 (체 위에서의 나눗셈과 정수 계산). 체 $\mathbb{F}$에서는 0이 아닌 모든 원소로 나눌 수 있다. 그러나 정수만을 허용하는 문제에서는 0이 아닌 정수로 나눈 결과가 정수가 아닐 수 있으므로, 체 위에서 성립하는 계산을 그대로 정수 계산으로 해석해서는 안 된다.

1.1 일차방정식과 연립방정식

정의 1.1 (일차방정식과 해) 미지수 $x_1, \dots, x_n$에 관한 **일차방정식**(*linear equation*)은

$$a_1 x_1 + \cdots + a_n x_n = b \tag{1.1}$$

형태의 식이다. 계수 a_j와 상수항 b는 미리 주어져 있으며 미지수에 의존하지 않는다. 여러 일차방정식에 동시에 대입하여 모두 참으로 만드는 순서 있는 n개의 수를 그 연립방정식의 **해**(*solution*)라고 한다.

$x + 2y = 3$은 일차방정식이지만 $xy = 3$, $x^2 + y = 1$, $\sin x + y = 0$은 그렇지 않다. 반면 어떤 고정된 각도 θ에 대해 $(\cos\theta)x + y = 1$은 x, y에 관한 일차방정식이다. 무엇이 미지수이고 무엇이 매개변수인지 지정해야 일차성을 판단할 수 있다.

예제 1.2 (두 직선의 교점)

$$x + y = 5, \qquad 2x - y = 1$$

을 더하면 $3x = 6$이므로 $x = 2$, $y = 3$이다. 두 식에 다시 대입하면 $2 + 3 = 5$, $4 - 3 = 1$로 확인된다. 계산에서 얻은 값을 원래 식에 대입하는 검산은 가장 직접적인 오류 탐지 방법이다.

식이 많다고 항상 해가 하나로 정해지지는 않는다. $x + y = 5$와 $2x + 2y = 10$은 같은 조건을 반복해서 말한다. 반대로 $x + y = 5$와 $2x + 2y = 11$은 서로 모순된다. 방정식의 개수보다 독립적인 제약이 몇 개 있는지가 중요하며, 소거법은 이 차이를 드러낸다.

1.2 행렬로 계수를 정리하기

m개의 식과 n개의 미지수를 가진 계는

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1n}x_n &= b_1, \\ &\vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n &= b_m \end{aligned} \tag{1.2}$$

이다. 계수들을 m행 n열 **행렬** $A = (a_{ij})$로 모으면 $Ax = b$라고 쓸 수 있다. 여기서 x는 $n \times 1$, b는 $m \times 1$ **열벡터**이며,

$$(Ax)_i = \sum_{j=1}^{n} a_{ij} x_j \tag{1.3}$$

로 정의한다. 행은 방정식, 열은 각 미지수의 계수에 해당한다.

정의 1.3 (확대행렬) 계수행렬 A의 오른쪽에 상수항 열벡터 b를 붙인 $[A \mid b]$를 **확대행렬**(*augmented matrix*)이라고 한다. 세로선은 연산 기호가 아니라 계수와 상수항을 구분하는 표시다.

예제 1.4 (직사각형 행렬의 의미)

$$A = \begin{pmatrix} 1 & 2 & -1 \\ 0 & 1 & 3 \end{pmatrix}, \qquad x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

이면

$$Ax = \begin{pmatrix} x_1 + 2x_2 - x_3 \\ x_2 + 3x_3 \end{pmatrix}.$$

행렬이 정사각형일 필요는 없다. 이 행렬은 세 성분의 입력을 두 성분의 출력으로 바꾼다. 식의 수가 2이고 변수의 수가 3이라는 정보가 행렬의 모양에 들어 있다.

행렬의 크기를 먼저 쓰는 습관은 이후에도 유용하다. 행렬곱 AB에서는 A의 열 수와 B의 행 수가 맞아야 한다. 아직 정의하지 않은 역행렬을 모든 행렬에 대해 쓰거나, 직사각형 행렬에 정사각형의 공식을 적용하는 실수는 크기를 확인하면 상당수 피할 수 있다.

1.3 해를 보존하는 기본 행 연산

다음 연산을 **기본 행 연산**(*elementary row operation*)이라고 한다.

(1) 두 행을 서로 바꾼다.

(2) 한 행에 0이 아닌 상수를 곱한다.

(3) 한 행에 다른 행의 상수배를 더한다.

상수항을 포함한 확대행렬 전체에 연산해야 한다. 계수 쪽만 바꾸고 오른쪽 상수항을 그대로 두면 원래와 다른 방정식이 된다.

정리 1.5 (기본 행 연산과 해집합) 확대행렬에 기본 행 연산을 적용하면 연립일차방정식의 해집합은 변하지 않는다.

증명. 행 교환은 방정식의 순서만 바꾼다. 비영 상수배는 같은 상수의 역수로 되돌릴 수 있으므로 등식의 조건이 같다. 세 번째 연산에서 i번째 식에 c배의 j번째 식을 더했다고 하자. 원래 두 식을 만족하는 값은 새 식도 만족한다. 반대로 새 계에는 j번째 식이 남아 있으므로, 새 i번째 식에서 c배의 j번째 식을 빼면 원래 식을 얻는다. 따라서 양방향으로 해가 일치한다. □

주의 (허용되지 않는 연산). 0을 곱하는 연산을 허용하지 않는 이유도 위 증명에서 보인다. $x = 1$에 0을 곱하면 $0 = 0$이 되어 제약을 잃는다. 두 행을 더한 뒤 원래 두 행을 모두 없애는 것도 일반적인 기본 행 연산이 아니다. 한 행을 바꾸되 되돌리는 데 필요한 다른 행을 보존해야 한다.

예제 1.6 (한 단계의 소거)

$$\left[\begin{array}{cc|c} 1 & 1 & 5 \\ 2 & -1 & 1 \end{array}\right] \xrightarrow{R_2 \leftarrow R_2 - 2R_1} \left[\begin{array}{cc|c} 1 & 1 & 5 \\ 0 & -3 & -9 \end{array}\right].$$

둘째 행에서 $y = 3$을 얻고 첫째 행에서 $x = 2$를 얻는다. R_2는 둘째 행을 뜻한다. 이 표기는 어떤 식을 어떤 식으로 바꾸었는지 명확하게 기록한다.

1.4 Gauss 소거와 뒤에서부터 대입하기

정의 1.7 (행 사다리꼴과 피벗) 행렬이 **행 사다리꼴**(*row echelon form*)이라는 것은 영이 아닌 행이 영행보다 위에 있고, 각 행의 첫 비영 성분이 아래로 갈수록 오른쪽으로 이동하며, 그 성분 아래는 모두 0이라는 뜻이다. 각 행의 첫 비영 성분을 **선도성분** 또는 **피벗**(*pivot*)이라고 한다. 피벗을 모두 1로 만들고 그 위쪽 성분까지 0으로 만든 행 사다리꼴을 **기약 행 사다리꼴**(*reduced row echelon form*)이라고 한다.

Gauss 소거(*Gaussian elimination*)는 적절한 행 교환과 행 더하기로 행 사다리꼴을 만드는 절차다.

알고리즘 1.8 (Gauss 소거법) 확대행렬 $[A \mid b]$에 대하여 다음을 반복한다.

1단계. 아직 처리하지 않은 가장 왼쪽 열 가운데 영이 아닌 성분을 가진 행을 찾아 맨 위로 옮긴다(필요하면 행을 바꾼다).

2단계. 그 행의 선도성분을 피벗으로 삼아, 아래의 모든 행에서 피벗이 있는 열의 성분이 0이 되도록 피벗 행의 적당한 배수를 더한다.

3단계. 처리한 행과 열을 제외한 나머지 부분행렬에 대해 과정을 반복한다.

모든 행과 열을 처리하면 확대행렬은 행 사다리꼴이 된다. 이후 가장 아래 피벗 행부터 차례로 대입하는 **후진대입**(*back substitution*)으로 각 피벗 변수의 값을 얻는다.

예제 1.9 (세 변수의 완전한 계산)

$$\begin{cases} x + 2y - z = 2, \\ 2x + 5y + z = 15, \\ -x - y + 2z = 3 \end{cases}$$

의 확대행렬에서 둘째 행에 첫째 행의 -2배를 더하고, 셋째 행에 첫째 행을 더하면

$$\left[\begin{array}{ccc|c} 1 & 2 & -1 & 2 \\ 0 & 1 & 3 & 11 \\ 0 & 1 & 1 & 5 \end{array}\right]$$

가 된다. 이제 $R_3 \leftarrow R_3 - R_2$를 적용하면

$$\left[\begin{array}{ccc|c} 1 & 2 & -1 & 2 \\ 0 & 1 & 3 & 11 \\ 0 & 0 & -2 & -6 \end{array}\right].$$

마지막 식에서 $z = 3$, 그 위 식에서 $y = 11 - 9 = 2$, 첫 식에서 $x = 2 - 4 + 3 = 1$이다. 원래 식에 넣으면 왼쪽이 각각 $1 + 4 - 3 = 2$, $2 + 10 + 3 = 15$, $-1 - 2 + 6 = 3$이므로 검산된다.

기약 형태의 유일성은 행들이 만들어내는 선형 조건을 통해 이해할 수 있다. 피벗 위치는 독립적인 열이 처음 등장하는 위치를 기록하고, 피벗 열에 단위벡터가 놓이도록 정규화하면 각 피벗 변수의 식이 고정된다. 이 사실의 완전한 구조적 설명은 열공간과 행공간, 계수를 배운 뒤 다시 볼 수 있다(제7권 제3장). 실제 계산에서는 유일성을 이용하여 서로 다른 방법의 결과를 비교할 수 있다.

참고 (계산 과정과 최종 정보). 같은 행렬의 기약 행 사다리꼴은 유일하지만, 중간의 소거 순서와 (기약이 아닌) 행 사다리꼴은 여러 가지일 수 있다. 계산 과정의 차이와 최종 정보의 차이를 구분해야 한다.

1.5 피벗 변수와 자유변수

예제 1.10 (자유변수 하나가 만드는 해의 직선)

$$\left[\begin{array}{ccc|c} 1 & 2 & 1 & 4 \\ 0 & 1 & -1 & 1 \end{array}\right]$$

는 $x + 2y + z = 4$, $y - z = 1$을 나타낸다. 피벗이 없는 셋째 변수 z를 t로 두면

$$z = t, \qquad y = 1 + t, \qquad x = 2 - 3t.$$

따라서 모든 해는

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} + t \begin{pmatrix} -3 \\ 1 \\ 1 \end{pmatrix}, \qquad t \in \mathbb{F}$$

이다. 실수체에서는 공간 속 직선으로 해석할 수 있다.

자유변수(*free variable*)는 아무 값이나 골라도 된다는 뜻이지만, **피벗 변수**까지 마음대로 고를 수 있다는 뜻은 아니다. 자유변수의 값이 정해지면 피벗 변수는 남은 식으로 결정된다. 자유변수가 여러 개이면 각각 독립적인 매개변수를 사용한다.

상수항이 모두 0인 계를 **동차계**(*homogeneous system*)라고 하고, 그렇지 않은 계를 **비동차계**라고 한다. 동차계 $Ax = 0$은 항상 영벡터를 해로 가지며, 자유변수가 있으면 영벡터가 아닌 해도 있다. 비동차계 $Ax = b$는 해가 없을 수도 있다. 해 x_p를 하나 알고 있다면 모든 해가 x_p에 동차계의 해를 더한 형태라는 사실은 제7권 제2장에서 일반적으로 증명한다.

1.6 해가 없는 경우와 매개변수의 분기

예제 1.11 (모순을 나타내는 행)

$$x + y = 1, \qquad 2x + 2y = 3$$

에서 둘째 식에 첫째 식의 -2배를 더하면 $0 = 1$이다. 확대행렬에는 $[0\ \ 0 \mid 1]$이 나타난다. 미지수에 어떤 값을 넣어도 만족할 수 없으므로 해가 없다. 계수 부분만 보고 영행이라고 판단하면 이 모순을 놓친다.

예제 1.12 (매개변수가 있을 때 먼저 나누지 않기)

$$x + y = 1, \qquad 2x + \lambda y = \mu$$

를 소거하면 $(\lambda - 2)y = \mu - 2$이다. 따라서

$$\begin{aligned} &\lambda \neq 2 && y = (\mu - 2)/(\lambda - 2), \quad x = (\lambda - \mu)/(\lambda - 2), \\ &\lambda = 2,\ \mu = 2 && (x, y) = (1 - t, t), \quad t \in \mathbb{F}, \\ &\lambda = 2,\ \mu \neq 2 && \text{해 없음} \end{aligned}$$

으로 나뉜다.

흔한 오류 (나누기 전에 경우를 나누기). 예제 1.12에서 $\lambda - 2$로 바로 나누면 $\lambda = 2$인 두 경우를 놓친다. 매개변수가 들어간 계수로 나누기 전에는 그 계수가 0이 되는 경우를 먼저 따로 다루어야 한다.

실수 또는 복소수 위에서는 해의 수가 0개, 1개, 무한히 많은 경우 중 하나다. 해가 두 개 x, y 있고 $x \neq y$라면, 뒤에서 다룰 선형성으로 $x + t(y - x)$가 모든 t에 대해 해가 된다. 유한체에서는 자유변수의 선택지가 유한하므로 "무한히 많다"는 표현이 맞지 않는다. 예를 들어 q개 원소를 갖는 체에서 자유변수가 k개인 일관된 계의 해는 q^k개다.

1.7 해의 존재와 자유도의 판정

정리 1.13 (해의 존재성과 자유도) 체 $\mathbb{F}$ 위의 $m \times n$ 행렬 A를 소거했을 때, 확대행렬에 $[0 \cdots 0 \mid c]$ 이고 $c \neq 0$인 행이 나타나면 $Ax = b$는 해가 없다. 그런 행이 없고 계수 부분의 피벗 수가 r이면 자유변수는 $n - r$개다. 특히 모든 열에 피벗이 있으면 해는 하나다.

증명. 모순행이 있으면 어떤 대입도 해당 식을 만족시키지 못한다. 모순행이 없으면 피벗이 없는 변수들을 임의로 정한 후 마지막 피벗 식부터 역으로 대입하여 모든 피벗 변수를 결정할 수 있다. 피벗 열이 r개이므로 나머지 열은 $n - r$개다. 자유변수가 없을 때에는 선택할 매개변수가 없어서 해가 유일하다. $\square$

$m < n$인 동차계에는 피벗이 많아도 m개뿐이므로 자유변수가 적어도 하나 있다. 따라서 비자명한 해가 존재한다. 반면 $m > n$이어도 해가 없다고 단정할 수 없다. 많은 식이 서로 종속되거나 하나의 해에 모두 맞을 수 있다.

예제 1.14 (식이 변수보다 많아도 해가 존재하는 경우)

$$x - y = 0, \qquad x + y = 2, \qquad 2x + y = 3$$

은 $m = 3$, $n = 2$이다. 첫 식에서 $x = y$이고 둘째 식에 대입하면 $2x = 2$, 즉 $x = y = 1$이다. 셋째 식에 대입하면 $2 \cdot 1 + 1 = 3$이 성립하므로 세 식을 모두 만족하는 해 $(1, 1)$이 존재한다. 식이 변수보다 많다고 해서 자동으로 해가 없는 것은 아니다.

직사각형 행렬을 판단할 때는 개수만으로 단정하지 말고 피벗과 일관성을 함께 확인한다.

핵심 수식

$$Ax = b, \qquad [A \mid b] \tag{1.4}$$

확대행렬 $[A \mid b]$를 소거해 얻은 피벗 수를 r, 미지수의 수를 n이라 하면: $[0 \cdots 0 \mid c]$, $c \neq 0$ 꼴의 행이 있으면 해가 없다; 그런 행이 없고 $r = n$이면 해가 유일하다; $r < n$이면 자유변수가 $n - r$개이고 무한체 위에서는 해가 무한히 많다.

1.8 정확한 계산과 수치 계산

분수로 계산하면 대수적 동치가 정확히 유지된다. 컴퓨터의 부동소수점 연산에서는 반올림 오차가 생긴다. 특히 매우 작은 수를 피벗으로 사용하여 나누면 오차가 커질 수 있다. 수치 소거에서는 현재 열에서 크기가 큰 원소를 피벗으로 택하는 **부분 피벗팅**(*partial pivoting*)을 자주 사용한다.

예제 1.15 (작은 피벗의 위험을 보여 주는 계)

$$\varepsilon x + y = 1, \qquad x + y = 2$$

에서 첫 행의 ε으로 나누면 $1/\varepsilon$ 규모의 계수가 나타난다. 두 행을 먼저 바꾸면 첫 피벗은 1이 되어 불필요한 큰 중간값을 줄일 수 있다. 정확한 산술에서는 두 방법의 해가 같지만 유한 정밀도에서는 오차의 전파가 다를 수 있다.

대수적으로 0인 값과 수치적으로 작게 나온 값을 동일하게 취급하면 안 된다. 근사 데이터에서 어느 값이 사실상 0인지 판단하는 기준은 문제의 단위와 오차 크기에 달려 있다. 이 권의 손계산은 특별히 말하지 않으면 정확한 산술을 뜻하며, 수치적 안정성의 상세한 분석은 수치해석에서 이어 다룬다.

역사 (Gauss 소거법의 이름과 기원). 연립일차방정식을 행 연산으로 소거해 푸는 절차는 중국의 고전 수학서 『구장산술(九章算術)』에 이미 기록되어 있었다. C. F. Gauss는 19세기 초 소행성 Ceres의 궤도를 최소제곱법으로 계산하는 과정에서 이 절차를 사용하였고, "Gauss 소거법"이라는 이름은 이 계산에서 유래했다. 방법 자체는 Gauss보다 훨씬 앞서 알려져 있었다.

1.9 연습문제와 해설

연습문제 1.16 $x + 2y = 4$, $3x - y = 5$를 풀고 원래 식에 대입하여 검산하라.

풀이. 첫 식의 3배에서 둘째 식을 빼면 $7y = 7$이므로 $y = 1$, $x = 2$이다. 대입하면 $2 + 2 = 4$, $6 - 1 = 5$이다. 소거에서 어느 식을 어느 식으로 바꾸었는지 기록하면 부호 오류를 줄일 수 있다.

연습문제 1.17 $x + y + z = 0$, $2x + 2y + 2z = 0$의 모든 실수해를 매개변수로 나타내라.

풀이. 둘째 식은 첫째 식의 2배이므로 피벗은 하나다. $y = s$, $z = t$를 자유롭게 정하면 $x = -s - t$이다. 따라서

$$(-s - t,\ s,\ t) = s(-1, 1, 0) + t(-1, 0, 1)$$

이다. 변수 3개에서 독립적인 제약 1개를 빼면 자유도가 2개 남는다.

연습문제 1.18 확대행렬의 한 행이 $[0\ 0\ 0 \mid 0]$인 것과 $[0\ 0\ 0 \mid 1]$인 것의 의미를 비교하라.

풀이. 첫 행은 항상 참인 $0 = 0$이므로 추가 제약을 주지 않는다. 둘째 행은 거짓인 $0 = 1$이므로 전체 계의 해가 없다. 두 경우의 계수 부분이 같더라도 상수항 때문에 결론이 달라진다.

연습문제 1.19 2×4 행렬 A에 대해 $Ax = 0$이 실수 위에서 유일한 해를 가질 수 있는가? $Ax = b$가 모든 $b \in \mathbb{R}^2$에 대해 해를 가질 수 있는가?

풀이. 피벗은 최대 2개이므로 자유변수가 적어도 2개 남아 동차계의 해가 유일할 수 없다. 그러나 모든 b에 대해 해가 존재할 수는 있다. 예를 들어 $A = [I_2 \ \ 0]$이면 앞의 두 변수에 b의 성분을 넣으면 된다. 존재와 유일성은 다른 조건이다.

연습문제 1.20 $x + ay = 1$, $2x + 4y = 3$의 해를 매개변수 a에 따라 분류하라.

풀이. 소거하면 $(4 - 2a)y = 1$이다. $a = 2$이면 모순이므로 해가 없다. $a \neq 2$이면 $y = 1/(4 - 2a)$이고 $x = 1 - ay = (4 - 3a)/(4 - 2a)$로 유일하다. 이 문제에서는 해가 무한히 많은 매개변수 값은 없다.

연습문제 1.21 $\mathbb{F}_2 = \{0, 1\}$에서 $x + y + z = 0$의 해를 모두 구하라. 덧셈은 법 2로 계산한다.

풀이. y, z를 정하면 $x = y + z$이다. 해는 $(0,0,0)$, $(1,1,0)$, $(1,0,1)$, $(0,1,1)$의 4개다. 자유변수 두 개가 각각 두 값을 가지므로 $2^2 = 4$개이며, 실수체에서의 무한히 많은 해와 구분된다.

소거법의 피벗 수와 자유변수 수는 이후 차원 정리로 설명된다. 먼저 어떤 대상들을 더하고 상수배할 수 있는지 살펴본다(제7권 제2장).

제 2 장

벡터공간과 부분공간

개요 벡터공간(*vector space*)은 덧셈과 스칼라배라는 두 연산이 정의되어 있고, 그 연산이 결합법칙·교환법칙·분배법칙 등 정해진 공리를 만족하는 집합이다. 벡터를 화살표로 생각하면 덧셈과 길이의 직관을 얻기 쉽지만, 선형대수의 벡터는 공간 속 화살표일 필요가 없다. 다항식, 함수, 행렬, 수열도 적절한 덧셈과 상수배를 갖추면 벡터가 되며, 서로 다른 분야에서 같은 정리가 성립하는 이유는 대상의 모양이 아니라 연산의 공통된 구조에 있다. 이 장은 벡터공간의 공리에서 출발하여, 부분집합이 부분공간(*subspace*)이 되는 판정법, 생성공간(*span*), 부분공간의 교집합·합·직합, 비동차 연립방정식의 해집합을 기술하는 아핀 부분공간을 차례로 세운다. 선행 지식: 벡터의 성분별 덧셈과 상수배, 연립일차방정식(제1장)이며, 함수와 다항식의 기본적인 계산을 예제로 사용한다.

2.1 스칼라와 벡터를 함께 지정하기

정의 2.1 (벡터공간) 체 $\mathbb{F}$ 위의 **벡터공간** V는 벡터의 덧셈 $u+v$와 스칼라배 av가 정의된 집합으로서 다음 성질을 만족한다.

(1) 덧셈은 결합법칙과 교환법칙을 만족한다: $(u+v)+w=u+(v+w)$, $u+v=v+u$.

(2) 영벡터 0이 존재하여 $v+0=v$이고, 각 v에 덧셈의 역원 $-v$가 있어 $v+(-v)=0$이다.

(3) $a(u+v)=au+av$, $(a+b)v=av+bv$이다.

(4) $a(bv)=(ab)v$, $1v=v$이다.

여기서 $u,v\in V$, $a,b\in\mathbb{F}$이며, 덧셈과 스칼라배의 결과는 다시 V에 속한다.

같은 기호 0이 스칼라와 영벡터에 쓰이지만 역할은 구분된다. 스칼라 0을 벡터 v에 곱한 결과가 영벡터라는 사실은 다음과 같이 공리에서 도출된다.

명제 2.2 (영벡터와 역원의 계산 법칙) 모든 벡터 v와 스칼라 a에 대해 $0v=0$, $a0=0$, $(-1)v=-v$이다. 또한 $av=0$이고 $a\neq 0$이면 $v=0$이다.

증명. $0v=(0+0)v=0v+0v$에서 $0v$의 덧셈 역원을 더하면 $0v=0$이다. 같은 방식으로 $a0=a(0+0)=a0+a0$에서 $a0=0$이다. $v+(-1)v=(1-1)v=0v=0$이므로 $(-1)v$는 v의 역원이다. 마지막으로 $av=0$의 양변에 a^{-1}을 곱하면 $a^{-1}(av)=(a^{-1}a)v=1v=v$이고 $a^{-1}0=0$이므로 $v=0$이다. □

공리는 계산을 제한하는 규칙이면서 동시에 계산을 허용하는 근거다. 예를 들어 $a\neq 0$이라는 조건 없이 $av=0$에서 $v=0$을 결론 내릴 수는 없다. 스칼라의 곱과 벡터의 덧셈을 구분하면 이런 조건을 놓치지 않게 된다.

2.2 좌표벡터와 행렬공간

가장 기본적인 벡터공간은 $\mathbb{F}^n$ 이다. 덧셈과 스칼라배를 성분별로 정의한다.

$$(x_1,\dots,x_n)+(y_1,\dots,y_n)=(x_1+y_1,\dots,x_n+y_n),\qquad a(x_1,\dots,x_n)=(ax_1,\dots,ax_n).$$

각 공리는 체의 연산 성질을 성분마다 적용하여 확인한다. $\mathbb{R}^n$ 과 $\mathbb{C}^n$ 은 비슷한 표기를 쓰지만 스칼라의 종류가 다르다.

> **예제 2.3 (실수와 복소수를 바꾸어 보는 공간)** $\mathbb{C}$ 는 복소수 스칼라로 보아도 벡터공간이고, 실수 스칼라로 보아도 벡터공간이다. 실수 스칼라만 허용하면 1의 상수배로 i 를 만들 수 없다. 복소수 스칼라를 허용하면 $i = i\cdot 1$ 이다. 따라서 같은 집합이라도 어느 체 위에서 생각하는지에 따라 생성과 독립성이 달라진다.

$m\times n$ 행렬 전체의 집합 $M_{m,n}(\mathbb{F})$ 도 성분별 연산으로 벡터공간이 된다. 행렬끼리의 곱셈은 벡터공간의 정의에 필요하지 않다. 두 2×3 행렬은 서로 더할 수 있지만 보통의 행렬곱으로 서로 곱할 수는 없다. 그래도 완전한 벡터공간이다.

> **예제 2.4 (행렬을 벡터로 계산하기)**
>
> $$A=\begin{pmatrix}1 & 0\\ -1 & 2\end{pmatrix},\qquad B=\begin{pmatrix}0 & 3\\ 1 & -2\end{pmatrix}$$
>
> 이면
>
> $$2A-B=\begin{pmatrix}2 & -3\\ -3 & 6\end{pmatrix}.$$
>
> 이 계산은 $\mathbb{F}^4$ 의 성분별 계산과 같다. 행렬 모양을 유지하는 것은 행과 열의 역할을 나중에 선형사상과 연결하기 위해 유용하다.

2.3 다항식과 함수도 벡터다

차수가 d 이하인 다항식 전체에 영다항식을 포함한 집합을 $\mathcal{P}_d(\mathbb{F})$ 라 하자. 영다항식의 차수를 특별히 정하지 않아도 이 집합에는 영다항식이 들어간다고 명시하면 된다. 두 다항식을 더하거나 상수배해도 차수가 d 를 넘지 않으므로 벡터공간이다.

> **예제 2.5 (다항식의 선형결합)** $p(t)=1+t$, $q(t)=t+t^2$ 라 하면
>
> $$2p(t)-q(t)=2+t-t^2.$$
>
> 여기서 벡터는 다항식 전체이고 스칼라는 2 와 -1 이다. 변수 t 는 다항식이 평가될 입력이며 벡터공간의 스칼라로 새롭게 움직이는 미지수와 구분된다.

흔한 오류 (차수가 정확히 d 인 다항식의 집합). 차수가 정확히 d 인 다항식만 모으면 일반적으로 벡터공간이 아니다. 예를 들어 두 일차다항식 t 와 $-t$ 를 더하면 영다항식이 되어 집합 밖으로 나간다. 최고차항이 상쇄될 수 있으므로 "d 이하"라는 조건이 중요하다.

집합 X에서 $\mathbb{F}$로 가는 모든 함수의 집합도 점별 연산

$$(f+g)(x)=f(x)+g(x),\qquad (af)(x)=af(x)$$

으로 벡터공간이다. 연속함수나 미분가능함수처럼 선형결합 아래에서 유지되는 성질을 가진 함수들은 그 안의 부분공간을 이룬다.

> **예제 2.6 (함수공간의 부분적인 조건)** $C([0,1],\mathbb{R})$는 연속함수의 실벡터공간이다. $f(0)=0$을 만족하는 함수들은 더하고 실수배해도 그 조건을 만족한다. 그러나 $f(0)=1$을 만족하는 함수들은 두 개를 더하면 값이 2가 되므로 벡터공간이 아니다.

유한한 좌표가 없어도 선형대수의 언어는 적용된다. 다만 유한차원에서 성립하는 모든 정리를 그대로 옮길 수는 없다. 이 권은 주로 유한차원을 다루되 함수공간을 예로 사용하여 정의가 어떤 범위까지 확장되는지 보여 준다.

2.4 부분공간 판정법

> **정의 2.7 (부분공간)** 벡터공간 V의 부분집합 W가 V에서의 연산을 그대로 사용하여 벡터공간이 되면 W를 V의 **부분공간**(*subspace*)이라고 한다.

> **정리 2.8 (부분공간 판정법)** $W\subseteq V$가 부분공간일 필요충분조건은 $0\in W$이고, 모든 $u,v\in W$와 $a,b\in\mathbb{F}$에 대해 $au+bv\in W$인 것이다.

증명. 부분공간이면 벡터공간의 닫힘 성질에 의해 조건이 성립한다. 반대로 조건을 가정하면 $a=b=1$을 택하여 덧셈에 닫혀 있음을 알 수 있고, $b=0$을 택하여 상수배에 닫혀 있음을 알 수 있다. $a=-1$을 사용하면 역원도 W에 있다. 결합법칙과 분배법칙 등 나머지 성질은 V에서 이미 성립하므로 W에도 제한되어 성립한다. □

W가 비어 있지 않고 모든 선형결합에 닫혀 있다고 가정해도 된다. 원소 $w\in W$를 하나 택하고 $0w$를 만들면 영벡터가 들어 있기 때문이다. 빈집합은 덧셈과 상수배의 조건을 공허하게 만족할 수 있지만 영벡터가 없으므로 부분공간이 아니다.

참고 (자명한 부분공간). 모든 벡터공간 V에 대하여 $\{0\}$과 V 자신은 항상 V의 부분공간이다. 이 둘을 **자명한 부분공간**이라고 하며, 그 밖의 부분공간을 **진부분공간**이라고 한다.

> **예제 2.9 (동차 선형 조건)**
>
> $$W=\{(x,y,z)\in\mathbb{R}^3 : x+2y-z=0\}$$
>
> 를 생각하자. 두 벡터 u,v가 조건을 만족하면 $au+bv$의 성분을 식에 넣은 값은 $a\cdot 0+b\cdot 0=0$이다. 따라서 부분공간이다. 매개변수로 쓰면 $(x,y,z)=(s,t,s+2t)$이며 원점을 지나는 평면이다.

> **예제 2.10 (선형처럼 보이지 않는 실패)** $S=\{(x,y)\in\mathbb{R}^2 : xy=0\}$은 두 좌표축의 합집합이다. $(1,0)$과 $(0,1)$은 S에 있지만 합 $(1,1)$은 없다. 영벡터를 포함하고 상수배에 닫혀 있어도 덧셈에 닫혀 있지 않으면 부분공간이 아니다.

2.5 생성공간: 필요한 모든 선형결합 모으기

정의 2.11 (생성공간) 벡터 $v_1, \dots, v_k$의 **생성공간**(*span*)은

$$\operatorname{span}(v_1, \dots, v_k) = \{a_1 v_1 + \cdots + a_k v_k : a_j \in \mathbb{F}\}$$

이다. 무한집합의 생성공간도 각 원소를 유한 개의 벡터의 선형결합으로 만든 집합으로 정의한다. 무한급수의 수렴은 이 대수적 정의에 포함되지 않는다.

명제 2.12 (생성공간의 최소성) 집합 S의 생성공간은 S를 포함하는 가장 작은 부분공간이다.

증명. 영벡터는 모든 계수를 0으로 놓아 얻는다. 두 유한 선형결합을 더하거나 상수배하면 다시 유한 선형결합이므로 생성공간은 부분공간이다. S를 포함하는 부분공간은 닫힘 성질 때문에 S의 모든 유한 선형결합도 포함한다. 따라서 생성공간보다 작게 줄일 수 없다. □

예제 2.13 (생성공간의 방정식 찾기) $u = (1, 0, 1)$, $v = (0, 1, 1)$이면

$$au + bv = (a, b, a + b).$$

따라서 $\operatorname{span}(u, v) = \{(x, y, z) : z = x + y\}$이다. 벡터 $(2, 3, 5)$는 $2u + 3v$로 표현되지만 $(2, 3, 6)$은 이 평면에 없다. 포함 여부를 묻는 문제는 계수를 미지수로 한 연립방정식으로 바꿀 수 있다.

생성 벡터를 많이 적었다고 생성공간이 반드시 커지는 것은 아니다. 이미 포함된 벡터를 추가하면 아무 변화가 없다. 예를 들어 위의 u, v에 $u + v$를 추가해도 생성공간은 같다. 어떤 벡터가 중복인지 체계적으로 판단하는 개념이 다음 장의 선형독립이다(제7권 제3장).

2.6 부분공간의 교집합과 합

명제 2.14 (교집합과 합) 벡터공간 V의 부분공간들의 교집합은 부분공간이다. 두 부분공간 U, W에 대해

$$U + W = \{u + w : u \in U,\ w \in W\}$$

도 부분공간이며 $U \cup W$를 포함하는 가장 작은 부분공간이다.

증명. 교집합의 원소들은 모든 해당 부분공간에 속하므로 선형결합도 모든 부분공간에 속한다. 합에 대해서는

$$a(u_1 + w_1) + b(u_2 + w_2) = (au_1 + bu_2) + (aw_1 + bw_2)$$

를 사용한다. 앞 괄호는 U, 뒤 괄호는 W에 속한다. U, W를 모두 포함하는 부분공간은 두 원소의 합도 포함하므로 최소성도 성립한다. □

예제 2.15 (두 평면의 합과 교집합) $U = \{(x, y, 0)\}$, $W = \{(0, y, z)\}$라 하자. 공통 원소는 $(0, y, 0)$이므로 교집합은 y축이다. 임의의 (x, y, z)는 $(x, y, 0) + (0, 0, z)$로 쓸 수 있으므로 $U + W = \mathbb{R}^3$이다. 두 평면을 합한다는 말은 점들의 합집합만 취하는 것보다 더 많은 점을 포함한다.

명제 2.16 (합집합이 부분공간일 조건) 두 부분공간의 합집합은 일반적으로 부분공간이 아니다. 더 정확히 말하면 $U \cup W$가 부분공간일 필요충분조건은 둘 중 하나가 다른 하나에 포함되는

것이다.

증명. 포함관계가 있으면 합집합은 큰 쪽의 부분공간이다. 어느 쪽도 다른 쪽에 포함되지 않는다면 $u \in U \setminus W$, $w \in W \setminus U$를 택할 수 있다. 합집합이 부분공간이라면 $u+w$가 U 또는 W에 속해야 한다. 첫 경우에는 $w = (u+w) - u \in U$라는 모순이 생기고, 둘째 경우에는 $u \in W$라는 모순이 생긴다. □

2.7 직합과 표현의 유일성

정의 2.17 (직합) $U \cap W = \{0\}$일 때 부분공간의 합 $U+W$를 **직합**(*direct sum*)이라고 하며 $U \oplus W$로 쓴다.

정리 2.18 (표현의 유일성) $U+W$의 모든 벡터가 $u+w$ 꼴로 유일하게 표현될 필요충분조건은 $U \cap W = \{0\}$이다.

증명. 교집합이 0이라고 하자. $u_1+w_1 = u_2+w_2$이면 $u_1-u_2 = w_2-w_1$은 U와 W에 모두 속하므로 0이다. 따라서 두 표현이 같다. 반대로 표현이 유일하다고 하고 $v \in U \cap W$라 하자. $v = v+0 = 0+v$의 두 표현을 비교하면 $v = 0$이어야 한다. □

예제 2.19 (대칭·반대칭 부분으로 분해하기) 실수 정사각행렬 A는

$$A = \frac{A + A^{\mathrm{T}}}{2} + \frac{A - A^{\mathrm{T}}}{2}$$

로 분해된다. 첫 행렬은 **대칭**(*symmetric*)이고 둘째는 **반대칭**(*skew-symmetric*)이다. 둘 다 해당하면 $S = S^{\mathrm{T}} = -S$이므로 실수 위에서는 $S = 0$이다. 따라서 대칭행렬 공간과 반대칭행렬 공간의 직합이 전체 행렬공간이다. 예를 들어

$$\begin{pmatrix} 1 & 4 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 3 & 3 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

특성 2인 체에서는 2로 나눌 수 없으므로 이 분해 공식을 사용할 수 없다.

직합 기호를 썼다고 직교한다는 뜻은 아니다. $\mathbb{R}^2$에서 x축과 $(1,1)$ 방향의 직선은 교집합이 0이므로 직합을 만들지만 수직은 아니다. 직교성은 내적을 도입한 뒤에 정의되는 추가 구조다(제7권 제8장).

2.8 아핀 부분공간과 비동차 해집합

부분공간은 반드시 원점을 포함한다. 그러나 비동차 연립방정식의 해집합은 원점을 지나지 않는 직선이나 평면인 경우가 많다. 이때는 부분공간을 평행이동한 **아핀 부분공간**(*affine subspace*)으로 해석한다.

정리 2.20 (비동차 해집합의 구조) $Ax = b$의 특정 해 x_p가 존재하면 해집합은

$$x_p + \{z : Az = 0\}$$

이다.

증명. $Az = 0$이면 $A(x_p + z) = Ax_p + Az = b$이다. 반대로 $Ax = b$이면 $A(x - x_p) = b - b = 0$이므로 $x = x_p + z$로 쓸 수 있다. 행렬의 성분별 분배법칙만 사용했다. □

> **예제 2.21** $x + y + z = 1$의 특정 해로 $(1,0,0)$을 택하면 모든 해는
>
> $$(1,0,0) + s(-1,1,0) + t(-1,0,1)$$
>
> 이다. 두 해의 합은 일반적으로 해가 아니지만, 계수의 합이 1인 아핀 결합은 다시 해다. 실제로 $Ax = Ay = b$이면 $A((1-t)x + ty) = (1-t)b + tb = b$이다.

이 차이는 좌표를 옮길 때 중요하다. 방향을 나타내는 벡터공간과 위치를 나타내는 아핀 공간을 구별하면, 원점의 선택에 의존하는 문장과 그렇지 않은 문장을 분리할 수 있다.

역사 (공리로서의 벡터공간). 벡터공간의 공리적 정의는 G. Peano가 1888년에 H. Grassmann의 1844년 저작 『확장론(*Ausdehnungslehre*)』의 아이디어를 다듬어 처음으로 명시적으로 제시했다. 그 이전에는 좌표 공간이나 기하학적 벡터 각각에 대해 따로 성질을 증명했다.

핵심 수식

$$W \subseteq V\text{가 부분공간} \iff 0 \in W \text{ 이고 모든 } u, v \in W,\ a, b \in \mathbb{F}\text{에 대해 } au + bv \in W, \tag{2.1}$$

$$U + W\text{가 직합} \iff U \cap W = \{0\}. \tag{2.2}$$

2.9 연습문제와 해설

> **연습문제 2.22** $\mathbb{R}^3$의 집합 $W = \{(x,y,z) : x - y + 2z = 0\}$가 부분공간임을 보이고 생성 벡터 두 개를 찾아라.

풀이. 조건이 동차 선형이므로 영벡터를 포함하고 선형결합에 닫혀 있다. $y = s$, $z = t$라 놓으면 $x = s - 2t$이므로 $(x,y,z) = s(1,1,0) + t(-2,0,1)$이다.

> **연습문제 2.23** $\{(x,y) : x \geq 0\}$, $\{(x,y) : x + y = 1\}$, $\{(x,y) : y = 3x\}$ 중 부분공간을 골라라.

풀이. 첫 집합은 $(1,0)$의 -1배를 포함하지 않는다. 둘째는 영벡터를 포함하지 않는다. 셋째는 $\operatorname{span}((1,3))$이므로 부분공간이다. 각각 다른 실패 조건을 확인하는 문제다.

> **연습문제 2.24** $\mathcal{P}_2(\mathbb{R})$에서 $W = \{p : p(1) = 0\}$의 모든 원소를 $(t-1)$을 이용하여 표현하라.

풀이. $p(1) = 0$이면 인수정리에 의해 $p(t) = (t-1)(a + bt)$로 쓸 수 있다. 따라서 $W = \operatorname{span}(t - 1,\ t^2 - t)$이다. 영다항식은 $a = b = 0$으로 포함된다.

> **연습문제 2.25** $\mathbb{R}$를 $\mathbb{C}$의 부분집합으로 볼 때, 실수 스칼라와 복소수 스칼라에 대해 각각 부분공간인지 판단하라.

풀이. 실수 덧셈과 실수배에는 닫혀 있으므로 실벡터공간의 부분공간이다. 그러나 $1 \in \mathbb{R}$에 복소수 i를 곱하면 $i \notin \mathbb{R}$이므로 복소벡터공간의 부분공간은 아니다. 스칼라체를 명시하지 않으면 질문이 완성되지 않는다.

> **연습문제 2.26** $U = \operatorname{span}((1,0))$, $W = \operatorname{span}((1,1))$에 대해 $(3,2)$의 직합 표현을 구하라.

풀이. $a(1,0)+b(1,1)=(a+b,b)=(3,2)$이므로 $b=2$, $a=1$이다. $U\cap W=\{0\}$이므로 이 표현은 유일하다. 두 방향은 직교하지 않아도 직합을 이룬다.

> **연습문제 2.27** 두 아핀 해 x_1, x_2가 $Ax=b$를 만족한다. $2x_1-x_2$는 항상 해인가? x_1+x_2는 어떤 조건에서 해인가?

풀이. $A(2x_1-x_2)=2b-b=b$이므로 첫 벡터는 항상 해다. 두 번째는 $2b$를 출력하므로 $2b=b$, 즉 $b=0$일 때 해다. 첫 결합은 계수의 합이 1이고 두 번째는 그렇지 않다는 차이를 볼 수 있다.

생성공간을 설명하는 벡터 목록에는 중복이 있을 수 있다. 중복을 제거하면서 모든 벡터를 유일하게 표현하는 목록이 기저이며, 이는 다음 장에서 다룬다(제7권 제3장).

제 3 장

선형독립 · 기저 · 차원

개요 이 장은 벡터 목록의 **선형독립**(*linear independence*)과 **선형종속**(*linear dependence*), 공간 전체를 생성하면서 중복이 없는 벡터 목록인 **기저**(*basis*), 그리고 모든 기저가 공유하는 길이인 **차원**(*dimension*)을 정의하고 그 성질을 증명한다. 하나의 평면을 기술하는 데는 보통 서로 평행하지 않은 두 방향이면 충분하다. 세 번째 방향을 더 적을 수는 있지만 이미 앞의 두 방향으로 표현된다면 새로운 정보를 주지 않는다. 선형독립은 이러한 중복이 없는 상태를 정확하게 정의하고, 기저는 공간 전체를 생성하면서 중복이 없는 목록을 가리키며, 그 목록의 길이가 차원이다. 차원이 잘 정의되려면 서로 다른 기저가 모두 같은 길이를 가진다는 사실을 증명해야 한다. 이 사실을 평면이나 공간에 대한 그림의 직관만으로 받아들이면 함수나 행렬을 벡터로 보는 상황에서는 근거가 약해진다. 이 장에서는 생성 목록과 독립 목록 사이의 교환 원리를 통해 차원의 의미를 확립한다. 선행 지식: 벡터공간, 생성공간, 동차 연립방정식. 이 장의 차원 비교 정리는 유한차원 공간을 대상으로 한다.

3.1 영벡터를 만드는 방법이 자명한가

정의 3.1 (선형독립과 선형종속) 벡터 목록 $v_1, \dots, v_k$가 **선형독립**이라는 것은

$$a_1 v_1 + \cdots + a_k v_k = 0 \implies a_1 = \cdots = a_k = 0$$

임을 뜻한다. 계수 중 적어도 하나가 0이 아닌데 합이 영벡터가 되는 경우가 있으면 **선형종속**이라고 한다.

정의에는 두 단계가 있다. 모든 선형결합이 영벡터가 아니라는 뜻이 아니다. 모든 계수가 0인 결합은 언제나 영벡터를 만든다. 그 외의 방법이 있는지를 묻는 것이다. 벡터들 중 영벡터가 포함되면 그 벡터의 계수만 1로 두어 비자명한 관계를 만들 수 있으므로 종속이다.

예제 3.2 (두 벡터와 세 벡터) $u = (1,0,1)$, $v = (0,1,1)$에 대해 $au + bv = (a, b, a+b) = 0$이면 $a = b = 0$이다. 따라서 두 벡터는 독립이다. 하지만 $w = (1,1,2)$를 추가하면 $u + v - w = 0$이므로 세 벡터는 종속이다. 각 벡터가 영이 아니어도 전체 목록은 종속일 수 있다.

명제 3.3 (종속성과 선형결합 표현) 유한한 벡터 목록이 종속일 필요충분조건은 그중 한 벡터를 나머지 벡터들의 선형결합으로 표현할 수 있다는 것이다.

증명. 비자명한 관계 $\sum a_j v_j = 0$에서 $a_i \neq 0$인 계수를 고르면

$$v_i = -\sum_{j \neq i} \frac{a_j}{a_i} v_j$$

이다. 반대로 이러한 표현이 있으면 한쪽으로 모두 옮겨 v_i의 계수가 1인 비자명한 영벡터 관계를 얻는다. □

여기서 “그중 한 벡터”라는 말이 중요하다. 종속 목록의 모든 벡터가 반드시 나머지로 표현되는 것은 아니다. 예를 들어 $(1,0),(2,0),(0,1)$은 종속이지만 마지막 벡터는 앞의 두 벡터로 만들 수 없다. 둘째 벡터가 첫째 벡터의 2배이므로 종속성은 첫째와 둘째 사이에만 있고, 그 관계가 전체 목록을 종속으로 만드는 데에는 충분하다.

3.2 연립방정식으로 독립성을 검사하기

벡터들을 열로 모은 행렬 $A = [v_1 \ \cdots \ v_k]$에 대해 선형관계는 $Aa = 0$이다. 따라서 열벡터들이 독립일 필요충분조건은 동차계가 영해만 갖는 것이다. 소거법으로 모든 열에 피벗이 생기는지 확인하면 된다.

> **예제 3.4 (매개변수에 따른 독립성)**
>
> $$v_1 = (1, 1), \qquad v_2 = (1, \lambda)$$
>
> 가 독립인지 본다. $av_1 + bv_2 = 0$은
>
> $$a + b = 0, \qquad a + \lambda b = 0$$
>
> 이다. 두 식을 빼면 $(\lambda - 1)b = 0$이다. $\lambda \neq 1$이면 $a = b = 0$이므로 독립이고, $\lambda = 1$이면 두 벡터가 같아 종속이다. 행렬식을 사용하지 않고도 완전히 판정할 수 있다.

n개의 성분을 가진 벡터를 n개보다 많이 모으면 종속이다. 대응하는 동차계의 방정식 수가 변수 수보다 작으므로 자유변수가 생기기 때문이다. 이 주장은 $\mathbb{F}^n$에서 직관적인 차원의 한계를 계산으로 보여 준다.

> **예제 3.5 (다항식의 독립성)** $1, t, t^2$이 다항식 공간에서 독립임을 보이려면 $a + bt + ct^2$이 영다항식인 경우를 보면 된다. 다항식의 계수 비교로 $a = b = c = 0$이다. 어떤 특정한 t 한 값에만 대입해 0이 되었다는 조건으로는 충분하지 않다. 예를 들어 $1 - t$는 $t = 1$에서 0이지만 영다항식은 아니다.

3.3 기저와 좌표의 유일성

> **정의 3.6 (기저와 좌표)** 벡터공간 V의 **기저**는 V를 생성하는 선형독립 목록이다. 순서 있는 기저 $\mathcal{B} = (b_1, \dots, b_n)$에 대하여
>
> $$v = c_1 b_1 + \cdots + c_n b_n$$
>
> 일 때 계수열 $[v]_{\mathcal{B}} = (c_1, \dots, c_n)^{\mathsf{T}}$를 v의 $\mathcal{B}$**-좌표**(*coordinates*)라고 한다.

> **정리 3.7 (좌표의 존재와 유일성)** $\mathcal{B}$가 기저이면 모든 벡터는 그 기저의 선형결합으로 유일하게 표현된다. 반대로 모든 벡터가 목록의 선형결합으로 유일하게 표현되면 그 목록은 기저이다.

증명. 생성 조건이 표현의 존재를 준다. 두 표현 $\sum c_j b_j = \sum d_j b_j$가 있다면 $\sum (c_j - d_j) b_j = 0$이고 독립성으로 $c_j = d_j$이다. 반대로 유일한 표현이 존재하면 생성 조건이 성립한다. 영벡터의 자명한 표현 외에 다른 표현이 있을 수 없으므로 독립성도 성립한다. $\square$

예제 3.8 (같은 다항식의 다른 좌표) $\mathcal{B} = (1, 1+t, 1+t+t^2)$는 $\mathcal{P}_2(\mathbb{R})$의 기저이다. $p(t) = 2+3t+t^2$을

$$p = c_1 + c_2(1+t) + c_3(1+t+t^2)$$

로 놓고 계수를 비교하면 $c_3 = 1$, $c_2 = 2$, $c_1 = -1$이다. 따라서 $[p]_{\mathcal{B}} = (-1, 2, 1)^{\mathsf{T}}$이다. 표준 기저 $(1, t, t^2)$에서는 좌표가 $(2, 3, 1)^{\mathsf{T}}$이므로 좌표와 벡터 자체를 구분해야 한다.

표준 기저 e_j는 j번째 성분만 1이고 나머지가 0인 벡터들이다. $\mathbb{F}^n$의 모든 벡터는 $x_1e_1+\cdots+x_ne_n$으로 유일하게 표현된다. 이 때문에 표준 좌표에서는 벡터와 좌표열이 같은 표기로 보이지만, 일반 기저에서는 더 이상 같지 않다.

3.4 생성 목록을 줄이고 독립 목록을 늘리기

명제 3.9 (중복 제거와 확장) 유한 생성 목록이 종속이면 적어도 한 벡터를 제거해도 생성공간이 변하지 않는다. 독립 목록에 그 생성공간 밖의 벡터를 추가하면 독립성이 유지된다.

증명. 첫째는 제거할 벡터를 나머지의 선형결합으로 표현하면 된다. 그 벡터를 사용한 모든 표현을 나머지로 바꿀 수 있다. 둘째에서 새 벡터 w를 포함한 관계

$$a_1v_1 + \cdots + a_kv_k + bw = 0$$

를 본다. $b \neq 0$이면 w가 기존 벡터들의 생성공간에 속한다는 모순이 생긴다. 따라서 $b = 0$이고 기존 독립성으로 모든 $a_j = 0$이다. □

유한차원 공간에서는 유한 생성 목록에서 중복을 차례로 제거하면 기저를 얻는다. 이미 알고 있는 독립 목록이 있다면, 아직 생성하지 못하는 벡터를 추가하여 기저로 확장할 수 있다. 유한성 때문에 이 과정은 끝난다. 일반적인 무한차원 공간에서 기저의 존재를 논할 때에는 별도의 집합론적 원리가 등장할 수 있지만 여기서는 유한차원으로 제한한다.

예제 3.10 (독립 목록의 기저 확장) $u = (1, 1, 0)$, $v = (0, 1, 1)$은 독립이다. 두 벡터의 생성공간은 $(a, a+b, b)$ 형태이므로 $(0, 0, 1)$은 그 안에 없다. 따라서 u, v, e_3은 독립이고 $\mathbb{R}^3$의 기저가 된다. 실제로 $(x, y, z) = xu + (y-x)v + (z-y+x)e_3$이다.

3.5 교환 보조정리와 차원의 정의

보조정리 3.11 (교환 원리) V를 생성하는 m개의 벡터가 있고 V 안에 k개의 독립 벡터가 있으면 $k \le m$이다.

증명. 생성 목록을 $w_1, \dots, w_m$, 독립 목록을 $u_1, \dots, u_k$라 한다. u_1은 영이 아니며 w_j들의 선형결합이므로 적어도 하나의 계수가 비영이다. 그 w_j를 u_1과 나머지 w들로 풀어 쓸 수 있어, 생성 목록에서 w_j를 u_1로 바꾸어도 여전히 전체를 생성한다.

이제 u_2를 새 생성 목록으로 표현한다. u_1만으로 표현된다면 독립성에 모순이므로 아직 남은 w 중 하나의 계수가 비영이다. 그 벡터를 u_2로 바꿀 수 있다. 같은 과정을 반복할 때 매번 새로운 u는 아직 남은 w 하나를 대체해야 한다. 만약 $k > m$이라면 m번 바꾼 뒤 $u_1, \dots, u_m$이 V를 생성하므로 u_{m+1}이 $u_1, \dots, u_m$의 선형결합이 되어 독립성에 모순이다. 따라서 $k \le m$이다. □

정리 3.12 (기저 길이의 불변성) 유한차원 벡터공간의 모든 기저는 같은 개수의 벡터를 갖는다.

증명. 두 기저의 길이를 n, m이라 한다. 첫 기저가 독립이고 둘째가 생성하므로 교환 원리(보조정리 3.11)에 의해 $n \le m$이다. 역할을 바꾸면 $m \le n$이다. 따라서 $n = m$이다. □

정의 3.13 (차원) 유한차원 공간 V의 기저 길이를 **차원**이라고 하며 $\dim_{\mathbb{F}} V$로 쓴다. 스칼라체가 명확하면 아래첨자를 생략한다. 영공간 $\{0\}$의 기저는 빈 목록이고 차원은 0이다.

핵심 수식

$$\dim \mathbb{F}^n = n, \tag{3.1}$$

$$\dim \mathcal{P}_d(\mathbb{F}) = d + 1, \tag{3.2}$$

$$\dim M_{m,n}(\mathbb{F}) = mn. \tag{3.3}$$

마지막 공간은 각 위치에 1을 하나 넣은 행렬 E_{ij}들을 기저로 갖는다. 행렬의 행 수나 열 수 하나만을 차원이라고 부르는 것은 식 (3.3)의 벡터공간 차원과 다르다.

3.6 차원으로 독립성과 생성을 연결하기

따름정리 3.14 (차원과 벡터 개수) $\dim V = n$일 때 n개의 벡터에 대해서는 선형독립과 생성 조건 중 하나만 확인해도 기저임을 알 수 있다. n개보다 많은 벡터는 종속이고, n개보다 적은 벡터는 전체를 생성할 수 없다.

증명. 독립인 n개가 전체를 생성하지 않으면 생성공간 밖의 벡터를 추가하여 독립인 $n+1$개를 만들 수 있어 교환 원리에 모순이다. 생성하는 n개가 종속이면 하나를 제거하여 $n-1$개로 전체를 생성할 수 있어 역시 모순이다. 나머지 주장도 교환 원리에서 바로 나온다. □

예제 3.15 (스칼라체에 따른 차원) $\mathbb{C}$는 실수 위에서는 $(1, i)$를 기저로 하므로 차원이 2이다. 복소수 위에서는 (1)이 기저이므로 차원이 1이다. 따라서 $\dim \mathbb{C}$라는 표기만 쓰면 어느 체 위의 차원인지 문맥을 확인해야 한다. 복소벡터공간 $\mathbb{C}^n$을 실벡터공간으로 보면 차원은 $2n$이다.

함수공간이 모두 유한차원인 것은 아니다. $1, t, t^2, \dots, t^N$은 임의의 N에 대해 실수 다항식 공간에서 독립이므로 전체 다항식 공간은 유한차원이 아니다. $C([0,1], \mathbb{R})$ 안에서도 이 함수들은 독립이다. 0이 아닌 다항식은 한 구간 전체에서 0일 수 없기 때문이다. 이 논증은 아무리 큰 유한 목록을 잡아도 더 많은 독립 벡터를 찾을 수 있음을 보인다.

3.7 소거법에서 실제 기저 추출하기

예제 3.16 (열공간의 기저는 원래 열에서 고른다)

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 1 \\ 1 & 2 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

에서 피벗 열은 첫째와 셋째 열이다. 따라서 원래 열공간의 기저로

$$\begin{pmatrix}1\\0\\1\end{pmatrix},\qquad \begin{pmatrix}0\\1\\1\end{pmatrix}$$

를 택한다. 둘째 원래 열은 첫째 원래 열의 2배이다. 소거한 행렬의 피벗 열 $(1,0,0)^{\mathsf{T}}, (0,1,0)^{\mathsf{T}}$는 일반적으로 원래 열공간의 벡터가 아니므로 대신 가져오면 안 된다.

기본 행 연산은 열들 사이의 선형관계를 보존한다. 계수열 c에 대해 $Ac = 0$인지를 나타내는 동차계를 변환했기 때문이다. 따라서 피벗 위치를 찾는 데는 소거한 행렬을 사용하고, 원래 공간의 기저를 쓸 때는 원래 열을 사용한다.

행공간은 다르게 다룬다. 기본 행 연산은 새 행을 원래 행들의 선형결합으로 만들며 역연산도 가능하므로 행공간 자체를 보존한다. 따라서 사다리꼴에서 영이 아닌 행들을 가져오면 원래 행공간의 기저가 된다. 영이 아닌 사다리꼴 행들은 서로 다른 피벗 위치를 가져 독립이다.

3.8 부분공간의 차원과 합의 공식

정리 3.17 (부분공간의 차원과 합의 공식) 유한차원 공간의 부분공간 $W \subseteq V$에 대해 $\dim W \le \dim V$이다. 차원이 같으면 $W = V$이다. 두 유한차원 부분공간 U, W에 대해서는

$$\dim(U + W) = \dim U + \dim W - \dim(U \cap W) \tag{3.4}$$

이다.

증명. W의 기저는 V 안의 독립 목록이므로 길이가 $\dim V$를 넘지 않는다. 길이가 같으면 V의 기저이므로 전체를 생성한다.

합의 공식에서는 $U \cap W$의 기저 $c_1, \dots, c_r$를 택한다. 이를 U의 기저 $c_1, \dots, c_r, u_1, \dots, u_p$와 W의 기저 $c_1, \dots, c_r, w_1, \dots, w_q$로 각각 확장한다. 이 목록들을 공통 c를 한 번만 적어 합치면 $U+W$를 생성한다.

독립성을 보이기 위해 $\sum \alpha_i c_i + \sum \beta_j u_j + \sum \gamma_k w_k = 0$이라 한다. w들의 결합을 반대편으로 보내면 그 결합은 $U \cap W$에 속하므로 c들의 결합이다. W의 기저 독립성에 의해 모든 $\gamma_k = 0$이다. 남은 관계에서 U의 기저 독립성을 쓰면 모든 $\alpha_i, \beta_j = 0$이다. 따라서 차원은 $r+p+q = (r+p)+(r+q)-r$이다. □

예제 3.18 (교집합을 먼저 구하는 계산) $U = \operatorname{span}((1,1,0),(0,1,1))$, $W = \operatorname{span}(e_1, e_2)$라 한다. U의 벡터는 $(a, a+b, b)$이고, W에 속하려면 $b = 0$이어야 한다. 따라서 $U \cap W = \operatorname{span}((1,1,0))$이다. 두 공간의 차원은 각각 2, 교집합의 차원은 1이므로 합의 차원은 3이다. 실제로 합은 $\mathbb{R}^3$이다.

3.9 연습문제와 해설

연습문제 3.19 $(1,2),(2,4)$와 $(1,2),(2,3)$의 독립성을 각각 판정하라.

풀이. 첫 목록은 둘째 벡터가 첫째의 2배여서 종속이다. 둘째 목록에서 $a+2b=0$, $2a+3b=0$을 풀면 $b=0$, $a=0$이므로 독립이다. 영벡터를 만드는 관계를 직접 확인했다.

연습문제 3.20 $\mathcal{P}_2(\mathbb{R})$에서 $(1, t, 1+t^2)$가 기저임을 보이고 $3-2t+4t^2$의 좌표를 구하라.

풀이. $a+bt+c(1+t^2)=0$이면 $c=0$, $b=0$, $a=0$이므로 독립이다. 공간 차원이 3이고 벡터가 세 개이므로 기저이다. 계수 비교로 $c=4$, $b=-2$, $a=-1$이므로 좌표는 $(-1,-2,4)^{\mathsf{T}}$이다.

연습문제 3.21 $\mathbb{R}^4$에서 독립인 벡터 세 개가 주어졌다. 이것만으로 전체 공간을 생성하는가? 기저로 만들려면 무엇이 필요한가?

풀이. 전체 차원이 4이므로 세 벡터만으로 생성할 수 없다. 기존 생성공간 밖의 벡터 하나를 골라 추가하면 독립인 네 벡터가 되어 기저가 된다. 아무 벡터나 추가하는 것이 아니라 생성공간 밖이라는 조건이 필요하다.

연습문제 3.22 실수 2×2 대칭행렬 공간의 기저와 차원을 구하라.

풀이. 모든 원소는 $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$이므로 기저로 $E_{11}, E_{12}+E_{21}, E_{22}$를 택할 수 있다. 세 계수가 유일하므로 차원은 3이다. 전체 2×2 행렬공간의 차원 4와 구분된다.

연습문제 3.23 $\dim V = 5$이고 $U, W \subseteq V$의 차원이 각각 3과 4라면 교집합의 차원은 최소 얼마인가?

풀이. 합의 차원이 최대 5이므로 식 (3.4)에서 $\dim(U\cap W) = 3+4-\dim(U+W) \geq 2$이다. 그림 없이도 두 큰 부분공간이 적어도 두 차원의 정보를 공유해야 함을 알 수 있다.

연습문제 3.24 소거한 행렬의 피벗 열을 원래 열공간의 기저로 그대로 가져오면 왜 잘못될 수 있는가? 간단한 예를 들어라.

풀이. 열벡터의 성분은 행 연산으로 바뀐다. 예를 들어 열이 하나인 $A=(1,1)^{\mathsf{T}}$를 소거하면 $(1,0)^{\mathsf{T}}$가 되지만 두 벡터가 생성하는 직선은 다르다. 보존되는 것은 열 사이의 관계와 피벗 위치이며, 원래 공간의 벡터를 제시할 때는 원래 열을 골라야 한다.

기저를 고르면 추상적 벡터에 좌표를 붙일 수 있다. 다음 장에서는 벡터를 다른 벡터로 보내는 선형사상을 정의하고, 어떤 정보가 사라지고 어떤 정보가 남는지 차원으로 계산한다(제7권 제4장).

제 4 장

선형사상 · 핵 · 상과 차원 정리

개요 이 장은 벡터공간의 덧셈과 스칼라배를 보존하는 사상인 **선형사상**(*linear map*)과, 그 사상이 입력에서 잃어버리는 정보를 모은 **핵**(*kernel*), 실제로 도달하는 출력을 모은 **상**(*image*)을 정의하고, 두 정보의 차원을 합하면 정의역의 차원이 된다는 차원 정리를 증명한다. 벡터공간이 더하고 상수배할 수 있는 대상을 설명한다면, 선형사상은 그 연산을 보존하면서 대상을 옮기는 방법을 설명한다. 행렬곱은 선형사상의 대표적인 예지만 유일한 예는 아니다. 미분, 특정 점에서 함수값을 구하는 연산, 좌표의 일부를 버리는 연산도 선형일 수 있다. 사상을 이해하는 두 질문은 어떤 입력이 0으로 가는가와 어떤 출력이 실제로 나오는가이다. 첫 질문의 답이 핵이고 둘째의 답이 상이다. 핵은 잃어버리는 정보를, 상은 도달 가능한 정보를 나타낸다. 유한차원에서는 두 정보의 차원을 합하면 입력공간의 차원이 된다는 기본 정리가 성립한다. 선행 지식: 기저, 차원, 부분공간, 동차계와 비동차계의 해집합(제7권 제2장, 제7권 제3장). 정의역과 공역을 구분하여 읽는다.

4.1 정의역과 공역을 포함한 선형성

정의 4.1 (선형사상) 같은 체 $\mathbb{F}$ 위의 벡터공간 V, W 사이의 사상 $T : V \to W$가 모든 $u, v \in V$와 $a, b \in \mathbb{F}$에 대해

$$T(au + bv) = aT(u) + bT(v)$$

를 만족하면 **선형사상**이라고 한다.

선형성은 덧셈 보존과 스칼라배 보존의 두 조건으로 나누어 검사할 수 있다. 선형사상은 반드시 $T(0) = 0$을 만족한다. 그러나 $T(0) = 0$은 선형성의 필요조건일 뿐 충분조건이 아니다. $T(x) = x^2$는 0을 0으로 보내지만 $T(1+1) = 4 \neq 2 = T(1) + T(1)$이다.

예제 4.2 (행렬이 정의하는 선형사상)

$$T : \mathbb{R}^3 \to \mathbb{R}^2, \qquad T(x, y, z) = (x + y, y + z)$$

는 선형이다. 각 출력 성분이 입력의 선형결합이므로 분배법칙을 성분별로 적용하면 된다. 대응하는 행렬은

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

이고 $T(x) = Ax$이다. 출력이 두 성분이라고 입력도 두 성분일 필요는 없다.

예제 4.3 (상수항이 있는 아핀 사상) $S(x, y) = (2x + y + 1, x - y)$는 선형이 아니다. $S(0,0) = (1,0) \neq 0$이기 때문이다. $S(x) = Ax + b$ 형태에서 $b = 0$일 때만 선형이고, 일반적인 경우는 **아핀 사상**(*affine map*)이라고 한다. 직선을 직선으로 보낸다는 기하적 성질만으로 선형성을 판단할

수 없다.

4.2 미분·평가·켤레의 예

예제 4.4 (미분은 다항식 공간 사이의 선형사상)

$$D : \mathcal{P}_3(\mathbb{R}) \to \mathcal{P}_2(\mathbb{R}), \qquad Dp = p'$$

는 $(ap+bq)' = ap' + bq'$ 이므로 선형이다. 예를 들어

$$D(2 - 3t + t^2 + 4t^3) = -3 + 2t + 12t^2.$$

입력과 출력이 함수여도 벡터공간의 연산을 보존하면 선형사상이다.

예제 4.5 (두 점에서 값을 읽기)

$$E : \mathcal{P}_2(\mathbb{R}) \to \mathbb{R}^2, \qquad E(p) = (p(0), p(1))$$

는 선형이다. $p = a + bt + ct^2$ 이면 $E(p) = (a, a+b+c)$ 이다. 서로 다른 다항식이 같은 두 값을 가질 수 있으므로, 선형이라는 사실만으로 입력을 복원할 수 있는 것은 아니다.

예제 4.6 (복소켤레는 어느 체 위에서 선형인가) $C : \mathbb{C} \to \mathbb{C}$, $C(z) = \bar{z}$는 실수 a, b에 대해 $\overline{az+bw} = a\bar{z} + b\bar{w}$를 만족하므로 실선형이다. 그러나 복소수 스칼라 i에 대해 $C(i \cdot 1) = -i$ 이고 $iC(1) = i$이므로 복소선형이 아니다. 복소켤레는 복소 스칼라를 켤레로 바꾸는 반선형 사상이다.

정의역과 공역의 체를 바꾸면 선형성 판정도 달라진다. 함수의 수식만 적는 대신 $T : V \to W$와 스칼라체를 함께 쓰는 것이 필요한 이유다.

4.3 기저의 상을 정하면 사상이 정해진다

정리 4.7 (기저의 상에 의한 결정) V의 기저가 $b_1, \dots, b_n$이고 $w_1, \dots, w_n \in W$가 임의로 주어졌다고 한다. 각 j에 대해 $T(b_j) = w_j$를 만족하는 선형사상 $T : V \to W$가 유일하게 존재한다.

증명. 벡터 $v = \sum c_j b_j$의 기저 표현은 유일하므로 $T(v) = \sum c_j w_j$로 정의하면 모호함이 없다. 계수의 덧셈과 상수배를 이용하여 선형성을 확인할 수 있다. 다른 선형사상도 기저 벡터의 값을 알면 $T(\sum c_j b_j) = \sum c_j T(b_j)$로 계산되어야 하므로 같은 값을 갖는다. □

예제 4.8 (표준 기저가 아닌 입력 자료) $T : \mathbb{R}^2 \to \mathbb{R}^2$가 $T(1,1) = (2,0)$, $T(1,-1) = (0,3)$을 만족한다고 한다. 두 입력 벡터는 기저이다. $(x,y) = \frac{x+y}{2}(1,1) + \frac{x-y}{2}(1,-1)$ 이므로

$$T(x,y) = \left(x + y,\ \frac{3}{2}(x-y) \right).$$

기저에 대한 정보만으로 전체 사상이 결정된다.

입력 목록이 기저가 아니라 종속 목록이면 원하는 출력들을 마음대로 지정할 수 없다. $v_3 = v_1 + v_2$ 라면 반드시 $T(v_3) = T(v_1) + T(v_2)$ 여야 한다. 선형관계를 보존해야 하므로 입력의 관계와 모순되는 출력 지정은 선형사상으로 확장되지 않는다.

4.4 핵과 상의 정의 및 부분공간성

정의 4.9 (핵과 상) 선형사상 $T : V \to W$ 의 **핵**과 **상**은 각각

$$\ker T = \{v \in V : T(v) = 0\}, \qquad \operatorname{im} T = \{T(v) : v \in V\}$$

이다. 핵은 정의역의 부분집합이고 상은 공역의 부분집합이다.

명제 4.10 (핵과 상의 부분공간성) $\ker T$ 와 $\operatorname{im} T$ 는 각각 V, W 의 부분공간이다.

증명. $T(0) = 0$ 이다. $u, v \in \ker T$ 이면 $T(au + bv) = a0 + b0 = 0$ 이므로 핵은 선형결합에 닫혀 있다. 상의 두 벡터가 $T(u), T(v)$ 이면 $aT(u) + bT(v) = T(au + bv)$ 도 상에 속한다. □

예제 4.11 (직사각형 행렬의 핵과 상) 앞의 $T(x, y, z) = (x + y, y + z)$ 에서 핵의 조건은 $x = -y$, $z = -y$ 이다. 따라서

$$\ker T = \operatorname{span}((1, -1, 1)).$$

임의의 $(a, b) \in \mathbb{R}^2$ 는 $T(a, 0, b)$ 이므로 상은 $\mathbb{R}^2$ 전체다. 입력의 한 방향이 사라지지만 두 성분의 출력은 모두 만들 수 있다.

예제 4.12 (미분과 평가의 핵) 미분 $D : \mathcal{P}_3(\mathbb{R}) \to \mathcal{P}_2(\mathbb{R})$ 의 핵은 상수다항식의 공간이다. 모든 이차 이하 다항식은 삼차 이하 원시함수를 가지므로 상은 공역 전체이다. 평가사상 $E(p) = (p(0), p(1))$ 의 핵은 $p(0) = p(1) = 0$ 인 다항식이므로 $\operatorname{span}(t(t-1))$ 이다. 임의의 (a, b) 는 $p(t) = a + (b - a)t$ 의 출력이므로 E 도 전사이다.

4.5 단사·전사와 해의 복원

정리 4.13 (단사성과 전사성의 판정) 선형사상 $T : V \to W$ 가 **단사**(*injective*)일 필요충분조건은 $\ker T = \{0\}$ 이다. **전사**(*surjective*)일 필요충분조건은 $\operatorname{im} T = W$ 이다.

증명. 단사이면 $T(v) = 0 = T(0)$ 에서 $v = 0$ 이다. 반대로 핵이 0이고 $T(u) = T(v)$ 이면 $T(u - v) = 0$ 이므로 $u - v = 0$ 이다. 전사에 대한 주장은 모든 공역 원소가 실제 출력이라는 정의를 그대로 표현한 것이다. □

예제 4.14 (공역에 따라 바뀌는 전사성) $P : \mathbb{R}^3 \to \mathbb{R}^3$, $P(x, y, z) = (x, y, 0)$ 는 세 번째 좌표를 버리는 사영이다. 상은 xy 평면이므로 $\mathbb{R}^3$ 로는 전사가 아니다. 같은 규칙을 $P : \mathbb{R}^3 \to \{(x, y, 0)\}$ 로 보면 전사이다. 공역을 적는 이유가 여기에 있다. 두 경우 모두 핵은 z 축이어서 단사는 아니다.

$T(v) = w$ 의 해가 하나 존재하면 모든 해는 그 특정 해에 $\ker T$ 를 더한 형태다. 출력이 같은 두 입력의 차이는 핵에 속한다. 따라서 핵이 0일 때만 존재하는 입력을 유일하게 복원할 수 있다. 존재 여부는 상이 결정하고, 유일성은 핵이 결정한다.

4.6 계수와 영차원: rank–nullity 정리

정의 4.15 (계수와 영차원) 유한차원 정의역을 가진 선형사상에 대해 $\operatorname{rank} T = \dim \operatorname{im} T$를 **계수**(*rank*)라고 하고 $\operatorname{nullity} T = \dim \ker T$를 **영차원**(*nullity*)이라고 한다. 계수는 출력공간 전체의 차원이 아니라 실제로 도달하는 상의 차원이다.

정리 4.16 (차원 정리) V가 유한차원이고 $T : V \to W$가 선형이면

$$\dim V = \dim \ker T + \dim \operatorname{im} T \tag{4.1}$$

이다. 공역 W 전체가 유한차원일 필요는 없다.

증명. 핵의 기저를 $k_1, \dots, k_r$라 하고 이를 V의 기저

$$k_1, \dots, k_r, v_1, \dots, v_s$$

로 확장한다. 임의의 입력은 이 기저의 선형결합이므로 출력은 $T(v_1), \dots, T(v_s)$의 선형결합이다. 따라서 이 출력 목록은 상을 생성한다.

또 $\sum a_j T(v_j) = 0$이면 $\sum a_j v_j \in \ker T$이다. 따라서 어떤 b_i에 대해 $\sum a_j v_j = \sum b_i k_i$이고, 전체 기저의 독립성으로 모든 $a_j = 0$이다. 그러므로 출력 목록은 상의 기저이다. 따라서 $\dim \ker T = r$, $\dim \operatorname{im} T = s$이며 $\dim V = r + s$이다. □

예제 4.17 (정보가 사라지는 차원의 계산) $T : \mathbb{R}^5 \to \mathbb{R}^3$의 계수가 2라면 영차원은 $5 - 2 = 3$이다. 정의역 차원에서 빼야 하므로 $3 - 2 = 1$로 계산하면 안 된다. $T(x) = b$가 풀리는 경우마다 해집합은 3차원 핵을 평행이동한 아핀 집합이다. 공역의 나머지 한 차원 방향에는 도달하지 못한다.

4.7 직사각형 행렬의 세 가지 차원

$m \times n$ 행렬 A는 $\mathbb{F}^n \to \mathbb{F}^m$의 선형사상을 정의한다. 열공간의 차원을 $\operatorname{rank} A = r$라 하면

$$\dim \ker A = n - r, \qquad r \le \min(m, n).$$

$Ax = b$가 모든 $b \in \mathbb{F}^m$에 대해 풀리려면 $r = m$이어야 한다. 해가 있을 때마다 유일하려면 $r = n$이어야 한다. 두 조건이 동시에 성립하려면 $m = n = r$이어야 한다.

정리 4.18 (행공간과 열공간의 차원) 행렬의 행공간 차원과 열공간 차원은 같고, 소거법의 피벗 수와 같다.

증명. 행 연산은 행공간을 보존한다. 사다리꼴의 영이 아닌 행들은 서로 다른 피벗 위치를 가지므로 독립이며 행공간을 생성한다. 따라서 행공간 차원은 피벗 수 r이다.

행 연산은 열들 사이의 선형관계를 보존한다. 기약 사다리꼴에서 피벗 열은 서로 다른 단위벡터이므로 독립이고, 다른 열은 그 피벗 열들의 결합이다. 같은 선형관계와 독립성이 원래 열들에도 성립하므로 열공간 차원도 r이다. □

따름정리 4.19 (해의 존재 조건) $Ax = b$가 해를 가질 필요충분조건은 $\operatorname{rank} A = \operatorname{rank}[A \mid b]$이다.

증명. 해가 있다는 것은 b가 A의 열공간에 속한다는 뜻이다. 이미 열공간에 있는 벡터를 추가하면 차원이 늘지 않는다. 반대로 차원이 늘지 않았다면 기존 열공간을 포함하는 새 열공간의 차원이 같으므로 두 공간이 같고 b가 기존 공간에 속한다. □

4.8 합성과 역함수

$T : U \to V$, $S : V \to W$가 선형이면 $S \circ T$도 선형이다. 이때

$$\ker T \subseteq \ker(S \circ T), \qquad \operatorname{im}(S \circ T) \subseteq \operatorname{im} S.$$

앞 단계에서 사라진 정보는 뒤 단계에서 되살릴 수 없고, 합성의 출력은 마지막 사상의 상 안에 있어야 한다. 유한차원에서는 $\operatorname{rank}(S \circ T) \le \min(\operatorname{rank} S, \operatorname{rank} T)$이다.

> **예제 4.20 (각 단계는 비영이어도 합성은 0일 수 있다)** $T : \mathbb{R} \to \mathbb{R}^2$, $T(t) = (t, 0)$와 $S : \mathbb{R}^2 \to \mathbb{R}$, $S(x, y) = y$는 모두 영사상이 아니다. 그러나 $S(T(t)) = 0$이므로 합성은 영사상이다. 첫 사상의 상이 둘째 사상의 핵에 들어 있기 때문이다.

> **정리 4.21 (역사상의 선형성)** 전단사 선형사상 $T : V \to W$의 역함수 $T^{-1} : W \to V$도 선형이다. 이러한 사상을 벡터공간의 **동형사상**(*isomorphism*)이라고 한다.

증명. $u = T(x)$, $v = T(y)$라 놓으면 선형성에 의해 $au + bv = T(ax + by)$이다. 양변에 역함수를 적용하면 $T^{-1}(au + bv) = aT^{-1}(u) + bT^{-1}(v)$를 얻는다. □

두 유한차원 공간이 동형일 필요충분조건은 같은 체 위에서 차원이 같다는 것이다. 동형사상은 기저를 기저로 보내므로 차원을 보존한다. 반대로 같은 길이의 기저를 하나씩 대응시키면 기저의 상 지정 정리(정리 4.7)로 동형사상을 만들 수 있다. 그러나 두 공간의 차원이 같다는 사실이 모든 선형사상이 가역이라는 뜻은 아니다. 영사상은 영공간을 제외하면 가역이 아니다.

4.9 선형함수와 초평면

$\ell : V \to \mathbb{F}$인 선형사상을 **선형함수**(*linear functional*) 또는 **선형범함수**라고 한다. 좌표공간에서

$$\ell(x_1, \dots, x_n) = a_1 x_1 + \cdots + a_n x_n$$

는 가장 일반적인 형태다. 표준 기저의 값 $a_j = \ell(e_j)$를 알면 전체 함수가 결정되기 때문이다.

$\ell \neq 0$이면 그 상은 1차원 공간 $\mathbb{F}$ 전체다. 실제로 $\ell(v_0) = c \neq 0$인 벡터가 있으면 임의의 a는 $\ell((a/c)v_0)$로 얻는다. 따라서 $\dim V = n$일 때 비영 선형함수의 핵은 차원 $n - 1$의 부분공간이다. 이를 **초평면**(*hyperplane*)이라고 한다.

> **예제 4.22 (초평면과 그 평행이동)** $\ell(x, y, z) = 2x - y + z$의 핵은 원점을 지나는 평면이다. $\ell(x, y, z) = 5$의 해집합은 그 평면의 평행이동이다. 선형조건 하나가 차원을 하나 줄인다는 말은 그 조건이 실제로 비영일 때의 진술이다. $0x + 0y + 0z = 0$은 아무 차원도 줄이지 않는다.

4.10 연습문제와 해설

연습문제 4.23 $T:\mathbb{R}^2\to\mathbb{R}^2$, $T(x,y)=(x+2y,3x+6y)$의 핵과 상의 기저를 구하라.

풀이. $T(x,y)=(x+2y)(1,3)$이므로 상의 기저는 $(1,3)$이다. 핵은 $x=-2y$이므로 $(-2,1)$이 기저다. 계수와 영차원이 각각 1이며 합은 정의역 차원 2다.

연습문제 4.24 $T:\mathcal{P}_2(\mathbb{R})\to\mathcal{P}_2(\mathbb{R})$, $T(p)=p'$는 단사인가, 전사인가?

풀이. 상수다항식이 핵에 있으므로 단사가 아니다. 상은 일차 이하 다항식으로 이루어져 t^2에 도달하지 못하므로 전사도 아니다. 공역을 $\mathcal{P}_1(\mathbb{R})$로 바꾸면 전사이지만 단사성은 여전히 실패한다.

연습문제 4.25 $T:\mathbb{R}^4\to\mathbb{R}^2$의 영차원이 2인 선형사상을 생각한다. 모든 $b\in\mathbb{R}^2$에 대해 $T(x)=b$가 풀리는가? 그 해는 유일한가?

풀이. 계수는 $4-2=2$이므로 상이 공역 전체이고 모든 b에 대해 풀린다. 핵의 차원이 2이므로 어떤 경우에도 해가 유일하지 않다. 각 해집합은 2차원 아핀 부분공간이다.

연습문제 4.26 $T(1,0)=(1,2)$, $T(0,1)=(3,4)$인 선형사상에서 $T(2,-1)$을 구하라. 여기에 $T(1,1)=(5,6)$이라는 조건을 추가할 수 있는가?

풀이. 선형성으로 $T(2,-1)=2(1,2)-(3,4)=(-1,0)$이다. 또한 $T(1,1)=(1,2)+(3,4)=(4,6)$이어야 하므로 추가 조건은 모순이다. 종속된 입력의 출력은 독립적으로 지정할 수 없다.

연습문제 4.27 유한차원 V에서 선형사상 $T:V\to V$가 단사이면 전사임을 차원 정리로 증명하라. 유한차원 가정이 쓰이는 곳을 밝혀라.

풀이. 단사이므로 핵의 차원은 0이고 차원 정리(정리 4.16)에 의해 상의 차원이 $\dim V$와 같다. 상은 V의 부분공간이므로 같은 유한차원이라는 사실에서 상이 전체임을 얻는다. 무한차원에서는 이 유한한 차원 계산과 같은 차원 부분공간의 동일성 결론을 그대로 사용할 수 없다.

연습문제 4.28 $T(x,y,z)=(x+y,y+z)$에 대해 $T(x,y,z)=(2,3)$의 모든 해를 특정 해와 핵의 합으로 나타내어라.

풀이. 특정 해로 $(2,0,3)$을 택할 수 있다. 핵은 $\operatorname{span}((1,-1,1))$이므로 모든 해는 $(2,0,3)+t(1,-1,1)$이다. 직접 대입하면 첫 출력은 $2+t-t=2$, 둘째는 $-t+3+t=3$이다.

선형사상은 좌표를 선택하기 전에도 존재한다. 기저를 고르면 행렬이 생기며, 기저를 바꾸면 같은 사상이 다른 행렬로 보인다. 다음 장은 이 관계를 정확한 변환 공식으로 정리한다(제7권 제5장).

제 5 장

행렬표현과 기저변환

개요 행렬표현은 유한차원 벡터공간 사이의 선형사상을 정의역과 공역에 각각 기저를 고정하여 수 배열로 나타내는 대응이고, 기저변환은 같은 선형사상을 다른 기저로 표현할 때 행렬이 어떻게 바뀌는지를 다스리는 규칙이다. 이 장은 기저를 고정한 선형사상의 행렬을 세우는 법에서 출발하여, 행렬곱이 사상의 합성을 그대로 나타낸다는 사실, 가역행렬과 연립방정식의 관계, 직사각형 행렬의 한쪽 역, 기저변환에 따른 행렬의 변화, 전치·대각합 같은 불변량, 블록 구조를 이용한 계산까지 차례로 다룬다. 선형사상 자체는 기저 선택과 무관하지만 그것을 나타내는 행렬의 성분은 기저에 따라 달라지므로, 두 층위를 구분하는 것이 이 장 전체의 핵심이다. 선행 지식: 기저와 좌표, 선형사상, 핵과 상. 모든 행렬의 행 수와 열 수를 적어 가며 계산한다.

선형사상 자체와 그것을 나타내는 행렬은 구분된다. 같은 평면의 회전을 동서·남북 방향으로 측정할 수도 있고 다른 두 기저 방향으로 측정할 수도 있다. 사상이 같아도 좌표 선택에 따라 행렬의 성분은 바뀐다. 반대로 행렬의 성분이 다르다는 이유만으로 사상의 본질이 다르다고 판단할 수는 없다.

이 장에서는 열벡터를 기본 약속으로 사용한다. 따라서 행렬은 좌표열의 왼쪽에서 곱하고, 합성에서는 먼저 작용하는 사상의 행렬이 오른쪽에 놓인다. 이 약속을 처음부터 끝까지 유지하면 기저변환 공식의 역행렬 위치를 외우지 않고도 유도할 수 있다.

5.1 기저벡터의 상을 열로 세우기

$T : V \to W$가 선형이고 $\mathcal{B} = (b_1, \dots, b_n)$, $\mathcal{C} = (c_1, \dots, c_m)$가 각각 기저라고 하자. 각 $T(b_j)$를 출력 기저로 나타내어

$$T(b_j) = \sum_{i=1}^{m} a_{ij} c_i$$

라 쓰면 $m \times n$ 행렬 $A = (a_{ij})$를 얻는다. 이를 **행렬표현**(*matrix representation*) $[T]_{\mathcal{C} \leftarrow \mathcal{B}}$라고 쓴다. 화살표는 입력 기저에서 출력 기저로의 방향을 나타낸다.

정리 5.1 위 행렬은 모든 $v \in V$에 대해

$$[T(v)]_{\mathcal{C}} = A\,[v]_{\mathcal{B}} \tag{5.1}$$

를 만족하는 유일한 행렬이다.

증명. $v = \sum_j x_j b_j$라 쓰면 $T(v) = \sum_j x_j T(b_j) = \sum_i \bigl(\sum_j a_{ij} x_j\bigr) c_i$이다. 따라서 출력의 i번째 좌표는 행렬곱의 i번째 성분과 같다. 또 입력 좌표를 e_j로 택하면 j번째 열이 $[T(b_j)]_{\mathcal{C}}$여야 하므로 유일하다. □

예제 5.2 (직사각형 미분행렬) $D : \mathcal{P}_2(\mathbb{R}) \to \mathcal{P}_1(\mathbb{R})$에 입력 기저 $(1, t, t^2)$, 출력 기저 $(1, t)$를 사용하자. $D1 = 0$, $Dt = 1$, $Dt^2 = 2t$이므로

$$[D] = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

$[2 + 3t + 4t^2] = (2, 3, 4)^{\mathsf{T}}$를 곱하면 $(3, 8)^{\mathsf{T}}$를 얻고 이는 미분한 다항식 $3 + 8t$의 좌표다. 실제로 $2 + 3t + 4t^2$를 미분하면 $3 + 8t$이므로 식 (5.1)과 일치한다. 행렬 크기 2×3은 출력 차원과 입력 차원을 각각 나타낸다.

주의 (행과 열의 혼동). 열을 만드는 데 사용한 벡터는 입력 기저의 상이다. 행렬의 각 행을 $T(b_j)$라고 적으면 대체로 전치된 행렬을 얻게 된다. 입력 표준벡터 e_j를 곱해 실제로 j번째 열이 나오는지 확인하면 이 혼동을 줄일 수 있다.

5.2 행렬곱은 합성을 표현한다

$T : U \to V$, $S : V \to W$를 각각 행렬 B, A로 표현하면

$$[S(T(u))] = A(B[u]) = (AB)[u]$$

이다. 따라서 합성 $S \circ T$의 행렬은 AB다. A가 $p \times m$, B가 $m \times n$이면 AB는 $p \times n$이며,

$$(AB)_{ij} = \sum_{k=1}^{m} a_{ik} b_{kj}$$

로 정의된다. 가운데 차원 m이 맞아야 한다는 조건은 첫 출력이 다음 입력으로 들어가야 한다는 조건이다.

예제 5.3 (직사각형 곱의 계산)

$$A = \begin{pmatrix} 1 & 0 & 2 \\ -1 & 3 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \\ 2 & -1 \end{pmatrix}$$

이면

$$AB = \begin{pmatrix} 5 & 0 \\ 1 & 0 \end{pmatrix}.$$

예를 들어 둘째 행 첫째 열은 $(-1)\cdot 1 + 3 \cdot 0 + 1 \cdot 2 = 1$이다. B는 두 성분을 세 성분으로, A는 세 성분을 다시 두 성분으로 바꾸므로 합성은 2×2 행렬이다. BA도 이 예에서는 정의되지만 크기는 3×3이다.

행렬곱은 결합법칙 $(AB)C = A(BC)$와 분배법칙을 만족한다. 결합법칙은 유한합의 순서를 바꾸거나 선형사상 합성의 결합법칙으로 확인할 수 있다. 그러나 교환법칙 $AB = BA$는 일반적으로 성립하지 않는다.

예제 5.4 (순서를 바꾸면 다른 전단)

$$A=\begin{pmatrix}1&1\\0&1\end{pmatrix},\qquad B=\begin{pmatrix}1&0\\1&1\end{pmatrix}$$

에 대해

$$AB=\begin{pmatrix}2&1\\1&1\end{pmatrix},\qquad BA=\begin{pmatrix}1&1\\1&2\end{pmatrix}.$$

두 사상은 각각 한 방향으로 다른 좌표를 더하는 전단이다. 어느 전단을 먼저 적용하는지가 최종 결과에 영향을 준다.

5.3 항등행렬·거듭제곱·행렬 다항식

$n\times n$ **항등행렬** I_n은 대각성분이 1이고 나머지가 0인 행렬이다. $I_mA=A=AI_n$이지만 왼쪽과 오른쪽 항등행렬의 크기가 다를 수 있다. 정사각행렬 A에는 $A^0=I$, $A^{k+1}=A^kA$로 거듭제곱을 정의한다.

행렬 다항식 $p(A)=c_0I+c_1A+\cdots+c_dA^d$도 정의된다. 같은 행렬의 거듭제곱끼리는 교환하지만 서로 다른 행렬들이 모두 교환하는 것은 아니다. 따라서 $(A+B)^2=A^2+2AB+B^2$는 $AB=BA$ 같은 조건 없이 사용할 수 없다. 일반적으로 중간항은 $AB+BA$이다.

예제 5.5 (유한한 기하급수)

$$N=\begin{pmatrix}0&1&0\\0&0&1\\0&0&0\end{pmatrix}$$

이면 N^2의 $(1,3)$ 성분만 1이고 $N^3=0$이다. 따라서

$$(I-N)(I+N+N^2)=I-N^3=I.$$

오른쪽 순서로 곱해도 같으므로 $(I-N)^{-1}=I+N+N^2$이다. 무한급수의 수렴을 사용한 것이 아니라 유한한 항등식이다.

일반적인 $I-A$에 대해 무작정 $I+A+A^2+\cdots$를 역행렬이라고 쓸 수는 없다. 그때에는 수렴 조건이 필요하다. 예 5.5처럼 거듭제곱이 유한 번 만에 실제로 0이 되는 **멱영**(*nilpotent*) 행렬에서는 이러한 문제가 없다.

5.4 역행렬과 연립방정식

정의 5.6 정사각행렬 $A\in M_n(\mathbb{F})$에 대해 $AB=BA=I_n$을 만족하는 B가 있으면 A는 **가역**(*invertible*)이라고 하며 $B=A^{-1}$로 쓴다.

역행렬은 존재하면 유일하다. B,C가 둘 다 역행렬이면 $B=B(AC)=(BA)C=C$이다. 유한차원 정사각행렬에서는 $AB=I$ 한쪽 조건만으로도 가역성을 얻는다. 대응하는 사상 A가 전사

이므로 같은 차원의 정의역과 공역 사이에서 단사이고, 따라서 전단사이기 때문이다. 이 결론을 직사각형에 그대로 적용하면 안 된다.

예제 5.7 (역행렬 계산과 검산)

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}$$

를 곱하면 $AB = BA = I_2$이다. 따라서 $Ax = (3,2)^{\mathsf{T}}$의 해는

$$x = B\begin{pmatrix} 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

여러 상수항을 반복해서 풀 때 같은 역행렬을 사용할 수 있지만, 실제 수치 계산에서는 역행렬 전체를 직접 만드는 대신 분해를 재사용하는 방법이 더 적절할 수 있다.

확대행렬 $[A \mid I]$를 행 연산으로 $[I \mid B]$로 만들었다면 $B = A^{-1}$이다. 각 기본 행 연산은 왼쪽에서 기본행렬을 곱하는 연산이다. 이들을 모두 곱한 행렬을 E라 하면 $EA = I$이고 오른쪽은 $EI = E$이므로 $B = E$이다. 반대로 왼쪽을 I로 만들 수 없다면 피벗이 없는 열이 있으므로 가역이 아니다.

예제 5.8 (증대행렬의 실제 소거)

$$\left[\begin{array}{cc|cc} 2 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{array}\right] \xrightarrow{R_1 \leftrightarrow R_2} \left[\begin{array}{cc|cc} 1 & 1 & 0 & 1 \\ 2 & 1 & 1 & 0 \end{array}\right]$$

에서 $R_2 \leftarrow R_2 - 2R_1$, $R_2 \leftarrow -R_2$, $R_1 \leftarrow R_1 - R_2$를 차례로 적용하면

$$\left[\begin{array}{cc|cc} 1 & 0 & 1 & -1 \\ 0 & 1 & -1 & 2 \end{array}\right]$$

를 얻는다. 오른쪽은 예 5.7에서 앞서 검산한 역행렬과 같다.

5.5 직사각형의 왼쪽 역과 오른쪽 역

$m \times n$ 행렬 A에 대해 $LA = I_n$이면 L을 **왼쪽 역**, $AR = I_m$이면 R을 **오른쪽 역**이라고 한다. 왼쪽 역이 있으면 $Ax = 0$에서 $x = LAx = 0$이므로 A는 단사다. 오른쪽 역이 있으면 모든 b가 $A(Rb)$이므로 전사다.

유한차원에서는 단사 사상은 왼쪽 역을, 전사 사상은 오른쪽 역을 갖는다. 단사인 경우 상의 기저를 공역의 기저로 확장하여 상에서는 원래 입력으로 되돌리고 보충 기저에서는 0으로 보내면 된다. 전사인 경우 공역 기저의 원상들을 하나씩 골라 그에 따라 선형사상을 정의하면 된다. 두 역은 일반적으로 유일하지 않다.

예제 5.9 (한쪽 곱만 항등이 되는 경우)

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}$$

이면

$$AB = I_2, \qquad BA = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \neq I_3.$$

A는 좌표를 버리고 B는 마지막 성분을 0으로 채운다. 이미 버린 세 번째 좌표는 복원되지 않는다.

따라서 "역행렬을 곱해 풀면 된다"는 말은 정사각형 가역행렬인지 먼저 확인해야 한다. 직사각형의 해 문제는 존재와 유일성을 따로 조사하고, 필요한 경우 최소제곱이나 최소노름 조건을 추가하여 다룬다(제7권 제8장).

5.6 좌표변환 행렬의 방향

같은 공간 V의 옛 기저를 $\mathcal{B}$, 새 기저를 $\mathcal{B}'$라 하자. 새 기저벡터들을 옛 좌표로 쓴 열들을 모아 P를 만든다.

$$P = \big[\,[b'_1]_{\mathcal{B}} \;\cdots\; [b'_n]_{\mathcal{B}}\,\big].$$

그러면 모든 v에 대해

$$[v]_{\mathcal{B}} = P\,[v]_{\mathcal{B}'}, \qquad [v]_{\mathcal{B}'} = P^{-1}\,[v]_{\mathcal{B}}.$$

새 좌표를 옛 좌표로 바꾸는 행렬이 P다. "기저를 바꾸는 행렬"이라는 말만으로 방향을 생략하면 역행렬 위치를 혼동하기 쉽다.

예제 5.10 (두 대각선 방향의 기저변환) $\mathcal{B}$를 $\mathbb{R}^2$의 표준 기저, $\mathcal{B}' = ((1,1),(1,-1))$라 하면

$$P = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad P^{-1} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

$v = (3,1)$에 대해 새 좌표는 $(2,1)^{\mathsf{T}}$이다. 실제로 $2(1,1) + 1(1,-1) = (3,1)$이다. 기저벡터의 길이가 1이 아니므로 $P^{-1} = P^{\mathsf{T}}$라고 할 수는 없다.

5.7 입력과 출력의 기저를 함께 바꾸기

$A = [T]_{C \leftarrow \mathcal{B}}$라 하자. 입력 기저변환 P와 출력 기저변환 Q를

$$[v]_{\mathcal{B}} = P\,[v]_{\mathcal{B}'}, \qquad [w]_{C} = Q\,[w]_{C'}$$

로 정의한다. 그러면

$$Q\,[T(v)]_{C'} = A\,P\,[v]_{\mathcal{B}'}$$

이므로 새 행렬은

$$A' = Q^{-1}AP.$$

$T : V \to V$에서 입력과 출력에 같은 기저를 사용하면 $Q = P$가 되어 $A' = P^{-1}AP$이다. 이러한 관계를 **닮음**(*similarity*)이라고 한다.

핵심 수식

$$[T(v)]_{\mathcal{C}} = A[v]_{\mathcal{B}}, \tag{5.2}$$

$$[v]_{\mathcal{B}} = P[v]_{\mathcal{B}'}, \qquad [v]_{\mathcal{B}'} = P^{-1}[v]_{\mathcal{B}}, \tag{5.3}$$

$$A' = Q^{-1}AP. \tag{5.4}$$

예제 5.11 (반사를 대각행렬로 보기) $T(x,y) = (y,x)$의 표준 행렬은 $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$이다. 앞의 기저 $b_1' = (1,1)$, $b_2' = (1,-1)$를 사용하면 $T(b_1') = b_1'$, $T(b_2') = -b_2'$이므로

$$P^{-1}AP = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

같은 반사인데 기저를 잘 고르면 두 방향을 유지하거나 부호만 바꾸는 단순한 형태로 보인다.

예제 5.12 (서로 다른 차원의 기저변환) $T(x,y) = (x+y, 2x, y)$의 표준 행렬은

$$A = \begin{pmatrix} 1 & 1 \\ 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

입력 새 기저를 $(1,1), (1,-1)$로, 출력 새 기저를 $d_1 = (1,0,0)$, $d_2 = (1,1,0)$, $d_3 = (0,0,1)$로 택하면

$$P = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad Q = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$Q^{-1}AP = \begin{pmatrix} 0 & -2 \\ 2 & 2 \\ 1 & -1 \end{pmatrix}.$$

첫 열은 $T(1,1) = (2,2,1) = 2d_2 + d_3$, 둘째 열은 $T(1,-1) = (0,2,-1) = -2d_1 + 2d_2 - d_3$로 검산된다. 입력과 출력의 차원이 다르므로 닮음 공식 하나로 쓰지 않는다.

가역행렬을 왼쪽이나 오른쪽에 곱해도 계수는 변하지 않는다. 오른쪽의 가역변환은 가능한 모든 입력을 다시 매개화하고, 왼쪽의 가역변환은 상을 동형으로 옮기기 때문이다. 그러나 개별 열공간이나 핵의 좌표 위치는 바뀔 수 있다. 보존되는 차원과 변하는 좌표를 구분한다.

5.8 전치·켤레전치와 대각합

전치행렬 A^{T}는 행과 열을 바꾸어 $(A^{\mathsf{T}})_{ij} = a_{ji}$로 정의한다. 복소수 행렬의 **켤레전치**는 $A^{*} = \overline{A}^{\mathsf{T}}$다. 복소수에서는 전치와 켤레전치가 다르다.

$$(AB)^{\mathsf{T}} = B^{\mathsf{T}}A^{\mathsf{T}}, \qquad (AB)^{*} = B^{*}A^{*}.$$

첫 항등식은 성분을 계산하면 $\sum_{k} a_{jk}b_{ki}$가 양쪽에 나타남을 확인할 수 있다. 순서가 뒤집힌다는 점이 중요하다.

> **예제 5.13**
> $$A = \begin{pmatrix} 1 & i \\ 0 & 1-i \end{pmatrix} \Longrightarrow A^{\mathsf{T}} = \begin{pmatrix} 1 & 0 \\ i & 1-i \end{pmatrix}, \qquad A^{*} = \begin{pmatrix} 1 & 0 \\ -i & 1+i \end{pmatrix}.$$

내적과 직교성을 다룰 때 복소수에서는 켤레전치를 사용해야 하는 경우가 많다(제7권 제8장). 실수 행렬에서는 두 연산이 같아 이 차이가 가려져 있다.

정사각행렬의 **대각합**은 $\operatorname{tr} A = \sum_{i} a_{ii}$다. A가 $m \times n$, B가 $n \times m$이면

$$\operatorname{tr}(AB) = \sum_{i}\sum_{j} a_{ij}b_{ji} = \sum_{j}\sum_{i} b_{ji}a_{ij} = \operatorname{tr}(BA).$$

두 곱의 크기가 달라도 대각합이라는 스칼라는 같다. 이 식은 $AB = BA$를 뜻하지 않는다. 또한 P가 가역이면 $\operatorname{tr}(P^{-1}AP) = \operatorname{tr} A$이므로 대각합은 기저변환 아래 불변이다.

5.9 블록 행렬로 큰 계산을 조직하기

큰 행렬을 작은 직사각형 블록으로 나눌 수 있다. 블록의 크기가 맞는다면 행렬곱은 블록 수준에서도 같은 규칙을 따른다. 예를 들어

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} E & F \\ G & H \end{pmatrix} = \begin{pmatrix} AE+BG & AF+BH \\ CE+DG & CF+DH \end{pmatrix}.$$

각 블록도 행렬이므로 곱의 순서를 유지해야 한다. 실수 계산처럼 무심코 순서를 바꾸면 틀린다.

대각 블록 A, D가 가역인 상삼각 블록 행렬은

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}^{-1} = \begin{pmatrix} A^{-1} & -A^{-1}BD^{-1} \\ 0 & D^{-1} \end{pmatrix}$$

를 역행렬로 갖는다. 오른쪽 위 블록은 $A(-A^{-1}BD^{-1}) + BD^{-1} = 0$이 되고 나머지 대각 블록은 항등이 되는 것으로 검산할 수 있다. 역행렬을 블록마다 따로 취하는 것만으로는 가운데 보정항을 얻을 수 없다.

역사 (행렬 연산의 기원). Cayley는 1858년 논문 *A Memoir on the Theory of Matrices*에서 선형치환의 합성에 대응하도록 행렬의 덧셈과 곱셈을 정의하고, 행렬 자체를 독립된 대수적 대상으로 다루었다. 이 장에서 행렬곱을 합성으로 정의한 방식은 그 관점을 그대로 이어받은 것이다.

5.10 연습문제와 해설

연습문제 5.14 $T:\mathbb{R}^2\to\mathbb{R}^3$, $T(x,y)=(2x-y,x+3y,4y)$의 표준 행렬을 구하라.

풀이. $T(e_1)=(2,1,0)$, $T(e_2)=(-1,3,4)$를 열로 놓으면 $\begin{pmatrix}2&-1\\1&3\\0&4\end{pmatrix}$이다. 입력 차원 2, 출력 차원 3이므로 크기는 3×2다.

연습문제 5.15 가역행렬 A,B에 대해 $(AB)^{-1}$을 A^{-1},B^{-1}로 나타내고 순서를 설명하라.

풀이. $(AB)^{-1}=B^{-1}A^{-1}$이다. $(AB)(B^{-1}A^{-1})=AIA^{-1}=I$이고 반대 곱도 I이다. 합성을 되돌리려면 마지막에 적용한 변환부터 거꾸로 되돌린다.

연습문제 5.16 기저 $\mathcal{B}=((1,0),(1,2))$에 대한 $(4,6)$의 좌표를 구하라.

풀이. $a(1,0)+b(1,2)=(a+b,2b)$이므로 $b=3$, $a=1$이다. 새 기저를 표준 좌표로 모은 행렬은 $P=\begin{pmatrix}1&1\\0&2\end{pmatrix}$이고 $P^{-1}(4,6)^{\mathsf T}=(1,3)^{\mathsf T}$로도 확인할 수 있다.

연습문제 5.17 A가 5×3 행렬이다. A에 왼쪽 역이 있을 수 있는가? 오른쪽 역이 있을 수 있는가?

풀이. 열들이 독립이면 계수가 3이므로 왼쪽 역이 있다. 예를 들어 위쪽 세 행이 I_3, 아래 두 행이 0인 행렬이 그렇다. 오른쪽 역은 계수가 5여야 하지만 계수는 최대 3이므로 불가능하다.

연습문제 5.18 $A=\begin{pmatrix}1&2\\0&3\end{pmatrix}$에 대해 A^2를 계산하고 $A^2-4A+3I$를 구하라.

풀이. $A^2=\begin{pmatrix}1&8\\0&9\end{pmatrix}$이다. 따라서 $A^2-4A+3I=0$이다. 행렬 다항식을 계산할 때 상수항 3은 스칼라를 행렬에 그대로 더하는 것이 아니라 $3I$를 뜻한다.

연습문제 5.19 두 닮은 행렬의 대각합이 같음을 대각합의 곱 순환 성질로 증명하라. 같은 대각합이면 닮았다고 할 수 있는가?

풀이. $B=P^{-1}AP$이면 $\operatorname{tr}B=\operatorname{tr}(PP^{-1}A)=\operatorname{tr}A$이다. 역은 거짓이다. 영행렬과 $\begin{pmatrix}0&1\\0&0\end{pmatrix}$은 대각합이 모두 0이지만 계수가 각각 0과 1이므로 닮지 않았다.

기저변환에 따라 변하지 않는 양을 찾으면 행렬의 본질을 조사할 수 있다. 다음 장에서는 부피의 배율과 가역성을 연결하는 행렬식을 다룬다.

제 6 장

행렬식: 가역성 · 부피 · 방향

개요 행렬식은 정사각행렬에 수 하나를 대응시키는 함수이며, 그 값은 선형변환이 부피를 얼마나 바꾸는지와 관련되고 0인지 아닌지로 가역성을 판정한다. 이 장은 2×2 행렬에서 넓이로 출발하여 일반 정의와 교대다중선형성, 소거법에 따른 행렬식의 변화, 곱셈 공식, 가역성 판정 정리, 여인수 전개, 수반행렬과 Cramer 공식, 블록 구조와 계수 1 갱신, 실수 부피와 복소수 행렬식의 차이를 차례로 세운다. 행렬식만으로 행렬 전체를 알 수는 없다는 점, 곧 서로 다른 많은 변환이 같은 부피 배율을 가질 수 있다는 점을 거듭 확인한다. 선행 지식: 행렬곱, 기본 행 연산, 선형독립, 가역행렬. 행렬식은 정사각행렬에 정의한다.

행렬식 계산을 처음 배울 때 작은 행렬의 공식을 외우는 데 머무르기 쉽다. 더 유용한 관점은 각 행 또는 열에 대해 선형이며, 같은 방향이 반복되면 0이 된다는 구조를 이해하는 것이다. 이 구조가 소거법, 곱셈 공식, 역행렬, 고유값과 연결된다.

6.1 이차원에서 출발하기

정의 6.1 2×2 행렬 $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$의 **행렬식**(*determinant*)은 $\det A = ad-bc$이다.

열벡터 $(a,c)^{\mathsf T}$, $(b,d)^{\mathsf T}$가 만드는 평행사변형의 넓이는 $|ad-bc|$다. 부호는 두 열의 순서에 따른 방향을 구분한다. 한 열이 다른 열의 상수배이면 넓이가 0이고 두 방향이 한 직선으로 무너진다.

예제 6.2 (넓이와 부호)

$$A=\begin{pmatrix} 2 & 1 \\ 0 & 3 \end{pmatrix}$$

의 행렬식은 6이다. 밑변의 길이 2와 높이 3인 평행사변형의 넓이와 같다. 두 열을 바꾸면 행렬식은 -6이지만 넓이는 여전히 6이다. 순서와 부피를 구분하기 위해 절댓값이 필요하다.

예제 6.3 (넓이는 보존해도 길이는 바뀐다) $S=\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$는 행렬식이 1인 전단이다. e_2를 $(k,1)$로 보내므로 보통 길이와 각도는 바뀌지만 넓이는 보존한다. 행렬식의 절댓값이 1이라는 조건만으로 직교변환이라고 할 수 없다.

6.2 일반적인 정의와 교대다중선형성

n개의 원소를 순열하는 집합을 S_n이라 하자. 순열 σ의 부호를 $\operatorname{sgn}(\sigma)$로 쓰면 행렬식의 일반 정의는

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)}$$

이다. 각 항은 서로 다른 행과 서로 다른 열에서 성분을 하나씩 고른 곱이다. 순열 부호는 두 원소의 교환을 한 번 할 때마다 바뀐다.

이 정의에서 다음 성질을 얻는다.

(1) 다른 행을 고정하면 한 행에 대해 선형이다. 열에 대해서도 마찬가지다.

(2) 두 행 또는 두 열을 바꾸면 부호가 바뀐다.

(3) 두 행 또는 두 열이 같으면 행렬식은 0이다.

(4) $\det I_n = 1$이다.

같은 행이 있을 때 0이라는 성질을 **교대성**이라고 한다. 특성 2인 체에서도 순열항들의 대응을 통해 교대성은 성립한다. 단순히 $d = -d$이므로 $d = 0$이라고 하는 논증은 2로 나눌 수 없는 체에서는 충분하지 않다.

> **보조정리 6.4** 열벡터들에 관한 교대다중선형 함수는 표준 기저 목록에서의 값 하나로 결정된다. 특히 그 값이 1이면 행렬식이다.

증명. 각 열을 표준 기저의 선형결합으로 쓰고 다중선형성으로 전개한다. 어떤 표준 기저벡터가 두 번 선택된 항은 교대성으로 0이다. 살아남는 항에서는 $e_1, \dots, e_n$이 한 번씩 등장하며, 그 순서의 부호와 표준 기저에서의 함수값을 곱하면 된다. 따라서 모든 값이 하나의 기준값으로 결정된다. $\square$

이 원리는 부피의 배율을 일반화하는 데도 쓰인다. 각 방향에 대해 선형으로 변하고 같은 방향이 반복되면 부피가 0이 되는 함수는, 단위 정육면체의 부피를 1로 정하면 행렬식과 같은 구조를 갖는다.

6.3 소거법과 행렬식의 변화

기본 행 연산에 따른 변화는 다음과 같다.

표 6.1 기본 행 연산과 행렬식의 변화

행 연산	행렬식에 미치는 효과
두 행 교환	$\det$에 -1을 곱함
한 행에 c를 곱함	$\det$에 c를 곱함
한 행에 다른 행의 c배를 더함	$\det$ 불변

마지막 성질은 바꾼 행에 대한 선형성으로 전개하면 알 수 있다. 원래 행렬식에, 다른 두 행이 같아지는 행렬식의 c배가 더해지는데 그 항은 0이다.

명제 6.5 상삼각 또는 하삼각 행렬의 행렬식은 대각성분의 곱이다.

증명. 상삼각 행렬에서는 $i > j$인 성분이 0이다. 순열 정의에서 비영 항을 얻으려면 모든 i에 대해 $\sigma(i) \geq i$여야 한다. 양변을 합하면 등호가 같으므로 모든 위치에서 $\sigma(i) = i$여야 한다. 따라서 항등순열의 항 $a_{11}\cdots a_{nn}$만 남는다. 하삼각도 같은 방식이다. □

예제 6.6 (소거로 계산하는 3차 행렬식)

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 3 & 1 \\ 2 & 0 & 1 \end{pmatrix}$$

에서 $R_3 \leftarrow R_3 - 2R_1$을 적용하면 셋째 행이 $(0,-4,1)$이다. 이어 $R_3 \leftarrow R_3 + \frac{4}{3}R_2$를 적용하면 셋째 행은 $(0,0,7/3)$이다. 두 연산 모두 행렬식을 보존하므로

$$\det A = 1 \cdot 3 \cdot \frac{7}{3} = 7.$$

분수가 불편하면 여인수 전개로 같은 값을 구할 수도 있다(예 6.11).

행 하나의 상수배와 행렬 전체의 상수배를 구분해야 한다. $n \times n$ 행렬의 모든 행에 c가 곱해지므로 $\det(cA) = c^n \det A$이다. 예를 들어 $\det(2I_3) = 8$이지 2가 아니다. 행 연산 도중 피벗을 1로 정규화했다면 그때 나눈 상수를 반드시 추적해야 한다.

6.4 행렬식의 곱셈 공식

정리 6.7 같은 크기의 정사각행렬 A, B에 대해

$$\det(AB) = \det A \det B.$$

또한 $\det A^{\mathsf{T}} = \det A$이다.

증명. B의 열들을 $b_1, \dots, b_n$이라 하자. AB의 열들은 $Ab_1, \dots, Ab_n$이다. 함수

$$F(b_1, \dots, b_n) = \det(Ab_1, \dots, Ab_n)$$

는 교대다중선형이며 표준 기저에서의 값은 $\det A$다. 앞의 유일성 보조정리(보조정리 6.4)에 의해 $F(B) = \det A \det B$이다. 전치에 관한 식은 순열 정의에서 순열을 역순열로 바꾸면 얻는다. 순열과 역순열의 부호는 같다. □

예제 6.8 (곱과 합은 다르다) $A = B = I_2$라 하면 $\det(AB) = 1 = \det A \det B$이다. 그러나

$$\det(A + B) = \det(2I_2) = 4 \neq 2 = \det A + \det B.$$

행렬식은 행렬 전체에 대한 선형함수가 아니라 다른 행 또는 열을 고정했을 때 한 행 또는 열에 대해 선형이다.

가역행렬 P에 대해 $\det(P^{-1}AP) = \det A$이므로 행렬식은 닮음 아래 불변이다. $\det(P^{-1}) = 1/\det P$이기 때문이다. 기저가 바뀌어도 선형변환의 부피 배율은 달라지지 않는다는 해석과 일치한다.

6.5 가역성 판정과 행렬식 0의 의미

정리 6.9 $A \in M_n(\mathbb{F})$에 대해 다음 조건들은 동치다.

(1) A가 가역이다.

(2) $\det A \neq 0$이다.

(3) A의 열들이 독립이다.

(4) $\operatorname{rank} A = n$이다.

(5) 모든 $b \in \mathbb{F}^n$에 대해 $Ax = b$가 유일한 해를 갖는다.

증명. 열의 독립성, 계수, 유일한 해와 가역성의 관계는 앞 장들의 선형사상 결과(제7권 제3장, 제7권 제4장)에서 얻는다. 가역이면 $1 = \det I = \det A \det A^{-1}$이므로 행렬식은 비영이다. 가역이 아니면 열들이 종속이고, 한 열을 나머지의 결합으로 쓸 수 있다. 그 열에 대해 다중선형성을 적용하면 반복되는 열을 가진 항들만 남으므로 행렬식은 0이다. $\square$

예제 6.10 (매개변수와 특이행렬)

$$A_t = \begin{pmatrix} t & 1 \\ 1 & t \end{pmatrix}$$

의 행렬식은 $t^2 - 1$이다. 실수 또는 복소수 위에서 $t \neq \pm 1$이면 가역이고 $t = 1, -1$이면 특이하다. $t = 1$에서 핵은 $(1, -1)$ 방향이고 $t = -1$에서는 $(1, 1)$ 방향이다. 행렬식은 어느 방향이 사라지는지는 직접 알려 주지 않으므로 핵 계산이 추가로 필요하다.

행렬식 0은 출력의 n차원 부피가 0이라는 뜻이지 모든 출력이 영벡터라는 뜻은 아니다. 평면을 직선으로 사영하는 행렬은 행렬식이 0이지만 많은 벡터를 비영벡터로 보낸다. 또한 행렬식이 매우 작다는 사실만으로 수치적인 민감도를 완전히 판단할 수는 없다. 단위를 바꾸어 행렬 전체를 작게 만들면 행렬식도 작아지기 때문이다.

6.6 소행렬·여인수 전개

A에서 i행과 j열을 제거한 $(n-1)\times(n-1)$ 행렬을 A_{ij}라고 하자. **여인수**는 $C_{ij} = (-1)^{i+j}\det A_{ij}$다. 한 행 또는 한 열을 고정하면

$$\det A = \sum_{j=1}^{n} a_{ij} C_{ij} = \sum_{i=1}^{n} a_{ij} C_{ij}$$

로 전개할 수 있다. 첫 합에서는 i가 고정되고 둘째 합에서는 j가 고정된다. 둘을 한꺼번에 모든 i, j에 대해 더하는 공식이 아니다.

예제 6.11 (0이 많은 행을 이용하기) 앞의 $A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 3 & 1 \\ 2 & 0 & 1 \end{pmatrix}$를 첫 행으로 전개하면

$$\det A = 1\begin{vmatrix} 3 & 1 \\ 0 & 1 \end{vmatrix} - 2\begin{vmatrix} 0 & 1 \\ 2 & 1 \end{vmatrix} + 0 = 3 - 2(-2) = 7.$$

부호는 첫 행에서 $+, -, +$ 순서다. 0이 많은 행이나 열을 택하면 계산할 소행렬의 수를 줄일 수 있다.

n이 커질수록 순열 정의와 반복적인 여인수 전개는 많은 연산을 요구한다. 정의를 이해하고 작은 예를 계산할 때 유용하지만, 큰 행렬의 실제 계산에는 소거법이나 분해를 사용한다. 이론적 정의와 효율적인 알고리즘은 서로 다른 역할을 한다.

6.7 수반행렬과 Cramer 공식

여인수들을 전치하여 놓은 행렬을 고전적 **수반행렬**이라 하고 $\operatorname{adj}(A) = (C_{ji})$로 쓴다. 복소 내적에서의 수반 A^{*}와 이름이 비슷하지만 다른 연산이다.

정리 6.12 정사각행렬 A에 대해

$$A\operatorname{adj}(A) = \operatorname{adj}(A)A = (\det A) I.$$

따라서 $\det A \neq 0$이면 $A^{-1} = \operatorname{adj}(A)/\det A$이다.

증명. 곱의 (i,j) 성분은 $\sum_{k} a_{ik} C_{jk}$이다. $i = j$이면 i행 여인수 전개로 $\det A$다. $i \neq j$이면 j행을 i행으로 바꾼 행렬의 여인수 전개이며, 같은 두 행을 가져 0이다. 다른 곱도 열에 관한 같은 논증으로 보인다. □

예제 6.13 (2차 역행렬 공식) $ad - bc \neq 0$일 때

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

대각성분을 바꾸고 나머지 두 성분의 부호를 바꾸는 규칙은 수반행렬 공식의 특수한 경우다. 분모가 0이면 이 식을 사용할 수 없다.

정리 6.14 (Cramer 공식) A가 가역이고 $Ax = b$라 하자. A의 j번째 열을 b로 바꾼 행렬을 $A^{(j)}$라 하면

$$x_j = \frac{\det A^{(j)}}{\det A}.$$

증명. A의 열들을 $a_1, \dots, a_n$이라 하면 $b = \sum_{k} x_k a_k$이다. $A^{(j)}$의 j열을 이 결합으로 전개하면 $k \neq j$인 항은 같은 열이 반복되어 0이다. $k = j$인 항만 남아 $\det A^{(j)} = x_j \det A$이다. □

예제 6.15 $2x+y=3$, $x+3y=4$에서 $\det A = 5$이다. 첫 열을 상수항으로 바꾼 행렬식은 $3\cdot 3 - 4\cdot 1 = 5$, 둘째 열을 바꾼 행렬식도 $2\cdot 4 - 1\cdot 3 = 5$이므로 $x=y=1$이다. 대입하면 원래 두 식을 만족한다.

역사 (행렬식 개념의 형성). Cramer는 1750년에 연립방정식의 풀이 공식을 발표했고, Cauchy는 1812년의 논문에서 $\det(AB)=\det A\det B$를 증명하며 행렬식을 지금과 같은 뜻으로 다루었다. 행렬 자체보다 행렬식이 먼저 체계적으로 연구된 것이다.

6.8 블록 구조와 계수 1 갱신

정사각 대각 블록을 갖는 블록 상삼각 행렬은

$$\det\begin{pmatrix} B & C \\ 0 & D \end{pmatrix} = \det B \det D$$

를 만족한다. 순열 정의에서 아래쪽 행들이 위쪽 열을 선택하면 0이 되므로 비영 항은 두 대각 블록 안의 순열로 나뉜다. B, D의 가역성을 가정할 필요는 없다.

명제 6.16 (계수 1 갱신의 작은 행렬식 공식) 열벡터 $u, v \in \mathbb{F}^n$에 대해

$$\det(I + uv^{\mathsf{T}}) = 1 + v^{\mathsf{T}}u.$$

여기서 $v^{\mathsf{T}}u$는 전치이며 복소켤레를 취하지 않는 대수적 공식이다.

증명. j번째 열은 $e_j + v_j u$이다. 열에 대한 다중선형성으로 전개하면 u를 두 열 이상에서 택한 항은 반복 열 때문에 0이다. 모두 e_j를 택한 항은 1이다. j번째 열에서만 $v_j u$를 택한 항은 $v_j u_j$이므로 모두 합하면 $1 + \sum_j v_j u_j$다. □

예제 6.17 $u=(1,2)^{\mathsf{T}}$, $v=(3,4)^{\mathsf{T}}$이면

$$I + uv^{\mathsf{T}} = \begin{pmatrix} 4 & 4 \\ 6 & 9 \end{pmatrix}, \qquad \det(I+uv^{\mathsf{T}}) = 36 - 24 = 12.$$

공식의 오른쪽도 $1+3+8=12$다. 큰 행렬에 한 방향의 갱신을 가할 때 행렬식을 다시 전부 계산하지 않아도 되는 구조를 보여 준다.

$1 + v^{\mathsf{T}}u \neq 0$이면 직접 곱하여

$$(I+uv^{\mathsf{T}})^{-1} = I - \frac{uv^{\mathsf{T}}}{1+v^{\mathsf{T}}u}$$

를 확인할 수 있다. 검산에는 $(uv^{\mathsf{T}})^2 = u(v^{\mathsf{T}}u)v^{\mathsf{T}}$를 사용한다. 분모가 0인 경우에는 앞의 행렬식 공식으로 특이함을 알 수 있다. 간단한 공식에도 가역 조건이 반드시 붙는다.

6.9 실수 부피와 복소수 행렬식

실수 선형변환의 n차원 부피 배율은 $|\det A|$이고, 행렬식의 부호는 방향의 보존 또는 반전을 나타낸다. 복소수 행렬식에는 일반적인 양·음의 순서가 없으므로 같은 표현을 그대로 사용하면 안 된다.

예제 6.18 (복소수 한 번 곱하기를 실평면에서 보기) 복소수 $z = a + bi$를 곱하는 사상을 실수 기저 $(1, i)$로 표현하면

$$M_z = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \qquad \det_{\mathbb{R}} M_z = a^2 + b^2 = |z|^2 .$$

복소 1차원에서의 행렬식은 z이지만 실수 2차원에서의 넓이 배율은 $|z|^2$이다. 스칼라체와 실제 공간의 차원을 구분하면 두 값이 왜 다른지 알 수 있다.

6.10 연습문제와 해설

연습문제 6.19 $A = \begin{pmatrix} 2 & 1 & 4 \\ 0 & -1 & 3 \\ 0 & 0 & 5 \end{pmatrix}$의 행렬식을 구하고, 첫째와 셋째 행을 바꾼 뒤의 행렬식도 구하라.

풀이. 상삼각이므로 대각곱은 $2 \cdot (-1) \cdot 5 = -10$이다. 행을 한 번 바꾸면 부호가 반대가 되어 10이다. 교환 뒤의 행렬이 삼각형이 아니어도 다시 전개할 필요가 없다.

연습문제 6.20 3×3 행렬 A의 행렬식이 4이다. 둘째 행에 2를 곱하고 셋째 행에 첫째 행의 5배를 더하여 B를 만들었다. $\det B$와 $\det(2A)$를 비교하라.

풀이. 한 행의 2배는 행렬식을 2배로 만들고 행 더하기는 보존하므로 $\det B = 8$이다. 전체 행렬을 2배 하면 세 행 모두 2배가 되므로 $\det(2A) = 2^3 \cdot 4 = 32$이다.

연습문제 6.21 $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$의 역행렬을 구하고 곱으로 확인하라.

풀이. 행렬식은 -2이므로 $A^{-1} = \begin{pmatrix} -2 & 1 \\ 3/2 & -1/2 \end{pmatrix}$이다. 왼쪽 곱의 첫 행은 $(1, 0)$, 둘째 행은 $(0, 1)$이 된다. 정사각 가역행렬이므로 반대 곱도 항등이다.

연습문제 6.22 두 열이 독립인 3×2 행렬에 일반적인 행렬식을 정의하여 가역성을 판정할 수 있는가?

풀이. 이 장의 행렬식은 정사각행렬에 정의된다. 3×2 행렬은 단사 사상을 나타낼 수 있지만 $\mathbb{R}^2$와 $\mathbb{R}^3$ 사이의 전단사일 수 없고 양쪽 역행렬도 없다. 열의 독립성은 계수가 2인지로 판단한다. 이후 Gram 행렬 $A^{\mathsf{T}}A$의 행렬식을 이용하는 다른 질문과 혼동하지 않는다(제7권 제8장).

연습문제 6.23 $u = (1, -1)^{\mathsf{T}}$, $v = (2, 1)^{\mathsf{T}}$에 대해 $I + uv^{\mathsf{T}}$가 가역인지 판정하고 역행렬을 구하라.

풀이. $v^{\mathsf{T}}u = 1$이므로 행렬식은 2다. $uv^{\mathsf{T}} = \begin{pmatrix} 2 & 1 \\ -2 & -1 \end{pmatrix}$이고 역행렬은 $I - uv^{\mathsf{T}}/2 = \begin{pmatrix} 0 & -1/2 \\ 1 & 3/2 \end{pmatrix}$이다. 원래 행렬 $\begin{pmatrix} 3 & 1 \\ -2 & 0 \end{pmatrix}$와 곱하면 항등을 얻는다.

연습문제 6.24 복소수 i를 곱하는 사상을 복소 1차원과 실수 2차원에서 각각 표현하고 행렬식을 비교하라.

풀이. 복소 행렬은 $[i]$이고 행렬식은 i다. 실수 행렬은 $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$이고 행렬식은 1이다. 이는 실평면의 90도 회전이며 넓이와 방향을 보존한다.

어떤 방향이 선형변환 아래에서 자기 자신과 평행하게 남는지 묻는 것이 고유값 문제다. 행렬식은 그 방향을 찾는 방정식을 만들어 준다.

제 7 장

고유값·고유벡터와 대각화

개요 이 장은 선형사상 $T\colon V \to V$가 방향은 그대로 두고 크기만 일정한 배율로 바꾸는 특별한 방향, 곧 **고유벡터**와 그 배율인 **고유값**을 정의하고, 특성다항식으로 고유값의 후보를 구하는 방법을 세운다. 서로 다른 고유값에 속한 고유벡터들이 선형독립임을 증명한 뒤, 고유벡터로 기저를 구성하여 선형사상을 대각행렬로 표현하는 **대각화**의 정확한 필요충분조건—모든 고유값에서 기하적 중복도가 대수적 중복도와 같다는 것—을 세운다. 이어서 대각화를 행렬의 거듭제곱, 확률 전이, 상수계수 미분방정식, Cayley–Hamilton 정리에 응용하고, 교환하는 두 사상이 고유공간을 공유하는 경우를 살펴본다. 선행 지식: 행렬식, 기저변환, 선형사상의 핵과 상(제7권 제4장, 제7권 제6장). 실수체 위에서는 존재하지 않던 고유값이 복소수체로 확장하면 나타날 수 있으므로, 결론이 어느 체 위에서 성립하는지 항상 함께 밝혀야 한다.

7.1 고유벡터는 반드시 영이 아니어야 한다

선형변환은 보통 벡터의 방향과 크기를 함께 바꾼다. 그러나 어떤 특별한 방향에서는 방향이 유지되고 크기만 일정한 배율로 바뀔 수 있다. 그러한 방향을 찾으면 반복 적용이나 미분방정식을 훨씬 쉽게 분석할 수 있다. 고유벡터는 이 특별한 방향을, 고유값은 그 배율을 나타낸다.

정의 7.1 (고유값과 고유벡터) 체 $\mathbb{F}$ 위의 벡터공간 V에서 정의된 선형사상 $T\colon V \to V$와 스칼라 $\lambda \in \mathbb{F}$에 대하여, $v \neq 0$이고

$$T(v) = \lambda v$$

를 만족하는 $v \in V$가 존재하면 λ를 T의 **고유값**(*eigenvalue*)이라 하고, 이때 v를 λ에 대한 **고유벡터**(*eigenvector*)라고 한다. 고유값 λ에 대한 **고유공간**(*eigenspace*)은

$$E_\lambda = \ker(T - \lambda I) \tag{7.1}$$

이다. 고유공간에는 영벡터가 포함되지만 영벡터 자체를 고유벡터라고 하지는 않는다.

참고 (영벡터를 제외하는 이유). 영벡터를 허용하면 $T(0) = \lambda 0$이 모든 λ에 대해 성립하여 고유값의 의미가 사라진다. 고유벡터의 비영 상수배도 같은 고유값의 고유벡터이므로, 고유벡터를 하나의 정해진 길이나 부호로 유일하게 찾으려 하지 말고 그 방향과 고유공간 전체를 찾아야 한다.

예제 7.2 (두 특별한 방향) 행렬

$$A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

에 대해 $A(1,1)^{\mathsf{T}} = 3(1,1)^{\mathsf{T}}$, $A(1,-1)^{\mathsf{T}} = (1,-1)^{\mathsf{T}}$이다. 두 방향은 각각 3배와 1배로 바뀐다. 임의의 벡터는 이 두 방향의 결합으로 쓸 수 있으므로, 이 행렬은 그 결합의 두 성분을 서로 다른 배율로 바꾸는 변환이다.

참고 (고유값 0과 가역성). 0도 고유값이 될 수 있다. 이는 핵에 비영벡터가 있다는 뜻이므로 정사각행렬이 가역이 아니라는 것과 동치다. 고유값이 0이라는 사실은 모든 고유값이 0이라는 뜻도, 행렬 자체가 영행렬이라는 뜻도 아니다.

7.2 특성다항식으로 후보를 찾기

정의 7.3 (특성다항식) $A \in M_n(\mathbb{F})$에 대해 $(A-\lambda I)v = 0$이 비영해 v를 가질 필요충분조건은 제7권 제6장의 결과에 의해 $\det(A-\lambda I) = 0$이다. 이 책에서는 최고차항의 계수를 1로 고정하기 위해 **특성다항식**(*characteristic polynomial*)을

$$p_A(t) = \det(tI - A) \tag{7.2}$$

로 정의한다. p_A는 최고차항 계수가 1인 n차 다항식이고, A의 고유값은 정확히 p_A가 $\mathbb{F}$ 안에 갖는 근이다.

예제 7.4 (이차 특성다항식의 계산) $A = \begin{pmatrix} 4 & 1 \\ 0 & 2 \end{pmatrix}$이면 $p_A(t) = (t-4)(t-2)$이다. $\lambda = 4$일 때 $A - 4I$의 핵은 $(1,0)$ 방향이다. $\lambda = 2$일 때는 $A - 2I = \begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix}$이므로 $2x + y = 0$이고, $(-1,2)$를 고유벡터로 택할 수 있다. 특성다항식으로 고유값을 찾은 뒤에는 각각의 핵을 풀어 고유벡터를 구해야 한다.

명제 7.5 (대각합·행렬식과 고유값) 일반적인 2×2 정사각행렬에는

$$p_A(t) = t^2 - (\operatorname{tr} A)t + \det A$$

가 성립한다. 더 일반적으로, 복소수 위에서 고유값을 중복도까지 $\lambda_1, \dots, \lambda_n$이라 쓰면

$$\operatorname{tr} A = \sum_{j} \lambda_j, \qquad \det A = \prod_{j} \lambda_j \tag{7.3}$$

이다.

증명. 근과 계수의 관계로 $p_A(t) = \prod_j (t-\lambda_j) = t^n - \left(\sum_j \lambda_j\right) t^{n-1} + \cdots + (-1)^n \prod_j \lambda_j$이다. 한편 $\det(tI - A)$를 여인수로 전개하면 t^{n-1}의 계수는 $-\operatorname{tr} A$이고 상수항(즉 $t=0$에서의 값)은 $\det(-A) = (-1)^n \det A$이다. 두 전개에서 같은 차수의 계수를 비교하면 식 (7.3)을 얻는다. □

대각화 가능성을 가정하지 않아도 특성다항식의 계수 비교만으로 식 (7.3)이 성립한다. 다만 대각합과 행렬식 두 값만으로 고유벡터나 Jordan 구조까지 결정할 수는 없다.

명제 7.6 (삼각행렬의 고유값) 삼각행렬의 고유값은 그 대각성분들이다.

증명. $tI - A$도 삼각행렬이므로 그 행렬식은 대각성분의 곱 $\prod_i (t - a_{ii})$이다. 따라서 특성다항식이 $(t-a_{ii})$들의 곱이 되어, 근은 정확히 대각성분이다. □

주의 (삼각행렬과 대각화 가능성). 삼각행렬이라고 해서 항상 대각행렬과 닮은 것은 아니다. 고유값을 모두 알아도 대각화 가능성은 별도로 확인해야 한다(정리 7.15).

7.3 서로 다른 고유값과 독립성

정리 7.7 (서로 다른 고유값에 속한 고유벡터의 독립성) 서로 다른 고유값 $\lambda_1, \dots, \lambda_k$에 속하는 고유벡터 $v_1, \dots, v_k$는 선형독립이다.

증명. k에 대해 귀납한다. $k = 1$에서는 고유벡터가 비영이므로 성립한다. $\sum_{j=1}^{k} a_j v_j = 0$이라 하자. 양변에 $T - \lambda_k I$를 적용하면

$$\sum_{j=1}^{k-1} a_j (\lambda_j - \lambda_k) v_j = 0$$

이다. 귀납가정과 고유값들의 차이가 비영이라는 사실로 $a_1 = \cdots = a_{k-1} = 0$을 얻는다. 원래 식에서 $a_k v_k = 0$이므로 $a_k = 0$이다. □

참고 (서로 다르다는 조건의 뜻). 정리 7.7에서 "서로 다르다"는 조건은 같은 고유공간 안의 벡터들이 무조건 종속이라는 뜻이 아니다. 항등사상에서는 모든 비영벡터가 고유값 1에 대한 고유벡터이며, 그 가운데서 전체 공간의 기저를 고를 수 있다. 같은 고유값에 속한 독립 벡터가 몇 개 있는지는 별도로 조사해야 한다.

예제 7.8 (다른 고유공간의 교집합) $v \in E_\lambda \cap E_\mu$이고 $\lambda \neq \mu$이면 $\lambda v = T(v) = \mu v$이므로 $(\lambda - \mu)v = 0$, 따라서 $v = 0$이다. 두 고유공간의 교집합은 영벡터뿐이다. 서로 다른 여러 고유공간의 합도 같은 논증의 확장으로 직합임을 보일 수 있다.

7.4 대각화의 정확한 조건

정의 7.9 (대각화 가능) A에 대해 가역행렬 P와 대각행렬 D가 존재하여 $P^{-1}AP = D$이면 A가 **대각화 가능**(*diagonalizable*)하다고 한다. 어느 체 위의 P, D를 허용하는지 함께 지정한다.

정리 7.10 (대각화의 필요충분조건) $n \times n$ 행렬 A가 대각화 가능할 필요충분조건은 그 스칼라체 위에서 n개의 독립인 고유벡터가 존재하는 것이다. 이들을 P의 열로 놓으면 D의 대각성분은 그 열들에 대응하는 고유값이다.

증명. $P = (v_1 \ \cdots \ v_n)$이라 하고 $Av_j = \lambda_j v_j$라 하면 $AP = PD$이다. 열들이 독립이므로 P가 가역이고 $P^{-1}AP = D$를 얻는다. 반대로 이 식이 성립하면 $AP = PD$의 각 열을 비교하여 P의 비영 독립 열들이 고유벡터임을 알 수 있다. □

예제 7.11 (실제 대각화와 역행렬) 앞의 $A = \begin{pmatrix} 4 & 1 \\ 0 & 2 \end{pmatrix}$에 대해

$$P = \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix}, \qquad P^{-1} = \begin{pmatrix} 1 & 1/2 \\ 0 & 1/2 \end{pmatrix}, \qquad D = \begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix}$$

를 택하면 $AP = PD$이고 따라서 $A = PDP^{-1}$이다. 첫 열과 둘째 열의 순서를 바꾸면 D의 4와 2도 함께 순서를 바꾸어야 한다.

따름정리 7.12 (서로 다른 고유값과 대각화 가능성) $n \times n$ 행렬이 서로 다른 고유값을 n개 가지면 정리 7.7에 의해 그 고유벡터들이 독립이므로 자동으로 대각화 가능하다. 그러나 이는 충분조건일 뿐 필요조건은 아니다. 같은 고유값이 반복되어도 각 고유공간 안에 필요한 수만큼 독립인 고유벡터가 있으면 대각화할 수 있다.

7.5 대수적 중복도와 기하적 중복도

정의 7.13 (대수적 중복도와 기하적 중복도) 고유값 λ가 특성다항식의 근으로 몇 번 나타나는지를 **대수적 중복도**(*algebraic multiplicity*)라고 한다. 고유공간 E_λ의 차원은 **기하적 중복도**(*geometric multiplicity*)다. 두 수는 서로 다를 수 있다.

명제 7.14 (중복도의 부등식) 고유값 λ에 대해

$$1 \le \dim E_\lambda \le \lambda\text{의 대수적 중복도}$$

이다.

증명. 고유공간에 비영벡터가 있으므로 첫 부등식이 성립한다. E_λ의 기저 r개를 전체 공간의 기저로 확장하면 A는 그 기저에서

$$\begin{pmatrix} \lambda I_r & B \\ 0 & C \end{pmatrix}$$

형태가 된다. 블록 삼각행렬의 행렬식 공식에 의해 특성다항식에 $(t-\lambda)^r$이 인수로 들어가므로 r은 대수적 중복도 이하이다. □

정리 7.15 (중복도에 의한 대각화 판정) 특성다항식이 선택한 체에서 일차식으로 완전히 분해된다는 조건 아래, A가 대각화 가능할 필요충분조건은 각 고유값의 기하적 중복도가 대수적 중복도와 같은 것이다.

증명. 필요성. A가 대각화 가능하면 정리 7.10에 의해 독립인 고유벡터로 기저 전체를 만들 수 있다. 고유값 λ에 대응하는 기저벡터의 개수는 그 대수적 중복도와 같아야 한다(그렇지 않으면 특성다항식의 차수가 n을 넘거나 모자란다). 한편 이 벡터들은 모두 E_λ 안에 있으므로 $\dim E_\lambda$는 적어도 그 개수이고, 명제 7.14에 의해 그 이하이므로 두 중복도가 같다.

충분성. 모든 고유값에서 두 중복도가 같다고 하자. 각 E_{λ_i}의 정규직교와 무관한 임의의 기저를 모아 합치면, 서로 다른 고유공간의 합이 직합이라는 사실(예제 7.8)에 의해 이 벡터들은 전체적으로 독립이다. 가정에 의해 그 개수의 합은 대수적 중복도의 합, 곧 특성다항식의 차수 n과 같으므로 전체 공간의 기저를 이루고 정리 7.10에 의해 대각화 가능하다. □

서로 다른 고유공간의 직합 차원을 더하면 필요한 고유벡터의 전체 개수를 알 수 있다.

예제 7.16 (같은 특성다항식, 다른 대각화 가능성)

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \qquad J = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$$

는 둘 다 특성다항식 $(t-2)^2$을 갖는다. A의 고유공간은 $\mathbb{F}^2$ 전체이지만, J에서는 $(J-2I)(x,y)^{\mathsf{T}} = (y,0)^{\mathsf{T}}$이므로 고유공간이 x축뿐이다. A는 대각화 가능하고 J는 불가능하다. 특성다항식의 근을 모두 찾았다는 사실만으로 대각화가 끝나지 않는다.

7.6 실수에서 없던 고유값이 복소수에서는 나타난다

예제 7.17 (90도 회전)

$$R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

의 특성다항식은 t^2+1이다. 실수에서는 근이 없어 실고유값도 없다. 복소수에서는 고유값 $i, -i$가 서로 다르므로 대각화 가능하다. 각각 $(1,-i)^{\mathsf{T}}$, $(1,i)^{\mathsf{T}}$를 고유벡터로 택할 수 있다.

실평면의 90도 회전에는 비영 실벡터가 자기 자신과 평행하게 남는 방향이 없다는 기하적 설명과 일치한다. 복소수로 확대하면 허용하는 좌표와 배율이 달라져 새로운 고유방향이 생긴다. 복소수에서 대각화했다는 결과를 실수 대각화라고 보고해서는 안 된다.

예제 7.18 (매개변수에 따른 세 경우)

$$A_s = \begin{pmatrix} 0 & 1 \\ -1 & s \end{pmatrix}$$

의 특성다항식은 $t^2 - st + 1$이다. $s \in \mathbb{R}$일 때 $|s| > 2$이면 서로 다른 실근 두 개가 있어 실수 위에서 대각화된다. $|s| < 2$이면 서로 다른 비실수 켤레근이 있어 복소수 위에서는 대각화되지만 실수 위에서는 안 된다. $s = \pm 2$이면 고유값이 중복되며 $A_s \neq \pm I$이므로 고유공간 차원은 1이고 복소수에서도 대각화되지 않는다.

7.7 거듭제곱과 반복되는 변환

$A = PDP^{-1}$이면 중간의 $P^{-1}P$가 상쇄되어

$$A^k = PD^kP^{-1} \qquad (k \geq 0) \tag{7.4}$$

이다. 대각행렬의 거듭제곱은 대각성분의 거듭제곱만 계산하면 된다. A가 가역인 경우 음의 정수 거듭제곱에도 같은 식을 쓸 수 있다.

예제 7.19 (큰 거듭제곱을 한 식으로) $A = \begin{pmatrix} 4 & 1 \\ 0 & 2 \end{pmatrix}$의 앞 대각화를 사용하면

$$A^k = \begin{pmatrix} 4^k & (4^k - 2^k)/2 \\ 0 & 2^k \end{pmatrix}$$

이다. $k=0$에서는 항등행렬이고 $k=1$에서는 원래 행렬이다. 대각성분만 거듭제곱하고 비대각성분 1을 그대로 두는 것은 올바른 행렬 거듭제곱이 아니다.

표기 (Jordan 블록과 Jordan 표준형). 고유값 λ에 대한 $m \times m$ **Jordan 블록**(*Jordan block*) $J_m(\lambda)$은 대각성분이 모두 λ이고 그 바로 윗대각선 성분이 모두 1이며 나머지 성분이 모두 0인 행렬이다. 대각화가 불가능한 행렬도 적당한 가역행렬 P에 대해 $P^{-1}AP$를 몇 개의 Jordan 블록을 대각에 배열한 **Jordan 표준형**(*Jordan canonical form*)으로 만들 수 있다는 사실이 알려져 있으며, 이 중복도와 블록 구조의 존재·유일성에 관한 증명은 이 권의 범위를 넘는다. 이 장에서 쓰는 $J = \lambda I + N$, $N^2 = 0$ 꼴은 2×2 Jordan 블록이다.

대각화 불가능한 경우에도 이 구조를 이용할 수 있다. $J = \lambda I + N$, $N^2 = 0$이면 λI와 N이 교환하므로 이항정리에 의해 $k \geq 1$에서

$$J^k = \lambda^k I + k\lambda^{k-1} N$$

이다. $\lambda = 0$일 때 $k = 1$은 별도로 $J = N$으로 읽고 $k \geq 2$에서는 0이다. 대각화가 실패하면 고유값의 지수항 외에 k와 같은 다항식 요인이 생길 수 있다.

7.8 확률 전이의 작은 모형

예제 7.20 (두 상태 사이의 반복 이동) 두 상태의 확률을 열벡터 p_k로 쓰고

$$p_{k+1} = A p_k, \qquad A = \begin{pmatrix} 4/5 & 3/10 \\ 1/5 & 7/10 \end{pmatrix}$$

라 하자. 각 열의 합이 1이므로 확률의 총합이 보존된다. $A(3,2)^{\mathsf{T}} = (3,2)^{\mathsf{T}}$이고 $A(1,-1)^{\mathsf{T}} = \tfrac{1}{2}(1,-1)^{\mathsf{T}}$이다. 따라서 초기분포 $p_0 = (1,0)^{\mathsf{T}}$는

$$p_0 = \begin{pmatrix} 3/5 \\ 2/5 \end{pmatrix} + \frac{2}{5}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

로 분해되고,

$$p_k = \begin{pmatrix} 3/5 \\ 2/5 \end{pmatrix} + \frac{2}{5}\left(\frac{1}{2}\right)^{k}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

이다. 따라서 정상분포 $(3/5, 2/5)^{\mathsf{T}}$로 수렴한다.

이 예에서는 고유값 1의 성분은 유지되고 절댓값이 1보다 작은 고유값의 성분은 사라진다. 모든 확률전이행렬이 같은 방식으로 하나의 정상분포에 수렴하는 것은 아니다. $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$은 두 상태를 번갈아 바꾸며 고유값 -1 때문에 진동한다. 전이행렬의 수렴에는 비주기성 등 추가 구조가 중요하다.

주의 (열벡터 약속과 행벡터 약속). 열합을 1로 정한 약속과 행합을 1로 정한 약속을 섞으면 안 된다. 이 권의 열벡터 약속에서는 $p_{k+1} = A p_k$에 맞추어 열합을 사용했다. 행벡터로 확률을 적는 문헌에서는 전치된 관례를 자주 사용한다.

7.9 미분방정식에서의 분리된 방향

상수행렬을 가진 미분방정식 $x'(t) = Ax(t)$에서 $A = PDP^{-1}$라면 $x = Pz$로 치환하여 $z' = Dz$를 얻는다. 각 성분은 $z_j' = \lambda_j z_j$이므로 $z_j(t) = e^{\lambda_j t} z_j(0)$이다. 이를 다시 합치면

$$x(t) = P\,\mathrm{diag}(e^{\lambda_1 t}, \dots, e^{\lambda_n t})\,P^{-1}x(0) \tag{7.5}$$

이다. 미분방정식의 여러 성분이 고유기저에서 분리되는 것이다.

예제 7.21 $A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$와 $x(0) = (1,0)^{\mathsf T}$에 대해

$$x(t) = \frac{1}{2}e^{3t}\begin{pmatrix}1\\1\end{pmatrix} + \frac{1}{2}e^{t}\begin{pmatrix}1\\-1\end{pmatrix}$$

이다. $t=0$에서 두 항을 더하면 초기값을 얻고, 미분하면 각 항에 해당 고유값이 곱해져 $Ax(t)$와 같다. 이 예에서는 두 고유값이 양수라 두 방향 모두 성장한다.

복소 고유값을 사용하여 실수 미분방정식을 풀 때에는 켤레쌍을 묶어 실수해를 얻을 수 있다. 예를 들어 회전행렬의 고유값 $\pm i$는 $e^{\pm it}$를 만들며, 이들의 실수·허수 부분이 $\cos t, \sin t$다. 복소수 계산은 실수의 진동을 조직하는 도구로도 사용된다.

7.10 Cayley–Hamilton 정리와 행렬 다항식

정리 7.22 (Cayley–Hamilton) 정사각행렬은 자신의 특성다항식을 만족한다. 즉

$$p_A(A) = 0 \tag{7.6}$$

이다.

증명. $p_A(t) = t^n + c_{n-1}t^{n-1} + \cdots + c_0$이라 쓰자. 수반행렬 항등식으로

$$(tI - A)C(t) = p_A(t)I, \qquad C(t) = \mathrm{adj}(tI - A)$$

이다. $C(t) = \sum_{j=0}^{n-1} C_j t^j$로 전개하고 계수를 비교하면 $C_{n-1} = I$, $C_{j-1} - AC_j = c_j I$ $(1 \le j \le n-1)$, $-AC_0 = c_0 I$를 얻는다. 각 식에 적절한 A의 거듭제곱을 왼쪽에서 곱하여 더하면 C_j를 포함한 항들이 상쇄되고 $A^n + c_{n-1}A^{n-1} + \cdots + c_0 I = 0$이 남는다. $\square$

주의 (행렬계수 다항식에 $t = A$를 대입하는 논증). 행렬계수 다항식에 단순히 스칼라처럼 $t = A$를 넣는 논증에는 곱의 순서에 대한 주의가 필요하다. 정리 7.22의 증명은 계수 비교와 상쇄를 사용하여 그 문제를 피했다. 정리는 대각화 가능성을 가정하지 않는다.

예제 7.23 (고차 거듭제곱을 낮추기) $A = \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$의 특성다항식은 $t^2 - 4t + 3$이다. 따라서 $A^2 = 4A - 3I$이며,

$$A^3 = 4A^2 - 3A = 13A - 12I$$

이다. 큰 거듭제곱도 I, A의 결합으로 줄일 수 있다. 실제 행렬곱과 비교하면 $A^3 = \begin{pmatrix} 1 & 26 \\ 0 & 27 \end{pmatrix}$이다.

참고 (고유벡터에서의 다항식 작용). 고유벡터 v에 대해서는 $p(A)v = p(\lambda)v$이다. 이는 $A^k v = \lambda^k v$를 귀납으로 보이면 바로 얻는다. 하지만 모든 벡터가 고유벡터라는 뜻은 아니고, 고유벡터가 부족한 행렬에서는 이를 공간 전체에 대한 대각 계산으로 바꿀 수 없다.

7.11 서로 교환하는 사상의 특별한 경우

명제 7.24 (교환하는 사상과 고유공간) $AT = TA$이고 $Av = \lambda v$이면 $A(Tv) = T(Av) = \lambda Tv$이므로 Tv는 E_λ 안에 있다. 즉 T는 A의 각 고유공간을 보존한다. A가 서로 다른 고유값 n개를 가지면 각 고유공간이 1차원이므로 T도 그 방향을 상수배한다. 따라서 두 사상은 같은 고유기저에서 동시에 대각화된다.

주의 (교환성만으로는 부족하다). 교환한다는 조건만으로 임의의 두 행렬이 동시에 대각화되는 것은 아니다. 항등행렬은 모든 행렬과 교환하지만 대각화 불가능한 Jordan 행렬을 대각화 가능하게 만들지는 못한다. 명제 7.24의 논증에서 고유공간이 충분히 작은 차원으로 분해된다는 가정이 어떤 역할을 했는지 확인해야 한다.

7.12 연습문제와 해설

연습문제 7.25 $A = \begin{pmatrix} 3 & 0 \\ 0 & -2 \end{pmatrix}$의 고유값과 고유공간을 구하라. $(1,1)$은 고유벡터인가?

풀이. 고유값은 3과 -2이고 고유공간은 각각 두 좌표축이다. $A(1,1) = (3,-2)$는 $(1,1)$의 상수배가 아니므로 그 벡터는 고유벡터가 아니다. 고유벡터들의 합이 항상 고유벡터인 것은 아니다.

연습문제 7.26 $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$의 고유값과 두 중복도를 구하고 대각화 가능성을 판단하라.

풀이. 특성다항식은 $(t-1)^2$이므로 대수적 중복도는 2다. 핵 $\ker(A - I)$는 x축이므로 기하적 중복도는 1이다. 독립인 고유벡터가 하나뿐이어서 어느 체 위에서도 대각화되지 않는다.

연습문제 7.27 $A = \begin{pmatrix} 0 & -4 \\ 1 & 0 \end{pmatrix}$는 실수와 복소수에서 각각 대각화 가능한가?

풀이. 특성다항식은 $t^2 + 4$이다. 실수 고유값이 없어 실수 대각화는 불가능하다. 복소수에서는 고유값 $2i, -2i$가 서로 다르므로 대각화 가능하다. 예를 들어 $2i$에 대한 고유벡터로 $(2i, 1)^{\mathsf{T}}$를 택할 수 있다.

연습문제 7.28 대각화 가능한 행렬 A의 모든 고유값이 0이라면 $A = 0$임을 보이라. 대각화 가정을 빼면 어떤가?

풀이. 대각화한 D의 모든 대각성분이 0이므로 $A = P0P^{-1} = 0$이다. 가정을 빼면 $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$이 반례다. 이 행렬은 영행렬이 아니지만 특성다항식이 t^2이다.

연습문제 7.29 A가 가역이고 $Av = \lambda v$라면 A^{-1}의 대응 고유값은 무엇인가? $A + 2I$의 대응 고유값은 무엇인가?

풀이. 가역성이 있으므로 $\lambda \neq 0$이다. 양변에 A^{-1}을 적용하면 $A^{-1}v = \lambda^{-1}v$를 얻는다. 또한 $(A + 2I)v = (\lambda + 2)v$다. 고유벡터는 그대로이고 고유값만 해당 함수로 바뀐다.

연습문제 7.30 예제 7.20의 확률전이 예에서 $p_0 = (0, 1)^{\mathsf{T}}$일 때 p_k를 구하라.

풀이. $p_0 = (3/5, 2/5)^{\mathsf{T}} - (3/5)(1, -1)^{\mathsf{T}}$이므로 $p_k = (3/5, 2/5)^{\mathsf{T}} - (3/5)2^{-k}(1, -1)^{\mathsf{T}}$이다. 총합은 항상 1이며 같은 정상분포로 수렴하지만 초기 고유성분의 계수가 달라졌다.

다음 연결. 일반 행렬은 대각화가 실패할 수 있지만, 대칭행렬과 Hermitian 행렬에는 훨씬 강한 정리가 있다. 내적을 도입하면 직교·사영·최소제곱과 함께 이 구조를 설명할 수 있다(제7권 제8장).

제 8 장

내적 · 직교 · 최소제곱

개요 이 장은 벡터공간에 길이와 각도의 정보를 더하는 **내적**을 정의하고, Cauchy–Schwarz 부등식과 삼각부등식, 정규직교기저와 Gram–Schmidt 과정, 직교여공간과 직교분해, 최소제곱법과 정규방정식, Hermitian 행렬의 스펙트럼 정리, 길이를 보존하는 변환, 직사각행렬의 특이값 분해를 차례로 증명한다. 벡터공간 공리만으로는 길이와 각도를 비교할 수 없다. 기저를 바꾸어도 덧셈과 상수배는 그대로 남지만 좌표성분을 제곱해 더한 값이 언제나 같은 길이를 나타내지는 않는다. 내적은 이 정보를 공간에 추가하여, 방정식에 정확한 해가 없을 때 무엇을 가장 가까운 해로 택할지도 정의할 수 있게 한다. 선행 지식: 복소수의 켤레, 기저와 좌표, 행렬의 전치와 켤레전치, 제7장의 고유값의 뜻(제7권 제7장). 이 장의 공간은 별도 언급이 없으면 실수 또는 복소수 위의 유한차원 공간이다.

8.1 실수와 복소수의 내적

정의 8.1 (내적, 이 책의 켤레 규약) 복소수 벡터공간 V의 **내적**(*inner product*)은 $\langle x, y\rangle \in \mathbb{C}$로서 다음 조건을 만족하는 함수다.

$$\langle x, ay + bz\rangle = a\langle x, y\rangle + b\langle x, z\rangle, \qquad \langle x, y\rangle = \overline{\langle y, x\rangle}, \qquad \langle x, x\rangle \geq 0, \quad \langle x, x\rangle = 0 \iff x = 0.$$

첫째 자리에서는 켤레선형, 둘째 자리에서는 선형이다. 실수 공간에서는 켤레가 사라져 양쪽 자리에서 선형이고 대칭이다. 벡터의 **노름**(*norm*)은 $\|x\| = \sqrt{\langle x, x\rangle}$로 정의한다.

켤레대칭성과 둘째 자리 선형성을 함께 사용하면

$$\langle ax + by, z\rangle = \bar{a}\langle x, z\rangle + \bar{b}\langle y, z\rangle$$

이다. 어떤 책은 첫째 자리에서 선형인 규약을 쓴다. 그 규약도 옳지만 투영계수의 내적 순서까지 함께 바꾸어야 한다. 여기서는 열벡터에 대해 $\langle x, y\rangle = x^{*}y$를 일관되게 쓴다.

예제 8.2 (복소수에서 전치만 쓰면 생기는 문제) $x = (1, i)^{\mathsf{T}}$이면 $x^{\mathsf{T}}x = 1 + i^2 = 0$이지만 $x \neq 0$이다. 따라서 $x^{\mathsf{T}}y$는 복소수 공간의 표준 내적이 아니다. 켤레전치를 쓰면 $x^{*}x = 1 + (-i)i = 2$가 되어 양의 정부호 조건이 성립한다. $y = (i, 1)^{\mathsf{T}}$에 대해서는 $x^{*}y = i - i = 0$이므로 x, y는 서로 직교하고 각각 길이가 $\sqrt{2}$다.

예제 8.3 (가중 내적) $\mathbb{R}^2$에서

$$\langle x, y\rangle_G = x_1y_1 + 4x_2y_2$$

는 내적이다. $x \neq 0$이면 $x_1^2 + 4x_2^2 > 0$이기 때문이다. 이 길이에서 $(1, 0)$의 노름은 1, $(0, 1)$의 노름은 2다. 반면 $x_1y_1 - x_2y_2$는 $(0, 1)$에 대해 자기 내적이 -1이므로 내적이 아니다. 후자는 다른 기하학에서 사용하는 부정부호 형식이며, 이 장의 거리 정리를 그대로 적용할 수 없다.

일반적으로 $G = G^{*}$이고 $x^{*}Gx > 0$이 모든 $x \neq 0$에 대해 성립하면 $\langle x, y\rangle_G = x^{*}Gy$는 내적이다. 또 연속 실함수의 유한차원 부분공간에서는 $\int_a^b f(t)g(t)\,\mathrm{d}t$도 $a < b$일 때 내적이다. 연속함수의 제곱적분이 0이면 함수가 모든 점에서 0이라는 사실이 양의 정부호성을 보장한다. 한 점에서라도 0이 아니면 연속성으로 양의 면적이 생긴다.

8.2 Cauchy–Schwarz 부등식과 삼각부등식

정리 8.4 (Cauchy–Schwarz) 내적공간의 모든 x, y에 대해

$$|\langle x, y\rangle| \le \|x\|\,\|y\| \tag{8.1}$$

가 성립한다. 등호는 x, y가 선형종속일 때, 그리고 그때에만 성립한다.

증명. $x = 0$이면 양변이 0이고 두 벡터는 종속이다. $x \neq 0$이면 $c = \langle x, y\rangle / \langle x, x\rangle$라 놓는다. $y - cx$의 자기 내적을 전개하면

$$0 \le \|y - cx\|^2 = \|y\|^2 - \frac{|\langle x, y\rangle|^2}{\|x\|^2}$$

이다. 양변에 $\|x\|^2$을 곱하면 식 (8.1)을 얻는다. 등호는 $y - cx = 0$과 동치이므로 정확히 종속일 때 성립한다. □

이 증명은 부등식뿐 아니라 투영계수도 알려 준다. cx를 빼면 남은 벡터가 x와 수직이 된다. 다음 절에서는 한 방향에 대한 이 분해를 여러 직교 방향으로 확장한다.

명제 8.5 (노름의 기본 성질) $\|ax\| = |a|\,\|x\|$, $\|x\| \ge 0$, $\|x\| = 0 \iff x = 0$이며

$$\|x + y\| \le \|x\| + \|y\|$$

이다. 따라서 $d(x, y) = \|x - y\|$는 거리다.

증명. 앞의 세 성질은 내적의 공리에서 바로 따른다. 삼각부등식은

$$\|x + y\|^2 = \|x\|^2 + 2\,\mathrm{Re}\langle x, y\rangle + \|y\|^2 \le \|x\|^2 + 2\,\|x\|\,\|y\| + \|y\|^2 = (\|x\| + \|y\|)^2$$

에서 양변의 제곱근을 취하면 얻는다. 거리의 대칭성은 $\|-v\| = \|v\|$, 삼각부등식은 $x - z = (x - y) + (y - z)$에 적용해 얻는다. □

예제 8.6 (수치로 읽는 부등식) $x = (1, 2)$, $y = (2, -1)$이면 내적은 0이고 두 노름은 모두 $\sqrt{5}$다. 합은 $(3, 1)$이므로 $\|x + y\| = \sqrt{10} < 2\sqrt{5}$다. 직교성 때문에 $\|x + y\|^2 = \|x\|^2 + \|y\|^2$도 성립한다. 반면 $y = 3x$라면 두 벡터가 같은 방향이어서 삼각부등식에도 등호가 성립한다.

실수 내적공간에서 $x, y \neq 0$이면 각도를 $\cos\theta = \langle x, y\rangle / (\|x\|\,\|y\|)$로 정할 수 있다. 복소수 내적은 일반적으로 복소수이므로 이 식을 실수 평면의 각도처럼 무조건 읽지는 않는다. 복소수 공간에서도 $\langle x, y\rangle = 0$이라는 직교성은 명확하고 투영 이론에 충분하다.

8.3 정규직교 집합과 좌표

정의 8.7 (직교집합과 정규직교기저) $\langle q_i, q_j\rangle = 0$인 서로 다른 벡터들의 집합을 **직교집합**이라 한다. 각 벡터의 노름도 1이면 **정규직교집합**(*orthonormal set*)이다. 이런 벡터들이 공간 전체의 기저이면 **정규직교기저**(*orthonormal basis*)다.

영벡터가 없는 직교집합은 선형독립이다. 실제로 $\sum c_j q_j = 0$의 양변에 첫째 인자를 q_i로 하는 내적을 취하면 $c_i \|q_i\|^2 = 0$이어서 모든 $c_i = 0$이다. 정규직교기저에서는 이 계산이 좌표를 직접 준다.

정리 8.8 (직교좌표와 Parseval 등식) $q_1, \dots, q_n$이 V의 정규직교기저이면

$$x = \sum_{j=1}^{n} q_j \langle q_j, x\rangle, \qquad \|x\|^2 = \sum_{j=1}^{n} \left|\langle q_j, x\rangle\right|^2 \tag{8.2}$$

이다.

증명. 기저 전개 $x = \sum c_j q_j$에 $\langle q_i, \cdot\rangle$을 적용하면 $c_i = \langle q_i, x\rangle$다. 전개의 자기 내적을 계산하면 교차항은 직교성으로 0이고 대각항만 남는다. □

예제 8.9 (대각선 좌표) $q_1 = (1,1)/\sqrt{2}$, $q_2 = (1,-1)/\sqrt{2}$는 $\mathbb{R}^2$의 정규직교기저다. $x = (3,1)$의 좌표는 $(2\sqrt{2}, \sqrt{2})$이므로

$$x = 2\sqrt{2}\, q_1 + \sqrt{2}\, q_2, \qquad \|x\|^2 = 10 = (2\sqrt{2})^2 + (\sqrt{2})^2$$

이다.

기저를 단순히 $(1,1), (1,-1)$로 쓰면 좌표는 $(2,1)$이지만 그 제곱합은 5다. 좌표 제곱합이 바로 원래 노름 제곱이 되는 이유는 기저의 정규직교성이다.

정규직교집합이 기저 전체가 아니면 해당 방향들의 성분만 얻는다. 이때 나머지 성분의 노름 제곱이 음이 아니므로 $\sum_j \left|\langle q_j, x\rangle\right|^2 \le \|x\|^2$라는 **Bessel 부등식**(*Bessel's inequality*)이 나온다. 등호는 x가 그 벡터들의 생성공간에 있을 때 성립한다.

8.4 Gram–Schmidt 과정과 QR 분해

독립인 벡터 $u_1, \dots, u_k$를 같은 생성공간을 갖는 정규직교벡터로 바꾸려면 이미 만든 방향을 차례로 제거한다.

알고리즘 8.10 (Gram–Schmidt 과정)

$$v_1 = u_1, \qquad q_1 = v_1 / \|v_1\|,$$

$$v_j = u_j - \sum_{i=1}^{j-1} q_i \langle q_i, u_j\rangle, \qquad q_j = v_j / \|v_j\|.$$

귀납적으로 v_j는 앞의 모든 q_i와 직교한다. 또 $v_j = 0$이면 u_j가 앞 u_i들의 생성공간에 들어가 독립성에 모순이므로 나눗셈이 가능하다. 각 단계에서 생성공간은 변하지 않는다. 입력에 종속 벡터가 있으면 영벡터가 나타날 수 있고, 그 벡터는 정규화하지 않고 제외해야 한다.

예제 8.11 (세 벡터의 직교화) $u_1=(1,1,0)^{\mathsf T}$, $u_2=(1,0,1)^{\mathsf T}$, $u_3=(0,1,1)^{\mathsf T}$로 시작하자. 첫 벡터는

$$q_1=\frac{1}{\sqrt{2}}(1,1,0)^{\mathsf T}.$$

둘째 단계에서는 $\langle q_1,u_2\rangle=1/\sqrt{2}$이므로

$$v_2=(1/2,-1/2,1)^{\mathsf T},\qquad \|v_2\|=\sqrt{6}/2,\qquad q_2=\frac{1}{\sqrt{6}}(1,-1,2)^{\mathsf T}.$$

셋째 단계의 계수는 $\langle q_1,u_3\rangle=1/\sqrt{2}$, $\langle q_2,u_3\rangle=1/\sqrt{6}$이다. 따라서

$$v_3=(-2/3,2/3,2/3)^{\mathsf T},\qquad q_3=\frac{1}{\sqrt{3}}(-1,1,1)^{\mathsf T}.$$

세 내적을 직접 계산하면 서로 직교하고 각 노름이 1임을 확인할 수 있다. 원래 벡터들이 서로 수직이 아니어도 독립이면 같은 공간의 정규직교기저를 만들 수 있다.

$m\times n$ 행렬 A의 열들이 독립일 때, 이 과정으로 얻은 벡터들을 Q의 열로 놓으면

$$A=QR,\qquad Q^{*}Q=I_n \tag{8.3}$$

이다. Q는 $m\times n$, R은 $n\times n$ 상삼각행렬이며 $r_{ij}=\langle q_i,u_j\rangle$다. 대각성분 $r_{jj}=\|v_j\|>0$이므로 R은 가역이다. 이를 **축약 QR 분해**(*reduced QR decomposition*)라 한다.

위 예에서 R은

$$\begin{pmatrix}\sqrt{2} & 1/\sqrt{2} & 1/\sqrt{2}\\ 0 & \sqrt{6}/2 & 1/\sqrt{6}\\ 0 & 0 & 2/\sqrt{3}\end{pmatrix}$$

이다. 정확한 산술에서 성립하는 직교화 증명과 컴퓨터의 반올림오차 문제는 구별해야 한다. 거의 종속인 벡터에서는 작은 차이를 빼는 과정이 민감해질 수 있다. 수치 계산에서는 수정 Gram–Schmidt나 Householder 변환 등을 사용하며, 어느 알고리즘이든 입력의 조건과 오차를 확인한다.

8.5 직교여공간과 직교분해

정의 8.12 (직교여공간) 부분공간 $W\subset V$의 **직교여공간**(*orthogonal complement*)은

$$W^{\perp}=\{v\in V:\langle w,v\rangle=0\ \text{for all } w\in W\}$$

이다. 내적의 선형성으로 $W^{\perp}$ 역시 부분공간이다.

정리 8.13 (유한차원 직교분해) 유한차원 내적공간에서 $V=W\oplus W^{\perp}$이고

$$\dim W^{\perp}=\dim V-\dim W$$

이다. 모든 x는 유일하게 $x=w+r$로 분해되며 $w\in W$, $r\in W^{\perp}$이다.

증명. W의 정규직교기저를 $q_1,\dots,q_k$라 하고 $w=\sum_{j}q_j\langle q_j,x\rangle$라 놓는다. 각 q_i에 대해 $\langle q_i,x-w\rangle=0$이므로 $r=x-w\in W^{\perp}$다. $v\in W\cap W^{\perp}$이면 $\langle v,v\rangle=0$이어서 $v=0$이다. 따라서 합은 직합이고 분해는 유일하다. 직합의 차원을 더하면 차원 공식이 나온다. $\square$

이 정리로 정의되는 사상 $P_W x = w$를 W로의 **직교투영**(*orthogonal projection*)이라 한다. W의 기저를 다른 정규직교기저로 바꾸어도 분해의 유일성 때문에 같은 벡터를 얻는다. 또한 $(W^\perp)^\perp = W$다. 포함관계 $W \subset (W^\perp)^\perp$와 양쪽 차원이 같다는 사실을 결합하면 된다.

> **예제 8.14 (평면의 법선벡터)** $W = \{(x,y,z) : x+2y-z=0\}$이면 모든 벡터가 $n=(1,2,-1)$과 직교한다. W는 한 개의 독립 방정식으로 정해져 차원이 2이고 $W^\perp$는 1차원이므로 $W^\perp = \operatorname{span}\{n\}$이다. $b=(2,0,1)$에서 법선성분은
>
> $$\frac{n^{\mathsf T} b}{n^{\mathsf T} n}\, n = \frac{1}{6}(1,2,-1),$$
>
> 따라서 평면으로의 투영은 $(11/6, -1/3, 7/6)$이다. 이 점은 $x+2y-z=0$을 만족하며 뺀 벡터는 평면의 법선 방향이다.

8.6 가장 가까운 점과 투영행렬

> **정리 8.15 (최선근사)** $x \in V$이고 W가 부분공간이면 $P_W x$는 W에서 x와의 거리를 최소화하는 유일한 점이다. 모든 $z \in W$에 대해
>
> $$\|x - z\|^2 = \|x - P_W x\|^2 + \|P_W x - z\|^2 \tag{8.4}$$
>
> 이다.

증명. $x - P_W x \in W^\perp$이고 $P_W x - z \in W$이므로 두 벡터가 직교한다. 합의 자기 내적을 전개하면 교차항이 사라진다. 오른쪽 둘째 항은 음이 아니고 $z = P_W x$일 때에만 0이다. □

> **예제 8.16 (상수값으로 세 관측을 근사)** $b = (1,2,4)^{\mathsf T}$를 $(c,c,c)^{\mathsf T}$로 근사하자. $W = \operatorname{span}\{(1,1,1)^{\mathsf T}\}$이므로 투영계수는 평균 $c = 7/3$이다. 잔차는
>
> $$b - P_W b = (-4/3, -1/3, 5/3)^{\mathsf T}, \qquad \|b - P_W b\|^2 = 14/3.$$
>
> 잔차 성분의 합이 0이라는 것은 상수 방향과의 직교성을 뜻한다. 임의의 c에 대해 제곱오차는 $14/3 + 3(c-7/3)^2$이므로 평균이 유일한 최솟값을 준다는 사실도 직접 보인다.

> **명제 8.17 (투영행렬의 특징)** Q의 열들이 W의 정규직교기저이면 투영행렬은
>
> $$P = QQ^{*}, \qquad P^2 = P, \qquad P^{*} = P$$
>
> 다. 반대로 표준 내적에서 이 두 행렬 등식을 만족하는 정사각행렬은 자신의 상으로의 직교투영이다.

증명. $x = Px + (I-P)x$이고

$$\langle Pu, (I-P)x \rangle = u^{*} P^{*} (I-P) x = u^{*}(P - P^2)x = 0$$

이므로 직교분해 정리를 적용하면 된다. □

흔한 오류. $P^2 = P$만으로 직교투영이라고 부르면 안 된다. $P = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$는 멱등이지만 자기수반이 아니다. $(0,1)$을 $(1,0)$으로 보내는데, x축에서 $(0,1)$에 가장 가까운 점은 $(0,0)$이다. 일반 투영과 직교투영은 다르다.

8.7 최소제곱과 정규방정식

$A \in \mathbb{C}^{m\times n}$, $b \in \mathbb{C}^m$를 주었을 때 $Ax = b$가 불가능할 수 있다. **최소제곱**(*least squares*) 문제는

$$\min_{x\in\mathbb{C}^n} \|Ax - b\|^2$$

이다. 허용된 예측 Ax들은 열공간 $\operatorname{im} A$를 이루므로 먼저 b를 이 부분공간에 투영하면 된다. 예측 벡터 Ax는 유일하지만 그 벡터를 만드는 계수 x는 여럿일 수 있다.

정리 8.18 (정규방정식과 유일성) x가 최소제곱해인 것은

$$A^*(Ax - b) = 0, \qquad \text{즉} \qquad A^*Ax = A^*b \tag{8.5}$$

와 동치이다. 최소제곱해는 항상 존재한다. 모든 최소제곱해는 하나의 해 x_0에 대해 $x_0 + \ker A$이며, 해가 유일할 필요충분조건은 A의 열들이 독립인 것이다. 이 경우

$$x = (A^*A)^{-1}A^*b.$$

증명. 최선근사 정리에 의해 $Ax = P_{\operatorname{im} A} b$인 것이 최소화 조건이고, 이는 잔차 $b - Ax$가 A의 모든 열에 직교한다는 조건과 같다. 그 내적들을 행렬로 모으면 $A^*(b - Ax) = 0$이다. 투영벡터는 정의상 $\operatorname{im} A$ 안에 있으므로 어떤 x_0가 이를 만든다. 같은 예측을 만드는 두 계수의 차이는 $\ker A$에 있고 그 역도 성립한다.

또한 모든 z에 대해 $z^*A^*Az = \|Az\|^2$이다. 따라서 $\ker(A^*A) = \ker A$이고, A가 열독립일 때에만 정사각행렬 A^*A가 가역이다. 이 경우 정규방정식을 역행렬로 풀면 표시한 식을 얻는다. □

정규방정식은 정의와 증명에 매우 유용하지만 수치적으로 반드시 가장 좋은 계산 절차인 것은 아니다. A^*A를 명시적으로 만들면 특이값의 비가 제곱되어 오차에 민감해질 수 있다. 열독립인 경우 QR 분해로 $Rx = Q^*b$를 풀면 같은 정확한 해를 얻고 역행렬을 직접 계산할 필요도 없다.

예제 8.19 (세 점에 직선을 맞추기) 관측점 $(0,1), (1,2), (2,2)$에 $y = \alpha + \beta t$를 맞춘다. 설계행렬과 데이터는

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 2 \end{pmatrix}, \qquad b = \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}.$$

정규방정식은

$$\begin{pmatrix} 3 & 3 \\ 3 & 5 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 5 \\ 6 \end{pmatrix}$$

이므로 $\alpha = 7/6$, $\beta = 1/2$다. 예측과 잔차는

$$A x = \begin{pmatrix} 7/6 \\ 5/3 \\ 13/6 \end{pmatrix}, \qquad r = b - Ax = \begin{pmatrix} -1/6 \\ 1/3 \\ -1/6 \end{pmatrix}.$$

r의 합은 0이고 $0 r_1 + r_2 + 2 r_3 = 0$이므로 A의 두 열에 모두 직교한다. 제곱오차는 $1/36 + 1/9 + 1/36 = 1/6$이다. 직선이 어느 한 관측점을 꼭 통과할 필요는 없지만 잔차의 두 직교 조건은 반드시 성립한다.

예제 8.20 (계수는 유일하지 않은 최소제곱) $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$, $b = (1,3)^{\mathsf T}$이면 예측은 (x_1+x_2, x_1+x_2)다. 평균값 2가 최선이므로 최소제곱해 전체는

$$x_1 + x_2 = 2, \qquad x = (t, 2 - t)^{\mathsf T}$$

이다. 예측은 $(2,2)$, 잔차는 $(-1,1)$로 유일하지만 계수는 유일하지 않다. 그중 계수의 노름까지 최소화하면

$$t^2 + (2-t)^2 = 2(t-1)^2 + 2$$

에 의해 $x = (1,1)$을 얻는다. $A^{*}A$가 특이하다는 이유로 최소제곱해가 존재하지 않는다고 결론 내리면 안 된다.

참고 (가중 최소제곱). 가중 제곱오차 $(Ax-b)^{*} G (Ax-b)$에서 G가 양의 정부호 Hermitian 행렬이면 정규방정식은 $A^{*}GAx = A^{*}Gb$이다. 오차의 각 성분을 다르게 평가하는 문제이므로 표준 최소제곱과 다른 답이 나올 수 있다. 가중치가 양수라는 가정은 여전히 거리와 유일성 논증의 기초다.

8.8 수반과 Hermitian 행렬

표준 내적에서

$$\langle Ax, y \rangle = x^{*} A^{*} y = \langle x, A^{*} y \rangle$$

이므로 켤레전치 A^{*}는 선형사상을 내적의 다른 자리로 옮기는 연산이다.

정의 8.21 (수반행렬과 Hermitian 행렬) $A = A^{*}$인 행렬을 **Hermitian** 또는 **자기수반**(*self-adjoint*) 행렬이라 한다. 실수에서는 $A = A^{\mathsf T}$인 **대칭행렬**이다.

명제 8.22 Hermitian 행렬의 고유값은 실수이며 서로 다른 고유값에 속하는 고유벡터는 서로 직교한다.

증명. $Av = \lambda v$, $v \neq 0$이면 $v^{*}Av = \lambda \|v\|^2$다. $A = A^{*}$이므로 $\overline{v^{*}Av} = v^{*}A^{*}v = v^{*}Av$이고 왼쪽은 실수다. 따라서 λ도 실수다. $Aw = \mu w$이면

$$\lambda \langle v, w \rangle = \langle Av, w \rangle = \langle v, Aw \rangle = \mu \langle v, w \rangle.$$

$\lambda \neq \mu$이면 내적은 0이다. 첫 번째 등식은 일반적으로 $\bar{\lambda}$를 쓰지만 이미 고유값이 실수임을 증명했으므로 위와 같이 적을 수 있다. □

정리 8.23 (유한차원 스펙트럼 정리) 복소 Hermitian 행렬 A는 정규직교 고유기저를 가지므로 $A = UDU^{*}$로 쓸 수 있다. 여기서 $U^{*}U = UU^{*} = I$이고 D는 실수 대각행렬이다. 실수 대칭행렬이면 U도 실수로 택할 수 있어 $A = QDQ^{\mathsf{T}}$, $Q^{\mathsf{T}}Q = I$이다.

증명. 복소수에서 특성다항식은 근을 가지므로 단위 고유벡터 q_1을 택할 수 있다. 고유값은 실수다. $w \perp q_1$이면

$$\langle q_1, Aw \rangle = \langle Aq_1, w \rangle = \lambda_1 \langle q_1, w \rangle = 0$$

이므로 $q_1^{\perp}$는 A에 의해 보존된다. 이 부분공간에 제한한 사상 역시 자기수반이다. 차원에 관한 귀납법을 적용해 그 안에서 정규직교 고유기저를 얻고 q_1을 더한다.

실수 대칭행렬에서도 복소수로 확장한 행렬의 고유값은 실수다. 실수 행렬 $A - \lambda I$가 복소수에서 특이하면 실수에서도 행연산의 계수와 피벗이 같으므로 실수 핵이 0이 아니다. 실수 단위고유벡터를 택한 뒤 실수 직교여공간에서 같은 귀납법을 진행한다. □

예제 8.24 (이차형식의 축 바꾸기) $A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$의 단위 고유벡터는 $q_1 = (1,1)/\sqrt{2}$, $q_2 = (1,-1)/\sqrt{2}$이고 고유값은 3과 1이다. $x = sq_1 + tq_2$라 쓰면

$$x^{\mathsf{T}}Ax = 3s^2 + t^2.$$

원래 좌표에서는 $2x_1^2 + 2x_1x_2 + 2x_2^2$이지만 수직인 고유축에서는 교차항이 사라진다. 두 고유값이 모두 양수이므로 $x \neq 0$에서 이 값도 항상 양수다.

따름정리 8.25 (양의 정부호성과 고유값) 스펙트럼 정리로 Hermitian 행렬이 **양의 정부호**(*positive definite*)인 것과 모든 고유값이 양수인 것이 동치임을 알 수 있다. 모든 고유값이 0 이상이면 양의 준정부호다. 행렬식이 양수라는 조건 하나만으로 양의 정부호가 되지는 않는다. 예를 들어 $-I_2$는 행렬식이 1이지만 모든 비영벡터에 대해 이차형식이 음수다.

8.9 길이를 보존하는 변환과 반사

정의 8.26 (유니터리 행렬과 직교행렬) 정사각행렬 U가 $U^{*}U = I$를 만족하면 **유니터리**(*unitary*) 행렬이라 한다. 이때 $U^{-1} = U^{*}$여서 $UU^{*} = I$도 성립한다. 실수 유니터리 행렬을 **직교행렬**(*orthogonal matrix*)이라 한다.

모든 x, y에 대해

$$\langle Ux, Uy \rangle = x^{*}U^{*}Uy = \langle x, y \rangle$$

이므로 내적과 길이를 보존한다. $\det(U^{*}U) = |\det U|^2 = 1$이므로 복소수에서는 행렬식의 절댓값이 1, 실수에서는 행렬식이 1 또는 -1이다.

참고 (부분 정규직교 직사각행렬). 직사각행렬 $Q \in \mathbb{C}^{m \times n}$의 열들이 정규직교하면 $Q^{*}Q = I_n$이고 $\|Qx\| = \|x\|$이다. 그러나 $m > n$이면 QQ^{*}는 m차원 공간 전체의 항등행렬이 아니라 열공간으로의 직교투영이다. 두 등식의 행렬 크기를 적어 보면 차이가 분명해진다.

예제 8.27 (Householder 반사) $u \neq 0$일 때 $P = uu^*/(u^*u)$는 u의 생성공간으로의 직교투영이다. $H = I - 2P$라 놓으면

$$H^* = H, \qquad H^2 = I - 4P + 4P^2 = I.$$

따라서 H는 유니터리이며 $Hu = -u$, $Hw = w$ for $w \perp u$이다. $u = (1, -1)^{\mathsf{T}}$인 실수 예에서는

$$P = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, \qquad H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

두 좌표를 바꾸는 변환은 직선 $x_1 = x_2$에 대한 반사다. 이 변환을 조합하면 벡터를 좌표축 방향으로 옮길 수 있어 안정적인 QR 계산에도 쓰인다. 이러한 반사를 **Householder 반사**(*Householder reflection*)라 한다.

8.10 직사각행렬을 이해하는 특이값 분해

고유값은 정사각행렬의 같은 공간 안에서의 방향을 다룬다. 직사각행렬 $A\colon \mathbb{C}^n \to \mathbb{C}^m$은 출발 공간과 도착 공간이 다르므로 대신 두 공간에 각각 맞는 정규직교기저를 택한다.

정리 8.28 (특이값 분해) 모든 $A \in \mathbb{C}^{m\times n}$는

$$A = U\Sigma V^* \tag{8.6}$$

로 쓸 수 있다. U와 V는 각각 $m\times m$, $n\times n$ 유니터리 행렬이고, Σ는 $m\times n$으로서 대각 위치에 $\sigma_1 \geq \cdots \geq \sigma_r > 0$이 있고 나머지는 0이다. $r = \operatorname{rank} A$이며 σ_j를 **특이값**(*singular value*)이라 한다. 실수 행렬이면 U, V를 실수 직교행렬로 택할 수 있다.

증명. A^*A는 Hermitian 양의 준정부호 행렬이다. 스펙트럼 정리로 정규직교 고유기저 v_j를 택하고 양의 고유값을 σ_j^2라 쓰자. 양의 고유값에 대해 $u_j = Av_j/\sigma_j$라 놓으면

$$\langle u_i, u_j\rangle = \frac{v_i^* A^* A v_j}{\sigma_i \sigma_j} = \frac{\sigma_j^2}{\sigma_i\sigma_j}\langle v_i, v_j\rangle$$

이므로 $u_1, \dots, u_r$는 정규직교다. 이들을 도착 공간의 정규직교기저로 확장한다. 고유값이 0인 v_j는 $\|Av_j\|^2 = v_j^*A^*Av_j = 0$이므로 $Av_j = 0$이다. 따라서 이 두 기저에 대한 행렬이 Σ다. 0이 아닌 Av_j의 개수가 상의 차원이므로 $r = \operatorname{rank} A$다. □

예제 8.29 (서로 다른 두 공간의 축)

$$A = \begin{pmatrix} 3 & 0 \\ 0 & 0 \\ 0 & 2 \end{pmatrix} : \mathbb{R}^2 \longrightarrow \mathbb{R}^3$$

이면 $A^{\mathsf T}A = \operatorname{diag}(9,4)$ 여서 특이값은 3과 2다. 출발 공간의 e_1, e_2는 도착 공간의 e_1, e_3 방향으로 각각 3배, 2배 늘어난다. $V = I_2$이고 U의 열을 e_1, e_3, e_2 순서로 두면

$$\Sigma = \begin{pmatrix} 3 & 0 \\ 0 & 2 \\ 0 & 0 \end{pmatrix}, \qquad A = U\Sigma V^{\mathsf T}.$$

A는 정사각행렬이 아니어서 행렬식이나 같은 공간의 고유벡터를 요구하지 않지만, 단사성·상의 차원·늘어남은 모두 정확히 설명된다.

A의 최소제곱을 특이값 좌표로 옮기면 $\min_z \|\Sigma z - U^{*}b\|^2$가 된다. 양의 특이값 방향에서는 $z_j = (u_j^{*}b)/\sigma_j$로 정해지고, 핵 방향의 성분은 예측에 영향을 주지 않는다. 그 성분을 0으로 택하면 노름이 최소인 유일한 최소제곱해

$$x_{\min} = \sum_{j=1}^{r} \frac{u_j^{*}b}{\sigma_j} v_j \tag{8.7}$$

를 얻는다.

정의 8.30 (Moore–Penrose 의사역행렬) 식 (8.7)로 $b \mapsto x_{\min}$을 대응시키는 선형사상을 **Moore–Penrose 의사역행렬**(*Moore–Penrose pseudoinverse*) A^{+}라 한다. 모든 $A \in \mathbb{C}^{m\times n}$에 대해 A^{+}가 유일하게 존재하며, $x_{\min} = A^{+}b$다.

주의 (작은 특이값과 수치적 랭크). 아주 작은 양의 특이값은 나눗셈으로 데이터 오차를 크게 키울 수 있다. 정확한 0과 수치적으로 작다는 말은 다르며, 근사 랭크를 정할 때에는 데이터의 오차 수준과 기준을 따로 밝혀야 한다.

8.11 연습문제와 해설

연습문제 8.31 $x = (1, i)$, $y = (2, 1-i)$에 대해 표준 복소 내적 $\langle x, y\rangle$와 $\langle y, x\rangle$를 구하고 켤레대칭성을 확인하라.

풀이. $\langle x, y\rangle = 2 - i(1-i) = 1 - i$이다. 반대 순서는 $2 + (1+i)i = 1 + i$여서 서로 켤레다. 첫째 벡터의 모든 성분에 켤레를 적용해야 하며, $(-i)(-i) = -1$임에도 주의한다.

연습문제 8.32 $(1,0,1)$, $(1,1,0)$을 Gram–Schmidt 과정으로 정규직교화하라.

풀이. 첫 단위벡터는 $q_1 = (1,0,1)/\sqrt{2}$다. 둘째 벡터에서 $(1/2, 0, 1/2)$를 빼면 $(1/2, 1, -1/2)$이고 그 노름은 $\sqrt{6}/2$이다. 따라서 $q_2 = (1, 2, -1)/\sqrt{6}$다. 내적은 $(1-1)/\sqrt{12} = 0$이다.

연습문제 8.33 $b = (2,1,0)$을 평면 $x + y + z = 0$에 투영하고 평면까지의 거리를 구하라.

풀이. 법선은 $n = (1,1,1)$이고 법선성분은 $(n^{\mathsf T}b)/(n^{\mathsf T}n)\, n = n$이다. 따라서 투영은 $(1, 0, -1)$, 거리는 $\|n\| = \sqrt{3}$이다. 투영의 세 성분 합은 0이며 잔차는 법선 방향이므로 두 조건으로 검산할 수 있다.

연습문제 8.34 $P = \frac{1}{5}\begin{pmatrix}1 & 2\\ 2 & 4\end{pmatrix}$가 어느 부분공간으로의 직교투영인지 구하라.

풀이. $u = (1,2)^{\mathsf T}$이면 $P = uu^{\mathsf T}/(u^{\mathsf T}u)$이므로 $\operatorname{span}\{(1,2)\}$로의 투영이다. $P^{\mathsf T} = P$, $P^2 = P$로도 검증할 수 있다. $Pu = u$이고 $P(2,-1)^{\mathsf T} = 0$이어서 보존 방향과 제거 방향이 보인다.

연습문제 8.35 원점을 지나는 직선 $y = \beta t$로 두 관측 $(1,2), (2,1)$을 최소제곱 근사하라. 절편을 허용하는 문제와 왜 다른가?

풀이. $A = (1,2)^{\mathsf T}$, $b = (2,1)^{\mathsf T}$이므로 $5\beta = 4$, $\beta = 4/5$다. 잔차 $(6/5, -3/5)$는 $(1,2)$와 직교한다. 절편을 허용하면 두 점을 정확히 지나는 $y = 3 - t$가 가능하지만, 원점 통과라는 제약에서는 상수열을 설계행렬에 넣을 수 없다.

연습문제 8.36 $A = \begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}$, $b = (2,4)^{\mathsf T}$의 최소제곱해 전체와 최소노름해를 구하라.

풀이. 예측은 평균인 $(3,3)$이어야 하므로 $x_1 + x_2 = 3$이다. 해 전체는 $(t, 3-t)$이고 노름 제곱은 $2(t-3/2)^2 + 9/2$이다. 최소노름해는 $(3/2, 3/2)$, 잔차 제곱노름은 2다. 최소제곱의 최소화와 계수 노름의 최소화는 서로 다른 두 단계다.

연습문제 8.37 실수 대칭행렬의 서로 다른 고유값에 속하는 고유벡터가 직교한다는 것을 이용해 $A = \begin{pmatrix}5 & 0\\ 0 & 2\end{pmatrix}$의 이차형식 최솟값을 $\|x\| = 1$ 아래에서 구하라.

풀이. $x^{\mathsf T}Ax = 5x_1^2 + 2x_2^2 = 2 + 3x_1^2 \ge 2$이다. 최솟값은 작은 고유값 2이며 $x = (0, \pm 1)$에서 얻는다. 일반 대칭행렬도 정규직교 고유좌표로 바꾸면 단위구 위의 이차형식이 고유값의 가중평균이 된다는 같은 논증을 쓸 수 있다.

연습문제 8.38 $Q = \begin{pmatrix}1 & 0\\ 0 & 1\\ 0 & 0\end{pmatrix}$에 대해 $Q^{\mathsf T}Q$, $QQ^{\mathsf T}$를 계산하라. 두 결과가 왜 모두 항등행렬일 수 없는가?

풀이. $Q^{\mathsf T}Q = I_2$이지만 $QQ^{\mathsf T} = \operatorname{diag}(1,1,0)$이다. 뒤의 행렬은 $\mathbb{R}^3$의 xy평면으로의 투영이고 핵이 z축이다. 랭크가 2이므로 랭크 3인 I_3와 같을 수 없다.

연습문제 8.39 $A = \begin{pmatrix}0 & 2\\ 0 & 0\end{pmatrix}$의 고유값과 특이값을 비교하라.

풀이. 특성다항식은 t^2이므로 고유값은 모두 0이다. 그러나 $A^{\mathsf T}A = \operatorname{diag}(0,4)$이므로 특이값은 2와 0이다. A는 e_2를 길이 2인 $2e_1$로 보낸다. 고유값이 0이라는 사실이 행렬이 모든 벡터를 0으로 보낸다는 뜻은 아니다.

다음 연결. 선형대수의 중심 질문은 해의 존재와 자유도, 좌표와 사상의 구별, 적합한 기저의 선택이다. 미적분에서는 미분이 선형근사로 나타나고(제9권 제2장), 확률·통계에서는 공분산과 최소제곱이 내적 구조를 사용한다(제20권 제5장). 추상대수와 함수해석으로 나아갈 때에는(제

13권 제2장) 여기서 사용한 유한차원성, 체, 내적의 양의 정부호성이 어느 정리에 쓰였는지 다시 확인하면 된다.

제 8 권

미분·적분·급수

제8권은 일변수 실함수의 미적분을 극한의 엄밀한 정의 위에서 세운 권이다. 제1장은 ε-δ 방식의 극한과 연속, 중간값정리와 최댓값·최솟값 정리를 다루고, 제2장은 미분계수와 도함수를 정의하여 미분가능성을 일차 근사의 조건으로 다시 특징짓는다. 제3장은 평균값정리와 최적화, 제4장은 Riemann 적분과 미적분 기본정리, 제5장은 적분기법과 이상적분을 다룬다. 제6장은 수열과 급수의 수렴, Taylor 근사의 조건과 오차를 구별하여, 다변수 해석과 실해석으로 넘어가는 다리를 놓는다.

제 1 장

함수의 극한과 연속

개요 이 장은 실변수 실함수의 극한을 ε-δ 방식으로 엄밀하게 정의하고, 이로부터 좌극한·우극한, 극한의 대수 법칙, 조임정리, 무한대에서의 극한과 무한 극한, 연속성, 중간값정리, 최댓값·최솟값 정리를 차례로 세운다. 모든 결과는 극한의 정의 하나에서 출발하며, 뒤에서 다루는 미분가능성과 적분의 엄밀한 서술이 이 장의 정의에 의존한다. 선행 지식: 실수의 대소관계, 절댓값, 함수와 그래프, 지수·로그·삼각함수의 기본 뜻. 극한의 정의 자체는 이 장에서 시작한다.

미적분은 변하는 양을 다루지만 변화량을 무조건 0으로 놓는 계산은 아니다. 먼저 작은 변화가 함수값에 어떤 영향을 주는지 극한으로 정하고, 그 뒤 변화율과 누적량을 정의한다. 극한을 정확히 이해하면 분모가 0이 되는 식, 불연속인 함수, 무한구간의 적분을 서로 구분할 수 있다.

이 권에서는 실변수 실함수를 중심으로 다룬다. 특별한 언급이 없으면 함수의 극한은 주어진 정의역 안에서 접근한다. "x가 a에 가까워진다"는 말은 $x = a$에서의 함숫값을 요구하는 말과 다르며, 극한점 근처에 접근 가능한 점이 실제로 있어야 한다.

1.1 가까워진다는 말의 수학적 뜻

정의 1.1 (유한한 극한) a가 함수 $f : D \to \mathbb{R}$의 정의역 D의 **집적점**(*accumulation point*)이라고 하자. a에서 f의 **극한**(*limit*)이 L이라는 것은, $\lim_{x \to a} f(x) = L$로 쓰며, 모든 $\varepsilon > 0$에 대해 어떤 $\delta > 0$가 존재하여

$$x \in D, \quad 0 < |x - a| < \delta \implies |f(x) - L| < \varepsilon \tag{1.1}$$

이 성립한다는 뜻이다. 집적점이라는 조건은 임의로 작은 근방에 a와 다른 정의역 점이 존재한다는 뜻이다.

ε은 결과값에 허용하는 오차, δ는 그것을 보장하기 위한 입력의 범위다. δ는 ε에 따라 달라져도 되지만, 조건을 만족하는 개별 x를 본 뒤 따로 고르면 안 된다. 또한 $0 < |x - a|$이므로 $f(a)$가 정의되지 않아도 극한은 존재할 수 있다.

역사 (엄밀화의 역사). ε-δ 방식의 극한 정의는 "한없이 가까워진다"는 직관적 표현을 정량적 부등식으로 바꾼 것으로, 19세기에 Cauchy와 Weierstrass를 중심으로 한 해석학의 엄밀화 과정에서 정착하였다. 이 정식화 이후에야 극한·연속·수렴 개념이 증명 가능한 명제로 다루어질 수 있었다.

예제 1.2 (선형함수의 오차 보장) $\lim_{x \to 2}(3x + 1) = 7$임을 정의로 보이자. $|(3x + 1) - 7| = 3|x - 2|$이므로 주어진 $\varepsilon > 0$에 대해 $\delta = \varepsilon/3$으로 두면 된다. 입력 오차를 결과 오차의 3분의 1보다 작게 하면 원하는 부등식이 모든 해당 x에서 성립한다.

예제 1.3 (제곱함수에서는 먼저 범위를 제한한다) $\lim_{x \to 2} x^2 = 4$에서 $\left|x^2 - 4\right| = |x - 2|\,|x + 2|$

다. $|x-2|<1$로 제한하면 $1<x<3$이고 $|x+2|<5$다. 따라서

$$\delta = \min(1, \varepsilon/5)$$

로 택하면 $|x^2-4|<5\delta\le\varepsilon$이다. 두 인자 중 하나를 일정한 상수로 제한한 뒤 나머지 인자를 작게 만드는 방법은 많은 극한 증명에 쓰인다.

정리 1.4 (극한의 유일성) 한 함수가 같은 점에서 유한한 극한을 가지면 그 값은 하나뿐이다.

증명. 서로 다른 두 극한 L, M이 있다고 가정하자. $\varepsilon = |L-M|/3$을 두 극한 정의에 적용하고 두 δ 중 작은 것을 택한다. a는 집적점이므로 그 범위에 $x\neq a$인 정의역 점이 있다. 삼각부등식으로

$$|L-M| \le |L-f(x)| + |f(x)-M| < \frac{2}{3}|L-M|$$

이 되어 모순이다. □

1.2 함수값·좌극한·우극한

정의 1.5 (좌극한과 우극한) **우극한** $\lim_{x\to a+} f(x)=L$에서는 $0<x-a<\delta$로, **좌극한** $\lim_{x\to a-} f(x)=L$에서는 $0<a-x<\delta$로 접근 방향을 제한한다.

양쪽에서 접근할 수 있는 정의역에서 양측 극한이 존재할 필요충분조건은 좌극한과 우극한이 모두 존재하고 같은 값인 것이다.

예제 1.6 (뚫린 점은 극한을 바꾸지 않는다)

$$f(x)=\frac{x^2-1}{x-1},\qquad x\neq 1$$

이면 $f(x)=x+1$이므로 $\lim_{x\to1} f(x)=2$다. 원래 함수는 1에서 정의되지 않는다. 그 점에 값을 2로 채우면 연속이 되지만, 7로 채워도 극한 자체는 여전히 2다. 약분은 $x\neq1$에서의 등식이고 그 사실만으로 극한 계산에는 충분하다.

참고 (제거 가능한 불연속점). 함수가 한 점에서 정의되지 않거나 그 점의 함숫값이 극한과 다르더라도 극한 자체가 존재하면, 그 점의 값을 극한으로 다시 정의하여 연속인 함수로 바꿀 수 있다. 이러한 불연속을 **제거 가능한 불연속점**(*removable discontinuity*)이라고 한다. 예제 1.6의 1이 그러한 점이다. 좌극한과 우극한이 다른 예제 1.7의 0처럼 극한 자체가 존재하지 않는 점은 어떤 값으로 채워도 연속이 되지 않으므로 제거 가능하지 않다.

예제 1.7 (양쪽에서 다른 값에 접근) $f(x)=-1$ for $x<0$, $f(x)=1$ for $x\ge0$라 하자. 0에서 좌극한은 -1, 우극한은 1이므로 양측 극한은 없다. $f(0)$을 어떻게 바꾸어도 양쪽 근방의 값이 달라지지 않으므로 이 불연속을 한 점 수정으로 없앨 수 없다.

$\sqrt{x}$를 $[0,\infty)$ 위의 함수로 보면 0에서의 접근은 정의역 안의 오른쪽 접근이다. 끝점에서 연속이라고 할 때에는 이러한 상대적 의미를 쓴다. 정의역 바깥의 값을 새로 요구하는 것은 아니다.

1.3 극한의 대수 법칙과 분모 조건

정리 1.8 (극한의 대수 법칙) $\lim f(x)=L$, $\lim g(x)=M$이 유한하다고 하자. 그러면

$$\lim (af+bg)=aL+bM, \qquad \lim (fg)=LM \tag{1.2}$$

이다. 또 $M\neq 0$이면 g가 충분히 가까운 뚫린 근방에서 0이 아니며 $\lim (f/g)=L/M$이다.

증명. 합은 $|af+bg-aL-bM|\le |a|\,|f-L|+|b|\,|g-M|$로 제어한다. 곱에서는 $fg-LM=f(g-M)+M(f-L)$로 쓴다. $f\to L$이면 근방에서 $|f|\le |L|+1$로 제한되므로 각 작은 오차를 적절히 나누어 주면 된다.

몫에서는 먼저 $|g-M|<|M|/2$가 되도록 제한한다. 그러면 $|g|>|M|/2$여서 분모가 0에서 떨어져 있고,

$$\left|\frac{1}{g}-\frac{1}{M}\right|=\frac{|g-M|}{|g|\,|M|}\le \frac{2\,|g-M|}{|M|^2}$$

이므로 역수의 극한과 곱의 법칙을 적용한다. □

예제 1.9 (0으로 가는 분모) $x\to 0$일 때 $x/x=1$, $x^2/x=x\to 0$, $x/x^2=1/x$는 유한 양측 극한이 없다. 셋 다 분자와 분모가 0으로 가지만 결과는 다르다. $0/0$은 답이 아니라 추가 분석이 필요함을 나타내는 **부정형**이다.

다항식의 극한은 각 항에 법칙을 적용하여 대입으로 얻는다. 유리함수는 대입한 분모가 0이 아닐 때에만 바로 대입할 수 있다. 분모가 0이면 인수분해, 켤레식 곱하기, 지배적인 항 비교 등 구조에 맞는 변형을 먼저 한다.

1.4 조임정리와 진동하는 함수

정리 1.10 (조임정리) a의 충분히 가까운 뚫린 근방에서 $g(x)\le f(x)\le h(x)$이고 g,h의 극한이 모두 L이면 f의 극한도 L이다.

증명. 주어진 $\varepsilon>0$에 대해 두 극한 조건을 동시에 만족하도록 근방을 줄이면 $L-\varepsilon<g(x)\le f(x)\le h(x)<L+\varepsilon$이다. 따라서 $|f(x)-L|<\varepsilon$이다. □

예제 1.11 (진동의 진폭이 줄어드는 경우) $x\neq 0$에서 $f(x)=x\sin(1/x)$이면 $-|x|\le f(x)\le |x|$다. 따라서 $x\to 0$에서 극한은 0이다. 반면 $\sin(1/x)$는 $x_n=1/(\pi/2+2\pi n)$에서는 1, $y_n=1/(3\pi/2+2\pi n)$에서는 -1이므로 극한이 없다. 진동한다는 사실만이 아니라 진폭이 어떻게 변하는지를 살펴야 한다.

명제 1.12 (극한의 수열 판정) $\lim_{x\to a} f(x)=L$일 필요충분조건은 $x_n\to a$, $x_n\neq a$인 임의의 정의역 수열에 대해 $f(x_n)\to L$인 것이다.

증명. 순방향은 ε-δ 정의에서 바로 따른다. 주어진 $\delta>0$에 대해 $x_n\to a$인 수열은 어떤 N 이후 $0<|x_n-a|<\delta$를 만족하므로 그 이후 $|f(x_n)-L|<\varepsilon$이다.

역방향은 대우로 보인다. 극한 정의가 실패하면 어떤 $\varepsilon_0>0$에 대해 모든 $\delta>0$에서 조건을 어기는 점이 있다. $\delta=1/n$마다 그러한 점 x_n을 골라 $0<|x_n-a|<1/n$이고 $|f(x_n)-L|\ge\varepsilon_0$이게 하면 $x_n\to a$이지만 $f(x_n)\to L$이 아닌 반례 수열을 얻는다. □

1.5 무한대와 무한 극한

정의 1.13 (무한대에서의 극한과 무한 극한) $\lim_{x\to\infty} f(x) = L$은 임의의 $\varepsilon > 0$에 대해 어떤 R이 존재하여 $x > R$인 모든 정의역 점에서 $|f(x) - L| < \varepsilon$이라는 뜻이다. $\lim_{x\to a} f(x) = +\infty$는 임의의 실수 M에 대해 어떤 $\delta > 0$가 존재하여 $0 < |x - a| < \delta$인 모든 정의역 점에서 $f(x) > M$이라는 뜻이다. $+\infty$는 실수 함숫값 하나가 아니라 제한 없이 커지는 성질이다.

예제 1.14 (차수 비교)

$$\lim_{x\to\infty} \frac{3x^2 - x + 1}{2x^2 + 5} = \lim_{x\to\infty} \frac{3 - 1/x + 1/x^2}{2 + 5/x^2} = \frac{3}{2}.$$

최고차항의 차수가 같아서 계수의 비가 남는다. $1/x^2 \to 0$ 같은 보조 극한은 $x > 1/\sqrt{\varepsilon}$이면 된다는 정의로 확인할 수 있다.

예제 1.15 (방향에 따라 다른 발산) $x \to 0$일 때 $1/x^2 \to +\infty$지만 $1/x$는 오른쪽에서는 $+\infty$, 왼쪽에서는 $-\infty$로 간다. 따라서 $1/x$의 양측 극한을 단순히 "무한대"라고 적으면 접근 방향의 차이를 숨기게 된다.

1.6 연속과 합성

정의 1.16 (연속) $a \in D$에서 f가 **연속**(*continuous*)이라는 것은 임의의 $\varepsilon > 0$에 대해 어떤 $\delta > 0$가 존재하여 $x \in D$, $|x - a| < \delta$이면 $|f(x) - f(a)| < \varepsilon$이라는 뜻이다. a가 집적점이면 이는 $\lim_{x\to a} f(x) = f(a)$와 같다.

연속함수의 합과 곱은 연속이고 분모가 0이 아닌 곳에서 몫도 연속이다. g가 a에서 연속이고 f가 $g(a)$에서 연속이면 $f \circ g$도 a에서 연속이다. 이때 g의 함숫값이 f의 정의역에 들어간다는 조건이 필요하다. 합성의 증명은 f에 요구하는 입력 오차를 g의 출력 오차로 넘겨 주는 방식으로 이루어진다.

예제 1.17 (연속이 되도록 값 정하기) $f(x) = (\sqrt{1+x} - 1)/x$ for $x \neq 0$, $f(0) = c$라 하자. 0 근처에서 켤레식을 곱하면 $f(x) = 1/(\sqrt{1+x} + 1)$이다. 따라서 극한은 $1/2$이고 연속이 되는 값은 오직 $c = 1/2$다. 원래 식의 정의역 $x \geq -1$도 함께 유지한다.

1.7 중간값정리: 해의 존재를 보장하기

정리 1.18 (중간값정리) f가 $[a, b]$에서 연속이고 $f(a) < y < f(b)$이면 어떤 $c \in (a, b)$가 존재하여 $f(c) = y$다. 부등호 방향을 바꾼 경우도 같다.

증명. $S = \{x \in [a, b] : f(x) < y\}$는 공집합이 아니고 위로 유계이므로 실수의 완비성에 의해 $c = \sup S$가 존재한다. 연속성으로 $a < c < b$임을 알 수 있다. $f(c) < y$라면 c의 조금 오른쪽에서도 $f < y$여서 상한에 모순이다. $f(c) > y$라면 c의 근방에서 모두 $f > y$인데, 상한의 정의상 S의 점들이 c 바로 왼쪽까지 와야 하므로 모순이다. 따라서 $f(c) = y$다. □

예제 1.19 (근의 존재와 개수는 다른 질문) $f(x)=x^3+x-1$은 연속이고 $f(0)=-1$, $f(1)=1$이므로 $(0,1)$에 근이 있다. $x<y$이면 $f(y)-f(x)=(y-x)(x^2+xy+y^2+1)>0$이므로 엄격히 증가하여 근은 하나뿐이다. 중간값정리는 존재를 보장했고, 유일성은 별도의 증가성으로 보였다.

방법 (이분법). 부호가 다른 양 끝점 사이에서 중점을 반복해 고르면 **이분법**(*bisection method*)을 얻는다. 초기 구간 길이가 $b-a$라면 n번 절반으로 줄인 구간의 길이는 $(b-a)/2^n$이다. 그 중점을 근의 근삿값으로 택할 경우 오차는 그 길이의 절반 이하이다. 이 보장은 연속성과 양 끝점의 부호 조건에 의존한다.

1.8 최댓값·최솟값 정리와 가정의 역할

정리 1.20 (닫힌 유계구간에서의 극값 정리) f가 $[a,b]$에서 연속이면 유계이고, 어떤 $u,v\in[a,b]$에 대해 $f(u)\le f(x)\le f(v)$가 모든 $x\in[a,b]$에서 성립한다.

증명. 이 정리의 바탕은 닫힌 유계구간의 임의의 수열이 구간 안에서 수렴하는 부분수열을 갖는다는 실수의 완비성 결과다. f가 위로 유계가 아니라면 $f(x_n)>n$인 점들을 고를 수 있다. 수렴 부분수열 $x_{n_k}\to c\in[a,b]$에 연속성을 적용하면 $f(x_{n_k})\to f(c)$여서 모순이다. 이제 $M=\sup f([a,b])$에 가까워지는 함숫값의 점열을 고르고 같은 논증을 적용하면 $f(v)=M$인 점을 얻는다. 최솟값은 $-f$에 적용한다. $\square$

예제 1.21 (닫힘·유계성·연속성) $(0,1)$에서 $f(x)=x$는 위로 유계지만 최댓값 1을 실제로 갖지 않는다. $[0,\infty)$에서 같은 함수는 위로 유계도 아니다. $[0,1]$에서 $f(x)=x$ for $x<1$, $f(1)=0$으로 두면 닫힌 유계구간 위의 함수이지만 불연속 때문에 상한 1을 달성하지 못한다. 각 가정이 어떤 실패를 막는지 구분할 수 있다.

1.9 연습문제와 해설

연습문제 1.22 $\lim_{x\to -1}(2x-3)=-5$를 극한 정의로 증명하라.

풀이. 함숫값 오차는 $|(2x-3)+5|=2|x+1|$이다. $\delta=\varepsilon/2$로 택하면 모든 해당 x에 대해 오차가 ε보다 작다. x마다 다른 δ를 고르지 않았다.

연습문제 1.23 $\lim_{x\to 3}(x^2-9)/(x-3)$을 구하고 원래 함수의 3에서의 값과 구분하라.

풀이. $x\neq 3$에서 식은 $x+3$이므로 극한은 6이다. 원래 함수의 값은 정의되지 않는다. 극한값을 함숫값으로 추가해야만 그 점까지 연속인 확장이 된다.

연습문제 1.24 $x^2\cos(1/x)$의 0에서의 극한을 구하라. $\cos(1/x)$ 자체와 비교하라.

풀이. 절댓값이 x^2 이하이므로 첫 극한은 0이다. 두 번째는 $x_n=1/(2\pi n)$에서 1, $y_n=1/((2n+1)\pi)$에서 -1이므로 극한이 없다. 모든 n은 양의 정수로 택한다.

연습문제 1.25 $\lim_{x\to\infty}(5x-1)/(x^2+1)$을 구하라.

풀이. 분자와 분모를 x^2으로 나누면 $(5/x-1/x^2)/(1+1/x^2)$이어서 0이다. 분자의 차수가 더 작으면 이와 같은 이유로 유리함수의 극한이 0이 된다.

연습문제 1.26 $f(x) = x^2 - 2$가 $(1, 2)$에서 적어도 하나의 영점을 가짐을 보이라. 중간값정리만으로 영점의 유일성까지 결론 낼 수 있는가?

풀이. $f(1) = -1$, $f(2) = 2$이고 연속이므로 영점이 존재한다. 유일성은 중간값정리 자체의 결론이 아니다. 이 예에서는 양수 영역에서 x^2이 엄격히 증가한다는 추가 사실로 유일성을 보인다.

연습문제 1.27 $1/x$가 $(0, 1]$에서 연속이라는 사실과 최댓값이 없다는 사실은 왜 모순이 아닌가?

풀이. 구간이 실수 안에서 닫혀 있지 않아 극값 정리의 가정을 만족하지 않는다. $x_n = 1/n$이면 값이 n으로 커지므로 상한조차 유한하지 않다. 최솟값 1은 $x = 1$에서 존재한다.

다음 연결. 연속은 입력 변화가 작으면 출력 변화도 작다는 뜻이다. 다음 장의 미분가능성은 한 걸음 더 나아가 그 변화를 하나의 선형식으로 얼마나 정확히 근사할 수 있는지를 묻는다.

제 2 장

미분과 계산법

개요 이 장은 평균변화율의 극한으로 미분계수와 도함수를 정의하고, 미분가능성을 함수가 한 점 근처에서 일차식으로 얼마나 정확히 근사되는지에 대한 조건으로 다시 특징짓는다. 이어서 합·곱·몫의 미분법, 합성함수의 연쇄법칙, 거듭제곱·지수·로그·삼각함수 등 기본 함수의 도함수와 정의역, 역함수의 미분, 음함수와 매개변수로 주어진 곡선의 미분, 관련변화율, 고계도함수를 차례로 다룬다. 선행 지식: 극한·연속과 함수의 합성(제1장). 삼각함수의 각은 별도 표시가 없으면 라디안이다.

평균변화율은 두 점을 잇는 할선의 기울기다. 두 점을 가까이 보내어 얻는 극한이 미분계수다. 미분가능성은 단지 기울기 공식을 적용할 수 있다는 뜻이 아니라, 한 점 근처에서 함수가 직선과 닮는 정도에 대한 정량적 조건이다.

2.1 미분계수와 접선

정의 2.1 (**미분계수와 도함수**) a의 열린 근방에서 정의된 함수 f에 대해

$$f'(a) = \lim_{h \to 0} \frac{f(a+h) - f(a)}{h} \tag{2.1}$$

가 유한하게 존재하면 f는 a에서 **미분가능**(*differentiable*)하다고 한다. 이 값이 **미분계수**이며 각 점의 미분계수를 모은 함수가 **도함수**(*derivative*)다.

끝점에서는 한쪽 미분계수를 따로 정의할 수 있다. $+\infty$로 발산하는 차분몫은 이 정의의 유한한 미분계수가 아니다. 그래프에 수직접선이 있다는 기하적 표현과 도함수가 실수로 존재한다는 명제는 구분한다.

예제 2.2 (**제곱함수의 정의에 따른 계산**) $f(x) = x^2$이면

$$\frac{(a+h)^2 - a^2}{h} = 2a + h \qquad (h \neq 0)$$

이므로 $f'(a) = 2a$다. $a = 3$에서 **접선**은 $y = 9 + 6(x-3)$이다. $h = 0$을 원래 몫에 직접 대입한 것이 아니라, $h \neq 0$에서 식을 바꾼 뒤 극한을 구했다.

예제 2.3 (**연속이지만 미분가능하지 않은 함수**) $f(x) = |x|$는 0에서 연속이다. 그러나 차분몫 $|h|/h$가 $h > 0$에서는 1, $h < 0$에서는 -1이므로 미분계수가 없다. 연속은 미분가능성의 충분조건이 아니다.

2.2 선형근사로 읽는 미분가능성

정리 2.4 (선형근사에 의한 특징) f가 a에서 미분가능할 필요충분조건은 어떤 실수 L과 함수 r에 대해

$$f(a+h) = f(a) + Lh + r(h), \qquad \frac{r(h)}{h} \longrightarrow 0 \tag{2.2}$$

로 쓸 수 있는 것이다. 그때 $L = f'(a)$다.

증명. 미분계수가 L이면 $r(h) = f(a+h) - f(a) - Lh$로 정의하면 된다. 반대로 이 등식을 $h \neq 0$에서 나누면 차분몫이 $L + r(h)/h$이므로 극한은 L이다. □

이를 $r(h) = o(h)$라고도 쓴다. 오차가 0으로 가는 것만으로는 충분하지 않고, 입력 변화 h에 비해서도 작은 차수여야 한다. 미분가능하면 $Lh + r(h) \to 0$이므로 연속이다. 따라서 불연속인 점에서는 유한한 미분계수가 존재하지 않는다.

예제 2.5 (정확한 나머지) $f(x) = x^2$에서 $f(a+h) = a^2 + 2ah + h^2$이다. 선형근사의 오차는 정확히 h^2이고 $h^2/h = h \to 0$이다. 같은 선형근사를 $g(x) = \sqrt{x}$에 적용하면 $g'(x) = 1/(2\sqrt{x})$이므로 $g(4) = 2$, $g'(4) = 1/4$에서 $\sqrt{4.04}$를 선형근사하면 $2 + (1/4)\cdot 0.04 = 2.01$이다. 이 값은 근사이며 오차의 수치 상한을 주장하려면 나중의 평균값정리나 Taylor 정리로 추가 검증해야 한다.

2.3 합·곱·몫의 미분법

정리 2.6 (합·곱·몫의 미분법칙) f, g가 a에서 미분가능하면

$$(cf + dg)'(a) = cf'(a) + dg'(a), \tag{2.3}$$

$$(fg)'(a) = f'(a)g(a) + f(a)g'(a) \tag{2.4}$$

이다. 또 $g(a) \neq 0$이면 근방에서 몫이 정의되고

$$\left(\frac{f}{g}\right)'(a) = \frac{f'(a)g(a) - f(a)g'(a)}{g(a)^2} \tag{2.5}$$

이다.

증명. 합은 차분몫의 선형성으로 따른다. 곱의 차분은

$$f(a+h)g(a+h) - f(a)g(a) = [f(a+h) - f(a)]g(a+h) + f(a)[g(a+h) - g(a)]$$

로 나눌 수 있다. h로 나누고 연속성 $g(a+h) \to g(a)$를 쓰면 곱의 법칙을 얻는다. 역수에서는

$$\frac{1/g(a+h) - 1/g(a)}{h} = -\frac{[g(a+h) - g(a)]/h}{g(a+h)g(a)}$$

이므로 도함수는 $-g'(a)/g(a)^2$이다. 이 결과에 곱의 법칙을 적용하면 몫의 법칙을 얻는다. □

예제 2.7 (곱의 미분은 도함수들의 곱이 아니다) $f(x) = x^2 \sin x$이면 $f'(x) = 2x\sin x + x^2\cos x$이다. 두 인자가 모두 변하므로 두 항이 생긴다. $(x^2)'(\sin x)' = 2x\cos x$로 쓰는 것은 곱의 법칙이 아니다.

예제 2.8 (유리함수의 도함수) $f(x) = (x+1)/(x-1)$, $x \neq 1$이면

$$f'(x) = \frac{(x-1)-(x+1)}{(x-1)^2} = -\frac{2}{(x-1)^2}.$$

도함수가 음수라는 사실은 각각의 구간 $(-\infty, 1)$, $(1, \infty)$에서 감소한다는 뜻과 연결된다. 정의역을 가로질러 1을 통과하는 하나의 구간으로 취급하면 안 된다.

2.4 합성함수와 연쇄법칙

정리 2.9 (연쇄법칙) g가 a에서 미분가능하고 f가 $g(a)$에서 미분가능하면

$$(f \circ g)'(a) = f'(g(a))\,g'(a) \tag{2.6}$$

이다.

증명. $b = g(a)$라 하자. 미분가능성으로 $f(b+k) = f(b) + f'(b)k + \eta(k)k$라 쓸 수 있으며 $\eta(k) \to 0$이다. $\eta(0) = 0$으로 두면 $k = 0$일 때도 식이 성립한다. $k = g(a+h) - g(a)$를 대입하고 h로 나누면

$$\frac{f(g(a+h)) - f(g(a))}{h} = \left[f'(b) + \eta(k)\right]\frac{g(a+h)-g(a)}{h}$$

이다. g의 연속성으로 $k \to 0$이고 두 인자의 극한을 곱하면 된다. 중간 변화량 k가 0이 되는 점이 있어도 그 값으로 나누지 않았으므로 증명에 문제가 없다. $\square$

예제 2.10 (안쪽 변화율을 빠뜨리지 않기) $f(x) = (1+x^2)^5$이면 바깥 함수는 다섯제곱, 안쪽 함수는 $1+x^2$다. 따라서

$$f'(x) = 5(1+x^2)^4 \cdot 2x = 10x(1+x^2)^4.$$

$\sin(x^2)$의 도함수도 $2x\cos(x^2)$이지 $\cos(x^2)$만이 아니다.

2.5 초등함수의 도함수와 정의역

양의 정수 n에 대해 $(x^n)' = nx^{n-1}$은 곱의 법칙으로 귀납 증명할 수 있다. 음의 정수 지수는 $x \neq 0$에서 역수 법칙으로 얻는다. 실수 지수 α의 함수 $x^\alpha = \exp(\alpha \log x)$는 일반적으로 $x > 0$에서 정의하여

$$(x^\alpha)' = \alpha x^{\alpha-1} \tag{2.7}$$

을 얻는다. 특정 유리 지수는 음수 입력에서도 정의할 수 있지만 그 정의역과 0에서의 미분가능성은 따로 확인해야 한다.

기본 도함수는 다음과 같다.

표 2.1 기본 함수의 도함수와 주요 정의역 조건

$f(x)$	$f'(x)$	주요 정의역 조건
e^x	e^x	$x \in \mathbb{R}$
$\log x$	$1/x$	$x > 0$
a^x	$a^x \log a$	$a > 0$
$\sin x$	$\cos x$	$x \in \mathbb{R}$
$\cos x$	$-\sin x$	$x \in \mathbb{R}$
$\tan x$	$1/\cos^2 x$	$\cos x \neq 0$

$a = 1$일 때 지수함수의 도함수는 0이며 공식도 일치한다. 삼각함수의 표는 라디안 기준이다. 도 단위 입력 t에 대한 $\sin(\pi t/180)$의 도함수에는 $\pi/180$ 인자가 추가된다.

유도 (삼각함수 도함수의 유도). 삼각함수의 미분은 $\lim_{h\to 0}\sin h/h = 1$, $\lim_{h\to 0}(\cos h - 1)/h = 0$과 덧셈정리에서 얻는다. 첫 극한은 단위원의 부채꼴 넓이 비교로 $0 < h < \pi/2$에서 $\sin h < h < \tan h$를 얻어 조임정리(정리 1.10)를 적용하는 방법으로 증명한다. 둘째 극한은 $1 - \cos h = 2\sin^2(h/2)$로 첫 극한에 환원된다. 지수·로그의 정의를 적분이나 급수로 도입하는 접근에서는 해당 도함수를 뒤의 기본정리나 급수 정리로 정당화하며, 두 결과를 서로의 유일한 증명으로 쓰는 순환을 피한다.

> **예제 2.11 (로그미분)** $x > 0$에서 $y = x^x$라 하자. $\log y = x\log x$이므로 $y'/y = \log x + 1$이고
>
> $$y' = x^x(\log x + 1).$$
>
> 밑과 지수가 둘 다 변하기 때문에 고정 지수의 거듭제곱 법칙만 적용할 수 없다. 양수 조건은 로그를 취하는 단계에 사용되었다.

2.6 역함수의 미분

> **정리 2.12 (일변수 역함수 미분)** f가 열린 구간에서 연속이고 엄격히 단조라고 하자. a에서 미분가능하고 $f'(a) \neq 0$이면 역함수는 $b = f(a)$에서 미분가능하며
>
> $$(f^{-1})'(b) = \frac{1}{f'(a)} \tag{2.8}$$
>
> 이다.

증명. 연속인 엄격 단조함수의 역함수는 상의 구간에서 연속이다(중간값정리 1.18로 함숫값이 중간값 성질을 가지며, 단조성과 결합하면 역함수가 뛰어넘을 수 있는 값이 없으므로 불연속이 생길 수 없다). $y = f(x) \to b$이면 $x \to a$이고, $y \neq b$에서

$$\frac{f^{-1}(y) - f^{-1}(b)}{y - b} = \frac{x - a}{f(x) - f(a)}$$

이다. 분모의 차분몫이 0이 아닌 $f'(a)$로 가므로 역수의 극한을 취할 수 있다. □

예제 2.13 (역삼각함수) $\sin$을 $[-\pi/2, \pi/2]$에 제한하면 연속이고 엄격 증가하여 역함수 $\arcsin\colon [-1,1] \to [-\pi/2, \pi/2]$가 있다. $|x| < 1$에서

$$(\arcsin x)' = \frac{1}{\cos(\arcsin x)} = \frac{1}{\sqrt{1-x^2}}.$$

제곱근의 부호가 양수인 이유는 선택한 역함수의 값 범위에서 코사인이 양수이기 때문이다. 끝점에서는 분모가 0이 되어 유한한 도함수 공식의 적용 범위 밖이다. 마찬가지로 $(\arctan x)' = 1/(1+x^2)$이다.

$f(x) = x^3$은 전 실수에서 역함수를 가지지만 $f'(0) = 0$이다. 역함수 $x^{1/3}$의 0에서의 차분몫은 $h^{-2/3}$로 발산하므로 유한한 도함수가 없다. 역함수가 있다는 것만으로 그 미분가능성이 자동으로 보장되지는 않는다.

2.7 음함수·매개변수·관련변화율

$F(x, y) = 0$을 만족하는 미분가능한 가지 $y = y(x)$가 주어지면 연쇄법칙으로 $F_x + F_y y' = 0$이므로 $F_y \neq 0$인 곳에서 $y' = -F_x/F_y$다. 이 계산 자체는 미분가능한 가지의 존재를 가정한다. 기초 예에서는 가지를 직접 풀어 확인하고, 일반적 존재 정리는 다변수 미적분에서 다룬다(제9권 제4장).

예제 2.14 (원의 접선) $x^2 + y^2 = 25$에서 $y \neq 0$인 근방에는 $y = \pm\sqrt{25 - x^2}$라는 가지가 있다. 미분하면 $2x + 2yy' = 0$이므로 $y' = -x/y$다. $(3, 4)$에서 기울기는 $-3/4$이고 접선은 $y - 4 = -(3/4)(x-3)$이다. $(5, 0)$에서는 이 나눗셈을 사용할 수 없으며 접선은 수직선 $x = 5$다.

매개변수 곡선 $x = x(t)$, $y = y(t)$에서 $x'(t_0) \neq 0$이고 근방에서 x를 역으로 풀 수 있으면 $\frac{dy}{dx} = y'(t)/x'(t)$이다. 분모가 0인 점에서는 별도의 분석이 필요하다. 특히 $x' = y' = 0$이면 형식적인 $0/0$으로 접선이 결정되지 않는다.

예제 2.15 (부피와 반지름의 변화율) 구의 반지름 $r(t) > 0$에 대해 $V = (4\pi/3) r^3$이므로

$$\frac{dV}{dt} = 4\pi r^2 \frac{dr}{dt}.$$

$r = 2\,\text{cm}$일 때 $\frac{dV}{dt} = 8\pi\,\text{cm}^3/\text{s}$라면 $\frac{dr}{dt} = 1/2\,\text{cm/s}$이다. r을 먼저 2로 고정해 상수 부피로 미분하면 시간에 따라 변하는 관계를 잃는다. 관계식을 미분한 뒤 해당 순간의 값을 대입해야 한다.

2.8 고계도함수와 규칙의 적용 순서

f'가 다시 미분가능하면 f''를 **이계도함수**라 하고 같은 방식으로 $f^{(n)}$을 정의한다. f''는 변화율이 어떻게 변하는지를 나타낸다. 위치 $s(t)$에서 속도는 s', 가속도는 s''이며 각각의 단위도 달라진다.

예제 2.16 (합성함수의 두 번째 미분) $f(x) = e^{x^2}$이면 $f' = 2x e^{x^2}$이다. 한 번 더 미분할 때에는 곱의 법칙과 연쇄법칙을 모두 적용하여

$$f'' = 2e^{x^2} + 4x^2 e^{x^2} = (2 + 4x^2) e^{x^2}$$

를 얻는다. 첫 도함수의 앞 계수만 미분하거나 지수함수만 미분하면 한 항을 놓친다.

2.9 연습문제와 해설

연습문제 2.17 $f(x)=1/x$의 $a\neq 0$에서의 도함수를 정의로 구하라.

풀이. 차분몫은 $[1/(a+h)-1/a]/h=-1/[a(a+h)]$다. $h\to 0$이면 $-1/a^2$로 간다. $a\neq 0$이므로 충분히 작은 h에서 원래 함수와 분모가 정의된다.

연습문제 2.18 $f(x)=x^2$ for $x\ge 0$, $f(x)=-x^2$ for $x<0$의 0에서의 미분가능성을 판정하라.

풀이. $f(0)=0$이고 차분몫은 $h\ge 0$에서 h, $h<0$에서 $-h$이므로 양쪽 모두 0으로 간다. 따라서 $f'(0)=0$이다. 그러나 $f'(x)=2|x|$이므로 $f''(0)$은 존재하지 않는다. 미분가능성이 모든 차수의 미분가능성을 뜻하지 않는다.

연습문제 2.19 $\log(1+x^2)$와 $\log|x|$의 도함수 및 정의역을 구하라.

풀이. 첫 함수는 모든 실수에서 정의되고 도함수는 $2x/(1+x^2)$다. 둘째는 $x\neq 0$에서 정의된다. $x>0$에서는 $\log x$, $x<0$에서는 $\log(-x)$를 미분하면 두 경우 모두 $1/x$이다.

연습문제 2.20 $y=(\sin x)^3$의 도함수와 $x=0$에서의 접선을 구하라.

풀이. 연쇄법칙으로 $y'=3\sin^2 x\cos x$다. 0에서 함숫값과 도함수가 모두 0이므로 접선은 $y=0$이다. 함수가 0 근처에서 상수라는 뜻은 아니다.

연습문제 2.21 $x=t^2$, $y=t^3$에서 $t\neq 0$일 때 $\dfrac{\mathrm{d}y}{\mathrm{d}x}$를 구하라. $t=0$에서는 같은 몫을 바로 쓸 수 있는가?

풀이. $3t^2/(2t)=3t/2$다. $t=0$에서는 분자·분모가 모두 0이므로 공식의 가정이 깨진다. 다만 곡선을 따로 분석하면 $x\ge 0$에서 $y=\pm x^{3/2}$라는 두 가지가 있고 각각 0에서 한쪽 기울기 0을 가진다. 특이점의 존재를 몫 계산만으로 지우면 안 된다.

연습문제 2.22 반지름이 초당 $0.2\,\mathrm{cm}$로 증가하는 원의 반지름이 $5\,\mathrm{cm}$일 때 넓이 변화율을 구하라.

풀이. $A=\pi r^2$에서 $A'=2\pi r r'$이므로 $2\pi\cdot 5\cdot 0.2=2\pi\,\mathrm{cm}^2/\mathrm{s}$다. 넓이 단위를 시간 단위로 나눈 결과이며 반지름의 증가율과 숫자가 같을 이유는 없다.

다음 연결. 미분법은 한 점의 기울기를 계산한다. 다음 장의 평균값정리는 그 국소 정보가 구간 전체의 증가·감소, 오차, 최적화와 어떻게 연결되는지 보장한다.

제 3 장

평균값정리와 최적화

개요 평균값정리는 구간 양 끝에서의 함수값 차이를 구간 내부 한 점에서의 순간변화율과 연결하는 정리이다. 이 장은 국소극값에서 도함수가 사라진다는 Fermat의 필요조건에서 출발하여 이를 이용해 Rolle 정리와 평균값정리를 증명하고, 평균값정리로부터 증가·감소 판정, 상수함수 판정, 도함수 상한에 의한 함수값 변화의 제어, 닫힌 구간에서의 전역최적화, 이계도함수를 이용한 극값·오목볼록 판정, Cauchy 평균값정리와 로피탈 규칙, Newton 방법의 근사수렴을 차례로 이끌어낸다. 선행 지식: 닫힌 유계구간 위의 연속함수에 대한 극값 정리, 미분의 정의와 기본 계산법 (제8권 제1장, 제8권 제2장). 닫힌 구간의 끝점과 열린 구간의 내부를 구분해서 읽어야 한다.

도함수의 부호를 보고 그래프가 증가한다고 판단하는 일은 직관적으로 자연스럽지만, 정확한 정리가 필요하다. 도함수는 한 점에서의 극한으로 정의되고 증가성은 서로 떨어진 두 점의 함수값을 비교하는 성질이기 때문이다. 평균값정리가 이 간격을 연결한다.

3.1 내부 극값에서의 필요조건

정의 3.1 (국소극값) 함수 f의 정의역에 속하는 점 a에 대하여, a의 어떤 근방이 존재하여 그 근방과 정의역의 교집합에 속하는 모든 x에 대해 $f(x) \le f(a)$이면 a를 f의 **국소최대점**이라 한다. 반대 부등식 $f(x) \ge f(a)$가 성립하면 a를 **국소최소점**이라 하고, 둘을 통틀어 **국소극값점**이라 한다. 부등식이 정의역 전체에서 성립하면 a를 **전역최대점** 또는 **전역최소점**이라 한다.

정리 3.2 (Fermat의 필요조건) a가 열린 구간의 내부점이고 f가 a에서 미분가능하며 a에서 국소극값을 가지면 $f'(a) = 0$이다.

증명. a가 국소최대점이라 하자. a에 충분히 가까운 h에 대해 $f(a+h) - f(a) \le 0$이다. $h > 0$이면 차분몫 $\dfrac{f(a+h)-f(a)}{h}$은 0 이하이고, $h < 0$이면 같은 차분몫이 0 이상이다. f가 a에서 미분가능하므로 $h \to 0^+$와 $h \to 0^-$의 두 극한은 같은 유한한 값 $f'(a)$로 존재해야 하는데, 한쪽은 0 이하, 다른 쪽은 0 이상이므로 $f'(a) = 0$이다. 국소최소점인 경우는 모든 부등식의 부호가 반대이므로 같은 결론을 얻는다. □

예제 3.3 (필요조건을 충분조건으로 바꾸면 안 된다) $f(x) = x^3$는 $f'(0) = 0$이지만 0의 양옆에서 함수값이 음수와 양수이므로 0은 극값점이 아니다. $f(x) = |x|$는 0에서 전역최소이지만 0에서 미분가능하지 않으므로 정리 3.2의 가정을 만족하지 않는다. $f(x) = x$를 $[0,1]$에 제한하면 양 끝점 $0, 1$에서 전역극값을 갖지만 두 점 모두 열린 구간의 내부점이 아니므로 역시 정리의 가정에 해당하지 않는다. 첫째 예는 $f'(a) = 0$이 극값의 충분조건이 아님을, 둘째와 셋째 예는 각각 '미분가능성', '내부점' 이라는 가정이 빠지면 결론이 깨질 수 있음을 보인다.

3.2 Rolle 정리와 평균값정리

정리 3.4 (Rolle) f가 $[a,b]$에서 연속이고 (a,b)에서 미분가능하며 $f(a)=f(b)$이면, 어떤 $c\in(a,b)$에 대해 $f'(c)=0$이다.

증명. f가 상수함수이면 (a,b)의 임의의 점을 c로 택할 수 있다. f가 상수가 아니라고 하자. f는 $[a,b]$에서 연속이므로 극값 정리에 의해 최댓값과 최솟값을 모두 가지며, f가 상수가 아니므로 둘 중 적어도 하나는 양 끝점의 공통값 $f(a)=f(b)$와 다르다. f가 그 극값을 달성하는 점은 끝점일 수 없으므로 (a,b)의 내부점 c이고, f는 c에서 국소극값을 가진다. 정리 3.2에 의해 $f'(c)=0$이다. □

정리 3.5 (평균값정리) f가 $[a,b]$에서 연속이고 (a,b)에서 미분가능하면, 어떤 $c\in(a,b)$에 대해

$$f'(c)=\frac{f(b)-f(a)}{b-a} \tag{3.1}$$

이다.

증명. 할선의 기울기를 $m=\dfrac{f(b)-f(a)}{b-a}$라 하고 $g(x)=f(x)-m(x-a)$라 놓는다. g는 f와 같은 구간에서 연속이고 미분가능하며

$$g(b)-g(a)=[f(b)-f(a)]-m(b-a)=0$$

이므로 $g(a)=g(b)$이다. Rolle 정리 3.4에 의해 $g'(c)=0$인 $c\in(a,b)$가 있다. $g'=f'-m$이므로 $f'(c)=m$, 곧 식 (3.1)을 얻는다. □

예제 3.6 (평균기울기와 같은 접선) $f(x)=x^2$를 $[1,3]$에서 보면 평균기울기는 $(9-1)/(3-1)=4$이다. $f'(c)=2c=4$인 $c=2$가 구간 내부에 있다. 정리는 일반적으로 그러한 점의 존재만 보장할 뿐, 점이 유일하거나 구간의 중점이라는 결론은 주지 않는다. 이 예에서 $c=2$가 $[1,3]$의 중점과 일치한 것은 x^2의 특수성 때문이고, 일반적인 함수에서는 기대할 수 없다.

예제 3.7 (미분가능성 가정이 빠진 반례) $f(x)=|x|$를 $[-1,1]$에서 보면 양 끝점 값이 같아 평균기울기는 0이다. 그러나 미분 가능한 모든 점에서 도함수는 -1 또는 1이고 0인 곳이 없다. 내부점 0에서 미분가능하지 않으므로 Rolle 정리와 평균값정리의 가정이 깨지고, 두 정리를 적용할 수 없다.

3.3 증가·감소와 상수함수 판정

따름정리 3.8 (단조성 판정) 구간 I에서 미분가능한 함수 f에 대해 $f'\ge 0$이면 f는 비감소, $f'>0$이면 엄격 증가한다. $f'\le 0$이면 비증가, $f'<0$이면 엄격 감소한다. $f'=0$이 I 전체에서 성립하면 f는 I에서 상수다.

증명. I의 임의의 $x<y$에 평균값정리 3.5를 적용하면 어떤 $c\in(x,y)$에 대해 $f(y)-f(x)=f'(c)(y-x)$이다. $y-x>0$이므로 $f(y)-f(x)$의 부호는 $f'(c)$의 부호와 같고, 이로부터 네 가지 단조성 판정이 모두 따른다. $f'=0$이면 모든 $x<y$에 대해 $f(y)=f(x)$이므로 f는 상수다. □

예제 3.9 (엄격 증가와 양의 도함수는 동치가 아니다) x^3은 $\mathbb{R}$ 전체에서 엄격 증가하지만 도함수 $3x^2$는 $x=0$에서 0이다. 따라서 $f'>0$은 편리한 충분조건이지 모든 엄격 증가함수가 만족해야 할 필요조건은 아니다. 반면 미분가능한 비감소함수의 도함수는 음수가 될 수 없다. 차분몫 $(f(x+h)-f(x))/h$의 부호를 $h\to 0$에서 직접 보면 된다.

주의 (구간 연결성 가정). 단조성·상수함수 판정에는 정의역이 구간이라는 가정이 필요하다. $f(x)=0\ (x<0)$, $f(x)=1\ (x>0)$은 $\mathbb{R}\setminus\{0\}$에서 도함수가 모두 0이지만 정의역 전체에서 하나의 상수는 아니다. 서로 떨어진 두 구간 사이에는 평균값정리를 적용할 연결 구간이 없기 때문이다.

참고 (원시함수의 유일성). 두 함수 F, G가 같은 구간에서 $F'=G'$을 만족하면 $(F-G)'=0$이므로 따름정리 3.8에 의해 $F-G$는 상수다. 이것이 부정적분을 원시함수 하나에 임의상수 하나만 더해 나타내는 이유이며, 다음 장의 미적분 기본정리에서 원시함수의 유일성(상수 차이까지)을 설명하는 근거이기도 하다.

3.4 도함수 상한으로 오차를 제어하기

명제 3.10 (Lipschitz형 오차 한계) f가 $[a,b]$에서 연속이고 (a,b)에서 미분가능하며 $|f'|\le M$이면, 모든 $x,y\in[a,b]$에 대해

$$|f(x)-f(y)|\le M\,|x-y| \tag{3.2}$$

이다.

증명. $x\neq y$이면 x,y 사이의 닫힌 구간에 평균값정리를 적용하여 $f(x)-f(y)=f'(c)(x-y)$인 c를 얻고, 양변에 절댓값을 취하면 $|f(x)-f(y)|=|f'(c)|\,|x-y|\le M|x-y|$다. $x=y$이면 식 (3.2)의 양변이 0이다. □

예제 3.11 (삼각함수와 제곱근의 입력 오차) $|\cos x|\le 1$이므로 $|\sin x-\sin y|\le|x-y|$이다. 또 $x,y\in[4,5]$에서는 $\sqrt{x}$의 도함수가 $1/(2\sqrt{x})\le 1/4$이므로 $\left|\sqrt{x}-\sqrt{y}\right|\le|x-y|/4$이다. 같은 입력 오차라도 함수와 작업 구간에 따라 출력 오차의 상한이 달라진다.

미분계수 하나만 알고 모든 입력에서 오차가 그 기울기만큼이라고 단정할 수는 없다. 명제 3.10은 두 점 사이의 전체 구간에서 도함수를 제한한 결과이다. 선형근사의 더 세밀한 오차는 이계도함수나 고계도함수를 제한하는 Taylor 정리로 다룬다(제8권 제6장).

3.5 극값 후보와 닫힌 구간 최적화

방법 (닫힌 구간에서의 전역최적화). 연속함수의 $[a,b]$에서의 전역극값을 찾을 때에는 먼저 극값 정리로 존재가 보장됨을 확인한다. 내부의 미분가능한 점에서 달성되는 극값은 $f'=0$인 점에 있어야 하지만, 미분불가능한 점과 양 끝점도 후보로 남겨야 한다. 후보가 유한개인 계산 문제에서는 각 후보에서의 함수값을 비교해 전역최대·최소를 정한다.

예제 3.12 (모든 후보의 함수값 비교) $f(x)=x^3-3x$를 $[-2,2]$에서 보자. 도함수 $3x^2-3$이 0

인 내부점은 $x = \pm 1$이다. 후보 값은

$$f(-2) = -2, \qquad f(-1) = 2, \qquad f(1) = -2, \qquad f(2) = 2$$

이다. 따라서 최댓값은 2이고 $-1, 2$에서 달성하며, 최솟값은 -2이고 $-2, 1$에서 달성한다. 전역극값을 갖는 점은 하나일 필요가 없다.

예제 3.13 (정의역 제약을 먼저 정하기) 둘레가 20인 직사각형의 두 변을 $x, y > 0$라 하면 $x + y = 10$이므로 넓이는 $A(x) = x(10 - x)$, $0 < x < 10$이다. $A'(x) = 10 - 2x$는 5의 왼쪽에서 양수, 오른쪽에서 음수이므로 넓이는 $x = y = 5$에서 최대 25다. 퇴화한 직사각형까지 허용하면 $[0, 10]$에서 끝점 넓이가 0이다. 원래 양수 조건에서는 최솟값 0은 달성되지 않고 하한일 뿐이다.

3.6 일계·이계도함수 판정과 변곡점

f'가 점 a의 왼쪽에서 양수, 오른쪽에서 음수이면 a는 엄격 국소최대점이다. 부호가 반대로 바뀌면 국소최소점이다. 이는 따름정리 3.8에 의한 a 양옆에서의 증가·감소로 이해할 수 있다.

$f'(a) = 0$이고 $f''(a) > 0$이면 a는 국소최소, $f''(a) < 0$이면 국소최대라는 **이계도함수 판정**도 있다. f''가 a의 근방에서 연속이면 $f''(a) \neq 0$인 경우 그 부호가 근방에서 유지되므로 f'의 부호 변화를 바로 얻어 일계도함수 판정으로 환원된다. 보다 일반적으로 f'가 근방에서 정의되고 $f''(a) > 0$이면

$$\frac{f'(a+h) - f'(a)}{h} > 0$$

이 작은 비영 h에서 성립하므로, $f'(a) = 0$을 대입하면 $h > 0$에서 $f'(a+h) > 0$, $h < 0$에서 $f'(a+h) < 0$을 얻어 f'의 연속성을 가정하지 않고도 같은 결론에 이른다. 이계도함수가 0인 경우에는 이 판정이 결론을 주지 않는다.

예제 3.14 (같은 영인 이계도함수, 다른 모양) x^4, $-x^4$, x^3는 모두 0에서 일계·이계도함수가 0이다. 첫 함수는 0에서 최소, 둘째는 최대, 셋째는 극값이 없다. $f'(0) = f''(0) = 0$이라는 값만으로 셋 중 어느 경우인지 결정할 수 없다.

구간에서 $f'' \geq 0$이면 f'가 비감소하고 f는 **볼록**(*convex*)하다. 볼록성은 $0 \leq t \leq 1$에 대해

$$f((1-t)x + ty) \leq (1-t)f(x) + tf(y)$$

로 정의할 수 있다. 미분가능한 경우에는 그래프의 접선이 항상 그래프 아래에 놓인다는 성질과 연결된다. **변곡점**은 오목·볼록의 성질이 바뀌는 점이다. $f''(a) = 0$은 변곡점의 흔한 후보 조건이지만 충분조건이 아니며 (위 예의 x^4, $-x^4$가 이를 보인다), 이계도함수가 존재하지 않는 점에서도 볼록성의 변화가 일어날 수 있다.

예제 3.15 (접선으로 얻는 부등식) e^x는 이계도함수가 $e^x > 0$이어서 볼록하다. 0에서의 접선은 $1 + x$이므로 $e^x \geq 1 + x$다. 이를 평균값정리와 도함수 부호로도 보일 수 있다. $g(x) = e^x - 1 - x$는 $g'(x) = e^x - 1$이 0의 왼쪽에서 음수, 오른쪽에서 양수이고 $g(0) = 0$이므로, 따름정리 3.8에 의해 g는 0의 왼쪽에서 감소, 오른쪽에서 증가하여 전역최소 0을 $x = 0$에서 달성한다.

3.7 Cauchy 평균값정리와 로피탈 규칙

정리 3.16 (Cauchy 평균값정리) f, g가 $[a,b]$에서 연속이고 (a,b)에서 미분가능하면, 어떤 $c \in (a,b)$에 대해

$$[f(b)-f(a)]g'(c) = [g(b)-g(a)]f'(c) \tag{3.3}$$

이다.

증명. $h(x) = [f(b)-f(a)]g(x) - [g(b)-g(a)]f(x)$라 하면

$$h(b)-h(a) = [f(b)-f(a)][g(b)-g(a)] - [g(b)-g(a)][f(b)-f(a)] = 0$$

이므로 $h(a)=h(b)$다. h는 f,g와 같은 구간에서 연속이고 미분가능하므로 Rolle 정리 3.4에 의해 $h'(c)=0$인 $c\in(a,b)$가 있고, 이는 식 (3.3)과 같다. □

명제 3.17 (로피탈 규칙, $0/0$형) f, g가 $(a, a+\eta)$에서 미분가능하고 그 위에서 $g' \neq 0$이며 $f(x), g(x) \to 0$ as $x \to a^+$이고 $f'(x)/g'(x) \to L \in \mathbb{R}$이면

$$\lim_{x \to a^+} \frac{f(x)}{g(x)} = L$$

이다.

증명. f, g를 a에서 0으로 연속하게 확장한다. $x \in (a, a+\eta)$마다 $[a,x]$에 Cauchy 평균값정리 3.16를 적용하면 어떤 $c_x \in (a,x)$에 대해 $f(x)g'(c_x) = g(x)f'(c_x)$이다. $g' \neq 0$이므로 Rolle 정리에 의해 충분히 작은 근방에서 $g(x) \neq 0$이고, 따라서 $f(x)/g(x) = f'(c_x)/g'(c_x)$이다. $x \to a^+$이면 $c_x \to a^+$이므로 가정에 의해 이 비는 L로 간다. □

왼쪽·무한대로의 접근 및 극한값이 무한한 경우에도 대응하는 로피탈 규칙이 있지만, 적용할 때마다 해당 가정(부정형, $g' \neq 0$, 도함수 비의 극한 존재)을 항상 확인해야 한다.

예제 3.18 (정해진 부정형에서만 사용) $\lim_{x\to 0}(e^x-1)/x$는 $0/0$형이며 도함수의 비가 $e^x \to 1$이므로 극한값은 1이다. 하지만 $(x+1)/(x+2)$를 $x \to 0$에서 미분한 비 $1/1 = 1$로 바꾸면 틀린다. 원래 극한은 $1/2$이며 $0/0$형도 ∞/∞형도 아니었으므로 로피탈 규칙의 가정 자체가 성립하지 않는다.

흔한 오류 (부정형이 아닌데 몫의 규칙을 적용함). $0\cdot\infty$, $\infty-\infty$, 1^∞는 몫의 로피탈 규칙을 그대로 적용하는 형태가 아니다. 적절한 몫이나 로그로 바꾸어 $0/0$ 또는 ∞/∞형인지 다시 확인해야 한다. 또한 도함수의 비가 수렴하지 않는다고 원래 몫의 극한도 없다고 단정할 수 없다. 로피탈 규칙은 충분조건이지 모든 극한의 필요조건은 아니다.

3.8 Newton 방법: 접선 계산과 수렴 보장의 구별

$f(x)=0$을 풀기 위해 현재 근사 x_n에서의 접선이 x축을 만나는 점을 다음 근사로 택하면 **Newton 방법**(*Newton's method*)의 반복식

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)} \tag{3.4}$$

을 얻는다. 분모가 0이면 이 단계는 정의되지 않는다. 좋은 초기값과 충분한 매끄러움, 근에서 0이 아닌 도함수 아래에서는 빠른 국소수렴을 기대할 수 있지만, 임의의 시작점에서 항상 수렴하는 방법은 아니다.

예제 3.19 (제곱근의 반복) $f(x)=x^2-2$이면 식 (3.4)은 $x_{n+1}=(x_n+2/x_n)/2$이다. $x_0=1$에서

$$x_1=\frac{3}{2},\qquad x_2=\frac{17}{12},\qquad x_3=\frac{577}{408}$$

을 얻는다. 양의 x_n에 대해 오차 $e_n=x_n-\sqrt{2}$는

$$e_{n+1}=\frac{e_n^2}{2x_n} \tag{3.5}$$

를 만족한다. 이는 $x_{n+1}=\dfrac{x_n^2+2}{2x_n}$에서 분자를 $x_n^2+2=(x_n-\sqrt{2})^2+2\sqrt{2}\,x_n$으로 다시 쓰면 $x_{n+1}-\sqrt{2}=\dfrac{(x_n-\sqrt{2})^2}{2x_n}$을 얻어 확인된다. 첫 단계 이후 $x_n\ge\sqrt{2}$이고 값이 감소하므로 이 예에서는 수렴을 직접 증명할 수 있다. 오차가 제곱되는 식 (3.5)이 빠른 수렴(이차수렴)의 근거다.

예제 3.20 (반복이 두 점을 오가는 반례) $f(x)=x^3-2x+2$에서 $x_0=0$이면 $f(0)=2$, $f'(0)=-2$이므로 $x_1=0-2/(-2)=1$이다. $f(1)=1$, $f'(1)=1$이므로 $x_2=1-1/1=0$이다. 이후 0과 1을 반복하므로 근으로 수렴하지 않는다. 각 단계의 도함수가 0이 아니어도 전역수렴은 보장되지 않는다. 실제 계산에서는 이분법의 구간 보장과 Newton 단계를 함께 쓰거나, 잔차 $f(x_n)$과 변화량 $x_{n+1}-x_n$을 함께 점검한다.

역사 (Rolle과 미분법에 대한 회의). Michel Rolle(1652–1719)은 정리 3.4의 특수한 경우를 1691년에 발표했으나, 정작 당시 새로 등장한 미분법 자체에는 회의적이었다고 전해진다. 평균값정리를 현재의 일반적 형태로 정리한 사람은 Augustin-Louis Cauchy이며, 정리 3.16의 일반화된 형태도 그의 이름을 딴다.

핵심 수식

$$f'(c)=\frac{f(b)-f(a)}{b-a},\qquad c\in(a,b) \tag{3.6}$$

$$[f(b)-f(a)]g'(c)=[g(b)-g(a)]f'(c),\qquad c\in(a,b) \tag{3.7}$$

$$x_{n+1}=x_n-\frac{f(x_n)}{f'(x_n)} \tag{3.8}$$

차례로 평균값정리, Cauchy 평균값정리, Newton 방법의 반복식이다.

3.9 연습문제와 해설

연습문제 3.21 $f(x)=x^3$의 $[0,2]$에서 평균값정리가 보장하는 점을 구하라.

풀이. 평균기울기는 $(8-0)/(2-0)=4$이고 $f'(c)=3c^2=4$다. $c=\pm 2/\sqrt{3}$ 가운데 구간 $(0,2)$ 안의 점은 $c=2/\sqrt{3}$이다. 음의 해는 지정된 구간 밖이므로 정리의 점으로 택하지 않는다.

연습문제 3.22 $f'(x) = 0$인 점을 모두 구하는 것만으로 $f(x) = |x - 1|$의 $[0, 3]$에서의 최솟값을 찾을 수 있는가?

풀이. 도함수는 정의된 곳에서 -1 또는 1이어서 0인 점이 없다. 그러나 미분불가능한 점 $x = 1$에서 최솟값 0을 가진다. 끝점 값은 각각 $f(0) = 1$, $f(3) = 2$다. 극값 후보에는 미분불가능점도 포함해야 한다(방법 3.5).

연습문제 3.23 $\log x \le x - 1$이 모든 $x > 0$에서 성립함을 도함수로 보여라.

풀이. $g(x) = x - 1 - \log x$라 하면 $g'(x) = 1 - 1/x$다. g'은 1의 왼쪽에서 음수, 오른쪽에서 양수이고 $g(1) = 0$이므로 따름정리 3.8에 의해 g는 0을 전역최솟값으로 가진다. 등호는 $x = 1$에서만 성립한다.

연습문제 3.24 $f(x) = x^4 - 4x^2$의 국소극값을 판정하라.

풀이. $f'(x) = 4x^3 - 8x = 4x(x^2 - 2)$이므로 후보는 $0, \pm\sqrt{2}$다. $f''(x) = 12x^2 - 8$이므로 $f''(0) = -8 < 0$에서 국소최댓값 $f(0) = 0$, $f''(\pm\sqrt{2}) = 16 > 0$에서 국소최솟값 $f(\pm\sqrt{2}) = 4 - 8 = -4$다. 정의역 전체에서는 $f(x) \to +\infty$이므로 전역최댓값은 없다.

연습문제 3.25 $|f'| \le 3$이 $[1, 2]$에서 성립할 때 $|f(1.8) - f(1.2)|$에 대한 상한을 구하라.

풀이. 명제 3.10에서 $M = 3$으로 두면 $|f(1.8) - f(1.2)| \le 3 \cdot |1.8 - 1.2| = 3 \cdot 0.6 = 1.8$이다. 실제 차이가 반드시 1.8이라는 뜻은 아니며, 도함수의 상한으로 얻은 최악의 경우 보장이다.

연습문제 3.26 $\lim_{x \to 0} \sin x / x$를 로피탈 규칙으로 보일 때 삼각함수 도함수의 증명과 어떤 순환이 생길 수 있는가?

풀이. $(\sin x)' = \cos x$를 바로 그 극한 $\lim_{x \to 0} \sin x / x = 1$을 이용해 증명했다면, 로피탈 규칙으로 같은 극한을 최초로 정당화하는 것은 순환논증이다. 기하적인 조임정리 등 미분과 무관한 독립적인 방법으로 기본 극한을 먼저 확립한 뒤에야 로피탈 규칙을 검산에 사용할 수 있다.

도함수가 같은 함수들은 상수 차이만 난다(원시함수의 유일성). 다음 장에서는 누적량을 적분으로 정의하고, 그 누적량의 변화율이 원래 함수라는 미적분 기본정리로 미분과 적분 두 방향을 연결한다(제8권 제4장).

제 4 장

리만적분과 미적분 기본정리

개요 **리만적분**(*Riemann integral*)은 구간을 잘게 나눈 직사각형 넓이들의 합을 분할을 더 잘게 할수록 하나의 값으로 수렴시켜 정적분을 정의하는 방법이다. 이 장은 분할, 위·아래 합, 리만합을 도입하여 적분가능성을 원시함수와 독립적으로 정의하고, 연속함수와 단조함수가 적분가능함을 증명하며, 정적분의 선형성·가법성·부호 성질을 정리한 뒤, 미적분 기본정리의 두 부분으로 미분과 적분을 서로 역연산으로 연결한다. 선행 지식: 실수의 상한·하한, 함수의 연속성과 균등연속, 평균값정리, 유한합의 계산(제8권 제1장, 제8권 제3장). 이 장은 닫힌 유계구간 위의 유계함수만 다룬다. 무한구간이나 끝점에서 발산하는 함수의 이상적분은 다음 장에서 별도의 극한으로 정의하며, 그때의 이상적분과 이 장의 리만적분을 같은 정의로 혼동해서는 안 된다(제8권 제5장).

미분이 한 점 근처의 변화를 측정한다면 적분은 구간 전체의 작은 기여를 합한다. 직사각형 넓이들의 합을 잘게 나눌수록 하나의 값으로 정해지는 경우 그 값을 **정적분**이라 한다. 모든 함수가 이런 방식으로 적분되는 것은 아니므로, 적분가능성은 정의의 일부이며 뒤늦게 붙이는 장식이 아니다.

4.1 분할과 위·아래 합

정의 4.1 (분할, 위·아래 합) $[a,b]$의 **분할**(*partition*)은 $P=(x_0,\dots,x_n)$으로서 $a=x_0<x_1<\cdots<x_n=b$인 점열이다. $\Delta x_i=x_i-x_{i-1}$라 하고, 분할의 **망 크기**(*mesh*)는 $\|P\|=\max_i \Delta x_i$다. 유계함수 f에 대해

$$m_i=\inf_{[x_{i-1},x_i]} f,\qquad M_i=\sup_{[x_{i-1},x_i]} f$$

라 놓고, **아래합**과 **위합**을

$$L(f,P)=\sum_{i=1}^{n} m_i\Delta x_i,\qquad U(f,P)=\sum_{i=1}^{n} M_i\Delta x_i$$

로 정의한다.

분할의 각 구간에서 표본점 $\xi_i\in[x_{i-1},x_i]$를 택하면 **리만합** $S(f,P,\xi)=\sum_i f(\xi_i)\Delta x_i$를 얻는다. $m_i\le f(\xi_i)\le M_i$를 각 항에 적용하면 항상 $L(f,P)\le S(f,P,\xi)\le U(f,P)$다.

참고 (세분과 두 분할의 비교). 분할에 점을 추가하는 것을 **세분**(*refinement*)이라 한다. 구간 $[x_{i-1},x_i]$를 두 개로 나누면 각 조각에서의 하한은 원래 구간의 하한 m_i보다 작을 수 없으므로 두 조각의 하한·길이 곱의 합은 $m_i\Delta x_i$ 이상이고, 따라서 세분하면 아래합은 커지거나 같다. 같은 논리로 상한은 커질 수 없으므로 위합은 작아지거나 같다. 서로 다른 두 분할 P_1,P_2는 두 분할점을 모두 합친 공통 세분 $P_1\cup P_2$를 가지므로

$$L(f,P_1)\le L(f,P_1\cup P_2)\le U(f,P_1\cup P_2)\le U(f,P_2)$$

이고, 임의의 아래합은 임의의 위합보다 작거나 같다.

정의 4.2 (Darboux 방식의 리만적분) 아래적분 $\underline{I} = \sup_P L(f,P)$과 위적분 $\overline{I} = \inf_P U(f,P)$가 같으면 f는 **리만적분가능**하며 그 공통값을 $\int_a^b f(x)\,\mathrm{d}x$라 한다.

명제 4.3 (적분가능성의 Cauchy 판정) 유계함수 f가 $[a,b]$에서 리만적분가능할 필요충분조건은, 임의의 $\varepsilon > 0$에 대해 $U(f,P) - L(f,P) < \varepsilon$을 만족하는 분할 P가 존재하는 것이다.

증명. ($\Rightarrow$) $\underline{I} = \overline{I}$라 하자. 정의에 의해 $\underline{I} - \varepsilon/2 < L(f,P_1)$인 P_1과 $U(f,P_2) < \overline{I} + \varepsilon/2$인 P_2가 있다. 공통 세분 $P = P_1 \cup P_2$를 취하면 레마 4.1에 의해 $L(f,P) \ge L(f,P_1)$, $U(f,P) \le U(f,P_2)$이므로

$$U(f,P) - L(f,P) \le U(f,P_2) - L(f,P_1) < \left(\overline{I} + \frac{\varepsilon}{2}\right) - \left(\underline{I} - \frac{\varepsilon}{2}\right) = \varepsilon$$

이다 ($\underline{I} = \overline{I}$이므로 마지막 항은 ε).

($\Leftarrow$) 모든 P에 대해 $L(f,P) \le \underline{I} \le \overline{I} \le U(f,P)$이므로, $U(f,P) - L(f,P) < \varepsilon$인 P가 존재하면 $0 \le \overline{I} - \underline{I} < \varepsilon$이다. $\varepsilon > 0$이 임의이므로 $\overline{I} = \underline{I}$다. □

4.2 리만합의 극한과 기본 계산

참고 (망 크기에 의한 특징). 리만적분가능성은 분할의 망 크기가 0으로 갈 때 모든 표본점 선택의 리만합이 하나의 값 I로 간다는 것과 동치이다. 여기서 "모든 선택"이 중요하다. 우연히 특정한 분할·표본점 열에서만 같은 값이 나오는 것으로는 적분가능성을 보장할 수 없다. 이 동치의 한 방향은 좋은 분할(위·아래 합의 차가 작은 분할)을 먼저 고정하면 이해할 수 있다. 아주 촘촘한 임의의 분할이 그 고정된 분할점들을 가로지르는 구간들의 총 길이는 작아지고, 가로지르지 않는 구간에서는 좋은 분할의 진동 상한으로 오차를 제어하며, 가로지르는 유한개의 구간에서는 함수의 유계성으로 그 기여를 제한한다. 반대 방향은 각 구간의 상한·하한에 가깝게 표본점을 골라 위합과 아래합의 차이를 임의로 작게 만들면 된다.

예제 4.4 (상수함수의 적분) $f(x) = c$이면 어느 분할에서나 위합과 아래합이 모두 $c\sum_i \Delta x_i = c(b-a)$다. 따라서

$$\int_a^b c\,\mathrm{d}x = c(b-a).$$

$c < 0$일 때 값이 음수인 것은 높이에 부호를 붙여 합했기 때문이다. 정적분은 항상 기하적 넓이 그 자체인 것은 아니다.

예제 4.5 (제곱함수를 합으로 적분) $[0,1]$을 n등분하고 오른쪽 끝점을 택하면

$$R_n = \frac{1}{n}\sum_{k=1}^{n}\left(\frac{k}{n}\right)^2 = \frac{n(n+1)(2n+1)}{6n^3} \longrightarrow \frac{1}{3}.$$

왼쪽 합은 $L_n = (n-1)n(2n-1)/(6n^3)$이고 $R_n - L_n = 1/n \to 0$이다. x^2은 $[0,1]$에서 증가함수이므로 L_n, R_n은 왼쪽·오른쪽 끝점 선택에서 각각 아래합·위합이다. 따라서 이 계산은 특정 리만합의 극한뿐 아니라 명제 4.3에 의한 적분가능성도 함께 보이며 $\int_0^1 x^2\,\mathrm{d}x = 1/3$이다. 유한합 공식 $\sum_{k=1}^{n} k^2 = n(n+1)(2n+1)/6$은 귀납법으로 증명할 수 있다. 적분의 값과 원시함수 공식이 아직 연결되지 않은 단계에서도 이러한 유한합을 통해 누적량을 직접 계산할 수 있다.

4.3 어떤 함수가 적분가능한가

정리 4.6 닫힌 유계구간 위의 연속함수는 리만적분가능하다. 같은 구간 위의 단조함수도 리만적분가능하다.

증명. 연속함수 f는 $[a,b]$에서 균등연속이다(제8권 제1장). 그렇지 않다고 가정하면, 어떤 $\eta>0$에 대해 모든 $\delta>0$마다 $|x_\delta-y_\delta|<\delta$이면서 $|f(x_\delta)-f(y_\delta)|\ge\eta$인 $x_\delta,y_\delta\in[a,b]$가 존재한다. $\delta=1/n$으로 두어 얻은 점열 $(x_n),(y_n)$은 $|x_n-y_n|<1/n\to0$이고 $|f(x_n)-f(y_n)|\ge\eta$를 만족한다. $[a,b]$가 유계이므로 (x_n)에는 수렴하는 부분수열 (x_{n_k})이 있고, $[a,b]$가 닫혀 있으므로 그 극한 x^*는 $[a,b]$에 속한다. $|x_{n_k}-y_{n_k}|\to0$이므로 (y_{n_k})도 같은 극한 x^*로 수렴한다. f가 x^*에서 연속이므로 $f(x_{n_k})\to f(x^*)$, $f(y_{n_k})\to f(x^*)$이고, 따라서 $\bigl|f(x_{n_k})-f(y_{n_k})\bigr|\to0$인데 이는 모든 k에서 $\bigl|f(x_{n_k})-f(y_{n_k})\bigr|\ge\eta$라는 가정과 모순이다. 그러므로 f는 균등연속이다.

주어진 $\eta>0$에 대해 $\delta>0$를 균등연속의 정의대로 택하면, 망 크기가 δ보다 작은 분할에서는 각 구간에서의 진동이 $M_i-m_i\le\eta$이므로

$$U-L=\sum_{i}(M_i-m_i)\Delta x_i\le\eta\sum_{i}\Delta x_i=\eta(b-a)$$

이다. η를 충분히 작게 택하면 명제 4.3의 판정을 만족하므로 f는 리만적분가능하다.

단조증가함수는 n등분 분할에서 $m_i=f(x_{i-1})$, $M_i=f(x_i)$이므로

$$U-L=\frac{b-a}{n}\sum_{i=1}^{n}[f(x_i)-f(x_{i-1})]=\frac{b-a}{n}[f(b)-f(a)]\to0.$$

감소함수는 $-f$에 같은 논증을 적용한다. □

예제 4.7 (점프가 있어도 적분될 수 있다) $[0,1]$에서 $f(x)=0$ $(x<1/2)$, $f(x)=1$ $(x\ge1/2)$라 하자. 점프를 포함하는 구간의 총 길이만 작게 만들면 위합과 아래합의 차이를 작게 만들 수 있다. 정적분은 $1/2$다. 한 점에서 불연속이라는 사실은 적분불가능성을 뜻하지 않는다.

예제 4.8 (유계이지만 리만적분불가능) $[0,1]$에서 유리수 점에는 1, 무리수 점에는 0을 주는 함수(*Dirichlet function*)를 생각하자. 모든 양의 길이 구간에 유리수와 무리수가 모두 있으므로 어떤 분할에서도 $m_i=0$, $M_i=1$이다. 따라서 아래합은 0, 위합은 1로 간격이 줄어들지 않는다. 이 함수는 리만적분가능하지 않다.

참고 (유한개 점에서의 값 변경). 유계함수의 값을 유한개 점에서 바꾸어도 리만적분가능성과 적분값은 바뀌지 않는다. 바뀐 점들을 총 길이가 임의로 작은 유한개 구간에 가두고 함수값 차이의 유계성을 쓰면 된다. 이 성질을 무한개 점의 임의 변경으로 확대할 수는 없다. 예제 4.8는 유리수라는 무한집합에서의 변경이 리만적분가능성을 바꾼다는 것을 보여 준다.

4.4 정적분의 대수와 부호

명제 4.9 (정적분의 선형성, 가법성, 부호) 적분가능한 f,g에 대해 다음이 성립한다.

(1) (선형성) 상수 c,d에 대해 $\displaystyle\int_a^b (cf+dg)\,\mathrm{d}x=c\int_a^b f\,\mathrm{d}x+d\int_a^b g\,\mathrm{d}x$.

(2) (구간 가법성) $a < c < b$이면 $\displaystyle\int_a^b f = \int_a^c f + \int_c^b f$. 방향을 뒤집은 적분은 $\displaystyle\int_b^a f = -\int_a^b f$로, 길이가 0인 적분은 0으로 정의한다.

(3) (순서 보존) $f \le g$이면 $\displaystyle\int f \le \int g$이고, $m \le f \le M$이면 $m(b-a) \le \displaystyle\int_a^b f \le M(b-a)$.

(4) (삼각부등식) $|f|$도 적분가능하며 $\left|\displaystyle\int_a^b f(x)\,\mathrm{d}x\right| \le \int_a^b |f(x)|\,\mathrm{d}x$.

증명. 선형성은 공통 분할에서의 리만합에 대해 $\sum_i (cf+dg)(\xi_i)\Delta x_i = c\sum_i f(\xi_i)\Delta x_i + d\sum_i g(\xi_i)\Delta x_i$가 성립하고, 양변의 망 크기를 0으로 보낸 극한을 취하면 얻는다. 순서 보존은 각 표본점에서의 부등식 $f(\xi_i) \le g(\xi_i)$를 리만합에 합하고 극한을 취하면 되고, $m \le f \le M$인 경우는 $g \equiv m$, $g \equiv M$에 같은 논증을 적용한 뒤 예제 4.4를 쓴다. $\big||u|-|v|\big| \le |u-v|$이므로 $|f|$의 위·아래 합의 차는 f의 위·아래 합의 차를 넘지 않아 $|f|$도 적분가능하고, $-|f| \le f \le |f|$를 적분하면 삼각부등식을 얻는다. □

예제 4.10 (상쇄와 총넓이) $\int_{-1}^{1} x\,\mathrm{d}x = 0$은 원점 아래의 기여와 위의 기여가 상쇄된 결과다. 그래프와 축 사이의 넓이는 $\int_{-1}^{1} |x|\,\mathrm{d}x = 1$이다. 적분값이 0이라는 이유로 함수가 0이거나 넓이가 없다고 결론 내릴 수 없다.

명제 4.11 (영 적분과 비음함수) 연속함수 $f \ge 0$가 $[a,b]$에서 $\int_a^b f = 0$을 만족하면 f는 구간 전체에서 0이다.

증명. 어떤 점 $x_0 \in [a,b]$에서 $f(x_0) > 0$이라 하면, 연속성에 의해 x_0의 어떤 근방(구간에서는 양의 길이 2δ의 구간)에서 $f \ge f(x_0)/2 > 0$이다. 이 구간에서의 적분은 적어도 $f(x_0)\delta$이고, $f \ge 0$이므로 나머지 구간의 적분은 음이 아니다. 명제 4.9의 구간 가법성에 의해 $\int_a^b f \ge f(x_0)\delta > 0$인데 이는 가정과 모순이다. 따라서 f는 모든 점에서 0이다. 연속성이 없으면 유계 비음함수가 유한개의 점에서만 양수인 반례가 있다. □

4.5 누적함수의 변화율: 기본정리 제1부

정리 4.12 (미적분 기본정리 제1부) f가 $[a,b]$에서 연속이고

$$F(x) = \int_a^x f(t)\,\mathrm{d}t$$

이면 F는 (a,b)에서 미분가능하며 $F'(x) = f(x)$이다. 끝점에서는 대응하는 한쪽 도함수가 성립한다.

증명. 내부점 x에서

$$\frac{F(x+h)-F(x)}{h} - f(x) = \frac{1}{h}\int_x^{x+h} \big[f(t)-f(x)\big]\,\mathrm{d}t.$$

h가 양수이든 음수이든 이 식의 절댓값은 x와 $x+h$ 사이에서의 $|f(t)-f(x)|$의 상한 이하이다. f가 x에서 연속이므로 이 상한은 $h \to 0$일 때 0으로 간다. 따라서 차분몫은 $f(x)$로 간다. □

실제로 f가 전체 구간에서 적분가능하고 관심 있는 점 x에서만 연속이어도 같은 증명이 된다. 그러나 적분가능하다는 조건만으로 모든 점에서 $F' = f$라고 말할 수는 없다.

예제 4.13 (불연속인 적분함수의 누적량) 예제 4.7의 계단함수에서 $F(x) = \int_0^x f(t)\,\mathrm{d}t$는 $x \le 1/2$에서 0, $x \ge 1/2$에서 $x - 1/2$이다. F는 연속이지만 $1/2$에서 왼쪽 기울기 0, 오른쪽 기울기 1이므로 미분가능하지 않다. 적분이 점프를 누적해 연속적인 꺾임으로 바꾸었지만 미분가능성까지 자동으로 보장하지는 않았다.

예제 4.14 (원시함수를 모르는 함수도 미분할 수 있다) $F(x) = \int_0^x e^{-t^2}\,\mathrm{d}t$이면 $F'(x) = e^{-x^2}$다. 이 적분을 초등함수 몇 개의 조합으로 표현할 필요는 없다. 기본정리는 연속함수의 원시함수가 적어도 적분을 통해 존재함을 보장한다.

4.6 원시함수로 누적량 계산하기: 기본정리 제2부

정리 4.15 (미적분 기본정리 제2부) f가 $[a,b]$에서 연속이고 G가 $[a,b]$에서 연속, (a,b)에서 미분가능하며 $G' = f$이면

$$\int_a^b f(x)\,\mathrm{d}x = G(b) - G(a).$$

증명. 제1부의 $F(x) = \int_a^x f$는 (a,b)에서 $F' = f = G'$이다. 따라서 따름정리 3.8(제8권 제3장)에 의해 $G - F$는 상수이고, G, F 모두 끝점까지 연속이므로 $G(b) - G(a) = F(b) - F(a) = F(b) - 0 = \int_a^b f$이다. □

참고 (원시함수와 부정적분). $G' = f$인 G를 f의 **원시함수**라 한다. 부정적분 $\int f(x)\,\mathrm{d}x = G(x) + C$는 원시함수들의 가족을 나타내고, 정적분은 지정된 구간의 수 하나다. 상수 차이는 끝점 값을 빼면 없어지므로 정적분 결과 뒤에 $+C$를 붙이지 않는다.

예제 4.16 (다항식의 정적분)

$$\int_0^2 (3x^2 - 2x + 1)\,\mathrm{d}x = \left[x^3 - x^2 + x\right]_0^2 = 8 - 4 + 2 = 6.$$

원시함수를 미분하면 원래 적분함수가 되는지 먼저 확인할 수 있다. 기호 $[G(x)]_a^b$는 $G(b) - G(a)$를 뜻하며 위·아래 값을 더하는 기호가 아니다.

예제 4.17 (미분한 것을 적분할 때의 조건) $G(x) = \sin x$는 C^1 함수이므로 $\int_0^{\pi/2} G'(x)\,\mathrm{d}x = G(\pi/2) - G(0) = 1$이다. 그러나 내부에 정의되지 않은 점이 있는 원시함수 표현을 가로질러 같은 공식을 적용하면 안 된다. 예컨대 $1/x$의 원시함수 $\log|x|$는 0을 가로지르는 구간에서 연속인 원시함수가 아니므로, 정리 4.15의 가정(원시함수가 구간 전체에서 연속)이 깨진다.

4.7 변하는 적분 한계와 평균값

명제 4.18 (변동 한계를 갖는 적분의 미분) f가 연속이고 u, v가 미분가능하여 값이 f의 정의역 안에 있으면

$$\frac{\mathrm{d}}{\mathrm{d}x}\int_{u(x)}^{v(x)} f(t)\,\mathrm{d}t = f(v(x))v'(x) - f(u(x))u'(x).$$

증명. 고정된 기준점 a에 대해 $\int_{u(x)}^{v(x)} f = \int_a^{v(x)} f - \int_a^{u(x)} f = F(v(x)) - F(u(x))$이고, 여기서 $F(x) = \int_a^x f$다. 기본정리 제1부 4.12와 연쇄법칙을 적용하면 $\dfrac{\mathrm{d}}{\mathrm{d}x}F(v(x)) = f(v(x))v'(x)$, $\dfrac{\mathrm{d}}{\mathrm{d}x}F(u(x)) = f(u(x))u'(x)$이고 두 식을 빼면 결론을 얻는다. 아래 한계는 구간을 빼는 방향이므로 음수가 붙는다. □

> **예제 4.19 (두 끝점이 함께 움직임)**
>
> $$H(x) = \int_{x^2}^{\sin x} (1+t^2)\,\mathrm{d}t$$
>
> 이면 $H'(x) = (1+\sin^2 x)\cos x - (1+x^4)\cdot 2x$이다. $\sin x < x^2$인 구간도 방향 있는 적분의 정의로 같은 공식이 성립한다.

흔한 오류 (적분함수 자체에 변수가 들어가는 경우). 적분함수 자체에 x가 들어가면 끝점 공식만으로 미분이 끝나지 않는다. $\int_0^x xt\,\mathrm{d}t = x\cdot\dfrac{x^2}{2} = \dfrac{x^3}{2}$의 도함수는 $3x^2/2$인데, 윗끝점 대입만 하면 $x\cdot x = x^2$만 얻는다. 적분함수의 매개변수 의존성에 따른 항을 추가해야 한다. 일반적인 미분 교환은 별도의 조건 아래 다변수 미적분에서 다룬다.

> **정리 4.20 (적분의 평균값정리)** f가 $[a,b]$에서 연속이면, 어떤 $c\in[a,b]$에 대해
>
> $$f(c) = f_{\text{avg}} := \frac{1}{b-a}\int_a^b f$$
>
> 이다.

증명. f의 최솟값과 최댓값을 각각 m, M이라 하면 명제 4.9에 의해 $m(b-a) \le \int_a^b f \le M(b-a)$, 곧 $m \le f_{\text{avg}} \le M$이다. f는 연속이므로 중간값정리에 의해 $f(c) = f_{\text{avg}}$인 $c\in[a,b]$가 있다. □

> **예제 4.21 (평균 높이)** $f(x) = x^2$의 $[0,2]$에서 평균은 $f_{\text{avg}} = \dfrac{1}{2}\cdot\dfrac{8}{3} = \dfrac{4}{3}$이다. 따라서 $f(c) = 4/3$인 $c = 2/\sqrt{3}$가 구간에 있다. 평균 함수값 $4/3$은 중점의 함수값 $f(1) = 1$과 일반적으로 다르다.

4.8 넓이 · 변위 · 누적량의 모델

두 연속 그래프 사이의 넓이는 위 함수와 아래 함수의 차이를 적분한다. 어느 함수가 위에 있는지 바뀌면 교점을 기준으로 구간을 나눈다. 함수 차이에 절댓값을 붙여 $\int |f-g|$로 쓰는 것도 같은 뜻이다.

> **예제 4.22 (두 곡선 사이의 넓이)** $y = 2x$와 $y = x^2$의 교점은 $x = 0, 2$다. 그 사이에서 $2x \ge x^2$이므로 넓이는
>
> $$\int_0^2 (2x - x^2)\,\mathrm{d}x = \left[x^2 - x^3/3\right]_0^2 = \frac{4}{3}.$$
>
> 둘의 순서를 반대로 적분하면 음수가 되므로 그것은 넓이값이 아니다.

> **예제 4.23 (변위와 이동거리)** 속도가 $v(t) = t - 1$인 입자가 $0 \le t \le 3$ 동안 움직이면 변위는
>
> $$\int_0^3 v(t)\,\mathrm{d}t = \left[t^2/2 - t\right]_0^3 = \frac{3}{2}.$$

이동거리는 속력 $|v|$를 적분하므로

$$\int_0^1 (1-t)\,\mathrm{d}t + \int_1^3 (t-1)\,\mathrm{d}t = \frac{1}{2} + 2 = \frac{5}{2}.$$

처음 1초 동안 음의 방향으로 이동한 거리도 총 이동거리에는 양수로 더한다.

참고 (적분의 단위). 양이 누적되는 단위도 확인해야 한다. 길이당 질량밀도 $\rho(x)$를 길이에 대해 적분하면 질량이 되고, 시간당 유입률을 시간에 대해 적분하면 총 유입량이 된다. 기호의 모양이 같아도 적분함수의 단위와 적분변수의 단위를 곱한 것이 결과의 단위다.

4.9 근사합의 검산과 간단한 오차 보장

원시함수를 구하기 어렵거나 관측 데이터만 있으면 적분을 유한합으로 근사한다. 증가함수의 좌·우 끝점 합은 적분의 아래·위 경계를 직접 준다. 등간격 n분할에서는 두 합의 차이가 $(b-a)(f(b)-f(a))/n$이다. 함수의 단조성이 확인되었다면 근사값뿐 아니라 이를 포함하는 구간도 제시할 수 있다.

예제 4.24 (제곱함수 적분의 범위) $f(x)=x^2$를 $[0,1]$에서 10등분하면

$$L_{10} = \frac{9\cdot 10\cdot 19}{6000} = 0.285, \qquad R_{10} = \frac{10\cdot 11\cdot 21}{6000} = 0.385.$$

따라서 참값 $1/3$은 이 사이에 있다. 두 값의 평균 0.335는 사다리꼴 근사이고 이 예에서는 참값보다 $1/600$만큼 크다. 단조성만으로는 이 더 작은 오차를 자동으로 주장할 수 없으며, 제곱함수의 정확한 합 공식으로 검산한 결과다.

역사 (Riemann과 Darboux의 두 정식화). Bernhard Riemann은 1854년 교수자격논문에서 삼각급수로 나타낼 수 있는 함수의 범위를 다루며 현재 리만적분으로 불리는 적분가능성 기준을 리만합의 수렴으로 처음 제시했다(레마 4.2의 형태). Jean Gaston Darboux는 1875년 무렵 상한·하한으로 정의되는 위·아래 합을 도입하여 같은 적분을 동치인 방식으로 재정식화했다(정의 4.2). 오늘날 교과서에서는 다루기 쉬운 Darboux의 정식화로 적분을 정의하고, 리만의 원래 판정 기준을 명제 4.3의 동치 조건으로 증명하는 경우가 많다.

핵심 수식

$$\frac{\mathrm{d}}{\mathrm{d}x}\int_a^x f(t)\,\mathrm{d}t = f(x) \qquad \text{(기본정리 제1부)} \tag{4.1}$$

$$\int_a^b f(x)\,\mathrm{d}x = G(b)-G(a), \quad G'=f \qquad \text{(기본정리 제2부)} \tag{4.2}$$

4.10 연습문제와 해설

연습문제 4.25 $[0,2]$의 상수함수 $f=3$에서 임의의 분할에 대한 위합과 아래합을 구하라.

풀이. 모든 구간의 상한·하한이 3이므로 두 합은 모두 $3\sum \Delta x_i = 6$이다. 분할을 더 잘게 할 필요도 없이 적분이 6으로 결정된다.

연습문제 4.26 $[0,1]$에서 $f(1/2)=7$이고 나머지 점에서 0인 함수의 리만적분을 구하라.

풀이. 아래합은 0이다. $1/2$를 포함하는 구간들의 총 길이를 $\varepsilon/7$보다 작게 만들면 위합은 ε보다 작다. 따라서 적분은 0이다. 한 점의 높이는 양수여도 누적 길이가 0이어서 정적분을 바꾸지 않는다.

연습문제 4.27 $F(x)=\int_{1}^{x^3}\cos(t^2)\,dt$의 도함수를 구하라.

풀이. 적분함수 $\cos(t^2)$는 연속이므로 기본정리 제1부와 연쇄법칙으로 $F'(x)=\cos(x^6)\cdot 3x^2=3x^2\cos(x^6)$이다. 적분함수의 t를 x^3으로 바꾸면 내부 제곱은 x^6이 된다.

연습문제 4.28 $\int_{-1}^{2}(2x+1)\,dx$와 $\int_{-1}^{2}|2x+1|\,dx$를 비교하라.

풀이. 첫 적분은 $[x^2+x]_{-1}^{2}=6-0=6$이다. 부호는 $x=-1/2$에서 바뀐다. $x\in[-1,-1/2]$에서 $2x+1\le 0$이고 그 구간의 적분은 $[x^2+x]_{-1}^{-1/2}=(-1/4)-0=-1/4$이므로, 음수인 부분의 적분은 $-1/4$다. 절댓값 적분은 부호를 바꾼 양만큼을 더해 $6+2\cdot(1/4)=13/2$다. 직접 구간을 나누어도 같은 값을 얻는다.

연습문제 4.29 연속인 f가 $[0,1]$에서 $2\le f\le 5$를 만족할 때 적분에 대해 무엇을 보장할 수 있는가?

풀이. 명제 4.9에 의해 $2\le\int_0^1 f\le 5$이며 구간 평균값도 같은 범위에 있다. 특정 함수값을 더 알지 못하면 하나의 정확한 적분값을 결정할 수는 없다.

연습문제 4.30 $\int_0^1 f=0$이고 f가 연속이면 반드시 $f=0$인가? $f\ge 0$을 추가하면 어떤가?

풀이. 추가 가정이 없으면 $f(x)=x-1/2$가 반례다. $f\ge 0$까지 있으면 명제 4.11에 의해 f는 모든 점에서 0이다.

정적분을 원시함수로 계산할 수 있게 되었지만 원시함수를 구하는 방법은 별도로 필요하다. 다음 장에서는 미분법을 거꾸로 읽는 치환·부분적분과, 무한구간을 극한으로 처리하는 이상적분을 다룬다(제8권 제5장).

제 5 장

적분기법과 이상적분

개요 적분기법은 미분 규칙을 거꾸로 적용하여 원시함수(*antiderivative*)를 구성하는 절차들의 모음이고, **이상적분**(*improper integral*)은 무한구간이거나 적분함수가 유계가 아닌 점을 포함하는 적분의 수렴을 유한구간 적분의 극한으로 정의하는 이론이다. 치환적분은 연쇄법칙에서, 부분적분은 곱의 법칙에서 각각 나오며, 유리함수의 부분분수 분해와 삼각함수·제곱근 치환은 이 두 기법을 구체적인 식의 모양에 적용하는 방법이다. 공식을 적용한 뒤에는 원시함수를 다시 미분해 검산하고, 정의역과 적분 한계가 보존되는지 확인해야 한다. 이상적분에서는 유한구간 계산을 마친 뒤 적분 한계(무한대이거나 특이점에 다가가는 끝점)의 극한이 존재하는지 판단하는 절차가 하나 더 필요하다. 원시함수에 기호 ∞를 숫자처럼 대입하거나 내부 특이점을 건너뛰어 끝점만 제외하는 방법은 올바른 정의가 아니다. 비교판정과 절대수렴은 정확한 값을 구하지 않고도 수렴 여부와 오차의 크기를 판단하는 수단을 준다. 선행 지식: 미분의 연쇄법칙과 곱의 법칙, 미적분 기본정리(제8권 제4장), 극한과 부등식을 사용한다.

5.1 원시함수의 기본 표와 구간

연속한 구간에서 성립하는 기본 공식은 다음과 같다.

핵심 수식

$$\int x^{\alpha}\,dx = \frac{x^{\alpha+1}}{\alpha+1} + C, \qquad \alpha \neq -1,\ x > 0, \tag{5.1}$$

$$\int \frac{1}{x}\,dx = \log|x| + C, \qquad x \neq 0, \tag{5.2}$$

$$\int e^{x}\,dx = e^{x} + C, \tag{5.3}$$

$$\int \cos x\,dx = \sin x + C, \tag{5.4}$$

$$\int \sin x\,dx = -\cos x + C, \tag{5.5}$$

$$\int \frac{1}{1+x^{2}}\,dx = \arctan x + C. \tag{5.6}$$

정수 지수 등에서는 식 (5.1)의 정의역을 더 넓힐 수 있다. 식 (5.2)에서 $1/x$의 정의역은 서로 떨어진 두 구간 $(-\infty,0)$과 $(0,\infty)$이므로, 두 구간에서 원시함수의 적분상수는 서로 달라도 된다. 하나의 연결된 구간에서만 두 원시함수의 차이가 하나의 상수라는 평균값정리의 결과를 쓴다.

예제 5.1 (역미분으로 검산) $x \neq 0$에서

$$\int \left(4x^{3} - 2x^{-2}\right)\,dx = x^{4} + \frac{2}{x} + C$$

이다. 양변을 미분하면 $4x^3 - 2/x^2$으로 돌아온다. x^{-2}의 지수를 하나 올리면 x^{-1}이고 나누는 수가 -1이므로 부호가 바뀐다.

5.2 치환적분: 변수와 한계를 함께 바꾸기

정리 5.2 (치환적분) f가 관련 구간에서 연속이고 g가 $[a,b]$에서 C^1이며 그 값들이 f의 정의역에 있으면

$$\int_a^b f(g(x))g'(x)\,dx = \int_{g(a)}^{g(b)} f(u)\,du \tag{5.7}$$

이다.

증명. f의 원시함수 F를 택하면 연쇄법칙으로 $(F\circ g)' = f(g)g'$이다. 양변에 미적분 기본정리를 적용하면 좌변과 우변은 모두 $F(g(b)) - F(g(a))$가 된다. □

참고. 식 (5.7)은 g가 단조일 필요가 없다. $f(g(x))g'(x)$라는 피적분함수의 구조와 $f\circ g$, g'의 연속성만으로 증명되었기 때문이다. 반면 x를 u의 단일한 역함수로 풀어 피적분함수 전체를 u의 식으로 다시 쓰는 계산에서는 역함수의 가지와 단조 구간을 별도로 확인해야 한다. 이 두 사용법을 구분하면 치환공식의 가정을 지나치게 제한하거나 지나치게 넓히는 오류를 피할 수 있다.

예제 5.3 (한 번의 치환으로 끝나는 적분) $u = x^2$라 두면 $du = 2x\,dx$이며 새 끝점은 $u(0)=0$, $u(1)=1$이다. 따라서

$$\int_0^1 2xe^{x^2}\,dx = \int_0^1 e^u\,du = e - 1.$$

부정적분이면 답을 $e^{x^2}+C$로 원래 변수에 되돌릴 수 있다. 정적분에서는 변수와 한계를 모두 바꿨다면 u로 계산을 끝내도 된다.

예제 5.4 (한계가 뒤집히는 치환) $u = \cos x$라 두면 $du = -\sin x\,dx$이고 $x = 0, \pi/2$에 대응하는 새 끝점은 $u = 1, 0$이다. 따라서

$$\int_0^{\pi/2} \sin x\cos x\,dx = -\int_1^0 u\,du = \int_0^1 u\,du = \frac{1}{2}$$

이다. du의 음수 부호와 감소하는 한계의 방향을 둘 다 기록해야 한다. 둘 중 하나만 처리하면 부호가 틀어진다.

예제 5.5 (미분계수가 숨어 있는 형태) $\int x/(1+x^2)\,dx$에서 $u = 1+x^2$라 두면 $du = 2x\,dx$이므로 답은 $\tfrac{1}{2}\log(1+x^2)+C$다. 괄호 안이 항상 양수이므로 절댓값 없이 로그를 쓸 수 있다. 검산하면 $(1/2)\cdot 2x/(1+x^2)$이 되어 계수 $1/2$의 필요성을 확인한다.

5.3 부분적분: 곱의 법칙을 거꾸로 쓰기

곱의 법칙(제8권 제2장)의 양변을 적분하면 다음 정리를 얻는다.

정리 5.6 (부분적분) u, v가 $[a,b]$에서 C^1이면

$$\int_a^b u(x)v'(x)\,dx = \big[u(x)v(x)\big]_a^b - \int_a^b u'(x)v(x)\,dx \tag{5.8}$$

이다.

증명. $(uv)' = u'v + uv'$를 적분하고 미적분 기본정리를 적용한 뒤 항을 이항하면 식 (5.8)을 얻는다. □

어느 부분을 미분할지 선택하면 새 적분이 더 쉬워질 수 있다. 다항식은 미분하면 차수가 낮아지고, 로그는 미분하면 유리함수가 되며, 지수·삼각함수는 적분해도 비슷한 형태를 유지한다. 이런 구조를 기준으로 고르되, 정해진 이름 순서만으로 모든 적분이 단순해진다고 보장하지는 않는다.

예제 5.7 (다항식과 지수함수) $u = x$, $v' = e^x$로 두면 $v = e^x$이고

$$\int x e^x \, \mathrm{d}x = x e^x - \int e^x \, \mathrm{d}x = (x-1)e^x + C$$

이다. 따라서 $\int_0^1 x e^x \, \mathrm{d}x = \left[(x-1)e^x\right]_0^1 = 1$이다. 정적분에서는 부분적분의 경계항도 반드시 남겨야 한다.

예제 5.8 (로그를 적분하기) $x > 0$에서 $u = \log x$, $v' = 1$로 두면

$$\int \log x \, \mathrm{d}x = x \log x - x + C$$

이다. 원래 피적분함수가 하나의 인자처럼 보여도 $\log x \cdot 1$이라는 곱으로 볼 수 있다. 이 식은 뒤에서 $\int_0^1 \log x \, \mathrm{d}x$의 이상적분을 계산할 때도 쓰이되, 0에서의 극한을 따로 취해야 한다(예제 5.19).

예제 5.9 (원래 적분으로 돌아오는 경우) $I = \int e^x \sin x \, \mathrm{d}x$라 놓고 두 번 부분적분하면

$$I = e^x \sin x - \int e^x \cos x \, \mathrm{d}x = e^x \sin x - e^x \cos x - I$$

이다. 상수는 최종적으로 합쳐

$$I = \frac{1}{2} e^x (\sin x - \cos x) + C$$

를 얻는다. 같은 적분이 다시 나왔다는 이유로 실패한 것이 아니라, I에 대한 대수적으로 풀 수 있는 방정식이 생긴 것이다.

5.4 유리함수와 부분분수

유리함수의 분자 차수가 분모 차수 이상이면 먼저 다항식 나눗셈을 한다. 나머지 분수의 분모를 실수에서 인수분해하면 일차인자와 기약 이차인자로 나눌 수 있다. 반복인자 $(x-a)^k$에 대해서는 1부터 k까지 각 차수의 항을 모두 포함해야 한다.

예제 5.10 (서로 다른 일차인자)

$$\frac{1}{x(x+1)} = \frac{1}{x} - \frac{1}{x+1}$$

이므로 $x \neq 0, -1$의 각 연결 구간에서

$$\int \frac{1}{x(x+1)}\,dx = \log|x| - \log|x+1| + C$$

이다. 분수를 합쳐 원래 식과 같아지는지 검산할 수 있다. 이 원시함수 표현이 특이점 0이나 -1을 가로지르는 정적분의 수렴까지 보장하지는 않는다.

예제 5.11 (반복인자의 두 항)

$$\frac{2x+1}{(x-1)^2} = \frac{2}{x-1} + \frac{3}{(x-1)^2}$$

이므로 원시함수는 $2\log|x-1| - 3/(x-1) + C$다. 분자를 $2(x-1)+3$으로 다시 쓰면 계수들이 바로 보인다. $(x-1)^{-2}$ 항만 넣으면 일반적인 분자를 표현할 수 없다.

완전제곱 $x^2+2x+5 = (x+1)^2+4$를 만들면 역탄젠트 적분으로 연결된다. 예를 들어

$$\int \frac{dx}{x^2+2x+5} = \frac{1}{2}\arctan\frac{x+1}{2} + C$$

이다. 분자에 $x+1$이 있다면 분모의 도함수와 비례하므로 로그 항도 함께 나올 수 있다.

5.5 삼각함수와 제곱근 치환

$\sin^2 x = (1-\cos 2x)/2$ 같은 항등식은 거듭제곱 적분을 단순하게 만든다. 제곱근 $\sqrt{a^2-x^2}$에는 $x = a\sin\theta$, $\sqrt{a^2+x^2}$에는 $x = a\tan\theta$ 같은 치환이 맞지만, 제곱근의 부호를 결정할 구간을 함께 정해야 한다.

예제 5.12 (제곱 항등식)

$$\int_0^{\pi} \sin^2 x\,dx = \int_0^{\pi} \frac{1-\cos 2x}{2}\,dx = \frac{\pi}{2}.$$

흔한 오류. $\sin^2 x$를 $\sin(x^2)$로 읽으면 전혀 다른 함수가 된다. 지수와 괄호의 위치를 구분한다.

예제 5.13 (반원의 넓이) $a > 0$일 때 $x = a\sin\theta$, $-\pi/2 \le \theta \le \pi/2$로 두면 $\cos\theta \ge 0$이므로 $\sqrt{a^2-x^2} = a\cos\theta$다. 따라서

$$\int_{-a}^{a} \sqrt{a^2-x^2}\,dx = a^2\int_{-\pi/2}^{\pi/2} \cos^2\theta\,d\theta = \frac{\pi a^2}{2}$$

이며, 이는 반원 넓이와 일치한다.

흔한 오류. 임의의 θ에서 $\sqrt{a^2\cos^2\theta} = a\cos\theta$라고 쓰면 틀리고, 일반적으로는 $a|\cos\theta|$다. 예제 5.13에서 선택한 구간 $-\pi/2 \le \theta \le \pi/2$이 $\cos\theta \ge 0$을 보장하여 절댓값을 제거하게 해 준다.

초등적인 피적분함수가 항상 초등적인 원시함수를 갖는 것은 아니다. 그런 경우에도 정적분은 정의될 수 있고, 급수나 수치적분으로 원하는 오차 이내의 값을 얻을 수 있다. 이 권의 계산법 목록은 모든 적분을 닫힌 식으로 바꾼다는 약속이 아니다.

5.6 무한구간의 이상적분

정의 5.14 (무한구간 이상적분) f가 모든 유한구간 $[a, R]$에서 적분가능할 때

$$\int_a^{\infty} f(x)\,\mathrm{d}x = \lim_{R\to\infty} \int_a^{R} f(x)\,\mathrm{d}x$$

의 유한한 극한이 존재하면 **이상적분이 수렴**한다고 한다. $\int_{-\infty}^{b}$도 같은 방식이다. 양방향 무한구간에서는 하나의 유한한 c를 정해 두 적분 $\int_{-\infty}^{c} f$와 $\int_{c}^{\infty} f$가 각각 수렴할 때 그 합으로 정의한다.

흔한 오류. 원시함수에 기호 ∞를 숫자처럼 그대로 대입하는 것은 정의가 아니다. 정의 5.14이 요구하는 것은 어디까지나 유한한 극한 $\lim_{R\to\infty}$의 존재다.

예제 5.15 (p-적분의 무한대 판정) $p \neq 1$이면

$$\int_1^{R} x^{-p}\,\mathrm{d}x = \frac{R^{1-p}-1}{1-p}$$

이다. $R\to\infty$일 때 $p>1$이면 $R^{1-p}\to 0$이므로

$$\int_1^{\infty} x^{-p}\,\mathrm{d}x = \frac{1}{p-1} \qquad (p>1)$$

으로 수렴하고, $p<1$이면 $R^{1-p}\to\infty$여서 발산한다. $p=1$이면 $\int_1^R x^{-1}\,\mathrm{d}x = \log R \to \infty$여서 역시 발산한다. 따라서 $\int_1^{\infty} x^{-p}\,\mathrm{d}x$는 $p>1$일 때에만 수렴한다. 함수값이 0으로 간다는 것만으로 적분의 수렴을 보장하지 않는 대표적 예다.

예제 5.16 (지수 감쇠와 꼬리 오차) $\alpha>0$이면

$$\int_0^{\infty} e^{-\alpha x}\,\mathrm{d}x = \frac{1}{\alpha}, \qquad \int_R^{\infty} e^{-\alpha x}\,\mathrm{d}x = \frac{e^{-\alpha R}}{\alpha}.$$

두 번째 식은 무한구간을 $[0,R]$에서 잘랐을 때의 정확한 꼬리 오차다. $\alpha=0$이면 상수함수여서 발산하고, $\alpha<0$이면 함수가 증가하므로 역시 수렴하지 않는다.

5.7 유한 끝점의 특이성과 내부 분할

정의 5.17 (끝점 이상적분) f가 $(a,b]$에서 정의되고 모든 $[c,b]$, $c>a$에서 적분가능하면

$$\int_a^{b} f = \lim_{c\downarrow a} \int_c^{b} f$$

의 유한한 존재로 왼쪽 끝점 이상적분을 정의한다. 오른쪽 끝점도 마찬가지다. 내부 특이점 $s\in(a,b)$가 있으면 $\int_a^s f$와 $\int_s^b f$가 각각 수렴해야 한다.

예제 5.18 (p-적분의 0 근처 판정)

$$\int_0^{1} x^{-p}\,\mathrm{d}x$$

는 $p<1$일 때에만 수렴하며 값은 $1/(1-p)$이다. 계산식은 같은 거듭제곱 원시함수이지만, 이제 작은 끝점 $c\downarrow 0$에서 c^{1-p}를 살핀다. 무한대에서의 조건 $p>1$(예제 5.15)과 방향이 반대다.

예제 5.19 (값은 발산하지만 적분은 수렴) $x \downarrow 0$일 때 $\log x \to -\infty$이지만

$$\int_0^1 \log x \, dx = \lim_{c \downarrow 0} \big[x \log x - x\big]_c^1 = -1$$

이다. 여기서 $c \log c \to 0$이다. $c = e^{-t}$로 바꾸면 $c \log c = -te^{-t} \to 0$임을 확인할 수 있다. 적분함수의 발산과 적분의 발산은 다른 질문이다.

예제 5.20 (주값과 이상적분은 다르다) 대칭적으로 자른 합은

$$\int_{-1}^{-\varepsilon} \frac{dx}{x} + \int_{\varepsilon}^{1} \frac{dx}{x} = 0$$

이지만 $\int_{-1}^{0} dx/x$와 $\int_{0}^{1} dx/x$는 각각 발산한다. 따라서 보통의 이상적분 $\int_{-1}^{1} dx/x$는 수렴하지 않는다. 대칭적 제한에서 얻은 0은 **Cauchy 주값**이라는 별도 개념이다.

주의. 양쪽 발산을 임의로 상쇄하여 Cauchy 주값을 정적분값이라 쓰지 않는다. 정의 5.17가 요구하는 두 독립적인 극한(또는 정의 5.14의 두 독립적인 극한)을 각각 확인해야 한다.

5.8 비교판정과 절대수렴

정리 5.21 (비음함수 비교판정) 충분히 큰 x에서 $0 \le f(x) \le g(x)$이고 각 함수가 유한 부분구간에서 적분가능하다고 하자. $\int_a^\infty g$가 수렴하면 $\int_a^\infty f$도 수렴한다. $\int_a^\infty f$가 발산하면 $\int_a^\infty g$도 발산한다.

증명. 비음함수의 잘린 적분 $F(R) = \int_a^R f$는 R에 대해 비감소한다. 위에서 유계이면 실수의 완비성(제1권 제6장)으로 유한한 극한을 갖는다. $f \le g$는 $F(R)$의 상한을 제공한다. 발산에 관한 주장은 같은 부등식의 반대 방향 추론이다. 유한한 초기구간의 적분은 수렴 여부에 영향을 주지 않는다. $\square$

참고 (극한비교판정). $f, g > 0$이고 $f/g \to L$ with $0 < L < \infty$이면 충분한 근방에서 $(L/2)g \le f \le (3L/2)g$로 두 함수가 서로의 양의 상수배 사이에 놓이므로, 정리 5.21에 의해 두 적분은 함께 수렴하거나 함께 발산한다. $L = 0$이면 $\int g$의 수렴이 $\int f$의 수렴을 보장하지만 $\int g$의 발산에서는 $\int f$에 대해 결론을 낼 수 없고, $L = \infty$이면 그 반대로 $\int g$의 발산이 $\int f$의 발산을 보장할 뿐이다.

예제 5.22 (꼬리의 비교) $x \ge 1$에서 $0 < 1/(1+x^2) \le 1/x^2$이므로 $\int_1^\infty dx/(1+x^2)$는 수렴한다. 실제 값은 $\big[\arctan x\big]_1^\infty = \pi/4$다. $x/(1+x^2)$는 $1/x$와의 비가 $x^2/(1+x^2) \to 1$이므로 무한대 적분이 발산한다.

부호가 바뀌는 함수에서 $\int |f|$가 수렴하면 $\int f$도 수렴하며 이를 **절대수렴**(*absolute convergence*)이라 한다. 유한구간에서 $\left|\int_R^S f\right| \le \int_R^S |f|$이므로 절댓값 적분의 꼬리가 작아지면 원래 적분의 꼬리도 작아지고, 실수의 완비성에 따른 Cauchy 조건으로 극한이 존재한다. 원래 적분은 수렴하지만 절댓값 적분이 발산하면 **조건수렴**(*conditional convergence*)이라 한다.

5.9 진동에 의한 수렴의 한 예

예제 5.23 ($\sin x/x$의 무한대 적분) $1 \le R < S$에서 부분적분하면

$$\int_R^S \frac{\sin x}{x}\,dx = \left[-\frac{\cos x}{x}\right]_R^S - \int_R^S \frac{\cos x}{x^2}\,dx$$

이다. 따라서 절댓값은

$$\frac{1}{R} + \frac{1}{S} + \int_R^S x^{-2}\,dx \le \frac{2}{R}$$

이하이다. $R \to \infty$이면 모든 $S > R$에 대해 이 값이 작아지므로 $\int_1^\infty \sin x/x\,dx$는 수렴한다. 이는 정확한 적분값을 구하지 않고도 수렴과 꼬리 상한을 보인 것이다.

반면 절댓값 적분은 발산한다. 각 $[k\pi + \pi/6,\ k\pi + 5\pi/6]$에서 $|\sin x| \ge 1/2$이고 $x \le (k+1)\pi$이므로 해당 구간의 적분은 적어도

$$\frac{1}{2}\cdot\frac{2\pi/3}{(k+1)\pi} = \frac{1}{3(k+1)}$$

이다. 이 하한들을 더하면 조화급수가 되어 발산한다(조화급수의 발산은 제8권 제6장에서 묶음이나 적분비교로 증명한다). 따라서 $\int_1^\infty \sin x/x\,dx$는 조건수렴의 예다. 양수 부분과 음수 부분의 상쇄를 통제하는 진동 구조가 수렴의 원인이다.

5.10 연습문제와 해설

연습문제 5.24 $\displaystyle\int_0^1 3x^2\sqrt{1+x^3}\,dx$를 구하라.

풀이. $u = 1 + x^3$으로 두면 한계는 1에서 2이고 $du = 3x^2\,dx$이다. 값은

$$\int_1^2 u^{1/2}\,du = \frac{2}{3}\left(2^{3/2} - 1\right)$$

이다. 치환 후에도 원래의 0과 1을 한계로 남기면 안 된다.

연습문제 5.25 $\displaystyle\int_0^1 x\log(1+x)\,dx$를 부분적분으로 구하라.

풀이. $u = \log(1+x)$, $v' = x$라 두면 값은 $\frac{1}{2}\log 2 - \frac{1}{2}\int_0^1 x^2/(1+x)\,dx$다. $x^2/(1+x) = x - 1 + 1/(1+x)$이므로 남은 적분은 $-1/2 + \log 2$이고, 결과는

$$\frac{1}{2}\log 2 - \frac{1}{2}\left(-\frac{1}{2} + \log 2\right) = \frac{1}{4}$$

이다.

연습문제 5.26 $\displaystyle\int_1^\infty x^{-3/2}\,dx$와 $\displaystyle\int_0^1 x^{-3/2}\,dx$의 수렴을 비교하라.

풀이. 무한대에서는 $p = 3/2 > 1$이므로 수렴하고 값은 2다. 0 근처에서는 $p < 1$ 조건이 실패하므로 발산한다. 같은 함수라도 어느 끝점을 보는지에 따라 판정이 달라진다.

연습문제 5.27 $\displaystyle\int_0^{\infty} e^{-2x}\,\mathrm{d}x$를 $[0,R]$에서 잘라 오차를 10^{-4} 이하로 만들려면 어떤 R이면 충분한가?

풀이. 꼬리 오차는 $e^{-2R}/2$다. $e^{-2R}/2 \le 10^{-4}$를 풀면 $R \ge \tfrac{1}{2}\log 5000$이면 된다. 근삿값을 계산하지 않아도 이 식이 명시적인 오차 보장을 준다.

연습문제 5.28 $\displaystyle\int_0^{1} \mathrm{d}x/(x(1+x))$의 수렴을 판정하라.

풀이. 0 근처에서 $1/[x(1+x)]$와 $1/x$의 비가 1이므로 발산한다. 또는 $0<x\le 1$에서 피적분함수가 $1/(2x)$ 이상임을 써도 된다. 부분분수의 원시함수를 찾았다는 사실과 이상적분의 수렴은 별개다.

연습문제 5.29 $\displaystyle\int_{-\infty}^{\infty} x/(1+x^2)\,\mathrm{d}x$를 대칭 상쇄로 0이라 할 수 있는가?

풀이. 대칭적으로 $[-R,R]$만 적분하면 홀함수여서 0이지만, 양쪽 반직선 적분은 각각 발산한다. 보통의 이상적분은 존재하지 않고 대칭 주값만 0이다. 정의가 요구하는 두 독립적인 극한을 확인해야 한다.

연습문제 5.30 $\displaystyle\int_0^{\infty} |\sin x|\,e^{-x}\,\mathrm{d}x$가 수렴함을 정확한 원시함수 없이 보이라.

풀이. $0 \le |\sin x|\,e^{-x} \le e^{-x}$이고 지수함수의 적분이 1로 수렴하므로 비교판정으로 수렴한다. 따라서 $\int_0^{\infty} \sin x\,e^{-x}\,\mathrm{d}x$도 절대수렴한다.

이상적분의 수렴에서는 작은 꼬리들이 누적되어 유한한 값에 도달하는지를 보았다. 급수도 같은 질문을 이산적인 합에 대해 묻는다. 다음 장(제8권 제6장)은 수열·급수의 수렴과 함수의 Taylor 근사를 연결하되, 무한히 미분가능하다는 사실과 급수 표현의 일치를 구별한다.

제 6 장

수열·급수와 Taylor 근사의 조건 및 오차

개요 수열의 수렴, 급수의 수렴, 함수가 자신의 Taylor 급수와 일치하는 것은 모두 무한과정을 다루지만 서로 다른 정의를 가지는 세 가지 질문이다. 수열의 수렴은 항이 어떤 값에 다가가는지를, 급수의 수렴은 부분합이라는 수열의 수렴을, Taylor 근사가 참함수와 같아지는 조건은 유한 다항식의 나머지가 0으로 가는지를 각각 묻는다. 계산기 화면의 소수 몇 자리나 그래프만으로는 이 가운데 어느 것도 판단할 수 없다. 이 장은 수열의 ε-N 수렴 정의(제1권 제6장의 실수의 완비성에 의지한다)에서 출발하여 단조수렴, 부분수열, Cauchy 조건을 세우고, 이를 급수의 수렴 판정(비교·적분·비율·근·교대급수 판정)과 거듭제곱급수의 수렴반지름으로 확장한다. 마지막으로 유한 Taylor 다항식의 Lagrange 나머지와 적분형 나머지를 증명하고, 나머지가 0으로 가는 조건을 확인해야만 무한 Taylor 급수가 원래 함수와 같아진다는 것을 보인다. 유한한 Taylor 다항식은 가까운 곳의 근사식이고, 무한 Taylor 급수는 부분합의 극한이며, 다항식 근사의 오차를 0으로 보낼 수 있을 때에만 그 무한합이 원래 함수를 나타낸다. 이 조건을 확인하는 것이 전개의 마지막 단계이며 가장 중요한 검산이다. 선행 지식: 극한의 정의, 평균값정리(제8권 제3장), 정적분과 이상적분의 비교판정(제8권 제5장)을 사용한다. 무한합은 유한합의 극한으로 정의한다.

6.1 수열의 수렴과 기본 성질

정의 6.1 (수열의 수렴) 실수 수열 (a_n)이 L로 **수렴**한다는 것은 임의의 $\varepsilon > 0$에 대해 어떤 정수 N이 존재하여 $n \ge N$이면 $|a_n - L| < \varepsilon$라는 뜻이다. 이때 $a_n \to L$이라 쓴다.

함수 극한과 달리 입력이 자연수이므로 충분히 뒤에 있는 모든 항을 제어한다. 유한개의 처음 항은 수렴값을 바꾸지 않는다. 수렴 수열은 유계이며 극한은 유일하다. 유계성은 뒤의 항들이 $L \pm 1$ 사이에 있고 남은 처음 항은 유한개라는 사실로 보인다. 유일성은 두 후보 극한 사이의 거리를 삼각부등식으로 비교하면 된다.

예제 6.2 (명시적인 항 번호) $a_n = 1/n$이면 $n > 1/\varepsilon$일 때 $|a_n| < \varepsilon$이므로 0으로 수렴한다. $a_n = (3n+1)/(n+2)$는

$$a_n - 3 = -\frac{5}{n+2}$$

이므로 3으로 수렴한다. 예컨대 오차를 10^{-3}보다 작게 하려면 $n + 2 > 5000$이면 충분하다.

예제 6.3 (유계성만으로 부족) $a_n = (-1)^n$은 -1과 1 사이에 있지만 수렴하지 않는다. 짝수 부분수열은 1, 홀수 부분수열은 -1이므로 하나의 극한이 존재할 수 없다. 반면 $(-1)^n/n$은 절댓값이 $1/n$이어서 조임정리로 0에 수렴한다.

수열에도 합·곱·몫의 극한 법칙과 조임정리가 성립한다. 몫은 분모의 극한이 0이 아닐 때 적용한다. $a_n \to L$이고 f가 L에서 연속이며 각 항이 정의역에 있으면 $f(a_n) \to f(L)$이다. 점화식의 양변에 극한을 취할 때 바로 이 연속성을 사용한다.

6.2 단조수렴과 반복수열

정리 6.4 (단조수렴) 위로 유계인 비감소 실수 수열은 수렴한다. 아래로 유계인 비증가 실수 수열도 수렴한다.

증명. 첫 경우 $L = \sup\{a_n : n \in \mathbb{N}\}$이라 놓는다. 실수의 완비성(제1권 제6장)에 의해 이 상한은 존재한다. 상한의 정의로 임의의 $\varepsilon > 0$에 대해 $L - \varepsilon < a_N \le L$인 항이 있다. $n \ge N$이면 단조성으로 $L - \varepsilon < a_N \le a_n \le L$이므로 수렴 정의를 만족한다. 둘째는 $-a_n$에 적용한다. $\square$

예제 6.5 (먼저 수렴을 증명하고 방정식을 푼다) $a_1 = 1$, $a_{n+1} = \sqrt{2 + a_n}$이라 하자. $0 < a_n < 2$이면 $0 < a_{n+1} < 2$이므로 귀납적으로 2가 상한이다. $a_2 > a_1$이고 제곱근 함수가 증가하므로 $a_{n+1} > a_n$도 귀납적으로 성립한다. 따라서 수렴하며 극한을 L이라 하면 연속성으로 $L = \sqrt{2 + L}$이다. $L^2 - L - 2 = 0$의 두 근 중 $L \ge 0$인 값은 2이므로 $a_n \to 2$다.

주의. 수렴을 보이기 전에 $L = \sqrt{2 + L}$만 풀면 가능한 극한 후보만 얻은 것이다. 실제로 수열이 발산하거나 여러 값 사이를 오갈 수 있으므로, 극한 방정식의 해가 존재한다는 사실이 원래 반복 수열의 수렴 증명을 대신하지는 않는다.

6.3 부분수열과 Cauchy 조건

인덱스 $n_1 < n_2 < \cdots$를 택해 얻은 (a_{n_k})를 **부분수열**이라 한다. 원래 수열이 L로 수렴하면 모든 부분수열도 같은 L로 수렴한다. 역으로 어떤 부분수열 하나가 수렴한다고 전체 수열이 수렴하지는 않는다.

정리 6.6 (Bolzano–Weierstrass 정리) 유계 실수 수열은 수렴하는 부분수열을 가진다.

증명. 한 증명은 모든 항을 담는 닫힌 구간을 절반씩 나누면서 무한히 많은 항을 포함하는 절반을 계속 고르는 것이다. 구간 길이는 0으로 가고 실수의 완비성으로 공통 극한점이 존재한다. 각 단계에서 인덱스를 증가시키며 그 구간 안의 항을 하나씩 선택하면 그 점으로 수렴하는 부분수열을 얻는다. $\square$

역사. 수열의 ε-N 수렴 정의는 Augustin-Louis Cauchy가 1821년 저서 *Cours d'analyse*에서 제시한 형태에 가깝고, 정리 6.6는 Bernard Bolzano와 Karl Weierstrass의 이름을 딴 것이다.

정의 6.7 (Cauchy 수열) 임의의 $\varepsilon > 0$에 대해 어떤 N이 존재하여 $m, n \ge N$이면 $|a_m - a_n| < \varepsilon$인 수열을 **Cauchy 수열**이라 한다.

실수에서는 수렴과 Cauchy 조건이 동치이다. 수렴하면 $|a_m - a_n| \le |a_m - L| + |a_n - L|$로 바로 보인다. Cauchy 수열은 유계이므로 정리 6.6에 의해 수렴 부분수열을 갖고, Cauchy 조건으로 나머지 충분히 뒤의 항들도 그 부분수열의 극한에 가까움을 보이면 전체가 수렴한다. 이 조건은 극한값을 미리 몰라도 수렴을 보일 수 있다는 장점이 있다.

예제 6.8 (인접 항 차이가 작다는 것과 다르다) $a_n = \sum_{k=1}^{n} 1/k$이면 $a_{n+1} - a_n = 1/(n+1) \to 0$이다. 하지만

$$a_{2n} - a_n = \sum_{k=n+1}^{2n} \frac{1}{k} \ge \frac{1}{2}$$

이므로 Cauchy 조건이 실패한다. 이웃한 항만 비교하는 것과 모든 충분히 뒤의 두 항을 비교하는 것은 다르다.

6.4 급수의 정의와 첫 번째 판정

정의 6.9 (급수의 수렴) 수열 (a_n)의 **급수** $\sum_{n=1}^{\infty} a_n$이 수렴한다는 것은 부분합 $S_N = \sum_{n=1}^{N} a_n$이 유한한 극한 S를 가진다는 뜻이다. 그때 합을 S라 한다. 꼬리 또는 나머지는 $R_N = S - S_N$이다.

명제 6.10 (일반항의 필요조건) 급수가 수렴하면 $a_n \to 0$이다.

증명. $n \ge 2$에서 $a_n = S_n - S_{n-1}$이고 두 부분합 수열이 같은 S로 수렴하므로 차이는 0으로 간다. □

역은 성립하지 않는다. 조화급수 $\sum 1/n$은 일반항이 0으로 가지만

$$1 + \frac{1}{2} + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \cdots + \frac{1}{8}\right) + \cdots$$

에서 각 괄호의 합이 $1/2$ 이상이므로 부분합이 제한 없이 커진다. 일반항 조건은 수렴의 빠른 탈락 검사이며, 통과했다고 수렴이 확정되는 판정은 아니다.

예제 6.11 (등비급수와 정확한 꼬리) $r \neq 1$이면 $1 + r + \cdots + r^N = (1 - r^{N+1})/(1 - r)$이다. $|r| < 1$이면

$$\sum_{n=0}^{\infty} r^n = \frac{1}{1 - r}, \qquad R_N = \frac{r^{N+1}}{1 - r}.$$

$r = 1$이면 부분합이 증가하고 $r = -1$이면 진동한다. $|r| > 1$이면 일반항도 0으로 가지 않는다. 따라서 이 등비급수는 정확히 $|r| < 1$에서 수렴한다.

예제 6.12 (망원급수)

$$\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$$

이므로 $S_N = 1 - 1/(N+1)$이고 $\sum_{n=1}^{\infty} 1/[n(n+1)] = 1$이다. 무한히 많은 항을 막연히 취소한 것이 아니라 유한 부분합을 먼저 정리한 뒤 극한을 취했다. 오차는 정확히 $1/(N+1)$이다.

6.5 양항급수의 비교판정과 적분판정

$a_n \ge 0$이면 부분합은 비감소한다. 따라서 양항급수는 부분합이 위로 유계일 때에만 수렴한다. $0 \le a_n \le b_n$이 충분히 큰 n에서 성립하면 $\sum b_n$ 수렴은 $\sum a_n$ 수렴을, $\sum a_n$ 발산은 $\sum b_n$ 발산을 보장한다.

또 $a_n, b_n > 0$이고 $a_n / b_n \to L \in (0, \infty)$이면 충분히 뒤에서 $(L/2) b_n \le a_n \le (3L/2) b_n$으로 끼울 수 있어 두 급수의 수렴 여부가 같다. 유한개의 처음 항은 수렴 여부를 바꾸지 않는다.

정리 6.13 (적분판정과 나머지 경계) f가 $[1, \infty)$에서 연속·비음·비증가하고 $a_n = f(n)$이라 하자. 급수 $\sum a_n$과 이상적분(제8권 제5장) $\int_1^{\infty} f$는 함께 수렴하거나 함께 발산한다. 수렴할 때

$$\int_{N+1}^{\infty} f(x)\,\mathrm{d}x \le R_N \le \int_{N}^{\infty} f(x)\,\mathrm{d}x. \tag{6.1}$$

증명. 각 $[n, n+1]$에서 $f(n+1) \le f(x) \le f(n)$이므로 적분하여 직사각형의 넓이와 비교한다. n에 대해 합한 뒤 유한 상한을 무한대로 보내면 수렴 판정과 식 (6.1)의 꼬리 부등식을 동시에 얻는다. □

예제 6.14 (p-급수와 오차) $p > 0$에서 x^{-p}에 적분판정을 적용하면 $\sum_{n=1}^{\infty} n^{-p}$는 정확히 $p > 1$에서 수렴한다. $p \le 0$에서는 일반항이 0으로 가지 않아 발산한다. $p = 2$인 경우

$$\frac{1}{N+1} \le \sum_{n=N+1}^{\infty} \frac{1}{n^2} \le \frac{1}{N}.$$

따라서 처음 1000항을 더하면 오차는 10^{-3} 이하라는 보장을 얻는다. 합의 정확한 값이 무엇인지 알 필요는 없다.

예제 6.15 (경계 차수의 로그) $\sum_{n=2}^{\infty} 1/[n(\log n)^{q}]$는 $q > 1$일 때 수렴하고 $q \le 1$일 때 발산한다. 함수는 충분히 큰 곳에서 양수·감소하며 $u = \log x$ 치환으로

$$\int_{2}^{\infty} \frac{\mathrm{d}x}{x(\log x)^{q}} = \int_{\log 2}^{\infty} u^{-q}\, \mathrm{d}u$$

가 되어 p-적분 판정에 연결된다. $1/n$에 가까운 식에서는 작은 로그 요인이 실제로 수렴 여부를 바꿀 수 있다.

6.6 비율판정과 근판정

정리 6.16 (비율판정) 충분히 뒤에서 $a_n \neq 0$이고 $|a_{n+1}/a_n| \to L$이라고 하자. $L < 1$이면 $\sum a_n$은 절대수렴한다. $L > 1$이면 일반항이 0으로 가지 않아 발산한다. $L = 1$이면 이 판정만으로 결론을 낼 수 없다.

증명. $L < 1$이면 $L < q < 1$을 택하여 충분히 뒤에서 $|a_{n+1}| \le q\,|a_n|$로 제한할 수 있다. 귀납적으로 뒤의 항들이 수렴하는 등비급수의 항 이하이므로 절댓값 급수가 수렴한다. $L > 1$이면 어떤 $q > 1$에 대해 충분히 뒤에서 $|a_{n+1}| \ge q\,|a_n|$이므로 0으로 갈 수 없다. □

근판정은 $|a_n|^{1/n} \to L$일 때 $L < 1$이면 절대수렴, $L > 1$이면 발산이며 $L = 1$은 미정이라는 대응 결과다. $L < q < 1$을 택하면 $|a_n| \le q^{n}$으로 비교할 수 있어 증명의 원리는 같다. 극한 대신 상극한을 사용한 더 일반적 형태도 있지만 이 권의 예에서는 보통의 극한으로 충분하다.

예제 6.17 (팩토리얼과 지수) 고정된 실수 x에 대해 $a_n = x^{n}/n!$이면 $x \neq 0$에서

$$\left|\frac{a_{n+1}}{a_n}\right| = \frac{|x|}{n+1} \to 0.$$

따라서 $\sum x^{n}/n!$은 모든 실수 x에서 절대수렴한다. $x = 0$은 첫 항 뒤가 모두 0이라 즉시 수렴한다. 아직 이 합이 e^{x}라는 사실까지 보인 것은 아니며, 그 동일성은 Taylor 나머지로 뒤에서 확인한다(예제 6.29).

예제 6.18 (판정이 미정인 경우) $a_n = 1/n$과 $b_n = 1/n^{2}$는 모두 이웃 항 비의 극한이 1이다. 앞의 급수는 발산하고 뒤의 급수는 수렴한다.

흔한 오류. 비율판정의 결과가 1이면 "발산"이 아니라 "다른 방법이 필요함"이라고 기록해야 한다(예제 6.18).

6.7 교대급수와 절대수렴

정리 6.19 (교대급수 판정과 오차) $b_n \ge 0$이 비증가하고 $b_n \to 0$이면

$$S = \sum_{n=1}^{\infty} (-1)^{n-1} b_n$$

은 수렴한다. 부분합 S_N의 오차는 $|S - S_N| \le b_{N+1}$이며 나머지의 부호는 다음 항의 부호와 같거나 0이다.

증명. 짝수 부분합은 $(b_{2k-1} - b_{2k}) \ge 0$을 더하므로 비감소하고, 홀수 부분합은 비증가한다. 각 짝수 부분합은 뒤의 홀수 부분합 이하이고 두 종류의 차이는 $b_n \to 0$인 하나의 항이다. 단조수렴(정리 6.4)으로 공통 극한이 존재하며 그 값은 인접한 두 부분합 사이에 있다. 따라서 오차는 두 부분합 차이인 다음 항의 크기 이하이다. □

예제 6.20 (교대 조화급수) $1 - 1/2 + 1/3 - 1/4 + \cdots$는 교대급수 판정으로 수렴하고, 처음 N항의 오차는 $1/(N+1)$ 이하이다. 절댓값 급수는 조화급수여서 발산하므로 조건수렴한다. 합이 $\log 2$라는 식은 예제 6.30에서 확인한다.

정리 6.21 (절대수렴이면 수렴) $\sum |a_n|$이 수렴하면 $\sum a_n$도 수렴한다.

증명. $m > n$에 대해 $|S_m - S_n| \le \sum_{k=n+1}^{m} |a_k|$이다. 오른쪽은 절댓값 급수의 Cauchy 조건으로 충분히 작은 값이 되므로 원래 부분합도 Cauchy 수열이다. 실수의 완비성으로 수렴한다. □

절대수렴 급수는 순서를 바꾸어도 합이 같다. 절댓값 꼬리합을 ε보다 작게 만드는 유한개의 핵심 항을 먼저 정한 뒤, 새 순서에서도 그 항들이 모두 포함되는 곳을 택하면 남은 차이를 꼬리 절댓값으로 제어할 수 있다. 조건수렴 급수에서는 이런 제어가 없으므로, 유한합에서 쓰던 임의의 순서 교환을 그대로 허용하면 안 된다.

6.8 거듭제곱급수와 수렴반지름

거듭제곱급수(*power series*)는 $\sum_{n=0}^{\infty} c_n (x-a)^n$ 꼴이다. 어떤 **수렴반지름** $R \in [0, \infty]$가 존재하여 $|x-a| < R$에서는 절대수렴, $|x-a| > R$에서는 발산한다. 경계 $x = a \pm R$에서는 각 점을 따로 검사해야 한다.

수렴 영역이 이런 모양인 이유는, 한 점 $x_0 \ne a$에서 수렴하면 항 $c_n (x_0-a)^n$들이 유계이고, 더 안쪽의 x에서는

$$|c_n (x-a)^n| \le M \left| \frac{x-a}{x_0-a} \right|^n$$

이라는 등비 비교가 되기 때문이다. 그러므로 한 점에서 수렴하면 중심에 더 가까운 모든 점에서 절대수렴한다.

참고 (Cauchy–Hadamard 공식). 반지름은 계수의 성장률로 정확히

$$R = \frac{1}{\limsup_{n\to\infty} |c_n|^{1/n}}$$

로 주어지며(관례로 $1/0 = \infty$, $1/\infty = 0$), 가능한 경우에는 비율판정으로 더 쉽게 구할 수 있다.

예제 6.22 (끝점마다 다른 결론)

$$\sum_{n=1}^{\infty} \frac{x^n}{n}$$

의 비율 극한은 $|x|$이므로 반지름은 1이다. $x = 1$에서는 조화급수로 발산하고 $x = -1$에서는 교대급수로 수렴한다. 따라서 실수 수렴구간은 $[-1, 1)$이다. 반지름만으로 양 끝점의 포함 여부를 결정할 수 없다.

반지름 안에서는 항별 미분·적분이 가능하며 얻은 거듭제곱급수의 수렴반지름도 같다. 닫힌 작은 구간 $|x - a| \le r < R$에서 더 큰 $r < s < R$를 택하면 계수들을 등비급수로 균등하게 제어할 수 있기 때문이다. 미분 항의 추가 인자 n도 $n(r/s)^n$의 수렴으로 제어된다. 이 균등한 꼬리 제어가 합과 미분·적분을 교환하는 근거다. 경계점에서는 이 정리를 그대로 적용하지 않는다.

예제 6.23 (등비급수를 미분해 합 구하기) $|x| < 1$에서 $\sum_{n=0}^{\infty} x^n = 1/(1-x)$를 미분하면

$$\sum_{n=1}^{\infty} n x^{n-1} = \frac{1}{(1-x)^2}.$$

양변에 x를 곱하고 $x = 1/2$를 넣으면 $\sum_{n=1}^{\infty} n/2^n = 2$이다. 항별 미분을 수렴반지름 내부에서 했다는 조건이 계산을 정당화한다.

6.9 유한 Taylor 정리와 Lagrange 나머지

정의 6.24 (Taylor 다항식) f가 a에서 n차까지 미분가능하면 n차 **Taylor 다항식**은

$$T_n(x) = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!}(x-a)^k$$

이다. $a = 0$이면 **Maclaurin 다항식**이라 한다.

계수 $1/k!$는 k번 미분한 값을 맞추기 위해 필요하다. $T_n^{(k)}(a) = f^{(k)}(a)$ for $0 \le k \le n$이며 이러한 차수 이하의 다항식은 유일하다. 그러나 한 점에서의 도함수 일치만으로 멀리 떨어진 모든 점에서 정확하다는 뜻은 아니다.

정리 6.25 (Taylor 정리: 충분한 가정의 한 형태) a와 x를 포함하는 닫힌 구간의 열린 근방에서 f가 C^{n+1}이라고 하자. $x \ne a$이면 두 점 사이의 어떤 ξ에 대해

$$f(x) = T_n(x) + R_n(x), \qquad R_n(x) = \frac{f^{(n+1)}(\xi)}{(n+1)!}(x-a)^{n+1}. \tag{6.2}$$

특히 두 점 사이에서 $\left|f^{(n+1)}\right| \le M$이면

$$|R_n(x)| \le \frac{M\,|x-a|^{n+1}}{(n+1)!}. \tag{6.3}$$

증명. x를 고정하고 $K = [f(x) - T_n(x)]/(x-a)^{n+1}$라 놓는다. 함수

$$H(t) = f(t) - T_n(t) - K(t-a)^{n+1}$$

는 $H(x) = H(a) = 0$이고 $H'(a) = \cdots = H^{(n)}(a) = 0$이다. Rolle 정리(제8권 제3장)를 먼저 a, x 사이에 적용하고, 얻은 영점과 a 사이에 다시 적용하는 과정을 반복하면 어떤 ξ에서 $H^{(n+1)}(\xi) = 0$이다. 따라서 $f^{(n+1)}(\xi) - (n+1)!K = 0$이고 K를 원래 식에 대입하면 식 (6.2)을 얻는다. $\square$

C^{n+1}은 이해하기 쉬운 충분조건이며 더 약한 가정으로도 정리를 만들 수 있다. 여기서는 각 단계의 연속성과 미분가능성이 Rolle 정리에 충분하도록 명시했다. 중요한 것은 나머지의 도함수를 중심점 a에서만이 아니라 두 점 사이 전체에서 제어한다는 점이다.

예제 6.26 (지수함수의 실제 오차) e^x를 0에서 3차까지 근사하면 $T_3(x) = 1 + x + x^2/2 + x^3/6$이다. $x = 0.1$에서는 $T_3 = 1.1051666\ldots$이고

$$|R_3(0.1)| \le \frac{e^{0.1}(0.1)^4}{24} < \frac{2 \cdot 10^{-4}}{24} < 8.34 \cdot 10^{-6}.$$

여기서는 간단한 상한 $e^{0.1} < 2$를 사용했다. 실제 도함수 상한을 더 좁히면 보장도 더 좋아진다. 근삿값과 오차 상한을 함께 제시해야 유효한 자릿수를 판단할 수 있다.

예제 6.27 (사인 근사의 차수 선택) $\sin x$의 0에서 4차 Taylor 다항식은 $x - x^3/6$이다. 짝수차 계수가 0이므로 표시된 최고차는 3이지만 4차까지 맞춘 다항식이다. 5차 도함수의 절댓값이 1 이하이므로

$$\left|\sin x - \left(x - \frac{x^3}{6}\right)\right| \le \frac{|x|^5}{120}.$$

3차 정리는 $|x|^4/24$라는 상한을 준다. $0 < |x| < 5$에서는 위의 5차 오차 상한이 더 작다. 두 상한의 비교는 x의 범위에 따라 달라진다.

6.10 적분형 나머지와 선형근사의 보강

충분히 연속인 고계도함수가 있으면 반복적인 미적분 기본정리와 부분적분으로

$$R_n(x) = \frac{1}{n!}\int_a^x f^{(n+1)}(t)(x-t)^n \, \mathrm{d}t \tag{6.4}$$

라는 적분형 나머지를 얻는다. $n = 0$에서는 기본정리 $f(x) - f(a) = \int_a^x f'$이다. 일반 n은 적분형 나머지를 부분적분하여 한 차수 낮은 나머지와 Taylor 항으로 나누는 귀납법으로 확인할 수 있다. 방향 있는 적분 덕분에 $x < a$에서도 성립한다.

예제 6.28 (제곱근 선형근사의 오차) $f(x) = \sqrt{x}$를 $a = 4$에서 선형근사하면 $T_1(x) = 2 + (x-4)/4$이다(제8권 제2장). $[4, 4.04]$에서 $|f''(x)| = 1/(4x^{3/2}) \le 1/32$이므로

$$\left|\sqrt{4.04} - 2.01\right| \le \frac{1/32}{2}(0.04)^2 = 0.000025.$$

또 $f'' < 0$이어서 함수는 오목하므로 접선 근사 2.01이 참값 이상이다. 선형근사에 이제 오차의 크기와 방향이 모두 붙었다.

나머지 공식은 최적화의 이계도함수 판정도 설명한다. $f'(a)=0$이고 f''가 연속이며 $f''(a)>0$이면 가까운 $x\neq a$에서 $f(x)-f(a)=\tfrac{1}{2}f''(\xi)(x-a)^2>0$이다. 국소최소는 값의 부호만이 아니라 해당 근방의 도함수 제어에서 나온다.

6.11 Taylor 급수가 실제 함수와 같아지는 조건

무한히 미분가능한 함수의 Taylor 급수는

$$\sum_{k=0}^{\infty}\frac{f^{(k)}(a)}{k!}(x-a)^k$$

이다. 이 급수가 수렴할 수는 있지만 그 합이 반드시 $f(x)$인 것은 아니다. 정의상 부분합이 $T_n(x)$이므로 두 값이 같을 필요충분조건은 $R_n(x)=f(x)-T_n(x)\to 0$이다.

예제 6.29 (지수함수와 삼각함수의 전개) 고정된 x에 대해 $a=0$과 x 사이의 모든 지수함수 도함수는 $e^{|x|}$ 이하로 제한된다. 따라서

$$|R_n(x)|\le e^{|x|}\frac{|x|^{n+1}}{(n+1)!}\to 0.$$

마지막 수열의 연속 항 비는 $|x|/(n+2)\to 0$이므로 0으로 간다. 따라서 모든 실수에서

$$e^x=\sum_{n=0}^{\infty}\frac{x^n}{n!},\tag{6.5}$$

$$\sin x=\sum_{n=0}^{\infty}\frac{(-1)^n x^{2n+1}}{(2n+1)!},\tag{6.6}$$

$$\cos x=\sum_{n=0}^{\infty}\frac{(-1)^n x^{2n}}{(2n)!}.\tag{6.7}$$

사인·코사인은 모든 도함수의 절댓값이 1 이하이므로 같은 논증이 더 간단하다. 무한 미분가능성 외에 나머지가 0으로 간다는 별도의 검증을 했다.

예제 6.30 (로그 전개와 끝점 확인) $|x|<1$에서 $1/(1+x)=\sum_{k=0}^{\infty}(-x)^k$를 0에서 x까지 항별 적분하면

$$\log(1+x)=\sum_{n=1}^{\infty}\frac{(-1)^{n-1}x^n}{n}.$$

$x=1$은 정리 6.25의 내부 적용 범위 밖이지만, 유한 등비식

$$\frac{1}{1+t}=\sum_{k=0}^{N-1}(-t)^k+\frac{(-t)^N}{1+t}$$

을 $[0,1]$에서 적분하면 나머지 절댓값이 $\int_0^1 t^N\,\mathrm{d}t=1/(N+1)$ 이하이다. 따라서 끝점에서도

$$\log 2=1-\frac{1}{2}+\frac{1}{3}-\cdots$$

가 정당화된다(예제 6.20). $x=-1$에서는 원래 로그가 정의되지 않고 급수도 음의 조화급수로 발산한다.

6.12 매끄럽지만 Taylor 급수와 다른 반례

예제 6.31 (한 점에서 모든 도함수가 0)

$$f(x) = \begin{cases} e^{-1/x^2}, & x \neq 0, \\ 0, & x = 0 \end{cases}$$

를 생각하자. 임의의 $m > 0$에 대해 $|x|^{-m} e^{-1/x^2} \to 0$이다. $t = 1/x^2 \to \infty$로 바꾸면 $t^{m/2} e^{-t} \to 0$이라는 지수 감쇠 성질이 된다. 예를 들어 $e^t \geq t^k/k!$에서 $k > m/2$를 택하면 바로 제어된다.

$x \neq 0$에서 f를 반복 미분하면 $1/x$의 다항식에 e^{-1/x^2}를 곱한 형태다. 위의 감쇠를 이용하면 이 식들의 극한이 모두 0이고, 0에서 차분몫으로 미분하는 과정에도 같은 성질이 적용된다. 귀납적으로 모든 $f^{(n)}(0) = 0$이다. 따라서 0에서의 Taylor 급수는 영급수지만 $x \neq 0$에서는 $f(x) > 0$이다.

핵심. 예제 6.31의 함수는 모든 차수로 미분가능하지만 원점 근처에서 자신의 Taylor 급수와 일치하지 않는다. 자기 Taylor 급수와 어떤 근방에서 일치하는 함수를 그 점에서 **해석적**(*analytic*)이라고 한다. 실변수에서 매끄러움과 해석성은 다른 성질이다. 초등 미적분에서 흔히 쓰는 지수·삼각·로그 함수는 적절한 구간에서 해석적이지만, 그 익숙한 사례를 모든 매끄러운 함수로 확대하면 안 된다.

이 반례는 유한 근사 정리가 실패한다는 뜻이 아니다. 고정된 차수에서는 Taylor 정리가 여전히 성립하며, 원점에 가까워질수록 이 함수는 그 어떤 고정된 거듭제곱보다도 작다. 문제는 고정된 비영 x에서 차수를 무한히 올릴 때 나머지가 0으로 간다고 자동으로 결론 내릴 수 없다는 것이다.

6.13 판정과 오차를 함께 고르는 절차

방법 (판정과 오차의 선택). 급수나 근사식을 만났을 때 먼저 질문을 나눈다. 일반항이 0으로 가는가, 절댓값을 취하면 수렴하는가, 부호의 상쇄를 이용해야 하는가, 실제 합의 근사가 필요한가를 구분한다. 수렴 판정만으로 원하는 자릿수가 자동으로 얻어지지는 않는다.

양항 p-급수에는 적분 꼬리 경계(식 (6.1)), 교대급수에는 다음 항 경계(정리 6.19), 등비급수에는 정확한 꼬리식(예제 6.11), 함수 근사에는 Taylor 나머지(식 (6.3) 또는 식 (6.4))가 자연스럽다. 비율판정으로 수렴을 보였더라도 충분히 뒤에서의 비를 $q < 1$로 제한하면 남은 꼬리를 등비급수로 제어할 수 있다.

예제 6.32 (팩토리얼 급수의 꼬리를 직접 제어) $e = \sum_{n=0}^{\infty} 1/n!$의 N차 부분합 뒤 첫 항은 $1/(N+1)!$이다. 이후 이웃 항 비는 모두 $1/(N+2)$ 이하이므로

$$0 < R_N \leq \frac{1}{(N+1)!} \cdot \frac{1}{1 - 1/(N+2)}.$$

$N = 6$이면 상한은 $8/(7 \cdot 5040) = 1/4410$이다. 이는 "급수가 수렴한다"보다 더 구체적으로, 해당 유한합이 참값보다 작으며 차이가 얼마 이하인지 알려 준다.

6.14 연습문제와 해설

연습문제 6.33 $a_n = (2n^2-1)/(n^2+3)$의 극한을 구하고 유계성이 어떻게 확인되는지 설명하라.

풀이. $a_n = 2 - 7/(n^2+3)$이므로 극한은 2다. $n \ge 1$에서 $1/4 \le a_n < 2$여서 유계성도 직접 확인된다. 유계성만으로 수렴을 증명한 것이 아니라 정확한 차이가 0으로 감을 사용했다.

연습문제 6.34 $\sum_{n=1}^{\infty} 3/4^n$의 합과 처음 N항의 오차를 구하라.

풀이. 첫 항은 3/4, 공비는 1/4이므로 합은 1이다. N항 뒤 꼬리는 $3\cdot 4^{-(N+1)}/(1-1/4) = 4^{-N}$이다. 시작 인덱스가 0인지 1인지에 따라 첫 항과 합이 달라진다.

연습문제 6.35 $\sum_{n=1}^{\infty} n/(n^3+1)$의 수렴을 판정하라.

풀이. $1/n^2$와의 비가 $n^3/(n^3+1) \to 1$이다. $p=2$ 급수가 수렴하므로 극한비교판정으로 수렴한다. 도함수를 계산하거나 합의 정확한 값을 구할 필요가 없다.

연습문제 6.36 $\sum_{n=1}^{\infty} (-1)^{n-1}/\sqrt{n}$은 절대수렴인가, 조건수렴인가?

풀이. $1/\sqrt{n}$은 감소하여 0으로 가므로 교대급수는 수렴한다. 절댓값 급수는 $p=1/2$여서 발산한다. 따라서 조건수렴이다. N항 근사의 오차는 $1/\sqrt{N+1}$ 이하이다.

연습문제 6.37 $\sum_{n=1}^{\infty} (x-2)^n/n^2$의 수렴반지름과 실수 수렴구간을 구하라.

풀이. 비율판정의 극한은 $|x-2|$이므로 반지름은 1이다. $x=3$에서는 $\sum 1/n^2$, $x=1$에서는 $\sum (-1)^n/n^2$가 되어 둘 다 절대수렴한다. 따라서 수렴구간은 $[1,3]$이다.

연습문제 6.38 $\cos x$를 $1 - x^2/2$로 근사할 때 모든 실수 x에 대해 $\left|\cos x - 1 + x^2/2\right| \le |x|^4/24$임을 보이라.

풀이. 0에서의 3차 Taylor 다항식은 홀수차 계수가 0이어서 $1 - x^2/2$이다. 4차 도함수 $\cos\xi$의 절댓값이 1 이하이므로 Lagrange 나머지(식 (6.3))에 의해 결론이 성립한다. $|x|$가 커지면 경계가 커져 근사의 실용성은 낮아질 수 있다.

연습문제 6.39 $\log(1+x)$의 0에서 2차 Taylor 다항식으로 $\log 1.1$을 근사하고 오차 상한을 구하라.

풀이. $T_2(x) = x - x^2/2$이므로 값은 0.095다. $[0, 0.1]$에서 세 번째 도함수 $2/(1+x)^3$는 2 이하이므로 오차는 $2(0.1)^3/6 = 1/3000$ 이하이다. 세 번째 도함수가 양수이므로 참값은 이 근사보다 크다.

연습문제 6.40 어떤 함수가 모든 차수로 미분가능하고 $f^{(n)}(0) = 0$ for all n이라면 반드시 원점 근처에서 영함수인가?

풀이. 아니다. 예제 6.31의 e^{-1/x^2}를 0에서 0으로 확장한 함수가 반례다. 해석적이라는 가정을 추가하면 Taylor 급수와 일치하므로 어떤 원점 근방에서 영함수라고 결론 내릴 수 있다. 매끄러움과 해석성을 구분해야 한다.

일변수 미적분의 핵심은 극한·변화율·누적량·오차를 연결하는 조건들이다. 여러 변수로 확장하면 미분은 선형사상(제9권 제2장), 이계미분은 이차형식(제9권 제3장)으로 나타난다. 무한차원

이론으로 나아갈 때에는 수열과 함수열의 수렴 방식이 미분·적분과 언제 교환되는지가 새로운 중심 문제가 된다(제10권 제2장).

제 9 권

다변수 · 벡터해석

제9권은 일변수 미적분을 $\mathbb{R}^n$ 위의 함수로 확장하고 벡터해석의 세 적분 정리까지 이르는 권이다. 제1장은 유클리드 노름으로 거리와 열린집합, 극한과 연속을 정의하고, 제2–3장은 편미분·전미분·연쇄법칙과 Hessian을 이용한 다변수 Taylor 정리와 극값 판정을 다룬다. 제4장은 선형근사가 가역이면 원래 사상도 국소적으로 가역이라는 생각에서 역함수 정리, 음함수 정리, Lagrange 승수법을 이끌어낸다. 제5–7장은 중적분과 Fubini 정리, 선적분·면적분, Green·Stokes·발산 정리를 세우고, 제8장은 이 세 정리가 미분형식의 일반화된 Stokes 정리 하나에서 나온다는 것을 입문 수준으로 보인다.

제 1 장

$\mathbb{R}^n$의 거리, 열린집합, 극한과 연속

개요 이 장은 $\mathbb{R}^n$ 위에 유클리드 노름으로 거리를 정의하고, 그 거리로 열린집합·점열의 수렴과 완비성·콤팩트성을 차례로 세운 뒤, 이 언어로 다변수 함수의 극한과 연속을 다시 정의한다. 일변수 미적분에서 "x가 a에 가까워진다"는 말은 수직선 위의 거리 $|x-a|$로 정확히 정해지지만, 여러 변수에서는 점이 a에 접근하는 방향이 무한히 많다. 그래서 거리를 먼저 정하고, 열린집합·수렴·콤팩트성을 거리로 정의한 뒤 극한과 연속을 다시 말한다. 이 순서를 지키면 "모든 직선을 따라 극한이 같으면 극한이 존재한다"는 식의 잘못된 추론을 피할 수 있다. 선행 지식: 제7권의 벡터공간과 내적, 제8권의 일변수 극한과 연속, 제1권의 실수 완비성.

1.1 유클리드 공간과 노름

$\mathbb{R}^n$은 실수 n개의 순서쌍 $x=(x_1,\dots,x_n)$의 집합이며 성분별 덧셈과 스칼라곱으로 벡터공간이 된다. 표준 내적과 **유클리드 노름**(*Euclidean norm*)을

$$x\cdot y=\sum_{i=1}^{n}x_iy_i,\qquad \|x\|=\sqrt{x\cdot x}$$

로 정의한다. 두 점 사이의 **거리**(*distance*)는 $\|x-y\|$이다.

명제 1.1 (Cauchy–Schwarz와 삼각부등식) 모든 $x,y\in\mathbb{R}^n$에 대해 $|x\cdot y|\le\|x\|\|y\|$이고 $\|x+y\|\le\|x\|+\|y\|$이다. 첫 부등식의 등호는 x,y가 일차종속일 때 그리고 그때에만 성립한다.

증명. $y=0$이면 자명하다. $y\neq 0$이면 모든 실수 t에 대해

$$0\le\|x-ty\|^2=\|x\|^2-2t\,x\cdot y+t^2\|y\|^2.$$

$t=(x\cdot y)/\|y\|^2$을 대입하면 $0\le\|x\|^2-(x\cdot y)^2/\|y\|^2$이다. 등호는 $x=ty$일 때이다. 삼각부등식은 $\|x+y\|^2=\|x\|^2+2x\cdot y+\|y\|^2\le(\|x\|+\|y\|)^2$에서 얻는다. □

역사 (Cauchy–Schwarz 부등식). 이 부등식은 급수에 대해 Augustin-Louis Cauchy가 1821년에, 적분에 대해 Viktor Bunyakovsky가 1859년에, 다시 Hermann Schwarz가 1888년에 독립적으로 증명하였다. 그래서 "Cauchy–Schwarz" 또는 "Cauchy–Bunyakovsky–Schwarz" 부등식이라 불린다.

노름은 유클리드 노름만 있는 것이 아니다.

정의 1.2 (노름) 함수 $N:\mathbb{R}^n\to[0,\infty)$가 모든 $x,y\in\mathbb{R}^n$과 $c\in\mathbb{R}$에 대해

$$N(x)=0\iff x=0,\qquad N(cx)=|c|N(x),\qquad N(x+y)\le N(x)+N(y)$$

를 만족하면 N을 **노름**(*norm*)이라 한다.

자주 쓰는 예는

$$\|x\|_1 = \sum_{i} |x_i|, \qquad \|x\|_\infty = \max_i |x_i|$$

이다. 이들은 서로 상수배로 비교된다.

$$\|x\|_\infty \le \|x\| \le \|x\|_1 \le \sqrt{n}\,\|x\| \le n\|x\|_\infty. \tag{1.1}$$

셋째 부등식은 $(1,\dots,1)$과 $(|x_1|,\dots,|x_n|)$에 Cauchy–Schwarz를 적용한 결과이다. 유한차원에서는 실제로 모든 노름이 서로 동치이며(이 장의 콤팩트성 결과로 증명된다), 따라서 아래에서 정의하는 열린집합·수렴·연속은 어떤 노름을 써도 같다. 무한차원 함수공간에서는 이 사실이 실패하며 이는 제13권의 주제이다.

1.2 열린 공, 열린집합, 닫힌집합

정의 1.3 (열린 공, 열린집합, 닫힌집합) 점 $a \in \mathbb{R}^n$과 $r > 0$에 대해 $B(a,r) = \{x : \|x-a\| < r\}$를 **열린 공**(*open ball*)이라 한다. 집합 $U \subseteq \mathbb{R}^n$의 모든 점 a에 대해 $B(a,r) \subseteq U$인 $r > 0$이 있으면 U를 **열린집합**(*open set*)이라 한다. 여집합이 열린집합인 집합을 **닫힌집합**(*closed set*)이라 한다.

열린 공 자체가 열린집합이다. $x \in B(a,r)$이면 $s = r - \|x-a\| > 0$에 대해 삼각부등식으로 $B(x,s) \subseteq B(a,r)$이기 때문이다. 열린집합의 임의의 합집합과 유한 교집합은 열린집합이다. 유한이라는 조건은 필요하다. $\bigcap_{k\ge 1} B(0,1/k) = \{0\}$은 열린집합이 아니다.

정의 1.4 (내부, 폐포, 경계) 집합 $S \subseteq \mathbb{R}^n$에 대해 **내부** $\operatorname{int} S$는 S에 포함되는 열린 공을 가진 점들의 집합이고, **폐포** $\overline{S}$는 모든 열린 공이 S와 만나는 점들의 집합이며, **경계** $\partial S = \overline{S} \setminus \operatorname{int} S$이다. 점 a가 $\overline{S}$에 속할 필요충분조건은 S의 점열 $x_k \to a$가 존재하는 것이다.

예제 1.5 (열린 것도 닫힌 것도 아닌 집합) $S = [0,1)\times(0,1] \subseteq \mathbb{R}^2$를 보자. 점 $(0,1/2) \in S$를 중심으로 하는 어떤 열린 공도 $x < 0$인 점을 포함하므로 S는 열린집합이 아니다. 또 $(1/2,0) \notin S$이지만 $(1/2, 1/k) \in S$가 이 점으로 수렴하므로 여집합이 열린집합이 아니고, S는 닫힌집합도 아니다. $\operatorname{int} S = (0,1)\times(0,1)$, $\overline{S} = [0,1]^2$이다.

흔한 오류 (“열린”과 “닫힌”은 반대말이 아니다). $\emptyset$과 $\mathbb{R}^n$은 둘 다이며, 예제 1.5처럼 둘 다 아닌 집합도 흔하다. 또 열린성은 전체 공간에 따라 달라진다. $[0,1)$은 $\mathbb{R}$에서 열린집합이 아니지만, 전체 공간을 $[0,\infty)$로 잡으면 그 안에서 열린집합이다.

1.3 점열의 수렴과 완비성

정의 1.6 (점열의 수렴과 Cauchy 점열) 점열 $x_k \in \mathbb{R}^n$이 a로 **수렴**한다는 것은 $\|x_k - a\| \to 0$이라는 뜻이다. 점열 x_k가 **Cauchy 점열**(*Cauchy sequence*)이라는 것은 모든 $\varepsilon > 0$에 대해 N이 있어 $j,k \ge N$이면 $\|x_j - x_k\| < \varepsilon$이라는 뜻이다.

식 (1.1)의 노름 비교에 의해 이는 각 성분이 수렴하는 것과 동치이다.

$$|x_{k,i} - a_i| \le \|x_k - a\| \le \sqrt{n}\,\max_i |x_{k,i} - a_i|.$$

마찬가지로 점열이 Cauchy 점열일 필요충분조건은 각 성분 실수열이 Cauchy 수열인 것이다. $\mathbb{R}$이 완비이므로 다음을 얻는다.

명제 1.7 $\mathbb{R}^n$은 **완비**(*complete*)이다. 즉 모든 Cauchy 점열은 $\mathbb{R}^n$의 점으로 수렴한다.

정리 1.8 (Bolzano–Weierstrass) $\mathbb{R}^n$의 유계 점열은 수렴하는 부분점열을 갖는다.

증명. 첫 성분은 유계 실수열이므로 수렴하는 부분수열을 갖는다(제8권). 그 부분점열에서 둘째 성분의 수렴 부분수열을 다시 뽑는다. 이를 n번 반복하면 모든 성분이 수렴하는 부분점열을 얻고, 성분별 수렴은 점열의 수렴과 같다. □

1.4 콤팩트 집합

정의 1.9 (점열 콤팩트) $K \subseteq \mathbb{R}^n$의 모든 점열이 K의 점으로 수렴하는 부분점열을 가지면 K를 (점열) **콤팩트**(*compact*)라고 한다.

정리 1.10 (Heine–Borel의 점열 형태) $K \subseteq \mathbb{R}^n$이 콤팩트일 필요충분조건은 K가 닫혀 있고 유계인 것이다.

증명. 닫혀 있고 유계이면 점열은 유계이므로 Bolzano–Weierstrass로 수렴 부분점열을 갖고, 극한은 닫힌집합 K 안에 있다. 역으로 K가 유계가 아니면 $\|x_k\| \geq k$인 점열은 수렴 부분점열을 가질 수 없다. K가 닫혀 있지 않으면 K 밖의 점 $a \in \overline{K}$로 수렴하는 K의 점열이 있고, 그 모든 부분점열도 $a \notin K$로 수렴하므로 K 안의 극한을 갖지 못한다. □

일반 위상공간에서는 "모든 열린 덮개가 유한 부분덮개를 갖는다"를 콤팩트성의 정의로 쓰며, 거리공간에서는 점열 콤팩트성과 동치이다(제16권). $\mathbb{R}^n$에서는 세 조건 "닫힘과 유계, 점열 콤팩트, 덮개 콤팩트"가 모두 같다. 그러나 무한차원 노름공간에서는 닫힌 단위공이 닫혀 있고 유계이지만 콤팩트가 아니다.

1.5 다변수 함수의 극한

정의 1.11 (다변수 함수의 극한) $f : D \to \mathbb{R}^m$, $D \subseteq \mathbb{R}^n$이고 a가 D의 집적점이라 하자. 모든 $\varepsilon > 0$에 대해 $\delta > 0$이 있어 $x \in D$, $0 < \|x - a\| < \delta$이면 $\|f(x) - L\| < \varepsilon$일 때 $\lim_{x \to a} f(x) = L$이라 한다.

이 정의는 a로 가는 모든 경로를 한꺼번에 통제한다. 한 경로를 따른 극한이 다르면 극한은 존재하지 않지만, 여러 경로의 극한이 같다는 사실만으로 극한의 존재를 결론 낼 수는 없다.

예제 1.12 (직선마다 다른 값) $f(x,y) = \dfrac{xy}{x^2 + y^2}$, $(x,y) \neq (0,0)$. 직선 $y = mx$ 위에서 $f = m/(1+m^2)$로 상수이므로 기울기마다 다른 값을 준다. 따라서 $(0,0)$에서 극한이 없다.

예제 1.13 (모든 직선에서 같아도 극한이 없는 경우) $g(x,y) = \dfrac{x^2 y}{x^4 + y^2}$, $(x,y) \neq (0,0)$. 직선 $y = mx$ $(m \neq 0)$에서 $g = mx^3/(x^4 + m^2x^2) = mx/(x^2 + m^2) \to 0$이고, 두 좌표축 위에서는 $g = 0$이다. 그러나 포물선 $y = x^2$ 위에서는 $g = x^4/(2x^4) = 1/2$이다. 따라서 극한은 존재하지 않는다.

극한이 존재함을 보일 때에는 경로에 의존하지 않는 상계를 찾는 것이 표준 방법이다. 예를 들어 $h(x,y)=\dfrac{x^2y}{x^2+y^2}$는 $x^2\le x^2+y^2$이므로 $|h|\le|y|\le\|(x,y)\|$이고, 따라서 $(0,0)$에서 극한 0을 갖는다. 극좌표 $x=r\cos\theta$, $y=r\sin\theta$로 $|h|\le C(r)$이며 $C(r)\to0$이 θ와 무관함을 보이는 것도 같은 방법이다. θ에 의존하는 상계로는 부족하다는 점을 주의한다.

1.6 연속성과 콤팩트 집합 위의 결과

$f:D\to\mathbb{R}^m$이 $a\in D$에서 **연속**이라는 것은 모든 $\varepsilon>0$에 대해 $\delta>0$이 있어 $x\in D$, $\|x-a\|<\delta$이면 $\|f(x)-f(a)\|<\varepsilon$이라는 뜻이다. 동치로, D 안의 모든 점열 $x_k\to a$에 대해 $f(x_k)\to f(a)$이다. 다항식, 연속함수의 합·곱·합성, 분모가 0이 아닌 곳에서의 몫은 연속이다. f가 D 전체에서 연속일 필요충분조건은 모든 열린집합 V에 대해 $f^{-1}(V)$가 D에서 열린집합인 것이다.

정리 1.14 K가 콤팩트이고 $f:K\to\mathbb{R}^m$이 연속이면 $f(K)$는 콤팩트이다. 특히 $m=1$이면 f는 K 위에서 최댓값과 최솟값을 갖는다.

증명. $f(K)$의 점열 $f(x_k)$를 잡자. K의 콤팩트성으로 $x_{k_j}\to a\in K$인 부분점열이 있고, 연속성으로 $f(x_{k_j})\to f(a)\in f(K)$이다. $m=1$이면 $f(K)$는 닫혀 있고 유계인 실수 집합이므로 상한과 하한을 원소로 포함한다. □

정리 1.15 콤팩트 집합 위의 연속함수는 **균등연속**(*uniformly continuous*)이다.

증명. 아니라고 하면 어떤 $\varepsilon>0$과 $\|x_k-y_k\|<1/k$이지만 $\|f(x_k)-f(y_k)\|\ge\varepsilon$인 점열이 있다. 부분점열을 택해 $x_{k_j}\to a\in K$라 하면 $y_{k_j}\to a$이고, 연속성으로 $f(x_{k_j})-f(y_{k_j})\to0$이 되어 모순이다. □

예제 1.16 (콤팩트성이 빠지면) $f(x,y)=x+y$는 열린 단위원판 $B(0,1)$ 위에서 연속이지만 최댓값이 없다. 상한 $\sqrt{2}$는 경계점 $(1/\sqrt{2},1/\sqrt{2})$에서만 도달되고 그 점은 원판에 속하지 않는다. 유계라는 조건만으로는 부족하고 닫혀 있어야 한다.

유한차원 노름의 동치성도 정리 1.14와 정리 1.15로 증명된다. 임의의 노름 N은 $N(x)\le(\max_i N(e_i))\|x\|_1\le C\|x\|$를 만족하므로 유클리드 노름에 대해 연속이다. 단위구면 $\{\|x\|=1\}$은 콤팩트이므로 N은 거기서 양의 최솟값 c를 갖고, 동차성으로 $c\|x\|\le N(x)\le C\|x\|$를 얻는다.

1.7 연결성과 중간값

집합 S의 임의의 두 점을 S 안의 연속곡선 $\gamma:[0,1]\to S$로 이을 수 있으면 S를 **경로연결**(*path-connected*)이라 한다. 볼록집합, 특히 열린 공은 선분으로 이을 수 있으므로 경로연결이다.

명제 1.17 (중간값 정리의 다변수 형태) S가 경로연결이고 $f:S\to\mathbb{R}$가 연속이며 $f(p)<c<f(q)$이면 $f(x)=c$인 $x\in S$가 있다.

증명. p와 q를 잇는 곡선 γ에 대해 $f\circ\gamma:[0,1]\to\mathbb{R}$는 연속이고 양 끝값이 c를 사이에 둔다. 일변수 중간값 정리로 $f(\gamma(t))=c$인 t가 있다. □

열린집합이 연결되어 있으면(두 개의 서로소인 비어 있지 않은 열린집합의 합으로 나눌 수 없으면) 경로연결이다. 이 사실은 뒤에서 "기울기가 0인 함수는 연결된 열린집합 위에서 상수"

라는 결론에 쓰인다. 연결성이 없으면 결론이 실패한다. $\{x \neq 0\} \subseteq \mathbb{R}$에서 $\operatorname{sgn} x$는 도함수가 0이지만 상수가 아니다.

1.8 연습문제와 해설

연습문제 1.18 $\|x\|_1 \le \sqrt{n}\|x\|$를 증명하고 등호 조건을 구하라.

풀이. $\|x\|_1 = \sum_i 1 \cdot |x_i| \le \sqrt{\sum_i 1^2}\sqrt{\sum_i x_i^2} = \sqrt{n}\|x\|$이다. 등호는 $(|x_1|,\dots,|x_n|)$이 $(1,\dots,1)$의 상수배, 즉 모든 $|x_i|$가 같을 때이다.

연습문제 1.19 $f(x,y) = \dfrac{x^3 - y^3}{x^2 + y^2}$의 $(0,0)$에서의 극한을 판정하라.

풀이. $|x^3 - y^3| \le |x|^3 + |y|^3 \le (|x| + |y|)(x^2 + y^2)$이므로 $|f| \le |x| + |y| \le \sqrt{2}\,\|(x,y)\| \to 0$이다. 극한은 0이며 경로와 무관한 상계로 확인했다.

연습문제 1.20 $S = \{(x,y) : x^2 + y^2 \le 1,\ y \ge 0\}$가 콤팩트인지 판정하고 $f(x,y) = y - x^2$의 최댓값이 존재하는 이유를 말하라.

풀이. S는 두 닫힌 조건의 교집합이므로 닫혀 있고 단위원판에 포함되어 유계이다. 따라서 콤팩트이고 연속함수 f는 최댓값을 갖는다. 실제로 $y \le \sqrt{1 - x^2}$이므로 $f \le \sqrt{1 - x^2} - x^2$이고 $x = 0$, $y = 1$에서 최댓값 1이다.

연습문제 1.21 $\{(x,y) : xy = 1\}$은 닫혀 있는가? 유계인가? 연속함수 $x + y$는 이 집합 위에서 최솟값을 갖는가?

풀이. 연속함수 xy의 값 1의 역상이므로 닫혀 있지만 $(k, 1/k)$가 있어 유계가 아니다. $x, y < 0$인 가지에서 $x + y$는 아래로 유계가 아니므로 최솟값이 없다. 반면 $x, y > 0$인 가지로 제한하면 산술기하평균으로 $x + y \ge 2$이고 $(1,1)$에서 최솟값이 된다. 콤팩트성이 없을 때는 최댓값·최솟값의 존재를 따로 보여야 한다.

연습문제 1.22 열린집합 U의 유한 교집합이 열린집합임을 보이고, 닫힌집합의 무한 합집합이 닫혀 있지 않은 예를 들라.

풀이. $a \in U_1 \cap \cdots \cap U_m$이면 각 j에 대해 $B(a, r_j) \subseteq U_j$이고 $r = \min_j r_j > 0$에 대해 $B(a,r)$이 교집합에 포함된다. 무한 교집합에서는 최솟값이 0이 될 수 있다. 닫힌집합 $[1/k, 1]$의 합집합은 $(0,1]$로 닫혀 있지 않다.

참고 (다음 연결). 거리와 극한이 준비되었으므로 제9권 제2장에서는 여러 변수 함수의 미분을 "가장 좋은 선형근사"로 정의한다. 편미분이 모두 존재해도 미분가능하지 않을 수 있다는 점이 첫 번째 주의점이다.

제 2 장

미분가능성: 편미분, 전미분, 연쇄법칙

개요 이 장은 여러 변수 함수의 미분을 "한 점 근처에서 가장 잘 맞는 선형사상"으로 정의하고, 편미분·방향미분·그래디언트가 그 선형사상의 어떤 정보인지 정리한다. 일변수에서는 도함수가 존재한다는 것과 접선이 존재한다는 것이 같았다. 여러 변수에서는 각 좌표축 방향의 변화율(편미분)이 모두 있어도 함수가 그 점에서 연속조차 아닐 수 있다. 따라서 미분가능성은 편미분의 존재보다 강한 조건으로 정의해야 한다. 선행 지식: 제9권 제1장의 극한과 연속, 제7권의 선형사상과 행렬표현.

2.1 편미분과 방향미분

정의 2.1 (방향미분과 편미분) $U \subseteq \mathbb{R}^n$ 이 열린집합이고 $f : U \to \mathbb{R}$라 하자. $a \in U$와 벡터 $v \in \mathbb{R}^n$에 대해

$$D_v f(a) = \lim_{t \to 0} \frac{f(a + tv) - f(a)}{t}$$

가 존재하면 이를 v 방향의 **방향미분**(*directional derivative*)이라 한다. $v = e_i$일 때를 **편미분**(*partial derivative*)이라 하고 $\partial_i f(a)$ 또는 $\dfrac{\partial f}{\partial x_i}(a)$로 쓴다.

편미분은 다른 변수를 고정하고 한 변수에 대해 일변수 미분을 한 것이다. 예를 들어 $f(x, y) = x^2 y + \sin(xy)$이면 $\partial_x f = 2xy + y\cos(xy)$, $\partial_y f = x^2 + x\cos(xy)$이다. 방향미분의 정의에서 v를 단위벡터로 제한하는 책도 있다. 이 권에서는 일반 벡터를 허용하므로 $D_{2v} f = 2 D_v f$이다.

예제 2.2 (편미분은 있지만 연속이 아닌 함수) $f(x, y) = \dfrac{xy}{x^2 + y^2}$, $f(0,0) = 0$이라 하자. 두 좌표축 위에서 $f = 0$이므로 $\partial_x f(0,0) = \partial_y f(0,0) = 0$이다. 그러나 예제 1.12에서 본 것처럼 $(0,0)$에서 극한이 없으므로 연속이 아니다. 편미분은 두 방향의 정보만 보기 때문이다.

2.2 전미분: 가장 좋은 선형근사

정의 2.3 (미분가능성과 전미분) $f : U \to \mathbb{R}^m$, $a \in U$라 하자. 선형사상 $L : \mathbb{R}^n \to \mathbb{R}^m$이 존재하여

$$\lim_{h \to 0} \frac{\| f(a + h) - f(a) - Lh \|}{\|h\|} = 0$$

이면 f가 a에서 **미분가능**하다고 하고, L을 f의 a에서의 (전)미분 $Df(a)$라 한다.

이 극한은 h가 0으로 가는 모든 방식을 통제한다. L이 존재하면 유일하다. 실제로 $h = tv$를 넣으면 $Lv = \lim_{t\to 0}(f(a+tv) - f(a))/t = D_v f(a)$가 되어 L이 방향미분으로 결정된다. 표준기저에 대한 $Df(a)$의 행렬은 편미분들로 이루어진 **Jacobi 행렬**이다.

$$Df(a) = \left(\frac{\partial f_i}{\partial x_j}(a) \right)_{1 \le i \le m,\, 1 \le j \le n}.$$

역사 (Fréchet 미분). 선형근사로 미분을 정의하는 방법은 **Fréchet 미분**(*Fréchet derivative*)이라 불리며, Maurice Fréchet가 1925년 논문에서 일반적인 노름공간 위의 함수로 확장하였다. 이 장의 정의는 $\mathbb{R}^n$ 위로 제한한 특수한 경우이다.

명제 2.4 f가 a에서 미분가능하면 (i) f는 a에서 연속이고, (ii) 모든 방향미분이 존재하며 $D_v f(a) = Df(a)v$로 v에 대해 선형이다.

증명. (i) $\|f(a+h)-f(a)\| \le \|f(a+h)-f(a)-Lh\| + \|L\|\|h\|$이고 두 항 모두 $h\to 0$일 때 0으로 간다. 여기서 $\|L\|$은 연산자 노름이다. (ii)는 정의 뒤의 계산과 같다. □

예제 2.5 (모든 방향미분이 있어도 미분불가능) $g(x,y) = \dfrac{x^2 y}{x^2+y^2}$, $g(0,0)=0$. 제9권 제1장에서 보았듯 g는 연속이다. $v=(v_1,v_2)\neq 0$이면 $g(tv) = t v_1^2 v_2/(v_1^2+v_2^2)$이므로

$$D_v g(0,0) = \frac{v_1^2 v_2}{v_1^2+v_2^2}.$$

이 식은 v에 대해 선형이 아니다. 예를 들어 $D_{e_1}g = D_{e_2}g = 0$이지만 $D_{(1,1)}g = 1/2$이다. 미분가능했다면 $D_{(1,1)}g = D_{e_1}g + D_{e_2}g = 0$이어야 하므로 g는 $(0,0)$에서 미분가능하지 않다.

2.3 연속인 편미분은 미분가능성을 보장한다

정리 2.6 $f:U\to\mathbb{R}$의 모든 편미분이 a의 근방에서 존재하고 a에서 연속이면 f는 a에서 미분가능하다.

증명. $n=2$에서 적는다. 일반 경우도 좌표를 하나씩 바꾸는 같은 논증이다. $h=(h_1,h_2)$가 작을 때

$$f(a+h)-f(a) = [f(a_1+h_1,a_2+h_2)-f(a_1,a_2+h_2)] + [f(a_1,a_2+h_2)-f(a_1,a_2)].$$

각 괄호에 일변수 평균값정리를 적용하면 $0<\theta_1,\theta_2<1$이 있어

$$f(a+h)-f(a) = \partial_1 f(a_1+\theta_1 h_1, a_2+h_2)\,h_1 + \partial_2 f(a_1, a_2+\theta_2 h_2)\,h_2.$$

따라서 $|f(a+h)-f(a)-\partial_1 f(a)h_1-\partial_2 f(a)h_2| \le (\varepsilon_1(h)+\varepsilon_2(h))\|h\|$이고, 편미분의 연속성으로 $\varepsilon_i(h)\to 0$이다. □

편미분이 열린집합 U 전체에서 존재하고 연속인 함수를 C^1 **함수**라 한다. 위 정리로 C^1 함수는 U의 모든 점에서 미분가능하다. 역은 성립하지 않는다. $\mathbb{R}$에서 $f(x)=x^2\sin(1/x)$, $f(0)=0$은 모든 점에서 미분가능하지만 f'이 0에서 연속이 아니다. 같은 현상이 다변수에서도 일어나므로 "미분가능"과 "C^1"은 구분한다.

2.4 그래디언트, 접평면, 등위집합

실수값 함수 f가 a에서 미분가능하면 $Df(a)$는 $1\times n$ 행렬이다. 내적으로 이를 벡터로 나타낸 것이 **그래디언트**(*gradient*)

$$\nabla f(a) = (\partial_1 f(a),\dots,\partial_n f(a)), \qquad D_v f(a) = \nabla f(a)\cdot v$$

이다. 단위벡터 u에 대해 Cauchy–Schwarz로 $D_u f(a) \le \|\nabla f(a)\|$이고, $\nabla f(a) \neq 0$이면 등호는 $u = \nabla f(a)/\|\nabla f(a)\|$일 때뿐이다. 즉 그래디언트는 가장 빠르게 증가하는 방향과 그 변화율을 함께 준다.

$n = 2$일 때 그래프 $z = f(x,y)$의 $(a, f(a))$에서의 **접평면**은

$$z = f(a) + \partial_x f(a)(x - a_1) + \partial_y f(a)(y - a_2)$$

이다. 미분가능성의 정의는 이 평면과 그래프의 차이가 $\|h\|$보다 빨리 0으로 간다는 뜻이다.

> **명제 2.7** f가 C^1이고 곡선 $\gamma(t)$가 등위집합 $\{f = c\}$ 안에 있으며 $\gamma(0) = a$, $\gamma'(0)$이 존재하면 $\nabla f(a) \cdot \gamma'(0) = 0$이다.

증명. $f(\gamma(t)) = c$를 다음 절의 연쇄법칙으로 미분하면 $\nabla f(a) \cdot \gamma'(0) = 0$이다. □

따라서 $\nabla f(a) \neq 0$이면 그래디언트는 등위곡선(곡면)의 법선이다. 예를 들어 구면 $x^2+y^2+z^2 = 9$ 위의 점 $(1,2,2)$에서 $\nabla(x^2+y^2+z^2) = (2,4,4)$이므로 접평면은 $2(x-1)+4(y-2)+4(z-2) = 0$, 즉 $x + 2y + 2z = 9$이다.

2.5 연쇄법칙

> **정리 2.8 (연쇄법칙)** $f : U \to \mathbb{R}^m$이 a에서 미분가능하고 $g : V \to \mathbb{R}^p$가 $f(a)$에서 미분가능하며 $f(U) \subseteq V$이면 $g \circ f$는 a에서 미분가능하고
>
> $$D(g \circ f)(a) = Dg(f(a))\, Df(a).$$

증명. $b = f(a)$, $A = Df(a)$, $B = Dg(b)$라 하고 $f(a+h) = b + Ah + r(h)$, $g(b+k) = g(b) + Bk + s(k)$로 쓰자. 여기서 $\|r(h)\|/\|h\| \to 0$, $\|s(k)\|/\|k\| \to 0$이다. $k = f(a+h) - b = Ah + r(h)$를 넣으면

$$g(f(a+h)) - g(b) - BAh = Br(h) + s(k).$$

첫 항은 $\|B\|\|r(h)\| = o(\|h\|)$이다. 둘째 항은 $\|k\| \le (\|A\| + 1)\|h\|$가 충분히 작은 h에서 성립하므로 $\|s(k)\| = o(\|k\|) = o(\|h\|)$이다. ($k = 0$인 경우에는 $s(k) = 0$으로 둔다.) □

성분으로 쓰면 $z = g(y)$, $y = f(x)$일 때 $\dfrac{\partial z_i}{\partial x_j} = \sum_k \dfrac{\partial z_i}{\partial y_k}\dfrac{\partial y_k}{\partial x_j}$이다. 행렬곱의 순서가 합성의 순서와 같다는 점이 중요하다.

> **예제 2.9 (극좌표에서의 편미분)** $u(x,y)$가 C^1이고 $x = r\cos\theta$, $y = r\sin\theta$라 하자. $w(r,\theta) = u(r\cos\theta, r\sin\theta)$이면
>
> $$w_r = u_x\cos\theta + u_y\sin\theta, \qquad w_\theta = -u_x r\sin\theta + u_y r\cos\theta.$$
>
> $r > 0$에서 이를 풀면 $u_x^2 + u_y^2 = w_r^2 + r^{-2} w_\theta^2$이다. 즉 $\|\nabla u\|^2$을 극좌표로 쓸 때 각 방향 항에 r^{-2}가 붙는다.

흔한 오류 (같은 기호가 다른 양을 가리킴). 같은 기호 $\partial u/\partial x$가 "어떤 변수를 고정했는가"에 따라 다른 양이 될 수 있다. 열역학에서 $(\partial U/\partial T)_V$와 $(\partial U/\partial T)_P$를 구분하는 이유이다. 변수 묶음을 바꿀 때에는 고정한 변수를 명시한다.

2.6 평균값 부등식

일변수 평균값정리의 등식 형태는 벡터값 함수에서 성립하지 않는다. $\gamma(t) = (\cos t, \sin t)$는 $\gamma(2\pi) - \gamma(0) = 0$이지만 $\gamma'(t)$는 한 번도 0이 아니다. 대신 부등식은 남는다.

> **정리 2.10 (평균값 부등식)** U가 볼록 열린집합이고 $f : U \to \mathbb{R}^m$이 미분가능하며 모든 $x \in U$에서 $\|Df(x)\| \le M$이면 $\|f(b) - f(a)\| \le M\|b - a\|$이다.

증명. $v = f(b) - f(a)$라 하고 $\varphi(t) = v \cdot f(a + t(b-a))$로 둔다. φ는 실수값이므로 일변수 평균값정리로 $\varphi(1) - \varphi(0) = \varphi'(\tau) = v \cdot Df(c)(b-a)$인 c가 선분 위에 있다. 좌변은 $\|v\|^2$이고 우변은 $\|v\| M \|b-a\|$ 이하이다. $\square$

이 부등식에서 $M = 0$으로 두면, 연결된 열린집합 위에서 $Df = 0$인 함수는 상수임을 얻는다. 먼저 각 볼록 근방에서 상수이고, 제9권 제1장의 경로연결성으로 전체가 상수가 된다.

2.7 연습문제와 해설

> **연습문제 2.11** $f(x,y) = \sqrt{|xy|}$가 $(0,0)$에서 편미분을 갖지만 미분가능하지 않음을 보여라.

풀이. 축 위에서 $f = 0$이므로 두 편미분은 0이다. 미분가능하다면 $Df(0) = 0$이어야 하지만 $h = (t,t)$에서 $|f(h)|/\|h\| = |t|/(\sqrt{2}|t|) = 1/\sqrt{2}$로 0으로 가지 않는다.

> **연습문제 2.12** $f(x,y) = x^2 - 3xy + y^3$의 $(1,2)$에서 $u = (3/5, 4/5)$ 방향의 방향미분과 최대 증가율을 구하라.

풀이. $\nabla f = (2x - 3y, -3x + 3y^2)$이므로 $\nabla f(1,2) = (-4, 9)$이다. $D_u f = (-4)(3/5) + 9(4/5) = 24/5$이고 최대 증가율은 $\|\nabla f\| = \sqrt{97}$이다.

> **연습문제 2.13** $z = g(x,y)$, $x = s^2 - t^2$, $y = 2st$이고 g가 C^1일 때 z_s와 z_t를 g_x, g_y로 나타내어라.

풀이. 연쇄법칙으로 $z_s = 2s\,g_x + 2t\,g_y$, $z_t = -2t\,g_x + 2s\,g_y$이다. 이는 복소함수 $w = \zeta^2$, $\zeta = s + it$의 실수부·허수부와 같은 구조이다.

> **연습문제 2.14** $F(x) = \|x\|$의 $x \neq 0$에서의 그래디언트를 구하고 0에서 미분가능한지 판정하라.

풀이. $x \neq 0$에서 $\partial_i F = x_i / \|x\|$이므로 $\nabla F = x/\|x\|$인 단위벡터이다. 0에서는 $F(tv) = |t|\|v\|$이므로 $t \to 0^{\pm}$의 한쪽 극한이 $\pm\|v\|$로 달라 방향미분 자체가 존재하지 않는다. 따라서 미분가능하지 않다.

> **연습문제 2.15** 볼록이 아닌 열린집합에서는 평균값 부등식이 $\|Df\|$의 상계만으로 성립하지 않을 수 있음을 예로 보여라.

풀이. $U = \{(x,y) : x^2 + y^2 > 1\}$에서 음이 아닌 x축 $\{(x,0) : x \ge 0\}$을 제거한 열린집합에서 편각 $\theta \in (0, 2\pi)$를 생각하자. $\|\nabla\theta\| = 1/r$이므로 U 전체에서 $\|D\theta\| < 1$이다. 그러나 $(2, \varepsilon)$과 $(2, -\varepsilon)$의 거리는 2ε인데 θ 값의 차는 2π에 가까워진다. 두 점을 잇는 선분이 영역 밖으로 나가기 때문이다.

참고 (다음 연결). 미분을 한 번 더 하면 이차형식이 나온다. 제9권 제3장에서는 Hessian 행렬로 Taylor 근사와 극값 판정을 정리한다.

제 3 장

고계 도함수, Taylor 정리, 극값 판정

개요 이 장은 이계 이상의 편미분으로 Hessian 행렬을 구성하고, 이를 이용하여 함수를 이차식으로 근사하는 다변수 Taylor 정리를 세운 뒤, 임계점이 극값인지 안장점인지 판정하는 이차 판정법을 정리한다. 또한 그 판정이 결론을 주지 못하는 경계 경우를 구분한다. 선행 지식: 제9권 제2장의 미분과 연쇄법칙, 제7권의 대칭행렬과 고유값, 제8권의 일변수 Taylor 정리.

3.1 고계 편미분과 혼합 편미분의 대칭

f의 편미분 $\partial_j f$가 다시 편미분가능하면 $\partial_i \partial_j f = \partial_i(\partial_j f)$로 **이계 편미분**을 정의한다. 모든 k계 편미분이 존재하고 연속이면 f를 C^k **함수**라 한다. 혼합 편미분의 순서를 바꾸어도 되는지는 조건이 필요하다.

> **정리 3.1 (Schwarz–Clairaut)** f가 열린집합 $U \subseteq \mathbb{R}^2$에서 C^2이면 모든 점에서 $\partial_x \partial_y f = \partial_y \partial_x f$이다.

증명. $(a,b) \in U$와 작은 $h, k \neq 0$에 대해 이계 차분

$$\Delta(h,k) = f(a+h,b+k) - f(a+h,b) - f(a,b+k) + f(a,b)$$

를 생각한다. $\varphi(x) = f(x,b+k) - f(x,b)$로 두면 $\Delta = \varphi(a+h) - \varphi(a)$이고, 평균값정리를 x와 y에 차례로 적용하면 $\Delta = hk\,\partial_y \partial_x f(\xi,\eta)$인 점 (ξ,η)가 (a,b)와 $(a+h,b+k)$를 꼭짓점으로 하는 직사각형 안에 있다. 변수의 역할을 바꾸어 같은 계산을 하면 $\Delta = hk\,\partial_x \partial_y f(\xi',\eta')$이다. 두 식을 hk로 나누고 $(h,k) \to 0$으로 보내면 이계 편미분의 연속성으로 두 값이 같아진다. $\square$

역사 (Clairaut와 Schwarz). Alexis Clairaut는 1740년에 혼합 편미분의 대칭을 기술하였고, Hermann Schwarz는 1873년에 연속성 가정 아래의 정확한 증명을 주었다. 그래서 이 정리는 Clairaut 정리 또는 Schwarz 정리로 불린다.

> **예제 3.2 (연속성이 없으면 순서가 바뀔 수 있다)** $f(x,y) = \dfrac{xy(x^2-y^2)}{x^2+y^2}$, $f(0,0) = 0$이라 하자. 정의로 계산하면 $\partial_x f(0,y) = -y$, $\partial_y f(x,0) = x$이다. 따라서 $\partial_y(\partial_x f)(0,0) = -1$이지만 $\partial_x(\partial_y f)(0,0) = 1$이다. 이 함수의 이계 편미분은 원점에서 연속이 아니다.

3.2 Hessian 행렬과 이차 근사

$f : U \to \mathbb{R}$이 C^2일 때 **Hessian 행렬**을

$$H_f(a) = \left(\partial_i \partial_j f(a)\right)_{i,j=1}^{n}$$

로 정의한다. 정리 3.1로 $H_f(a)$는 대칭행렬이다. 함수 $g(t) = f(a+th)$를 미분하면 연쇄법칙으로

$$g'(t) = \nabla f(a+th)\cdot h, \qquad g''(t) = h^{\mathsf{T}} H_f(a+th)\, h \tag{3.1}$$

이다. 이차형식 $h \mapsto h^{\mathsf{T}} H_f(a) h$는 방향 h를 따라 본 "이차 변화율"이다.

3.3 다변수 Taylor 정리

정리 3.3 (이차 Taylor 정리) f가 a와 $a+h$를 잇는 선분을 포함하는 열린집합에서 C^2이면 $0<\theta<1$이 존재하여

$$f(a+h) = f(a) + \nabla f(a)\cdot h + \frac{1}{2} h^{\mathsf{T}} H_f(a+\theta h)\, h.$$

또한 $h \to 0$일 때

$$f(a+h) = f(a) + \nabla f(a)\cdot h + \frac{1}{2} h^{\mathsf{T}} H_f(a) h + o(\|h\|^2) \tag{3.2}$$

이다.

증명. $g(t) = f(a+th)$에 일변수 Taylor 정리(Lagrange 나머지)를 적용하면 식 (3.1)로 $g(1) = g(0) + g'(0) + \tfrac{1}{2} g''(\theta)$이다. 둘째 주장은

$$|h^{\mathsf{T}}(H_f(a+\theta h) - H_f(a))h| \le \|H_f(a+\theta h) - H_f(a)\|\,\|h\|^2$$

와 H_f의 연속성에서 나온다. $\square$

일반 차수의 Taylor 공식은 다중지표 $\alpha = (\alpha_1,\dots,\alpha_n)$, $|\alpha| = \sum \alpha_i$, $\alpha! = \prod \alpha_i!$, $h^\alpha = \prod h_i^{\alpha_i}$를 쓰면

$$f(a+h) = \sum_{|\alpha|\le k} \frac{\partial^\alpha f(a)}{\alpha!} h^\alpha + o(\|h\|^k) \qquad (f \in C^k)$$

이다. 예를 들어 $n=2$, $k=2$이면 $h^{\mathsf{T}} H h/2 = \tfrac{1}{2} f_{xx} h_1^2 + f_{xy} h_1 h_2 + \tfrac{1}{2} f_{yy} h_2^2$으로 앞의 공식과 같다. 혼합항의 계수가 $1/2$이 아니라 1인 이유는 f_{xy}와 f_{yx} 두 항이 합쳐지기 때문이다.

3.4 임계점과 이차 판정법

f가 a에서 미분가능하고 a가 국소 극값점이면 $\nabla f(a) = 0$이다. 각 좌표 방향으로 제한한 일변수 함수가 극값을 갖기 때문이다. $\nabla f(a) = 0$인 점을 **임계점**이라 한다. 임계점이라고 극값인 것은 아니다.

정리 3.4 (이차 판정법) f가 C^2이고 $\nabla f(a) = 0$이라 하자.

(1) $H_f(a)$가 양의 정부호이면 a는 엄격한 국소 최솟점이다.
(2) $H_f(a)$가 음의 정부호이면 a는 엄격한 국소 최댓점이다.
(3) $H_f(a)$가 양과 음의 고유값을 모두 가지면 a는 안장점이다.
(4) 위 어느 것도 아니면(반정부호이고 고유값 0이 있으면) 이 판정으로는 결론이 없다.

증명. (1) $H = H_f(a)$의 최소 고유값을 $\lambda > 0$이라 하면 $h^{\mathsf{T}} H h \ge \lambda \|h\|^2$이다. 식 (3.2)로 $f(a+h) - f(a) = \tfrac{1}{2} h^{\mathsf{T}} H h + o(\|h\|^2) \ge (\lambda/2 - \varepsilon)\|h\|^2$이 충분히 작은 $h \neq 0$에서 성립하고, $\varepsilon < \lambda/2$로 택하면 양수이다. (2)는 $-f$에 적용한다. (3) 양의 고유값의 고유벡터 v 방향으로 $f(a+tv) - f(a) = \tfrac{t^2}{2} v^{\mathsf{T}} H v + o(t^2) > 0$이고, 음의 고유값 방향으로는 음수이다. $\square$

$n=2$에서 $D = f_{xx}f_{yy} - f_{xy}^2 = \det H$를 쓰면 판정이 간단해진다. $D>0$이고 $f_{xx}>0$이면 최솟점, $D>0$이고 $f_{xx}<0$이면 최댓점, $D<0$이면 안장점이다. $D=0$이면 결론이 없다. 두 고유값의 곱이 D이고 합이 $f_{xx}+f_{yy}$라는 사실에서 나온다.

> **예제 3.5 (판정이 결론을 주지 못하는 세 함수)** x^4+y^4, $-(x^4+y^4)$, x^4-y^4은 모두 원점에서 $\nabla f=0$, $H_f=0$이다. 그러나 차례로 최솟점, 최댓점, 안장점이다. $D=0$일 때 "극값이 아니다"라고 결론 내리는 것은 틀린 추론이다.

3.5 계산 예

> **예제 3.6** $f(x,y)=x^3-3x+y^2-2y$의 임계점을 분류하자. $f_x=3x^2-3$, $f_y=2y-2$이므로 임계점은 $(1,1)$과 $(-1,1)$이다. $H=\operatorname{diag}(6x,2)$이다.
>
> - $(1,1)$: $D=12>0$, $f_{xx}=6>0$이므로 국소 최솟점이며 $f(1,1)=-3$이다.
> - $(-1,1)$: $D=-12<0$이므로 안장점이며 $f(-1,1)=1$이다.
>
> $f(x,1)=x^3-3x-1\to-\infty$ $(x\to-\infty)$이므로 국소 최솟값 -3은 전역 최솟값이 아니다.

3.6 콤팩트 영역의 최대·최소와 볼록성

닫혀 있고 유계인 영역에서 연속함수는 최댓값과 최솟값을 가진다(제9권 제1장). 그 위치는 내부의 임계점, 미분불가능한 점, 경계 중 하나이다. 경계에서의 조사는 경계를 매개화하거나 제9권 제4장의 Lagrange 승수법으로 한다.

> **예제 3.7** $f(x,y)=x^2+2y^2-x$를 원판 $x^2+y^2\le 1$에서 최대·최소화하자. 내부 임계점은 $f_x=2x-1=0$, $f_y=4y=0$에서 $(1/2,0)$이고 $f=-1/4$이다. 경계에서 $y^2=1-x^2$를 넣으면 $f=2-x-x^2$ $(-1\le x\le 1)$이고, 이는 $x=-1/2$에서 최댓값 $9/4$, $x=1$에서 최솟값 0을 갖는다. 따라서 최댓값은 $(-1/2,\pm\sqrt{3}/2)$에서 $9/4$, 최솟값은 $(1/2,0)$에서 $-1/4$이다.

볼록 열린집합 U의 모든 점에서 H_f가 양의 반정부호이면 f는 **볼록함수**(*convex function*)이고, 그러면 임계점은 곧 전역 최솟점이다. 실제로 Taylor 정리의 나머지 항이 음이 아니므로 $f(x)\ge f(a)+\nabla f(a)\cdot(x-a)$가 모든 x에서 성립한다. 이 사실은 제25권의 최적화에서 핵심 도구가 된다.

3.7 연습문제와 해설

> **연습문제 3.8** $f(x,y)=x^2+xy+y^2-3x$의 임계점을 찾고 분류하라. 전역 최솟값인가?

풀이. $f_x=2x+y-3=0$, $f_y=x+2y=0$에서 $(2,-1)$이고 $f(2,-1)=-3$이다. $H=\begin{pmatrix}2&1\\1&2\end{pmatrix}$는 고유값이 $1,3$으로 양의 정부호이다. H가 상수이므로 f는 볼록이고 이 점은 전역 최솟점이다.

> **연습문제 3.9** $f(x,y)=x^2y^2$의 임계점 집합을 구하고 각 점의 성격을 판정하라.

풀이. $\nabla f = (2xy^2, 2x^2y) = 0$이면 $x = 0$ 또는 $y = 0$이다. 두 축 위의 모든 점이 임계점이고 $f \geq 0 = f$이므로 모두 (엄격하지 않은) 최솟점이다. 예를 들어 $(1,0)$에서 $H = \operatorname{diag}(0,2)$로 $D = 0$이라 이차 판정은 결론을 주지 않지만 직접 비교로 결론이 난다.

연습문제 3.10 $e^x \cos y$의 원점에서의 이차 Taylor 다항식을 구하라.

풀이. $f = 1$, $f_x = 1$, $f_y = 0$, $f_{xx} = 1$, $f_{xy} = 0$, $f_{yy} = -1$이므로 $1 + x + \tfrac{1}{2}(x^2 - y^2)$이다. 이는 $\operatorname{Re} e^{x+iy}$의 이차 근사 $\operatorname{Re}(1 + z + z^2/2)$와 같다.

연습문제 3.11 $H_f(a)$가 양의 반정부호이고 $\nabla f(a) = 0$이면 a가 국소 최솟점이라는 주장은 옳은가?

풀이. 아니다. $f(x,y) = x^2 + y^3$은 원점에서 $H = \operatorname{diag}(2,0)$로 양의 반정부호이지만 $f(0,t) = t^3$이 음수가 될 수 있으므로 최솟점이 아니다. 반정부호는 필요조건(국소 최솟점이면 H는 양의 반정부호)일 뿐 충분조건이 아니다.

참고 (다음 연결). Hessian은 함수의 모양을, Jacobi 행렬은 사상의 국소적 가역성을 결정한다. 제9권 제4장에서는 역함수 정리와 음함수 정리로 "방정식을 국소적으로 풀 수 있는 조건"을 다룬다.

제 4 장

역함수 정리, 음함수 정리, Lagrange 승수법

개요 이 장은 "선형근사가 가역이면 원래 사상도 국소적으로 가역이다"라는 하나의 생각에서 역함수 정리, 음함수 정리, Lagrange 승수법을 차례로 이끌어낸다. 선행 지식: 제9권 제2장와 제9권 제3장의 미분과 평균값 부등식, 제7권의 가역행렬과 차원 정리.

4.1 선형근사에서 국소 가역성으로

선형사상 $L:\mathbb{R}^n\to\mathbb{R}^n$은 $\det L\neq 0$일 때 전단사이다. 미분가능한 사상 f는 a 근처에서 $f(a)+Df(a)(x-a)$와 거의 같으므로, $Df(a)$가 가역이면 f도 a 근처에서 가역일 것으로 기대한다. 이 기대는 옳지만 두 가지를 주의해야 한다. 첫째, 결론은 국소적이다. 둘째, f가 C^1이라는 조건이 필요하다. 미분가능하기만 하고 C^1이 아니면 $f'(0)\neq 0$인데도 0 근방에서 단사가 아닌 일변수 함수가 있다. 예를 들어 $f(x)=x+2x^2\sin(1/x)$, $f(0)=0$은 $f'(0)=1$이지만 0의 어떤 근방에서도 단조가 아니다.

4.2 축약사상 원리

정리 4.1 (축약사상 원리) $X\subseteq\mathbb{R}^n$이 닫힌집합이고 $\varphi:X\to X$가 어떤 $0\le q<1$에 대해 $\|\varphi(x)-\varphi(y)\|\le q\|x-y\|$를 만족하면 φ는 유일한 **고정점**(*fixed point*)을 갖는다. 임의의 $x_0\in X$에서 $x_{k+1}=\varphi(x_k)$는 그 고정점으로 수렴한다.

증명. $\|x_{k+1}-x_k\|\le q^k\|x_1-x_0\|$이므로 $j>k$에서 $\|x_j-x_k\|\le q^k\|x_1-x_0\|/(1-q)$이다. 따라서 Cauchy 점열이고 $\mathbb{R}^n$의 완비성과 X의 닫힘으로 $x^*\in X$로 수렴한다. 연속성으로 $\varphi(x^*)=x^*$이다. 두 고정점 x^*,y^*가 있으면 $\|x^*-y^*\|\le q\|x^*-y^*\|$이므로 같다. $\square$

이 정리는 존재·유일성과 함께 오차 $\|x_k-x^*\|\le q^k\|x_1-x_0\|/(1-q)$까지 준다. 제12권의 미분방정식 해의 존재 정리와 제25권의 고정점 반복도 같은 원리를 쓴다.

4.3 역함수 정리

정리 4.2 (역함수 정리) $U\subseteq\mathbb{R}^n$이 열린집합이고 $f:U\to\mathbb{R}^n$이 C^1이며 $Df(a)$가 가역이라 하자. 그러면 a의 열린 근방 V와 $f(a)$의 열린 근방 W가 있어 $f:V\to W$는 전단사이고, 역사상 $f^{-1}:W\to V$는 C^1이며

$$D(f^{-1})(f(x))=(Df(x))^{-1}\qquad (x\in V).$$

증명의 뼈대. $A=Df(a)$라 하고 y를 고정하여 $\varphi_y(x)=x+A^{-1}(y-f(x))$로 둔다. $\varphi_y(x)=x$는 $f(x)=y$와 같다. $D\varphi_y(x)=I-A^{-1}Df(x)$이고 Df의 연속성으로 a를 중심으로 한 작은 닫힌 공 $\overline{B}$

에서 $\|D\varphi_y\| \le 1/2$이다. 평균값 부등식으로 φ_y는 $\overline{B}$에서 축약이며, y가 $f(a)$에 충분히 가까우면 $\overline{B}$를 자기 자신으로 보낸다. 축약사상 원리(정리 4.1)로 $f(x)=y$의 해가 $\overline{B}$ 안에 유일하게 있다.

역사상의 미분가능성과 미분 공식은 $f\circ f^{-1}=\mathrm{id}$에 연쇄법칙을 적용하는 계산으로 확인하며, $Df^{-1}=(Df)^{-1}\circ f^{-1}$이 연속함수의 합성이므로 C^1이다. □

예제 4.3 (국소적으로만 가역인 사상) $f(x,y)=(e^x\cos y,\ e^x\sin y)$의 Jacobi 행렬식은 $e^{2x}\neq 0$이므로 모든 점에서 국소적으로 가역이다. 그러나 $f(x,y+2\pi)=f(x,y)$이므로 전체에서 단사가 아니다. 복소지수함수 $z\mapsto e^z$와 같은 사상이다. 국소 가역성을 모든 점에서 확인해도 전역 가역성이 따라오지 않는다.

극좌표 $(r,\theta)\mapsto(r\cos\theta, r\sin\theta)$도 $\det = r$이므로 $r>0$에서 국소적으로 가역이고, $r=0$에서는 정리를 적용할 수 없다. 실제로 원점 근처에서는 θ가 결정되지 않는다.

4.4 음함수 정리

정리 4.4 (음함수 정리) $F:\mathbb{R}^n\times\mathbb{R}^m\supseteq U\to\mathbb{R}^m$이 C^1이고 $F(a,b)=0$이며 $m\times m$ 행렬 $D_yF(a,b)=(\partial F_i/\partial y_j)$가 가역이라 하자. 그러면 a의 열린 근방 V, b의 열린 근방 W와 유일한 C^1 함수 $g:V\to W$가 있어, $(x,y)\in V\times W$에 대해 $F(x,y)=0 \iff y=g(x)$이고

$$Dg(x)=-(D_yF(x,g(x)))^{-1}D_xF(x,g(x)).$$

증명. $\Phi(x,y)=(x,F(x,y))$로 두면 $D\Phi(a,b)=\begin{pmatrix} I & 0\\ D_xF & D_yF\end{pmatrix}$는 가역이다. 역함수 정리(정리 4.2)로 Φ의 국소 역사상 Ψ가 있고, $g(x)$는 $\Psi(x,0)$의 둘째 성분이다. 미분 공식은 $F(x,g(x))=0$을 연쇄법칙으로 미분하여 $D_xF+D_yF\,Dg=0$을 푸는 것이다. □

예제 4.5 (원에서 국소적으로 함수 꺼내기) $F(x,y)=x^2+y^2-1$이라 하자. $(0,1)$에서 $F_y=2\neq 0$이므로 근처에서 $y=g(x)=\sqrt{1-x^2}$로 풀리며 $g'(x)=-F_x/F_y=-x/y$이다. $(1,0)$에서는 $F_y=0$이라 y를 x의 함수로 풀 수 없다. 실제로 $x<1$ 근처에서 $y=\pm\sqrt{1-x^2}$ 두 값이 있다. 그러나 $F_x=2\neq 0$이므로 x를 y의 함수로는 풀 수 있다.

조건 D_yF의 가역성은 충분조건이다. $F(x,y)=y^3-x$는 원점에서 $F_y=0$이지만 $y=x^{1/3}$으로 전역적으로 풀린다. 다만 그 함수는 원점에서 미분가능하지 않다. 정리가 보장하는 것은 C^1 해의 존재이다.

4.5 정칙값과 곡면

정의 4.6 (정칙값과 매개화 곡면) $F:U\subseteq\mathbb{R}^n\to\mathbb{R}^m$ $(m<n)$이 C^1이고 $F(p)=c$인 모든 점에서 $DF(p)$의 계수가 m이면 c를 **정칙값**(*regular value*)이라 한다. 이때 $M=F^{-1}(c)$는 각 점 근처에서 $n-m$개의 변수로 매개화되는 C^1 곡면(일반적으로 $(n-m)$차원 다양체)이고, p에서의 접공간은

$$T_pM=\ker DF(p)$$

이다.

예를 들어 $F(x,y,z)=x^2+y^2-z^2$의 값 1은 정칙값이므로 일엽쌍곡면은 매끄러운 곡면이다. 값 0은 원점에서 $DF=0$이므로 정칙값이 아니며, 실제로 원뿔은 꼭짓점에서 매끄럽지 않다.

4.6 Lagrange 승수법

정리 4.7 (Lagrange 승수법) $f, g_1, \dots, g_m$이 C^1이고 a가 $M=\{g_1=\cdots=g_m=0\}$ 위에서 f의 국소 극값점이라 하자. $\nabla g_1(a),\dots,\nabla g_m(a)$가 일차독립이면 실수 $\lambda_1,\dots,\lambda_m$이 존재하여

$$\nabla f(a)=\sum_{i=1}^{m}\lambda_i \nabla g_i(a). \tag{4.1}$$

증명. 일차독립 조건으로 M은 a 근처에서 곡면이고 $T_aM=\bigcap_i \nabla g_i(a)^{\perp}$이다. $v\in T_aM$이면 $\gamma(0)=a,\ \gamma'(0)=v$인 M 위의 C^1 곡선이 있다. $f(\gamma(t))$는 $t=0$에서 극값을 가지므로 $\nabla f(a)\cdot v=0$이다. 즉 $\nabla f(a)\in (T_aM)^{\perp}=\operatorname{span}\{\nabla g_i(a)\}$이다. $\square$

역사 (Lagrange 승수법). Joseph-Louis Lagrange는 1788년의 저작 *Méchanique analitique*에서 제약 조건 아래의 극값 문제를 미정 승수의 방법으로 다루었다. 승수 λ_i의 이름은 여기에서 비롯된다.

예제 4.8 구면 $x^2+y^2+z^2=9$ 위에서 $f=x+2y+2z$의 최댓값과 최솟값을 구하자. $(1,2,2)=\lambda(2x,2y,2z)$이므로 (x,y,z)는 $(1,2,2)$에 평행하고, 구면 조건으로 $\pm(1,2,2)$이다. 구면은 콤팩트이므로 최댓값·최솟값이 존재하며 후보는 이 둘뿐이다. 최댓값 9, 최솟값 -9이다. 이는 Cauchy–Schwarz 부등식 $|(1,2,2)\cdot v|\le 3\|v\|$의 등호 조건과 같은 결과이다.

흔한 오류 (제약 자격 조건을 빠뜨리면). 일차독립(제약 자격) 조건을 빠뜨리면 실제 극값점을 놓칠 수 있다. 곡선 $g(x,y)=y^2-x^3=0$ 위에서는 $x=y^{2/3}\ge 0$이므로 $f=x$의 최솟값은 원점에서 0이다. 그런데 원점에서 $\nabla g=(-3x^2,2y)=(0,0)$이므로 $\nabla f=(1,0)=\lambda\nabla g$를 만족하는 λ가 없다. 승수 방정식의 해만 찾으면 이 최솟점이 빠진다. 제약의 기울기가 0이 되는 점은 따로 조사한다.

4.7 승수의 의미

제약값을 c로 바꾼 문제 $\max\{f : g=c\}$의 최댓값을 $V(c)$라 하자. 최적점 $x(c)$와 승수 $\lambda(c)$가 c에 대해 미분가능하게 움직이면 연쇄법칙으로

$$V'(c)=\nabla f\cdot x'(c)=\lambda\nabla g\cdot x'(c)=\lambda\frac{\mathrm{d}}{\mathrm{d}c}g(x(c))=\lambda$$

이다. (식 (4.1)의 단일 제약 형태 $\nabla f=\lambda\nabla g$를 썼다.) 승수는 제약을 한 단위 완화했을 때 최적값의 변화율이다. 경제학의 그림자 가격, 물리학에서 구속력의 크기, 제25권의 쌍대변수가 모두 이 해석을 공유한다.

4.8 연습문제와 해설

연습문제 4.9 $x+y+z=1,\ x^2+y^2+z^2=1$의 교선 위에서 $f=z$의 최댓값과 최솟값을 구하라.

풀이. $\nabla z = (0,0,1) = \lambda(1,1,1) + \mu(2x, 2y, 2z)$에서 첫 두 성분을 빼면 $2\mu(x-y) = 0$이다. $\mu = 0$이면 $\lambda = 0$이 되어 셋째 성분이 모순이므로 $x = y$이다. $2x + z = 1$, $2x^2 + z^2 = 1$에서 $6x^2 - 4x = 0$이고 $x = 0$이면 $z = 1$, $x = 2/3$이면 $z = -1/3$이다. 교선은 원(콤팩트)이고 두 기울기는 이 점들에서 독립이므로 최댓값 1, 최솟값 $-1/3$이다.

> **연습문제 4.10** $f(x,y) = (x^2 - y^2, 2xy)$는 어느 점에서 국소적으로 가역인가? 전역적으로 단사인가?

풀이. $\det Df = \det \begin{pmatrix} 2x & -2y \\ 2y & 2x \end{pmatrix} = 4(x^2+y^2)$이므로 원점을 제외한 모든 점에서 국소적으로 가역이다. 그러나 $f(-x,-y) = f(x,y)$이므로 $\mathbb{R}^2 \setminus \{0\}$에서도 단사가 아니다. 이는 복소함수 $z \mapsto z^2$이다.

> **연습문제 4.11** 넓이가 1인 직사각형 중 둘레가 최소인 것을 Lagrange 승수법으로 구하고, 승수의 의미를 확인하라.

풀이. $x, y > 0$, $xy = 1$에서 $2x + 2y$를 최소화한다. $(2,2) = \lambda(y,x)$이므로 $x = y = 1$, $\lambda = 2$이다. 넓이를 c로 바꾸면 최소 둘레는 $V(c) = 4\sqrt{c}$이고 $V'(1) = 2 = \lambda$이다. 경계 $x \to 0$에서 둘레가 무한대로 가므로 이 임계점이 실제 최솟점이다.

참고 (다음 연결). 미분의 국소 이론이 끝났다. 제9권 제5장에서는 적분으로 넘어가, 반복적분의 순서를 바꾸는 조건과 Jacobi 행렬식이 넓이의 확대율이 되는 이유를 다룬다.

제 5 장

중적분: Fubini 정리와 변수변환

개요 중적분(*multiple integral*)은 유계함수 f를 $\mathbb{R}^n$의 직사각형이나 일반 영역 위에서 적분하는 연산이며, 일변수 Riemann 적분을 분할·하합·상합의 틀 그대로 여러 변수로 확장한 것이다. 이 장은 영집합과 Lebesgue 판정법으로 어떤 함수가 적분가능한지 정리하고, 실제 계산의 두 핵심 도구인 Fubini 정리(반복적분으로 바꾸기)와 변수변환 공식(좌표를 바꾸어 적분을 단순화하기)을 정확한 가정과 함께 증명한다. 이어서 극좌표·원통좌표·구면좌표의 부피 요소, 질량중심과 관성모멘트, 비유계 영역·함수에 대한 이상 중적분을 다룬다. 측도론적 일반화(가측함수와 Lebesgue 적분, Fubini–Tonelli 정리)는 제10권에서 다룬다. 선행 지식: 제8권의 Riemann 적분과 이상적분, 제7권의 행렬식과 부피.

5.1 직사각형 위의 Riemann 적분

닫힌 직사각형 $R = [a_1, b_1] \times \cdots \times [a_n, b_n]$을 각 변의 분할로 작은 직사각형 R_α들로 나눈 것을 R의 분할 P라 한다. 유계함수 $f : R \to \mathbb{R}$에 대해 **하합**과 **상합**을

$$L(f, P) = \sum_{\alpha} \Big(\inf_{R_\alpha} f \Big) \, |R_\alpha| , \qquad U(f, P) = \sum_{\alpha} \Big(\sup_{R_\alpha} f \Big) \, |R_\alpha|$$

로 정의한다. 여기서 $|R_\alpha|$는 R_α의 부피(각 변 길이의 곱)이다. 분할을 세분하면 하합은 감소하지 않고 상합은 증가하지 않으므로, 모든 분할에 걸친 하합의 최소상계와 상합의 최대하계가 항상 존재하고 전자가 후자를 넘지 않는다. 둘이 같으면 f가 R 위에서 **(Riemann) 적분가능**(*Riemann integrable*)하다고 하고 그 공통값을 $\int_R f$로 쓴다.

R 위의 연속함수는 적분가능하다. 콤팩트 집합 위의 연속함수는 균등연속이므로, $\varepsilon > 0$이 주어지면 분할을 충분히 가늘게 하여 모든 작은 직사각형에서 f의 진동(그 위에서의 상한과 하한의 차)을 ε 미만으로 만들 수 있다. 그러면 $U(f,P) - L(f,P) < \varepsilon\,|R|$이 되어 임의로 작은 ε에 대해 두 합의 차를 줄일 수 있으므로 적분가능하다. 이 논증은 일변수 Riemann 적분에서 연속함수가 적분가능함을 보이는 논증과 형태가 같다.

5.2 영집합과 일반 영역

정의 5.1 (Lebesgue 영집합) 집합 $Z \subseteq \mathbb{R}^n$이 모든 $\varepsilon > 0$에 대해 부피의 합이 ε보다 작은 가산개의 직사각형으로 덮이면 Z를 **(Lebesgue) 영집합**(*null set*)이라 한다.

선분, 연속함수의 그래프, 매끄러운 곡면처럼 "차원이 낮은" 콤팩트 집합은 영집합이다. 가산개의 영집합의 합집합도 영집합이다. k번째 영집합을 부피의 합이 $\varepsilon/2^k$보다 작은 가산개의 직사각형으로 덮고 이들을 모두 합치면, 전체 부피의 합이 $\sum_{k} \varepsilon/2^k = \varepsilon$보다 작은 가산개의 직사각형 덮개를 얻기 때문이다. 다음 판정법은 증명 없이 사용하며, 증명은 Lebesgue 측도를 도입하는 제10권에서 다룬다.

정리 5.2 (Lebesgue 판정법) 직사각형 위의 유계함수 f가 Riemann 적분가능할 필요충분조건은 f의 불연속점 집합이 영집합인 것이다.

유계 영역 D 위의 적분은 D를 포함하는 직사각형 R에서 $f\mathbf{1}_D$를 적분하여 정의한다. 여기서 $\mathbf{1}_D$는 D 위에서 1, 그 밖에서 0인 **지시함수**(*indicator function*)이다. D의 경계가 영집합이고 f가 $\overline{D}$에서 연속이면 $f\mathbf{1}_D$의 불연속점은 ∂D 안에 있으므로 정리 5.2에 의해 적분가능하다. $f \equiv 1$일 때 $\int_D 1$을 D의 **넓이**(또는 **부피**)라 한다.

5.3 Fubini 정리

정리 5.3 (Fubini, 연속함수의 경우) f가 $R=[a,b]\times[c,d]$에서 연속이면

$$\iint_R f = \int_a^b \left(\int_c^d f(x,y)\,\mathrm{d}y \right) \mathrm{d}x = \int_c^d \left(\int_a^b f(x,y)\,\mathrm{d}x \right) \mathrm{d}y \tag{5.1}$$

이다.

증명의 뼈대. $F(x)=\int_c^d f(x,y)\,\mathrm{d}y$는 f의 균등연속성에 의해 x에 대해 연속이다. 분할 P의 각 작은 직사각형 $[x_{i-1},x_i]\times[y_{j-1},y_j]$ 위에서

$$\inf f \cdot \Delta y \le \int_{y_{j-1}}^{y_j} f(x,y)\,\mathrm{d}y \le \sup f \cdot \Delta y$$

가 성립하므로, 이를 j에 대해 더한 뒤 다시 i에 대해 더하면

$$L(f,P) \le \int_a^b F(x)\,\mathrm{d}x \le U(f,P)$$

를 얻는다. 분할을 가늘게 하면 좌변과 우변이 모두 $\iint_R f$로 수렴하므로 $\int_a^b F(x)\,\mathrm{d}x = \iint_R f$이다. y를 먼저 고정하고 x로 적분하는 순서도 같은 논증이다. $\square$

영역이 $D=\{(x,y): a\le x\le b,\ \varphi_1(x)\le y\le \varphi_2(x)\}$ (φ_1,φ_2는 연속) 꼴이면

$$\iint_D f = \int_a^b \int_{\varphi_1(x)}^{\varphi_2(x)} f\,\mathrm{d}y\,\mathrm{d}x$$

이다. 적분 순서를 바꿀 때에는 영역을 다른 변수를 기준으로 다시 기술해야 한다.

예제 5.4 (순서를 바꾸어야 풀리는 적분) $I=\int_0^1\int_y^1 \mathrm{e}^{x^2}\,\mathrm{d}x\,\mathrm{d}y$의 안쪽 적분은 초등함수로 계산되지 않는다. 영역은 $0\le y\le x\le 1$이므로

$$I=\int_0^1\int_0^x \mathrm{e}^{x^2}\,\mathrm{d}y\,\mathrm{d}x=\int_0^1 x\mathrm{e}^{x^2}\,\mathrm{d}x=\frac{\mathrm{e}-1}{2}$$

이다.

예제 5.5 (절대적분가능성이 없으면 순서가 중요하다) $f(x,y)=\dfrac{x^2-y^2}{(x^2+y^2)^2}$를 $(0,1]^2$에서 생

각하자. $\partial_y \big(y/(x^2+y^2)\big) = f$ 이므로 $\int_0^1 f\,\mathrm{d}y = 1/(1+x^2)$ 이고

$$\int_0^1 \int_0^1 f\,\mathrm{d}y\,\mathrm{d}x = \int_0^1 \frac{\mathrm{d}x}{1+x^2} = \frac{\pi}{4}$$

이다. $f(y,x) = -f(x,y)$ 인 대칭성으로 반대 순서는 $-\pi/4$ 이다. 원점 근처에서 $\iint |f| = \infty$ 이기 때문이며, 제10권의 Fubini–Tonelli 정리는 $\iint |f| < \infty$ 이면 두 순서가 같음을 보장한다.

역사. Fubini 정리라는 이름은 Guido Fubini가 1907년에 Lebesgue 적분에 대한 일반적인 형태로 증명한 데서 비롯한다. 여기서 다룬 연속함수에 대한 경우는 그보다 단순하며 Riemann 적분의 범위 안에서 완결된다.

5.4 변수변환 공식

선형사상 T 는 모든 직사각형의 부피를 $|\det T|$ 배 한다(제7권). 매끄러운 사상 φ 는 각 점 근처에서 그 미분 $D\varphi$ 라는 선형사상으로 근사되므로, 작은 조각의 부피를 그 점에서의 $|\det D\varphi|$ 배 한다. 이를 정리하면 다음 공식이 된다.

정리 5.6 (변수변환) $U \subseteq \mathbb{R}^n$ 이 열린집합이고 $\varphi : U \to \mathbb{R}^n$ 이 단사 C^1 사상이며 모든 점에서 $\det D\varphi \neq 0$ 이라 하자. 경계가 영집합인 콤팩트 집합 $D \subseteq U$ 와 $\varphi(D)$ 에서 연속인 f 에 대해

$$\int_{\varphi(D)} f(y)\,\mathrm{d}y = \int_D f(\varphi(x))\,\big|\det D\varphi(x)\big|\,\mathrm{d}x \tag{5.2}$$

이다.

단사성과 $\det \neq 0$ 조건은 영집합 위에서는 깨져도 된다. 예를 들어 극좌표 사상은 $r = 0$ 이나 $\theta = 0, 2\pi$ 에서 단사가 아니지만 그 집합들은 영집합이므로 공식에 영향이 없다. 절댓값을 빠뜨리면 방향을 뒤집는 변환에서 부호가 틀린다.

5.5 극·원통·구면 좌표

- 극좌표 $x = r\cos\theta,\ y = r\sin\theta$: $\mathrm{d}x\,\mathrm{d}y = r\,\mathrm{d}r\,\mathrm{d}\theta$.
- 원통좌표 $x = r\cos\theta,\ y = r\sin\theta,\ z = z$: $\mathrm{d}V = r\,\mathrm{d}r\,\mathrm{d}\theta\,\mathrm{d}z$.
- 구면좌표 $x = \rho\sin\phi\cos\theta,\ y = \rho\sin\phi\sin\theta,\ z = \rho\cos\phi$ ($0 \le \phi \le \pi$ 는 z 축과 이루는 각): $\mathrm{d}V = \rho^2\sin\phi\,\mathrm{d}\rho\,\mathrm{d}\phi\,\mathrm{d}\theta$.

물리학 문헌은 θ 와 ϕ 의 역할을 반대로 쓰는 경우가 많다(제9권 제7장). 어느 각이 극각인지 먼저 확인한다.

핵심 수식

$$\iint_R f = \int_a^b \int_c^d f\,\mathrm{d}y\,\mathrm{d}x = \int_c^d \int_a^b f\,\mathrm{d}x\,\mathrm{d}y \quad \text{(Fubini)}, \tag{5.3}$$

$$\int_{\varphi(D)} f = \int_D (f\circ\varphi)\,\big|\det D\varphi\big| \quad \text{(변수변환)}, \tag{5.4}$$

$$\mathrm{d}V = r\,\mathrm{d}r\,\mathrm{d}\theta\,\mathrm{d}z = \rho^2\sin\phi\,\mathrm{d}\rho\,\mathrm{d}\phi\,\mathrm{d}\theta \quad (\text{원통}\cdot\text{구면좌표}). \tag{5.5}$$

예제 5.7 (Gauss 적분) $I = \int_{-\infty}^{\infty} \mathrm{e}^{-x^2}\,\mathrm{d}x$라 하자. 피적분함수가 양수이므로 정사각형 $[-R,R]^2$과 원판 $r \le R$ 어느 쪽으로 넓혀도 $R\to\infty$에서 같은 극한을 얻는다(두 영역은 서로를 포함하는 관계로 끼워진다). 따라서

$$I^2 = \iint_{\mathbb{R}^2} \mathrm{e}^{-(x^2+y^2)}\,\mathrm{d}x\,\mathrm{d}y = \int_0^{2\pi}\int_0^{\infty} \mathrm{e}^{-r^2} r\,\mathrm{d}r\,\mathrm{d}\theta = 2\pi\cdot\frac{1}{2} = \pi,$$

즉 $I = \sqrt{\pi}$이다.

예제 5.8 (구의 부피) 반지름 R인 공의 부피는

$$\int_0^{2\pi}\int_0^{\pi}\int_0^{R} \rho^2\sin\phi\,\mathrm{d}\rho\,\mathrm{d}\phi\,\mathrm{d}\theta = 2\pi\cdot 2\cdot\frac{R^3}{3} = \frac{4}{3}\pi R^3$$

이다.

5.6 질량중심과 관성모멘트

밀도 δ인 평면 판 D의 **질량**(*mass*)은 $M = \iint_D \delta$, **질량중심**(*center of mass*)은

$$\bar{x} = \frac{1}{M}\iint_D x\delta, \qquad \bar{y} = \frac{1}{M}\iint_D y\delta$$

이다. 축에서의 거리 d에 대한 **관성모멘트**(*moment of inertia*)는 $I = \iint_D d^2\delta$이다.

예제 5.9 (반원판의 질량중심) 균일한 반원판 $x^2+y^2\le R^2$, $y\ge 0$의 질량중심을 구하자. 대칭으로 $\bar{x}=0$이다. 넓이는 $\pi R^2/2$이고

$$\iint_D y = \int_0^{\pi}\int_0^{R} r^2\sin\theta\,\mathrm{d}r\,\mathrm{d}\theta = \frac{2R^3}{3}$$

이므로 $\bar{y} = \dfrac{2R^3/3}{\pi R^2/2} = \dfrac{4R}{3\pi}$이다. 질량중심이 영역의 "가운데 높이" $R/2$보다 아래에 있음을 확인한다($4/(3\pi)\approx 0.42 < 0.5$).

5.7 이상 중적분

무한 영역이나 비유계 함수의 **이상 중적분**(*improper multiple integral*)은 콤팩트 영역들의 증가열 $D_k \uparrow D$($D_k \subseteq D_{k+1}$이고 $\bigcup_k D_k = D$)로 근사하여

$$\int_D f = \lim_{k\to\infty}\int_{D_k} f$$

로 정의한다. 피적분함수가 음이 아니면 이 극한은 증가열의 선택과 무관하다. 부호가 바뀌는 함수는 $\int |f| < \infty$일 때만 이 정의가 안정적이다.

예제 5.10 (수렴 판정) $\displaystyle\iint_{\mathbb{R}^2} (1+x^2+y^2)^{-p}\,dx\,dy = 2\pi\int_0^\infty r(1+r^2)^{-p}\,dr$에서 $u = 1+r^2$로 치환하면

$$2\pi\int_0^\infty r(1+r^2)^{-p}\,dr = \pi\int_1^\infty u^{-p}\,du = \frac{\pi}{p-1} \qquad (p>1)$$

으로 수렴하고 $p \le 1$이면 발산한다. 일변수 $\int_1^\infty x^{-p}\,dx$의 판정 경계 $p=1$과 비교하면, 넓이 요소 $r\,dr$ 때문에 경계가 이동했다. 일반적으로 $\mathbb{R}^n$에서 $\|x\|^{-s}$는 무한대 근처에서 $s > n$일 때 적분가능하다.

5.8 연습문제와 해설

연습문제 5.11 $\displaystyle\int_0^2\int_{x/2}^1 \cos(y^2)\,dy\,dx$를 계산하라.

풀이. 영역은 $0 \le x \le 2y$, $0 \le y \le 1$이다. 순서를 바꾸면

$$\int_0^1\int_0^{2y}\cos(y^2)\,dx\,dy = \int_0^1 2y\cos(y^2)\,dy = \bigl[\sin(y^2)\bigr]_0^1 = \sin 1$$

이다.

연습문제 5.12 D가 꼭짓점이 $(0,0),(1,1),(2,0),(1,-1)$인 정사각형일 때 $x = u+v$, $y = u-v$로 $\displaystyle\iint_D (x^2-y^2)\,dx\,dy$를 계산하라.

풀이. 꼭짓점들은 $(u,v) = (0,0),(1,0),(1,1),(0,1)$에 대응하므로 D는 단위정사각형 $[0,1]^2$의 상이다. $|\det| = \left|\det\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\right| = |-1-1| = 2$이고 $x^2-y^2 = (x+y)(x-y) = 4uv$이므로 적분은

$$\int_0^1\int_0^1 4uv\cdot 2\,du\,dv = 8\Bigl(\int_0^1 u\,du\Bigr)\Bigl(\int_0^1 v\,dv\Bigr) = 8\cdot\frac{1}{2}\cdot\frac{1}{2} = 2$$

이다.

연습문제 5.13 구면좌표의 Jacobi 행렬식이 $\rho^2\sin\phi$임을 확인하고, 밀도 $\delta = z^2$인 단위공의 질량을 구하라.

풀이. Jacobi 행렬의 행렬식을 첫 행으로 전개해도 되고, 다른 방법으로 원통좌표 (r,θ,z)에서 $(r,z) = (\rho\sin\phi, \rho\cos\phi)$인 평면 극좌표 변환의 합성으로 보아도 된다. 두 변환의 Jacobi 행렬식의 곱은 $r\cdot\rho = (\rho\sin\phi)\cdot\rho = \rho^2\sin\phi$이다. $z = \rho\cos\phi$이므로 질량은

$$\int_0^{2\pi}\int_0^{\pi}\int_0^{1}\rho^2\cos^2\phi\cdot\rho^2\sin\phi\,d\rho\,d\phi\,d\theta = 2\pi\cdot\Bigl(\int_0^{\pi}\cos^2\phi\sin\phi\,d\phi\Bigr)\cdot\frac{1}{5} = 2\pi\cdot\frac{2}{3}\cdot\frac{1}{5} = \frac{4\pi}{15}$$

이다.

연습문제 5.14 $\displaystyle\iint_{x^2+y^2\le 1}\frac{dx\,dy}{(x^2+y^2)^{a}}$가 수렴하는 a의 범위를 구하라.

풀이. 극좌표로 $2\pi\int_0^1 r^{1-2a}\,dr$이므로 $1-2a > -1$, 즉 $a < 1$일 때 수렴하고 값은 $\pi/(1-a)$이다. 원점 근처의 특이성은 $\mathbb{R}^n$에서 $\|x\|^{-s}$가 $s < n$일 때 적분가능하다는 일반 규칙의 $n=2$ 경우이다.

참고 (다음 장과의 연결). 적분 영역이 곡선과 곡면으로 바뀌면 방향과 넓이 요소가 새로 필요하다. 다음 장에서는 선적분과 면적분을 정의하고 보존장의 판정법을 정리한다.

제 6 장

선적분, 보존장, 면적분

개요 이 장은 곡선과 곡면 위에서 함수와 벡터장을 적분하는 방법을 정의한다. 호의 길이와 곡면의 넓이처럼 방향이 필요 없는 적분과, 일이나 선속처럼 방향이 필요한 적분을 구분하는 것이 핵심이다. 선적분의 기본정리로 기울기장(보존장)의 선적분이 양 끝점만으로 정해짐을 보이고, 회전이 0인 조건이 보존장의 필요조건이지만 영역의 모양(별모양, 단순연결)에 따라서만 충분조건이 됨을 구멍 난 평면의 예로 확인한다. 이어서 매개곡면의 넓이, 면적분, 향할 수 있는 곡면과 선속을 정의한다. 선행 지식: 앞 장의 중적분과 변수변환(제9권 제5장), 제2장의 연쇄법칙(제9권 제2장).

6.1 곡선의 매개화와 호의 길이

C^1 사상 $\boldsymbol{\gamma}:[a,b]\to\mathbb{R}^n$을 **매개곡선**(*parametrized curve*)이라 하고, 모든 t에서 $\boldsymbol{\gamma}'(t)\neq 0$이면 **정칙**(*regular*)이라 한다. **호의 길이**(*arc length*)는

$$L(\boldsymbol{\gamma})=\int_a^b \|\boldsymbol{\gamma}'(t)\|\,dt$$

이다. $\sigma:[c,d]\to[a,b]$가 C^1 전단사이고 $\sigma'>0$이면 $\boldsymbol{\gamma}\circ\sigma$는 같은 곡선의 같은 방향 **재매개화**(*reparametrization*)이다. 연쇄법칙으로 $(\boldsymbol{\gamma}\circ\sigma)'(t)=\boldsymbol{\gamma}'(\sigma(t))\sigma'(t)$이고 $\sigma'(t)>0$이므로

$$L(\boldsymbol{\gamma}\circ\sigma)=\int_c^d \|\boldsymbol{\gamma}'(\sigma(t))\|\,\sigma'(t)\,dt \overset{s=\sigma(t)}{=} \int_a^b \|\boldsymbol{\gamma}'(s)\|\,ds = L(\boldsymbol{\gamma})$$

이므로 치환적분으로 길이가 같다. $\sigma'<0$이면 $(\sigma(c)=b,\ \sigma(d)=a$이므로) 같은 치환에 절댓값 $|\sigma'(t)|=-\sigma'(t)$이 붙어 적분 구간이 한 번 더 뒤집히고, 결과는 방향만 반대이고 길이는 여전히 같다.

> **예제 6.1** (나선의 길이) $\boldsymbol{\gamma}(t)=(\cos t,\sin t,t)$, $0\le t\le 2\pi$의 길이는 $\boldsymbol{\gamma}'(t)=(-\sin t,\cos t,1)$에서 $\|\boldsymbol{\gamma}'\|=\sqrt{2}$이므로 $2\sqrt{2}\,\pi$이다.

6.2 두 종류의 선적분

연속함수 f의 곡선 C 위의 **(스칼라) 선적분**(*line integral*)과 연속 벡터장 $\mathbf{F}$의 선적분을

$$\int_C f\,ds=\int_a^b f(\boldsymbol{\gamma}(t))\,\|\boldsymbol{\gamma}'(t)\|\,dt,\qquad \int_C \mathbf{F}\cdot d\mathbf{r}=\int_a^b \mathbf{F}(\boldsymbol{\gamma}(t))\cdot\boldsymbol{\gamma}'(t)\,dt$$

로 정의한다. 첫째는 곡선의 질량 같은 양으로 방향과 무관하다(앞 절의 호의 길이 계산과 같은 이유로, 방향을 뒤집으면 $|\sigma'|$만 곱해지고 적분값은 바뀌지 않는다). 둘째는 힘이 한 일이나 순환 같은 양으로, 방향을 뒤집으면 $\sigma'<0$에서 절댓값 없이 σ' 그대로가 곱해지므로 부호가 바뀐다. 둘 다 같은 방향의 재매개화에 대해 불변이다.

예제 6.2 (단위원을 따른 순환) $\mathbf{F} = (-y, x)$를 단위원 $\boldsymbol{\gamma}(t) = (\cos t, \sin t)$, $0 \le t \le 2\pi$를 따라 적분하면 $\mathbf{F} \cdot \boldsymbol{\gamma}' = \sin^2 t + \cos^2 t = 1$이므로 $\oint_C \mathbf{F} \cdot d\mathbf{r} = 2\pi$이다. 시계 방향으로 돌면 -2π이다.

직관. 벡터장 $\mathbf{F}$가 힘을 나타내면 $\int_C \mathbf{F} \cdot d\mathbf{r}$는 그 힘이 물체를 곡선 C를 따라 움직이는 동안 하는 일이다. $\mathbf{F} = \nabla\varphi$인 보존장이면 이 일은 $\varphi(B) - \varphi(A)$로 경로의 모양과 무관하게 양 끝점에서만 정해진다. 물리학에서는 흔히 위치 에너지를 $U = -\varphi$로 두므로, 보존력이 한 일은 위치 에너지의 감소량과 같다. 이것이 역학적 에너지 보존 법칙의 수학적 근거이다.

6.3 보존장과 경로독립

정리 6.3 (선적분의 기본정리) φ가 C^1이고 C가 A에서 B로 가는 조각마다 C^1인 곡선이면 $\displaystyle\int_C \nabla\varphi \cdot d\mathbf{r} = \varphi(B) - \varphi(A)$이다.

증명. $\frac{d}{dt}\varphi(\boldsymbol{\gamma}(t)) = \nabla\varphi(\boldsymbol{\gamma}(t)) \cdot \boldsymbol{\gamma}'(t)$에 미적분 기본정리를 적용하고, 곡선이 조각마다 C^1이면 각 조각에 적용한 값을 더한다. □

정리 6.4 연결된 열린집합 $U \subseteq \mathbb{R}^n$ 위의 연속 벡터장 $\mathbf{F}$에 대해 다음은 동치이다.

(1) 어떤 C^1 함수 φ에 대해 $\mathbf{F} = \nabla\varphi$이다(**보존장**, *conservative field*).

(2) $\displaystyle\int_C \mathbf{F} \cdot d\mathbf{r}$는 $C \subseteq U$의 양 끝점만으로 정해진다(**경로독립**, *path independence*).

(3) 모든 닫힌 곡선 $C \subseteq U$에서 $\displaystyle\oint_C \mathbf{F} \cdot d\mathbf{r} = 0$이다.

증명. (1)⇒(2)는 정리 6.3이고, (2)⇔(3)은 두 경로를 이어 붙인 닫힌 곡선을 생각하면 된다. (2)⇒(1): 점 $p_0 \in U$를 고정하고 $\varphi(x) = \int_{p_0}^{x} \mathbf{F} \cdot d\mathbf{r}$로 정의한다(경로와 무관하므로 잘 정의된다). x에서 $x + t\mathbf{e}_i$로 가는 선분을 덧붙이면 $\varphi(x + t\mathbf{e}_i) - \varphi(x) = \int_0^t F_i(x + s\mathbf{e}_i)\, ds$이고, $\mathbf{F}$의 연속성으로 $\partial_i\varphi = F_i$이다. □

참고 (경로연결성). 위 증명의 (2)⇒(1)은 p_0에서 임의의 $x \in U$로 가는 꺾인 선분 경로가 U 안에 존재한다는 사실을 쓴다. $\mathbb{R}^n$의 열린집합에서는 연결성과 (꺾인 선분으로 잇는) 경로연결성이 일치한다: p_0와 선분들로 이을 수 있는 점들의 집합은 열려 있고(그 점의 작은 공 전체가 다시 선분으로 이어진다), 그 여집합도 U 안에서 열려 있으므로, U가 연결되어 있으면 둘 중 하나는 공집합이어야 하고 p_0를 포함하는 쪽이 U 전체와 같다.

6.4 회전이 0인 장과 영역의 모양

$\mathbf{F} = \nabla\varphi$이고 $\varphi \in C^2$이면 혼합 편미분의 대칭으로 $\partial_i F_j = \partial_j F_i$이다. $\mathbb{R}^3$에서는 이것이 $\nabla \times \mathbf{F} = \nabla \times \mathbf{F} = \mathbf{0}$이다. 이 조건은 필요조건이지만 영역에 따라 충분조건이 아니다.

예제 6.5 (구멍 난 평면) $U = \mathbb{R}^2 \setminus \{0\}$에서 $\mathbf{F} = \left(\dfrac{-y}{x^2+y^2}, \dfrac{x}{x^2+y^2}\right)$는

$$\partial_x F_2 = \partial_y F_1 = \frac{y^2 - x^2}{(x^2+y^2)^2}$$

를 만족한다. 그러나 단위원을 따라 $\oint_C \mathbf{F}\cdot d\mathbf{r} = 2\pi \neq 0$이므로 보존장이 아니다. 국소적으로는 $\mathbf{F} = \nabla\theta$(편각)이지만 θ를 U 전체에서 연속함수로 정의할 수 없다.

정리 6.6 (Poincaré 보조정리의 벡터장 형태) U가 **별모양**(*star-shaped*) 열린집합(어떤 점 p와 U의 모든 점을 잇는 선분이 U 안에 있음)이고 $\mathbf{F}$가 C^1이며 $\partial_i F_j = \partial_j F_i$이면 $\mathbf{F}$는 보존장이다.

증명의 뼈대. $p = 0$이라 하고 $\varphi(x) = \int_0^1 \mathbf{F}(tx)\cdot x\, dt$로 둔다. 적분 기호 안에서 미분하고 대칭 조건을 쓰면

$$\begin{aligned}\partial_i\varphi(x) &= \int_0^1 \Big[t\sum_j \partial_i F_j(tx)\,x_j + F_i(tx)\Big]\,dt \\ &= \int_0^1 \Big[t\sum_j \partial_j F_i(tx)\,x_j + F_i(tx)\Big]\,dt \\ &= \int_0^1 \frac{d}{dt}\big(tF_i(tx)\big)\,dt = F_i(x)\end{aligned}$$

이다(첫째에서 둘째 줄은 가정 $\partial_i F_j = \partial_j F_i$를, 둘째에서 셋째 줄은 $\sum_j \partial_j F_i(tx)x_j = \frac{d}{dt}F_i(tx)$와 곱미분 $\frac{d}{dt}(tF_i(tx)) = F_i(tx) + t\frac{d}{dt}F_i(tx)$를 쓴다). □

더 일반적으로 **단순연결**(*simply connected*) 영역(모든 닫힌 곡선을 영역 안에서 한 점으로 연속적으로 줄일 수 있는 영역)에서도 같은 결론이 성립한다. 구멍의 존재와 보존성의 실패 사이의 관계는 제16권의 기본군과 제17권의 de Rham 코호몰로지로 정밀해진다.

예제 6.7 (퍼텐셜 찾기) $\mathbf{F} = (2xy + z, x^2, x)$는 $\mathbb{R}^3$에서 $\nabla\times\mathbf{F} = (0-0, 1-1, 2x-2x) = \mathbf{0}$이다. $\varphi_x = 2xy + z$를 x로 적분하면 $\varphi = x^2y + xz + g(y,z)$이고, $\varphi_y = x^2$에서 $g_y = 0$, $\varphi_z = x$에서 $g_z = 0$이므로 $\varphi = x^2y + xz$(상수 차이)이다.

6.5 매개곡면과 넓이

C^1 사상 $\mathbf{r}: D \to \mathbb{R}^3$ $(D \subseteq \mathbb{R}^2)$에서 $\mathbf{r}_u \times \mathbf{r}_v \neq \mathbf{0}$이면 **정칙 매개곡면**(*regular parametrized surface*)이라 한다. 작은 직사각형 $\Delta u\,\Delta v$는 변이 $\mathbf{r}_u\Delta u$, $\mathbf{r}_v\Delta v$인 평행사변형으로 근사되므로

$$\text{넓이}(S) = \iint_D \|\mathbf{r}_u \times \mathbf{r}_v\|\,du\,dv.$$

그래프 $z = g(x,y)$이면 $\mathbf{r} = (x, y, g)$, $\mathbf{r}_x\times\mathbf{r}_y = (-g_x, -g_y, 1)$이므로 $dS = \sqrt{1 + g_x^2 + g_y^2}\,dx\,dy$이다.

예제 6.8 (구면의 넓이) $\mathbf{r}(\phi,\theta) = R(\sin\phi\cos\theta, \sin\phi\sin\theta, \cos\phi)$이면 $\|\mathbf{r}_\phi\times\mathbf{r}_\theta\| = R^2\sin\phi$이므로 넓이는 $\displaystyle\int_0^{2\pi}\int_0^{\pi} R^2\sin\phi\,d\phi\,d\theta = 4\pi R^2$이다.

6.6 면적분과 선속

곡면 S 위의 함수 f의 **면적분**(*surface integral*)은 $\displaystyle\iint_S f\,dS = \iint_D f(\mathbf{r})\,\|\mathbf{r}_u\times\mathbf{r}_v\|\,du\,dv$이다. 연속적으로 단위법선 $\hat{\mathbf{n}}$을 고를 수 있는 곡면을 **향할 수 있는 곡면**(*orientable surface*)이라 하며, 이때

벡터장 $\mathbf{F}$의 **선속**(*flux*)을

$$\iint_S \mathbf{F}\cdot\hat{\mathbf{n}}\,\mathrm{d}S = \iint_D \mathbf{F}(\mathbf{r}(u,v))\cdot(\mathbf{r}_u\times\mathbf{r}_v)\,\mathrm{d}u\,\mathrm{d}v$$

로 정의한다. 둘째 식은 $\mathbf{r}_u\times\mathbf{r}_v$가 선택한 $\hat{\mathbf{n}}$과 같은 방향일 때 성립하고, 반대이면 부호를 바꾼다. Möbius 띠는 향할 수 없으므로 선속을 정의할 수 없다.

> **예제 6.9 (구면을 지나는 선속)** $\mathbf{F}=(x,y,z)$의 반지름 R인 구면을 지나는 바깥 방향 선속은 $\mathbf{F}\cdot\hat{\mathbf{n}}=\|\mathbf{r}\|=R$이므로 $R\cdot 4\pi R^2 = 4\pi R^3$이다. 다음 장의 발산 정리로 $\iiint \nabla\cdot\mathbf{F}\,\mathrm{d}V = 3\cdot\frac{4}{3}\pi R^3$과 같음을 확인할 수 있다.

흔한 오류. 면적분 $\iint f\,\mathrm{d}S$와 선속 $\iint \mathbf{F}\cdot\hat{\mathbf{n}}\,\mathrm{d}S$는 서로 다른 개념이다. 앞의 것은 방향과 무관하고, 뒤의 것은 법선의 방향을 정하지 않으면 값이 정해지지 않는다. 선적분의 두 종류와 정확히 대응한다.

6.7 연습문제와 해설

> **연습문제 6.10** $\mathbf{F}=(y^2, 2xy+\mathrm{e}^z, y\mathrm{e}^z)$가 보존장인지 판정하고 $(0,0,0)$에서 $(1,1,1)$까지의 선적분을 구하라.

풀이. $\nabla\times\mathbf{F} = (\mathrm{e}^z-\mathrm{e}^z, 0-0, 2y-2y)=\mathbf{0}$이고 $\mathbb{R}^3$은 별모양이므로 보존장이다. $\varphi = xy^2 + y\mathrm{e}^z$가 퍼텐셜이고 값은 $\varphi(1,1,1)-\varphi(0,0,0) = 1+\mathrm{e}$이다.

> **연습문제 6.11** 곡선 $y=x^2$ 위의 $(0,0)$에서 $(1,1)$까지 $\mathbf{F}=(xy, y-x)$의 선적분을 구하라.

풀이. $\boldsymbol{\gamma}(t)=(t,t^2)$, $\boldsymbol{\gamma}'=(1,2t)$이므로

$$\int_0^1 \big(t^3 + 2t(t^2-t)\big)\,\mathrm{d}t = \int_0^1 (3t^3-2t^2)\,\mathrm{d}t = \frac{3}{4}-\frac{2}{3} = \frac{1}{12}$$

이다. 직선 $y=x$를 따라가면 $\int_0^1 t^2\,\mathrm{d}t = 1/3$로 달라지므로 보존장이 아니다.

> **연습문제 6.12** 포물면 $z=x^2+y^2$, $z\le 1$의 넓이를 구하라.

풀이. $\mathrm{d}S = \sqrt{1+4r^2}\,r\,\mathrm{d}r\,\mathrm{d}\theta$이므로

$$2\pi\int_0^1 r\sqrt{1+4r^2}\,\mathrm{d}r = \frac{\pi}{6}\big(5\sqrt{5}-1\big)$$

이다.

> **연습문제 6.13** $U=\mathbb{R}^3\setminus\{z\text{축}\}$에서 회전이 0이지만 보존장이 아닌 벡터장을 하나 들어라.

풀이. $\mathbf{F}=\left(\dfrac{-y}{x^2+y^2}, \dfrac{x}{x^2+y^2}, 0\right)$은 U에서 회전이 0이고, z축을 한 번 감는 원 위에서 순환이 2π이다. 무한히 긴 직선 전류가 만드는 자기장과 같은 구조이다. 반면 $\mathbb{R}^3$에서 한 점만 뺀 영역은 단순연결이므로 그런 예가 없다.

참고 (다음 장과의 연결). 닫힌 곡선의 순환과 내부의 회전, 닫힌 곡면의 선속과 내부의 발산을 잇는 정리가 다음 장의 Green · Stokes · 발산 정리이다.

제 7 장

Green · Stokes · 발산 정리와 벡터 항등식

개요 이 장의 세 정리는 “경계에서의 적분 = 내부에서의 미분의 적분” 이라는 미적분 기본정리의 다변수 형태이다. Green 정리는 평면 영역의 경계를 따른 선적분을 영역 안에서의 이중적분으로, Stokes 정리는 곡면의 경계를 따른 순환을 곡면 위에서의 회전의 선속으로, 발산 정리는 닫힌 곡면을 지나는 선속을 내부에서의 발산의 부피적분으로 바꾼다. 발산과 회전을 극한으로 다시 해석하고, 벡터 항등식과 Green의 두 항등식, 곡선좌표의 미분 연산자를 정리한다. 물리학의 Gauss 법칙, Ampère 법칙, 연속방정식이 모두 여기서 나온다. 선행 지식: 앞 장의 선적분·면적분과 방향(제9권 제6장), 제5장의 중적분(제9권 제5장).

7.1 Green 정리

평면 영역 D의 경계 ∂D가 유한개의 조각마다 C^1인 단순 닫힌 곡선으로 이루어져 있을 때, 영역을 왼쪽에 두고 걷는 방향을 양의 방향으로 정한다. 구멍이 있으면 바깥 경계는 반시계, 안쪽 경계는 시계 방향이다.

정리 7.1 (Green 정리) P, Q가 $\overline{D}$를 포함하는 열린집합에서 C^1이면

$$\oint_{\partial D} P\,\mathrm{d}x + Q\,\mathrm{d}y = \iint_D \left(\frac{\partial Q}{\partial x} - \frac{\partial P}{\partial y}\right)\mathrm{d}A. \tag{7.1}$$

증명의 뼈대. $D = \{a \le x \le b,\ \varphi_1(x) \le y \le \varphi_2(x)\}$ 꼴이면 Fubini 정리(정리 5.3)로

$$-\iint_D P_y\,\mathrm{d}A = -\int_a^b \big[P(x,\varphi_2(x)) - P(x,\varphi_1(x))\big]\,\mathrm{d}x = \oint_{\partial D} P\,\mathrm{d}x$$

이다. 마지막 등식은 아래 경계를 오른쪽으로, 위 경계를 왼쪽으로 지나고(양의 방향이 그렇게 정해지므로) 수직 변에서는 $\mathrm{d}x = 0$이기 때문이다. Q 항은 y 방향으로 같은 계산을 한다. 일반 영역은 이런 조각들로 나누면 조각 사이의 내부 경계의 선적분이 서로 반대 방향으로 두 번 나타나 상쇄된다. □

$P = -y/2,\ Q = x/2$로 두면 넓이 공식 $|D| = \frac{1}{2}\oint_{\partial D}(x\,\mathrm{d}y - y\,\mathrm{d}x)$를 얻는다. 타원 $(a\cos t, b\sin t)$이면 $\frac{1}{2}\int_0^{2\pi} ab\,\mathrm{d}t = \pi ab$이다. 측량기(*planimeter*)가 경계를 따라가서 넓이를 재는 원리이다.

7.2 발산과 회전의 의미

$\mathbb{R}^3$의 C^1 벡터장 $\mathbf{F}$에 대해 **발산**(*divergence*)과 **회전**(*curl*)을

$$\nabla\cdot\mathbf{F} = \nabla\cdot\mathbf{F} = \partial_x F_1 + \partial_y F_2 + \partial_z F_3, \qquad \nabla\times\mathbf{F} = \nabla\times\mathbf{F} = \begin{vmatrix} \mathbf{i} & \mathbf{j} & \mathbf{k} \\ \partial_x & \partial_y & \partial_z \\ F_1 & F_2 & F_3 \end{vmatrix}$$

로 정의한다.

주의. $\nabla \times \mathbf{F}$의 행렬식 표현은 계산을 돕는 형식적인 장치일 뿐이다. 둘째 줄의 성분이 수(數)가 아니라 미분 연산자이므로 실제 행렬식의 성질(다중선형성, 행 교환에 따른 부호 등)이 그대로 성립한다고 가정해서는 안 되며, 전개는 항상 연산자가 오른쪽의 F_i에 작용하는 순서로 읽는다.

아래 두 정리를 작은 공 $B_\varepsilon(p)$와 작은 원판에 적용하면

$$\nabla \cdot \mathbf{F}(p) = \lim_{\varepsilon \to 0} \frac{1}{|B_\varepsilon|} \oint_{\partial B_\varepsilon} \mathbf{F} \cdot \hat{\mathbf{n}} \, dS, \qquad \hat{\mathbf{n}} \cdot \nabla \times \mathbf{F}(p) = \lim_{\varepsilon \to 0} \frac{1}{\pi \varepsilon^2} \oint_{\partial D_\varepsilon} \mathbf{F} \cdot d\mathbf{r}$$

를 얻는다. 발산은 단위 부피당 나가는 선속, 회전의 법선 성분은 그 법선에 수직인 평면에서의 단위 넓이당 순환이다. 이 해석은 좌표계와 무관하다.

7.3 Stokes 정리

정리 7.2 (Stokes 정리) S가 조각마다 C^1인 경계 ∂S를 갖는 향을 준 매끄러운 곡면이고, ∂S의 방향은 법선 $\hat{\mathbf{n}}$에 대해 오른손 법칙으로 정한다(법선 쪽에서 볼 때 반시계). $\mathbf{F}$가 S의 근방에서 C^1이면

$$\oint_{\partial S} \mathbf{F} \cdot d\mathbf{r} = \iint_S (\nabla \times \mathbf{F}) \cdot \hat{\mathbf{n}} \, dS. \tag{7.2}$$

평면 영역에 $\hat{\mathbf{n}} = \mathbf{k}$를 택하면 Green 정리가 된다. 일반 곡면은 매개화를 통해 매개변수 영역의 Green 정리로 귀착시키며, 다음 장의 미분형식 언어에서는 한 줄로 증명된다.

예제 7.3 (같은 경계를 가진 두 곡면) $\mathbf{F} = (-y, x, 0)$이면 $\nabla \times \mathbf{F} = (0, 0, 2)$이다. 경계가 원 $x^2 + y^2 = R^2$, $z = 0$인 위쪽 반구면과 원판은 같은 순환 $\oint \mathbf{F} \cdot d\mathbf{r} = 2\pi R^2$을 준다. 원판에서는 $2 \cdot \pi R^2$이고, 반구면에서는 $(0,0,2) \cdot \hat{\mathbf{n}} \, dS$의 적분이 $\mathbf{k}$ 방향 사영넓이의 두 배이므로 역시 $2\pi R^2$이다. $\nabla \cdot \nabla \times \mathbf{F} = 0$이기 때문에 같은 경계를 가진 곡면들 사이에서 회전의 선속이 같다.

7.4 발산 정리

정리 7.4 (발산 정리, Gauss 정리) $V \subseteq \mathbb{R}^3$이 조각마다 매끄러운 경계 곡면 ∂V를 갖는 유계 영역이고 $\hat{\mathbf{n}}$이 바깥 단위법선이며 $\mathbf{F}$가 $\overline{V}$의 근방에서 C^1이면

$$\oint_{\partial V} \mathbf{F} \cdot \hat{\mathbf{n}} \, dS = \iiint_V \nabla \cdot \mathbf{F} \, dV. \tag{7.3}$$

예제 7.5 (역제곱 장과 Gauss 법칙) $\mathbf{F}(\mathbf{r}) = \mathbf{r}/\|\mathbf{r}\|^3$은 원점이 아닌 곳에서 $\nabla \cdot \mathbf{F} = 0$이다. 원점을 포함하지 않는 영역에서는 선속이 0이다. 원점을 포함하는 영역 V에서는 작은 공 B_ε을 빼고 정리를 적용하면 ∂V의 선속이 작은 구면의 바깥 선속과 같고, 그 값은 $\varepsilon^{-2} \cdot 4\pi\varepsilon^2 = 4\pi$이다. 분포의 언어로는 $\nabla \cdot (\mathbf{r}/r^3) = 4\pi\delta^{(3)}$이며, 전기장의 Gauss 법칙 $\oint \mathbf{E} \cdot d\mathbf{a} = Q/\varepsilon_0$의 수학적 내용이다.

예제 7.6 (연속방정식) 밀도 ρ, 흐름 밀도 $\mathbf{J}$인 보존량이 생성·소멸 없이 이동하면 고정된 영역 V에 대해 $\frac{d}{dt}\iiint_V \rho \, dV = -\oint_{\partial V} \mathbf{J} \cdot \hat{\mathbf{n}} \, dS$이다. 발산 정리로 우변을 부피적분으로 바꾸고 V가 임의라는 사실을 쓰면 $\partial_t \rho + \nabla \cdot \mathbf{J} = 0$을 얻는다. 피적분함수가 연속이라는 조건 아래, 모든

영역에서 적분이 0이면 피적분함수가 0이다.

7.5 벡터 항등식과 Green 항등식

C^2 함수 φ와 벡터장 $\mathbf{F}, \mathbf{G}$에 대해 다음이 성립한다.

$$\nabla \times (\nabla \varphi) = \mathbf{0}, \qquad \nabla \cdot (\nabla \times \mathbf{F}) = 0, \tag{7.4}$$

$$\nabla \cdot (\varphi \mathbf{F}) = \nabla\varphi \cdot \mathbf{F} + \varphi \nabla \cdot \mathbf{F}, \qquad \nabla \times (\varphi \mathbf{F}) = \nabla\varphi \times \mathbf{F} + \varphi \nabla \times \mathbf{F}, \tag{7.5}$$

$$\nabla \cdot (\mathbf{F} \times \mathbf{G}) = \mathbf{G} \cdot (\nabla \times \mathbf{F}) - \mathbf{F} \cdot (\nabla \times \mathbf{G}), \qquad \nabla \times (\nabla \times \mathbf{F}) = \nabla(\nabla \cdot \mathbf{F}) - \nabla^2 \mathbf{F}. \tag{7.6}$$

마지막 식의 $\nabla^2 \mathbf{F}$는 직교좌표 성분별 Laplacian이다. 곡선좌표에서는 성분별 Laplacian이 아니므로 이 항등식을 정의로 사용한다.

$\mathbf{F} = u\nabla v$에 발산 정리를 적용하면 Green의 제1항등식

$$\iiint_V \left(u \nabla^2 v + \nabla u \cdot \nabla v \right) \mathrm{d}V = \oint_{\partial V} u \, \frac{\partial v}{\partial n} \, \mathrm{d}S$$

를 얻고, u, v를 바꾸어 빼면 제2항등식

$$\iiint_V \left(u \nabla^2 v - v \nabla^2 u \right) \mathrm{d}V = \oint_{\partial V} \left(u \, \partial_n v - v \, \partial_n u \right) \mathrm{d}S$$

를 얻는다. 이 항등식으로 Laplace 방정식의 Dirichlet 문제의 해의 유일성을 보일 수 있다. 두 해의 차 w는 $\nabla^2 w = 0$이고 경계에서 $w = 0$이므로, 제1항등식에서 $\iiint_V \|\nabla w\|^2 \, \mathrm{d}V = 0$이다. 따라서 $\nabla w \equiv 0$, 즉 w는 (연결된 영역에서) 상수이고 경계값이 0이므로 $w \equiv 0$, 두 해는 같다.

7.6 곡선좌표의 미분 연산자

물리학 관례의 구면좌표 (r, θ, ϕ) (θ는 z축과의 각, ϕ는 방위각)에서 직교 단위벡터 $\hat{\mathbf{r}}, \hat{\theta}, \hat{\phi}$를 쓰면

$$\nabla f = \partial_r f \, \hat{\mathbf{r}} + \frac{1}{r} \partial_\theta f \, \hat{\theta} + \frac{1}{r \sin\theta} \partial_\phi f \, \hat{\phi}, \tag{7.7}$$

$$\nabla \cdot \mathbf{F} = \frac{1}{r^2} \partial_r (r^2 F_r) + \frac{1}{r \sin\theta} \partial_\theta (\sin\theta F_\theta) + \frac{1}{r \sin\theta} \partial_\phi F_\phi, \tag{7.8}$$

$$\nabla^2 f = \frac{1}{r^2} \partial_r (r^2 \partial_r f) + \frac{1}{r^2 \sin\theta} \partial_\theta (\sin\theta \, \partial_\theta f) + \frac{1}{r^2 \sin^2\theta} \partial_\phi^2 f. \tag{7.9}$$

원통좌표에서는 $\nabla^2 f = \frac{1}{r}\partial_r(r \partial_r f) + \frac{1}{r^2}\partial_\theta^2 f + \partial_z^2 f$이다. 제5장에서 수학 관례로 ϕ를 극각으로 썼던 것과 기호가 바뀌었음을 주의한다(제9권 제5장). 이 공식들은 **축척인자**(*scale factor*) $h_r = 1$, $h_\theta = r$, $h_\phi = r\sin\theta$로부터 일반 직교 곡선좌표 공식에 대입하여 얻는다.

예제 7.7 $f = 1/r$은 $r > 0$에서 $\nabla^2 f = \frac{1}{r^2}\partial_r\left(r^2 \cdot (-r^{-2})\right) = 0$으로 **조화함수**(*harmonic function*)이다. 앞의 Gauss 법칙 예와 합치면 $\nabla^2 (1/r) = -4\pi\delta^{(3)}$이다.

7.7 연습문제와 해설

연습문제 7.8 Green 정리로 $\oint_C (x^2 - y)\,\mathrm{d}x + (y^2 + x)\,\mathrm{d}y$를 계산하라. C는 단위원을 반시계 방향으로 한 바퀴 도는 곡선이다.

풀이. $Q_x - P_y = 1 - (-1) = 2$이므로 $\iint_D 2\,\mathrm{d}A = 2\pi$이다.

연습문제 7.9 $\mathbf{F} = (x^3, y^3, z^3)$의 단위구면을 지나는 바깥 선속을 구하라.

풀이. $\nabla \cdot \mathbf{F} = 3(x^2 + y^2 + z^2) = 3\rho^2$이므로

$$\iiint 3\rho^2 \cdot \rho^2 \sin\phi \,\mathrm{d}\rho\,\mathrm{d}\phi\,\mathrm{d}\theta = 3 \cdot \frac{1}{5} \cdot 4\pi = \frac{12\pi}{5}$$

이다.

연습문제 7.10 닫힌 곡면 S에 대해 $\oint_S (\nabla \times \mathbf{F}) \cdot \hat{\mathbf{n}}\,\mathrm{d}S = 0$임을 두 가지 방법으로 설명하라.

풀이. 발산 정리로 $\iiint \nabla \cdot (\nabla \times \mathbf{F})\,\mathrm{d}V = 0$이다. 또는 S를 닫힌 곡선으로 두 조각으로 자르면 Stokes 정리에서 두 조각의 경계 방향이 반대이므로 순환이 상쇄된다.

연습문제 7.11 Green 정리를 구멍 난 평면의 장 $\mathbf{F} = (-y, x)/(x^2 + y^2)$와 원점을 둘러싼 원판에 적용하면 왜 틀린 결론$(0 = 2\pi)$이 나오는가?

풀이. 정리의 가정은 P, Q가 $\overline{D}$ 전체에서 C^1인 것이다. 원점에서 장이 정의되지 않으므로 적용할 수 없다. 작은 원을 빼낸 고리 영역에서는 정리가 성립하며, 바깥 원과 안쪽 원의 순환이 같다는 올바른 결론을 준다.

역사. Green 정리라는 이름은 George Green이 1828년에 펴낸 전기 · 자기 퍼텐셜에 관한 소책자에서 비롯했다. Stokes 정리라는 이름은 William Thomson(켈빈 경)이 George Gabriel Stokes에게 보낸 편지에서 제안한 결과를, Stokes가 1854년 케임브리지 대학의 Smith's Prize 시험 문제로 출제하면서 널리 알려진 데서 비롯한다.

참고 (다음 장과의 연결). 세 정리는 모두 같은 구조를 가진다. 다음 장에서는 미분형식과 외미분을 도입하여 이들을 하나의 정리 $\int_M \mathrm{d}\omega = \int_{\partial M} \omega$로 묶는다.

제 8 장

미분형식과 일반화된 Stokes 정리

개요 이 장은 증명을 모두 갖춘 이론이 아니라, 앞 장의 Green·Stokes·발산 정리가 하나의 구조에서 나온다는 것을 보이는 입문이다. 방향까지 기억하는 넓이·부피 요소인 **미분형식**을 도입하고, 쐐기곱과 외미분의 계산 규칙을 세운 뒤, 일반화된 Stokes 정리 $\int_M d\omega = \int_{\partial M} \omega$가 미적분 기본정리·선적분의 기본정리·Green 정리·고전적 Stokes 정리·발산 정리를 모두 특수한 경우로 포함함을 확인한다. 다양체 위의 정밀한 이론은 제17권에서 다룬다. 선행 지식: 앞 장의 세 적분 정리(제9권 제7장), 제7권의 행렬식과 교대 다중선형사상.

8.1 방향이 있는 넓이 요소

적분 $\iint f\,dx\,dy$에서 변수변환을 하면(정리 5.6) $|\det|$가 나타났다. 그러나 선적분 $\int P\,dx + Q\,dy$와 선속에서는 방향을 바꾸면 부호가 바뀌었다. 방향까지 기억하는 넓이 요소를 쓰면 절댓값 없는 행렬식이 자연스럽게 나타난다. 그 대상이 **미분형식**(*differential form*)이다. 핵심 규칙은 하나다.

$$dx \wedge dy = -\,dy \wedge dx, \qquad dx \wedge dx = 0.$$

참고 (교대 다중선형사상과의 관계). 각 점에서 k-형식의 값은 그 점의 접공간 위의 교대(반대칭) k-선형함수이다(제7권). $dx_i \wedge dx_j$가 두 벡터 (v_1, v_2)에 주는 값은 v_1, v_2의 i, j 번째 성분으로 만든 2×2 행렬식 $v_{1i}v_{2j} - v_{1j}v_{2i}$이며, 일반적으로 $dx_{i_1} \wedge \cdots \wedge dx_{i_k}$는 k개 벡터의 해당 성분으로 만든 $k \times k$ 행렬식을 준다. 쐐기곱의 반대칭 규칙은 행렬식이 두 행을 바꾸면 부호가 바뀐다는 성질 그대로이다.

8.2 k-형식과 쐐기곱

열린집합 $U \subseteq \mathbb{R}^n$ 위의 0-형식은 함수이고, 1-형식은 $\omega = \sum_i a_i\,dx_i$, 2-형식은 $\sum_{i<j} a_{ij}\,dx_i \wedge dx_j$ 꼴이다. 일반적으로 k-형식은 $dx_{i_1} \wedge \cdots \wedge dx_{i_k}$ $(i_1 < \cdots < i_k)$들의 함수 계수 결합이며, 계수가 C^∞이면 매끄러운 형식이라 한다. **쐐기곱**(*wedge product*)은 다중선형이고 $\alpha \wedge \beta = (-1)^{kl}\beta \wedge \alpha$ (α는 k-형식, β는 l-형식)를 만족한다.

> **예제 8.1** $(dx + 2\,dy) \wedge (3\,dx - dy) = -\,dx \wedge dy + 6\,dy \wedge dx = -7\,dx \wedge dy$이다. 계수 -7은 행렬 $\begin{pmatrix} 1 & 2 \\ 3 & -1 \end{pmatrix}$의 행렬식이다. 쐐기곱은 행렬식을 계산하는 장치이기도 하다.

$\mathbb{R}^n$에서 $k > n$이면 모든 k-형식은 0이고, n-형식은 $f\,dx_1 \wedge \cdots \wedge dx_n$ 한 종류뿐이다.

8.3 외미분

정의 8.2 (외미분) 함수 f에 대해 $\mathrm{d}f = \sum_i \partial_i f \, \mathrm{d}x_i$로 정하고, $\omega = \sum_I a_I \, \mathrm{d}x_I$에 대해 $\mathrm{d}\omega = \sum_I \mathrm{d}a_I \wedge \mathrm{d}x_I$로 정한다. 여기서 $I = (i_1 < \cdots < i_k)$이고 $\mathrm{d}x_I = \mathrm{d}x_{i_1} \wedge \cdots \wedge \mathrm{d}x_{i_k}$이다.

외미분(*exterior derivative*)은 다음을 만족한다. (i) d는 선형이다. (ii) $\mathrm{d}(\alpha\wedge\beta) = \mathrm{d}\alpha\wedge\beta + (-1)^k \alpha \wedge \mathrm{d}\beta$ (α는 k-형식). (iii) $\mathrm{d}(\mathrm{d}\omega) = 0$. 셋째 성질은 혼합 편미분의 대칭과 $\mathrm{d}x_i \wedge \mathrm{d}x_j = -\mathrm{d}x_j \wedge \mathrm{d}x_i$가 정확히 상쇄되어 나온다. 예를 들어

$$\mathrm{d}(\mathrm{d}f) = \sum_{i,j} \partial_j \partial_i f \; \mathrm{d}x_j \wedge \mathrm{d}x_i = 0$$

이다. $\partial_j\partial_i f = \partial_i\partial_j f$인 항끼리 짝지으면 $\mathrm{d}x_j \wedge \mathrm{d}x_i = -\mathrm{d}x_i \wedge \mathrm{d}x_j$에 의해 쌍쌍이 상쇄되기 때문이다.

$\mathbb{R}^3$에서 벡터장 $\mathbf{F} = (F_1, F_2, F_3)$에 형식을 대응시키면

$$\omega_{\mathbf{F}} = F_1 \, \mathrm{d}x + F_2 \, \mathrm{d}y + F_3 \, \mathrm{d}z, \qquad \eta_{\mathbf{F}} = F_1 \, \mathrm{d}y \wedge \mathrm{d}z + F_2 \, \mathrm{d}z \wedge \mathrm{d}x + F_3 \, \mathrm{d}x \wedge \mathrm{d}y$$

이고 다음 대응표가 성립한다.

$$\mathrm{d}f = \omega_{\nabla f}, \qquad \mathrm{d}\omega_{\mathbf{F}} = \eta_{\nabla\times\mathbf{F}}, \qquad \mathrm{d}\eta_{\mathbf{F}} = (\nabla\cdot\mathbf{F}) \, \mathrm{d}x\wedge\mathrm{d}y\wedge\mathrm{d}z.$$

따라서 $\mathrm{d}^2 = 0$은 $\nabla\times(\nabla f) = \mathbf{0}$과 $\nabla\cdot(\nabla\times\mathbf{F}) = 0$을 동시에 말한다.

8.4 당김과 적분

C^∞ 사상 $\varphi : V \to U$와 U 위의 형식 ω에 대해, 좌표 $x = \varphi(u)$를 대입하고 $\mathrm{d}x_i = \sum_j \partial_j \varphi_i \, \mathrm{d}u_j$로 바꾼 것을 **당김**(*pullback*) $\varphi^*\omega$라 한다. 당김은 쐐기곱과 외미분을 보존한다($\varphi^*\,\mathrm{d}\omega = \mathrm{d}\varphi^*\omega$). n-형식의 당김에서는

$$\varphi^*(f \; \mathrm{d}x_1\wedge\cdots\wedge\mathrm{d}x_n) = (f\circ\varphi)\,\det D\varphi \; \mathrm{d}u_1\wedge\cdots\wedge\mathrm{d}u_n$$

이 성립한다. 향을 준 k차원 매개곡면 $\varphi : D \to U$ 위의 k-형식의 적분을 $\int_\varphi \omega = \int_D \varphi^*\omega$로 정의하면, 방향을 보존하는 재매개화에 대해 불변이고 방향을 뒤집으면 부호가 바뀐다. 선적분 $\int_C \mathbf{F}\cdot\mathrm{d}\mathbf{r} = \int_C \omega_{\mathbf{F}}$와 선속 $\iint_S \mathbf{F}\cdot\hat{\mathbf{n}}\,\mathrm{d}S = \int_S \eta_{\mathbf{F}}$가 이 정의의 특수한 경우이다.

예제 8.3 (극좌표의 넓이 요소) $\varphi(r,\theta) = (r\cos\theta, r\sin\theta)$이면 $\mathrm{d}x = \cos\theta\,\mathrm{d}r - r\sin\theta\,\mathrm{d}\theta$, $\mathrm{d}y = \sin\theta\,\mathrm{d}r + r\cos\theta\,\mathrm{d}\theta$이므로

$$\mathrm{d}x\wedge\mathrm{d}y = \cos^2\theta\, r\;\mathrm{d}r\wedge\mathrm{d}\theta + \sin^2\theta\, r\;\mathrm{d}r\wedge\mathrm{d}\theta = r\;\mathrm{d}r\wedge\mathrm{d}\theta$$

이다(교차항은 $\mathrm{d}r\wedge\mathrm{d}r = \mathrm{d}\theta\wedge\mathrm{d}\theta = 0$으로 사라진다). 변수변환의 Jacobi 행렬식이 계산 규칙만으로 나왔다.

8.5 일반화된 Stokes 정리

정리 8.4 (Stokes) M이 경계를 가진 향을 준 콤팩트 k차원 매끄러운 다양체(예: $\mathbb{R}^n$ 안의 경계 있는 곡면이나 영역)이고 ∂M에 유도된 방향을 주며 ω가 매끄러운 $(k-1)$-형식이면

$$\int_M d\omega = \int_{\partial M} \omega.$$

유도된 방향은 "바깥 법선을 먼저 쓰고 그 뒤에 경계의 방향 기저를 붙이면 M의 방향이 된다"는 규칙으로 정한다. 차원별로 읽으면 다음과 같다.

- $k=1$, $M=[a,b]$: $\int_a^b f'\,dx = f(b)-f(a)$ (미적분 기본정리, 경계 $\{b\}$는 $+$, $\{a\}$는 $-$).
- $k=1$, M이 곡선: 선적분의 기본정리(정리 6.3).
- $k=2$, $M\subseteq\mathbb{R}^2$: Green 정리(정리 7.1). $d(P\,dx+Q\,dy)=(Q_x-P_y)\,dx\wedge dy$.
- $k=2$, $M\subseteq\mathbb{R}^3$: 고전적 Stokes 정리(정리 7.2).
- $k=3$, $M\subseteq\mathbb{R}^3$: 발산 정리(정리 7.4).

증명의 핵심은 직육면체 위에서 미적분 기본정리를 쓰는 계산이고, 일반 다양체는 단위분할로 이 경우에 귀착시킨다(제17권).

8.6 닫힌 형식과 완전 형식

$d\omega=0$이면 ω를 **닫힌 형식**(*closed form*), $\omega=d\eta$이면 **완전 형식**(*exact form*)이라 한다. $d^2=0$이므로 완전 형식은 닫힌 형식이다. 역은 영역의 모양에 달려 있다.

정리 8.5 (Poincaré 보조정리) 별모양 열린집합 위의 닫힌 k-형식($k\ge 1$)은 완전 형식이다.

예제 8.6 $\mathbb{R}^2\setminus\{0\}$에서 $\omega=\dfrac{-y\,dx+x\,dy}{x^2+y^2}$는 닫힌 형식이지만, 단위원 위의 적분이 $2\pi\neq 0$이므로 완전 형식이 아니다. 만약 $\omega=d\eta$이면 Stokes 정리에서 경계가 없는 원 위의 적분이 0이어야 한다. 닫힌 형식을 완전 형식으로 나눈 몫공간을 **de Rham 코호몰로지**라 하며, 이 예에서 그 차원 1은 평면에 구멍이 하나 있음을 센다.

역사. 쐐기곱과 외대수의 체계는 Hermann Grassmann이 1844년에 세운 외대수(*exterior algebra*)에 뿌리를 두며, Élie Cartan이 20세기 초에 미분형식과 외미분을 쓰는 현재의 계산 체계(*calcul différentiel extérieur*)로 발전시켰다.

8.7 연습문제와 해설

연습문제 8.7 $\omega=xy\,dz$의 외미분을 구하고 대응하는 벡터 항등식을 말하라.

풀이. $d\omega=y\,dx\wedge dz+x\,dy\wedge dz=-y\,dz\wedge dx+x\,dy\wedge dz$이다. $\mathbf{F}=(0,0,xy)$에 대해 $\nabla\times\mathbf{F}=(x,-y,0)$이므로 $\eta_{\nabla\times\mathbf{F}}$와 일치한다.

연습문제 8.8 구면좌표 사상의 당김으로 $dx\wedge dy\wedge dz=\rho^2\sin\phi\,d\rho\wedge d\phi\wedge d\theta$임을 확인하라.($\phi$는 극각)

풀이. n-형식의 당김 공식에서 계수는 Jacobi 행렬식이며 제5장에서 계산한 값 $\rho^2 \sin\phi$이다(제9권 제5장). 순서 (ρ, ϕ, θ)가 오른손 방향이므로 부호는 양수이다. 순서를 (ρ, θ, ϕ)로 바꾸면 한 번의 호환(互換)만큼 부호가 바뀐다.

> **연습문제 8.9** 단위구면 S^2 위에서 $\int_{S^2} \mathrm{d}\eta = 0$임을 Stokes 정리로 설명하고, $\int_{S^2} x\, \mathrm{d}y \wedge \mathrm{d}z$를 구하라.

풀이. S^2는 경계가 없으므로 $\int_{S^2} \mathrm{d}\eta = \int_{\emptyset} \eta = 0$이다. 둘째 적분은 $\mathbf{F} = (x, 0, 0)$의 바깥 선속이고 발산 정리로 단위공의 부피 $4\pi/3$과 같다($\nabla \cdot \mathbf{F} = 1$). 따라서 $x\, \mathrm{d}y \wedge \mathrm{d}z$는 S^2에서 완전 형식이 아니다(닫힌 형식이지만). 이는 S^2의 2차 de Rham 코호몰로지가 0이 아님을 보여 준다.

제9권의 범위와 다음 읽기

이 권은 $\mathbb{R}^n$의 위상, 미분과 Taylor 근사, 역함수·음함수 정리와 승수법, 중적분과 변수변환, 선적분·면적분과 세 적분 정리, 미분형식을 다루었다. 측도론적 적분과 수렴 정리는 제10권, 복소변수의 선적분은 제11권, 미분방정식은 제12권, 다양체 위의 이론은 제17권으로 이어진다.

표준 참고서로 M. Spivak, *Calculus on Manifolds*; J. E. Marsden and A. Tromba, *Vector Calculus*; J. H. Hubbard and B. B. Hubbard, *Vector Calculus, Linear Algebra, and Differential Forms*; J. R. Munkres, *Analysis on Manifolds*가 있다. 정리의 정확한 가정은 책마다 다르게 진술될 수 있으므로 인용할 때 판본의 정의를 확인한다.

참고자료의 사용방식. 본문의 설명과 문제는 이 참고서를 위해 새로 작성했다. 아래 링크는 관련 주제를 더 넓은 교재와 대조해 읽기 위한 안내이며, 이 원고 전체가 해당 기관이나 저자의 검토를 받았다는 뜻은 아니다. 개별 정리의 정확한 가정과 기호 약속이 다를 수 있으므로 독자는 자료를 바꿀 때 정의를 확인해야 한다.

- MIT OpenCourseWare, *18.02SC Multivariable Calculus*: 강의 영상·연습문제와 함께 다변수 미적분을 복습하는 자료.
- OpenStax, *Calculus Volume 3*: 다변수 함수, 중적분, 벡터해석의 계산 연습.
- L. H. Loomis & S. Sternberg, *Advanced Calculus* (PDF): 미분형식과 Stokes 정리를 엄밀하게 다루는 고급 교재.

제 10 권

실해석 · 측도 · 적분

제10권은 길이와 적분의 개념을 가능한 한 넓은 범위의 집합과 함수로 확장하는 측도론과 Lebesgue 적분을 다룬다. 제1–2장은 실수의 위상과 상극한, 함수열의 균등수렴으로 극한 교환의 문제를 제기하고, 제3장은 σ-대수와 측도로 그 해결의 틀을 세운다. 제4–5장은 단순함수에서 출발하여 Lebesgue 적분을 정의하고 단조수렴정리, Fatou 보조정리, 지배수렴정리를 증명한다. 제6–8장은 곱측도와 Fubini–Tonelli 정리, Hölder · Minkowski 부등식과 L^p 공간, 유계변동 · 절대연속 · 미분정리로 미적분 기본정리를 Lebesgue 적분의 언어로 다시 세운다.

제 1 장

실수의 위상과 상극한

개요 이 장은 실수의 순서 완비성과 위상 구조에서 측도론에 필요한 도구를 정리한다. 확장된 실수 $\overline{\mathbb{R}}$ 위에서 상극한과 하극한을 정의하여 임의의 실수열이 항상 극한에 준하는 두 값을 갖도록 하고, $\mathbb{R}$의 열린집합이 가산 개의 서로소인 열린구간들의 합집합으로 유일하게 분해됨을 보이며, 유계 닫힌구간의 열린 덮개가 항상 유한 부분덮개를 갖는다는 Heine–Borel 정리를 증명한다. 끝으로 Cantor 집합을 구성하여, 집합의 크기를 재는 두 기준인 기수와 길이가 서로 독립적인 정보임을 보인다. 선행 지식: 제1권 제6장의 완비성 공리, 제8권 제1장의 수열의 극한, 제9권 제1장의 열린집합과 콤팩트성.

1.1 상한, 하한, 확장된 실수

공집합이 아니고 위로 유계인 실수 집합은 상한 $\sup A$를 갖는다(완비성 공리). 측도론에서는 값 $\pm\infty$를 허용하는 **확장된 실수**(*extended real number*)의 집합 $\overline{\mathbb{R}} = [-\infty, \infty]$를 쓴다. 위로 유계가 아닌 집합의 상한은 $+\infty$, 공집합의 상한은 $-\infty$로 약속한다. 연산 규칙은

$$a + \infty = \infty \quad (a > -\infty), \qquad 0 \cdot \infty = 0$$

이며, $\infty - \infty$는 정의하지 않는다.

참고 ($0\cdot\infty = 0$이라는 약속의 근거). 이 약속은 임의로 정한 것이 아니다. 넓이가 0인 집합 위에서 값 ∞를 갖는 함수의 적분, 또는 무한히 넓은 집합 위에서 값 0인 함수의 적분이 모두 0이어야 하기 때문이다(제4장의 단순함수 적분 참조). 그러나 극한에서는 $0\cdot\infty$ 꼴이 어떤 값으로도 갈 수 있으므로, 이 약속은 곱 자체의 값에만 적용하고 극한의 계산에는 쓰지 않는다.

1.2 상극한과 하극한

정의 1.1 (상극한과 하극한) 실수열 (a_k)에 대해

$$\limsup_{k\to\infty} a_k = \inf_{n\ge 1} \sup_{k\ge n} a_k, \tag{1.1}$$

$$\liminf_{k\to\infty} a_k = \sup_{n\ge 1} \inf_{k\ge n} a_k \tag{1.2}$$

로 정의한다. 두 값은 모두 $\overline{\mathbb{R}}$에 속한다.

핵심 수식

$$\limsup_{k\to\infty} a_k = \inf_{n\ge 1} \sup_{k\ge n} a_k, \qquad \liminf_{k\to\infty} a_k = \sup_{n\ge 1} \inf_{k\ge n} a_k.$$

$b_n = \sup_{k \ge n} a_k$는 n에 대해 감소하므로(수열이 뒤로 갈수록 집합 $\{a_k : k \ge n\}$이 줄어들기 때문) 극한 $\lim_n b_n = \inf_n b_n$이 $\overline{\mathbb{R}}$에서 항상 존재한다. 따라서 상극한과 하극한은 통상적인 극한과 달리 모든 실수열에 대해 언제나 정의된다. 상극한은 (a_k)의 부분수열의 극한으로 나타날 수 있는 값 가운데 가장 큰 값이고, 하극한은 가장 작은 값이다. 실제로 $\limsup a_k = L < \infty$이면 모든 $\varepsilon > 0$에 대해 $a_k < L + \varepsilon$인 k가 유한 개를 제외한 전부이고 $a_k > L - \varepsilon$인 k가 무한히 많으므로, 이 두 조건으로 L에 수렴하는 부분수열을 뽑을 수 있고 더 큰 극한을 갖는 부분수열은 존재하지 않는다.

명제 1.2 모든 실수열 (a_k)에 대해 $\liminf a_k \le \limsup a_k$이고, (a_k)가 $L \in \overline{\mathbb{R}}$로 수렴할 필요충분조건은 $\liminf a_k = \limsup a_k = L$인 것이다.

증명. $\inf_{k \ge n} a_k \le \sup_{k \ge n} a_k$이므로 양변에 $n \to \infty$의 극한을 취하면 $\liminf a_k \le \limsup a_k$이다. $a_k \to L$이면 모든 $\varepsilon > 0$에 대해 충분히 큰 k에서 $L - \varepsilon < a_k < L + \varepsilon$이므로 $\sup_{k \ge n} a_k$와 $\inf_{k \ge n} a_k$가 모두 L로 수렴한다. 역으로 $\liminf a_k = \limsup a_k = L$이면 $\inf_{k \ge n} a_k \le a_k \le \sup_{k \ge n} a_k$에서 조임 정리로 $a_k \to L$이다. $\square$

예제 1.3 $a_k = (-1)^k (1 + 1/k)$이면 $\limsup a_k = 1$, $\liminf a_k = -1$이다. 어떤 항도 정확히 1과 같지 않지만 짝수 번째 항들이 1로 접근한다. $\sup_k a_k = a_2 = 3/2$이므로, 상극한이 수열 전체의 상한과 다르다는 점을 확인할 수 있다.

집합열에도 같은 개념을 쓴다.

$$\limsup_{k} E_k = \bigcap_{n} \bigcup_{k \ge n} E_k, \qquad \liminf_{k} E_k = \bigcup_{n} \bigcap_{k \ge n} E_k.$$

$\limsup_k E_k$는 무한히 많은 E_k에 속하는 점들의 집합이고, $\liminf_k E_k$는 유한 개를 제외한 모든 E_k에 속하는 점들의 집합이다. 이 표기는 확률론(제20권 제1장)의 Borel–Cantelli 보조정리에서 쓰인다.

1.3 열린집합의 구조

명제 1.4 $\mathbb{R}$의 모든 열린집합은 서로소인 열린구간들의 가산 합집합이다.

증명. 열린집합 U의 점 x에 대해 x를 포함하고 U에 포함되는 가장 큰 열린구간 I_x를 잡는다(x를 포함하는 그런 구간들의 합집합). 서로 다른 두 I_x, I_y는 만나면 합집합도 그런 구간이 되어 최대성에 모순이므로 서로소이거나 같다. 각 구간은 유리수를 하나 포함하므로 구간의 개수는 가산이다. $\square$

이 사실 때문에 $\mathbb{R}$의 열린집합의 "길이"는 구성 구간들의 길이의 합으로 자연스럽게 정의된다(제3장의 외측도 참조). 고차원에서는 열린집합이 열린 직사각형들의 서로소 합집합이 되지는 않지만, 경계가 겹치는 닫힌 정육면체들의 가산 합집합으로 쓸 수 있다.

1.4 덮개 콤팩트성과 Heine–Borel 정리

정리 1.5 (Heine–Borel) $[a, b]$를 덮는 열린집합들의 모임은 유한 부분덮개를 갖는다.

증명. $\mathcal{U}$가 열린 덮개라 하고 $S = \{x \in [a,b] : [a,x]$가 $\mathcal{U}$의 유한 개로 덮인다$\}$라 하자. $a \in S$이므로 $c = \sup S$가 존재한다. $c \in U \in \mathcal{U}$인 U를 잡으면 어떤 $\varepsilon > 0$에 대해 $(c-\varepsilon, c+\varepsilon) \subseteq U$이다. 상한의 정의로 $x \in S$, $x > c-\varepsilon$인 점이 있고, $[a,x]$의 유한 덮개에 U를 더하면 $[a, \min(c+\varepsilon/2, b)]$가 덮인다. 따라서 $c = b$이고 $b \in S$이다. □

이 정리는 다음 장들에서 측도의 가산 가법성을 증명할 때 결정적이다. 예를 들어 $[a,b]$를 열린구간 I_k들로 덮으면 $\sum_k |I_k| \geq b-a$이다. 유한 부분덮개로 줄인 뒤 구간들을 이어 붙이는 기초 논증으로 증명된다. 유리수 집합에서는 같은 일이 일어나지 않는다. $[0,1] \cap \mathbb{Q}$를 나열한 q_k를 길이 $\varepsilon 2^{-k}$인 구간으로 덮으면 길이 합이 ε 이하이다.

1.5 Cantor 집합

$C_0 = [0,1]$에서 가운데 열린 삼등분 $(1/3, 2/3)$을 빼서 C_1을 만들고, 남은 각 구간에서 다시 가운데 삼등분을 빼는 과정을 반복한다. C_n은 길이 3^{-n}인 닫힌구간 2^n개로 이루어지며 $C = \bigcap_{n} C_n$을 **Cantor 집합**이라 한다.

- C는 $[0,1]$의 닫힌 부분집합이다. 정리 1.5에 의해 $[0,1]$이 콤팩트이고 콤팩트 공간의 닫힌 부분집합은 콤팩트이므로, C도 콤팩트이다.
- 제거한 구간들의 길이 합은 $\sum_{n\geq 0} 2^n 3^{-n-1} = 1$이다. 따라서 C의 "길이"는 0이다.
- C는 삼진법 전개에 숫자 1을 쓰지 않는 수들의 집합이다(끝이 $0222\cdots$와 $1000\cdots$처럼 두 전개를 갖는 점은 1이 없는 쪽을 택한다). 각 자리에 $0, 2$를 고르는 방법은 $\{0,1\}^{\mathbb{N}}$과 일대일 대응하므로 C는 비가산이다.
- C의 내부는 공집합이고 C의 모든 점은 C의 집적점이다.

참고 (완전집합). 닫혀 있고 모든 점이 자신의 집적점인 집합을 **완전집합**(*perfect set*)이라 한다. Cantor 집합은 내부가 비어 있으면서 비가산인 완전집합의 대표적인 예이다.

크기를 재는 두 기준, 즉 기수와 길이가 서로 다른 정보를 준다는 첫 예가 Cantor 집합이다. 비가산 집합도 길이 0일 수 있다. 제거하는 비율을 줄여서 길이가 양수인 "살찐" Cantor 집합(*fat Cantor set*, Smith–Volterra–Cantor 집합이라고도 한다)도 같은 방식으로 만들 수 있으며, 그 집합도 내부가 비어 있다.

1.6 연습문제와 해설

연습문제 1.6 $a_k = \sin k$의 상극한과 하극한을 구하라.

풀이. π가 무리수이므로 $\{k \bmod 2\pi\}$는 $[0, 2\pi)$에서 조밀하다(제15권 제4장의 연분수·Dirichlet 근사 또는 Kronecker 정리). 따라서 모든 $y \in [-1,1]$은 부분수열의 극한이고 $\limsup = 1$, $\liminf = -1$이다. 수열의 어떤 항도 정확히 ± 1이 되지는 않는다.

연습문제 1.7 $\limsup(a_k + b_k) \leq \limsup a_k + \limsup b_k$를 증명하고 등호가 실패하는 예를 들라(우변이 $\infty - \infty$ 꼴이 아니라고 가정한다).

풀이. $k \ge n$에서 $a_k + b_k \le \sup_{j\ge n} a_j + \sup_{j\ge n} b_j$이므로 양변의 $\sup_{k\ge n}$을 취한 뒤 $n \to \infty$로 보낸다. $a_k = (-1)^k$, $b_k = (-1)^{k+1}$이면 좌변은 0, 우변은 2이다.

연습문제 1.8 $1/4 \in C$임을 보여라.

풀이. $1/4 = (0.020202\cdots)_3$이다. 실제로 $\sum_{k\ge 1} 2\cdot 9^{-k} = 2/8 = 1/4$이다. 숫자 1이 없으므로 C에 속한다. $1/4$는 어떤 제거 구간의 끝점도 아니라는 점에서, C가 끝점들만으로 이루어진 것이 아님을 보여 준다.

연습문제 1.9 열린구간 $(0,1)$의 열린 덮개 중 유한 부분덮개가 없는 예를 들라.

풀이. $U_k = (1/k, 1)$, $k \ge 2$는 $(0,1)$을 덮지만 유한개의 합집합은 $(1/m, 1)$이므로 덮지 못한다. 정리 1.5의 가정인 "닫혀 있다"는 조건이 빠졌기 때문이다.

참고 (다음 연결). 수열의 극한을 정리했으므로 다음 장에서는 함수열의 극한으로 넘어간다. 점별수렴에서는 연속성과 적분값이 보존되지 않으며, 균등수렴이 첫 번째 해결책이다.

제 2 장

함수열과 균등수렴

개요 이 장은 "극한과 적분(또는 미분, 연속성)의 순서를 바꿀 수 있는가"라는 질문에 대한 고전적 답을 정리한다. 점별수렴만으로는 연속성, 적분값, 도함수가 모두 깨질 수 있음을 예시로 보이고, 균등수렴이라는 더 강한 수렴 개념이 이 세 성질을 보존함을 증명한다. 이어 Weierstrass M-판정법으로 함수항급수의 균등수렴을 판정하고, 이를 이용해 모든 연속함수가 다항식으로 균등근사됨을 보이는 Weierstrass 근사정리를 증명한다. 끝으로 함수공간에서 수렴하는 부분열을 뽑는 조건인 Arzelà–Ascoli 정리를 소개한다. 다음 장부터는 측도론으로 더 넓은 교환 조건을 얻는다. 선행 지식: 앞 장의 상극한, 제8권 제6장의 급수와 제8권 제4장의 Riemann 적분.

2.1 점별수렴이 보존하지 않는 것

함수열 $f_k : E \to \mathbb{R}$가 각 점에서 $f(x)$로 수렴하면 **점별수렴**(*pointwise convergence*)한다고 한다. 점별수렴은 다음을 보존하지 않는다.

> **예제 2.1 (연속성)** $f_k(x) = x^k$는 $[0,1]$에서 연속이지만 극한은 $x<1$에서 0, $x=1$에서 1인 불연속함수이다.

> **예제 2.2 (적분값)** $f_k = k\mathbf{1}_{(0,1/k)}$는 $[0,1]$의 모든 점에서 0으로 수렴하지만 $\int_0^1 f_k = 1$이다. 질량이 한 점으로 몰리면서 극한에서 사라진다. 연속함수로 바꾸어도 같은 현상이 있다. $g_k(x) = k^2 x\, e^{-kx}$는 점별로 0으로 가지만 $\int_0^\infty g_k = 1$이다.

> **예제 2.3 (도함수)** $h_k(x) = \sin(kx)/\sqrt{k}$는 $\mathbb{R}$에서 균등하게 0으로 수렴하지만 $h_k'(x) = \sqrt{k}\cos(kx)$는 $x=0$에서 발산한다. 함수가 가까워져도 기울기는 멀어질 수 있다.

2.2 균등수렴

> **정의 2.4 (균등수렴)** $\sup_{x\in E}|f_k(x)-f(x)| \to 0$이면 f_k가 E에서 f로 **균등수렴**(*uniform convergence*)한다고 한다.

균등수렴은 하나의 k가 모든 점에서 동시에 오차를 통제한다는 뜻이다. Cauchy 판정법도 있다. f_k가 균등수렴할 필요충분조건은 $\sup_x |f_k(x)-f_j(x)| \to 0\ (j,k\to\infty)$인 것이다.

> **정리 2.5** 연속함수열이 균등수렴하면 극한은 연속이다.

증명. $\varepsilon>0$에 대해 $\sup|f_k-f|<\varepsilon/3$인 k를 고정하고, f_k의 연속성으로 $|x-a|<\delta$이면 $|f_k(x)-f_k(a)|<\varepsilon/3$인 δ를 잡는다. 그러면

$$|f(x)-f(a)| \le |f(x)-f_k(x)| + |f_k(x)-f_k(a)| + |f_k(a)-f(a)| < \varepsilon$$

이다. $\square$

정리 2.6 (적분과 극한의 교환) f_k가 $[a,b]$에서 Riemann 적분가능하고 f로 균등수렴하면 f도 적분가능하고 $\int_a^b f_k \to \int_a^b f$이다.

증명. $\varepsilon_k = \sup_x |f_k(x)-f(x)| \to 0$이라 쓴다. 임의의 분할 P에 대해 상합과 하합은

$$U(f,P) - L(f,P) \le \big(U(f_k,P)-L(f_k,P)\big) + 2(b-a)\varepsilon_k$$

를 만족한다. $f-f_k$와 f_k-f가 각각 구간마다 ε_k 이하이므로 f의 상합·하합이 f_k의 상합·하합에서 각각 $(b-a)\varepsilon_k$ 이내로 어긋나기 때문이다. $\varepsilon>0$을 주면 k를 크게 잡아 $2(b-a)\varepsilon_k < \varepsilon/2$로 하고, f_k의 적분가능성으로 $U(f_k,P)-L(f_k,P)<\varepsilon/2$인 분할 P를 잡으면 $U(f,P)-L(f,P)<\varepsilon$이므로 f는 적분가능하다. 값의 수렴은

$$\left|\int_a^b f_k - \int_a^b f\right| \le (b-a)\sup_x |f_k-f| = (b-a)\varepsilon_k \to 0$$

에서 나온다. $\square$

구간이 무한하면 이 부등식이 무너진다. 예를 들어 $f_k = \frac{1}{k}\mathbf{1}_{[0,k]}$는 $[0,\infty)$에서 0으로 균등수렴하지만 $\int_0^\infty f_k = 1$이다.

정리 2.7 (미분과 극한의 교환) f_k가 $[a,b]$에서 C^1이고 f_k'이 g로 균등수렴하며, 어떤 점 x_0에서 $f_k(x_0)$가 수렴하면 f_k는 어떤 C^1 함수 f로 균등수렴하고 $f'=g$이다.

증명. $f_k(x) = f_k(x_0) + \int_{x_0}^x f_k'$에서 적분의 교환 정리(정리 2.6)로 $f(x) = f(x_0) + \int_{x_0}^x g$이며, g는 연속이므로 미적분의 기본정리로 $f'=g$이다. 균등수렴은 $|f_k(x)-f(x)| \le |f_k(x_0)-f(x_0)| + (b-a)\sup|f_k'-g|$에서 나온다. $\square$

흔한 오류 (가정은 도함수열의 균등수렴). 정리 2.7의 가정은 함수열 f_k 자체가 아니라 도함수열 f_k'의 균등수렴이다. 예제 2.3의 $h_k(x)=\sin(kx)/\sqrt{k}$는 h_k가 균등수렴하지만 h_k'이 균등수렴하지 않으므로 이 정리의 가정을 만족하지 않는다.

2.3 급수와 Weierstrass M-판정법

정리 2.8 (Weierstrass M-판정법) $|u_k(x)| \le M_k$가 모든 $x\in E$에서 성립하고 $\sum M_k < \infty$이면 $\sum u_k$는 E에서 절대수렴하고 균등수렴한다.

증명. 꼬리에 대해 $\sup_x \left|\sum_{k>n} u_k(x)\right| \le \sum_{k>n}|u_k(x)| \le \sum_{k>n} M_k \to 0$이기 때문이다. $\square$

예제 2.9 (어디서도 미분가능하지 않은 연속함수) $W(x)=\sum_{k\ge 0} a^k \cos(b^k \pi x)$, $0<a<1$은 M-판정법으로 $\mathbb{R}$ 전체에서 균등수렴하므로 연속이다. Weierstrass는 b가 홀수이고 $ab > 1+3\pi/2$이면 W가 모든 점에서 미분불가능함을 보였고, Hardy는 조건을 $ab\ge 1$로 완화했다. 균등수렴이 연속성은 보존하지만 미분가능성은 보존하지 않는다는 극단적 예이다.

멱급수 $\sum c_k x^k$가 수렴반지름 $R>0$을 가지면 $|x|\le r<R$에서 M-판정법이 적용되므로 그 안의 모든 닫힌구간에서 균등수렴한다. 이것이 멱급수를 항별로 미분하고 적분할 수 있는 근거이다(제8권 제6장). 열린구간 $(-R,R)$ 전체에서의 균등수렴은 일반적으로 성립하지 않는다($\sum x^k$는 $(-1,1)$에서 균등수렴하지 않는다).

2.4 Weierstrass 근사정리

정리 2.10 (Weierstrass 근사정리) $[a,b]$ 위의 모든 연속함수는 다항식들의 균등극한이다.

증명의 뼈대(Bernstein 다항식). $[0,1]$로 옮겨 생각한다. f에 대해

$$B_n f(x) = \sum_{k=0}^{n} f\!\left(\frac{k}{n}\right)\binom{n}{k} x^k (1-x)^{n-k}$$

로 둔다. 이는 성공확률 x인 이항분포 S_n에 대한 $\mathbb{E} f(S_n/n)$이다. $\operatorname{Var}(S_n/n) = x(1-x)/n \le 1/(4n)$이므로 Chebyshev 부등식으로 S_n/n이 x 근처에 몰린다. f의 균등연속성으로 $|x-y|<\delta$이면 $|f(x)-f(y)|<\varepsilon$이고, $|f|\le M$이라 하면

$$|B_n f(x) - f(x)| \le \varepsilon + 2M\,\mathbb{P}\big(|S_n/n - x| \ge \delta\big) \le \varepsilon + \frac{2M}{4n\delta^2}$$

이 x와 무관하다. n을 키우면 균등오차가 2ε 이하가 된다. $\square$

이 정리는 연속함수 공간에서 다항식이 조밀하다는 뜻이다. 일반화인 Stone–Weierstrass 정리는 콤팩트 공간 위의 실연속함수에서, 상수를 포함하고 점을 분리하는 부분대수가 조밀하다고 말한다. 삼각다항식이 2π 주기 연속함수를 균등근사한다는 사실도 그 따름정리이다.

2.5 Arzelà–Ascoli 정리

연속함수열에서 수렴하는 부분열을 뽑는 조건은 $\mathbb{R}^n$의 Bolzano–Weierstrass 정리에 해당한다. 함수공간에서는 유계성만으로 부족하다. 예를 들어 $[0,1]$에서 x^k는 모두 절댓값이 1 이하이지만 균등수렴하는 부분열이 없다. 어떤 부분열의 점별극한도 $x=1$에서 불연속이기 때문이다.

정의 2.11 (동등연속) 함수족 $\mathcal{F}$가 모든 $\varepsilon>0$에 대해 하나의 $\delta>0$으로 "$|x-y|<\delta$이면 모든 $f\in\mathcal{F}$에서 $|f(x)-f(y)|<\varepsilon$"을 만족하면 **동등연속**(*equicontinuous*)이라 한다.

정리 2.12 (Arzelà–Ascoli) K가 콤팩트 거리공간일 때 $C(K)$의 함수열이 균등유계이고 동등연속이면 균등수렴하는 부분열을 갖는다.

증명의 뼈대. K의 가산 조밀 부분집합 $\{q_j\}$를 잡고, 각 q_j에서 값이 수렴하도록 대각선 논법으로 부분열 f_{k_m}을 뽑는다. 동등연속성과 K의 콤팩트성(유한개의 q_j로 δ-망을 만들 수 있음)으로 이 부분열이 균등 Cauchy임을 보인다. $\square$

이 정리는 상미분방정식 해의 존재(Peano 정리, 제12권 제2장)와 변분법에서 최소화 함수의 존재를 증명하는 표준 도구이다. 예를 들어 $|f_k'|\le L$인 함수열은 Lipschitz 상수가 공통이므로 동등연속이다.

2.6 연습문제와 해설

연습문제 2.13 $f_k(x) = \dfrac{x}{1+kx^2}$가 $\mathbb{R}$에서 균등수렴하는지 판정하라.

풀이. 점별극한은 0이다. $x>0$에서 최댓값은 $x=1/\sqrt{k}$에서 $\dfrac{1}{2\sqrt{k}}$이므로 $\sup|f_k| = 1/(2\sqrt{k}) \to 0$이다. 균등수렴한다. 한편 $f_k'(0)=1$인데 극한함수의 도함수는 0이므로, 균등수렴만으로 도함수열의 수렴을 결론 낼 수 없다는 예이기도 하다.

> **연습문제 2.14** $\displaystyle\sum_{k\ge 1}\frac{\sin(kx)}{k^{2}}$가 연속함수를 정의함을 보이고, 항별 미분한 급수에 대해 무엇을 말할 수 있는지 설명하라.

풀이. $\left|\sin(kx)/k^{2}\right| \le 1/k^{2}$이고 $\sum 1/k^{2}<\infty$이므로 M-판정법으로 균등수렴하고 연속이다. 항별 미분한 급수 $\sum \cos(kx)/k$는 $x=0$에서 조화급수가 되어 발산하므로, 미분 교환 정리(정리 2.7)의 가정(도함수급수의 균등수렴)이 $\mathbb{R}$ 전체에서 성립하지 않는다.

> **연습문제 2.15** $f(x)=|x-1/2|$의 Bernstein 다항식 $B_2 f$를 구하라.

풀이. $f(0)=f(1)=1/2$, $f(1/2)=0$이므로

$$B_2 f(x) = \frac{1}{2}(1-x)^{2} + 0 + \frac{1}{2}x^{2} = x^{2}-x+\frac{1}{2}$$

이다. $x=1/2$에서 오차는 $|B_2 f(1/2)-f(1/2)| = 1/4$로 크다. Bernstein 근사는 항상 수렴하지만 느리며, 매끄럽지 않은 점에서 오차가 $n^{-1/2}$ 정도로 줄어든다.

> **연습문제 2.16** $[0,1]$에서 $f_k(x)=\sin(kx)$는 균등유계이다. 균등수렴하는 부분열이 없음을 보여라.

풀이. 균등수렴하는 부분열이 있다면 Arzelà–Ascoli의 역(콤팩트 영역에서 균등수렴하는 연속함수열은 동등연속)에 의해 그 부분열이 동등연속이어야 한다. 그러나 $x=0$과 $x=\pi/(2k)$에서 값의 차가 1이고 두 점의 거리가 0으로 가므로 어떤 무한 부분열도 동등연속이 아니다.

참고 (다음 연결). 균등수렴은 강한 가정이다. 실제 해석학에서는 점별수렴하지만 균등수렴하지 않는 함수열이 흔하며, 그때에도 적분과 극한을 교환하고 싶다. 다음 장에서 측도를 세우는 이유이다.

제 3 장

σ-대수와 측도

개요 이 장은 길이의 개념을 가능한 한 많은 부분집합으로 확장하는 틀을 세운다. 가산 합집합에 닫힌 집합족인 σ-대수를 정의하고, 그 위에서 가산 가법성을 만족하는 함수인 측도를 정의한다. Lebesgue 외측도와 Carathéodory 조건으로 실수의 Lebesgue 가측집합족을 구성하고, 그것이 Borel 집합을 모두 포함하는 σ-대수를 이룸을 밝힌다. 끝으로 선택공리를 쓰면 가측이 아닌 집합이 존재함을 보여, 모든 부분집합에 측도를 줄 수는 없는 이유를 설명한다. 선행 지식: 앞 두 장, 제5권 제5장의 가산성과 제5권 제6장의 선택공리, 제20권 제1장의 확률공리.

3.1 왜 새로운 적분이 필요한가

Riemann 적분은 연속함수에는 충분하지만 극한과 잘 맞지 않는다. $[0,1]$의 유리수를 $q_1, q_2, \dots$로 나열하고 $f_k = \mathbf{1}_{\{q_1,\dots,q_k\}}$라 하면 각 f_k는 적분값 0인 Riemann 적분가능 함수이고 f_k는 단조증가하며 점별로 Dirichlet 함수 $\mathbf{1}_{\mathbb{Q}\cap[0,1]}$로 수렴한다. 그러나 극한은 Riemann 적분가능하지 않다. 측도론적 적분에서는 극한의 적분이 0으로 정의되고, 단조 극한과 적분이 자동으로 교환된다.

3.2 σ-대수

정의 3.1 (σ-**대수**) 집합 X의 부분집합족 $\mathcal{A}$가 다음을 만족하면 σ-**대수**(σ-*algebra*)라 하고, $(X, \mathcal{A})$를 **가측공간**(*measurable space*)이라 한다.

(1) $X \in \mathcal{A}$,

(2) $A \in \mathcal{A} \Rightarrow A^{c} \in \mathcal{A}$,

(3) $A_1, A_2, \dots \in \mathcal{A} \Rightarrow \bigcup_{k} A_k \in \mathcal{A}$.

De Morgan 법칙으로 가산 교집합에도 닫혀 있다. 임의의 부분집합족 $\mathcal{E}$에 대해 $\mathcal{E}$를 포함하는 가장 작은 σ-대수 $\sigma(\mathcal{E})$가 존재한다(그런 σ-대수들의 교집합). $\mathbb{R}^n$의 열린집합들이 생성하는 σ-대수를 **Borel** σ-**대수**(*Borel* σ-*algebra*) $\mathcal{B}(\mathbb{R}^n)$이라 한다. 닫힌집합, 가산집합, 열린집합의 가산 교집합(G_δ), 닫힌집합의 가산 합집합(F_σ) 등이 모두 Borel 집합이다.

흔한 오류 (나열할 수 있다는 착각). σ-대수의 원소를 "구체적으로 나열"할 수 있다고 기대하면 안 된다. Borel 집합은 열린집합에서 출발해 여집합과 가산 합집합을 초한번 반복해야 모두 얻어진다. 실제 증명에서는 원소를 나열하는 대신 "원하는 성질을 가진 집합들의 모임이 σ-대수이고 생성집합들을 포함한다"를 보여 그 모임이 $\sigma(\mathcal{E})$를 포함함을 이끈다.

3.3 측도와 기본 성질

정의 3.2 (측도) 가측공간 $(X, \mathcal{A})$ 위의 함수 $\mu : \mathcal{A} \to [0, \infty]$가 $\mu(\emptyset) = 0$이고 서로소인 $A_k \in \mathcal{A}$에 대해

$$\mu\Big(\bigcup_{k} A_k\Big) = \sum_{k} \mu(A_k)$$

(**가산 가법성**, *countable additivity*)를 만족하면 **측도**(*measure*)라 한다. $(X, \mathcal{A}, \mu)$를 **측도공간**이라 한다.

예: **셈측도**($\mu(A) =$ 원소의 개수), 점 a의 **Dirac 측도**($\delta_a(A) = \mathbf{1}_A(a)$), **확률측도**($\mu(X) = 1$).

명제 3.3 측도 μ에 대해 다음이 성립한다.

(1) 단조성: $A \subseteq B \Rightarrow \mu(A) \le \mu(B)$.

(2) 가산 준가법성: $\mu\big(\bigcup_k A_k\big) \le \sum_k \mu(A_k)$.

(3) 아래로부터의 연속성: $A_1 \subseteq A_2 \subseteq \cdots$ 이면 $\mu\big(\bigcup_k A_k\big) = \lim_k \mu(A_k)$.

(4) 위로부터의 연속성: $A_1 \supseteq A_2 \supseteq \cdots$ 이고 $\mu(A_1) < \infty$이면 $\mu\big(\bigcap_k A_k\big) = \lim_k \mu(A_k)$.

증명. (1) $B = A \cup (B \setminus A)$는 서로소인 합집합이므로 $\mu(B) = \mu(A) + \mu(B \setminus A) \ge \mu(A)$이다.

(3) $B_1 = A_1$, $B_k = A_k \setminus A_{k-1}$은 서로소이고 $\bigcup B_k = \bigcup A_k$이므로 $\mu(\bigcup A_k) = \sum_k \mu(B_k) = \lim_n \mu(A_n)$이다(부분합 $\sum_{k=1}^{n} \mu(B_k)$이 $\mu(A_n)$과 같기 때문).

(4)는 $A_1 \setminus A_k$에 (3)을 적용하고 유한한 $\mu(A_1)$을 뺀다.

(2)는 $B_k = A_k \setminus \bigcup_{j<k} A_j$로 서로소화한 뒤 $B_k \subseteq A_k$에 (1)을 쓴다. $\square$

(4)의 유한성 조건은 필요하다. 셈측도에서 $A_k = \{k, k+1, \dots\}$이면 각 $\mu(A_k) = \infty$인데 $\bigcap A_k = \emptyset$이다.

3.4 외측도와 Carathéodory 구성

정의 3.4 (Lebesgue 외측도) $E \subseteq \mathbb{R}$의 **Lebesgue 외측도**(*outer measure*)를

$$m^*(E) = \inf\Big\{ \sum_{k} |I_k| : E \subseteq \bigcup_{k} I_k,\ I_k \text{는 열린구간} \Big\}$$

로 정의한다.

외측도는 모든 부분집합에 정의되고 단조이며 가산 준가법적이다. 앞 장의 Heine–Borel 논증(정리 1.5)으로 $m^*([a,b]) = b - a$이다. 가산집합의 외측도는 0이다. 그러나 m^*는 모든 부분집합에서 가법적이지는 않다. 가법성이 성립하는 집합만 골라내는 기준이 다음이다.

정의 3.5 (Carathéodory 조건) 모든 $T \subseteq \mathbb{R}$에 대해 $m^*(T) = m^*(T \cap E) + m^*(T \setminus E)$이면 E를 **Lebesgue 가측**이라 한다.

정리 3.6 Lebesgue 가측 집합들은 Borel 집합을 모두 포함하는 σ-대수 $\mathcal{L}$을 이루고, $m = m^*|_{\mathcal{L}}$은 측도이다. m은 구간의 길이를 확장하며 평행이동에 대해 불변이고, 외측도가 0인 집합은 모두 가측이다(완비성).

역사 (Carathéodory 구성). 이 정리의 증명은 외측도에서 출발해 측도 공간을 만드는 일반적인 방법인 **Carathéodory 확장정리**의 특수한 경우이다. Constantin Carathéodory가 1914년에 이 구성을 제시하였다. 생성 집합족 위에서 정의한 양을 전체 σ-대수로 확장한다는 같은 발상은 제6장에서 곱측도를 만들 때에도 나타난다. 이 조건 자체의 증명은 길어서, 여기서는 결과만 쓰고 자세한 증명은 측도론 전공서로 미룬다.

m을 **Lebesgue 측도**라 한다. $\mathbb{R}^n$에서도 구간 대신 직사각형으로 같은 구성을 하면 n차원 Lebesgue 측도를 얻는다. 가측 집합 E는 열린집합과 닫힌집합으로 근사된다. 모든 $\varepsilon > 0$에 대해 닫힌 F와 열린 U가 있어 $F \subseteq E \subseteq U$, $m(U \setminus F) < \varepsilon$이다(**정칙성**, *regularity*).

3.5 가측이 아닌 집합

모든 부분집합에 평행이동 불변이고 가산 가법적인 길이를 줄 수는 없다.

정리 3.7 (Vitali) 선택공리를 가정하면 Lebesgue 가측이 아닌 $[0,1]$의 부분집합이 존재한다.

증명. $x \sim y \iff x - y \in \mathbb{Q}$는 $[0,1]$ 위의 동치관계이다. 각 동치류에서 대표를 하나씩 골라 집합 V를 만든다(선택공리). $[-1,1]$의 유리수 r_k에 대해 $V + r_k$들은 서로소이고 $[0,1] \subseteq \bigcup_k (V + r_k) \subseteq [-1,2]$이다. V가 가측이면 평행이동 불변성과 가산 가법성으로 $1 \le \sum_k m(V) \le 3$인데, $m(V) = 0$이면 좌변이, $m(V) > 0$이면 우변이 모순이다. $\square$

이 결과는 선택공리를 실제로 사용한다. Solovay는 (도달불가능 기수의 존재와 무모순성이라는 가정 아래) ZF와 종속선택공리만으로는 모든 실수 집합이 Lebesgue 가측인 모형이 있음을 보였다. 일상적인 해석학에서 만나는 집합은 Borel 집합이므로 가측성 문제를 거의 일으키지 않지만, "모든 집합"이라는 말을 쓸 때는 이 한계를 의식한다.

3.6 영집합과 "거의 모든 곳"

$\mu(N) = 0$인 가측 집합을 **영집합**(*null set*)이라 한다. 어떤 성질이 영집합 밖의 모든 점에서 성립하면 **거의 모든 곳**(a.e.)에서 성립한다고 한다. 예를 들어 Dirichlet 함수는 Lebesgue 측도에 대해 거의 모든 곳에서 0이다. 가산집합, 앞 장의 Cantor 집합, $\mathbb{R}^2$의 직선은 모두 영집합이다.

영집합의 가산 합집합은 영집합이다. 그러나 비가산 합집합에서는 성립하지 않는다. $\mathbb{R}$은 한 점짜리 영집합들의 비가산 합집합이다. 확률론에서는 "거의 확실히"(a.s.)라는 말을 같은 뜻으로 쓴다.

3.7 연습문제와 해설

연습문제 3.8 $\mathcal{A} = \{A \subseteq \mathbb{R} : A$ 또는 A^c가 가산$\}$이 σ-대수임을 보여라. 이 σ-대수는 $[0,1]$을 포함하는가?

풀이. 여집합에 닫혀 있는 것은 정의상 분명하다. 가산 합집합에서 모든 A_k가 가산이면 합집합도 가산이고, 어떤 A_j^c가 가산이면 $(\bigcup A_k)^c \subseteq A_j^c$도 가산이다. $[0,1]$과 그 여집합은 모두 비가산이므로 속하지 않는다. 따라서 이 σ-대수는 Borel σ-대수보다 작다. 가산집합과 그 여집합은 모두 Borel

집합이므로 $\mathcal{A} \subseteq \mathcal{B}(\mathbb{R})$이고, $[0,1]$에 속하는 무리수 전체처럼 비가산이면서 그 여집합(유리수와 $\mathbb{R}\setminus[0,1]$의 합집합)도 비가산인 Borel 집합이 $\mathcal{A}$에는 없으므로 진부분집합이다.

> **연습문제 3.9** $m(\mathbb{Q}\cap[0,1])=0$이지만 $\mathbb{Q}\cap[0,1]$은 $[0,1]$에서 조밀하다. 조밀한 열린집합의 측도는 얼마나 작을 수 있는가?

풀이. 유리수 q_k 둘레에 길이 $\varepsilon 2^{-k}$인 열린구간을 놓으면 합집합 U는 조밀한 열린집합이고 $m(U)\le\varepsilon$이다. 조밀성과 측도는 서로 다른 크기 개념이다. 그 여집합 $[0,1]\setminus U$는 측도가 $1-\varepsilon$ 이상인데 내부가 비어 있는 닫힌집합이다.

> **연습문제 3.10** 위로부터의 연속성을 이용하여 Cantor 집합의 측도가 0임을 다시 보여라.

풀이. C_n은 감소하고 $m(C_0)=1<\infty$이며 $m(C_n)=(2/3)^n\to 0$이므로 $m(C)=\lim_n m(C_n)=0$이다.

참고 (다음 연결). 측도가 정해지면 적분은 "값 $\times$ 측도"의 합에서 출발한다. 다음 장에서는 가측함수와 Lebesgue 적분을 정의하고 단조수렴정리를 증명한다.

제 4 장

가측함수와 Lebesgue 적분

개요 이 장은 음이 아닌 함수의 적분을 단순함수의 적분에서 출발해 정의하고, 측도론의 첫 극한정리인 단조수렴정리와 Fatou 보조정리를 증명한다. 이후 모든 수렴정리는 이 둘에서 나온다. 가측함수는 극한에 대해 닫혀 있다는 점에서 Riemann 적분가능 함수족과 결정적으로 다르다. 선행 지식: 앞 장의 측도와 영집합.

4.1 가측함수

정의 4.1 (가측함수) 측도공간 $(X, \mathcal{A}, \mu)$ 위의 함수 $f : X \to \overline{\mathbb{R}}$가 모든 $a \in \mathbb{R}$에 대해 $\{f > a\} \in \mathcal{A}$를 만족하면 **가측**(*measurable*)이라 한다.

$\{f > a\}$ 대신 $\{f \ge a\}$, $\{f < a\}$, $\{f \le a\}$ 중 하나만 확인해도 동치이다. 예를 들어 $\{f \ge a\} = \bigcap_k \{f > a - 1/k\}$이다. 따라서 모든 Borel 집합 B에 대해 $f^{-1}(B)$가 가측이다. 연속함수와 단조함수는 Borel 가측이다.

명제 4.2 가측함수의 합, 곱, max, min은 가측이고, 가측함수열 f_k에 대해 $\sup_k f_k$, $\inf_k f_k$, $\limsup f_k$, $\liminf f_k$는 가측이다. 특히 점별극한은 가측이다.

증명. $\{\sup_k f_k > a\} = \bigcup_k \{f_k > a\}$이다. 상극한은 $\inf_n \sup_{k \ge n} f_k$이므로 위 결과를 두 번 적용한다. 합에 대해서는 $\{f+g > a\} = \bigcup_{r \in \mathbb{Q}} \{f > r\} \cap \{g > a - r\}$을 쓴다($\infty - \infty$가 생기지 않는다고 가정). 곱은 $fg = \tfrac{1}{4}\big[(f+g)^2 - (f-g)^2\big]$과 $f \mapsto f^2$가 가측임을 합쳐서 얻고, $\max(f,g) = \tfrac{1}{2}(f+g+|f-g|)$, $\min(f,g) = \tfrac{1}{2}(f+g-|f-g|)$에서 max, min도 가측이다. $\square$

극한에 대해 닫혀 있다는 점이 Riemann 적분가능 함수족과의 결정적 차이이다. 앞 장의 Dirichlet 함수도 가측이다.

4.2 단순함수 근사

유한개의 값만 갖는 가측함수 $s = \sum_{j=1}^{N} a_j \mathbf{1}_{A_j}$를 **단순함수**(*simple function*)라 한다(A_j 가측, 서로소).

명제 4.3 음이 아닌 가측함수 f에 대해 $0 \le s_1 \le s_2 \le \cdots \le f$이고 점별로 $s_k \uparrow f$인 단순함수열이 존재한다. f가 유계이면 수렴은 균등하다.

증명.

$$s_k = \sum_{j=1}^{k 2^k} \frac{j-1}{2^k} \mathbf{1}_{\{(j-1)2^{-k} \le f < j 2^{-k}\}} + k\, \mathbf{1}_{\{f \ge k\}}$$

로 둔다. 값의 범위 $[0, k)$를 2^{-k} 간격으로 자르는 것이며, $f(x) < k$인 점에서 $0 \le f - s_k < 2^{-k}$이다. $f \le M$이면 $k \ge M$에서 모든 점이 이 범위에 들어가므로 $\sup |f - s_k| \le 2^{-k} \to 0$이다. $\square$

Riemann 적분은 정의역을 잘게 나누고, Lebesgue 적분은 값의 범위를 잘게 나눈다는 것이 Lebesgue 자신의 비유이다.

4.3 음이 아닌 함수의 적분

단순함수 $s = \sum a_j \mathbf{1}_{A_j} \geq 0$에 대해 $\int s \, d\mu = \sum a_j \mu(A_j)$로 정의한다($0 \cdot \infty = 0$). 표현 방식과 무관함은 두 표현의 공통 세분을 취해 확인할 수 있다. 음이 아닌 가측함수에 대해서는

$$\int f \, d\mu = \sup\left\{ \int s \, d\mu : 0 \leq s \leq f,\ s\text{는 단순함수} \right\} \in [0, \infty] \tag{4.1}$$

로 정의한다. $f \leq g$이면 $\int f \leq \int g$이고, E 위의 적분은 $\int_E f = \int f \mathbf{1}_E$이다.

명제 4.4 $f \geq 0$이 가측이면 $\int f = 0 \iff f = 0$ a.e.이다.

증명. $f = 0$ a.e.이면 $s \leq f$인 단순함수는 영집합 밖에서 0이므로 적분이 0이다. 역으로 $\{f > 0\} = \bigcup_k \{f > 1/k\}$이고 $\frac{1}{k}\mu(\{f > 1/k\}) \leq \int f = 0$이므로 각 집합의 측도가 0이다. □

이 명제 때문에 Lebesgue 적분에서는 영집합 위의 값을 바꾸어도 적분이 변하지 않는다. 함수들을 "거의 모든 곳에서 같으면 같은 것"으로 보는 관점은 제7장의 L^p 공간에서 공식화된다.

4.4 단조수렴정리

정리 4.5 (단조수렴정리, MCT) 가측함수열이 $0 \leq f_1 \leq f_2 \leq \cdots$이고 점별로 $f_k \uparrow f$이면

$$\int f \, d\mu = \lim_{k \to \infty} \int f_k \, d\mu.$$

증명. $\int f_k$는 증가하고 $\int f_k \leq \int f$이므로 극한 $L \leq \int f$가 존재한다. 반대 부등식을 위해 $0 \leq s \leq f$인 단순함수와 $0 < c < 1$을 고정하고 $E_k = \{f_k \geq c s\}$로 둔다. E_k는 증가하고 $\bigcup E_k = X$이다 ($f(x) > c s(x)$이거나 $s(x) = 0$이므로). 따라서

$$\int f_k \geq \int_{E_k} f_k \geq c \int_{E_k} s \xrightarrow{k \to \infty} c \int s$$

이다. 마지막 수렴은 $A \mapsto \int_A s$가 측도이고 아래로부터 연속이기 때문이다. $L \geq c \int s$에서 $c \to 1$, s에 대한 상한을 취하면 $L \geq \int f$이다. □

따름정리로 음이 아닌 가측함수의 급수는 항별로 적분할 수 있다. $\int \sum_k g_k = \sum_k \int g_k$ ($g_k \geq 0$). 또 적분은 선형이다. 두 함수의 단순함수 근사열을 더해 MCT를 적용하면 $\int (f + g) = \int f + \int g$를 얻는다.

예제 4.6 $\displaystyle\sum_{k \geq 1} \int_0^1 x^{k-1}(1-x) \, dx = \sum_{k} \left(\frac{1}{k} - \frac{1}{k+1} \right) = 1$이다. 한편 $\sum_k x^{k-1}(1-x) = 1$이 $0 \leq x < 1$에서 성립하므로 좌변을 적분한 값과 일치한다. 음이 아닌 항이므로 교환에 조건이 필요 없다.

4.5 Fatou 보조정리

정리 4.7 (Fatou) 음이 아닌 가측함수열 f_k에 대해 $\int \liminf_k f_k \le \liminf_k \int f_k$이다.

증명. $g_n = \inf_{k\ge n} f_k$는 증가하여 $\liminf f_k$로 가고 $g_n \le f_k$ $(k \ge n)$이다. MCT로 $\int \liminf f_k = \lim_n \int g_n \le \lim_n \inf_{k\ge n} \int f_k = \liminf_k \int f_k$이다. □

부등식은 엄격할 수 있다. 앞 장의 $f_k = k\mathbf{1}_{(0,1/k)}$에서 좌변은 0, 우변은 1이다. 극한에서 질량이 "사라질" 수는 있어도 "생겨날" 수는 없다는 것이 Fatou 보조정리의 직관이다. 음이 아니라는 가정을 빼면 결론이 틀린다. $f_k = -k\mathbf{1}_{(0,1/k)}$이면 좌변 0, 우변 -1이다.

4.6 적분가능 함수

부호가 있는 가측함수 f는 $f^+ = \max(f,0)$, $f^- = \max(-f,0)$으로 $f = f^+ - f^-$, $|f| = f^+ + f^-$로 쓴다. $\int |f| < \infty$이면 f를 **적분가능**이라 하고 $\int f = \int f^+ - \int f^-$로 정의한다. 적분가능 함수 전체를 $L^1(\mu)$로 쓰며, 적분은 L^1에서 선형이고 $\left|\int f\right| \le \int |f|$이다.

Lebesgue 적분은 절대 적분이다. $\int_0^\infty \frac{\sin x}{x}\,\mathrm{d}x$는 이상 Riemann 적분으로 $\pi/2$에 수렴하지만 $\int_0^\infty |\sin x|/x\,\mathrm{d}x = \infty$이므로 $[0,\infty)$에서 Lebesgue 적분가능하지 않다. 이 경우 $\pi/2$라는 값은 Lebesgue 적분이 아니라 이상 Riemann 적분의 극한 $\lim_{R\to\infty}\int_0^R$으로 이해한다.

4.7 연습문제와 해설

연습문제 4.8 $\displaystyle\int_0^1 \sum_{k\ge 1} \frac{x^k}{k^2}\,\mathrm{d}x$를 항별 적분으로 계산하라.

풀이. 항이 음이 아니므로 MCT로 교환할 수 있다.

$$\sum_{k} \frac{1}{k^2(k+1)} = \sum_{k}\left(\frac{1}{k^2} - \frac{1}{k} + \frac{1}{k+1}\right) = \frac{\pi^2}{6} - 1$$

이다(부분분수 $\frac{1}{k^2(k+1)} = \frac{1}{k^2} - \frac{1}{k} + \frac{1}{k+1}$과 $\sum 1/k^2 = \pi^2/6$, 나머지 항의 망원급수 -1을 더한다).

연습문제 4.9 셈측도 μ를 갖는 $\mathbb{N}$에서 $\int f\,\mathrm{d}\mu = \sum_n f(n)$임을 보이고, 이 경우 MCT가 무엇을 말하는지 설명하라.

풀이. 단순함수 $\mathbf{1}_{\{n\}}$의 적분은 1이다. $f \ge 0$에 대해 $f_N = f\mathbf{1}_{\{0,\dots,N\}}$로 두면 $f_N \uparrow f$이므로 MCT로 $\int f = \lim_N \sum_{n\le N} f(n)$이다. 음이 아닌 이중수열에 대한 MCT는 "$a_{k,n} \uparrow a_n$이면 $\sum_n a_{k,n} \to \sum_n a_n$"이라는 급수의 단조수렴 정리이다.

연습문제 4.10 Fatou 보조정리를 이용하여, $f_k \ge 0$, $f_k \to f$ a.e., $\int f_k \le C$이면 $\int f \le C$임을 보여라.

풀이. a.e.에서 $\liminf f_k = f$이고 영집합은 적분에 영향을 주지 않으므로 $\int f \le \liminf \int f_k \le C$이다. 이 결론은 $\int f_k \to \int f$를 뜻하지 않는다.

참고 (다음 연결). 단조성이 없을 때 극한과 적분을 교환하려면 적분가능한 상계가 필요하다. 다음 장의 지배수렴정리가 그 조건을 준다.

제 5 장

지배수렴정리와 적분의 계산

개요 이 장의 지배수렴정리는 해석학과 확률론에서 가장 자주 쓰이는 극한 교환 도구이다. 단조성 대신 적분가능한 함수에 의한 지배를 가정하여, 점별 또는 거의 모든 곳에서 수렴하는 함수열의 적분이 극한의 적분으로 수렴함을 보장한다. 매개변수 적분의 연속성과 미분, Riemann 적분과의 관계도 함께 정리한다. 선행 지식: 앞 장의 단조수렴정리와 Fatou 보조정리.

5.1 지배수렴정리

정리 5.1 (지배수렴정리, DCT) 가측함수열 f_k가 거의 모든 곳에서 f로 수렴하고, 적분가능한 g가 있어 모든 k에 대해 $|f_k| \le g$ a.e.이면 f는 적분가능하고

$$\lim_{k\to\infty} \int |f_k - f| \, d\mu = 0, \qquad \lim_{k\to\infty} \int f_k \, d\mu = \int f \, d\mu.$$

증명. $|f| \le g$이므로 f는 적분가능하다. $2g - |f_k - f| \ge 0$에 Fatou 보조정리를 적용하면

$$\int 2g \le \liminf_{k} \int (2g - |f_k - f|) = \int 2g - \limsup_{k} \int |f_k - f|$$

이다. $\int 2g < \infty$이므로 빼면 $\limsup_k \int |f_k - f| \le 0$이다. 둘째 결론은 $\left|\int f_k - \int f\right| \le \int |f_k - f|$에서 나온다. □

지배함수 g는 k와 무관해야 한다. 앞 장들의 반례 $k\mathbf{1}_{(0,1/k)}$에서 가능한 가장 작은 공통 상계는 $\sup_k k\mathbf{1}_{(0,1/k)}(x) \approx 1/x$로 $(0,1)$에서 적분가능하지 않다. 측도가 유한하고 $|f_k| \le M$이면 상수 M이 지배함수가 되며, 이를 **유계수렴정리**(*bounded convergence theorem*)라 부른다.

예제 5.2 $\displaystyle\lim_{k\to\infty} \int_0^{\infty} \frac{dx}{(1+x/k)^k x^{1/2}}$를 구하자. $(1+x/k)^k$는 k에 대해 증가하여 e^x로 가므로 피적분함수는 $e^{-x}x^{-1/2}$로 감소하며 수렴한다. $k \ge 2$에서 $(1+x/k)^k \ge (1+x/2)^2$이므로 지배함수 $x^{-1/2}(1+x/2)^{-2}$는 $(0,\infty)$에서 적분가능하다. 따라서 극한은 $\int_0^\infty e^{-x}x^{-1/2}\,dx = \Gamma(1/2) = \sqrt{\pi}$이다.

5.2 매개변수 적분의 연속성과 미분

정리 5.3 $F(t) = \int f(x,t)\,d\mu(x)$, $t \in (a,b)$라 하자.

(1) 거의 모든 x에서 $t \mapsto f(x,t)$가 연속이고 $|f(x,t)| \le g(x)$, $g \in L^1$이면 F는 연속이다.

(2) 거의 모든 x에서 $\partial_t f(x,t)$가 존재하고 $|\partial_t f(x,t)| \le g(x)$, $g \in L^1$이며 $f(\cdot,t) \in L^1$이면 F는 미분가능하고 $F'(t) = \int \partial_t f(x,t)\,d\mu(x)$이다.

증명. (1) $t_k \to t$인 수열에 DCT를 적용한다. (2) 차분몫 $\dfrac{f(x,t+h_k)-f(x,t)}{h_k}$는 평균값정리로 $|\cdot| \le g(x)$이므로 DCT를 적용한다. □

예제 5.4 (적분 기호 아래의 미분) $I(t)=\displaystyle\int_0^\infty e^{-x}\frac{\sin(tx)}{x}\,dx$라 하자(피적분함수는 $x=0$에서 극한 t를 가지므로 제거가능한 특이점이다). $|\partial_t(\cdot)|=|e^{-x}\cos(tx)|\le e^{-x}$이므로

$$I'(t)=\int_0^\infty e^{-x}\cos(tx)\,dx=\frac{1}{1+t^2}$$

이다. $I(0)=0$이므로 $I(t)=\arctan t$이다.

5.3 Riemann 적분과의 관계

정리 5.5 f가 $[a,b]$에서 Riemann 적분가능하면 Lebesgue 적분가능하고 두 적분값은 같다.

증명의 뼈대. 분할을 계속 세분하는 분할열 P_k에 대해, 각 소구간에서 하한과 상한을 값으로 갖는 단순함수 $\ell_k\le f\le u_k$를 만든다. $\int \ell_k$와 $\int u_k$는 하합과 상합이므로 같은 값으로 수렴한다. ℓ_k는 증가, u_k는 감소하므로 극한 $\ell\le f\le u$가 있고 MCT(또는 DCT)로 $\int(u-\ell)=0$, 따라서 $\ell=f=u$ a.e.이다. f는 가측인 ℓ과 거의 모든 곳에서 같으므로(Lebesgue 측도의 완비성) 가측이고 적분값이 같다. □

이 증명에서 Lebesgue 판정법(불연속점 집합이 영집합임)도 함께 나온다. 반대 방향은 성립하지 않는다. Dirichlet 함수는 Lebesgue 적분값이 0이지만 Riemann 적분가능하지 않다. 이상 Riemann 적분까지 넓히면 이 포함관계가 깨진다. 앞 장의 $\sin x/x$는 $[0,\infty)$에서 이상 Riemann 적분이 존재하지만 Lebesgue 적분가능하지 않다. 피적분함수가 음이 아니면 이상 Riemann 적분과 Lebesgue 적분은 같다.

5.4 적분의 절대연속성

명제 5.6 $f\in L^1(\mu)$이면 모든 $\varepsilon>0$에 대해 $\delta>0$이 있어 $\mu(E)<\delta$이면 $\int_E|f|<\varepsilon$이다.

증명. $f_N=\min(|f|,N)\uparrow|f|$이므로 MCT로 $\int(|f|-f_N)<\varepsilon/2$인 N이 있다. $\delta=\varepsilon/(2N)$이면 $\int_E|f|\le\int(|f|-f_N)+N\mu(E)<\varepsilon$이다. □

이 성질은 제8장에서 부정적분 $F(x)=\int_a^x f$가 절대연속임을 보이는 핵심이다.

5.5 수렴정리의 비교

표 5.1 적분과 극한의 교환을 보장하는 네 정리의 가정과 결론

정리	가정	결론
단조수렴	$0\le f_k\uparrow f$	$\int f_k\to\int f$ (∞ 허용)
Fatou	$f_k\ge 0$	$\int\liminf f_k\le\liminf\int f_k$
지배수렴	$f_k\to f$ a.e., $\lvert f_k\rvert\le g\in L^1$	$\int\lvert f_k-f\rvert\to 0$
Vitali	$\mu(X)<\infty$, $f_k\to f$ a.e., 균등적분가능	$\int\lvert f_k-f\rvert\to 0$

마지막 줄의 **균등적분가능성**(*uniform integrability*)은 $\lim_{M\to\infty}\sup_k \int_{\{|f_k|>M\}} |f_k| = 0$이라는 조건이며, 지배함수가 없을 때 쓰는 일반화이다. 확률론의 마팅게일 수렴에서 중요하다.

5.6 연습문제와 해설

연습문제 5.7 $\displaystyle\lim_{k\to\infty}\int_0^1 \frac{kx}{1+k^2x^2}\,\mathrm{d}x$를 구하라. DCT를 그대로 적용할 수 있는가?

풀이. 점별극한은 0이지만 직접 계산하면 $\int_0^1 \frac{kx}{1+k^2x^2}\,\mathrm{d}x = \frac{\log(1+k^2)}{2k} \to 0$이다. 공통 지배함수로 $\sup_k \frac{kx}{1+k^2x^2} = \frac{1}{2}$ ($k=1/x$ 근처)를 쓸 수 있으므로 상수 $1/2$이 $[0,1]$에서 지배함수이고 DCT로도 극한 0을 얻는다.

연습문제 5.8 $\displaystyle\int_0^\infty e^{-tx^2}\,\mathrm{d}x = \frac{1}{2}\sqrt{\pi/t}$를 t로 미분하여 $\displaystyle\int_0^\infty x^2 e^{-x^2}\,\mathrm{d}x$를 구하라. 미분의 정당성도 확인하라.

풀이. $t \ge t_0 > 0$에서 $\left|\partial_t e^{-tx^2}\right| = x^2 e^{-tx^2} \le x^2 e^{-t_0 x^2} \in L^1$이므로 미분할 수 있다. $-\int x^2 e^{-tx^2}\,\mathrm{d}x = -\frac{\sqrt{\pi}}{4}t^{-3/2}$이고 $t=1$에서 $\int_0^\infty x^2e^{-x^2}\,\mathrm{d}x = \sqrt{\pi}/4$이다.

연습문제 5.9 $f_k = \mathbf{1}_{[k,k+1]}$에서 DCT의 결론이 실패하는 이유를 설명하라.

풀이. 점별극한은 0이고 $\int f_k = 1$이다. 공통 상계는 $\sup_k f_k = \mathbf{1}_{[1,\infty)}$ 이상이어야 하는데 이는 적분가능하지 않다. 질량이 무한대로 "달아나는" 현상이며, 측도가 유한하지 않은 공간에서 균등적분가능성만으로 부족하고 꼬리 조건이 필요한 이유이다.

참고 (다음 연결). 지금까지는 한 측도공간에서의 적분이었다. 다음 장에서는 두 측도의 곱을 만들고 반복적분의 순서를 바꾸는 Fubini–Tonelli 정리를 증명 뼈대와 함께 정리한다.

제 6 장

곱측도와 Fubini–Tonelli 정리

개요 곱측도는 두 측도공간 $(X,\mathcal{A},\mu)$, $(Y,\mathcal{B},\nu)$로부터 곱집합 $X\times Y$ 위에 만드는 측도 $\mu\otimes\nu$이고, 가측 직사각형의 측도를 $\mu(A)\nu(B)$로 정하는 조건으로 유일하게 정해진다. 이 장은 곱 σ-대수와 곱측도를 구성한 뒤, 이중적분 $\iint f\,d\mu\,d\nu$를 반복적분 $\int\left(\int f\,d\nu\right)d\mu$로 바꾸어 계산할 수 있는 정확한 조건을 Tonelli 정리(음이 아닌 함수)와 Fubini 정리(적분가능 함수)로 정리한다. 두 정리의 가정 가운데 하나라도 빠지면 반복적분의 두 순서가 다른 값을 줄 수 있으며, 이 장의 뒷부분은 그런 예를 구체적으로 다룬다. 선행 지식: 제5장의 단조수렴정리(MCT)·지배수렴정리(DCT)와 적분의 성질, 제9권 제5장의 Riemann 이중적분과 그곳의 Fubini 정리.

6.1 곱 σ-대수

측도공간 $(X,\mathcal{A},\mu)$, $(Y,\mathcal{B},\nu)$에 대해 $A\times B$ $(A\in\mathcal{A},\,B\in\mathcal{B})$ 꼴의 집합을 **가측 직사각형**(*measurable rectangle*)이라 하고, 이들 전체가 생성하는 σ-대수를 **곱 σ-대수**(*product σ-algebra*) $\mathcal{A}\otimes\mathcal{B}$라 한다. $\mathbb{R}$의 Borel σ-대수에 대해서는 $\mathcal{B}(\mathbb{R})\otimes\mathcal{B}(\mathbb{R})=\mathcal{B}(\mathbb{R}^2)$이 성립한다. 그러나 Lebesgue 가측 집합족에서는 사정이 다르다. $\mathcal{L}$을 $\mathbb{R}$의 Lebesgue 가측 집합족, $\mathcal{L}(\mathbb{R}^2)$을 $\mathbb{R}^2$의 Lebesgue 가측 집합족이라 하면

$$\mathcal{L}\otimes\mathcal{L}\subsetneq\mathcal{L}(\mathbb{R}^2)$$

이고, $\mathcal{L}(\mathbb{R}^2)$는 곱측도 $m\otimes m$(2차원 Lebesgue 측도)에 대한 $\mathcal{L}\otimes\mathcal{L}$의 완비화이다. 직관적으로는, $\mathcal{L}\otimes\mathcal{L}$의 원소는 두 가측 집합을 곱해 만든 모양을 countably 결합한 것이어야 하는데, $\mathcal{L}(\mathbb{R}^2)$에는 (영집합이 아닌 집합의) 측도 0인 단면들로 이루어진, 그런 식으로 분해되지 않는 집합까지 들어 있다.

집합 $E\subseteq X\times Y$에 대해 $x\in X$, $y\in Y$에서의 **단면**(*section*)을

$$E_x=\{y\in Y:(x,y)\in E\},\qquad E^y=\{x\in X:(x,y)\in E\}$$

로 정의한다.

> **보조정리 6.1 (단면의 가측성)** $E\in\mathcal{A}\otimes\mathcal{B}$이면 모든 $x\in X$에 대해 $E_x\in\mathcal{B}$이고 모든 $y\in Y$에 대해 $E^y\in\mathcal{A}$이다.

증명. $\mathcal{C}=\{E\subseteq X\times Y:E_x\in\mathcal{B}\ (\forall x),\ E^y\in\mathcal{A}\ (\forall y)\}$라 하자. 직사각형 $A\times B$의 단면은 $(A\times B)_x=B$ ($x\in A$일 때) 또는 $\emptyset$이므로 $A\times B\in\mathcal{C}$이다. $(E^c)_x=(E_x)^c$, $\left(\bigcup_n E_n\right)_x=\bigcup_n (E_n)_x$이고 E^y에 대해서도 같은 식이 성립하므로, $\mathcal{C}$는 여집합과 가산합집합에 닫혀 있다. $X\times Y\in\mathcal{C}$이므로 $\mathcal{C}$는 σ-대수이고 모든 직사각형을 포함한다. $\mathcal{A}\otimes\mathcal{B}$는 직사각형을 포함하는 가장 작은 σ-대수이므로 $\mathcal{A}\otimes\mathcal{B}\subseteq\mathcal{C}$이다. $\square$

6.2 σ-유한성과 곱측도

X가 측도가 유한한 가측 집합들의 가산 합집합으로 쓰이면 μ를 **σ-유한**(σ-*finite*)이라 한다. $\mathbb{R}^n$의 Lebesgue 측도와 $\mathbb{N}$ 위의 셈측도는 σ-유한이지만, 비가산 집합 위의 셈측도는 σ-유한이 아니다(측도가 유한한 가측 부분집합은 유한집합뿐이고, 유한집합을 가산 개 모아서는 비가산 전체를 덮을 수 없다).

정리 6.2 (곱측도의 존재와 유일성) μ, ν가 σ-유한이면, $\mathcal{A}\otimes\mathcal{B}$ 위에

$$\pi(A\times B)=\mu(A)\nu(B) \tag{6.1}$$

를 만족하는 측도 $\pi=\mu\otimes\nu$가 유일하게 존재하고, 모든 $E\in\mathcal{A}\otimes\mathcal{B}$에 대해

$$\pi(E)=\int_X \nu(E_x)\,\mathrm{d}\mu(x)=\int_Y \mu(E^y)\,\mathrm{d}\nu(y). \tag{6.2}$$

증명. 먼저 $\mu(X),\nu(Y)<\infty$라 하자. 보조정리 6.1에 의해 $x\mapsto\nu(E_x)$, $y\mapsto\mu(E^y)$는 잘 정의된다.

$$\mathcal{D}=\Big\{E\in\mathcal{A}\otimes\mathcal{B}: x\mapsto\nu(E_x),\ y\mapsto\mu(E^y)\text{가 가측이고 } \int_X\nu(E_x)\,\mathrm{d}\mu=\int_Y\mu(E^y)\,\mathrm{d}\nu\Big\}$$

로 두면, 직사각형 $A\times B$에 대해 $\nu((A\times B)_x)=\nu(B)\mathbf{1}_A(x)$이므로 양변의 적분이 모두 $\mu(A)\nu(B)$가 되어 $A\times B\in\mathcal{D}$이다. 측도가 유한하므로 $E\in\mathcal{D}$이면 $(E^c)_x=(E_x)^c$에서 $\nu((E^c)_x)=\nu(Y)-\nu(E_x)$이고 적분하면 등식이 보존되어 $E^c\in\mathcal{D}$이다. $E_n\uparrow E$ (또는 서로소인 가산합)이면 $\nu((E_n)_x)\uparrow\nu(E_x)$이므로 단조수렴정리로 $\mathcal{D}$는 가산 증가합집합에 닫혀 있다. 따라서 $\mathcal{D}$는 직사각형을 포함하는 λ-계이고, 직사각형의 모임은 교집합에 닫혀 있는 π-계이므로 Dynkin의 π-λ 정리(제10권 제3장)에 의해 $\mathcal{D}\supseteq\sigma(\{A\times B\})=\mathcal{A}\otimes\mathcal{B}$, 곧 $\mathcal{D}=\mathcal{A}\otimes\mathcal{B}$이다. 식 (6.2)의 공통값을 $\pi(E)$로 정의하면, 가산합집합에 대한 가법성은 단조수렴정리로 바로 따라오므로 π는 측도이다.

μ,ν가 σ-유한이면 $X=\bigcup_n X_n$, $Y=\bigcup_n Y_n$ ($X_n\uparrow X$, $Y_n\uparrow Y$, 측도 유한)로 쓰고, 유한측도의 경우를 $\mu|_{X_n},\nu|_{Y_n}$에 적용한 뒤 $n\to\infty$에서 단조수렴정리로 극한을 취하면 같은 결론을 얻는다.

유일성. π'이 같은 조건을 만족하는 또 다른 측도라 하면, π'과 π는 직사각형 위에서 일치하고 $X_n\times Y_n$ 위로 제한하면 모두 유한측도이므로, 유한측도 위에서의 유일성(두 유한측도가 교집합에 닫힌 생성계 위에서 일치하면 전체에서 일치한다는 π-λ 정리의 따름정리)에 의해 $X_n\times Y_n$ 위에서 $\pi=\pi'$이고, $n\to\infty$로 보내면 $\mathcal{A}\otimes\mathcal{B}$ 전체에서 $\pi=\pi'$이다. $\square$

이 증명의 구조—직사각형 위에서 확인하고 λ-계·단조수렴정리로 일반 가측집합으로 확장하는 방식—는 제20권 제4장에서 분포함수가 확률분포를 유일하게 결정한다는 정리의 증명과 같다.

6.3 Tonelli 정리와 Fubini 정리

정리 6.3 (Tonelli) μ,ν가 σ-유한이고 $f: X\times Y\to[0,\infty]$가 $\mathcal{A}\otimes\mathcal{B}$-가측이면, $x\mapsto\int_Y f(x,y)\,\mathrm{d}\nu(y)$와 $y\mapsto\int_X f(x,y)\,\mathrm{d}\mu(x)$는 가측이고

$$\int_{X\times Y} f\,\mathrm{d}\pi=\int_X\Big(\int_Y f\,\mathrm{d}\nu\Big)\mathrm{d}\mu=\int_Y\Big(\int_X f\,\mathrm{d}\mu\Big)\mathrm{d}\nu. \tag{6.3}$$

세 값이 모두 ∞일 수도 있다.

증명. $f = \mathbf{1}_E$ $(E \in \mathcal{A}\otimes\mathcal{B})$이면 식 (6.3)은 정리 6.2의 식 (6.2) 그 자체이다. $f = \sum_{i=1}^{n} c_i \mathbf{1}_{E_i}$ $(c_i \ge 0)$가 음이 아닌 단순함수이면 적분의 선형성으로 각 E_i에 대한 결과를 더해 같은 식을 얻는다. 일반적인 가측 $f \ge 0$에는 f로 증가하는 단순함수열 $\varphi_n \uparrow f$를 잡는다. 각 x에서 $\varphi_n(x,\cdot) \uparrow f(x,\cdot)$이므로 단조수렴정리로 $\int_Y \varphi_n(x,y)\,d\nu(y) \uparrow \int_Y f(x,y)\,d\nu(y)$이고, 왼쪽은 이미 가측인 함수들의 증가열이므로 극한도 x에 대해 가측이다. 다시 단조수렴정리를 x에 대한 적분에 적용하면

$$\int_X \Big(\int_Y \varphi_n \, d\nu\Big) d\mu \;\uparrow\; \int_X \Big(\int_Y f \, d\nu\Big) d\mu,$$

이고 왼쪽은 $\int_{X\times Y} \varphi_n \, d\pi \uparrow \int_{X\times Y} f \, d\pi$와 같으므로 식 (6.3)의 첫째 등식을 얻는다. 둘째 등식은 x, y의 역할을 바꾸어 같은 논증을 되풀이한다. □

> **정리 6.4 (Fubini)** μ, ν가 σ-유한이고 $f \in L^1(\pi)$이면, 거의 모든 x에서 $f(x,\cdot) \in L^1(\nu)$, 거의 모든 y에서 $f(\cdot,y) \in L^1(\mu)$이고, 식 (6.3)의 세 적분이 (모두 유한값으로) 같다.

증명. Tonelli 정리를 $|f|$에 적용하면 $\int_X \big(\int_Y |f|\,d\nu\big)\,d\mu = \int_{X\times Y} |f|\,d\pi < \infty$이므로, 안쪽 적분 $x \mapsto \int_Y |f(x,y)|\,d\nu(y)$는 거의 모든 x에서 유한하다. 곧 거의 모든 x에서 $f(x,\cdot) \in L^1(\nu)$이고, 대칭적으로 거의 모든 y에서 $f(\cdot,y) \in L^1(\mu)$이다. $f = f^+ - f^-$로 쓰면 $f^+, f^- \le |f|$는 음이 아니고 적분이 유한하므로 Tonelli를 각각에 적용할 수 있다. 거의 모든 x에서 $f^+(x,\cdot), f^-(x,\cdot)$가 모두 적분가능하므로 그 차를 빼면

$$\int_Y f \, d\nu = \int_Y f^+ \, d\nu - \int_Y f^- \, d\nu$$

가 거의 모든 x에서 성립하고, 양변을 μ에 대해 적분하면

$$\int_X \Big(\int_Y f\,d\nu\Big)d\mu = \int_X \Big(\int_Y f^+\,d\nu\Big)d\mu - \int_X \Big(\int_Y f^-\,d\nu\Big)d\mu = \int_{X\times Y} f^+\,d\pi - \int_{X\times Y} f^-\,d\pi = \int_{X\times Y} f\,d\pi$$

를 얻는다. 둘째 등식도 같은 방식이다. □

주의 (적분가능성은 먼저 확인한다). Tonelli 정리는 조건 없이 음이 아닌 함수의 적분 순서를 바꾸어 주지만, Fubini 정리는 $f \in L^1(\pi)$를 요구한다. 실제 계산에서는 먼저 $|f|$에 Tonelli 정리를 적용하여 $\iint |f|\,d\nu\,d\mu < \infty$를 확인한 뒤에 Fubini 정리로 순서를 바꾼다. 이 확인을 거르고 바로 순서를 바꾸는 것은 가장 흔한 오류이며, 6.4절의 두 예제가 그 결과를 보여 준다. 지시함수 $\to$ 단순함수 $\to$ 단조수렴정리 $\to$ 양수부·음수부로 이어지는 위 증명의 순서는 "표준 기계"라 불리며, 측도론의 거의 모든 정리가 같은 틀로 증명된다.

핵심 수식

$$\begin{aligned} \pi(E) &= \int_X \nu(E_x)\,d\mu(x) = \int_Y \mu(E^y)\,d\nu(y) \qquad \text{(곱측도)},\\ \int_{X\times Y} f\,d\pi &= \int_X \int_Y f\,d\nu\,d\mu \\ &= \int_Y \int_X f\,d\mu\,d\nu \qquad (f \ge 0,\ \text{Tonelli 정리}),\\ f \in L^1(\pi) &\;\Rightarrow\; \text{위 세 적분이 유한값으로 일치} \qquad \text{(Fubini 정리)}. \end{aligned}$$

역사. Guido Fubini(1879–1943)는 1907년에 적분가능 함수에 대한 순서 교환 정리를 증명하였고, Leonida Tonelli(1885–1946)는 1909년에 음이 아닌 가측함수에는 적분가능성 가정이 필요 없음을 보였다. 두 사람 모두 이탈리아의 해석학자이다.

6.4 가정이 빠지면 생기는 일

예제 6.5 (적분가능성이 없을 때) $X = Y = \mathbb{N}$ 위의 셈측도에서

$$a_{m,n} = \begin{cases} 1, & n = m, \\ -1, & n = m+1, \\ 0, & \text{그 밖}. \end{cases}$$

이라 하자. 행 m의 합은 $a_{m,m} + a_{m,m+1} = 1 - 1 = 0$이므로 $\sum_m \sum_n a_{m,n} = 0$이다. 열 $n = 0$의 합은 $a_{0,0} = 1$뿐이므로 1이고, $n \geq 1$이면 $a_{n,n} + a_{n-1,n} = 1 - 1 = 0$이므로 $\sum_n \sum_m a_{m,n} = 1$이다. 두 반복합이 다르므로 Fubini 정리의 결론이 깨지는데, 실제로 $\sum_{m,n} |a_{m,n}| = \infty$이어서 가정이 애초에 성립하지 않는다. 제9권 제5장에서 다룬 $\dfrac{x^2 - y^2}{(x^2+y^2)^2}$의 반복적분 예도 같은 현상(절댓값의 적분이 발산하여 순서를 바꿀 수 없음)을 보여 준다.

예제 6.6 (σ-유한성이 없을 때) $X = Y = [0,1]$, μ는 Lebesgue 측도, ν는 셈측도라 하고 대각선 $D = \{(x,x) : x \in [0,1]\}$을 생각하자. 단면 $D_x = \{x\}$는 한 점이므로 $\nu(D_x) = 1$이고

$$\int_X \nu(D_x)\, d\mu(x) = \int_0^1 1 \, dx = 1$$

이다. 반면 단면 $D^y = \{y\}$는 Lebesgue 측도 0인 집합이므로 $\mu(D^y) = 0$이고

$$\int_Y \mu(D^y)\, d\nu(y) = \sum_{y \in [0,1]} 0 = 0$$

이다. ν가 σ-유한이 아니므로([0,1]을 셈측도로 유한측도 집합의 가산합으로 쓸 수 없다) Tonelli 정리를 적용할 수 없고, 두 반복적분은 실제로 다른 값 $1 \neq 0$을 준다.

6.5 응용

예제 6.7 (분포함수와 기댓값) 확률변수 $X \geq 0$에 대해 $X(\omega) = \int_0^\infty \mathbf{1}_{\{t < X(\omega)\}}\, dt$이므로, $f(\omega, t) = \mathbf{1}_{\{t<X(\omega)\}} \geq 0$에 Tonelli 정리를 적용하면

$$\mathbb{E}X = \int_0^\infty P(X > t)\, dt$$

이다. 같은 방법을 $f(\omega,t) = p\, t^{p-1} \mathbf{1}_{\{t<X(\omega)\}}$ $(p > 0)$에 적용하면

$$\mathbb{E}X^p = \int_0^\infty p\, t^{p-1} P(X > t)\, dt$$

를 얻는다.

예제 6.8 (합성곱) $f, g \in L^1(\mathbb{R})$이면 $(f*g)(x) = \int f(x-y)g(y)\,dy$는 거의 모든 x에서 정의되고 $\|f*g\|_1 \le \|f\|_1 \|g\|_1$이다. 실제로 Tonelli 정리로

$$\iint |f(x-y)|\,|g(y)|\,dy\,dx = \int |g(y)| \left(\int |f(x-y)|\,dx \right) dy = \|f\|_1 \|g\|_1 < \infty$$

이므로 Fubini 정리를 쓸 수 있다. 확률론에서 독립인 두 확률변수의 합의 밀도함수가 각 밀도함수의 합성곱이라는 사실의 근거가 바로 이 계산이다.

예제 6.9 ($\int_0^\infty \frac{\sin x}{x}\,dx$ 다시 계산하기) $x>0$에서 $1/x = \int_0^\infty e^{-xt}\,dt$이므로

$$\int_0^R \frac{\sin x}{x}\,dx = \int_0^R \int_0^\infty \sin x\, e^{-xt}\,dt\,dx$$

로 쓴다. $[0,R]\times[0,\infty)$에서 $|\sin x\, e^{-xt}|$를 t에 대해 적분하면 $|\sin x|/x$이고, 이는 $x\to 0$에서 유계이므로 $[0,R]$ 위에서 적분가능하여 Fubini 정리를 적용할 수 있다. 순서를 바꾸고 안쪽 적분을 계산하면

$$\int_0^R \frac{\sin x}{x}\,dx = \int_0^\infty \left(\int_0^R \sin x\, e^{-xt}\,dx \right) dt \xrightarrow[R\to\infty]{} \int_0^\infty \frac{dt}{1+t^2} = \frac{\pi}{2}$$

를 얻는다(마지막 극한은 지배수렴정리로 정당화한다). $[0,\infty)\times[0,\infty)$ 전체에서 한꺼번에 순서를 바꾸려 하면 $\iint |\sin x\, e^{-xt}|\,dt\,dx = \int_0^\infty |\sin x|/x\,dx = \infty$이므로 가정이 성립하지 않는다.

6.6 연습문제와 해설

연습문제 6.10 $\displaystyle\int_0^1\int_0^1 \frac{dx\,dy}{1-xy} = \frac{\pi^2}{6}$임을 보여라.

풀이. $0 \le xy < 1$인 곳(경계 $\{xy=1\}\cap[0,1]^2 = \{(1,1)\}$은 영집합이므로 제외해도 적분값에 영향이 없다)에서 $\dfrac{1}{1-xy} = \sum_{k\ge 0}(xy)^k$이고 각 항이 음이 아니므로 Tonelli 정리와 단조수렴정리로 항별 적분을 할 수 있다.

$$\int_0^1\int_0^1 \frac{dx\,dy}{1-xy} = \sum_{k\ge 0}\int_0^1 x^k\,dx \int_0^1 y^k\,dy = \sum_{k\ge 0}\frac{1}{(k+1)^2} = \frac{\pi^2}{6}.$$

연습문제 6.11 $X\sim \mathrm{Exp}(\lambda)$에 대해 $\mathbb{E}X = \int_0^\infty P(X>t)\,dt$로 $\mathbb{E}X$를 구하라.

풀이. $P(X>t) = e^{-\lambda t}$이므로 $\mathbb{E}X = \int_0^\infty e^{-\lambda t}\,dt = 1/\lambda$이다.

연습문제 6.12 $f(x,y) = e^{-xy}\sin x$를 $[0,\infty)\times[1,\infty)$ 위에서 적분할 때 Fubini 정리를 쓸 수 있는지 판정하라.

풀이. $\displaystyle\int_1^\infty e^{-xy}\,dy = \frac{e^{-x}}{x}$이므로 Tonelli 정리로

$$\iint |f| = \int_0^\infty \frac{|\sin x|\,e^{-x}}{x}\,dx < \infty$$

이다($x \to 0$에서 피적분함수가 1로 유계이고, $x \to \infty$에서 e^{-x}가 지수적으로 감소한다). 따라서 Fubini 정리를 쓸 수 있다. 영역의 y 범위를 $[0,\infty)$로 넓히면 $\int_0^\infty e^{-xy}\,\mathrm{d}y = 1/x$가 되어 $\iint |f| = \int_0^\infty |\sin x|/x \,\mathrm{d}x = \infty$이므로 쓸 수 없다.

적분가능 함수들의 집합 $L^1(\mu)$는 벡터공간이고 $\|f\|_1 = \int |f|\,\mathrm{d}\mu$라는 노름을 갖는다. 다음 장에서는 이 노름을 L^p 공간 전체로 넓히고, 그 공간이 완비 노름공간임과 측도론에 등장하는 여러 수렴 개념의 관계를 정리한다.

제 7 장

L^p 공간

개요 $L^p(\mu)$ 공간은 p제곱 적분가능한 가측함수들을 거의 모든 곳에서 같은 것끼리 동일시하여 얻는, 노름 $\|\cdot\|_p$을 갖는 벡터공간이다. 이 장은 Hölder 부등식과 Minkowski 부등식으로 $\|\cdot\|_p$가 실제로 노름임을 보이고, Riesz–Fischer 정리로 L^p가 완비임을 증명한 뒤, 측도론에 등장하는 네 가지 수렴 개념(거의 모든 곳 수렴, 측도수렴, L^p 수렴, 균등수렴)의 함의 관계를 정리한다. 함수해석학(제13권)에서 다루는 노름공간 가운데 L^p 공간이 가장 중요한 예이다. 선행 지식: 앞 장들의 Lebesgue 적분과 수렴정리, 제7권 제8장의 노름과 내적.

7.1 정의와 동치류

$1 \le p < \infty$에 대해

$$\|f\|_p = \left(\int |f|^p \, d\mu \right)^{1/p},$$

$p = \infty$에 대해

$$\|f\|_\infty = \operatorname{ess\,sup} |f| = \inf\{ M \ge 0 : |f| \le M \text{ a.e.} \}$$

로 둔다. $\|f\|_p < \infty$인 가측함수 전체를 거의 모든 곳에서 같은 함수는 같은 것으로 보는 **동치류**(*equivalence class*)들의 공간을 $L^p(\mu)$라 한다. 동치류를 쓰는 이유는 $\|f\|_p = 0$이 ($p < \infty$일 때) $f = 0$ a.e.와 같은 뜻이기 때문이다. 실제로 $\int |f|^p \, d\mu = 0$이면 $|f|^p$가 음이 아니므로 $\{|f| > 0\}$의 측도는 0이어야 한다($\{|f| > 1/n\}$의 측도가 모두 0임을 보이고 가산합으로 합친다). 이 동일시 때문에 L^p의 원소에 대해 "한 점에서의 값"은 의미를 갖지 않고, 오직 거의 모든 곳에서의 성질만 의미를 갖는다.

7.2 Hölder 부등식과 Minkowski 부등식

$1 < p < \infty$이고 $\dfrac{1}{p} + \dfrac{1}{q} = 1$인 q를 p의 **켤레지수**(*conjugate exponent*)라 한다($p = 1$의 켤레지수는 $q = \infty$, $p = \infty$의 켤레지수는 $q = 1$로 정한다).

보조정리 7.1 (Young의 부등식) $a, b \ge 0$이면

$$ab \le \frac{a^p}{p} + \frac{b^q}{q}$$

이고, 등호는 $a^p = b^q$일 때 성립한다.

증명. $a = 0$ 또는 $b = 0$이면 자명하므로 $a, b > 0$이라 하자. $\log$는 오목함수이므로

$$\log\!\left(\frac{a^p}{p} + \frac{b^q}{q} \right) \ge \frac{1}{p}\log a^p + \frac{1}{q}\log b^q = \log a + \log b = \log(ab)$$

이고, log가 증가함수이므로 부등식이 따라온다. 오목함수의 등호 조건(가중평균의 등호는 두 점이 같을 때)에서 등호는 $a^p = b^q$ 일 때이다. □

정리 7.2 (Hölder) $1 \le p \le \infty$이고 q가 p의 켤레지수이면 $\|fg\|_1 \le \|f\|_p \, \|g\|_q$이다.

증명. $1 < p < \infty$이고 $\|f\|_p, \|g\|_q$가 모두 양의 유한값이라 하자(둘 중 하나가 0이면 $fg = 0$ a.e.이고, 하나가 ∞이면 부등식이 자명하다). $a = |f| / \|f\|_p$, $b = |g| / \|g\|_q$에 보조정리 7.1을 적용하고 양변을 적분하면

$$\int \frac{|fg|}{\|f\|_p \, \|g\|_q} \, \mathrm{d}\mu \le \int \left(\frac{a^p}{p} + \frac{b^q}{q} \right) \mathrm{d}\mu = \frac{1}{p} \cdot \frac{\|f\|_p^p}{\|f\|_p^p} + \frac{1}{q} \cdot \frac{\|g\|_q^q}{\|g\|_q^q} = \frac{1}{p} + \frac{1}{q} = 1$$

이므로 $\|fg\|_1 \le \|f\|_p \, \|g\|_q$이다. $p = 1$ ($q = \infty$)인 경우는 $|fg| \le |f| \, \|g\|_\infty$ a.e.에서 바로 적분하여 얻고, $p = \infty$인 경우는 역할을 바꾼다. □

$p = q = 2$이면 Hölder 부등식은 Cauchy–Schwarz 부등식이다. 측도가 유한하면 $1 \le r < p$에 대해 상수함수 1과 $|f|^r$에 지수 p/r로 Hölder 부등식을 쓰면

$$\|f\|_r \le \mu(X)^{1/r - 1/p} \, \|f\|_p$$

를 얻으므로 $L^p \subseteq L^r$이다. 측도가 무한하면 이 포함관계는 성립하지 않는다. $\mathbb{R}$에서 $1/x$를 $[1, \infty)$로 제한한 함수는 L^2에는 있지만($\int_1^\infty x^{-2} \, \mathrm{d}x < \infty$) L^1에는 없고($\int_1^\infty x^{-1} \, \mathrm{d}x = \infty$), $x^{-1/2} \mathbf{1}_{(0,1)}$은 L^1에는 있지만($\int_0^1 x^{-1/2} \, \mathrm{d}x = 2 < \infty$) L^2에는 없다($\int_0^1 x^{-1} \, \mathrm{d}x = \infty$).

정리 7.3 (Minkowski) $1 \le p \le \infty$이면 $\|f + g\|_p \le \|f\|_p + \|g\|_p$이다.

증명. $p = 1, \infty$인 경우는 삼각부등식 $|f + g| \le |f| + |g|$에서 바로 나온다. $1 < p < \infty$이라 하자. 볼록부등식 $|f + g|^p \le 2^{p-1}(|f|^p + |g|^p)$에서 $\|f + g\|_p < \infty$임을 먼저 확인한다. 그 다음

$$|f + g|^p = |f + g| \cdot |f + g|^{p-1} \le |f| \, |f + g|^{p-1} + |g| \, |f + g|^{p-1}$$

에 $(p - 1)q = p$(즉 $|f + g|^{p-1} \in L^q$)인 켤레지수 q로 Hölder 부등식을 적용하면

$$\|f + g\|_p^p \le \left(\|f\|_p + \|g\|_p \right) \|f + g\|_p^{p-1}$$

를 얻는다. $\|f + g\|_p$가 양의 유한값이면 양변을 $\|f + g\|_p^{p-1}$로 나누어 결론을 얻고, $\|f + g\|_p = 0$이면 부등식이 자명하다. □

따라서 $\|\cdot\|_p$ ($1 \le p \le \infty$)는 L^p 위의 노름이다. $0 < p < 1$이면 삼각부등식이 실패하므로 노름이 아니다. 양수 a, b에 대해 $a^p + b^p > (a + b)^p$이므로, 측도 1인 서로소 집합의 지시함수 f, g에서 $\|f + g\|_p = 2^{1/p} > 2 = \|f\|_p + \|g\|_p$이다.

핵심 수식

Young: $$ab \le \frac{a^p}{p} + \frac{b^q}{q},$$

Hölder: $$\|fg\|_1 \le \|f\|_p \, \|g\|_q \quad \left(\frac{1}{p} + \frac{1}{q} = 1 \right),$$

Minkowski:	$\|f+g\|_p \le \|f\|_p + \|g\|_p$.

7.3 완비성: Riesz–Fischer 정리

정리 7.4 (Riesz–Fischer) $1 \le p \le \infty$에 대해 $L^p(\mu)$는 완비이다. 또한 L^p에서 수렴하는 수열은 거의 모든 곳에서 수렴하는 부분수열을 갖는다.

증명의 뼈대 ($p < \infty$). Cauchy 수열 f_k에서 $\|f_{k_{j+1}} - f_{k_j}\|_p < 2^{-j}$인 부분수열을 뽑는다(Cauchy 수열의 정의에서 $\varepsilon = 2^{-j}$에 대응하는 꼬리를 차례로 고르면 된다). $g = |f_{k_1}| + \sum_j |f_{k_{j+1}} - f_{k_j}|$로 두면, 단조수렴정리와 Minkowski 부등식으로

$$\|g\|_p \le \|f_{k_1}\|_p + \sum_{j} \|f_{k_{j+1}} - f_{k_j}\|_p \le \|f_{k_1}\|_p + 1 < \infty$$

이므로 g는 거의 모든 곳에서 유한하다. 따라서 망원급수 $f_{k_1} + \sum_j (f_{k_{j+1}} - f_{k_j})$가 거의 모든 곳에서 절대수렴하여 극한 f를 정의하고, 부분합이 f_{k_j}이므로 $f_{k_j} \to f$ a.e.이다. $|f_{k_j} - f|^p \le (2g)^p \in L^1$이므로 지배수렴정리로 $f_{k_j} \to f$ (L^p)이다. Cauchy 수열이 수렴하는 부분수열을 가지면 전체 수열도 같은 극한으로 수렴하므로 L^p는 완비이고, 위에서 얻은 부분수열은 a.e. 수렴한다. □

$p = 2$인 경우 $\langle f, g\rangle = \int f\overline{g}\, d\mu$가 내적이므로 L^2는 Hilbert 공간이다. Fourier 급수가 $L^2[-\pi,\pi]$에서 수렴한다는 사실과, 양자역학의 파동함수 공간이 L^2라는 사실은 모두 이 완비성에 근거를 둔다.

7.4 조밀한 부분집합

$\mathbb{R}^n$의 Lebesgue 측도에서 $1 \le p < \infty$이면 다음 각각이 L^p에서 조밀하다.

(1) 단순함수,
(2) 측도가 유한한 집합 위의 단순함수,
(3) 계단함수(직사각형 지시함수들의 유한 일차결합),
(4) 콤팩트 지지를 갖는 연속함수 $C_c(\mathbb{R}^n)$,
(5) $C_c^\infty(\mathbb{R}^n)$ (콤팩트 지지를 갖는 무한 번 미분가능한 함수).

이 조밀성 덕분에 많은 정리를 매끄러운 함수에서 먼저 증명한 뒤 극한을 취해 일반 L^p 함수로 확장한다. $p = \infty$에서는 이 성질이 실패한다. $\mathbf{1}_{[0,\infty)}$와 연속함수 사이의 ∞-노름 거리는 항상 $1/2$ 이상이다(연속함수는 0을 지나면서 1과 0 사이의 값을 가지므로, 그 점 근처에서 $\mathbf{1}_{[0,\infty)}$와의 차이가 $1/2$을 넘을 수밖에 없다).

예제 7.5 (평행이동의 연속성) $f \in L^p(\mathbb{R})$, $1 \le p < \infty$이면 $\|f(\cdot + h) - f\|_p \to 0$ $(h \to 0)$이다. C_c 함수에서는 균등연속성으로 바로 성립하고, 조밀성과 $\|f(\cdot+h)\|_p = \|f\|_p$(평행이동이 Lebesgue 측도를 보존함)를 이용한 3ε 논법으로 일반 f에 확장한다. $p = \infty$에서는 $\mathbf{1}_{[0,\infty)}$가 반례이다($\|\mathbf{1}_{[h,\infty)} - \mathbf{1}_{[0,\infty)}\|_\infty = 1$이 모든 $h \neq 0$에서 성립한다).

7.5 여러 수렴 개념

측도공간 위의 가측함수열 f_k와 f에 대해 다음 수렴 개념들을 구분한다.

- 거의 모든 곳 수렴: $f_k(x) \to f(x)$ a.e.
- 측도수렴(*convergence in measure*): 모든 $\varepsilon > 0$에 대해 $\mu(\{|f_k - f| > \varepsilon\}) \to 0$.
- L^p 수렴: $\|f_k - f\|_p \to 0$.
- 균등수렴(a.e. 기준): $\|f_k - f\|_\infty \to 0$.

Chebyshev 부등식 $\mu(\{|h| > \varepsilon\}) \le \varepsilon^{-p}\,\|h\|_p^p$로 L^p 수렴은 측도수렴을 함의한다. 측도가 유한하면 거의 모든 곳 수렴도 측도수렴을 함의한다(Egorov 정리, 아래 참고). 그 밖의 함의는 일반적으로 성립하지 않는다.

> **예제 7.6 (측도수렴하지만 어디서도 점별수렴하지 않는 열)** $[0,1]$을 길이 $1/2, 1/3, 1/4, \dots$ 인 구간들로 차례로 덮어 나가는 "타자기" 열 $f_k = \mathbf{1}_{I_k}$를 생각하자. 길이 $1/m$인 구간들이 $[0,1]$을 한 바퀴 덮고 나면 길이 $1/(m+1)$인 구간들로 넘어간다. $\|f_k\|_p = |I_k|^{1/p} \to 0$이므로 f_k는 L^p 수렴하고(따라서 측도수렴도 하고) 0에 수렴하지만, 각 점 $x \in [0,1]$은 무한히 많은 I_k에 속하고 무한히 많은 I_k에 속하지 않으므로 $f_k(x)$는 어느 점에서도 수렴하지 않는다(값이 무한히 자주 0과 1을 오간다). Riesz–Fischer 정리가 말하는 대로, 적당한 부분수열(예컨대 m이 바뀌는 시점만 모은 부분수열)은 a.e. 수렴한다.

> **정리 7.7 (Egorov)** $\mu(X) < \infty$이고 $f_k \to f$ a.e.이며 모든 f_k가 a.e. 유한이면, 모든 $\varepsilon > 0$에 대해 $\mu(E) < \varepsilon$인 가측집합 E가 있어 $X \setminus E$에서 $f_k \to f$가 균등수렴한다.

7.6 연습문제와 해설

> **연습문제 7.8** $f(x) = x^{-a}\mathbf{1}_{(0,1)}(x)$가 $L^p(\mathbb{R})$에 속할 조건을 구하라. $g(x) = x^{-a}\mathbf{1}_{(1,\infty)}(x)$는 어떠한가?

풀이. $\displaystyle\int_0^1 x^{-ap}\,dx < \infty \iff ap < 1$이므로 $f \in L^p \iff p < 1/a$이다. g는 $\displaystyle\int_1^\infty x^{-ap}\,dx < \infty \iff ap > 1$이므로 $g \in L^p \iff p > 1/a$이다. 원점의 특이성은 작은 p를, 무한대에서의 느린 감소(긴 꼬리)는 큰 p를 선호한다.

> **연습문제 7.9** $\mu(X) = 1$이면 $\|f\|_1 \le \|f\|_2 \le \|f\|_\infty$임을 보여라.

풀이. 첫 부등식은 Hölder 부등식 $\int |f|\cdot 1\,d\mu \le \|f\|_2\,\|1\|_2 = \|f\|_2\sqrt{\mu(X)} = \|f\|_2$이다. 둘째 부등식은 $|f| \le \|f\|_\infty$ a.e.에서 $\int |f|^2\,d\mu \le \|f\|_\infty^2\,\mu(X) = \|f\|_\infty^2$이므로 따라온다. 확률공간에서는 $\mathbb{E}\,|X| \le (\mathbb{E}X^2)^{1/2}$와 같은 부등식이다.

> **연습문제 7.10** L^1 수렴하지만 L^2 수렴하지는 않는 예를 들라.

풀이. $f_k = \sqrt{k}\,\mathbf{1}_{(0,1/k)}$이면 $\|f_k\|_1 = \sqrt{k}\cdot\dfrac{1}{k} = k^{-1/2} \to 0$이지만 $\|f_k\|_2^2 = k\cdot\dfrac{1}{k} = 1$이어서 f_k는 0으로 L^2 수렴하지 않는다. L^1 수렴은 L^2 수렴을 함의하지 않는다.

마지막 장에서는 미적분 기본정리를 Lebesgue 적분으로 다시 세운다. "부정적분의 도함수는 원래 함수인가", "도함수를 적분하면 원래 함수로 돌아오는가"가 그 장의 정확한 물음이다.

제 8 장

미분과 적분: 유계변동, 절대연속, 미분정리

개요 이 장은 미적분 기본정리를 Lebesgue 적분의 언어로 다시 세운다. 리만 적분에서는 두 방향의 정리—도함수의 적분이 원래 함수를 돌려주는 방향과, 적분의 도함수가 피적분함수를 돌려주는 방향—가 모두 연속성 가정 위에서 성립했다. Lebesgue 적분에서는 연속성 대신 적분가능성과 "거의 모든 곳"이라는 말을 쓰며, 두 방향의 정리가 서로 다른 조건(전자는 항상 성립, 후자는 절대연속이라는 추가 조건 필요)을 요구한다는 것이 이 장의 핵심 내용이다. 유계변동 함수, 절대연속 함수, Cantor 함수(절대연속이 아닌 연속 증가함수의 표준 예)를 차례로 다루고, 측도의 Lebesgue 분해와 Radon–Nikodym 정리로 결과를 측도의 언어로 정리한다. 몇몇 깊은 정리(Lebesgue 미분정리의 미분가능성 부분, 단조함수의 a.e. 미분가능성)는 증명 전체보다 진술과 사용법 중심으로 다룬다. 선행 지식: 앞 장들의 Lebesgue 적분과 L^1, 제8권 제4장의 (Riemann 적분에 대한) 미적분 기본정리.

8.1 두 방향의 질문

Riemann 적분의 미적분 기본정리는 다음 두 문장으로 이루어져 있었다.

(A) f가 연속이면 $F(x) = \int_a^x f$는 미분가능하고 $F' = f$이다.

(B) F가 C^1이면 $\int_a^b F' = F(b) - F(a)$이다.

Lebesgue 적분에서는 연속성 대신 적분가능성과 "거의 모든 곳"이라는 조건을 쓴다.

(A의 일반화) $f \in L^1$이면 $F' = f$가 거의 모든 곳에서 성립하는가? 그렇다(정리 8.1, Lebesgue 미분정리).

(B의 일반화) F가 거의 모든 곳에서 미분가능하고 $F' \in L^1$이면 $\int_a^b F' = F(b) - F(a)$인가? 일반적으로는 아니다(8.4절의 Cantor 함수). **절대연속**이라는 조건이 추가로 필요하다(정리 8.7).

8.2 Lebesgue 미분정리

정리 8.1 (Lebesgue 미분정리) $f \in L^1_{\mathrm{loc}}(\mathbb{R}^n)$이면 거의 모든 x에서

$$\lim_{r \to 0} \frac{1}{|B(x,r)|} \int_{B(x,r)} |f(y) - f(x)| \, \mathrm{d}y = 0$$

이다. 이런 성질을 갖는 점 x를 f의 **Lebesgue 점**(*Lebesgue point*)이라 한다.

특히 $n = 1$이면 거의 모든 x에서 $\frac{1}{h}\int_x^{x+h} f \to f(x)$ $(h \to 0)$, 곧 $F(t) = \int_a^t f$에 대해 $F'(x) = f(x)$이다.

증명의 뼈대. Hardy–Littlewood 극대함수 $Mf(x) = \sup_{r>0} \frac{1}{|B(x,r)|}\int_{B(x,r)} |f|$에 대한 약 $(1,1)$ 부등식

$$|\{Mf > \lambda\}| \le \frac{3^n}{\lambda}\,\|f\|_1$$

을 Vitali 덮개 보조정리(유한 개의 서로소인 공으로 전체 덮개를 반지름 3배 확장하여 피복하는 보조정리)로 증명한다. 제7장에서 다룬, 콤팩트 지지를 갖는 연속함수가 L^1에서 조밀하다는 사실과 이 약 $(1,1)$ 부등식을 결합하면, 거의 모든 x에서 평균이 $f(x)$로 수렴한다는 결론을 얻는다. $\square$

> **예제 8.2** $f = \mathbf{1}_{[0,\infty)}$이면 $x \neq 0$인 모든 점이 Lebesgue 점이다. $x = 0$에서는
>
> $$\frac{1}{2r}\int_{-r}^{r} |f(y) - f(0)|\,\mathrm{d}y = \frac{1}{2r}\int_{-r}^{0} 1\,\mathrm{d}y = \frac{1}{2}$$
>
> 이므로 ($r \to 0$에서 이 값이 0으로 가지 않으므로) 0은 Lebesgue 점이 아니다. 예외 집합 $\{0\}$은 영집합이므로 정리의 결론(거의 모든 점이 Lebesgue 점)과 모순이 아니다.

8.3 단조함수와 유계변동 함수

> **정리 8.3 (Lebesgue)** $[a,b]$ 위의 단조함수는 거의 모든 곳에서 미분가능하다. 증가함수 F에 대해 $F' \in L^1[a,b]$이며
>
> $$\int_a^b F' \le F(b) - F(a).$$

부등식의 증명. 차분몫 $g_k(x) = \dfrac{F(x+1/k) - F(x)}{1/k} \ge 0$ (F를 $[b,b+1]$에서 $F(b)$로 연장)에 Fatou 보조정리를 적용하면

$$\int_a^b F' = \int_a^b \lim_{k\to\infty} g_k \le \liminf_{k\to\infty}\int_a^b g_k = \liminf_{k\to\infty}\Big(k\int_b^{b+1/k} F - k\int_a^{a+1/k} F\Big) \le F(b) - F(a)$$

을 얻는다(마지막 부등식은 F가 증가함수이므로 $k\int_b^{b+1/k} F \le F(b)$, $k\int_a^{a+1/k} F \ge F(a)$이기 때문이다). 미분가능성 자체(거의 모든 곳에서 극한 F'이 존재한다는 사실)는 Vitali 덮개 논법을 쓰는 더 깊은 정리이며 진술만 받아들인다. $\square$

> **정의 8.4 (전변동과 유계변동)** $F:[a,b]\to\mathbb{R}$의 **전변동**(*total variation*)을
>
> $$V_a^b(F) = \sup \sum_{j=1}^{n} \big|F(x_j) - F(x_{j-1})\big|$$
>
> (상한은 $a = x_0 < x_1 < \cdots < x_n = b$ 꼴의 모든 분할에 대해 취한다)로 정의하고, $V_a^b(F) < \infty$이면 F를 **유계변동**(*bounded variation*, BV) 함수라 한다. $x \in [a,b]$에 대해 $V_a^x(F)$도 같은 방식으로 정의한다.

> **명제 8.5 (Jordan 분해)** F가 유계변동일 필요충분조건은 F가 두 증가함수의 차로 쓰이는 것이다.

증명. ($\Leftarrow$) 두 증가함수의 전변동은 각각 $F_1(b)-F_1(a)$, $F_2(b)-F_2(a)$이고 $V_a^b(F_1-F_2) \le V_a^b(F_1) + V_a^b(F_2) < \infty$이므로 차도 유계변동이다.

($\Rightarrow$) $V(x) = V_a^x(F)$ (전변동 함수, $V(a) = 0$)라 하자. $x < y$이면 구간 $[x, y]$ 위의 분할에서

$$V(y) - V(x) = V_x^y(F) \geq |F(y) - F(x)| \geq F(y) - F(x)$$

이므로 $V + (-F)$, 곧 $V - F$는 증가함수이고, 같은 부등식에서 $V + F$도 증가함수이다. 따라서

$$F(x) - F(a) = V(x) - \big(V(x) - (F(x) - F(a))\big)$$

는 두 증가함수 $V(x)$와 $V(x) - F(x) + F(a)$의 차이고, 이는 곧 $F(x) = F(a) + \tfrac{1}{2}\big[(V(x) + F(x) - F(a)) - (V(x) - F(x) + F(a))\big]$로도 쓸 수 있다. $\square$

정리 8.3에 의해 증가함수는 거의 모든 곳에서 미분가능하므로, 명제 8.5에 의해 BV 함수도 두 증가함수의 차로서 거의 모든 곳에서 미분가능하다. C^1 함수 F는 $V_a^b(F) = \int_a^b |F'|$을 만족하는 BV 함수이다(구간을 잘게 나눌수록 $\sum |F(x_j) - F(x_{j-1})| = \sum |F'(\xi_j)|\,(x_j - x_{j-1})$이 Riemann 합으로 $\int |F'|$에 수렴하기 때문이다).

흔한 오류. 연속이라고 해서 유계변동인 것은 아니다. $F(x) = x\sin(1/x)$ $(x \neq 0)$, $F(0) = 0$은 $[0,1]$에서 연속이지만, 진동의 봉우리 높이의 합이 $\sum \frac{1}{k}$ 꼴의 조화급수처럼 발산하여 전변동이 무한하다.

8.4 Cantor 함수: 등식이 깨지는 예

Cantor 집합의 제거 구간 위에서 계단 모양으로 정의되는 **Cantor 함수**(*Cantor function*, 흔히 "악마의 계단"이라 불린다) $c : [0,1] \to [0,1]$은 다음과 같이 구성한다. 첫 단계에서 제거되는 가운데 구간 $(1/3, 2/3)$ 위에서 $c = 1/2$, 둘째 단계에서 제거되는 $(1/9, 2/9)$ 위에서 $c = 1/4$, $(7/9, 8/9)$ 위에서 $c = 3/4$로 두는 식으로 모든 제거 구간 위에서 값을 정하고, 남은 Cantor 집합 위에서는 연속이 되도록 극한으로 확장한다. 삼진법 전개 $x = (0.a_1a_2\cdots)_3$에서 처음 나오는 1 다음 자리를 버리고 그 앞까지의 2를 1로 바꾸어 이진법으로 읽은 값이 $c(x)$라는 공식으로도 쓸 수 있다.

Cantor 함수는 다음 성질을 갖는다.

- c는 연속이고 증가하며 $c(0) = 0$, $c(1) = 1$이다.
- 제거 구간 위에서 상수이고 Cantor 집합의 Lebesgue 측도가 0이므로, 거의 모든 곳(곧 Cantor 집합 밖)에서 $c' = 0$이다.
- 따라서 $\displaystyle\int_0^1 c' = 0 \neq 1 = c(1) - c(0)$.

c는 연속 증가함수이고 거의 모든 곳에서 미분가능하며 도함수가 (영함수로서) 적분가능한데도 미적분 기본정리의 (B)가 실패한다. c의 변화가 측도 0인 Cantor 집합에서 모두 일어났기 때문이다.

역사. Cantor 함수의 구성은 Georg Cantor가 1884년에 발표한 논문에서 비롯되었다. 이 함수는 연속이지만 거의 모든 곳에서 도함수가 0인 비상수 증가함수의 표준 예로, 미적분 기본정리의 두 번째 방향이 연속성과 거의 모든 곳에서의 미분가능성만으로는 성립하지 않음을 보여 주는 반례로 널리 쓰인다.

8.5 절대연속 함수와 미적분 기본정리

정의 8.6 (절대연속) 모든 $\varepsilon > 0$에 대해 $\delta > 0$이 있어, $[a,b]$ 안의 서로소인 유한개의 구간 (a_j, b_j)가 $\sum_j (b_j - a_j) < \delta$를 만족하면 $\sum_j |F(b_j) - F(a_j)| < \varepsilon$일 때, F를 **절대연속**(*absolutely continuous*, AC)이라 한다.

절대연속 함수는 균등연속이고(구간 하나만 쓰면 되는 특수한 경우) 유계변동이다(구간들을 길이 δ 미만으로 유지하면서 분할을 잘게 쪼개면 각 조각의 변동이 ε 미만이 되도록 조절할 수 있고, $[a,b]$를 유한 개의 그런 조각으로 나눌 수 있다). Lipschitz 함수(상수 L이 있어 $|F(x)-F(y)| \le L|x-y|$)는 $\delta = \varepsilon/L$로 두면 절대연속이다. Cantor 함수는 연속이지만 절대연속이 아니다. n단계에서 Cantor 집합을 덮는 2^n개의 구간은 길이의 합이 $(2/3)^n \to 0$이지만, 그 구간들 위에서 c의 값은 합쳐서 1만큼 변하기 때문이다.

정리 8.7 (Lebesgue 적분의 미적분 기본정리) $F:[a,b]\to\mathbb{R}$에 대해 다음은 동치이다.

(1) F는 절대연속이다.

(2) F는 거의 모든 곳에서 미분가능하고 $F' \in L^1$이며, 모든 $x \in [a,b]$에서 $F(x) = F(a) + \displaystyle\int_a^x F'(t)\,dt$이다.

(3) 어떤 $f \in L^1[a,b]$에 대해 $F(x) = F(a) + \displaystyle\int_a^x f$이다.

증명의 개요. (2)⇒(3)은 $f = F'$로 두면 자명하다. (3)⇒(1)은 제5장에서 다룬 적분의 절대연속성($\mu(E)\to 0$이면 $\int_E |f|\,d\mu \to 0$, $f\in L^1$)의 직접적인 결과이다. (3)⇒(2)에서 $F' = f$가 a.e.로 성립한다는 것은 정리 8.1(Lebesgue 미분정리)이다. (1)⇒(2)가 가장 깊은 부분이다. 절대연속 함수는 유계변동이므로 명제 8.5로 두 증가함수의 차로 쓰고, 정리 8.3에 의해 F가 거의 모든 곳에서 미분가능하며 $F' \in L^1$임을 얻는다. 이제 $G(x) = F(x) - F(a) - \int_a^x F'$로 두면 G는 절대연속이고(두 절대연속 함수의 차) $G' = 0$ a.e.이다. 절대연속 함수의 도함수가 거의 모든 곳에서 0이면 상수라는 사실을 Vitali 덮개 논법으로 보이면(단조증가 AC 함수에 적용한 뒤 Jordan 분해로 일반 AC로 확장) $G \equiv G(a) = 0$을 얻고, 이것이 바로 (2)의 등식이다. Cantor 함수는 이 마지막 단계에서 "절대연속"이라는 가정이 왜 필요한지 보여 준다. $c - c(a) - \int_a^x c' = c(x)$ ($x>0$에서)인데 이는 0이 아니다. c가 절대연속이 아니므로 "도함수가 a.e. 0이면 상수" 논법이 적용되지 않기 때문이다. $\square$

8.6 측도의 분해와 Radon–Nikodym 정리

오른쪽 연속인 증가함수 F는 $\mu_F((a,b]) = F(b) - F(a)$로 **Lebesgue–Stieltjes 측도**를 정한다. 앞 절의 결과는 측도의 언어로 다음 구조 정리가 된다.

정리 8.8 (Lebesgue 분해와 Radon–Nikodym) σ-유한 측도 ν, μ에 대해

$$\nu = \nu_{\mathrm{ac}} + \nu_{s}$$

로 유일하게 분해되며, ν_s는 μ와 서로 특이(*mutually singular*, 서로소인 두 집합에 각각 몰려 있음)하고 ν_{ac}는 μ에 대해 **절대연속**이다(곧 $\mu(E)=0 \Rightarrow \nu_{\mathrm{ac}}(E)=0$). 또한

$$\nu_{\mathrm{ac}}(E) = \int_E h \, d\mu$$

를 만족하는 음이 아닌 가측함수 $h = \dfrac{d\nu_{\mathrm{ac}}}{d\mu}$(**Radon–Nikodym 도함수**)가 μ-a.e.로 유일하게 존재한다.

$\mathbb{R}$의 확률분포는 이 정리에 의해 (i) 밀도함수를 갖는 절대연속 부분, (ii) 점질량들로 이루어진 이산 부분, (iii) Cantor 분포처럼 연속이지만 (i), (ii) 어느 쪽도 아닌 특이연속 부분으로 나뉜다. 제20권 제4장에서 "이산형 또는 연속형"이라는 두 분류만으로는 모든 분포를 설명할 수 없다고 하는 이유가 바로 이 세 번째 부분이다. 확률론에서 쓰는 조건부 기댓값 역시 (조건부 확률측도의) Radon–Nikodym 도함수로 정의된다.

역사. Johann Radon(1887–1956)이 1913년에 $\mathbb{R}^n$ 위의 측도에 대해, Otto Nikodym(1887–1974)이 1930년에 일반 σ-유한 측도공간에 대해 이 정리를 증명하였다.

8.7 연습문제와 해설

연습문제 8.9 $F(x)=\sqrt{x}$가 $[0,1]$에서 절대연속인지, Lipschitz인지 판정하라.

풀이. $F(x)=\displaystyle\int_0^x \frac{1}{2\sqrt{t}}\,dt$이고 $\dfrac{1}{2\sqrt{t}} \in L^1[0,1]$이므로($\int_0^1 t^{-1/2}\,dt = 2 < \infty$) 정리 8.7의 (3)에 해당하여 절대연속이다. 그러나 $F(h)/h = h^{-1/2} \to \infty$ $(h \to 0^+)$이므로 Lipschitz가 아니다. 절대연속은 Lipschitz보다 약한 조건이다.

연습문제 8.10 c가 Cantor 함수일 때 $\displaystyle\int_0^1 c(x)\,dx$를 구하라.

풀이. 대칭성 $c(1-x)=1-c(x)$(Cantor 집합과 그 구성이 $x \mapsto 1-x$에 대해 대칭이기 때문)에서

$$\int_0^1 c(x)\,dx = \int_0^1 c(1-x)\,dx = \int_0^1 \bigl(1-c(x)\bigr)\,dx = 1 - \int_0^1 c(x)\,dx$$

이므로 $\displaystyle\int_0^1 c = \frac{1}{2}$이다.

연습문제 8.11 $F(x)=x^2\sin(1/x^2)$ $(x\neq 0)$, $F(0)=0$은 $[-1,1]$의 모든 점에서 미분가능하지만 $F' \notin L^1$임을 설명하라. 이 함수에서 미적분 기본정리의 어느 가정이 실패하는가?

풀이. $x \neq 0$에서

$$F'(x) = 2x\sin\!\left(\frac{1}{x^2}\right) - \frac{2}{x}\cos\!\left(\frac{1}{x^2}\right)$$

이고, $F'(0) = \lim_{h\to 0} F(h)/h = \lim_{h\to 0} h\sin(1/h^2) = 0$이므로 모든 점에서 미분가능하다. 둘째 항의 절댓값을 적분할 때 $t = 1/x^2$로 바꾸면 $dt = -2x^{-3}\,dx$, 곧 $dx = -\tfrac{1}{2}t^{-3/2}\,dt$이고 $2/x = 2t^{1/2}$이므로

$$\int_0^1 \left|\frac{2}{x}\cos(1/x^2)\right| dx = \int_1^\infty 2t^{1/2}\,|\cos t|\cdot\frac{1}{2}t^{-3/2}\,dt = \int_1^\infty \frac{|\cos t|}{t}\,dt$$

꼴이 되는데, 이는 $|\cos t|$의 평균이 $2/\pi > 0$이므로 조화급수처럼 발산한다. 따라서 $F' \notin L^1[-1,1]$이고, F는 원점 근처에서 전변동이 무한하여 유계변동이 아니므로 절대연속도 아니다. 도함수가 모든 점에서 존재한다는 사실만으로는(거의 모든 곳에서의 미분가능성보다 강한 가정인데도) $F' \in L^1$이 보장되지 않으므로 정리 8.7를 적용할 수 없다.

제10권의 범위와 다음 읽기

제10권은 실수의 위상과 상극한, 함수열과 균등수렴, σ-대수와 측도, 가측함수와 Lebesgue 적분, 지배수렴정리와 적분의 계산, 곱측도와 Fubini–Tonelli 정리, L^p 공간, 미분과 적분의 관계(유계변동·절대연속·미분정리)를 다루었다. 제1 5장에서 측도와 적분의 기초를 세운 뒤, 제6 8장에서는 그 적분을 두 변수로 넓히고(곱측도), 적분가능 함수들의 공간에 노름과 완비성을 부여하고(L^p), 미분과 적분이 서로의 역연산이 되는 정확한 조건(절대연속)을 규명하였다. 제1권(무리수와 실수의 완비성), 제8권(미분·적분·급수)에서 다룬 완비성·수렴·오차의 개념이 이 권에서 측도와 적분가능 함수의 언어로 다시 나타나며, 제9권(다변수·벡터해석)의 Riemann 이중적분과 Fubini 정리는 제6장에서 측도론의 틀로 일반화되었다.

Hilbert 공간과 Banach 공간의 일반 이론은 제13권(함수해석학·편미분방정식)에서 이어지며, 그 책의 가장 중요한 예가 이 권 제7장의 L^p 공간이다. 확률론의 측도론적 기초—확률변수를 가측함수로, 기댓값을 적분으로, 조건부 기댓값을 Radon–Nikodym 도함수로 보는 관점—는 제20권(확률론)과 제21권(확률과정)에서 본격적으로 이어진다. 정수론에서 쓰이는 측도론적 논증(예컨대 소수 분포의 밀도 논증)은 제15권과 제28권에서 간접적으로 다시 나타난다.

표준 참고서로 W. Rudin, *Real and Complex Analysis*; G. B. Folland, *Real Analysis*; H. L. Royden and P. Fitzpatrick, *Real Analysis*; E. M. Stein and R. Shakarchi, *Real Analysis*; T. Tao, *An Introduction to Measure Theory*가 있다.

참고 자료의 사용 방식

본문의 설명과 문제는 이 참고서를 위해 새로 작성했다. 아래 목록은 관련 주제를 더 넓은 교재와 대조해 읽기 위한 안내이며, 이 원고 전체가 해당 기관이나 저자의 검토를 받았다는 뜻은 아니다. 개별 정리의 정확한 가정과 기호 약속은 자료마다 다를 수 있으므로, 독자는 다른 자료를 참고할 때마다 그 자료의 정의를 먼저 확인해야 한다.

- MIT OpenCourseWare, 18.100A *Real Analysis*: 실수의 완비성, 수열, 연속, 적분의 엄밀한 기초를 다루는 강의.
- J. K. Hunter, *Measure Theory* 강의노트(PDF): 측도와 Lebesgue 적분, 수렴정리의 증명을 체계적으로 전개한다.
- J. K. Hunter and B. Nachtergaele, *Applied Analysis*: 거리공간에서 L^p 공간, Hilbert 공간으로 이어지는 응용해석을 다룬다.

제 11 권

복소해석

제11권은 복소변수 함수의 미분가능성이 실변수의 경우보다 훨씬 강한 구조를 낳는다는 사실을 다루는 복소해석이다. 제1–2장은 정칙성과 Cauchy–Riemann 방정식, 멱급수와 지수·로그·거듭제곱 함수의 분지를 다루고, 제3–4장은 복소 선적분과 Cauchy 정리, Cauchy 적분공식과 그 결과를 증명한다. 제5–6장은 Laurent 급수와 고립특이점, 유수 정리와 실적분의 계산으로 이를 계산 도구로 바꾼다. 제7–8장은 편각 원리, Rouché 정리, 열린사상 정리와 등각사상, Möbius 변환, Riemann 사상정리로 정칙함수의 대역적 기하를 정리한다.

제 1 장

복소함수와 정칙성: Cauchy–Riemann 방정식

개요 정칙 함수는 열린집합의 모든 점에서 복소수 증분에 대한 미분계수를 갖는 복소함수이다. 이 장은 복소평면의 위상 용어를 정하고 복소미분을 정의한 다음, 복소수 하나에 대한 미분가능성이 실변수 두 개에 대한 미분가능성보다 훨씬 강한 조건임을 보이고 그 조건을 Cauchy–Riemann 방정식으로 정리한다. 이어서 같은 조건을 한 줄로 적는 Wirtinger 미분을 도입하고, 정칙 함수의 실수부와 허수부가 조화함수이며 서로 켤레 관계에 있음을 밝힌다. 선행 지식: 제1권 제10장의 복소수 연산과 극형식, 제9권 제2장의 편미분과 전미분.

1.1 복소평면의 위상

복소수 $z = x + iy$를 $\mathbb{R}^2$의 점 (x, y)와 같이 보면 $|z - w|$는 두 점 사이의 유클리드 거리이다. 따라서 열린집합, 수렴, 연속, 콤팩트성은 제9권 제1장의 정의를 그대로 쓴다. 중심 z_0, 반지름 $r > 0$인 열린 원판은

$$D(z_0, r) = \{ z \in \mathbb{C} : |z - z_0| < r \}$$

로 적는다. 이 권에서 **영역**(*domain*)은 연결된 열린집합을 뜻한다. 복소함수 $f : U \to \mathbb{C}$는 실수부와 허수부로 나누어

$$f = u + iv, \qquad u, v : U \to \mathbb{R}$$

로 쓴다. f가 z_0에서 연속인 것은 u와 v가 모두 (x_0, y_0)에서 연속인 것과 같다.

무한원점 ∞를 더한 집합 $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$를 **확장된 복소평면** 또는 **Riemann 구면**(*Riemann sphere*)이라 한다. 단위구면 $\xi^2 + \eta^2 + \zeta^2 = 1$의 북극 $N = (0, 0, 1)$에서 구면 위의 점 (ξ, η, ζ)를 지나는 직선이 평면 $\zeta = 0$과 만나는 점을 대응시키는 **입체사영**(*stereographic projection*)

$$z = \frac{\xi + i\eta}{1 - \zeta}, \qquad (\xi, \eta, \zeta) = \left(\frac{2x}{|z|^2 + 1},\ \frac{2y}{|z|^2 + 1},\ \frac{|z|^2 - 1}{|z|^2 + 1} \right)$$

은 북극을 뺀 구면과 $\mathbb{C}$ 사이의 일대일 대응이다. 북극을 ∞에 대응시키면 $\hat{\mathbb{C}}$ 전체가 구면과 일대일로 대응하며, $|z| \to \infty$는 구면 위에서 북극으로 접근하는 것에 해당한다.

1.2 복소미분

정의 1.1 (복소미분가능성과 정칙성) 열린집합 $U \subseteq \mathbb{C}$ 위의 함수 $f : U \to \mathbb{C}$와 점 $z_0 \in U$에 대해 극한

$$f'(z_0) = \lim_{h \to 0} \frac{f(z_0 + h) - f(z_0)}{h} \qquad (h \in \mathbb{C}) \tag{1.1}$$

가 존재하면 f가 z_0에서 **복소미분가능**하다고 하고, $f'(z_0)$을 z_0에서의 **복소미분계수**라 한다. U의 모든 점에서 복소미분가능하면 f를 U에서 **정칙**(*holomorphic*)이라 하고, $\mathbb{C}$ 전체에서 정칙인 함수를 **전해석함수**(*entire function*)라 한다.

h가 복소수이므로 $h \to 0$은 평면의 모든 방향에서의 접근을 포함한다. 식 (1.1)은

$$f(z_0+h) = f(z_0) + f'(z_0)\,h + o(|h|) \qquad (h \to 0)$$

와 같은 뜻이므로, 복소미분가능한 함수는 그 점에서 연속이다. 합, 곱, 몫(분모 $\neq 0$), 합성의 미분 공식

$$(f+g)' = f'+g', \qquad (fg)' = f'g + fg', \qquad \left(\frac{f}{g}\right)' = \frac{f'g - fg'}{g^2}, \qquad (g\circ f)' = (g'\circ f)\,f'$$

은 실변수의 경우와 같은 증명으로 성립한다. 상수함수와 z가 전해석함수이므로 다항식은 전해석함수이고, 유리함수는 분모의 영점을 제외한 곳에서 정칙이다.

> **예제 1.2 (켤레는 어디서도 정칙이 아니다)** $f(z) = \bar{z}$의 차분몫은 $\big(\overline{z_0+h} - \overline{z_0}\big)/h = \bar{h}/h$이다. h가 실수이면 $\bar{h}/h = 1$이고 순허수이면 $\bar{h}/h = -1$이다. 접근 방향에 따라 값이 달라 극한이 없으므로 $\bar{z}$는 어느 점에서도 복소미분가능하지 않다. $\bar{z}$는 실변수 함수 $(x,y)\mapsto(x,-y)$로서는 매끄러운 선형사상인데도 그렇다.

1.3 Cauchy–Riemann 방정식

아래에서 u_x, u_y는 편도함수 $\partial u/\partial x$, $\partial u/\partial y$를 뜻한다.

> **정리 1.3 (Cauchy–Riemann 방정식)** $f = u + iv$가 $z_0 = x_0 + iy_0$에서 복소미분가능하면 u, v의 편미분이 (x_0,y_0)에서 존재하고
>
> $$u_x = v_y, \qquad u_y = -v_x \qquad (z_0\text{에서}) \tag{1.2}$$
>
> 이며
>
> $$f'(z_0) = u_x + iv_x = v_y - iu_y \tag{1.3}$$
>
> 이다. 역으로 u, v가 z_0의 근방에서 C^1이고 z_0에서 식 (1.2)을 만족하면 f는 z_0에서 복소미분가능하다.

증명. 식 (1.1)에서 $h = t \in \mathbb{R}$로 두고 $t \to 0$으로 보내면 차분몫은

$$\frac{u(x_0+t,y_0)-u(x_0,y_0)}{t} + i\,\frac{v(x_0+t,y_0)-v(x_0,y_0)}{t}$$

이다. 복소숫값 함수의 극한이 존재하는 것은 실수부와 허수부의 극한이 각각 존재하는 것과 같으므로 u_x, v_x가 존재하고 $f'(z_0) = u_x + iv_x$이다. $h = it$로 두면 같은 이유로 u_y, v_y가 존재하고

$$f'(z_0) = \frac{1}{i}\,(u_y + iv_y) = v_y - iu_y$$

이다. 두 값의 실수부와 허수부를 비교하면 식 (1.2)을 얻는다.

역방향을 보인다. C^1 가정에서 사상 $(x,y)\mapsto(u,v)$는 (x_0,y_0)에서 실변수 미분가능하다(제9권 제2장). $a = u_x$, $b = v_x$로 두면 식 (1.2)에 의해 $u_y = -b$, $v_y = a$이므로 그 미분 행렬은

$$\begin{pmatrix} u_x & u_y \\ v_x & v_y \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

꼴이다. $h = s + it$로 쓰면

$$f(z_0+h) - f(z_0) = (as - bt) + i(bs + at) + o(|h|) = (a+ib)\,h + o(|h|)$$

이다. 곧 이 행렬은 복소수 $a+ib$를 곱하는 사상이고, f는 z_0에서 복소미분가능하며 $f'(z_0) = a+ib$이다. $\square$

참고 (역방향의 가정). 역방향의 증명에서 쓴 것은 (u,v)가 z_0에서 실변수 미분가능하다는 사실뿐이다. 거꾸로 f가 z_0에서 복소미분가능하면 $f(z_0+h) = f(z_0) + f'(z_0)h + o(|h|)$에서 (u,v)는 z_0에서 실변수 미분가능하다. 따라서 f가 z_0에서 복소미분가능할 필요충분조건은 (u,v)가 z_0에서 실변수 미분가능하고 식 (1.2)을 만족하는 것이다. C^1 조건은 이를 보장하는 편리한 충분조건이다. 편미분이 존재하고 식 (1.2)이 성립하는 것만으로는 부족하다(예제 1.5).

기하적으로 복소미분가능성은 실미분 행렬이 "회전과 확대"라는 뜻이다. 위 행렬의 행렬식은 $a^2+b^2 = |f'(z_0)|^2$이다. $f'(z_0) \neq 0$일 때 $f'(z_0) = \rho e^{i\alpha}$ $(\rho > 0)$로 쓰면 이 행렬은 각 α만큼의 회전과 ρ배 확대의 합성이다. 그러므로 $f'(z_0) \neq 0$이면 f는 z_0 근처에서 두 곡선이 이루는 각을 크기와 방향까지 보존한다. 이 성질을 **등각성**(*conformality*)이라 하며 제11권 제8장의 주제이다.

> **예제 1.4** $f(z) = z^2 = (x^2 - y^2) + i(2xy)$에서 $u_x = 2x = v_y$, $u_y = -2y = -v_x$이다. 편미분이 모두 연속이므로 f는 전해석함수이고 $f'(z) = u_x + iv_x = 2x + 2iy = 2z$로 실변수 공식과 같다.
>
> 반면 $g(z) = |z|^2 = x^2 + y^2$는 $u = x^2+y^2$, $v = 0$이므로 $u_x = 2x$, $u_y = 2y$, $v_x = v_y = 0$이다. 식 (1.2)은 $2x = 0$, $2y = 0$이 되어 $z = 0$에서만 성립한다. g는 원점에서만 복소미분가능하고 $(g'(0) = 0)$, 어떤 열린집합에서도 정칙이 아니다.

> **예제 1.5 (방정식만으로는 부족하다)** $f(z) = \bar{z}^2/z$ $(z \neq 0)$, $f(0) = 0$으로 둔다. 실수 x, y에 대해 $f(x) = x$, $f(iy) = iy$이므로 원점에서 $u_x = 1$, $v_x = 0$, $u_y = 0$, $v_y = 1$이고 식 (1.2)이 성립한다. 그러나 차분몫은 $f(h)/h = (\bar{h}/h)^2$이고, h가 실수이면 1, $h = t(1+i)$이면 $\bar{h}/h = -i$에서 -1이다. 따라서 f는 원점에서 복소미분가능하지 않다. u, v가 원점에서 실변수 미분가능하지 않기 때문이다.

흔한 오류. 한 점에서의 복소미분가능성과 정칙성은 다르다. 정칙성은 열린집합 위의 성질이며, 이 권의 강력한 정리들(무한 번 미분가능, 멱급수 전개, Cauchy 정리)은 모두 열린집합에서의 정칙성을 가정한다.

극좌표 형태

$z = re^{i\theta}$ $(r>0)$로 쓰고 u, v를 (r,θ)의 함수로 보면 연쇄법칙에서

$$u_r = u_x\cos\theta + u_y\sin\theta, \qquad u_\theta = -u_x\, r\sin\theta + u_y\, r\cos\theta$$

이고 v도 같다. 여기에 식 (1.2)을 넣으면 Cauchy–Riemann 방정식의 극좌표 형태

$$r\,u_r = v_\theta, \qquad r\,v_r = -u_\theta, \qquad f'(z) = e^{-i\theta}\,(u_r + iv_r) \tag{1.4}$$

을 얻는다. 마지막 식은 $u_r + iv_r = (u_x + iv_x)\cos\theta + (u_y + iv_y)\sin\theta = f'(z)\,e^{i\theta}$에서 나온다.

역사. 식 (1.2)은 d'Alembert의 1752년 유체역학 연구에 처음 나타났다. Cauchy는 1814년 논문에서 이 방정식을 복소 적분 이론에 사용하였고, Riemann은 1851년 학위논문에서 이 방정식을 복소함수론의 출발점으로 삼았다.

1.4 Wirtinger 미분

$z = x + iy$, $\bar{z} = x - iy$를 독립변수처럼 다루는 **Wirtinger 미분**은

$$\frac{\partial}{\partial z} = \frac{1}{2}\left(\frac{\partial}{\partial x} - i\,\frac{\partial}{\partial y}\right), \qquad \frac{\partial}{\partial \bar{z}} = \frac{1}{2}\left(\frac{\partial}{\partial x} + i\,\frac{\partial}{\partial y}\right) \tag{1.5}$$

로 정의하는 미분 연산자이다. 줄 안에서는 ∂_z, $\partial_{\bar{z}}$로 적는다. 계수는 $\partial_z z = 1$, $\partial_z \bar{z} = 0$, $\partial_{\bar{z}} z = 0$, $\partial_{\bar{z}} \bar{z} = 1$이 되도록 정한 것이다. $f = u + iv$에 적용하면

$$\frac{\partial f}{\partial \bar{z}} = \frac{1}{2}\big[(u_x - v_y) + i\,(u_y + v_x)\big], \qquad \frac{\partial f}{\partial z} = \frac{1}{2}\big[(u_x + v_y) + i\,(v_x - u_y)\big]$$

이다. 그러므로 Cauchy–Riemann 방정식은 한 줄

$$\frac{\partial f}{\partial \bar{z}} = 0 \tag{1.6}$$

이 되고, 이때 $\partial f/\partial z = u_x + i v_x = f'$이다. 이런 뜻에서 정칙 함수는 "$\bar{z}$에 의존하지 않는 함수"이다. 예를 들어 $|z|^2 = z\bar{z}$는 $\partial_{\bar{z}}\,|z|^2 = z$이므로 $z = 0$에서만 방정식을 만족하며, 이는 예제 1.4의 결론과 같다.

이 기호는 실수 형식의 계산을 자주 단순하게 만든다. 두 연산자를 곱하면

$$4\,\frac{\partial}{\partial z}\frac{\partial}{\partial \bar{z}} = \left(\frac{\partial}{\partial x} - i\,\frac{\partial}{\partial y}\right)\left(\frac{\partial}{\partial x} + i\,\frac{\partial}{\partial y}\right) = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}$$

이므로 C^2 함수에 대해 $\nabla^2 = 4\,\partial_z \partial_{\bar{z}}$이다.

핵심 수식

Cauchy–Riemann 방정식:	$u_x = v_y, \quad u_y = -v_x,$
미분계수:	$f' = u_x + i v_x = v_y - i u_y,$
Wirtinger 형태:	$\dfrac{\partial f}{\partial \bar{z}} = 0, \quad f' = \dfrac{\partial f}{\partial z}.$

1.5 조화함수와 켤레조화함수

정의 1.6 (조화함수) 열린집합 $U \subseteq \mathbb{R}^2$ 위의 C^2 실함수 u가 Laplace 방정식

$$\nabla^2 u = u_{xx} + u_{yy} = 0$$

을 만족하면 u를 **조화함수**(*harmonic function*)라 한다.

$f = u + iv$가 정칙이고 u, v가 C^2이면 Cauchy–Riemann 방정식과 혼합 편미분의 대칭성에서

$$u_{xx} + u_{yy} = (v_y)_x + (-v_x)_y = v_{yx} - v_{xy} = 0$$

이므로 u는 조화함수이고, 같은 이유로 v도 조화함수이다. C^2 가정은 실제로는 필요 없다. 정칙 함수가 무한 번 미분가능하다는 사실을 제11권 제4장에서 보인다. $u+iv$가 정칙이 되게 하는 조화함수 v를 u의 **켤레조화함수**(*harmonic conjugate*)라 한다. 이 관계는 대칭이 아니다. $-i(u+iv) = v - iu$가 정칙이므로 v의 켤레조화함수는 $-u$이다.

명제 1.7 (켤레조화함수의 존재) 단순연결 영역(특히 원판이나 볼록 영역)에서 조화함수 u는 켤레조화함수를 가지며, 그것은 상수 차이를 제외하고 유일하다.

증명. v가 만족해야 할 조건은 식 (1.2)에서 $\nabla v = (-u_y,\, u_x)$이다. 벡터장 $(P, Q) = (-u_y, u_x)$는 C^1이고 그 회전은

$$Q_x - P_y = u_{xx} + u_{yy} = 0$$

이므로, 단순연결 영역에서는 제9권 제6장의 Poincaré 보조정리(단순연결 영역에 대한 형태)에 의해 $\nabla v = (P, Q)$인 퍼텐셜 v가 존재한다. 이 v는 C^2이고 u, v가 식 (1.2)을 만족하므로 정리 1.3에 의해 $u + iv$는 정칙이다. 켤레조화함수 v_1, v_2가 있으면 $\nabla(v_1 - v_2) = 0$이고 영역이 연결되어 있으므로 $v_1 - v_2$는 상수이다. $\square$

예제 1.8 $u = x^3 - 3xy^2$은 $u_{xx} + u_{yy} = 6x - 6x = 0$이므로 조화함수이다. $v_y = u_x = 3x^2 - 3y^2$에서 $v = 3x^2 y - y^3 + g(x)$이고, $v_x = 6xy + g'(x) = -u_y = 6xy$에서 $g' = 0$이다. 따라서 $v = 3x^2 y - y^3 + c$ (c는 실수 상수)이고

$$f = u + iv = (x + iy)^3 + ic = z^3 + ic$$

이다.

구멍이 있는 영역에서는 켤레조화함수가 없을 수 있다. $u = \ln|z|$는 $\mathbb{C} \setminus \{0\}$에서 조화함수이지만, 그 켤레조화함수는 국소적으로 편각 $\arg z$이고 편각은 $\mathbb{C} \setminus \{0\}$ 전체에서 연속인 함수로 정의되지 않는다(제11권 제2장).

조화함수의 등위곡선 $u = c$와 켤레의 등위곡선 $v = c'$은

$$\nabla u \cdot \nabla v = u_x v_x + u_y v_y = u_x(-u_y) + u_y u_x = 0$$

이므로 $f' \neq 0$인 곳, 곧 두 기울기 벡터가 0이 아닌 곳에서 서로 직교한다. 2차원 정전기에서 등전위선과 전기력선, 이상유체의 흐름에서 속도 퍼텐셜의 등위선과 유선이 이 관계에 있다.

1.6 연습문제와 해설

연습문제 1.9 $f(z) = e^x(\cos y + i \sin y)$가 전해석함수임을 Cauchy–Riemann 방정식으로 확인하고 f'을 구하라.

풀이. $u = e^x \cos y$, $v = e^x \sin y$이다. $u_x = e^x \cos y = v_y$, $u_y = -e^x \sin y = -v_x$이고 편미분이 모두 연속이므로 정리 1.3에 의해 모든 점에서 복소미분가능하다. 곧 f는 전해석함수이고 $f' = u_x + iv_x = e^x \cos y + ie^x \sin y = f$이다. 제11권 제2장에서 이 함수를 e^z으로 정의한다.

연습문제 1.10 $f(z) = x^2 + iy^2$은 어디서 복소미분가능한가? 어디서 정칙인가?

풀이. $u = x^2$, $v = y^2$에서 $u_x = 2x$, $v_y = 2y$, $u_y = 0 = -v_x$이므로 식 (1.2)은 직선 $y = x$ 위에서만 성립한다. 편미분이 연속이므로 f는 그 직선의 점에서 복소미분가능하고, 그 밖의 점에서는 복소미분가능하지 않다. 직선은 내부가 없으므로 f가 정칙인 열린집합은 없다.

연습문제 1.11 영역에서 정칙인 f가 실숫값만 가지면 상수임을 보여라.

풀이. $v = 0$이므로 식 (1.2)에서 $u_x = v_y = 0$, $u_y = -v_x = 0$이다. 영역이 연결되어 있으므로 u는 상수이다(제9권 제2장).

같은 논증으로 $|f|$가 상수인 정칙 함수도 상수이다. $|f|^2 = u^2 + v^2 = c$를 x, y로 미분하고 식 (1.2)로 $v_x = -u_y$, $v_y = u_x$를 넣으면

$$u u_x - v u_y = 0, \qquad v u_x + u u_y = 0$$

이다. $c = 0$이면 $f = 0$이다. $c \neq 0$이면 이 연립방정식의 계수 행렬식이 $u^2 + v^2 = c \neq 0$이므로 $u_x = u_y = 0$이고, 따라서 $f' = u_x - i u_y = 0$이다. 그러면 u, v의 편미분이 모두 0이므로 f는 상수이다.

연습문제 1.12 $u(x, y) = e^{-y}\cos x$의 켤레조화함수를 구하고 $f = u + iv$를 z로 나타내어라.

풀이. $v_y = u_x = -e^{-y}\sin x$에서 $v = e^{-y}\sin x + g(x)$이고, $v_x = e^{-y}\cos x + g'(x) = -u_y = e^{-y}\cos x$에서 $g' = 0$이다. 따라서 $v = e^{-y}\sin x + c$이고

$$f = e^{-y}(\cos x + i \sin x) + ic = e^{-y+ix} + ic = e^{iz} + ic$$

이다. 여기서 c는 실수 상수이다.

참고 (다음 장과의 연결). 제11권 제2장에서는 정칙 함수의 대표인 지수함수, 삼각함수, 로그함수를 멱급수로 정의하고, 로그와 거듭제곱에서 생기는 분지의 문제를 다룬다.

제 2 장

멱급수와 초등함수: 지수, 로그, 거듭제곱

개요 멱급수는 $\sum a_n (z-z_0)^n$ 꼴의 함수항 급수이며, 수렴원판 안에서 정칙 함수를 정의한다. 이 장은 수렴반지름에 관한 Cauchy–Hadamard 정리와 항별 미분 정리를 증명하고, 멱급수로 지수함수와 삼각함수를 정의한 다음 그 역함수로서 로그와 거듭제곱을 정의한다. 로그와 거듭제곱은 값이 여러 개인 대응이므로 값을 하나로 정하는 방법, 곧 분지의 선택이 핵심이다. 끝으로 해석적 함수의 유일성을 말하는 일치의 원리를 증명한다. 선행 지식: 제11권 제1장의 복소미분, 제8권 제6장의 급수 판정법, 제10권 제2장의 균등수렴.

2.1 멱급수와 수렴반지름

정의 2.1 (멱급수) 복소수열 $(a_n)_{n\ge 0}$과 점 $z_0 \in \mathbb{C}$에 대해 함수항 급수

$$\sum_{n\ge 0} a_n (z-z_0)^n$$

을 z_0을 중심으로 하는 **멱급수**(*power series*)라 한다.

정리 2.2 (Cauchy–Hadamard) 멱급수 $\sum_{n\ge 0} a_n (z-z_0)^n$에 대해

$$R = \frac{1}{\limsup_{n\to\infty} |a_n|^{1/n}} \in [0,\infty] \tag{2.1}$$

로 두면(단 $1/0=\infty$, $1/\infty=0$으로 읽는다) 급수는 $|z-z_0|<R$에서 절대수렴하고 $|z-z_0|>R$에서 발산한다. $r<R$이면 닫힌 원판 $|z-z_0|\le r$에서 균등수렴한다.

증명. $|z-z_0|\le r<R$이라 하고 $r<\rho<R$인 ρ를 잡는다. $\limsup |a_n|^{1/n} = 1/R < 1/\rho$이므로 충분히 큰 n에서 $|a_n|^{1/n} < 1/\rho$이고

$$|a_n (z-z_0)^n| \le \left(\frac{r}{\rho}\right)^n$$

이다. $\sum (r/\rho)^n$이 수렴하므로 Weierstrass M-판정법(제10권 제2장)에 의해 급수는 $|z-z_0|\le r$에서 절대수렴하고 균등수렴한다. $|z-z_0|<R$인 점마다 $r=|z-z_0|$으로 두면 그 점에서의 절대수렴을 얻는다.

$|z-z_0|>R$이면 $\limsup |a_n|^{1/n} = 1/R > 1/|z-z_0|$이므로 무한히 많은 n에서 $|a_n|^{1/n} > 1/|z-z_0|$, 곧 $|a_n(z-z_0)^n|>1$이다. 일반항이 0으로 가지 않으므로 급수는 발산한다. $\square$

식 (2.1)의 R을 멱급수의 **수렴반지름**(*radius of convergence*), 원판 $|z-z_0|<R$을 **수렴원판**이라 한다. 충분히 큰 n에서 $a_n\neq 0$이고 극한 $\lim |a_n/a_{n+1}|$이 존재하면(값 ∞ 포함) 그 값이 R과 같다. 비의 극한이 존재하면 $\lim |a_n|^{1/n}$도 존재하고 두 극한이 같기 때문이다.

수렴원 위($|z-z_0|=R$)에서의 행동은 급수마다 다르다. 다음 세 급수는 모두 $R=1$이다. $\sum z^n$은 일반항의 절댓값이 1이므로 원 위의 모든 점에서 발산한다. $\sum z^n/n^2$은 $\sum 1/n^2$이 수렴하므로 원 위의 모든 점에서 절대수렴한다. $\sum z^n/n$은 $z=1$에서 조화급수가 되어 발산하지만, $|z|=1$, $z\neq 1$이면 부분합 $|z+\cdots+z^n|\le 2/|1-z|$가 유계이고 $1/n$이 0으로 단조감소하므로 Dirichlet 판정법에 의해 수렴한다. 곧 원 위에서 $z=1$에서만 발산한다.

정리 2.3 (항별 미분) 수렴반지름이 $R>0$인 멱급수 $f(z)=\sum_{n\ge 0} a_n (z-z_0)^n$은 $|z-z_0|<R$에서 정칙이고

$$f'(z)=\sum_{n\ge 1} n a_n (z-z_0)^{n-1} \tag{2.2}$$

이다. 이 급수의 수렴반지름도 R이다. 따라서 f는 무한 번 복소미분가능하고

$$a_n=\frac{f^{(n)}(z_0)}{n!} \tag{2.3}$$

이다.

증명. $n^{1/n}\to 1$이므로 $\limsup (n|a_n|)^{1/n}=\limsup |a_n|^{1/n}$이다. $\sum n a_n (z-z_0)^{n-1}$과 $\sum n a_n (z-z_0)^n$은 같은 점에서 수렴하므로 식 (2.2)의 급수 $g(z)$의 수렴반지름은 R이다. 같은 이유로 $\sum n(n-1)a_n(z-z_0)^{n-2}$의 수렴반지름도 R이다.

$z_0=0$이라 해도 일반성을 잃지 않는다. 먼저 $|z|,|w|\le r$이고 $n\ge 2$일 때

$$\left|\frac{w^n-z^n}{w-z}-nz^{n-1}\right|\le \frac{n(n-1)}{2}\,r^{n-2}\,|w-z| \qquad (w\neq z) \tag{2.4}$$

임을 보인다. $w^k-z^k=(w-z)\sum_{j=0}^{k-1} w^j z^{k-1-j}$에서 $\left|w^k-z^k\right|\le k r^{k-1}|w-z|$이다. 그러므로

$$\frac{w^n-z^n}{w-z}-nz^{n-1}=\sum_{k=0}^{n-1}\left(w^k z^{n-1-k}-z^{n-1}\right)=\sum_{k=1}^{n-1} z^{n-1-k}\,(w^k-z^k)$$

의 절댓값은 $\sum_{k=1}^{n-1} r^{n-1-k}\cdot k r^{k-1}|w-z|=\frac{n(n-1)}{2}r^{n-2}|w-z|$ 이하이다.

이제 $|z|<R$인 z를 고정하고 $|z|<r<R$인 r을 잡는다. $|w|\le r$, $w\neq z$이면 식 (2.4)에서

$$\left|\frac{f(w)-f(z)}{w-z}-g(z)\right|=\left|\sum_{n\ge 2} a_n\left(\frac{w^n-z^n}{w-z}-nz^{n-1}\right)\right|\le |w-z|\sum_{n\ge 2}\frac{n(n-1)}{2}\,|a_n|\,r^{n-2}$$

이다. 오른쪽 급수는 $r<R$이므로 수렴하고 w와 무관하다. $w\to z$로 보내면 $f'(z)=g(z)$를 얻는다.

같은 논증을 f', f'', ...에 되풀이하면 f는 무한 번 미분가능하고

$$f^{(k)}(z)=\sum_{n\ge k} n(n-1)\cdots(n-k+1)\,a_n (z-z_0)^{n-k}$$

이다. $z=z_0$을 넣으면 $f^{(k)}(z_0)=k!\,a_k$이다. $\square$

식 (2.3)에 의해 멱급수의 계수는 함수가 결정한다. 같은 중심의 두 멱급수가 z_0의 어떤 근방에서 같은 함수를 나타내면 계수가 모두 같다.

역사. 식 (2.1)은 Cauchy가 1821년 *Cours d'analyse*에서 제시하였으나 널리 알려지지 않았고, Hadamard가 1888년에 다시 발견하여 발표하였다.

2.2 지수함수와 삼각함수

정의 2.4 (지수함수와 삼각함수) 복소수 z에 대해 **지수함수**, **코사인**, **사인**을 멱급수

$$e^z = \sum_{n\ge 0} \frac{z^n}{n!}, \qquad \cos z = \sum_{n\ge 0} \frac{(-1)^n z^{2n}}{(2n)!}, \qquad \sin z = \sum_{n\ge 0} \frac{(-1)^n z^{2n+1}}{(2n+1)!} \tag{2.5}$$

로 정의한다. e^z은 $\exp z$로도 적는다.

세 급수는 모두 수렴반지름이 ∞이므로($a_n = 1/n!$에서 $|a_n/a_{n+1}| = n+1 \to \infty$) 정리 2.3에 의해 전해석함수이다. z가 실수이면 실변수의 지수함수, 코사인, 사인과 일치한다. 항별 미분으로

$$(e^z)' = e^z, \qquad (\sin z)' = \cos z, \qquad (\cos z)' = -\sin z$$

이다. 절대수렴하는 두 급수의 곱(Cauchy 곱)과 이항정리에서

$$e^z e^w = \sum_{n\ge 0}\sum_{k=0}^{n} \frac{z^k}{k!}\,\frac{w^{n-k}}{(n-k)!} = \sum_{n\ge 0} \frac{(z+w)^n}{n!} = e^{z+w}$$

이다. 식 (2.5)에서 e^{iz}의 급수를 짝수 차와 홀수 차로 나누면 모든 복소수 z에 대해 $e^{iz} = \cos z + i\sin z$이다. 특히 $z = y$가 실수이면 오른쪽의 두 항이 실수부와 허수부가 되어 **Euler 공식**

$$e^{iy} = \cos y + i \sin y \qquad (y \in \mathbb{R}) \tag{2.6}$$

을 얻는다. 따라서 $e^{x+iy} = e^x e^{iy} = e^x(\cos y + i\sin y)$이고, 이는 제11권 제1장의 연습문제 1.9에서 다룬 함수이다. 이로부터 다음 성질이 나온다.

- $|e^z| = e^{\operatorname{Re} z}$이고 $e^z \neq 0$이다. 앞의 식은 $|e^{iy}| = 1$에서, 뒤의 식은 $e^z e^{-z} = 1$에서 나온다.
- $e^z = 1 \iff z \in 2\pi i\mathbb{Z}$. $e^{x+iy} = 1$이면 절댓값에서 $x = 0$이고 $\cos y = 1$, $\sin y = 0$에서 $y \in 2\pi\mathbb{Z}$이기 때문이다. 따라서 e^z은 주기 $2\pi i$를 갖고, $e^z = e^w$은 $z - w \in 2\pi i\mathbb{Z}$와 동치이다.
- $e^{iz} = \cos z + i\sin z$와 $e^{-iz} = \cos z - i\sin z$를 더하고 빼면

$$\cos z = \frac{e^{iz} + e^{-iz}}{2}, \qquad \sin z = \frac{e^{iz} - e^{-iz}}{2i} \tag{2.7}$$

이다.

쌍곡선함수를 $\cosh z = (e^z + e^{-z})/2$, $\sinh z = (e^z - e^{-z})/2$로 정의하면 식 (2.7)에서 $\cos(iy) = \cosh y$, $\sin(iy) = i\sinh y$이다. 덧셈정리 $\sin(z+w) = \sin z\cos w + \cos z \sin w$는 식 (2.7)과 지수법칙에서 나오며, 이를 $z = x$, $w = iy$에 쓰면

$$\sin(x+iy) = \sin x \cosh y + i\cos x \sinh y, \qquad |\sin z|^2 = \sin^2 x + \sinh^2 y \tag{2.8}$$

이다. 그러므로 $\sin z$의 영점은 실수 $z = n\pi$ $(n \in \mathbb{Z})$뿐이다.

흔한 오류. 실수에서의 성질 $|\sin x| \le 1$은 복소수에서 성립하지 않는다. $\sin(iy) = i\sinh y$이므로 $y \to \pm\infty$일 때 $|\sin(iy)| \to \infty$이다. 실제로 제11권 제4장의 Liouville 정리에 의해 유계인 전해석함수는 상수뿐이므로, 상수가 아닌 $\sin z$는 $\mathbb{C}$에서 유계일 수 없다.

2.3 복소로그와 분지

표기. 이 권에서 $\ln$은 양의 실수의 자연로그를, $\log$는 아래에서 정의하는 복소로그를 뜻한다.

w가 $e^{w} = z$를 만족하면 w를 z의 **로그**라 한다. $e^{w} \neq 0$이므로 0의 로그는 없다. $z \neq 0$을 극형식 $z = re^{i\theta}$로 쓰고 $w = s + it$로 두면 $e^{s}e^{it} = re^{i\theta}$에서 해는

$$w = \ln r + i(\theta + 2\pi k) \qquad (k \in \mathbb{Z}) \tag{2.9}$$

로 무한히 많다. 편각 $\arg z$가 2π의 정수배만큼 결정되지 않기 때문이다. 이 값들의 집합을 $\log z$로 적는다. 영역 U에서 연속이고 모든 $z \in U$에서 $e^{L(z)} = z$인 함수 L을 U 위의 로그의 **분지**(*branch*)라 한다.

> **정의 2.5 (주편각과 주로그)** $z \neq 0$에 대해 $-\pi < \operatorname{Arg} z \le \pi$인 편각 $\operatorname{Arg} z$를 **주편각**이라 하고, **주로그**(*principal logarithm*)를
>
> $$\operatorname{Log} z = \ln|z| + i \operatorname{Arg} z \qquad (z \neq 0)$$
>
> 로 정의한다.

예를 들어 $\operatorname{Log}(-1) = i\pi$, $\operatorname{Log} i = i\pi/2$, $\operatorname{Log}(-i) = -i\pi/2$이다. Log는 음의 실수축의 모든 점에서 불연속이다. -1에 위쪽에서 접근하면 허수부가 π로, 아래쪽에서 접근하면 $-\pi$로 간다. 반직선 $(-\infty, 0]$을 **분지절단**(*branch cut*)이라 한다. 절단을 제거한 영역 $\mathbb{C} \setminus (-\infty, 0]$에서 Log는 연속이고, 지수함수를 띠 $-\pi < \operatorname{Im} w < \pi$로 제한한 것의 역함수이다. $w = \operatorname{Log} z$, $w' = \operatorname{Log} z'$으로 두면 $z' \to z$일 때 $w' \to w$이므로

$$\frac{\operatorname{Log} z' - \operatorname{Log} z}{z' - z} = \left(\frac{e^{w'} - e^{w}}{w' - w}\right)^{-1} \longrightarrow \frac{1}{e^{w}} = \frac{1}{z}$$

이다. 곧 Log는 $\mathbb{C} \setminus (-\infty, 0]$에서 정칙이고

$$(\operatorname{Log} z)' = \frac{1}{z} \tag{2.10}$$

이다. $u = \ln r$, $v = \theta$가 제11권 제1장의 극좌표 Cauchy–Riemann 방정식 $ru_r = v_\theta$, $rv_r = -u_\theta$를 만족하고 $f' = e^{-i\theta}(u_r + iv_r) = 1/z$라는 계산으로도 확인된다.

> **예제 2.6 ($\operatorname{Log}(1+z)$의 멱급수)** $|z| < 1$이면 $1 + z$의 실수부가 양수이므로 $\operatorname{Log}(1+z)$는 단위원판에서 정칙이고 도함수는 $1/(1+z) = \sum_{n \ge 0} (-1)^n z^n$이다. 멱급수 $S(z) = \sum_{n \ge 1} (-1)^{n-1} z^n / n$은 수렴반지름이 1이고 정리 2.3에 의해 $S'(z) = 1/(1+z)$이다. 두 함수는 도함수가 같고 $z = 0$에서 값이 모두 0이므로
>
> $$\operatorname{Log}(1+z) = z - \frac{z^2}{2} + \frac{z^3}{3} - \cdots \qquad (|z| < 1)$$
>
> 이다. 여기서 영역에서 도함수가 0인 정칙 함수 $h = u + iv$가 상수라는 사실을 썼다. $h' = u_x + iv_x = v_y - iu_y = 0$이면 u, v의 편미분이 모두 0이기 때문이다.

흔한 오류. 양의 실수에 대한 로그의 법칙 $\ln(ab) = \ln a + \ln b$를 주로그로 옮긴 식 $\operatorname{Log}(zw) = \operatorname{Log} z + \operatorname{Log} w$는 일반적으로 성립하지 않는다. $z = w = -1$이면 $\operatorname{Log}(zw) = \operatorname{Log} 1 = 0$이지만

$\operatorname{Log} z + \operatorname{Log} w = 2\pi i$ 이다. 성립하는 것은 $2\pi i$ 의 정수배 차이를 허용한 "집합으로서의" 등식 $\log(zw) = \log z + \log w$ 이다.

연속인 로그의 분지가 존재하려면 영역 안의 닫힌 곡선이 원점을 감지 않아야 한다. 정확히는 0 을 포함하지 않는 단순연결 영역 U 에서 정칙인 로그 분지가 존재한다. 제11권 제3장의 Cauchy 정리에 의해 U 안에서 $\int_{z_0}^{z} \mathrm{d}\zeta/\zeta$ 가 경로와 무관해지기 때문이다. 실제로 $e^{w_0} = z_0$ 인 w_0 을 골라

$$L(z) = w_0 + \int_{z_0}^{z} \frac{\mathrm{d}\zeta}{\zeta}$$

로 두면 $L'(z) = 1/z$ 이고 $\left(z e^{-L(z)}\right)' = e^{-L(z)} - z L'(z) e^{-L(z)} = 0$ 이므로 $z e^{-L(z)}$ 는 상수 $z_0 e^{-w_0} = 1$ 이다. 곧 $e^{L(z)} = z$ 이다.

반면 $\mathbb{C} \setminus \{0\}$ 전체에서는 연속인 분지가 존재하지 않는다. 그런 분지 L 이 있다면 $t \mapsto L(e^{it}) - it$ 는 $[0, 2\pi]$ 에서 연속이고 값이 $2\pi i\mathbb{Z}$ 에 속하므로 상수이다. 그러나 $t = 0$ 과 $t = 2\pi$ 에서 $L(e^{it})$ 의 값은 같고 it 는 $2\pi i$ 만큼 다르므로 모순이다.

2.4 복소 거듭제곱

$z \neq 0$ 과 $c \in \mathbb{C}$ 에 대해 **복소 거듭제곱**을 $z^c = e^{c \log z}$ 로 정의한다. $\log z$ 가 여러 값을 가지므로 z^c 의 값은

$$e^{c(\operatorname{Log} z + 2\pi i k)} = e^{c \operatorname{Log} z}\, e^{2\pi i k c} \qquad (k \in \mathbb{Z}) \tag{2.11}$$

이다. 값의 개수는 $e^{2\pi i k c}$ $(k \in \mathbb{Z})$ 가운데 서로 다른 것의 개수와 같다.

- c 가 정수이면 $e^{2\pi i k c} = 1$ 이라 값이 하나이고, 보통의 거듭제곱과 일치한다.
- $c = p/q$ $(q \geq 1$, 기약분수$)$ 이면 값이 정확히 q 개이다. $e^{2\pi i k p/q}$ 가 k 를 q 로 나눈 나머지에만 의존하고 $k = 0, 1, \ldots, q-1$ 에서 서로 다르기 때문이다. 예를 들어 $z^{1/2}$ 은 두 값 $\pm e^{\frac{1}{2}\operatorname{Log} z}$ 을 갖는다.
- c 가 무리수이거나 실수가 아니면 값이 무한히 많다. c 가 무리수이면 $e^{2\pi i k c}$ 가 모두 다르고, $\operatorname{Im} c \neq 0$ 이면 절댓값 $\left|e^{2\pi i k c}\right| = e^{-2\pi k \operatorname{Im} c}$ 가 모두 다르다.

> **예제 2.7** i 의 로그는 $i(\pi/2 + 2\pi k)$ 이므로
>
> $$i^i = e^{i \log i} = e^{i \cdot i(\pi/2 + 2\pi k)} = e^{-\pi/2 - 2\pi k} \qquad (k \in \mathbb{Z})$$
>
> 이다. 모든 값이 양의 실수이고 주값$(k = 0)$은 $e^{-\pi/2} \approx 0.2079$ 이다.

주분지 $z^c = e^{c \operatorname{Log} z}$ 은 $\mathbb{C} \setminus (-\infty, 0]$ 에서 정칙이고, 연쇄법칙과 식 (2.10)에서

$$(z^c)' = \frac{c}{z}\, e^{c \operatorname{Log} z} = c z^{c-1}$$

이다. 양변의 거듭제곱은 같은 주분지이다. 한 분지 안에서는 $z^a z^b = z^{a+b}$ 가 성립한다. 그러나 지수법칙 $(zw)^c = z^c w^c$, $(z^a)^b = z^{ab}$ 는 일반적으로 성립하지 않는다. 예를 들어 주분지에서 $\left((-1)^2\right)^{1/2} = 1^{1/2} = 1$ 이지만 $(-1)^{2\cdot 1/2} = -1$ 이다. 또 $z = w = -1$, $c = 1/2$ 이면 $(zw)^{1/2} = 1$ 이지만 $z^{1/2} w^{1/2} = i \cdot i = -1$ 이다.

2.5 해석적 함수와 일치의 원리

열린집합 U의 각 점 z_0에 대해 z_0을 중심으로 하는 어떤 원판에서 f가 수렴하는 멱급수 $\sum a_n (z-z_0)^n$과 일치하면 f를 U에서 **해석적**(*analytic*)이라 한다. 정리 2.3에 의해 해석적 함수는 정칙이고 무한 번 미분가능하다. 역으로 정칙 함수가 해석적임을 제11권 제4장에서 보인다. 여기서는 해석적 함수의 유일성에 관한 결과를 미리 적어 둔다.

> **정리 2.8 (일치의 원리)** 영역 U에서 해석적인 f의 영점들이 U 안에 집적점을 가지면 U에서 $f \equiv 0$이다. 따라서 U에서 해석적인 두 함수가 U 안에 집적점을 갖는 집합 위에서 같으면 U 전체에서 같다.

증명. 영점들의 집적점을 $z_0 \in U$라 하고, z_0 근방에서 $f(z) = \sum a_n (z-z_0)^n$이라 하자. 먼저 계수가 모두 0임을 보인다. 0이 아닌 계수가 있다고 하고 그 가운데 첫 번째를 a_m이라 하면

$$f(z) = (z-z_0)^m g(z), \qquad g(z) = \sum_{n \ge m} a_n (z-z_0)^{n-m}, \qquad g(z_0) = a_m \neq 0$$

이다. g는 같은 수렴반지름을 갖는 멱급수이므로 연속이고, 따라서 z_0의 어떤 근방에서 $g \neq 0$이다. 그 근방에서 f의 영점은 z_0뿐이므로 z_0이 영점들의 집적점이라는 가정에 어긋난다. 그러므로 계수가 모두 0이고 f는 z_0의 근방에서 0이다.

이제 $A = \{ z \in U : \text{모든 } n \ge 0 \text{에 대해 } f^{(n)}(z) = 0 \}$으로 둔다. 위에서 $z_0 \in A$이므로 A는 공집합이 아니다. 각 $f^{(n)}$이 연속이므로 A는 U에서 닫혀 있다. $z_1 \in A$이면 식 (2.3)에 의해 z_1을 중심으로 하는 멱급수의 계수가 모두 0이므로 f가 z_1의 근방에서 0이고, 그 근방은 A에 포함된다. 곧 A는 열려 있다. U가 연결되어 있으므로 $A = U$이고 $f \equiv 0$이다.

둘째 주장은 첫째 주장을 두 함수의 차에 적용한 것이다. $\square$

이 정리 때문에 실수축에서 성립하는 항등식은 복소평면으로 그대로 확장된다. 예를 들어 $\sin^2 z + \cos^2 z = 1$은 실수에서 성립하고 양변이 전해석함수이므로 모든 복소수에서 성립한다. 반면 실변수 C^∞ 함수에는 이런 일치의 원리가 없다. 제8권 제6장에서 다루는 함수 e^{-1/x^2}은 $x=0$에서 값과 모든 차수의 미분계수가 0이 되도록 확장된다. 그러므로 $x>0$에서 e^{-1/x^2}, $x \le 0$에서 0인 함수는 C^∞이고 반직선 $(-\infty, 0]$에서 0이지만 항등적으로 0은 아니다.

> **예제 2.9 (집적점은 영역 안에 있어야 한다)** $f(z) = \sin(1/z)$는 영역 $\mathbb{C} \setminus \{0\}$에서 정칙이고 영점 $z = 1/(n\pi)$ $(n = \pm 1, \pm 2, \dots)$은 0으로 모인다. 그러나 집적점 0이 영역에 속하지 않으므로 정리 2.8는 적용되지 않으며, 실제로 f는 항등적으로 0이 아니다.

2.6 연습문제와 해설

> **연습문제 2.10** $\displaystyle\sum_{n \ge 1} \frac{n!}{n^n} z^n$의 수렴반지름을 구하라.

풀이. $a_n = n!/n^n$으로 두면

$$\frac{a_{n+1}}{a_n} = \frac{(n+1)\,n^n}{(n+1)^{n+1}} = \left(\frac{n}{n+1}\right)^n = \left(1 + \frac{1}{n}\right)^{-n} \longrightarrow e^{-1}$$

이므로 $R = \lim |a_n/a_{n+1}| = e$이다. 비의 극한이 존재하면 $\lim |a_n|^{1/n}$도 같은 값이므로 식 (2.1)과 일치한다.

연습문제 2.11 $\cos z = 2$를 풀어라.

풀이. $w = e^{iz}$으로 두면 식 (2.7)에서 $w + 1/w = 4$, 곧 $w^2 - 4w + 1 = 0$이고 $w = 2 \pm \sqrt{3}$이다. 두 근이 모두 양의 실수이므로 식 (2.9)에서 $iz = \ln(2 \pm \sqrt{3}) + 2\pi i k$이다. $(2+\sqrt{3})(2-\sqrt{3}) = 1$에서 $\ln(2-\sqrt{3}) = -\ln(2+\sqrt{3})$이므로

$$z = 2\pi k \mp i \ln(2+\sqrt{3}) \qquad (k \in \mathbb{Z})$$

이다. $\ln(2+\sqrt{3}) \approx 1.3170$이다. 실수 해는 없다.

연습문제 2.12 $\operatorname{Log}(1+i)$와 $(1+i)^{1/2}$의 모든 값을 구하라.

풀이. $1 + i = \sqrt{2}\, e^{i\pi/4}$이므로 $\operatorname{Log}(1+i) = \frac{1}{2}\ln 2 + \frac{\pi}{4} i$이다. 식 (2.11)에서 제곱근의 값은 $e^{\frac{1}{2}\operatorname{Log}(1+i)} e^{\pi i k}$이므로 두 값

$$\pm 2^{1/4} e^{i\pi/8}$$

이고 주값은 $2^{1/4} e^{i\pi/8} \approx 1.0987 + 0.4551 i$이다.

연습문제 2.13 $\mathbb{C} \setminus [-1,1]$에서 $\sqrt{z^2-1}$의 정칙 분지가 존재함을 설명하라.

풀이. $g(z) = z\sqrt{1 - z^{-2}}$ (제곱근은 주분지)를 생각한다. 주분지가 정칙이 아닌 곳은 $1 - z^{-2} \in (-\infty, 0]$인 곳인데, 이는 $z^{-2} \geq 1$, 곧 $z^2 \in (0,1]$과 같고 $z \in [-1,1] \setminus \{0\}$일 때뿐이다. 그러므로 g는 $\mathbb{C} \setminus [-1,1]$에서 정칙이고

$$g(z)^2 = z^2\,(1 - z^{-2}) = z^2 - 1$$

이다. 또 $|z| \to \infty$에서 $g(z)/z \to 1$이다.

편각으로 보면 다음과 같다. 이 영역의 닫힌 곡선이 $[-1,1]$을 한 바퀴 감을 때 $z-1$과 $z+1$의 편각이 각각 2π씩 늘어 z^2-1의 편각은 4π, 제곱근의 편각은 2π 늘어나므로 값이 원래대로 돌아온다. 반면 $\mathbb{C} \setminus \{-1, 1\}$에서는 한 끝점만 감는 닫힌 곡선이 있고, 그 곡선을 따라가면 제곱근의 편각이 π만 늘어 부호가 바뀐다. 따라서 그 영역에는 정칙 분지가 존재하지 않는다.

참고 (다음 장과의 연결). 정칙 함수의 강한 성질들은 적분에서 나온다. 제11권 제3장에서는 복소선적분을 정의하고 Cauchy 정리를 증명한다.

제 3 장

복소 선적분과 Cauchy 정리

개요 복소 선적분은 평면 곡선을 따라 복소함수를 적분하는 연산이며, Cauchy 정리는 정칙 함수를 닫힌 곡선을 따라 적분하면 0이라는 정리이다. 이 장은 선적분을 정의하고 크기 평가(ML 부등식)를 증명하고 원 위의 기본 적분을 계산한 다음, 원시함수의 존재와 경로독립성이 동치임을 보인다. 이어서 삼각형에 대한 Goursat 정리를 증명하고, 이로부터 볼록 영역의 Cauchy 정리를 얻는다. "닫힌 곡선 적분이 0"이라는 결론에 영역과 곡선에 관한 어떤 조건이 붙는지가 핵심이며, 이 정리가 복소해석 전체의 출발점이다. 선행 지식: 제11권 제1장과 제11권 제2장의 정칙성과 초등함수, 제9권 제6장의 선적분, 제9권 제7장의 Green 정리.

3.1 복소 선적분

이 권에서 **곡선**은 연속이고 조각마다 C^1인 사상 $\gamma\colon [a,b]\to\mathbb{C}$를 뜻한다. $\gamma(a)$를 시작점, $\gamma(b)$를 끝점이라 하고, $\gamma(a)=\gamma(b)$이면 **닫힌 곡선**이라 한다. 닫힌 곡선이 양 끝점 말고는 같은 점을 두 번 지나지 않으면 **단순 닫힌 곡선**이라 한다. 곡선의 상 $\gamma([a,b])$를 간단히 "γ 위"라고 부른다. 두 점 z, w를 잇는 선분 $t\mapsto z+t(w-z)$ $(0\le t\le 1)$는 $[z,w]$로 적는다.

정의 3.1 (복소 선적분) 곡선 $\gamma\colon[a,b]\to\mathbb{C}$와 γ 위에서 연속인 f에 대해 **복소 선적분**(*contour integral*)을

$$\int_\gamma f(z)\,\mathrm{d}z=\int_a^b f(\gamma(t))\,\gamma'(t)\,\mathrm{d}t \tag{3.1}$$

로 정의한다. 오른쪽은 복소숫값 함수의 적분으로, 실수부와 허수부를 따로 적분한 것이다. 닫힌 곡선 위의 적분은 $\oint_\gamma$로도 적는다. 곡선의 **길이**는 $L(\gamma)=\int_a^b|\gamma'(t)|\,\mathrm{d}t$이다.

$f=u+iv$, $\mathrm{d}z=\mathrm{d}x+i\,\mathrm{d}y$로 쓰면

$$\int_\gamma f\,\mathrm{d}z=\int_\gamma (u\,\mathrm{d}x-v\,\mathrm{d}y)+i\int_\gamma (v\,\mathrm{d}x+u\,\mathrm{d}y) \tag{3.2}$$

로, 실벡터장 선적분 두 개의 결합이다. 따라서 제9권 제6장의 성질이 그대로 옮겨진다. 적분은 f에 대해 선형이고, 같은 방향의 재매개화에 대해 불변이다. 방향을 뒤집은 곡선 $-\gamma$에서는 부호가 바뀌어 $\int_{-\gamma}f\,\mathrm{d}z=-\int_\gamma f\,\mathrm{d}z$이며, 곡선을 이어 붙이면 적분은 더해진다.

명제 3.2 (ML 부등식) 곡선 γ 위에서 연속인 f에 대해

$$\left|\int_\gamma f\,\mathrm{d}z\right|\le \max_{\gamma}|f|\cdot L(\gamma) \tag{3.3}$$

이다. 여기서 $L(\gamma)=\int_a^b|\gamma'(t)|\,\mathrm{d}t$는 길이이다.

증명. 먼저 연속인 복소숫값 함수 $g\colon [a,b]\to\mathbb{C}$에 대해 $\left|\int_a^b g\,dt\right| \le \int_a^b |g|\,dt$임을 보인다. $\int_a^b g\,dt = \rho e^{i\phi}$ $(\rho\ge 0)$로 쓰면

$$\rho = \operatorname{Re}\left(e^{-i\phi}\int_a^b g\,dt\right) = \int_a^b \operatorname{Re}\bigl(e^{-i\phi}g(t)\bigr)\,dt \le \int_a^b |g(t)|\,dt$$

이다. $g(t)=f(\gamma(t))\gamma'(t)$에 적용하면

$$\left|\int_\gamma f\,dz\right| \le \int_a^b |f(\gamma(t))|\,|\gamma'(t)|\,dt \le \max_{\gamma}|f|\int_a^b |\gamma'(t)|\,dt. \qquad \square$$

이름은 상계를 $M=\max_\gamma|f|$와 길이 L의 곱 ML로 적는 관습에서 왔다.

3.2 가장 중요한 계산

예제 3.3 (원 위의 거듭제곱 적분) $\gamma(t)=z_0+re^{it}$, $0\le t\le 2\pi$ (반시계 방향 원)이면 $\gamma'(t)=ire^{it}$이므로 정수 n에 대해

$$\oint_\gamma (z-z_0)^n\,dz = \int_0^{2\pi} r^n e^{int}\,ire^{it}\,dt = ir^{n+1}\int_0^{2\pi} e^{i(n+1)t}\,dt = \begin{cases} 2\pi i, & n=-1,\\ 0, & n\neq -1 \end{cases} \tag{3.4}$$

이다. $n\neq -1$이면 $e^{i(n+1)t}$의 원시함수 $e^{i(n+1)t}/\bigl(i(n+1)\bigr)$이 $t=0$과 $t=2\pi$에서 같은 값을 갖고, $n=-1$이면 피적분함수가 1이다. 결과는 반지름 r과 무관하다.

이 한 줄 계산이 제11권 제6장의 유수 정리와 제11권 제5장의 Laurent 급수 계수 공식의 원형이다. $n\neq -1$이면 $(z-z_0)^n$은 $z\neq z_0$에서 원시함수 $(z-z_0)^{n+1}/(n+1)$을 가지므로 닫힌 곡선 적분이 0이다. $n=-1$이면 원시함수가 될 후보 $\log(z-z_0)$가 원을 따라 연속인 분지를 갖지 못한다(제11권 제2장).

예제 3.4 (경로에 따라 달라지는 적분) 1에서 -1로 가는 두 반원 $\gamma_\pm(t)=e^{\pm it}$, $0\le t\le\pi$에 대해

$$\int_{\gamma_\pm}\frac{dz}{z} = \int_0^{\pi}\frac{\pm ie^{\pm it}}{e^{\pm it}}\,dt = \pm i\pi$$

이다. 시작점과 끝점이 같아도 적분이 다르며, 두 값의 차 $2\pi i$가 식 (3.4)의 $n=-1$인 경우이다.

3.3 원시함수와 경로독립

열린집합 U에서 정칙인 F가 $F'=f$를 만족하면 F를 f의 **원시함수**(*primitive*)라 한다.

명제 3.5 (원시함수가 있을 때의 적분) U에서 $F'=f$이고 f가 연속이면, U 안의 z_1에서 z_2로 가는 모든 곡선 γ에 대해

$$\int_\gamma f\,dz = F(z_2)-F(z_1) \tag{3.5}$$

이다. 특히 닫힌 곡선 위의 적분은 0이다.

증명. γ가 C^1인 구간에서 연쇄법칙에 의해

$$\frac{d}{dt}F(\gamma(t)) = f(\gamma(t))\,\gamma'(t)$$

이므로 그 구간마다 미적분 기본정리를 적용하고 더한다. 이웃한 구간의 끝값이 상쇄되어 $F(\gamma(b)) - F(\gamma(a))$가 남는다. □

역으로 영역 U에서 연속인 f의 모든 닫힌 곡선 적분이 0이면 f는 원시함수를 갖는다. 점 $z_0 \in U$를 고정한다. 영역은 연결된 열린집합이므로 각 $z \in U$에 대해 z_0에서 z로 가는 U 안의 곡선이 있고, 그런 두 곡선 위의 적분의 차가 닫힌 곡선 적분이므로

$$F(z) = \int_{z_0}^{z} f(\zeta)\,\mathrm{d}\zeta$$

는 경로와 무관하게 정의된다. $D(z,\delta) \subseteq U$이고 $|h| < \delta$이면 $F(z+h) - F(z) = \int_{[z,z+h]} f\,\mathrm{d}\zeta$이고, $\int_{[z,z+h]} \mathrm{d}\zeta = h$와 명제 3.2에서

$$\left| \frac{F(z+h)-F(z)}{h} - f(z) \right| = \left| \frac{1}{h} \int_{[z,z+h]} \big(f(\zeta) - f(z)\big)\,\mathrm{d}\zeta \right| \le \max_{\zeta \in [z,z+h]} |f(\zeta) - f(z)|$$

이다. f가 z에서 연속이므로 오른쪽은 $h \to 0$일 때 0으로 간다. 곧 $F' = f$이다. 따라서 영역에서 연속인 함수에 대해 “모든 닫힌 곡선 적분이 0”과 “원시함수가 존재”는 동치이다. $1/z$은 $\mathbb{C} \setminus \{0\}$에서 원시함수를 갖지 않는다. 단위원 위의 적분이 $2\pi i \neq 0$이기 때문이다.

3.4 Goursat 정리

정리 3.6 (Cauchy–Goursat) f가 열린집합 U에서 정칙이고 닫힌 삼각형 영역 $T \subseteq U$이면

$$\oint_{\partial T} f\,\mathrm{d}z = 0$$

이다. 여기서 ∂T는 T의 둘레를 한 바퀴 도는 닫힌 곡선이다.

증명. $I = \left|\oint_{\partial T} f\,\mathrm{d}z\right|$라 하고, T의 둘레를 p, 지름(두 점 사이 거리의 최댓값)을 d라 하자. 세 변의 중점을 이어 T를 네 개의 합동인 삼각형으로 나누고 각각의 둘레를 ∂T와 같은 방향으로 돈다(그림 3.1). 내부의 변은 서로 반대 방향으로 두 번 지나므로 네 경계 적분의 합이 원래 적분이다. 그러므로 네 삼각형 가운데 하나 T_1은

$$\left|\oint_{\partial T_1} f\,\mathrm{d}z\right| \ge \frac{I}{4}$$

를 만족한다. T_1에 같은 분할을 되풀이하면 닫힌 삼각형의 감소열 $T \supseteq T_1 \supseteq T_2 \supseteq \cdots$를 얻고

$$\left|\oint_{\partial T_k} f\,\mathrm{d}z\right| \ge \frac{I}{4^k}, \qquad p_k = 2^{-k}p, \qquad d_k = 2^{-k}d$$

이다. 여기서 p_k, d_k는 T_k의 둘레와 지름이다. 공집합이 아닌 콤팩트 집합의 감소열이므로 공통점 $z_0 \in T \subseteq U$가 있다. f는 z_0에서 복소미분가능하므로

$$f(z) = f(z_0) + f'(z_0)(z - z_0) + \varepsilon(z)(z - z_0), \qquad \varepsilon(z) \to 0 \quad (z \to z_0)$$

로 쓸 수 있다. 처음 두 항은 z의 일차식이라 원시함수를 가지므로 명제 3.5에 의해 닫힌 곡선 적분이 0이다. $z \in \partial T_k$이면 $|z - z_0| \le d_k$이므로 명제 3.2에서

$$\left|\oint_{\partial T_k} f\,\mathrm{d}z\right| = \left|\oint_{\partial T_k} \varepsilon(z)(z - z_0)\,\mathrm{d}z\right| \le \sup_{T_k} |\varepsilon| \cdot d_k\, p_k$$

이고, 따라서

$$I \le 4^{k} \sup_{T_k} |\varepsilon| \cdot 4^{-k} dp = dp \sup_{T_k} |\varepsilon|$$

이다. $T_k \subseteq \{z : |z - z_0| \le d_k\}$이고 $d_k \to 0$이므로 $k \to \infty$일 때 $\sup_{T_k} |\varepsilon| \to 0$이다. 그러므로 $I = 0$이다. □

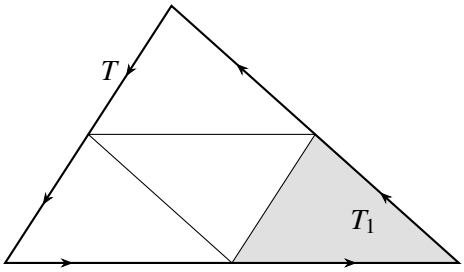

그림 3.1 Goursat 정리의 증명에 쓰는 분할. 세 변의 중점을 이으면 합동인 삼각형 네 개가 생긴다. 네 삼각형을 모두 바깥 둘레와 같은 방향(화살표)으로 돌면 내부의 변 위의 적분은 이웃한 삼각형끼리 상쇄된다. 네 삼각형 가운데 적분의 절댓값이 $I/4$ 이상인 것을 T_1로 고른다.

이 증명은 f'의 연속성을 쓰지 않는다. f'이 연속이라고 가정하면 Green 정리(제9권 제7장)로 더 간단히 증명할 수 있다. 조각마다 매끄러운 경계를 갖는 유계 영역 D가 경계와 함께 U에 포함되면

$$\oint_{\partial D} f \, \mathrm{d}z = \iint_{D} \left(i \frac{\partial f}{\partial x} - \frac{\partial f}{\partial y} \right) \mathrm{d}A = 2i \iint_{D} \frac{\partial f}{\partial \bar{z}} \, \mathrm{d}A = 0 \tag{3.6}$$

이다. 첫 등식은 $\oint f\,\mathrm{d}x + if\,\mathrm{d}y$에 Green 정리를 쓴 것이고, 둘째 등식은 Wirtinger 미분의 정의 $2\,\partial_{\bar z} f = f_x + i f_y$이며, 마지막은 Cauchy–Riemann 방정식 $\partial_{\bar z} f = 0$이다(제11권 제1장).

참고 (연속성 가정을 없애는 까닭). 정칙 함수의 도함수는 실제로 언제나 연속이다. 그러나 그 사실은 Cauchy 정리에서 나오는 적분공식으로 증명하므로(제11권 제4장), f'의 연속성을 미리 가정하지 않는 정리 3.6의 증명이 논리적으로 필요하다.

역사. Cauchy는 1825년 논문에서 이 정리를 f'이 연속이라는 가정 아래 제시하였다. Goursat는 1900년에 그 가정이 필요 없음을 보였고, 삼각형 분할을 쓰는 위 증명은 Pringsheim(1901)에서 비롯한다.

3.5 볼록 영역과 단순연결 영역의 Cauchy 정리

정리 3.7 (볼록 영역의 Cauchy 정리) 볼록 열린집합 U에서 정칙인 f는 U에서 원시함수를 갖고, U 안의 모든 닫힌 곡선 γ에 대해

$$\oint_{\gamma} f \, \mathrm{d}z = 0$$

이다.

증명. 점 $z_0 \in U$를 고정하고 $F(z) = \int_{[z_0, z]} f\,\mathrm{d}\zeta$ (선분 위의 적분)로 둔다. $z \in U$와 $D(z,\delta) \subseteq U$인 $\delta > 0$을 잡고 $0 < |h| < \delta$라 하자. 볼록성에 의해 세 점 z_0, z, $z+h$를 꼭짓점으로 하는 삼각형이 U

에 포함되므로 정리 3.6에서

$$\int_{[z_0,z]} f\,d\zeta + \int_{[z,z+h]} f\,d\zeta + \int_{[z+h,z_0]} f\,d\zeta = 0, \qquad \text{곧} \qquad F(z+h)-F(z) = \int_{[z,z+h]} f\,d\zeta$$

이다. 세 점이 한 직선 위에 있으면 이 등식은 선분 적분의 가법성에서 바로 나온다. 따라서

$$\frac{F(z+h)-F(z)}{h} - f(z) = \frac{1}{h}\int_{[z,z+h]} \big(f(\zeta)-f(z)\big)\,d\zeta \longrightarrow 0 \qquad (h\to 0)$$

이다. 수렴은 f의 연속성과 명제 3.2에서 나온다. 곧 $F'=f$이고, 닫힌 곡선 적분이 0이라는 결론은 명제 3.5에서 나온다. □

위 증명에서 볼록성은 고정한 점 z_0과 $\zeta\in[z,z+h]$를 잇는 선분 $[z_0,\zeta]$가 모두 U에 포함된다는 데에만 쓰였다. 삼각형은 이 선분들의 합집합이기 때문이다. 그러므로 같은 결론이 **별모양 영역**, 곧 어떤 점 $z_0\in U$에 대해 모든 $z\in U$의 선분 $[z_0,z]$가 U에 포함되는 영역에서 성립한다. $\mathbb{C}\setminus(-\infty,0]$은 볼록하지 않지만 $z_0=1$에 대해 별모양이다.

더 일반적으로 단순연결 영역에서 같은 결론이 성립한다. 일반 형태는 다음과 같다. U 안의 두 닫힌 곡선 $\gamma_0,\gamma_1\colon[a,b]\to U$에 대해 연속사상 $H\colon[0,1]\times[a,b]\to U$가 있어 $H(0,t)=\gamma_0(t)$, $H(1,t)=\gamma_1(t)$, $H(s,a)=H(s,b)$를 만족하면 두 곡선이 U 안에서 **호모토픽**(*homotopic*)하다고 한다. 이는 한 곡선을 U 안에서 닫힌 곡선인 채로 연속적으로 변형하여 다른 곡선으로 만들 수 있다는 뜻이다.

> **정리 3.8 (Cauchy 정리의 호모토피 형태)** f가 영역 U에서 정칙이고 닫힌 곡선 γ_0, γ_1이 U 안에서 호모토픽하면
>
> $$\oint_{\gamma_0} f\,dz = \oint_{\gamma_1} f\,dz$$
>
> 이다. 특히 U가 단순연결이면, 곧 U 안의 모든 닫힌 곡선이 한 점(상수 곡선)과 호모토픽하면, U 안의 모든 닫힌 곡선 γ에 대해 $\oint_\gamma f\,dz=0$이고 f는 U에서 원시함수를 갖는다.

증명은 H의 상을 U에 포함되는 유한 개의 작은 원판으로 덮고, 원판마다 정리 3.7의 원시함수를 써서 이웃한 곡선 위의 적분이 같음을 보이는 것이다. 자세한 증명은 싣지 않는다.

흔한 오류. "f가 곡선 위에서 정칙"이라는 조건만으로는 닫힌 곡선 적분이 0이 되지 않는다. 곡선이 둘러싼 내부 전체에서 정칙이어야 한다. $1/z$은 단위원 위의 모든 점에서 정칙이지만 내부의 원점에서 정의되지 않으므로 적분이 $2\pi i$이다.

핵심 수식

ML 부등식:
$$\left|\int_\gamma f\,dz\right| \le \max_{\gamma}|f|\cdot L(\gamma),$$

원 위의 기본 적분:
$$\oint_{|z-z_0|=r}(z-z_0)^n\,dz = \begin{cases} 2\pi i, & n=-1,\\ 0, & n\neq -1, \end{cases}$$

Cauchy 정리:
$$\oint_\gamma f\,dz = 0.$$

Cauchy 정리에서 f는 단순연결 영역 U에서 정칙이고 γ는 U 안의 닫힌 곡선이다.

3.6 곡선의 변형

Cauchy 정리의 가장 실용적인 형태는 다음과 같다. f가 두 단순 닫힌 곡선 γ_1(바깥)과 γ_2(안쪽) 사이의 고리 영역과 그 경계에서 정칙이면, 둘을 같은 방향으로 돌 때

$$\oint_{\gamma_1} f\,dz = \oint_{\gamma_2} f\,dz \tag{3.7}$$

이다. 고리를 두 절단선으로 잘라 단순연결 영역 두 개로 만들고 각각의 경계에 Cauchy 정리를 적용한 다음 더하면, 절단선 위의 적분은 반대 방향으로 두 번 나타나 상쇄되고 $\oint_{\gamma_1} f\,dz - \oint_{\gamma_2} f\,dz = 0$이 남는다. 이 성질 덕분에 복잡한 닫힌 곡선 위의 적분을 특이점 둘레의 작은 원 위의 적분으로 바꿀 수 있다.

예제 3.9 γ가 원 $|z-1|=2$를 반시계로 도는 곡선이면 원점이 원의 내부에 있다($|0-1|=1<2$). 식 (3.7)에 의해 $\oint_\gamma dz/z$는 원점을 중심으로 하는 작은 원 위의 적분과 같으므로 식 (3.4)에서 $2\pi i$이다. 원 $|z-3|=1$이면 $1/z$이 이 원판을 포함하는 볼록 영역 $\operatorname{Re} z>0$에서 정칙이므로 정리 3.7에 의해 적분이 0이다.

예제 3.10 (감김수) 닫힌 곡선 $\gamma\colon [\alpha,\beta]\to\mathbb{C}$와 곡선 위에 없는 점 a에 대해

$$n(\gamma,a)=\frac{1}{2\pi i}\oint_\gamma \frac{dz}{z-a} \tag{3.8}$$

를 a에 대한 γ의 **감김수**(*winding number*)라 한다. 이 값은 정수이며 γ가 a를 반시계 방향으로 감은 횟수이다. 정수임은 다음과 같이 보인다.

$$\phi(t)=\int_\alpha^t \frac{\gamma'(s)}{\gamma(s)-a}\,ds$$

로 두면 γ가 C^1인 구간에서

$$\frac{d}{dt}\left[e^{-\phi(t)}\big(\gamma(t)-a\big)\right]=e^{-\phi(t)}\big(-\phi'(t)(\gamma(t)-a)+\gamma'(t)\big)=0$$

이므로 연속함수 $e^{-\phi(t)}(\gamma(t)-a)$는 상수이다. $t=\alpha$와 $t=\beta$에서 비교하면 $\gamma(\alpha)=\gamma(\beta)$에서 $e^{\phi(\beta)}=1$, 곧 $\phi(\beta)=2\pi i\,n(\gamma,a)\in 2\pi i\mathbb{Z}$이다.

같은 계산에서 $\gamma(t)-a=(\gamma(\alpha)-a)\,e^{\phi(t)}$이므로 $\operatorname{Im}\phi(t)$는 $\gamma(t)-a$의 편각이 시작점부터 연속적으로 변한 양이다. 따라서 감김수는 $\gamma(t)$의 a에 대한 편각의 연속적 증가량을 2π로 나눈 값과 같다. 이 정수가 제11권 제6장의 유수 정리와 제11권 제7장의 편각 원리의 기본 단위이다.

3.7 연습문제와 해설

연습문제 3.11 γ가 0에서 $1+i$로 가는 선분일 때 $\int_\gamma \bar z\,dz$와 $\int_\gamma z\,dz$를 구하라. 같은 끝점을 잇는 다른 경로 $0\to 1\to 1+i$에서는 어떠한가?

풀이. 선분을 $z=(1+i)t$, $0\le t\le 1$로 매개화하면

$$\int_\gamma \bar z\,dz=\int_0^1 (1-i)t\,(1+i)\,dt=2\int_0^1 t\,dt=1$$

이다. 꺾인 경로에서는 $z = t$와 $z = 1 + it$ $(0 \le t \le 1)$를 차례로 지나므로

$$\int_0^1 t\,\mathrm{d}t + \int_0^1 (1 - it)\,i\,\mathrm{d}t = \frac{1}{2} + \left(i + \frac{1}{2}\right) = 1 + i$$

이다. 두 값이 다르므로 명제 3.5에 의해 $\bar{z}$는 원시함수를 갖지 않는다. z의 적분은 원시함수 $z^2/2$가 있으므로 두 경로 모두 $(1+i)^2/2 = i$이다.

연습문제 3.12 ML 부등식으로 $\left|\displaystyle\oint_{|z|=2} \frac{e^z}{z^2+1}\,\mathrm{d}z\right| \le \frac{4\pi e^2}{3}$ 임을 보여라.

풀이. $|z| = 2$에서 $|e^z| = e^{\operatorname{Re} z} \le e^2$이고, 삼각부등식에서 $|z^2 + 1| \ge |z|^2 - 1 = 3$이다. 곡선의 길이는 4π이므로 식 (3.3)의 상계는 $\dfrac{e^2}{3} \cdot 4\pi$이다. 정확한 값은 제11권 제6장의 유수 정리로 $2\pi i \sin 1$이며, 그 절댓값 $2\pi \sin 1 \approx 5.29$는 상계 $4\pi e^2/3 \approx 30.95$보다 훨씬 작다.

연습문제 3.13 $\displaystyle\oint_{|z|=1} \frac{\mathrm{d}z}{z^2 - 4}$를 구하라.

풀이. 피적분함수의 특이점 ± 2는 닫힌 단위원판 밖에 있다. 피적분함수가 반지름이 1보다 조금 큰 원판(볼록 영역), 예를 들어 $|z| < 2$에서 정칙이므로 정리 3.7에 의해 적분은 0이다.

연습문제 3.14 $\gamma(t) = e^{2it}$, $0 \le t \le 2\pi$일 때 $n(\gamma, 0)$을 정의로 계산하라.

풀이. 식 (3.8)과 $\gamma'(t) = 2ie^{2it}$에서

$$n(\gamma, 0) = \frac{1}{2\pi i} \int_0^{2\pi} \frac{2ie^{2it}}{e^{2it}}\,\mathrm{d}t = \frac{4\pi i}{2\pi i} = 2$$

이다. 이 곡선은 단위원을 반시계 방향으로 두 번 돈다.

참고 (다음 장과의 연결). Cauchy 정리를 $f(z)/(z - z_0)$에 적용하면 원판 안의 값이 경계값으로 완전히 결정된다는 Cauchy 적분공식을 얻는다. 제11권 제4장의 결과들은 모두 이 공식에서 나온다.

제 4 장

Cauchy 적분공식과 그 결과

개요 Cauchy 적분공식은 닫힌 원판을 포함하는 영역에서 정칙인 함수의 내부값이 경계 원 위의 값들로 완전히 결정된다는 정리이다. 이 장은 Cauchy 적분공식을 증명하고, 그로부터 정칙함수의 무한 번 미분가능성과 멱급수 전개, Cauchy 부등식, Liouville 정리, 대수학의 기본정리, 최대절댓값 원리, Schwarz 보조정리를 차례로 이끌어 낸다. 선행 지식: 앞 장(제11권 제3장)의 Cauchy 정리와 곡선의 변형.

4.1 Cauchy 적분공식

정리 4.1 (Cauchy 적분공식) f가 닫힌 원판 $\overline{D(z_0, r)}$를 포함하는 열린집합에서 정칙이면, $|z - z_0| < r$인 모든 z에 대해

$$f(z) = \frac{1}{2\pi i} \oint_{|\zeta - z_0| = r} \frac{f(\zeta)}{\zeta - z}\, d\zeta \tag{4.1}$$

이다.

증명. 곡선 변형(제11권 제3장)으로 적분은 z를 중심으로 하는 작은 원 $|\zeta - z| = \varepsilon$ 위의 적분과 같다. 그 위에서

$$\frac{1}{2\pi i}\oint \frac{f(\zeta)}{\zeta - z}\,d\zeta = f(z)\cdot\frac{1}{2\pi i}\oint \frac{d\zeta}{\zeta - z} + \frac{1}{2\pi i}\oint \frac{f(\zeta) - f(z)}{\zeta - z}\,d\zeta$$

이다. 첫 항은 $\oint_{|\zeta - z| = \varepsilon} d\zeta/(\zeta - z) = 2\pi i$(제11권 제3장)이므로 $f(z)$이다. 둘째 항은 피적분함수가 $\zeta \to z$일 때 $f'(z)$에 가까워져 ε에 무관하게 유계이므로, ML 부등식(길이 $2\pi\varepsilon$, 최댓값 $O(1)$)으로 크기가 $O(\varepsilon)$이다. $\varepsilon \to 0$이면 0이다. $\square$

참고 (평균값 성질). $z = z_0$를 넣고 $\zeta = z_0 + re^{it}$로 쓰면 **평균값 성질**

$$f(z_0) = \frac{1}{2\pi}\int_0^{2\pi} f(z_0 + re^{it})\,dt$$

를 얻는다. 실수부를 취하면 조화함수의 평균값 성질이 된다. 정칙 함수의 원판 내부값은 경계 원 위의 값만으로 완전히 결정되며, 실변수 함수에는 이런 현상이 없다(매끄러운 실함수의 구간 내부값은 양 끝점 값만으로 정해지지 않는다).

4.2 무한 번 미분가능성과 멱급수 전개

정리 4.2 열린집합 U에서 정칙인 f는 무한 번 미분가능하며, $\overline{D(z_0,r)} \subseteq U$이면

$$f^{(n)}(z) = \frac{n!}{2\pi i}\oint_{|\zeta - z_0| = r} \frac{f(\zeta)}{(\zeta - z)^{n+1}}\,\mathrm{d}\zeta \qquad (|z - z_0| < r) \tag{4.2}$$

이다. 또한 f는 $D(z_0,R) \subseteq U$인 가장 큰 원판에서 z_0 중심의 Taylor 급수로 전개된다.

증명. $|z - z_0| < |\zeta - z_0| = r$에서 기하급수

$$\frac{1}{\zeta - z} = \frac{1}{\zeta - z_0}\cdot\frac{1}{1 - \frac{z - z_0}{\zeta - z_0}} = \sum_{n \ge 0} \frac{(z - z_0)^n}{(\zeta - z_0)^{n+1}}$$

가 원 위에서 균등수렴하므로 Cauchy 적분공식(식 (4.1))에서 항별 적분하면 $f(z) = \sum_{n} a_n (z - z_0)^n$, $a_n = \frac{1}{2\pi i}\oint \frac{f(\zeta)}{(\zeta - z_0)^{n+1}}\,\mathrm{d}\zeta$를 얻는다. 멱급수는 무한 번 미분가능하고 $a_n = f^{(n)}(z_0)/n!$이다. r은 $D(z_0,R)$ 안에서 임의로 크게 잡을 수 있다. □

유도 (일반 점에서의 미분 공식). 위 증명은 식 (4.2)을 $z = z_0$에서($a_n = f^{(n)}(z_0)/n!$ 꼴로) 세웠을 뿐이므로, 원판 내부의 임의의 점 z에서도 성립함을 보충해야 한다. z를 고정하고 $0 < \delta < r - |z - z_0|$를 잡으면, 위와 같은 논증을 중심을 z_0 대신 z로 바꾸어 반지름 δ인 작은 원에 적용해 식 (4.2)을 z에서 먼저 얻는다. 이제 그 작은 원을 $|\zeta - z_0| = r$까지 넓히는 것은, 두 원 사이의 고리에서 피적분함수 $f(\zeta)/(\zeta - z)^{n+1}$가 ζ에 대해 정칙이므로 (분모가 0이 되는 $\zeta = z$가 고리 바깥에 있다) Cauchy 정리(제11권 제3장)에 따라 적분값이 바뀌지 않기 때문이다. 따라서 큰 원 하나로 원판 내부 모든 점에서의 도함수를 나타내는 식 (4.2)을 얻는다.

따라서 복소해석에서는 "한 번 복소미분가능(정칙)", "무한 번 미분가능", "해석적(멱급수 전개)"이 모두 같다. 정칙성은 다음 Morera 정리로 적분 조건으로도 특징지어진다.

정리 4.3 (Morera) U에서 연속인 f가 U 안의 모든 삼각형 경계에서 적분 0을 가지면 f는 정칙이다.

증명. 가정으로 각 원판에서 원시함수 F를 만들 수 있고(제11권 제3장의 증명), F가 정칙이므로 그 도함수 f도 정칙이다. □

참고. Morera 정리는 정칙 함수열의 균등극한이 정칙임을 보이는 데 쓰인다. 실변수에서 미분가능한 함수열의 균등극한이 미분가능하지 않을 수 있었던 것과 대조된다.

4.3 Cauchy 부등식과 Liouville 정리

따름정리 4.4 (Cauchy 부등식) 미분 공식 (4.2)에 ML 부등식을 쓰면, $|f| \le M$이 원 $|\zeta - z_0| = r$ 위에서 성립할 때

$$|f^{(n)}(z_0)| \le \frac{n!\,M}{r^n} \tag{4.3}$$

이다.

정리 4.5 (Liouville) 유계인 전해석함수는 상수이다.

증명. $|f| \le M$이면 식 (4.3)$(n=1)$로 모든 $r>0$에서 $|f'(z_0)| \le M/r$이고 $r \to \infty$로 $f'(z_0)=0$이다. 모든 점에서 $f'=0$이므로 상수이다. □

정리 4.6 (대수학의 기본정리) 차수가 1 이상인 복소계수 다항식은 $\mathbb{C}$에서 근을 갖는다.

증명. p가 근을 갖지 않으면 $1/p$는 전해석함수이다. $|z| \to \infty$에서 $|p(z)| \to \infty$이므로 $1/p$는 큰 원 밖에서 작고, 원판 안에서는 연속이라 유계이다. Liouville 정리로 $1/p$는 상수가 되어 모순이다. □

참고. 반복 적용하면 n차 다항식은 중복도를 세어 정확히 n개의 근을 갖는다. 제1권에서 실계수 다항식의 근이 켤레쌍으로 나타난다고 한 사실과 합치면, 실계수 다항식은 실수 위에서 일차식과 판별식이 음인 이차식의 곱으로 인수분해된다.

4.4 최대절댓값 원리

정리 4.7 (최대절댓값 원리) 영역 U에서 정칙인 f에 대해 $|f|$가 U의 한 점에서 국소 최댓값을 가지면 f는 상수이다. 따라서 U가 유계이고 f가 $\overline{U}$에서 연속이면 $\max_{\overline{U}}|f|$는 경계에서 도달된다.

증명. $|f(z_0)| \ge |f(z)|$가 $D(z_0,r)$에서 성립한다고 하자. 평균값 성질로

$$|f(z_0)| \le \frac{1}{2\pi}\int_0^{2\pi} |f(z_0+\rho e^{it})|\,dt \le |f(z_0)|$$

이므로 원 $|z-z_0|=\rho$ 위에서 $|f|=|f(z_0)|$이다$(\rho<r$ 임의$)$. 절댓값이 상수인 정칙 함수는 상수이므로 원판에서 상수이고, 일치의 원리로 U 전체에서 상수이다. □

참고. f가 영점이 없으면 $1/f$에 적용하여 $|f|$의 최솟값도 경계에서 도달됨을 안다. 영점이 있으면 이 논증은 실패한다. $f(z)=z$는 단위원판에서 최솟값 0을 내부에서 갖는다.

정리 4.8 (Schwarz 보조정리) f가 단위원판 $\mathbb{D}$에서 정칙이고 $|f|\le 1$, $f(0)=0$이면 $|f(z)| \le |z|$, $|f'(0)| \le 1$이다. 어느 하나에서 등호가 성립하면$(z\neq 0$에서$)$ $f(z)=e^{i\theta}z$인 회전이다.

증명. $g(z)=f(z)/z$ $(g(0)=f'(0))$는 정칙이다. $|z|=r<1$에서 $|g| \le 1/r$이므로 최대절댓값 원리로 $|z|\le r$에서 $|g|\le 1/r$이고, $r\to 1$로 $|g|\le 1$이다. 등호가 내부에서 성립하면 g는 절댓값 1인 상수이다. □

4.5 적분공식을 이용한 계산

예제 4.9 $\oint_{|z|=2} \dfrac{e^z}{(z-1)^3}\,dz$를 구하자. 미분 공식 (4.2)에서 $n=2$, $f=e^z$, $z_0=1$이므로 $\dfrac{2\pi i}{2!}f''(1)=\pi i e$이다.

예제 4.10 $\oint_{|z|=2} \dfrac{dz}{z^2(z-1)}$을 구하자. 원 안에 특이점 0과 1이 있다. 부분분수

$$\frac{1}{z^2(z-1)} = \frac{1}{z-1} - \frac{1}{z} - \frac{1}{z^2}$$

이므로 적분은 $2\pi i - 2\pi i - 0 = 0$이다. 큰 원 위에서 피적분함수가 $|z|^{-3}$ 정도로 작아지므로 반지름을 키우면 ML 부등식으로 0이라는 것도 확인된다.

4.6 연습문제와 해설

연습문제 4.11 전해석함수 f가 $|f(z)| \le C(1+|z|)^n$을 만족하면 f는 차수 n 이하의 다항식임을 보여라.

풀이. Cauchy 부등식으로 $|f^{(k)}(0)| \le k!\,C(1+r)^n/r^k$이고 $k > n$이면 $r \to \infty$에서 0이다. Taylor 계수 $a_k = 0$ $(k > n)$이므로 다항식이다.

연습문제 4.12 $\displaystyle\oint_{|z|=3} \frac{\sin z}{z^2(z-\pi)}\,dz$를 계산하라.

풀이. 부분분수 대신 각 특이점 근처를 작은 원으로 나누어 적분공식을 쓴다. $3 < \pi$이므로 $z=\pi$는 사실 $|z|=3$의 바깥에 있다. 그런데 $\sin\pi = 0$이므로 $z=\pi$에서는 $\sin z$의 단순 영점이 $1/(z-\pi)$의 단순극을 상쇄하여 피적분함수가 애초에 그 점에서 정칙이다(제거가능 특이점). 따라서 $z=\pi$ 근처의 기여는 $|z|=3$ 안쪽 여부와 무관하게 0이고, 적분에 실제로 기여하는 것은 $z=0$뿐이다. 0 근처에서

$$\frac{\sin z}{z^2(z-\pi)} = \frac{g(z)}{z^2}, \qquad g(z) = \frac{\sin z}{z-\pi}$$

이므로 유수는 $g'(0)$이고, $g'(z) = \dfrac{\cos z\,(z-\pi) - \sin z}{(z-\pi)^2}$에서 $g'(0) = \dfrac{\cos 0\cdot(-\pi) - \sin 0}{\pi^2} = -\dfrac{1}{\pi}$이다. 기여는 $2\pi i\, g'(0) = 2\pi i \cdot (-1/\pi) = -2i$이고, 이것이 적분값이다.

연습문제 4.13 f가 전해석함수이고 $\operatorname{Re} f \le 0$이면 f가 상수임을 보여라.

풀이. $g = e^{f}$는 전해석함수이고 $|g| = e^{\operatorname{Re} f} \le 1$이므로 Liouville 정리로 상수이다. 따라서 $g' = f' e^{f} = 0$이고 $e^{f} \neq 0$이므로 $f' = 0$이다.

연습문제 4.14 단위원판에서 정칙이고 $|f| \le 1$인 f에 대해 $f(1/2) = 0$이면 $|f(0)| \le 1/2$임을 보여라.

풀이. 원판의 자기동형 $\varphi(z) = \dfrac{z - 1/2}{1 - z/2}$는 $|z|=1$을 보존하고 $\varphi(1/2) = 0$이다. $h = f \circ \varphi^{-1}$은 $h(0) = f(1/2) = 0$, $|h| \le 1$이므로 Schwarz 보조정리로 $|h(w)| \le |w|$이다. $w = \varphi(0) = -1/2$를 넣으면 $|f(0)| = |h(-1/2)| \le 1/2$이다.

참고 (다음 연결). 정칙 함수가 한 점에서 정의되지 않으면 그 점 근처에서는 음의 거듭제곱까지 허용한 급수가 필요하다. 다음 장(제11권 제5장)의 Laurent 급수와 특이점의 분류가 주제이다.

제 5 장

Laurent 급수와 고립특이점

개요 Laurent 급수는 중심이 제외된 고리 영역에서 정칙인 함수를 양과 음의 거듭제곱 항으로 전개한 급수이다. 이 장은 Laurent 전개 정리를 증명하고, 전개의 음의 거듭제곱 부분(주요부)의 모양에 따라 고립특이점을 제거가능 특이점·극·진성 특이점으로 분류한 뒤, 각 경우의 전형적인 성질(Riemann의 정리, Casorati–Weierstrass 정리)과 전개 계산 기법을 정리한다. 선행 지식: 앞 장(제11권 제4장)의 Cauchy 적분공식과 Taylor 전개.

5.1 Laurent 전개

정리 5.1 (Laurent) f가 고리 $A = \{r < |z - z_0| < R\}$ $(0 \le r < R \le \infty)$에서 정칙이면

$$f(z) = \sum_{n=-\infty}^{\infty} a_n (z - z_0)^n, \qquad a_n = \frac{1}{2\pi i} \oint_{|\zeta - z_0| = \rho} \frac{f(\zeta)}{(\zeta - z_0)^{n+1}}\, d\zeta \tag{5.1}$$

가 A에서 성립하고 A 안의 모든 닫힌 부분고리에서 균등수렴한다. 여기서 $r < \rho < R$은 임의이며 계수는 ρ와 무관하고, 이런 전개는 유일하다.

증명의 뼈대. $z \in A$를 두 원 $|\zeta - z_0| = \rho_1 < |z - z_0| < \rho_2$ 사이에 두고 Cauchy 적분공식을 고리에 적용하면

$$f(z) = \frac{1}{2\pi i} \oint_{\rho_2} \frac{f(\zeta)}{\zeta - z}\, d\zeta - \frac{1}{2\pi i} \oint_{\rho_1} \frac{f(\zeta)}{\zeta - z}\, d\zeta$$

이다. 바깥 원에서는 앞 장처럼 $(z - z_0)/(\zeta - z_0)$의 기하급수로, 안쪽 원에서는 $(\zeta - z_0)/(z - z_0)$의 기하급수로 전개한다. 유일성은 급수를 원 위에서 항별 적분하여 계수 공식을 다시 얻는 것으로 보인다. $\square$

역사. 이 전개는 프랑스의 공병 장교였던 Pierre Alphonse Laurent가 1843년에 Académie des sciences에 제출한 논문에서 처음 제시했다.

정의 5.2 (주요부) Laurent 전개에서 음의 거듭제곱 부분 $\sum_{n<0} a_n (z - z_0)^n$을 **주요부**(*principal part*)라 한다. 계수 공식이 있지만 실제로는 알려진 급수를 조작하여 구하는 경우가 많다. 유일성 덕분에 어떤 방법으로 얻든 같은 계수이다.

예제 5.3 (영역에 따라 다른 전개) $f(z) = \dfrac{1}{(z-1)(z-2)} = \dfrac{1}{z-2} - \dfrac{1}{z-1}$을 $z_0 = 0$ 중심으로 전개하자.

- $|z| < 1$: $\dfrac{1}{z-2} = -\dfrac{1}{2}\sum_{n} (z/2)^n$, $-\dfrac{1}{z-1} = \sum_{n} z^n$ 이므로 $f = \sum_{n \ge 0} (1 - 2^{-n-1}) z^n$ (Taylor 급수).
- $1 < |z| < 2$: $-\dfrac{1}{z-1} = -\dfrac{1}{z}\cdot\dfrac{1}{1 - 1/z} = -\sum_{n \ge 1} z^{-n}$ 이므로 $f = -\sum_{n \ge 0} 2^{-n-1} z^n - \sum_{n \ge 1} z^{-n}$.
- $|z| > 2$: $f = \sum_{n \ge 2} (2^{n-1} - 1) z^{-n}$.

같은 함수라도 고리마다 전개가 다르다. 유일성은 한 고리 안에서의 유일성이다.

5.2 고립특이점의 분류

정의 5.4 (고립특이점) f가 $0<|z-z_0|<R$에서 정칙이면 z_0를 **고립특이점**(*isolated singularity*)이라 한다. Laurent 전개의 주요부 모양에 따라 다음과 같이 분류한다.

- **제거가능 특이점**(*removable singularity*): 주요부가 없다($a_n=0,\ n<0$).
- **m위 극**(*pole*): 주요부가 유한하고 $a_{-m}\neq 0$, $a_n=0\ (n<-m)$.
- **진성 특이점**(*essential singularity*): 주요부에 0이 아닌 항이 무한히 많다.

정리 5.5 (Riemann의 제거가능 특이점 정리) f가 z_0의 구멍 난 근방에서 유계이면 z_0는 제거가능 특이점이다.

증명. $|f|\le M$이면 계수 공식과 ML 부등식으로 $|a_n|\le M\rho^{-n}$이다. $n<0$이면 $\rho\to 0$에서 0이다. □

명제 5.6 z_0가 m위 극일 필요충분조건은 $f(z)=g(z)/(z-z_0)^m$이고 g가 z_0 근처에서 정칙이며 $g(z_0)\neq 0$인 것이다. 이때 $|f(z)|\to\infty\ (z\to z_0)$이다.

예제 5.7 예를 들어 $\dfrac{\sin z}{z}$는 0에서 제거가능 특이점이다($1-z^2/6+\cdots$). $\dfrac{1}{\sin z}$는 0에서 단순극, $\dfrac{\cos z}{z^3}$은 3위 극이다. 영점의 차수와 극의 차수는 역수 관계에 있다. g가 z_0에서 m위 영점을 가지면 $1/g$는 m위 극을 갖는다.

5.3 진성 특이점의 행동

예제 5.8 $e^{1/z}=\sum_{n\ge 0}\dfrac{z^{-n}}{n!}$은 0에서 진성 특이점이다. 양의 실수축으로 접근하면 ∞로, 음의 실수축으로 접근하면 0으로 가며, 허수축 $z=it$에서는 $|e^{1/z}|=1$이다. 극한이 방향에 따라 제각각이다.

정리 5.9 (Casorati–Weierstrass) z_0가 진성 특이점이면 z_0의 모든 구멍 난 근방에서 f의 상은 $\mathbb{C}$에서 조밀하다.

증명. 어떤 근방의 상이 $D(w,\varepsilon)$을 피한다면 $g(z)=\dfrac{1}{f(z)-w}$는 그 근방에서 $|g|\le 1/\varepsilon$으로 유계이다. 따라서 z_0는 g의 제거가능 특이점이고, $f=w+1/g$는 z_0에서 정칙이거나(제거가능) 극을 가진다. 진성 특이점이라는 가정에 모순이다. □

참고. 더 강한 Picard의 정리는 진성 특이점의 모든 구멍 난 근방에서 f가 많아야 한 값을 제외한 모든 복소수를 무한히 많이 취한다고 말한다. $e^{1/z}$는 0만 취하지 않는다.

5.4 무한원점에서의 특이점과 유리형 함수

$f(z)$의 ∞에서의 행동은 $f(1/w)$의 $w=0$에서의 행동으로 정의한다. 다항식은 차수만큼의 극을 ∞에 갖고, e^z, $\sin z$처럼 다항식이 아닌 전해석함수는 ∞에서 진성 특이점을 갖는다.

영역에서 극을 제외하고 정칙인 함수를 **유리형 함수**(*meromorphic function*)라 한다. $\widehat{\mathbb{C}}$ 전체에서 유리형인 함수(무한원점 포함)는 정확히 유리함수이다. 극이 유한개뿐이므로 각 극의 주요부를 빼면 $\widehat{\mathbb{C}}$에서 유계인 함수가 남고, Liouville 정리로 상수이기 때문이다. 이 결과는 부분분수 분해가 항상 가능하다는 사실의 복소해석적 증명이기도 하다.

5.5 계산 기법

Laurent 계수는 알려진 급수의 대입, 곱셈, 나눗셈으로 구한다.

예제 5.10 $\dfrac{1}{z\sin z}$의 0 근방 전개를 처음 세 항까지 구하자. $\sin z = z(1 - z^2/6 + z^4/120 - \cdots)$이므로

$$\frac{1}{z\sin z} = \frac{1}{z^2}\Big(1 - \frac{z^2}{6} + \frac{z^4}{120}\Big)^{-1} = \frac{1}{z^2}\Big(1 + \frac{z^2}{6} + \frac{7z^4}{360} + \cdots\Big).$$

$(1-u)^{-1} = 1 + u + u^2 + \cdots$에 $u = z^2/6 - z^4/120$을 넣으면 z^4의 계수는 $-\frac{1}{120} + \frac{1}{36} = \frac{7}{360}$이다. 따라서 0은 2위 극이고 z^{-1} 계수는 0이다.

5.6 연습문제와 해설

연습문제 5.11 $z^2 e^{1/z}$의 0 근방 Laurent 전개에서 z^{-1}의 계수를 구하라.

풀이. $z^2 \sum_{n} \dfrac{z^{-n}}{n!}$에서 z^{-1}은 $n = 3$일 때이므로 계수는 $1/3! = 1/6$이다.

연습문제 5.12 $\dfrac{1 - \cos z}{z^4}$의 0에서의 특이점 종류를 판정하라.

풀이. $1 - \cos z = \dfrac{z^2}{2} - \dfrac{z^4}{24} + \cdots$이므로 $\dfrac{1}{2z^2} - \dfrac{1}{24} + \cdots$이다. 2위 극이며 z^{-1} 계수는 0이다.

연습문제 5.13 $\tan z$의 극을 모두 찾고 각 극에서 주요부를 구하라.

풀이. $\cos z = 0$, 즉 $z_k = \pi/2 + k\pi$이다. $\cos$의 영점은 단순$(\cos'(z_k) = -\sin z_k = \mp 1 \neq 0)$이므로 단순극이다. 주요부는 $\dfrac{\sin z_k}{-\sin z_k}\cdot\dfrac{1}{z - z_k} = \dfrac{-1}{z - z_k}$이다.

연습문제 5.14 f가 전해석함수이고 ∞에서 극을 가지면 다항식임을 보여라.

풀이. $g(w) = f(1/w)$가 $w = 0$에서 m위 극을 가지면 $|w|$가 작을 때 $|g(w)| \le C|w|^{-m}$, 즉 큰 $|z|$에서 $|f(z)| \le C|z|^m$이다. 앞 장의 연습문제(연습문제 4.11)로 f는 차수 m 이하의 다항식이다.

참고 (다음 연결). 계수 a_{-1}은 특별하다. 원을 따라 적분하면 이 계수만 살아남기 때문이다. 다음 장(제11권 제6장)에서는 이 "유수"로 닫힌 곡선 적분과 실적분을 계산한다.

제 6 장

유수 정리와 실적분의 계산

개요 유수(留數, *residue*)는 고립특이점에서의 Laurent 전개 중 $(z-z_0)^{-1}$ 항의 계수이며, 유수 정리는 단순 닫힌 곡선을 따른 적분을 내부 특이점들의 유수의 합으로 바꾼다. 이 장은 유수 정리를 증명하고 유수를 계산하는 표준 공식을 정리한 뒤, 삼각함수의 유리식 적분, 무한구간의 유리함수·Fourier형 적분, 실축 위의 극이 있는 주값 적분, 분지절단이 있는 적분까지 실변수로는 어렵거나 불가능한 적분을 복소 경로적분으로 계산하는 기법을 조건과 함께 제시한다. 선행 지식: 앞 장(제11권 제5장)의 Laurent 급수와 극의 분류, 제3장(제11권 제3장)의 감김수.

6.1 유수와 유수 정리

정의 6.1 (유수) 고립특이점 z_0에서 Laurent 계수 a_{-1}을 **유수**(*residue*) $\operatorname{Res}_{z=z_0} f$라 한다. 작은 원을 따라 적분하면 $\oint f\,dz = 2\pi i\, a_{-1}$이다(제11권 제3장의 $\oint (z-z_0)^n\,dz$ 계산).

정리 6.2 (유수 정리) f가 단순 닫힌 곡선 γ와 그 내부에서 유한개의 고립특이점 $z_1,\dots,z_k$를 제외하고 정칙이며 γ 위에 특이점이 없으면, γ를 반시계 방향으로 돌 때

$$\oint_{\gamma} f(z)\,dz = 2\pi i \sum_{j=1}^{k} \operatorname{Res}_{z=z_j} f \tag{6.1}$$

이다.

증명. 각 특이점을 작은 원으로 둘러싸고 곡선 변형(제11권 제3장)을 쓰면 된다. 일반 닫힌 곡선에서는 각 유수에 감김수 $n(\gamma, z_j)$를 곱한다. $\square$

6.2 유수의 계산 공식

- 단순극: $\operatorname{Res}_{z_0} f = \lim_{z\to z_0} (z-z_0) f(z)$.
- $f = g/h$, $g(z_0)\neq 0$, h가 z_0에서 단순 영점: $\operatorname{Res}_{z_0} f = g(z_0)/h'(z_0)$.
- m위 극: $\operatorname{Res}_{z_0} f = \dfrac{1}{(m-1)!}\lim_{z\to z_0}\dfrac{d^{m-1}}{dz^{m-1}}\bigl[(z-z_0)^m f(z)\bigr]$.
- 진성 특이점: Laurent 전개에서 직접 a_{-1}을 읽는다.

예제 6.3 $f(z)=\dfrac{e^{z}}{z^2+1}$의 $z=i$에서의 유수는 둘째 공식으로 $\dfrac{e^{i}}{2i}$이다. $\dfrac{z}{(z-1)^2}$의 $z=1$에서의 유수는 셋째 공식($m=2$)으로 $\dfrac{d}{dz}z\Big|_{z=1}=1$이다.

6.3 삼각함수의 유리식 적분

$\int_0^{2\pi} R(\cos\theta,\sin\theta)\,d\theta$ 꼴은 $z=e^{i\theta}$ 로 단위원 위의 적분이 된다. $\cos\theta=\dfrac{z+z^{-1}}{2}$, $\sin\theta=\dfrac{z-z^{-1}}{2i}$, $d\theta=\dfrac{dz}{iz}$ 이다.

예제 6.4 $a>1$ 일 때 $I=\int_0^{2\pi}\dfrac{d\theta}{a+\cos\theta}$ 를 구하자.

$$I=\oint_{|z|=1}\frac{1}{a+\frac{z+z^{-1}}{2}}\frac{dz}{iz}=\frac{2}{i}\oint_{|z|=1}\frac{dz}{z^2+2az+1}.$$

근은 $z_\pm=-a\pm\sqrt{a^2-1}$ 이고 $z_+z_-=1$, $|z_+|<1<|z_-|$ 이다. 유수는 $\dfrac{1}{z_+-z_-}=\dfrac{1}{2\sqrt{a^2-1}}$ 이므로 $I=\dfrac{2}{i}\cdot 2\pi i\cdot\dfrac{1}{2\sqrt{a^2-1}}=\dfrac{2\pi}{\sqrt{a^2-1}}$ 이다.

6.4 무한구간의 유리함수 적분

명제 6.5 P,Q 가 다항식이고 $\deg Q\ge\deg P+2$ 이며 Q 가 실근을 갖지 않으면

$$\int_{-\infty}^{\infty}\frac{P(x)}{Q(x)}\,dx=2\pi i\sum_{\operatorname{Im} z_j>0}\operatorname{Res}_{z_j}\frac{P}{Q} \tag{6.2}$$

이다.

증명의 뼈대. 반지름 R 인 위쪽 반원 경로를 쓰고, 원호 위의 적분이 ML 부등식으로 $O(R\cdot R^{-2})\to 0$ 임을 확인한다. 차수 조건이 원호 적분의 소멸을 보장한다. □

예제 6.6 $\displaystyle\int_{-\infty}^{\infty}\frac{dx}{(x^2+1)^2}$: 위 반평면의 극은 i (2위)이고 $\operatorname{Res}_i=\dfrac{d}{dz}(z+i)^{-2}\Big|_{z=i}=-2(2i)^{-3}=\dfrac{1}{4i}$ 이다. 값은 $2\pi i\cdot\dfrac{1}{4i}=\dfrac{\pi}{2}$ 이다.

6.5 Fourier형 적분과 Jordan 보조정리

$\int_{-\infty}^{\infty}f(x)e^{i\omega x}\,dx$ $(\omega>0)$에서는 위 반평면에서 $|e^{i\omega z}|=e^{-\omega\operatorname{Im} z}\le 1$ 이므로 f 가 $\deg Q\ge\deg P+1$ 정도로만 감소해도 원호 적분이 사라진다.

보조정리 6.7 (Jordan) $\omega>0$ 이고 원호 $C_R=\{Re^{i\theta}:0\le\theta\le\pi\}$ 위에서 $|f|\le M_R\to 0$ 이면 $\int_{C_R}f(z)e^{i\omega z}\,dz\to 0$ 이다.

증명.

$$\left|\int_{C_R}\right|\le M_R\int_0^{\pi}e^{-\omega R\sin\theta}R\,d\theta\le 2M_R\int_0^{\pi/2}e^{-2\omega R\theta/\pi}R\,d\theta<\frac{\pi M_R}{\omega}$$

이다. 여기서 $[0,\pi/2]$ 에서 $\sin\theta\ge 2\theta/\pi$ 를 썼다. □

예제 6.8 $a>0$ 이면 $\displaystyle\int_{-\infty}^{\infty}\frac{\cos x}{x^2+a^2}\,dx=\operatorname{Re}\int\frac{e^{ix}}{x^2+a^2}\,dx=\operatorname{Re}\Big(2\pi i\frac{e^{-a}}{2ia}\Big)=\frac{\pi e^{-a}}{a}$ 이다. e^{-ix} 를 쓰면 아래 반평면을 닫아야 한다.

주의 (방향을 잘못 고르면). 부호를 잘못 고르면 원호 적분이 지수적으로 커진다. $e^{i\omega z}$ $(\omega>0)$는 위 반평면을, $e^{-i\omega z}$는 아래 반평면을 닫아야 Jordan 보조정리가 적용된다.

6.6 실축 위의 극과 주값

예제 6.9 $(\sin x/x)$ $\displaystyle\int_{-\infty}^{\infty}\frac{e^{iz}}{z}\,dz$는 원점의 극 때문에 그대로 정의되지 않는다. 원점을 반지름 ε인 위쪽 작은 반원으로 피해 가는 경로를 쓰면, 닫힌 경로 내부에 극이 없으므로 총합은 0이다. 큰 원호의 적분은 Jordan 보조정리로 0으로 가고, 작은 반원(시계 방향)의 적분은 $-\pi i\,\operatorname{Res}_0 = -\pi i$로 간다. 따라서 주값 $\mathrm{P.V.}\displaystyle\int\frac{e^{ix}}{x}\,dx=\pi i$이고 허수부를 취하면 $\displaystyle\int_{-\infty}^{\infty}\frac{\sin x}{x}\,dx=\pi$, 즉 $\displaystyle\int_{0}^{\infty}\frac{\sin x}{x}\,dx=\frac{\pi}{2}$이다.

보조정리 6.10 (작은 반원 보조정리) z_0가 단순극이면 중심각 α인 작은 원호(반시계) 위의 적분은 $\varepsilon\to 0$에서 $i\alpha\,\operatorname{Res}_{z_0} f$로 간다. 고차 극에서는 이 결론이 성립하지 않으며 주값이 존재하지 않을 수 있다.

6.7 분지절단이 있는 적분

예제 6.11 $0<a<1$일 때 $\displaystyle\int_0^{\infty}\frac{x^{a-1}}{1+x}\,dx=\frac{\pi}{\sin(\pi a)}$이다. z^{a-1}의 분지를 양의 실수축을 절단으로 하여 $0<\arg z<2\pi$로 정하고, 절단의 위와 아래를 지나는 열쇠구멍 경로를 쓴다. 위쪽에서는 x^{a-1}, 아래쪽에서는 $x^{a-1}e^{2\pi i(a-1)}$이 되고, 큰 원과 작은 원의 기여는 $0<a<1$ 조건 아래 사라진다. 내부 극 $z=-1=e^{i\pi}$의 유수는 $e^{i\pi(a-1)}$이므로

$$(1-e^{2\pi i(a-1)})I = 2\pi i e^{i\pi(a-1)},\qquad I=\frac{2\pi i}{e^{-i\pi(a-1)}-e^{i\pi(a-1)}}=\frac{\pi}{\sin(\pi a)}.$$

참고. 이 결과는 Gamma 함수의 반사공식 $\Gamma(a)\Gamma(1-a)=\pi/\sin(\pi a)$와 같은 내용이다.

6.8 연습문제와 해설

연습문제 6.12 $\displaystyle\int_0^{2\pi}\frac{d\theta}{5-4\sin\theta}$를 구하라.

풀이. $\sin\theta=\dfrac{z-z^{-1}}{2i}$를 넣으면

$$\oint\frac{dz}{iz\bigl(5-\frac{2}{i}(z-z^{-1})\bigr)}=\oint\frac{dz}{5iz-2z^2+2}=\oint\frac{-\,dz}{2z^2-5iz-2}$$

이다. $2z^2-5iz-2=0$의 근은 $z=2i$, $z=i/2$이고 원 안의 근은 $i/2$이다. 유수는 $\left.\dfrac{-1}{4z-5i}\right|_{z=i/2}=\dfrac{-1}{-3i}=\dfrac{1}{3i}$이므로 값은 $2\pi i\cdot\dfrac{1}{3i}=\dfrac{2\pi}{3}$이다.

연습문제 6.13 $\displaystyle\int_{-\infty}^{\infty}\frac{x^2}{x^4+1}\,dx$를 구하라.

풀이. 위 반평면의 극은 $e^{i\pi/4}$, $e^{3i\pi/4}$ 이다. 단순극에서 $\operatorname{Res} \dfrac{z^2}{z^4+1} = \dfrac{z^2}{4z^3} = \dfrac{1}{4z}$ 이므로 합은 $\dfrac{1}{4}(e^{-i\pi/4} + e^{-3i\pi/4}) = \dfrac{1}{4}(-i\sqrt{2})$ 이다. 값은 $2\pi i \cdot \dfrac{-i\sqrt{2}}{4} = \dfrac{\pi}{\sqrt{2}}$ 이다.

> **연습문제 6.14** $\displaystyle\oint_{|z|=1} e^{1/z}\,dz$ 와 $\displaystyle\oint_{|z|=1} e^{1/z^2}\,dz$ 를 구하라.

풀이. 진성 특이점의 유수는 Laurent 전개에서 읽는다. $e^{1/z}$ 의 z^{-1} 계수는 1 이므로 $2\pi i$ 이고, e^{1/z^2} 에는 z^{-1} 항이 없으므로 0 이다.

참고 (다음 연결). 유수 정리를 f'/f 에 적용하면 영점과 극의 개수를 세는 공식이 된다. 다음 장(제11권 제7장)의 편각 원리와 Rouché 정리이다.

제 7 장

편각 원리, Rouché 정리, 열린사상 정리

개요 이 장은 유리형 함수의 로그 미분 f'/f의 적분으로 영역 안의 영점과 극의 개수를 세는 **편각 원리**(*argument principle*)를 증명하고, 이를 Rouché 정리·Hurwitz 정리로 확장한 뒤, 정칙 함수가 국소적으로 몇 대 몇 사상인지를 밝히는 국소 사상 정리와 열린사상 정리를 이끌어 낸다. 제어공학의 Nyquist 판정법이 편각 원리의 대표적 응용이다. 선행 지식: 앞 장(제11권 제6장)의 유수 정리, 제3장(제11권 제3장)의 감김수.

7.1 로그 미분과 편각 원리

f가 z_0에서 m위 영점을 가지면 $f(z) = (z-z_0)^m g(z)$, $g(z_0) \neq 0$이므로

$$\frac{f'}{f} = \frac{m}{z-z_0} + \frac{g'}{g}$$

이고 $\operatorname{Res}_{z_0} f'/f = m$이다. m위 극이면 같은 계산으로 유수가 $-m$이다.

정리 7.1 (편각 원리) f가 단순 닫힌 곡선 γ와 그 내부에서 유리형이고 γ 위에 영점과 극이 없으면

$$\frac{1}{2\pi i}\oint_{\gamma} \frac{f'(z)}{f(z)}\,dz = Z - P \tag{7.1}$$

이다. 여기서 Z, P는 내부의 영점과 극의 개수(중복도 포함)이다.

좌변은 곡선 $f\circ\gamma$의 원점에 대한 감김수 $n(f\circ\gamma, 0)$과 같다. $w = f(z)$로 바꾸면 $\oint_\gamma \frac{f'}{f}\,dz = \oint_{f\circ\gamma} \frac{dw}{w}$이기 때문이다. 즉 γ를 한 바퀴 돌 때 $\arg f$의 총 증가량이 $2\pi(Z-P)$이다. 이름이 "편각 원리"인 이유이다.

예제 7.2 $p(z) = z^3 + 1$과 원 $|z| = 2$: 원 위에서 $p(z) = z^3(1 + z^{-3})$이고 $|z^{-3}| = 1/8$이므로 $\arg p$의 증가량은 $\arg z^3$의 증가량 6π와 같다. 따라서 원 안의 영점은 3개이다. 실제로 세 근 $e^{i\pi/3}, -1, e^{-i\pi/3}$의 절댓값은 모두 1이다.

7.2 Rouché 정리

정리 7.3 (Rouché) f, g가 단순 닫힌 곡선 γ와 그 내부에서 정칙이고 γ 위에서 $|g| < |f|$이면, f와 $f+g$는 γ 내부에서 같은 개수의 영점(중복도 포함)을 갖는다.

증명. γ 위에서 $f \neq 0$이고 $f + g = f(1 + g/f)$, $|g/f| < 1$이다. $h = 1 + g/f$는 γ 위에서 원판 $D(1,1)$ 안에 있으므로 $h\circ\gamma$는 원점을 감지 않고 $n(h\circ\gamma, 0) = 0$이다. 편각이 곱에서 더해지므로 $n((f+g)\circ\gamma, 0) = n(f\circ\gamma, 0)$이다. $\square$

참고. "개를 데리고 가로등 둘레를 걷는 사람" 비유가 있다. 목줄 $|g|$가 사람과 가로등의 거리 $|f|$보다 짧으면 개와 사람은 가로등을 같은 횟수로 돈다.

역사. Rouché 정리는 프랑스의 수학자 Eugène Rouché가 1862년에 발표했다.

> **예제 7.4** $z^5 + 3z + 1$의 단위원판 안 영점 개수를 구하자. $f = 3z$, $g = z^5 + 1$로 두면 $|z| = 1$에서 $|g| \le 2 < 3 = |f|$이므로 영점은 f와 같은 1개이다. 원 $|z| = 2$에서는 $f = z^5$, $g = 3z + 1$로 $|g| \le 7 < 32 = |z|^5$이므로 5개 모두 $|z| < 2$에 있다. 따라서 고리 $1 < |z| < 2$에 4개가 있다. ($|z| = 1$ 위에는 영점이 없다. $|z^5 + 1| \le 2 < 3 = |3z|$이므로 합이 0이 될 수 없다.)

참고. Rouché 정리로 대수학의 기본정리를 다시 얻을 수 있다. $p(z) = z^n + \cdots$에서 큰 원 위의 $|p(z) - z^n| < |z^n|$이므로 p는 그 안에서 n개의 영점을 갖는다.

7.3 Hurwitz 정리

> **정리 7.5 (Hurwitz)** 영역 U에서 정칙인 f_k가 콤팩트 부분집합 위에서 균등하게 f로 수렴하고 f가 상수가 아니면, f의 영점 근처 작은 원판에서 충분히 큰 k의 f_k는 f와 같은 수의 영점을 갖는다. 특히 각 f_k가 영점이 없으면 f도 영점이 없거나 $f \equiv 0$이다.

> **예제 7.6** 예를 들어 e^z의 Taylor 부분합 $s_n(z) = \sum_{k \le n} z^k/k!$는 e^z로 콤팩트 균등수렴하고 e^z는 영점이 없으므로, 고정된 유계 영역 안의 s_n의 영점은 n이 커지면 모두 그 영역 밖으로 나간다. 실제로 s_n의 영점은 반지름 약 n 정도의 곡선 근처에 몰린다.

7.4 열린사상 정리와 국소 구조

> **정리 7.7 (국소 사상 정리)** f가 z_0 근처에서 정칙이고 $f(z) - w_0$가 z_0에서 m위 영점($w_0 = f(z_0)$)이면, z_0의 작은 근방 V와 w_0의 근방 W가 있어 $W \setminus \{w_0\}$의 모든 점은 V 안에서 정확히 m개의 서로 다른 원상을 갖는다.

증명. 편각 원리로 원 $|z - z_0| = \delta$ 내부의 $f - w$의 영점 수가 w에 대해 연속이고 정수값이므로 w가 w_0 근처에서 일정($= m$)하다. 원상이 서로 다르다는 것은 f'이 z_0 근처에서 z_0 외에 영점이 없다는 사실에서 나온다. $\square$

> **정리 7.8 (열린사상 정리)** 영역에서 상수가 아닌 정칙 함수는 열린집합을 열린집합으로 보낸다.

이 정리에서 최대절댓값 원리가 바로 나온다. $|f(z_0)|$가 최대이면 $f(z_0)$를 포함하는 열린 원판이 상에 포함되어야 하는데 그 원판에는 $|w| > |f(z_0)|$인 점이 있기 때문이다. 또 $f'(z_0) \neq 0$이면 $m = 1$이므로 f는 z_0 근처에서 단사이고 역함수도 정칙이다. $f'(z_0) = 0$이면 z_0 근처에서 m대 1 사상이므로 단사가 아니다. 실변수에서 x^3은 도함수가 0인 점에서도 단사였지만, 복소수에서 z^3은 원점 근처에서 3대 1이다.

7.5 Nyquist 판정법: 공학에서의 편각 원리

폐루프 전달함수의 특성방정식 $1 + L(s) = 0$의 근(폐루프 극)이 오른쪽 반평면 $\operatorname{Re} s > 0$에 있으면 시스템이 불안정하다. 허수축과 큰 반원으로 이루어진 Nyquist 경로 γ를 시계 방향으로 돌 때 $L(\gamma)$

가 -1을 반시계로 감는 횟수를 N, 오른쪽 반평면에 있는 L의 극 수를 P라 하면, 편각 원리를 $1+L$에 적용하여 오른쪽 반평면의 폐루프 극의 수는

$$Z = P - N \tag{7.2}$$

이다(γ가 시계 방향이므로 부호가 바뀐다). 따라서 $Z=0$, 즉 안정성의 조건은 $N=P$이다. 개루프가 안정$(P=0)$이면 Nyquist 곡선이 -1을 감지 않아야 한다. 허수축 위에 L의 극이 있으면 작은 반원으로 피해 가며, 감는 방향의 부호 관계는 교재마다 다르므로 처음에 고정한다.

7.6 연습문제와 해설

연습문제 7.9 $z^4 - 6z + 3$의 영점 중 $|z|<1$에 있는 것과 $1<|z|<2$에 있는 것의 개수를 구하라.

풀이. $|z|=1$에서 $|z^4+3| \le 4 < 6 = |-6z|$이므로 단위원판 안에 1개이다. $|z|=2$에서 $|-6z+3| \le 15 < 16 = |z^4|$이므로 $|z|<2$에 4개이다. 경계 위에 영점이 없으므로 고리에 3개이다.

연습문제 7.10 $\lambda > 1$일 때 $ze^{\lambda - z} = 1$이 단위원판 안에서 정확히 하나의 근을 가지며 그 근이 실수임을 보여라.

풀이. $f = ze^{\lambda - z}$, $g = -1$로 두면 $|z|=1$에서 $|f| = e^{\lambda - \operatorname{Re} z} \ge e^{\lambda - 1} > 1 = |g|$이다. f는 원판 안에 영점 0 하나를 가지므로 $f-1$도 근 하나를 갖는다. 실변수 함수 $h(x) = xe^{\lambda - x} - 1$은 $h(0) = -1 < 0$, $h(1) = e^{\lambda-1} - 1 > 0$이므로 $(0,1)$에 실근이 있고, 근이 하나뿐이므로 그것이 그 근이다.

연습문제 7.11 단위원판에서 정칙인 f가 $|z|=1$ 근처까지 연속이고 $|z|=1$에서 $|f(z)|=1$이며 상수가 아니면, f는 원판 안에 영점을 가짐을 보여라.

풀이. 영점이 없으면 최대절댓값 원리를 f와 $1/f$에 적용하여 원판에서 $|f| \le 1$과 $|f| \ge 1$을 얻으므로 $|f| \equiv 1$이고 f는 상수가 된다. 모순이다.

참고 (다음 연결). 국소적으로 단사인 정칙 함수는 각을 보존한다. 다음 장(제11권 제8장)에서는 이 등각성으로 영역을 서로 변환하는 방법과 Riemann 사상정리를 다룬다.

제 8 장

등각사상과 Riemann 사상정리

개요 정칙함수는 도함수가 0이 아닌 점에서 각을 보존하는 **등각사상**(*conformal map*)을 이룬다. 이 장은 등각성의 의미를 정리하고, 대표적인 등각사상인 Möbius 변환과 몇 가지 표준 사상을 소개한 뒤, 단순연결 영역을 단위원판으로 바꿀 수 있다는 Riemann 사상정리와 그 응용인 평면 Dirichlet 문제를 다룬다. 선행 지식: 앞 장(제11권 제7장)의 국소 사상 정리, 제1장(제11권 제1장)의 조화함수, 제4장(제11권 제4장)의 Schwarz 보조정리.

8.1 등각성

f가 z_0에서 정칙이고 $f'(z_0) \neq 0$이면 z_0를 지나는 두 매끄러운 곡선이 이루는 각은 상에서도 크기와 방향이 보존된다. $\gamma(0) = z_0$이면 $(f\circ\gamma)'(0) = f'(z_0)\gamma'(0)$이므로 모든 접벡터가 같은 복소수 $f'(z_0)$를 곱하는 사상, 즉 $\arg f'(z_0)$만큼의 회전과 $|f'(z_0)|$배 확대를 받기 때문이다. $f'(z_0) = 0$이면 각이 m배가 된다(m은 앞 장의 국소 차수). 예를 들어 z^2은 원점에서 직각을 평각으로 만든다.

영역 U에서 V로 가는 정칙 전단사를 **등각동형**(*biholomorphism*)(쌍정칙 사상)이라 한다. 역함수도 자동으로 정칙이다(앞 장).

8.2 Möbius 변환

정의 8.1 $ad - bc \neq 0$인 복소수 a, b, c, d에 대해 $T(z) = \dfrac{az+b}{cz+d}$를 **Möbius 변환**(*Möbius transformation*) (일차분수 변환)이라 한다. $T(-d/c) = \infty$, $T(\infty) = a/c$로 정하면 $\widehat{\mathbb{C}}$의 전단사이다.

Möbius 변환들은 합성에 대해 군을 이루며, 행렬 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$의 곱과 합성이 대응한다 ($PGL_2(\mathbb{C})$와 동형). 평행이동, 회전·확대, 반전 $1/z$의 합성으로 쓰이므로 다음 성질을 갖는다.

- $\widehat{\mathbb{C}}$의 "원" (원 또는 직선)을 원으로 보낸다.
- 서로 다른 세 점 z_1, z_2, z_3을 임의의 서로 다른 세 점으로 보내는 Möbius 변환이 유일하게 존재한다.
- **교차비**(*cross ratio*) $(z, z_1, z_2, z_3) = \dfrac{(z-z_1)(z_2-z_3)}{(z-z_3)(z_2-z_1)}$를 보존한다.

예제 8.2 (Cayley 변환) $C(z) = \dfrac{z-i}{z+i}$는 위 반평면 $\mathbb{H} = \{\operatorname{Im} z > 0\}$을 단위원판 $\mathbb{D}$로 보낸다. $\operatorname{Im} z > 0$이면 z는 $-i$보다 i에 가까우므로 $|z-i| < |z+i|$이고, 실수축은 $|C| = 1$인 원으로 간다.

명제 8.3 단위원판의 등각자기동형은 정확히

$$\varphi(z) = e^{i\theta}\,\frac{z-a}{1-\overline{a}z} \qquad (|a| < 1,\ \theta \in \mathbb{R}) \tag{8.1}$$

꼴이다.

증명. 이런 φ가 원판을 원판으로 보내는 것은 $|z|=1$에서 $|z-a|=|\overline{z}(z-a)|=|1-\overline{a}z|$임에서 확인된다. 역으로 자기동형 f와 $a=f^{-1}(0)$에 대해 $g=f\circ\varphi_a^{-1}$은 0을 고정하는 자기동형이다. g와 g^{-1} 모두에 Schwarz 보조정리를 적용하면 $|g'(0)|=1$이므로 g는 회전이다. □

8.3 표준 사상들

- $z\mapsto z^{\alpha}$ (주분지, $\alpha>0$): 쐐기 $\{0<\arg z<\theta_0\}$ $(\theta_0\le\pi)$를 $\alpha\theta_0\le 2\pi$일 때 쐐기 $\{0<\arg w<\alpha\theta_0\}$로 등각적으로 보낸다. 예를 들어 z^2은 제1사분면을 위 반평면으로 보낸다.
- e^{z}: 띠 $\{0<\operatorname{Im} z<\pi\}$를 위 반평면으로 보낸다. Log는 그 역사상이다.
- $\sin z$: 반무한 띠 $\{-\pi/2<\operatorname{Re} z<\pi/2,\ \operatorname{Im} z>0\}$를 위 반평면으로 보낸다.
- Joukowski 사상 $J(z)=\tfrac{1}{2}(z+1/z)$: $\{|z|>1\}$을 $\mathbb{C}\setminus[-1,1]$로 보낸다. 원 $|z|=r>1$은 초점이 ±1인 타원으로 간다. 날개 단면 설계의 고전적 도구이다.

여러 사상을 합성하여 복잡한 영역을 원판이나 반평면으로 옮기는 것이 실제 계산의 방법이다.

8.4 Riemann 사상정리

정리 8.4 (Riemann 사상정리) $\mathbb{C}$ 전체가 아닌 단순연결 영역 U와 $z_0\in U$에 대해, $f(z_0)=0$, $f'(z_0)>0$인 등각동형 $f:U\to\mathbb{D}$가 유일하게 존재한다.

증명의 뼈대. $\mathbb{C}$를 제외하는 조건은 필요하다. $\mathbb{C}\to\mathbb{D}$인 정칙 함수는 유계 전해석함수이므로 Liouville 정리로 상수이다. 유일성은 앞 절의 자기동형 분류에서 나온다. 존재 증명은 $f(z_0)=0$, $|f|<1$인 단사 정칙 함수들 중 $|f'(z_0)|$를 최대로 하는 것을 찾는 극값 문제로 진행한다. 정칙 함수족의 콤팩트성(Montel 정리, Arzelà–Ascoli 정리의 복소판)과 Hurwitz 정리가 핵심이다. 존재는 보장되지만 명시적 공식이 있는 경우는 드물다. 수치 등각사상(Schwarz–Christoffel 사상의 수치 계산 등)이 별도의 분야인 이유이다. □

역사. Riemann은 1851년 박사학위 논문에서 이 정리를 처음 제시했으나, 그가 쓴 존재 증명은 당시에는 정당화되지 않은 변분 논증(지금의 Dirichlet 원리)에 기댄 것이었다. 결함이 없는 증명은 이후 여러 수학자의 작업을 거쳐 20세기 초에 완성되었다.

경계에 대해서는 Carathéodory 정리가 있다. U의 경계가 Jordan 곡선이면 Riemann 사상은 닫힌 영역 사이의 위상동형으로 연속 확장된다.

8.5 조화함수와 Dirichlet 문제

정칙 함수와 조화함수의 합성은 조화함수이다. h가 V에서 조화이고 $f:U\to V$가 정칙이면 $h\circ f$는 U에서 조화이다(국소적으로 $h=\operatorname{Re} g$, g 정칙이므로 $h\circ f=\operatorname{Re}(g\circ f)$). 따라서 복잡한 영역의 경계값 문제를 원판의 문제로 바꿀 수 있다.

정리 8.5 (Poisson 공식) φ가 단위원 위의 연속함수이면

$$u(re^{i\theta}) = \frac{1}{2\pi}\int_0^{2\pi} \frac{1-r^2}{1-2r\cos(\theta-t)+r^2}\,\varphi(e^{it})\,\mathrm{d}t \qquad (r<1) \tag{8.2}$$

는 원판에서 조화이고 경계에서 φ로 연속적으로 접근한다. 이 해는 유일하다.

Poisson 핵 $P_r(\theta) = \dfrac{1-r^2}{1-2r\cos\theta+r^2} = \operatorname{Re}\dfrac{1+re^{i\theta}}{1-re^{i\theta}}$은 양수이고 평균이 1이며, $r\to 1$에서 $\theta=0$에 몰리는 근사항등함수이다. 유일성은 최댓값 원리에서 나온다.

예제 8.6 위 반평면에서 경계값이 $x>0$에서 1, $x<0$에서 0인 유계 조화함수를 구하자. $\operatorname{Arg} z \in (0,\pi)$는 $\mathbb{H}$에서 조화($\operatorname{Log} z$의 허수부)이고 양의 실수축에서 0, 음의 실수축에서 π이다. 따라서 $u = 1 - \frac{1}{\pi}\operatorname{Arg} z$가 답이다. 등위선은 원점에서 나오는 반직선이다.

8.6 연습문제와 해설

연습문제 8.7 $-1, 0, 1$을 각각 $0, i, \infty$로 보내는 Möbius 변환을 구하라.

풀이. $T(z) = k\dfrac{z+1}{z-1}$로 두면 $T(-1)=0$, $T(1)=\infty$이다. $T(0) = -k = i$에서 $k=-i$이므로 $T(z) = -i\dfrac{z+1}{z-1} = i\dfrac{1+z}{1-z}$이다. 이 변환은 단위원판을 위 반평면으로 보낸다.

연습문제 8.8 제1사분면을 단위원판으로 보내는 등각사상을 하나 구하라.

풀이. z^2으로 위 반평면에 옮긴 뒤 Cayley 변환을 적용하면 $f(z) = \dfrac{z^2-i}{z^2+i}$이다.

연습문제 8.9 $\mathbb{D}$에서 $\mathbb{D}$로 가는 정칙 함수 f가 $f(0)=0$, $f(1/2)=0$을 만족하면 $|f'(0)| \le 1/2$임을 보여라.

풀이. $g(z) = f(z)/\bigl(z\cdot\dfrac{z-1/2}{1-z/2}\bigr)$는 정칙이고(두 영점을 나눔), 원판 경계 근처에서 분모의 절댓값이 1에 가까우므로 최대절댓값 원리로 $|g|\le 1$이다. $f'(0) = g(0)\cdot\dfrac{-1/2}{1}$이므로 $|f'(0)|\le \dfrac{1}{2}$이다.

제11권의 범위와 다음 읽기

이 권은 정칙성과 Cauchy–Riemann 방정식, 초등함수와 분지, Cauchy 정리와 적분공식, Laurent 급수와 유수, 편각 원리, 등각사상을 다루었다. 해석적 정수론의 ζ 함수(제15권), Fourier·Laplace 변환(제12·13권), 양자역학과 전자기학의 Green 함수와 분산관계가 이 권의 직접적 응용이다.

표준 참고서로 L. V. Ahlfors, *Complex Analysis*; E. M. Stein and R. Shakarchi, *Complex Analysis*; J. B. Conway, *Functions of One Complex Variable I*; T. Needham, *Visual Complex Analysis*; J. W. Brown and R. V. Churchill, *Complex Variables and Applications*가 있다.

참고자료의 사용방식. 본문의 설명과 문제는 이 참고서를 위해 새로 작성했다. 아래 목록은 관련 주제를 더 넓은 교재와 대조해 읽기 위한 안내이며, 이 원고 전체가 해당 기관이나 저자의 검토를 받았다는 뜻은 아니다. 개별 정리의 정확한 가정과 기호 약속이 다를 수 있으므로 독자는 자료를 바꿀 때 정의를 확인해야 한다.

- MIT OpenCourseWare, 18.04 Complex Variables with Applications: 유수 계산과 공학 응용을 포함한 복소해석 강의.
- American Institute of Mathematics, Open Textbook Initiative: 복소해석을 포함한 공개 교재 목록.

제 12 권

미분방정식 · 동역학

제12권은 상미분방정식의 풀이 기법과 해의 이론, 그리고 해의 장기 거동을 분석하는 동역학을 다룬다. 제1–2장은 미분방정식의 언어와 1계 방정식의 풀이, Lipschitz 조건 아래 해의 존재·유일성·연장과 초기값에 대한 의존성을 세운다. 제3–5장은 고계 선형 방정식과 급수해, 행렬지수에 의한 선형계의 풀이와 평면 상평면의 분류, Laplace 변환과 전달함수를 다룬다. 제6–8장은 비선형계의 평형점과 선형화에 의한 안정성 판정, 극한주기와 분기, 로지스틱 사상으로 대표되는 이산 동역학과 혼돈을 다룬다.

제 1 장

미분방정식의 언어와 1계 방정식

개요 **미분방정식**(*differential equation*)은 미지함수와 그 도함수 사이의 관계식이다. 이 장은 미분방정식을 상미분방정식과 편미분방정식, 계수(階數)와 선형성으로 분류하는 기본 용어를 정하고, 초기값 문제와 해의 정의역이라는 개념을 세운 뒤, 손으로 풀리는 1계 방정식의 네 가지 유형 — 변수분리형, 1계 선형, 완전방정식, 치환형(동차형·Bernoulli·Riccati) — 과 각 풀이법이 성립하는 조건을 정리한다. 방향장에 의한 정성적 분석과 자율방정식의 상수해의 안정성도 함께 다룬다. 선행 지식: 제8권의 미분과 적분 기법(제8권 제2장, 제8권 제5장), 제9권의 편미분(제9권 제2장).

1.1 용어와 분류

미지함수와 그 도함수 사이의 관계식을 **미분방정식**이라 한다. 미지함수가 한 변수의 함수이면 **상미분방정식**(*ordinary differential equation*, ODE)이고, 여러 변수의 함수이고 편미분이 나타나면 **편미분방정식**(*partial differential equation*, PDE, 제13권 제5장)이다. 방정식에 나타나는 가장 높은 도함수의 차수를 **계**라 한다. $F(t, y, y', \dots, y^{(n)}) = 0$이 $y, y', \dots, y^{(n)}$에 대해 일차식이면 **선형**이라 하고, 그렇지 않으면 **비선형**이라 한다.

- $y' = -ky$ $(k > 0)$: 1계 선형. 방사성 붕괴, RC 회로의 방전.
- $my'' + cy' + ky = F(t)$: 2계 선형. 감쇠 진동자, RLC 회로.
- $\theta'' + \dfrac{g}{L}\sin\theta = 0$: 2계 비선형. 진자.
- $y' = y(1 - y)$: 1계 비선형. 로지스틱 성장.

초기값 문제(*initial value problem*, IVP)는 방정식과 한 점에서의 값 $y(t_0) = y_0$(고계이면 $y'(t_0), \dots, y^{(n-1)}(t_0)$까지)를 함께 준 문제이다. **경계값 문제**(*boundary value problem*)는 두 점 이상에서의 조건을 준다. 해는 정의역(구간)과 함께 말해야 한다. $y' = y^2$, $y(0) = 1$의 해 $y = 1/(1 - t)$는 $(-\infty, 1)$에서만 해이며, $t = 1$을 넘어서는 같은 공식을 쓸 수 없다.

1.2 방향장과 정성적 분석

$y' = f(t, y)$는 평면의 각 점 (t, y)에 기울기 $f(t, y)$를 지정한다. 이 짧은 선분들의 그림인 **방향장**(*direction field*)을 따라가는 곡선이 해이다. 공식으로 풀 수 없을 때에도 방향장과 **등경사선**(*isocline*, $f = c$인 곡선)으로 해의 모양을 알 수 있다.

자율방정식(*autonomous equation*) $y' = f(y)$에서는 $f(y^*) = 0$인 상수해(**평형해**, *equilibrium solution*)가 중요하다. f가 y^*의 왼쪽에서 양, 오른쪽에서 음이면 근처 해들이 y^*로 다가가므로 **안정**하다고 하고, 부호가 반대이면 **불안정**하다고 한다. 로지스틱 방정식 $y' = y(1 - y)$에서 $y^* = 1$ 근처는 왼쪽에서 양, 오른쪽에서 음이므로 안정이고, $y^* = 0$ 근처는 왼쪽에서 음, 오른쪽에서

양이므로 불안정하다. **위상선**(*phase line*)으로 불리는 이 1차원 분석은 제12권 제6장의 안정성 이론의 가장 간단한 경우이다.

1.3 변수분리형

$y' = g(t)h(y)$ 꼴을 **변수분리형**(*separable equation*)이라 한다. $h(y) \neq 0$인 범위에서

$$\int \frac{\mathrm{d}y}{h(y)} = \int g(t)\,\mathrm{d}t + C$$

를 만족하는 $y(t)$가 해이다. 정당화는 연쇄법칙이다. $H' = 1/h$, $G' = g$로 두면, $y(t)$가 위 등식을 만족하는 것과 $H(y(t)) = G(t) + C$인 것은 같고, 이는 $\frac{\mathrm{d}}{\mathrm{d}t} H(y(t)) = H'(y(t))y'(t) = \dfrac{y'(t)}{h(y(t))} = g(t)$, 즉 $y' = g(t)h(y(t))$와 같다.

흔한 오류. $h(y^*) = 0$인 상수해 $y \equiv y^*$는 $h(y)$로 나누는 순간 사라진다. 예를 들어 $y' = y^2$을 분리하면 $-1/y = t + C$를 얻지만 $y \equiv 0$도 해이며 어떤 C에도 대응하지 않는다. 나눗셈 전에 h의 영점을 따로 기록해 두어야 한다.

> **예제 1.1 (로지스틱 방정식)** $y' = ry(1 - y/K)$, $y(0) = y_0 > 0$. 부분분수
>
> $$\frac{1}{y(1 - y/K)} = \frac{1}{y} + \frac{1/K}{1 - y/K}$$
>
> 로 적분하면
>
> $$y(t) = \frac{K}{1 + \left(\dfrac{K}{y_0} - 1\right) e^{-rt}} \tag{1.1}$$
>
> 를 얻는다. $t \to \infty$에서 K로 수렴한다. $0 < y_0 < K$이면 해 곡선은 $y = K/2$에서 변곡점을 갖는 S자 곡선이며, 그 변곡점은 $y_0 < K/2$일 때 $t = \dfrac{1}{r}\log\!\left(\dfrac{K}{y_0} - 1\right) > 0$에 있고, $y_0 \geq K/2$이면 $t \leq 0$ 쪽에 있어 관측 구간 $t \geq 0$에는 나타나지 않는다.

1.4 1계 선형 방정식과 적분인자

$y' + p(t)y = q(t)$에서 p, q가 구간 I에서 연속이라 하자. **적분인자**(*integrating factor*) $\mu(t) = e^{\int p\,\mathrm{d}t}$를 곱하면 좌변이 $(\mu y)'$이 되므로

$$y(t) = \frac{1}{\mu(t)}\left(\int \mu(s)q(s)\,\mathrm{d}s + C\right) \tag{1.2}$$

이다. 해는 I 전체에서 존재하고 초기값이 주어지면 유일하다. 선형 방정식은 계수가 연속인 구간 전체에서 해가 존재한다는 점이 다음 절부터 보는 비선형 방정식과 다르다.

역사. 적분인자를 이용해 1계 선형 방정식을 대수적으로 적분하는 방법은 17세기 말 Gottfried Wilhelm Leibniz와 Bernoulli 형제의 서신과 논문에서 비롯되었다.

> **예제 1.2 (RC 회로)** 저항 R, 축전기 C, 전원 $V(t)$인 직렬회로에서 축전기 전압 v는 $RCv' + v = V(t)$를 만족한다. $V = V_0$(상수), $v(0) = 0$이면 $\mu = e^{t/RC}$로
>
> $$v(t) = V_0\bigl(1 - e^{-t/\tau}\bigr), \qquad \tau = RC$$

> 를 얻는다. $t=\tau$에서 최종값의 $1-e^{-1}\approx 63.2\%$에 도달한다. 시정수(*time constant*)라는 이름의 의미이다.

해의 구조는 "동차방정식의 일반해 + 비동차방정식의 특수해"이다. 이는 선형성에서 나오며 제12권 제3장의 고계 선형 방정식에서도 같다.

1.5 완전방정식과 적분인자

$M(x,y)\,\mathrm{d}x + N(x,y)\,\mathrm{d}y = 0$에서 $M=\partial_x\Phi$, $N=\partial_y\Phi$인 Φ가 있으면 **완전방정식**(*exact equation*)이라 하고, 해는 $\Phi(x,y)=C$이다. 단순연결 영역(예: 직사각형)에서 M,N이 C^1이면 완전할 필요충분조건은 $M_y=N_x$이다(제9권 제6장의 보존장 판정과 같은 내용).

> **예제 1.3** $(2xy+3)\,\mathrm{d}x+(x^2-1)\,\mathrm{d}y=0$은 $M_y=2x=N_x$이므로 완전하다. $\Phi_x=2xy+3$에서 $\Phi=x^2y+3x+g(y)$이고 $\Phi_y=x^2+g'(y)=x^2-1$이므로 $g=-y$이다. 해는 $x^2y+3x-y=C$이다.

완전하지 않을 때에도 $\mu(x,y)$를 곱하여 완전하게 만들 수 있다. $\dfrac{M_y-N_x}{N}$이 x만의 함수이면 $\mu=\exp\displaystyle\int \frac{M_y-N_x}{N}\,\mathrm{d}x$가 적분인자이고, $\dfrac{N_x-M_y}{M}$이 y만의 함수이면 $\mu=\exp\displaystyle\int \frac{N_x-M_y}{M}\,\mathrm{d}y$가 적분인자이다.

1.6 치환으로 풀리는 방정식

- **동차형**(*homogeneous equation*) $y'=F(y/x)$: $v=y/x$로 두면 $y=vx$, $y'=v+xv'$에서 $xv'=F(v)-v$로 변수분리형이 된다.
- **Bernoulli 방정식**(*Bernoulli equation*) $y'+p(t)y=q(t)y^n$ $(n\neq 0,1)$: $w=y^{1-n}$으로 두면 $w'=(1-n)y^{-n}y'$이고 원래 식에 $(1-n)y^{-n}$을 곱해 정리하면 $w'+(1-n)p\,w=(1-n)q$로 선형이 된다.
- **Riccati 방정식**(*Riccati equation*) $y'=a(t)+b(t)y+c(t)y^2$: 특수해 y_1을 알면 $y=y_1+1/w$로 치환하여 w에 대한 선형 방정식을 얻는다. 일반적으로는 초등적으로 풀리지 않는다.

주의 ("동차"라는 말의 두 가지 뜻). 위의 **동차형** $y'=F(y/x)$에서 "동차"는 $F(y/x)$가 x,y를 같은 배로 늘려도 식의 꼴이 바뀌지 않는다는, 곧 우변이 0차 동차함수라는 뜻이다. 이는 제12권 제3장에서 말하는 "동차방정식" $L[y]=0$(비동차항 g가 없다는 뜻)의 "동차"와 전혀 다른 용법이므로 혼동하지 않는다.

> **예제 1.4** $y'+y=ty^2$ (Bernoulli, $n=2$). $w=y^{-1}$로 두면 $w'=-y^{-2}y'$이고, 원래 식의 양변에 $-y^{-2}$를 곱하면 $-y^{-2}y'-y^{-1}=-t$, 곧 $w'-w=-t$를 얻는다. 적분인자 e^{-t}로 풀면 $w=t+1+Ce^{t}$이다. 따라서
>
> $$y=\frac{1}{t+1+Ce^{t}}$$
>
> 이며, 앞서 주의한 대로 치환 과정에서 나눈 $y=0$에 대응하는 상수해 $y\equiv 0$을 따로 덧붙인다.

1.7 연습문제와 해설

연습문제 1.5 $y' = \dfrac{t}{y}$, $y(0) = -2$를 풀고 해의 최대 정의 구간을 구하라.

풀이. $y\,dy = t\,dt$에서 $y^2 = t^2 + 4$이고, 초기값 $y(0) = -2 < 0$에 맞추어 음의 가지 $y = -\sqrt{t^2+4}$를 택한다. 모든 t에서 $y \neq 0$이므로 해는 $\mathbb{R}$ 전체에서 정의된다.

연습문제 1.6 $ty' + 2y = t^2$, $y(1) = 1$을 풀어라. $t = 0$에서 해가 어떻게 되는가?

풀이. 표준형 $y' + \dfrac{2}{t}y = t$에서 $\mu = t^2$이다. $(t^2 y)' = t^3$이므로 $t^2 y = t^4/4 + C$이고, 초기값으로 $C = 3/4$이다. $y = \dfrac{t^2}{4} + \dfrac{3}{4t^2}$는 $(0,\infty)$에서만 해이다. 계수 $2/t$가 $t=0$에서 연속이 아니므로 선형 방정식의 존재 정리가 0을 넘어서까지 해의 존재를 보장하지 않는다.

연습문제 1.7 $(3x^2 y + y^3)\,dx + (x^3 + 3xy^2)\,dy = 0$을 풀어라.

풀이. $M_y = 3x^2 + 3y^2 = N_x$이므로 완전하다. $\Phi = x^3 y + xy^3$이고 해는 $x^3 y + xy^3 = C$이다.

연습문제 1.8 뉴턴의 냉각법칙 $T' = -k(T - T_a)$에서 $90\,^\circ\mathrm{C}$의 물이 $20\,^\circ\mathrm{C}$의 방에서 10분 뒤 $60\,^\circ\mathrm{C}$가 되었다. $40\,^\circ\mathrm{C}$가 되는 시각을 구하라.

풀이. $T_a = 20$이므로 $T - 20 = 70e^{-kt}$이다. $40 = 70e^{-10k}$에서 $k = \dfrac{1}{10}\log\dfrac{7}{4}$이다. $20 = 70e^{-kt}$, 곧 $40 = 70e^{-kt+10k}$가 아니라 직접 $T = 40$을 대입하면 $20 = 70e^{-kt}$에서

$$t = \frac{\log(7/2)}{k} = 10\,\frac{\log 3.5}{\log 1.75} \approx 22.4 \text{ 분}$$

이다.

연습문제 1.9 $y' = y^{1/3}$, $y(0) = 0$의 해를 두 개 이상 찾아라.

풀이. $y \equiv 0$과 $y = (2t/3)^{3/2}$ $(t \geq 0)$가 모두 해이다. 더 나아가 임의의 $c \geq 0$에 대해 $t \leq c$에서 0, $t > c$에서 $(2(t-c)/3)^{3/2}$인 함수도 해이므로 해가 무한히 많다. 제12권 제2장에서 이러한 비유일성이 $y^{1/3}$이 $y = 0$에서 Lipschitz 조건을 만족하지 않는 데에서 비롯됨을 본다.

다음 연결. 마지막 연습문제처럼 해가 유일하지 않거나, 다음 장의 예제처럼 해가 유한 시간에 폭발하는 경우가 있다. 제12권 제2장에서는 초기값 문제가 언제 해를 갖고 그 해가 언제 유일한지를 정확히 진술하고 증명한다.

제 2 장

해의 존재와 유일성, 연장과 의존성

개요 이 장은 초기값 문제 $y' = f(t,y)$, $y(t_0) = y_0$를 동치인 적분방정식으로 바꾸는 데에서 출발하여, 우변 f가 Lipschitz 조건을 만족할 때 해가 국소적으로 유일하게 존재한다는 Picard–Lindelöf 정리와, f가 연속이기만 해도 해는 존재한다는(다만 유일하지는 않을 수 있는) Peano 정리를 증명한다. 이어서 Grönwall 부등식으로 초기값에 대한 해의 연속 의존성을 얻고, 해가 어디까지 연장되는지, 유한 시간에 폭발할 수 있는지를 정리한다. 선행 지식: 제12권 제1장의 1계 방정식, 제9권 제4장의 축약사상 원리(제9권 제4장), 제10권 제2장의 Arzelà–Ascoli 정리(제10권 제2장).

2.1 적분방정식으로 바꾸기

f가 연속이면 초기값 문제 $y' = f(t,y)$, $y(t_0) = y_0$의 연속 해 y는 적분방정식

$$y(t) = y_0 + \int_{t_0}^{t} f(s, y(s))\,\mathrm{d}s$$

의 해와 같다. 한 방향은 미적분 기본정리로 적분방정식을 미분하면 얻고, 다른 방향은 적분방정식의 $t = t_0$ 대입과 피적분함수의 연속성에서 얻는다. 적분방정식은 미분가능성을 미리 요구하지 않으므로 반복법과 극한 논법에 적합하다. 이 절은 $y \in \mathbb{R}^n$인 연립 방정식에도 그대로 성립한다. 고계 방정식 $y^{(n)} = F(t, y, \dots, y^{(n-1)})$은 $Y = (y, y', \dots, y^{(n-1)})$로 두면 $Y' = \bigl(y', \dots, y^{(n-1)}, F(t,Y)\bigr)$인 1계 연립 방정식이 된다.

2.2 Lipschitz 조건

정의 2.1 상수 L이 있어 영역 D의 모든 $(t,y_1), (t,y_2)$에 대해 $\|f(t,y_1) - f(t,y_2)\| \le L\|y_1 - y_2\|$이면 f가 y에 대해 **Lipschitz**라 한다.

$\partial f/\partial y$가 볼록 영역에서 연속이고 유계이면 평균값 부등식으로 Lipschitz이다. 따라서 C^1인 f는 국소적으로 Lipschitz이다. $f(y) = y^{1/3}$은 $y = 0$ 근처에서 Lipschitz가 아니다. $|y^{1/3} - 0|/|y - 0| = |y|^{-2/3} \to \infty$이기 때문이다.

2.3 Picard–Lindelöf 정리

정리 2.2 (Picard–Lindelöf) f가 직사각형 $R = \{|t - t_0| \le a,\ \|y - y_0\| \le b\}$에서 연속이고 y에 대해 Lipschitz(상수 L)이며 $M = \max_R \|f\|$라 하자. $h = \min(a, b/M)$이면 $|t - t_0| \le h$에서 초기값 문제의 해가 유일하게 존재한다.

증명. 연속함수 공간 $X = \{y : [t_0 - h, t_0 + h] \to \mathbb{R}^n,\ \|y(t) - y_0\| \le b\}$에 사상

$$(Ty)(t) = y_0 + \int_{t_0}^{t} f(s, y(s))\,\mathrm{d}s$$

를 정의한다. $\|(Ty)(t)-y_0\| \le M|t-t_0| \le Mh \le b$이므로 $T: X \to X$이다. 가중 노름 $\|y\|_w = \sup_t e^{-2L|t-t_0|}\|y(t)\|$를 쓰면

$$\|(Ty)(t)-(Tz)(t)\| \le L\left|\int_{t_0}^{t} e^{2L|s-t_0|}\,\mathrm{d}s\right| \|y-z\|_w \le \frac{1}{2}e^{2L|t-t_0|}\|y-z\|_w$$

이므로 T는 비율 $1/2$의 축약이다. X는 이 노름(균등노름과 동치)에 대해 완비이므로 축약사상 원리로 유일한 고정점이 있다. □

이 정리는 직사각형 R 전체에서 하나의 Lipschitz 상수 L을 요구한다. C^1인 f는 콤팩트 집합에서 국소적으로 Lipschitz이므로, R을 충분히 작게 잡으면 이 가정이 자동으로 만족된다.

고정점 반복 $y_{k+1} = Ty_k$를 **Picard 반복**(*Picard iteration*)이라 한다. 예를 들어 $y' = y$, $y(0)=1$에서 $y_0 = 1$로 시작하면 $y_k = \sum_{j \le k} t^j/j!$로 e^t의 Taylor 부분합이 차례로 나온다.

2.4 비유일성과 Peano 정리

정리 2.3 (Peano) f가 R에서 연속이기만 하면 $|t-t_0| \le h$에서 해가 적어도 하나 존재한다.

증명. Euler 꺾은선 근사들이 균등유계이고 동등연속(기울기가 M 이하)이므로 Arzelà–Ascoli 정리로 수렴하는 부분열을 뽑으면, 그 극한이 적분방정식을 만족함을 보일 수 있다. □

유일성은 보장되지 않는다. 앞 장의 $y' = y^{1/3}$, $y(0)=0$은 무한히 많은 해를 갖는다. 물리적으로는 "물통에서 물이 다 빠진 시각"을 현재 상태(빈 물통)만으로 알 수 없는 Torricelli 문제 $h' = -c\sqrt{h}$가 같은 유형이다.

역사. Picard–Lindelöf 정리는 Émile Picard와 Ernst Lindelöf의 이름을 땄고, Giuseppe Peano는 19세기 말에 연속성만으로 해의 존재를 보장하는 정리를 증명하였다.

2.5 Grönwall 부등식과 연속 의존성

보조정리 2.4 (Grönwall) 연속함수 $u \ge 0$이 $u(t) \le A + \int_{t_0}^{t} K\,u(s)\,\mathrm{d}s$ ($t \ge t_0$, $K \ge 0$ 상수)를 만족하면 $u(t) \le A e^{K(t-t_0)}$이다.

증명. 우변을 $U(t)$라 하면 $U(t_0) = A$이고 $u \le U$이므로 $U' = Ku \le KU$이다. 따라서 $(Ue^{-K(t-t_0)})' = e^{-K(t-t_0)}(U' - KU) \le 0$이고, $U(t)e^{-K(t-t_0)} \le U(t_0)$, 곧 $U(t) \le U(t_0)e^{K(t-t_0)} = Ae^{K(t-t_0)}$이다. $u(t) \le U(t)$이므로 결론을 얻는다. □

정리 2.5 (초기값에 대한 연속 의존성) f가 Lipschitz(상수 L)이면 같은 방정식의 두 해에 대해

$$\|y(t)-z(t)\| \le \|y(t_0)-z(t_0)\|\, e^{L|t-t_0|}$$

이다.

증명. 적분방정식의 차에 Grönwall 부등식을 적용하면 된다. □

특히 $y(t_0) = z(t_0)$이면 $y = z$이므로 이는 유일성의 다른 증명이기도 하다. 이 상계는 지수적으로 커질 수 있다. 유한 시간에서 해는 초기값에 연속적으로 의존하지만, 긴 시간에서는 작은 오차가

크게 자랄 수 있으며 이것이 제12권 제8장 혼돈의 출발점이다. f가 C^1이면 해는 초기값에 대해 미분가능하고, 그 도함수는 선형화된 방정식(**변분방정식**, *variational equation*)을 만족한다.

2.6 해의 연장과 폭발

정리 2.6 (연장 정리) f가 열린집합 $D \subseteq \mathbb{R} \times \mathbb{R}^n$에서 연속이고 국소적으로 Lipschitz이면 각 초기값 문제는 유일한 최대 해 $y : (\alpha, \omega) \to \mathbb{R}^n$을 갖는다. $\omega < \infty$이면 $t \uparrow \omega$일 때 $(t, y(t))$는 D의 모든 콤팩트 집합을 결국 벗어난다. 특히 $D = \mathbb{R} \times \mathbb{R}^n$이면 $\|y(t)\| \to \infty$이다.

예제 2.7 (유한 시간 폭발) $y' = 1 + y^2$, $y(0) = 0$의 해는 $y = \tan t$이고 최대 구간은 $(-\pi/2, \pi/2)$이다. 우변이 모든 곳에서 매끄러운데도 해가 유한 시간에 무한대로 간다. 우변이 y에 대해 선형보다 빨리 자라기 때문이다.

명제 2.8 $\|f(t,y)\| \le a(t) + b(t)\|y\|$이고 a, b가 연속이면 해는 a, b가 정의된 구간 전체로 연장된다.

증명. Grönwall 부등식으로 $\|y\|$가 유한 시간에 무한대로 갈 수 없기 때문이다. 제12권 제1장에서 선형 방정식의 해가 계수가 연속인 구간 전체에서 존재했던 이유이다. $\square$

2.7 연습문제와 해설

연습문제 2.9 $y' = t + y$, $y(0) = 1$의 Picard 반복 y_1, y_2, y_3을 구하고 정확한 해와 비교하라.

풀이. $y_0 = 1$이면 $y_1 = 1 + t + t^2/2$, $y_2 = 1 + t + t^2 + t^3/6$, $y_3 = 1 + t + t^2 + t^3/3 + t^4/24$이다. 정확한 해는 $y = 2e^t - t - 1 = 1 + t + t^2 + t^3/3 + t^4/12 + \cdots$이므로 반복마다 맞는 차수가 하나씩 늘어난다.

연습문제 2.10 $y' = y^2$, $y(0) = y_0 > 0$의 최대 해 구간을 구하라.

풀이. $y = \dfrac{y_0}{1 - y_0 t}$이므로 최대 구간은 $(-\infty, 1/y_0)$이다. 초기값이 클수록 빨리 폭발한다.

연습문제 2.11 $y' = \sqrt{|y|}$, $y(0) = 0$의 해는 유일한가? $y(0) = 1$이면 어떤가?

풀이. $y \equiv 0$과 $y = t^2/4$ $(t \ge 0)$, 0 $(t < 0)$가 모두 해이므로 유일하지 않다. $y(0) = 1$이면 $y > 0$ 근처에서 $\sqrt{y}$가 매끄러우므로 국소적으로 유일하다. 해 $y = (t/2 + 1)^2$은 $t \ge -2$에서 유효하며, $t = -2$에서 $y = 0$에 도달한 뒤 과거 방향으로는 다시 유일성이 깨진다.

연습문제 2.12 $x' = -y + x(1 - x^2 - y^2)$, $y' = x + y(1 - x^2 - y^2)$의 해가 모든 $t \ge 0$에서 존재함을 보여라.

풀이. $r^2 = x^2 + y^2$이면 $(r^2)' = 2r^2(1 - r^2)$이다. $r^2 \le 1$이면 r^2는 1을 넘지 않고, $r^2 > 1$이면 감소하므로 $r(t) \le \max(r(0), 1)$이다. 해가 유계 집합에 머무르므로 연장 정리로 미래 방향으로 끝없이 연장된다. 이 계는 제12권 제7장에서 극한주기 $r = 1$의 예로 다시 나온다.

다음 연결. 해의 존재가 보장되면 선형 방정식에서는 해 전체의 구조까지 알 수 있다. 다음 장에서는 고계 선형 방정식의 해공간과 그 계산법을 다룬다.

제 3 장

고계 선형 방정식과 급수해

개요 이 장은 n계 선형 방정식 $L[y] = y^{(n)} + a_{n-1}(t)y^{(n-1)} + \cdots + a_0(t)y = g(t)$의 해공간이 n차원임을 보이고, 상수계수 동차방정식의 특성방정식에 의한 풀이, 미정계수법과 매개변수 변화법에 의한 비동차항 처리, 공명 현상, 그리고 변수계수 방정식의 정칙점·정칙 특이점에서의 급수해(Frobenius 방법)를 차례로 정리한다. 선행 지식: 제12권 제2장의 존재·유일성, 제7권의 벡터공간과 차원(제7권 제2장, 제7권 제3장), 제11권의 복소지수함수(제11권 제2장).

3.1 해공간의 구조

$L[y] = y^{(n)} + a_{n-1}(t)y^{(n-1)} + \cdots + a_0(t)y$에서 계수들이 구간 I에서 연속이라 하자. L은 선형 연산자이므로 **동차방정식** $L[y] = 0$의 해 전체는 벡터공간이다.

> **정리 3.1** $L[y] = 0$의 해공간은 n차원이다. 비동차방정식 $L[y] = g$의 일반해는 특수해 하나와 동차해의 합이다.

증명. $t_0 \in I$를 고정하고 해 y에 초기값 벡터 $(y(t_0), \dots, y^{(n-1)}(t_0)) \in \mathbb{R}^n$을 대응시키는 사상은 선형이다. 제12권 제2장의 존재 정리로 이 사상은 전사이고, 유일성으로 단사이다. 따라서 해공간은 $\mathbb{R}^n$과 동형이다. $\square$

해 $y_1, \dots, y_n$의 **Wronski 행렬식**(*Wronskian*)을 $W = \det\big(y_j^{(i-1)}\big)_{i,j}$로 정의한다. 해들이 일차독립일 필요충분조건은 어떤 한 점(그리고 따라서 모든 점)에서 $W \neq 0$인 것이다. **Abel 공식** $W(t) = W(t_0)\exp\!\big(-\int_{t_0}^{t} a_{n-1}\big)$ 때문에 W는 항상 0이거나 결코 0이 아니다. 해가 아닌 일반 함수들에서는 이 이분법이 성립하지 않는다. t^2과 $t|t|$는 $\mathbb{R}$에서 일차독립인데 Wronski 행렬식이 항등적으로 0이다.

3.2 상수계수 동차방정식

a_k가 상수이면 $y = e^{\lambda t}$를 넣어 **특성방정식** $p(\lambda) = \lambda^n + a_{n-1}\lambda^{n-1} + \cdots + a_0 = 0$을 얻는다. $L = p(D)$, $D = \mathrm{d}/\mathrm{d}t$로 쓸 수 있다.

> **정리 3.2** p의 서로 다른 근 λ_j(중복도 m_j)에 대해 함수들 $t^k e^{\lambda_j t}$ $(0 \le k < m_j)$는 해공간의 기저이다.

증명. 핵심 계산은 $(D-\lambda)^m (t^k e^{\lambda t}) = 0$ $(k < m)$이다. $(D-\lambda)(e^{\lambda t}u) = e^{\lambda t}u'$이므로 $(D-\lambda)^m$을 $e^{\lambda t}u$에 적용하는 것은 u를 m번 미분하는 것과 같고, $u = t^k$를 $m > k$번 미분하면 0이다. 중복도의 합이 n이므로 이렇게 얻은 n개의 함수가 3.1의 n차원 해공간을 채우고, 서로 다른 지수함수 계열은 일차독립이므로 기저가 된다. $\square$

실계수 방정식의 복소근 $\alpha \pm i\beta$에 대해서는 실수부와 허수부를 취해 $e^{\alpha t}\cos\beta t$, $e^{\alpha t}\sin\beta t$를 쓴다.

예제 3.3 (감쇠 진동자) $my'' + cy' + ky = 0$ $(m, k > 0, c \geq 0)$의 특성근은 $\lambda = \dfrac{-c \pm \sqrt{c^2 - 4mk}}{2m}$이다. $\omega_0 = \sqrt{k/m}$, 감쇠비 $\zeta = \dfrac{c}{2\sqrt{mk}}$로 쓰면

- $\zeta > 1$ (과감쇠): 두 음의 실근, 진동 없이 감소.
- $\zeta = 1$ (임계감쇠): 중근 $-\omega_0$, $y = (A + Bt)e^{-\omega_0 t}$. 진동 없이 가장 빨리 평형으로 돌아온다.
- $0 < \zeta < 1$ (부족감쇠): $y = e^{-\zeta\omega_0 t}(A\cos\omega_d t + B\sin\omega_d t)$, $\omega_d = \omega_0\sqrt{1-\zeta^2}$.

RLC 직렬회로 $Lq'' + Rq' + q/C = 0$은 $m \to L$, $c \to R$, $k \to 1/C$로 같은 방정식이다.

3.3 비동차항: 미정계수법

$g(t)$가 $t^k e^{\mu t}$, $e^{\alpha t}\cos\beta t$ 같은 함수들의 결합이면 같은 꼴의 특수해를 추측하는 **미정계수법**(*method of undetermined coefficients*)을 쓴다. μ가 특성근이 아니면 g와 같은 꼴, 중복도 s인 특성근이면 t^s를 곱한 꼴로 둔다.

예제 3.4 $y'' + y = 3\cos 2t$: $y_p = A\cos 2t$를 넣으면 $(-4A + A)\cos 2t = 3\cos 2t$, $-3A = 3$, $A = -1$이다. 일반해는 $y = c_1\cos t + c_2\sin t - \cos 2t$이다.

3.4 공명

$y'' + \omega_0^2 y = F_0\cos\omega t$에서 $\omega \neq \omega_0$이면 $y_p = \dfrac{F_0}{\omega_0^2 - \omega^2}\cos\omega t$이다. $\omega \to \omega_0$에서 진폭이 발산한다. $\omega = \omega_0$이면 $\pm i\omega_0$가 특성근이므로 t를 곱한 꼴로 두어

$$y_p = \frac{F_0}{2\omega_0}\, t\sin\omega_0 t$$

를 얻는다. 감쇠가 없으면 진폭이 선형으로 자란다. 감쇠 $2\zeta\omega_0 y'$이 있으면 정상상태 진폭은

$$|Y(\omega)| = \frac{F_0}{\sqrt{(\omega_0^2 - \omega^2)^2 + (2\zeta\omega_0\omega)^2}}$$

로 유계이며, $\zeta < 1/\sqrt{2}$일 때 $\omega_r = \omega_0\sqrt{1 - 2\zeta^2}$에서 최대가 된다. **공진 주파수** ω_r, **감쇠 진동수** ω_d, **고유진동수** ω_0는 서로 다른 양이므로 구분해야 한다.

3.5 매개변수 변화법

계수가 변수이거나 g가 특수한 꼴이 아니면 **매개변수 변화법**(*variation of parameters*)을 쓴다. 2계 $y'' + p(t)y' + q(t)y = g(t)$에서 동차해 y_1, y_2와 Wronskian W가 있으면

$$y_p(t) = -y_1(t)\int \frac{y_2 g}{W}\,\mathrm{d}t + y_2(t)\int \frac{y_1 g}{W}\,\mathrm{d}t$$

이다. $y_p = u_1 y_1 + u_2 y_2$로 두고 자유도를 줄이는 조건 $u_1' y_1 + u_2' y_2 = 0$을 부과하면, $y_p' = u_1 y_1' + u_2 y_2'$이고 $y_p'' = u_1' y_1' + u_2' y_2' + u_1 y_1'' + u_2 y_2''$이며, 이를 원래 방정식에 넣고 y_1, y_2가 동차해임을 쓰면

$u_1'y_1' + u_2'y_2' = g$를 얻는다. 두 조건 $u_1'y_1 + u_2'y_2 = 0$, $u_1'y_1' + u_2'y_2' = g$를 u_1', u_2'에 대해 Cramer 공식으로 풀면 위 식이 나온다.

> **예제 3.5** $y'' + y = \sec t$ $(|t| < \pi/2)$: $y_1 = \cos t$, $y_2 = \sin t$, $W = 1$이므로
>
> $$y_p = -\cos t \int \tan t \, dt + \sin t \int 1 \, dt = \cos t \log\cos t + t \sin t$$
>
> 이다. 미정계수법으로는 얻을 수 없는 특수해이다.

3.6 급수해와 Frobenius 방법

계수가 해석적인 점 t_0(**정칙점**, *ordinary point*) 근처에서는 해도 해석적이며, 해의 수렴반지름은 적어도 t_0에서 계수의 가장 가까운 복소 특이점까지의 거리이다. 해를 $y = \sum_{k} c_k (t - t_0)^k$로 두고 계수의 점화식을 푼다.

> **예제 3.6 (Airy 방정식)** $y'' = ty$에 $y = \sum_k c_k t^k$를 넣으면 $(k+2)(k+1)c_{k+2} = c_{k-1}$ $(k \ge 1)$, $c_2 = 0$이다. c_0, c_1이 자유이고 $c_3 = c_0/6$, $c_4 = c_1/12$, ...이다. 계수가 다항식이므로 해는 전해석함수이다.

$t_0 = 0$이 **정칙 특이점**(*regular singular point*, 곧 $t^2y'' + tP(t)y' + Q(t)y = 0$에서 P, Q가 해석적)이면 $y = t^r \sum_k c_k t^k$ $(c_0 \neq 0)$로 둔다. 최저차 항에서 **지표방정식** $r(r-1) + P(0)r + Q(0) = 0$을 얻는다. 두 근의 차가 정수가 아니면 두 개의 Frobenius 급수해가 있고, 정수이면 둘째 해에 $\log t$ 항이 나타날 수 있다.

> **예제 3.7 (Bessel 방정식)** $t^2y'' + ty' + (t^2 - \nu^2)y = 0$의 지표방정식은 $r^2 - \nu^2 = 0$이다. $r = \nu \ge 0$인 해는
>
> $$J_\nu(t) = \sum_{k \ge 0} \frac{(-1)^k}{k!\,\Gamma(k + \nu + 1)} \left(\frac{t}{2}\right)^{2k+\nu}$$
>
> 이다. ν가 정수가 아니면 $J_{-\nu}$가 둘째 독립해이고, 정수 n이면 $J_{-n} = (-1)^n J_n$이라 독립이 아니므로 로그항을 포함한 Neumann 함수 Y_n을 쓴다. 원형 막의 진동, 원통 도파관의 모드, FM 신호의 스펙트럼에 나타난다.

역사. 급수해의 정칙 특이점 분류와 지표방정식에 의한 방법은 1873년 Ferdinand Georg Frobenius의 논문에서 체계화되었고, 그 이름을 땄다. Bessel 함수는 Friedrich Bessel이 1824년에 행성 운동의 섭동 문제를 다루면서 연구하였다.

3.7 연습문제와 해설

> **연습문제 3.8** $y''' - y' = 0$의 일반해와 $y(0) = 0$, $y'(0) = 1$, $y''(0) = 2$인 해를 구하라.

풀이. 특성근 $0, \pm 1$이므로 $y = c_1 + c_2 e^{t} + c_3 e^{-t}$이다. 조건에서 $c_1 + c_2 + c_3 = 0$, $c_2 - c_3 = 1$, $c_2 + c_3 = 2$이므로 $c_2 = 3/2$, $c_3 = 1/2$, $c_1 = -2$이다.

> **연습문제 3.9** $y'' - 2y' + y = e^{t}$의 특수해를 구하라.

풀이. 1이 2중 특성근이므로 $y_p = At^2e^t$ 로 둔다. $(D-1)^2(t^2e^t) = e^t(t^2)'' = 2e^t$ 이므로 $A = 1/2$, $y_p = \dfrac{1}{2}t^2e^t$ 이다.

연습문제 3.10 $y_1 = t$가 $t^2y'' - 2ty' + 2y = 0$ $(t>0)$의 해임을 확인하고 둘째 해를 구하라.

풀이. $y_1 = t$를 넣으면 $t^2\cdot 0 - 2t\cdot 1 + 2t = 0$이다. 이는 Euler 방정식이므로 $y = t^r$ 에서 $r(r-1)-2r+2 = (r-1)(r-2) = 0$이고, 둘째 해는 t^2이다. 일반적으로는 $y_2 = y_1\int e^{-\int p}/y_1^2\,\mathrm{d}t$(차수 낮추기)로 구하며, 표준형의 $p = -2/t$이므로 $y_2 = t\displaystyle\int \frac{t^2}{t^2}\,\mathrm{d}t = t^2$이다.

연습문제 3.11 $(1+t^2)y''+y=0$의 $t=0$ 중심 급수해의 수렴반지름이 적어도 얼마인지 말하라.

풀이. 표준형 계수 $1/(1+t^2)$의 복소 특이점은 $\pm i$이고 원점에서의 거리는 1이다. 따라서 수렴반지름은 적어도 1이다. 실수축 위에는 특이점이 없는데도 반지름이 제한될 수 있다는 점이 복소해석(제11권 제2장)의 관점이다.

다음 연결. 고계 방정식은 1계 연립 방정식과 같다. 다음 장에서는 연립 선형계를 행렬지수로 풀고 평면 상평면의 궤도를 분류한다.

제 4 장

선형계와 행렬지수, 상평면

개요 이 장은 연립 선형 방정식 $x' = Ax$의 해를 행렬지수 e^{tA}로 직접 적분하는 방법을 세우고, 평면에서 원점 근처 궤도의 모양을 A의 고유값만으로 완전히 분류한다. 안정성의 엄밀한 정의와 그 선형계에서의 판정 조건을 정리한 뒤, 결합 진동자의 정규 모드를 예로 든다. 이 분류는 제12권 제6장에서 비선형계의 평형점을 분석하는 기준이 된다. 선행 지식: 제12권 제3장의 선형 방정식, 제7권의 고유값·대각화와 Jordan 구조(제7권 제7장).

4.1 행렬지수

정사각행렬 A에 대해

$$e^{tA} = \sum_{k \ge 0} \frac{t^k A^k}{k!}$$

는 모든 t에서 절대수렴하고($\|A^k\| \le \|A\|^k$), 항별 미분으로 $\frac{\mathrm{d}}{\mathrm{d}t} e^{tA} = A e^{tA}$이다. 따라서 $x(t) = e^{tA}x_0$가 $x' = Ax$, $x(0) = x_0$의 유일한 해이다.

명제 4.1 $AB = BA$이면 $e^{A+B} = e^A e^B$이다. 일반적으로는 성립하지 않는다.

증명. $AB = BA$이면 이항정리가 행렬에 그대로 적용되어 $(A+B)^k = \sum_{j=0}^{k} \binom{k}{j} A^j B^{k-j}$이고, 이를 지수급수에 대입해 Cauchy 곱으로 정리하면 $e^{A+B} = e^A e^B$를 얻는다. 교환하지 않는 반례로

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

을 들 수 있다. $A^2 = B^2 = 0$이므로 $e^A = I + A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $e^B = I + B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$이고

$$e^A e^B = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

이다. 한편 $M = A + B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$은 $M^2 = I$를 만족하므로 $e^{tM} = \cosh(t) I + \sinh(t) M$이고, $t = 1$에서

$$e^{A+B} = \begin{pmatrix} \cosh 1 & \sinh 1 \\ \sinh 1 & \cosh 1 \end{pmatrix}$$

이다. 두 결과가 다르므로 $e^A e^B \ne e^{A+B}$이다. 양자역학의 Baker–Campbell–Hausdorff 공식이 이 차이를 다룬다. $\square$

4.2 행렬지수의 계산

- 대각화 가능 $A = PDP^{-1}$: $e^{tA} = P\,\mathrm{diag}(e^{\lambda_1 t}, \dots, e^{\lambda_n t})\,P^{-1}$.
- **Jordan 블록** $J = \lambda I + N$, $N^m = 0$: λI와 N이 교환하므로 $e^{tJ} = e^{\lambda t}\sum_{k<m} \dfrac{t^k N^k}{k!}$.
- 일반적으로 e^{tA}의 성분은 $t^k e^{\lambda t}$ 꼴 함수들의 결합이며, 고유값의 실수부가 장기 행동을 결정한다.

예제 4.2 $A = \begin{pmatrix} 0 & -\omega \\ \omega & 0 \end{pmatrix}$이면 $A^2 = -\omega^2 I$이므로 급수를 짝수·홀수 항으로 나누어

$$e^{tA} = \cos(\omega t) I + \frac{\sin(\omega t)}{\omega} A = \begin{pmatrix} \cos\omega t & -\sin\omega t \\ \sin\omega t & \cos\omega t \end{pmatrix}$$

를 얻는다. 회전행렬이며, 복소수 $e^{i\omega t}$를 곱하는 사상의 실수 표현이다.

4.3 비동차계와 기본행렬

$x' = Ax + g(t)$의 해는 상수변화(**Duhamel 공식**, *Duhamel's formula*)

$$x(t) = e^{tA}x_0 + \int_0^t e^{(t-s)A} g(s)\ \mathrm{d}s$$

이다. 계수가 시간에 의존하는 $x' = A(t)x$에서는 $e^{\int A}$가 일반적으로 해가 아니다($A(t)$들이 서로 다른 시각에 교환하지 않으면). 대신 독립해들을 열로 갖는 **기본행렬**(*fundamental matrix*) $\Phi(t)$를 쓰고 $x(t) = \Phi(t)\Phi(t_0)^{-1}x_0$로 쓴다. 주기 계수 $A(t+T) = A(t)$의 경우 **Floquet 이론**이 $\Phi(t) = P(t)e^{tB}$ (P는 주기 T)로 구조를 준다.

4.4 평면 선형계의 분류

$x' = Ax$, $A \in M_2(\mathbb{R})$, $\det A \neq 0$이면 원점이 유일한 평형점이다. $\tau = \mathrm{tr}\,A$, $\Delta = \det A$로 두면 고유값은 $\lambda = \dfrac{\tau \pm \sqrt{\tau^2 - 4\Delta}}{2}$이다.

표 4.1 평면 선형계 $x' = Ax$의 원점 근처 궤도 분류

조건	고유값	원점의 유형
$\Delta < 0$	부호가 다른 실수	안장점(불안정)
$\Delta > 0$, $\tau^2 > 4\Delta$	같은 부호의 실수	마디: $\tau < 0$ 안정, $\tau > 0$ 불안정
$\Delta > 0$, $\tau^2 < 4\Delta$, $\tau \neq 0$	켤레 복소수	나선: $\tau < 0$ 안정, $\tau > 0$ 불안정
$\Delta > 0$, $\tau = 0$	순허수	중심(안정이지만 점근안정은 아님)
$\tau^2 = 4\Delta$	중근	퇴화 마디 또는 별 마디

안장점(*saddle point*)에서는 음의 고유값의 고유벡터 방향(**안정 다양체**, *stable manifold*)으로 들어오는 궤도만 원점으로 가고, 나머지는 멀어진다. **나선**(*spiral*)의 회전 방향은 A의 비대각

성분 부호로 정해진다. 예를 들어 점 $(1,0)$에서의 속도 (a_{11}, a_{21})의 둘째 성분이 양수이면 반시계 방향이다.

4.5 안정성의 정의와 선형계의 판정

평형점 0이 **안정**하다는 것은 모든 $\varepsilon > 0$에 대해 $\delta > 0$이 있어 $\|x(0)\| < \delta$이면 모든 $t \ge 0$에서 $\|x(t)\| < \varepsilon$이라는 뜻이다. 안정하고 근처의 해가 0으로 수렴하면 **점근안정**(*asymptotically stable*)이라 한다.

> **정리 4.3** $x' = Ax$에서 0이 점근안정할 필요충분조건은 A의 모든 고유값의 실수부가 음수인 것이다. 실수부가 양수인 고유값이 있으면 불안정하다. 실수부가 0인 고유값이 있으면, 그 고유값들의 Jordan 블록이 모두 1×1일 때만 안정하다.

마지막 조건은 t^k 인자 때문이다. $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$이면 $x_1 = x_1(0) + t x_2(0)$이 선형으로 자라 불안정하다. 다항식의 근을 직접 구하지 않고 실수부의 부호를 판정하는 **Routh–Hurwitz 판정법**이 제어공학에서 쓰인다. 2차 특성다항식 $\lambda^2 + a_1\lambda + a_0$에서는 $a_1 > 0$, $a_0 > 0$이 점근안정 조건이다.

4.6 결합 진동자와 정규 모드

질량 m인 두 물체가 용수철 상수 k인 벽 용수철과 중간 용수철 κ로 연결되면

$$m\ddot{x}_1 = -kx_1 - \kappa(x_1 - x_2), \qquad m\ddot{x}_2 = -kx_2 - \kappa(x_2 - x_1),$$

곧

$$\ddot{\mathbf{x}} = -K\mathbf{x}, \qquad K = \frac{1}{m}\begin{pmatrix} k+\kappa & -\kappa \\ -\kappa & k+\kappa \end{pmatrix}$$

이다. K의 고유벡터 $(1,1)$, $(1,-1)$은 각각 같은 방향 진동과 반대 방향 진동인 **정규 모드**(*normal mode*)이며, 진동수는 각각 $\sqrt{k/m}$, $\sqrt{(k+2\kappa)/m}$이다. 일반 운동은 두 정규 모드의 중첩이다. 두 진동수가 가까우면 맥놀이(*beat*)가 생겨 에너지가 두 물체 사이를 오간다.

4.7 연습문제와 해설

> **연습문제 4.4** $A = \begin{pmatrix} 1 & 1 \\ 4 & 1 \end{pmatrix}$에 대해 e^{tA}를 구하고 원점의 유형을 판정하라.

풀이. 고유값은 3(고유벡터 $(1,2)$)과 -1(고유벡터 $(1,-2)$)이다. 대각화하면

$$e^{tA} = \frac{1}{4}\begin{pmatrix} 2e^{3t} + 2e^{-t} & e^{3t} - e^{-t} \\ 4e^{3t} - 4e^{-t} & 2e^{3t} + 2e^{-t} \end{pmatrix}$$

이다. $\Delta = -3 < 0$이므로 안장점이다.

연습문제 4.5 $x' = \begin{pmatrix} -1 & 2 \\ -2 & -1 \end{pmatrix} x$의 원점은 어떤 유형이며 회전 방향은 어느 쪽인가?

풀이. 고유값 $-1 \pm 2i$이므로 안정 나선이다. 점 $(1,0)$에서 속도는 $(-1,-2)$로 둘째 성분이 음수이므로 시계 방향으로 돈다.

연습문제 4.6 $x'' + \varepsilon x' + x = 0$을 1계 계로 바꾸고 ε의 부호에 따른 원점의 유형을 말하라.

풀이. $(x, v)' = (v, -x - \varepsilon v)$에서 $\tau = -\varepsilon$, $\Delta = 1$이다. $0 < \varepsilon < 2$이면 안정 나선, $\varepsilon \geq 2$이면 안정 마디(경계 $\varepsilon = 2$는 퇴화 마디), $\varepsilon = 0$이면 중심, $-2 < \varepsilon < 0$이면 불안정 나선, $\varepsilon \leq -2$이면 불안정 마디이다.

연습문제 4.7 $A^2 = A$(사영행렬)이면 $e^{tA} = I + (e^t - 1)A$임을 보여라.

풀이. $k \geq 1$에서 $A^k = A$이므로 $e^{tA} = I + \sum_{k \geq 1} \frac{t^k}{k!} A = I + (e^t - 1)A$이다.

다음 연결. 선형 미분방정식을 대수 문제로 바꾸는 또 다른 도구가 Laplace 변환이다. 다음 장에서는 초기값 문제와 회로·제어의 전달함수를 이 변환으로 다룬다.

제 5 장

Laplace 변환과 전달함수

개요 **Laplace 변환**(*Laplace transform*)은 $t \ge 0$에서 정의된 함수를 복소변수 s의 함수로 바꾸는 적분변환이며, 미분을 s를 곱하는 대수 연산으로 바꾸므로 초기값이 주어진 선형 상수계수 방정식을 대수 방정식으로 바꾸어 푼다. 이 장은 변환의 정의와 존재 조건, 미분·이동·합성곱 등 기본 성질을 정리하고, 이를 이용해 초기값 문제와 불연속·임펄스 입력을 갖는 문제를 푼다. 이어서 회로·제어에서 쓰는 전달함수, 임펄스 응답, BIBO 안정성, 주파수 응답과 극한값 정리를 다룬다. 선행 지식: 제12권 제3장, 제12권 제4장의 선형 방정식, 제8권의 이상적분(제8권 제5장), 제11권의 유수 정리(제11권 제6장, 역변환 공식).

5.1 정의와 존재 조건

$t \ge 0$에서 정의된 함수 f의 **Laplace 변환**은

$$F(s) = \mathcal{L}\{f\}(s) = \int_0^{\infty} f(t) e^{-st}\, \mathrm{d}t$$

이다. f가 조각마다 연속이고 **지수 차수**(*exponential order*, $|f(t)| \le M e^{at}$)이면 $\operatorname{Re} s > a$에서 적분이 절대수렴하고 F는 그 반평면에서 정칙이다. e^{t^2}은 지수 차수가 아니므로 Laplace 변환이 없다.

표 5.1 기본 Laplace 변환 쌍

$f(t)$	$F(s)$
1	$1/s$
t^n	$n!/s^{n+1}$
e^{at}	$1/(s-a)$
$\cos \omega t,\ \sin \omega t$	$s/(s^2+\omega^2),\ \omega/(s^2+\omega^2)$
$u(t-c)$ (단위계단)	e^{-cs}/s
$\delta(t-c)$ $(c \ge 0)$	e^{-cs}

5.2 기본 성질

- 미분: $\mathcal{L}\{f'\} = sF(s) - f(0)$, $\mathcal{L}\{f''\} = s^2F - sf(0) - f'(0)$.
- s-이동: $\mathcal{L}\{e^{at} f(t)\} = F(s-a)$.
- t-이동: $\mathcal{L}\{u(t-c) f(t-c)\} = e^{-cs}F(s)$ $(c \ge 0)$.
- t를 곱하기: $\mathcal{L}\{t f(t)\} = -F'(s)$.

- **합성곱**(*convolution*): $(f*g)(t)=\int_0^t f(\tau)g(t-\tau)\,d\tau$이면 $\mathcal{L}\{f*g\}=FG$.

미분 공식은 부분적분 $\int_0^\infty f'e^{-st}=[fe^{-st}]_0^\infty+s\int fe^{-st}$에서 나오며, 초기값이 자동으로 들어간다는 점이 이 방법의 장점이다. 합성곱 공식은 제10권 제6장의 Fubini 정리로 증명한다.

5.3 초기값 문제의 풀이

예제 5.1 $y''+4y'+3y=0$, $y(0)=1$, $y'(0)=0$. 변환하면 $(s^2Y-s)+4(sY-1)+3Y=0$, 곧

$$Y=\frac{s+4}{(s+1)(s+3)}=\frac{3/2}{s+1}-\frac{1/2}{s+3}$$

이다. 따라서 $y=\frac{3}{2}e^{-t}-\frac{1}{2}e^{-3t}$이다.

역변환은 부분분수와 표를 쓴다. 일반적으로는 **Bromwich 적분**

$$f(t)=\frac{1}{2\pi i}\int_{\gamma-i\infty}^{\gamma+i\infty}F(s)e^{st}\,ds$$

(γ는 F의 모든 특이점보다 오른쪽)으로 주어지며, 유리함수 F에서는 왼쪽으로 닫는 경로에 유수정리를 쓰면 $f(t)=\sum \operatorname{Res}\big(F(s)e^{st}\big)$이다. 이는 부분분수 계산과 같은 결과이다. 연속함수에 대해 Laplace 변환은 단사이므로(**Lerch 정리**) 역변환은 연속인 해에 대해 유일하다.

역사. 초기값 문제를 대수 방정식으로 바꾸어 푸는 조작 방법은 1890년대에 Oliver Heaviside가 전신 회로 해석을 위해 고안한 연산자 미적분에서 비롯되었다. 이를 Laplace 변환의 복소적분(Bromwich 적분)으로 엄밀하게 정당화한 사람이 Thomas John I'Anson Bromwich이다.

5.4 불연속 입력과 임펄스

예제 5.2 (**스위치를 켜는 입력**) $y'+y=u(t-1)$, $y(0)=0$. $Y=\dfrac{e^{-s}}{s(s+1)}=e^{-s}\left(\dfrac{1}{s}-\dfrac{1}{s+1}\right)$이므로

$$y=u(t-1)\big(1-e^{-(t-1)}\big)$$

이다. $t<1$에서는 0이고, 입력이 켜진 뒤 지수적으로 1에 접근한다.

Dirac 델타는 함수가 아니라 $\int \delta(t-c)\varphi(t)\,dt=\varphi(c)$로 정의되는 분포(*distribution*, 제13권 제8장)이다. 넓이 1인 좁은 사각 펄스의 극한으로 생각할 수 있다. $y''+\omega^2y=\delta(t)$, $y(0^-)=y'(0^-)=0$의 해는 $y=u(t)\dfrac{\sin\omega t}{\omega}$이다. 순간적인 충격이 속도를 0에서 1로 바꾸고 위치는 연속이다. δ가 있는 문제에서는 $t=0^-$와 0^+의 초기값을 구분해야 한다.

5.5 전달함수와 임펄스 응답

선형 시불변계 $a_ny^{(n)}+\cdots+a_0y=b_mu^{(m)}+\cdots+b_0u$에서 모든 초기값이 0이면 $Y(s)=H(s)U(s)$,

$$H(s)=\frac{b_ms^m+\cdots+b_0}{a_ns^n+\cdots+a_0}$$

이다. H를 **전달함수**(*transfer function*)라 한다. $u=\delta$이면 $Y=H$이므로 $h=\mathcal{L}^{-1}\{H\}$는 **임펄스 응답**(*impulse response*)이고, 일반 입력에 대한 응답은 합성곱 $y=h*u$이다.

- H의 극은 특성방정식의 근이다(분자와 공통인 인수가 없을 때). $m\le n$인 진분수 전달함수의 모든 극이 왼쪽 반평면에 있으면 유계 입력에 대한 출력이 유계(**BIBO 안정**, *bounded-input bounded-output stability*)이다. $m>n$이면 미분기 $H=s$처럼 유계 입력 $\sin(t^2)$에 비유계 출력 $2t\cos(t^2)$을 줄 수 있으므로 BIBO 안정이 아니다.
- 정상상태 정현파 응답: 안정계에 $u=\cos\omega t$를 넣으면 과도 응답이 사라진 뒤 출력은

$$y_{\mathrm{ss}}(t)=|H(i\omega)|\cos\bigl(\omega t+\arg H(i\omega)\bigr)$$

  에 접근한다. $H(i\omega)$가 **주파수 응답**(*frequency response*)이며 **Bode 선도**는 $20\log_{10}|H(i\omega)|$와 $\arg H(i\omega)$를 $\log\omega$에 대해 그린 것이다.

> **예제 5.3 (RC 저역통과 필터)** $RCv'+v=u$의 전달함수는 $H(s)=\dfrac{1}{1+sRC}$이다. 차단주파수 $\omega_c=1/RC$에서 $|H|=1/\sqrt{2}$(약 -3 dB), 위상 -45°이다. $\omega\gg\omega_c$에서 이득은 10배 주파수마다 20 dB씩 감소한다.

5.6 극한값 정리

$sF(s)$의 극이 모두 왼쪽 반평면에 있으면 **최종값 정리** $\lim_{t\to\infty}f(t)=\lim_{s\to0}sF(s)$가 성립한다. 조건 없이 쓰면 틀린다. $f=e^{t}$이면 $sF=s/(s-1)\to0$이지만 $f\to\infty$이고, $f=\sin t$이면 $sF\to0$이지만 f는 수렴하지 않는다. **초기값 정리** $f(0^{+})=\lim_{s\to\infty}sF(s)$는 f가 0^{+}에서 극한을 가지면 성립한다.

5.7 연습문제와 해설

> **연습문제 5.4** $y''+y=\sin t$, $y(0)=y'(0)=0$을 Laplace 변환으로 풀어라.

풀이. $Y=\dfrac{1}{(s^2+1)^2}$이다. $\mathcal{L}\{\sin t-t\cos t\}=\dfrac{1}{s^2+1}-\dfrac{s^2-1}{(s^2+1)^2}=\dfrac{2}{(s^2+1)^2}$이므로 $y=\dfrac{1}{2}(\sin t-t\cos t)$이다. 공명으로 진폭이 t에 비례해 자란다.

> **연습문제 5.5** $\mathcal{L}\{te^{-2t}\cos t\}$를 구하라.

풀이. $\mathcal{L}\{t\cos t\}=-\frac{\mathrm{d}}{\mathrm{d}s}\dfrac{s}{s^2+1}=\dfrac{s^2-1}{(s^2+1)^2}$이고, s-이동으로 $\dfrac{(s+2)^2-1}{((s+2)^2+1)^2}$이다.

> **연습문제 5.6** $H(s)=\dfrac{1}{s^2+2s+5}$인 계의 단위계단 응답의 최종값과 감쇠비를 구하라.

풀이. 극 $-1\pm2i$는 왼쪽 반평면이므로 최종값 정리로 $\lim_{s\to0}s\cdot\dfrac{H(s)}{s}=H(0)=\dfrac{1}{5}$이다. $s^2+2\zeta\omega_n s+\omega_n^2$과 비교하면 $\omega_n=\sqrt{5}$, $\zeta=1/\sqrt{5}\approx0.447$이다.

> **연습문제 5.7** 적분방정식 $y(t)=t+\displaystyle\int_0^t\sin(t-\tau)y(\tau)\,\mathrm{d}\tau$를 풀어라.

풀이. 합성곱이므로 $Y = \dfrac{1}{s^2} + \dfrac{Y}{s^2+1}$, 곧 $Y\dfrac{s^2}{s^2+1} = \dfrac{1}{s^2}$, $Y = \dfrac{s^2+1}{s^4} = \dfrac{1}{s^2} + \dfrac{1}{s^4}$ 이다. $y = t + t^3/6$이다.

다음 연결. 지금까지는 대부분 선형 방정식이었다. 다음 장부터는 비선형계로 넘어가, 공식 없이 평형점의 안정성을 판정하는 선형화와 Lyapunov 방법을 다룬다.

제 6 장

비선형계의 평형점과 안정성

개요 이 장은 자율계 $x' = f(x)$의 평형점 근처 행동을, 그 점에서의 Jacobi 행렬로 얻는 선형화로 판정하는 정리와 그 판정이 실패하는 경우(쌍곡이 아닌 평형점)의 한계를 정리한다. 이어서 해를 직접 풀지 않고 에너지류의 함수 V만으로 안정성을 보이는 Lyapunov 방법과 LaSalle 불변원리를 다루고, 진자와 경쟁 모형을 예로 든다. 선행 지식: 제12권 제4장의 평면 선형계 분류, 제9권의 Jacobi 행렬과 Taylor 정리(제9권 제2장, 제9권 제3장).

6.1 자율계와 상공간

$x' = f(x)$, $x \in \mathbb{R}^n$ 처럼 우변이 시간에 직접 의존하지 않는 계를 **자율계**(*autonomous system*)라 한다. 해 곡선을 상공간(*phase space*)에 그린 것이 **궤도**(*orbit, trajectory*)이다. 자율계에서는 $x(t)$가 해이면 $x(t+c)$도 해이므로, 유일성이 성립하는 한 서로 다른 궤도는 교차하지 않는다. $f(x^*) = 0$인 점이 **평형점**(*equilibrium point*)이다. 2차원에서는 $\dfrac{\mathrm{d}y}{\mathrm{d}x} = \dfrac{g(x,y)}{f(x,y)}$로 시간을 소거하여 궤도의 방정식을 얻을 수 있다.

6.2 선형화와 Hartman–Grobman 정리

f가 C^1이고 x^*가 평형점이면 $u = x - x^*$에 대해 $u' = Df(x^*)u + o(\|u\|)$이다. $A = Df(x^*)$를 **선형화 행렬**(*linearization*)이라 한다.

> **정리 6.1 (선형화에 의한 안정성)** A의 모든 고유값의 실수부가 음수이면 x^*는 점근안정하다. 실수부가 양수인 고유값이 하나라도 있으면 불안정하다.

> **정리 6.2 (Hartman–Grobman)** A의 고유값 중 실수부가 0인 것이 없으면(**쌍곡 평형점**, *hyperbolic equilibrium*), x^* 근처의 궤도들은 선형계 $u' = Au$의 원점 근처 궤도들과 위상동형으로 대응한다.

이 두 정리는 쌍곡 평형점에서 비선형계의 국소적 상모양이 선형화와 정성적으로 같음을 보장하지만, 증명은 상당한 해석적 준비(안정·불안정 다양체 정리)를 필요로 하므로 생략한다. 쌍곡이 아닌 경우 선형화는 결론을 주지 않는다. 선형화가 중심(순허수 고유값)이면 비선형계는 중심일 수도, 안정 나선이나 불안정 나선일 수도 있다.

> **예제 6.3 (선형화가 결론을 주지 못하는 중심)** $x' = -y + \mu x(x^2+y^2)$, $y' = x + \mu y(x^2+y^2)$의 원점에서 선형화는 회전(중심)이다. 그러나 $r^2 = x^2 + y^2$에 대해
>
> $$(r^2)' = 2xx' + 2yy' = -2xy + 2\mu x^2(x^2+y^2) + 2xy + 2\mu y^2(x^2+y^2) = 2\mu r^4$$
>
> 이므로 $\mu < 0$이면 안정 나선, $\mu > 0$이면 불안정 나선, $\mu = 0$이면 중심이다. 같은 선형화가 세 가지 다른 행동을 낳는다.

6.3 예: 진자

$\theta'' + \sin\theta = 0$을 $x = \theta$, $y = \theta'$로 쓰면 $x' = y$, $y' = -\sin x$이다. 평형점은 $(k\pi, 0)$ $(k \in \mathbb{Z})$이다.

- $(0,0)$: $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, 중심. 선형화만으로는 판정이 안 된다.
- $(\pi,0)$: $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\Delta = -1 < 0$이므로 안장점(거꾸로 선 진자).

에너지 $E = \tfrac{1}{2}y^2 - \cos x$는 $E' = yy' + \sin x\, x' = 0$으로 보존된다. 원점 근처의 등위곡선은 닫힌 곡선이므로 $(0,0)$은 실제로 중심이다. $E = 1$인 곡선(**분리선**, *separatrix*)이 진동하는 궤도와 회전하는 궤도를 나눈다. 감쇠 $-\gamma y$를 더하면 $E' = -\gamma y^2 \le 0$이 되어 원점이 점근안정이 된다.

6.4 Lyapunov 방법

> **정리 6.4 (Lyapunov)** x^*의 근방 U에서 C^1 함수 V가 $V(x^*) = 0$, $x \neq x^*$에서 $V(x) > 0$을 만족한다고 하자. $\dot V(x) = \nabla V(x)\cdot f(x)$에 대해
> (1) U에서 $\dot V \le 0$이면 x^*는 안정하다.
> (2) $U \setminus \{x^*\}$에서 $\dot V < 0$이면 x^*는 점근안정하다.

증명의 뼈대. (1) 작은 구면 $\|x - x^*\| = \varepsilon$ 위의 V의 최솟값 $m > 0$을 잡고, $V < m$인 x^*의 근방에서 출발한 해는 V가 증가하지 않으므로 그 구면에 도달할 수 없다. (2) $V(x(t))$는 감소하여 극한 $c \ge 0$을 갖는다. $c > 0$이면 해가 $\{V \ge c\}$와 작은 공 안에 머무는 콤팩트 집합에서 $\dot V \le -\eta < 0$이 되어 $V \to -\infty$가 되므로 모순이다. $\square$

$\dot V$를 계산할 때 해를 알 필요가 없다는 것이 핵심이다. 적절한 V를 찾는 일반 방법은 없지만 물리계에서는 에너지가 좋은 후보이다.

역사. 해를 구하지 않고 에너지류의 함수만으로 안정성을 판정하는 이 방법은 Aleksandr Lyapunov가 1892년에 쓴 박사학위 논문 「운동의 안정성에 관한 일반 문제」에서 비롯되었다.

> **정리 6.5 (LaSalle 불변원리)** 콤팩트 양불변집합 K에서 $\dot V \le 0$이면 K에서 출발한 해는 $\{x \in K : \dot V(x) = 0\}$에 포함된 가장 큰 불변집합으로 접근한다.

감쇠 진자에서 $\dot V = -\gamma y^2$은 $y = 0$ 전체에서 0이라 Lyapunov 정리의 (2)를 직접 쓸 수 없다. 그러나 $y = 0$에 머무는 궤도는 $y' = -\sin x = 0$이어야 하므로 평형점뿐이고, LaSalle 원리로 원점 근처의 해가 원점으로 수렴함을 얻는다.

6.5 경쟁 모형의 예

두 종의 경쟁 모형 $x' = x(3 - x - 2y)$, $y' = y(2 - x - y)$의 평형점은 $(0,0)$, $(3,0)$, $(0,2)$, $(1,1)$이다. Jacobi 행렬은

$$Df = \begin{pmatrix} 3 - 2x - 2y & -2x \\ -y & 2 - x - 2y \end{pmatrix}$$

이다.

- $(0,0)$: $\mathrm{diag}(3,2)$, 불안정 마디.
- $(3,0)$: $\begin{pmatrix} -3 & -6 \\ 0 & -1 \end{pmatrix}$, 고유값 $-3, -1$, 안정 마디.
- $(0,2)$: $\begin{pmatrix} -1 & 0 \\ -2 & -2 \end{pmatrix}$, 고유값 $-1, -2$, 안정 마디.
- $(1,1)$: $\begin{pmatrix} -1 & -2 \\ -1 & -1 \end{pmatrix}$, $\Delta = -1 < 0$, 안장점.

두 종은 공존하지 못하고 초기 상태에 따라 한 종만 살아남는다. 안장점 $(1,1)$의 안정 다양체가 두 끌개의 영역을 나누는 경계이다.

6.6 연습문제와 해설

연습문제 6.6 $x' = y,\ y' = x - x^3$의 평형점을 분류하라.

풀이. 평형점은 $(0,0),\ (\pm 1, 0)$이다. $Df = \begin{pmatrix} 0 & 1 \\ 1 - 3x^2 & 0 \end{pmatrix}$이므로 원점은 $\Delta = -1$로 안장점, $(\pm 1, 0)$은 $\Delta = 2,\ \tau = 0$으로 선형화가 중심이다. 에너지 $E = \dfrac{1}{2}y^2 - \dfrac{1}{2}x^2 + \dfrac{1}{4}x^4$가 보존되고 $(\pm 1, 0)$에서 극소이므로 실제로 중심이다.

연습문제 6.7 $x' = -x^3 + y,\ y' = -x - y^3$의 원점 안정성을 $V = x^2 + y^2$로 판정하라.

풀이. $\dot V = 2x(-x^3 + y) + 2y(-x - y^3) = -2(x^4 + y^4) < 0\ (\neq 0)$이므로 점근안정이다. 선형화는 중심이라 결론을 주지 못하는 경우이다.

연습문제 6.8 $x' = x^2$의 원점은 안정한가? 선형화는 무엇을 말하는가?

풀이. 선형화는 $u' = 0$으로 판정 불가이다. $x(0) > 0$이면 $x = \dfrac{x_0}{1 - x_0 t}$가 폭발하므로 불안정하고, $x(0) < 0$이면 0으로 수렴한다. 한쪽에서만 끌어당기는 반안정 평형점이다.

다음 연결. 평형점이 모두 불안정해도 해가 유계에 머물 수 있다. 다음 장에서는 그런 해가 접근하는 닫힌 궤도, 즉 극한주기와 매개변수에 따른 정성적 변화(분기)를 다룬다.

제 7 장

극한주기와 분기

개요 극한주기는 고립된 닫힌 궤도, 곧 근처에 다른 닫힌 궤도가 없는 주기해의 궤적이다. 이 장은 먼저 평면 자율계에서 극한주기의 존재와 부재를 판정하는 두 정리, Poincaré–Bendixson 정리와 Bendixson–Dulac 판정법을 세우고, 발진기의 표준 모형인 van der Pol 방정식에 적용한다. 이어서 매개변수가 변할 때 평형점과 주기궤도의 개수·안정성이 바뀌는 **분기**(*bifurcation*)의 표준형—안장-마디, 초월임계, 갈퀴, Hopf 분기—를 정리한다. 선행 지식: 앞 장의 평형점 분석과 Lyapunov 함수(제12권 제6장), 제2장의 연장 정리(제12권 제2장).

7.1 극한주기

> **정의 7.1 (극한주기)** 평면(또는 일반적으로 상공간) 위의 자율계에서 고립된 닫힌 궤도, 곧 어떤 근방에도 다른 닫힌 궤도를 포함하지 않는 주기해의 궤적을 **극한주기**(*limit cycle*)라고 한다. 근처에서 출발한 궤도가 시간이 흐르며 그 극한주기로 접근하면 **안정 극한주기**, 모두 멀어지면 불안정 극한주기, 한쪽에서는 접근하고 다른 쪽에서는 멀어지면 반안정 극한주기라고 한다.

참고 (선형계에는 극한주기가 없다). 선형계 $x' = Ax$의 닫힌 궤도(존재한다면 중심 둘레의 타원)는 고립되지 않는다. 중심 평형점 주위의 모든 타원이 동시에 닫힌 궤도를 이루는 연속된 가족을 이루기 때문이다. 따라서 극한주기는 본질적으로 비선형 현상이며, 발진기 회로, 심장 박동, 포식자–피식자 개체수 진동 모형의 수학적 기초를 이룬다.

> **예제 7.2** 제2장 연습문제의 계(제12권 제2장) $x' = -y + x(1 - r^2)$, $y' = x + y(1 - r^2)$를 극좌표로 바꾸면
>
> $$r' = r(1 - r^2), \qquad \theta' = 1$$
>
> 이다. $r = 1$이 닫힌 궤도이고, $0 < r < 1$이면 $r' > 0$이어서 r이 증가하며 $r > 1$이면 $r' < 0$이어서 r이 감소하므로, $r = 1$은 안정 극한주기이다.

7.2 Poincaré–Bendixson 정리

> **정리 7.3 (Poincaré–Bendixson)** 평면 위의 C^1 자율계에서 어떤 해의 미래 궤도(양의 반궤도)가 콤팩트 집합 K에 머물고 K가 평형점을 포함하지 않으면, 그 궤도는 닫힌 궤도이거나 닫힌 궤도로 나선형으로 접근한다.

실제 사용법은 벡터장이 경계에서 안쪽을 향하는 고리 모양의 "갇힘 영역"을 만드는 것이다. 그 안에 평형점이 없으면 정리 7.3에 의해 안쪽에 극한주기가 존재한다. 이 정리는 평면, 더 정확히는 2차원에서만 성립한다. 3차원 이상에서는 제8장(제12권 제8장)의 Lorenz 계처럼 유계이지만 주기적이지 않은 궤도가 가능하다. 평면에서 그러한 혼돈적 거동이 불가능한 이유는 서로 다른 두 궤도가 교차할 수 없다는 사실과 Jordan 곡선 정리가 상공간을 안쪽·바깥쪽으로 가르기 때문이다.

정리 7.4 (Bendixson–Dulac 판정법) 단순연결 영역 $D \subset \mathbb{R}^2$에서 계 $x' = f(x,y)$, $y' = g(x,y)$를 벡터장 $\mathbf{f} = (f, g)$로 쓰자. C^1 함수 φ가 있어 $\nabla \cdot (\varphi \mathbf{f})$의 부호가 D에서 일정하고 어떤 열린부분집합에서도 항등적으로 0이 아니면, D 안에는 (전적으로 D에 포함되는) 닫힌 궤도가 없다.

증명. 닫힌 궤도 C가 D 안에서 내부 영역 R을 둘러싼다고 가정하면 발산 정리로

$$\iint_R \nabla \cdot (\varphi \mathbf{f}) \, \mathrm{d}A = \oint_C \varphi \mathbf{f} \cdot \hat{\mathbf{n}} \, \mathrm{d}s \tag{7.1}$$

이다. 궤도 C 위에서는 $\mathbf{f}$가 궤도의 접선 방향이므로 $\mathbf{f} \cdot \hat{\mathbf{n}} = 0$이고, 식 (7.1)의 우변은 0이다. 한편 좌변은 $\nabla \cdot (\varphi \mathbf{f})$의 부호가 R에서 일정하고 항등적으로 0이 아니라는 가정으로 0이 될 수 없다. 모순이므로 그러한 닫힌 궤도는 없다. $\square$

예제 7.5 감쇠 진동자 $x' = y$, $y' = -x - y$에서 $\varphi \equiv 1$로 두면 $\nabla \cdot \mathbf{f} = -1 < 0$이므로 정리 7.4에 의해 닫힌 궤도가 없다. 마찰이 있는 계에서는 영구적인 진동이 불가능하다는 직관과 일치한다.

7.3 van der Pol 발진기

$$x'' - \mu(1 - x^2)x' + x = 0 \qquad (\mu > 0) \tag{7.2}$$

은 변위 x가 작을 때 계수 $-\mu(1-x^2)$가 음의 감쇠(에너지를 계에 주입)로, x가 클 때는 양의 감쇠로 작용하는 비선형 진동자이며, 진공관·트랜지스터 발진기 회로의 표준 모형이다. Liénard 정리(비선형 2계 방정식의 극한주기 존재를 보장하는 판정법)로 이 계는 유일한 안정 극한주기를 가짐이 증명된다. μ가 작으면 진폭이 약 2인 거의 원형의 궤도이고, μ가 크면 변수가 천천히 움직이다 급격히 뛰는 **이완 진동**(*relaxation oscillation*)이 된다.

유도 (작은 μ에서 진폭의 평균화 계산). $\mu \ll 1$일 때 식 (7.2)의 해는 0차 근사로 $x = a\cos t$인 조화진동이고, 진폭 a는 비선형 항이 한 주기에 걸쳐 계에 넣거나 빼는 에너지가 상쇄되는 값으로 정해진다(평균화 방법).

1단계. $x = a\cos t$, $x' = -a\sin t$로 두고 식 (7.2)의 비선형 감쇠항이 한 주기 동안 하는 일을 적분한다. 감쇠항이 공급하는 일률은 $\mu(1-x^2)x' \cdot x' = \mu(1-x^2)(x')^2$이므로, 한 주기 동안의 알짜 일은

$$W(a) = \int_0^{2\pi} \mu\left(1 - a^2\cos^2 t\right) a^2 \sin^2 t \, \mathrm{d}t$$

이다.

2단계. 적분을 전개한다. $\int_0^{2\pi} \sin^2 t \, \mathrm{d}t = \pi$, $\int_0^{2\pi} \cos^2 t \sin^2 t \, \mathrm{d}t = \pi/4$이므로

$$W(a) = \mu a^2 \left(\pi - \frac{a^2 \pi}{4}\right) = \mu \pi a^2 \left(1 - \frac{a^2}{4}\right) \tag{7.3}$$

이다.

3단계. 정상 상태의 진폭은 $W(a) = 0$, $a \neq 0$인 해이다. 식 (7.3)에서 $1 - a^2/4 = 0$, 즉 $a = 2$이다.

검산. $a < 2$이면 $W(a) > 0$(에너지가 유입되어 진폭이 커짐), $a > 2$이면 $W(a) < 0$(에너지가 빠져나가 진폭이 작아짐)이므로 $a = 2$는 안정한 정상 진폭이다. 이는 극한주기의 안정성과 일치한다.

7.4 1차원 분기

매개변수 μ를 포함한 계 $x' = f(x,\mu)$에서 평형점의 개수나 안정성이 바뀌는 μ의 값을 **분기점**(*bifurcation point*)이라고 한다. 다음 세 표준형이 1차원 분기의 기본 유형이다.

$$\text{안장-마디 분기 :} \qquad x' = \mu - x^2, \tag{7.4}$$

$$\text{초월임계 분기 :} \qquad x' = \mu x - x^2, \tag{7.5}$$

$$\text{갈퀴 분기(초임계) :} \qquad x' = \mu x - x^3. \tag{7.6}$$

식 (7.4)의 **안장-마디 분기**에서는 $\mu < 0$이면 평형점이 없고, $\mu > 0$이면 $x = \pm\sqrt{\mu}$ 두 개가 생긴다(안정 $+\sqrt{\mu}$, 불안정 $-\sqrt{\mu}$). $\mu = 0$에서 두 평형점이 충돌해 사라진다.

식 (7.5)의 **초월임계 분기**에서는 평형점 0과 μ가 항상 존재하다가 $\mu = 0$에서 서로 만나 안정성을 교환한다: $\mu < 0$이면 0이 안정이고 μ가 불안정, $\mu > 0$이면 반대이다.

식 (7.6)의 **갈퀴 분기**(초임계)에서는 $\mu < 0$이면 $x = 0$만 안정하다가, $\mu > 0$이면 0이 불안정해지고 대칭인 두 평형점 $x = \pm\sqrt{\mu}$가 안정하게 생긴다. 대칭 $x \to -x$를 가진 계에서 나타나며, 상전이의 평균장 이론(물리학 마스터 레퍼런스의 Landau 평균장과 상전이 항목)과 같은 구조이다.

참고 (아임계 갈퀴 분기). 식 (7.6)의 부호를 바꾼 $x' = \mu x + x^3$은 **아임계 갈퀴 분기**이다. $\mu < 0$이면 $x = 0$이 안정하지만 그 흡인 영역은 불안정 평형점 $\pm\sqrt{-\mu}$로 둘러싸인 유한한 구간뿐이고, μ가 0을 지나면 $x = 0$마저 불안정해져 해가 유한 시간 안에 발산한다. 초임계·아임계의 구별은 제 7.5절 Hopf 분기에서도 같은 역할을 한다.

주의 (선형화가 실패하는 지점). 세 표준형 모두 분기점에서는 선형화 $f_x(x^*,\mu)$의 고유값이 0이 되므로, Hartman–Grobman 정리 (제12권 제6장)가 적용되지 않는다. 분기점 근처의 거동은 선형 항이 아니라 다음 차수의 비선형 항이 결정한다.

7.5 Hopf 분기

2차원 이상의 계에서 평형점의 선형화 고유값 가운데 복소켤레 쌍이 매개변수 변화에 따라 허수축을 가로지르면 평형점에서 주기궤도가 생겨난다.

> **정리 7.6 (Hopf 분기, 평면의 경우)** 평형점의 선형화 고유값이 $\alpha(\mu) \pm i\beta(\mu)$이고 $\alpha(0) = 0$, $\beta(0) \neq 0$, $\alpha'(0) \neq 0$을 만족하며, 비선형 항에서 계산되는 첫 Lyapunov 계수가 0이 아니면, $\mu = 0$ 근처의 한쪽에서 진폭이 $\sqrt{|\mu|}$에 비례하는 주기궤도가 생긴다.

표준형 $r' = \mu r - r^3$, $\theta' = 1$(초임계)에서는 $\mu > 0$일 때 반지름 $\sqrt{\mu}$인 안정 극한주기가 생긴다. 반대로 $r' = \mu r + r^3$(아임계)에서는 $\mu < 0$일 때 불안정 주기궤도가 있고, μ가 0을 지나면 궤도가 갑자기 먼 곳의 큰 진폭으로 튀는 위험한 전이가 일어난다. 공학에서 발진의 시작, 비행기 날개의 플러터, 화학 반응의 진동이 Hopf 분기로 설명된다.

7.6 연습문제와 해설

연습문제 7.7 $x' = y,\ y' = -x + y(1 - x^2 - 2y^2)$가 고리 $1/\sqrt{2} \le r \le 1$ 안에 극한주기를 가짐을 보여라.

풀이. $r^2 = x^2 + y^2$에서 $rr' = xx' + yy' = xy + y\bigl(-x + y(1 - x^2 - 2y^2)\bigr) = y^2(1 - x^2 - 2y^2)$이다. $r = 1$에서는 $x^2 + 2y^2 = 1 + y^2 \ge 1$이므로 $rr' \le 0$이고, $r = 1/\sqrt{2}$에서는 $x^2 + 2y^2 = \tfrac{1}{2} + y^2 \le 1$이므로 $rr' \ge 0$이다. 따라서 고리 $1/\sqrt{2} \le r \le 1$은 양불변집합이다(경계에서 벡터장이 안쪽을 향하거나 접한다). 이 계의 유일한 평형점은 원점이며 고리 바깥에 있으므로, 정리 7.3에 의해 고리 안에 닫힌 궤도가 있다.

경계에서 등호 $rr' = 0$이 성립하는 점들에서는 궤도가 경계를 따라 머무르지 않고 고리 안쪽으로 들어감을 추가로 확인해야 한다. $r = 1$에서 등호는 $y = 0$일 때, 즉 $(\pm 1, 0)$에서 성립하는데, 이 점에서 $y' = \mp 1 \neq 0$이므로 해는 곧바로 $y \neq 0$인 점으로 옮겨 가고, 그곳에서는 $rr' < 0$이다. $r = 1/\sqrt{2}$에서는 $x^2 + y^2 = \tfrac{1}{2}$이므로 $rr' = x^2 y^2$이고, 등호는 $xy = 0$인 네 점 $(\pm 1/\sqrt{2}, 0),\ (0, \pm 1/\sqrt{2})$에서 성립한다. 이 점들에서는 x' 또는 y' 가운데 0이 아닌 쪽이 있어 해가 곧바로 $xy \neq 0$인 점으로 옮겨 가고, 그곳에서는 $rr' > 0$이므로 해가 안쪽으로 들어간다. 따라서 고리는 진짜로 양불변이며 Poincaré–Bendixson 정리의 가정이 충족된다.

연습문제 7.8 $x' = x - y - x^3,\ y' = x$에서 닫힌 궤도가 존재할 수 있는 영역에 대해 Bendixson 판정법은 무엇을 말하는가?

풀이. $\varphi \equiv 1$로 두면 $\nabla \cdot \mathbf{f} = \partial_x(x - y - x^3) + \partial_y(x) = 1 - 3x^2$이다. 띠 $|x| < 1/\sqrt{3}$ 안에서는 $1 - 3x^2 > 0$이므로, 정리 7.4에 의해 그 띠 안에 완전히 들어 있는 닫힌 궤도는 없다. 따라서 닫힌 궤도가 있다면 반드시 그 띠를 벗어나야 한다. 이 계는 $u = x,\ v = -y$로 두면 $u' = v - (u^3 - u),\ v' = -u$인 Liénard 계이고, $x'' - (1 - 3x^2)x' + x = 0$에서 $X = \sqrt{3}\,x$로 놓으면 $\mu = 1$인 van der Pol 방정식이 된다. 따라서 실제로 띠를 넘나드는 극한주기를 갖는다.

연습문제 7.9 $x' = \mu + x - x^3$의 분기점을 구하라.

풀이. 평형점은 $\mu = x^3 - x =: g(x)$의 해이다. $g'(x) = 3x^2 - 1 = 0$은 $x = \mp 1/\sqrt{3}$에서 풀리고, 극값은

$$g\!\left(\frac{1}{\sqrt{3}}\right) = -\frac{2}{3\sqrt{3}}, \qquad g\!\left(-\frac{1}{\sqrt{3}}\right) = \frac{2}{3\sqrt{3}}$$

이다. μ가 이 두 극값을 지날 때 $\mu = g(x)$의 실근 개수가 3개에서 1개로(또는 그 반대로) 바뀌므로, $\mu = \pm\dfrac{2}{3\sqrt{3}}$에서 안장-마디 분기가 일어난다. 그 사이 $-\tfrac{2}{3\sqrt{3}} < \mu < \tfrac{2}{3\sqrt{3}}$에서는 평형점이 셋이고, 바깥쪽 둘이 안정, 가운데가 불안정이다. μ를 이 구간 밖에서 왕복시키면 평형점이 두 분기값에서 따로 뛰어오르는 **이력현상**(*hysteresis*)이 나타난다.

참고 (다음 연결). 연속시간 자율계에서 혼돈적 거동은 Poincaré–Bendixson 정리에 의해 3차원 이상에서만 가능하지만, 이산시간 사상에서는 변수가 하나뿐이어도 가능하다. 제8장(제12권 제8장)에서는 로지스틱 사상의 주기배가와 Lorenz 계를 통해 이산·연속 두 경우의 혼돈을 수학적으로 정의한다.

제 8 장

이산 동역학과 혼돈

개요 이 장은 연속시간의 흐름 대신 반복 사상 $x_{n+1} = f(x_n)$이 만드는 이산시간 동역학을 다룬다. 고정점·주기점의 안정성 판정, 로지스틱 사상의 주기배가 분기와 Feigenbaum 상수, Sharkovskii 정리, Lyapunov 지수에 의한 혼돈의 정의를 차례로 세우고, 마지막으로 연속시간에서 혼돈이 나타나는 가장 유명한 예인 Lorenz 계를 소개한다. 선행 지식: 앞 두 장의 안정성과 분기(제12권 제6장, 제12권 제7장), 제2장의 초기값 의존성(제12권 제2장).

8.1 고정점과 안정성

사상 $f:\mathbb{R}\to\mathbb{R}$의 반복에서 $f(x^*)=x^*$이면 x^*를 **고정점**이라 하고, $f^{k}(x^*)=x^*$를 만족하는 최소의 $k\ge 1$이 있으면 x^*를 **주기 k인 점**이라고 한다 (여기서 f^{k}는 f를 k번 합성한 사상이다).

명제 8.1 (고정점의 안정성 판정) f가 C^1이고 x^*가 고정점이면 다음이 성립한다.

- $|f'(x^*)|<1$이면 x^*는 끌어당기는(안정) 고정점이다.
- $|f'(x^*)|>1$이면 x^*는 밀어내는(불안정) 고정점이다.
- $|f'(x^*)|=1$이면 이 판정으로는 안정성을 알 수 없다.

증명. 평균값정리로 $x_{n+1}-x^*=f(x_n)-f(x^*)=f'(\xi_n)(x_n-x^*)$인 ξ_n이 x_n과 x^* 사이에 있으므로 $|x_{n+1}-x^*|=|f'(\xi_n)||x_n-x^*|$이다. f'이 연속이므로 x^* 근방에서 $|f'|$이 1보다 작은(또는 큰) 값으로 고르게 묶이고, 그 비율이 반복될 때마다 곱해져 $|x_n-x^*|$가 기하급수적으로 0으로 가거나 (또는 벗어나거나) 한다. $\square$

연속시간 자율계의 안정 판정 기준 "평형점 선형화 고유값의 실수부 <0"은 이산시간에서는 "고유값의 절댓값 <1"로 바뀐다. 주기 k 궤도 $\{x_0,\dots,x_{k-1}\}$의 안정성은 연쇄법칙으로

$$(f^{k})'(x_0)=\prod_{j=0}^{k-1} f'(x_j) \tag{8.1}$$

를 계산해 식 (8.1)의 절댓값과 1을 비교하여 판정한다. 시각적으로는 그래프 $y=f(x)$와 대각선 $y=x$ 사이를 오가며 그리는 거미줄 그림(*cobweb diagram*)으로 반복을 추적한다.

참고 (Newton 방법과의 비교). g의 단순근을 찾는 Newton 방법 $x_{n+1}=x_n-g(x_n)/g'(x_n)$은 사상 $f(x)=x-g(x)/g'(x)$의 반복이다. 단순근 x^*에서 $f'(x^*)=0$이므로 명제 8.1보다 훨씬 강한 초선형(실제로는 이차) 수렴이 일어난다. 수렴 속도와 초기값 의존성은 제25권의 수치해석에서 자세히 다룬다.

8.2 로지스틱 사상

$$f_r(x)=rx(1-x),\qquad 0\le r\le 4,\quad x\in[0,1] \tag{8.2}$$

는 계수 r을 늘려 가며 질적으로 다른 거동을 가장 단순하게 보여 주는 사상이다. 고정점은 $x=0$과 $x^{*}=1-1/r$이고, r에 따라 다음과 같이 분기한다.

- $0<r<1$: $f_r'(0)=r<1$이므로 0이 안정하다.
- $1<r<3$: $x^{*}>0$이 되어 의미를 가지며, $f_r'(x^{*})=2-r$이고 $|2-r|<1$이므로 x^{*}가 안정하다.
- $r=3$: $f_r'(x^{*})=-1$이 되어 고정점이 불안정해지며, 안정한 주기 2 궤도가 새로 생긴다 (**주기 배가 분기**, *period-doubling bifurcation*).
- $3<r<1+\sqrt{6}\approx 3.449$: 주기 2 궤도가 안정하다.
- 이후 주기 $4, 8, 16, \dots$로의 배가가 점점 짧아지는 r 간격으로 일어나 극한값 $r_{\infty}\approx 3.5699$에 집적한다.

분기점들의 간격 비 $\dfrac{r_{n}-r_{n-1}}{r_{n+1}-r_{n}}$은 $\delta\approx 4.6692$로 수렴하며, 이를 **Feigenbaum 상수**라고 한다. 이 상수는 x^{2} 꼴의 매끄러운 극대를 하나 갖는 사상족 전체에서 같은 값으로 나타난다는 **보편성**(*universality*)이 있으며, 실제 유체 실험과 전자 회로의 주기배가 실험에서도 측정되었다.

$r_{\infty}<r\le 4$에서는 대부분의 r에서 혼돈적 거동이 나타나지만, 그 사이사이에 안정한 주기궤도가 다시 나타나는 **주기 창**(*periodic window*)이 있다. 예를 들어 $r=1+\sqrt{8}\approx 3.8284$ 근처에 안정한 주기 3 궤도가 나타난다(제8.3절).

8.3 주기 3과 Sharkovskii 정리

> **정리 8.2 (Li–Yorke, Sharkovskii)** 구간 위의 연속사상이 주기 3인 점을 가지면, 모든 자연수 k에 대해 주기 k인 점을 갖는다.

Sharkovskii 정리는 더 정밀하게, 자연수 위에 다음과 같은 순서를 매긴다.

$$3 \triangleright 5 \triangleright 7 \triangleright \cdots \triangleright 2\cdot 3 \triangleright 2\cdot 5 \triangleright \cdots \triangleright 2^{2}\cdot 3 \triangleright \cdots \triangleright 2^{3} \triangleright 2^{2} \triangleright 2 \triangleright 1 \tag{8.3}$$

식 (8.3)의 순서에서 앞선 주기가 있으면 그 뒤의 모든 주기가 있다고 말한다. 증명의 핵심은 중간값정리와 "구간 I의 상이 구간 J를 덮는다"는 덮개 관계의 조합이다.

주의 (연속사상·구간이라는 가정). 정리 8.2와 식 (8.3)는 구간 위의 연속사상에만 성립한다. 원 위의 회전 $z\mapsto e^{2\pi i/3}z$는 주기 3만 가지며 다른 주기는 전혀 갖지 않는다. 원은 구간과 달리 중간값정리의 "덮개" 논법이 그대로 적용되지 않기 때문이다.

8.4 Lyapunov 지수와 혼돈의 정의

반복 사상에서 가까운 두 초기값의 차이는 한 번 반복할 때마다 대략 $|f'(x_{n})|$배가 된다. 장기 평균 증가율

$$\lambda=\lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N-1}\log\left|f'(x_{n})\right| \tag{8.4}$$

을 **Lyapunov 지수**라고 한다. $\lambda>0$이면 초기 오차가 대략 $e^{\lambda n}$으로 자라는 초기값 민감성이 있다.

> **예제 8.3 ($r=4$의 로지스틱 사상)** $x=\sin^{2}(\pi\theta)$로 치환하면 $f_{4}(x)=4x(1-x)=4\sin^{2}(\pi\theta)\cos^{2}(\pi\theta)=\sin^{2}(2\pi\theta)$이므로, f_{4}는 $\theta\mapsto 2\theta \bmod 1$과 반공액이다($h(\theta)=\sin^{2}(\pi\theta)$가

$h(2\theta \bmod 1) = f_4(h(\theta))$를 만족하며, θ와 $1-\theta$가 같은 x에 대응하는 2대1 대응이다). 이 사상은 초기값의 이진 전개를 한 자리씩 왼쪽으로 미는 자리이동 사상이므로, 초기값의 k번째 이진 자리가 $k-1$번 반복한 뒤 맨 앞자리로 온다. $f'(x) = 4 - 8x$이고 식 (8.4)의 평균을 θ에 대한 불변분포 $\dfrac{1}{\pi\sqrt{x(1-x)}}$로 계산하면 $\lambda = \log 2 > 0$이다. 거의 모든 초기값의 궤도는 이 분포를 따라 $[0,1]$을 조밀하게 채운다.

혼돈의 통일된 정의는 없지만 **Devaney의 정의**가 널리 쓰인다. 불변집합 위의 사상이 다음 세 조건을 만족하면 **혼돈적**(*chaotic*)이라고 한다.

(1) 초기값에 민감하다: 임의의 점 근처에도 궤도가 결국 멀리 벌어지는 점이 있다.

(2) 위상적으로 추이적이다: 어떤 열린집합에서 출발한 궤도도 언젠가 다른 임의의 열린집합에 도달한다.

(3) 주기점이 조밀하다.

결정론적 규칙만으로 장기 예측이 사실상 불가능해지는 이유는 측정 오차가 지수적으로 확대되기 때문이며(초기값 민감성), 규칙 자체에 무작위성이 있기 때문이 아니다.

8.5 Lorenz 계

$$x' = \sigma(y - x), \qquad y' = x(\rho - z) - y, \qquad z' = xy - \beta z \tag{8.5}$$

는 대류를 세 모드로 크게 단순화한 3차원 계이다. 표준 매개변수 $\sigma = 10$, $\beta = 8/3$, $\rho = 28$에서 다음이 알려져 있다.

- $\nabla \cdot \mathbf{f} = -(\sigma + 1 + \beta) < 0$이므로 상공간의 부피 요소가 시간에 따라 지수적으로 줄어든다. 따라서 장기적으로 궤도가 모여드는 끌개의 (3차원) 부피는 0이다.
- 원점과 $C_{\pm} = \left(\pm\sqrt{\beta(\rho-1)}, \pm\sqrt{\beta(\rho-1)}, \rho - 1\right)$이 평형점이며, $\rho = 28$에서는 셋 다 불안정하다.
- 해는 유계 영역에 갇히지만 어떤 평형점이나 주기궤도로도 수렴하지 않고, 나비 모양의 **이상 끌개**(*strange attractor*) 위를 영원히 움직인다. 이 끌개 위의 운동은 양의 Lyapunov 지수(약 0.9)를 가지며 혼돈적이다.

이 끌개가 실제로 존재하며 혼돈적이라는 사실은 Tucker(2002)가 구간 산술을 이용한 컴퓨터 보조 증명으로 확립했다. 수치 시뮬레이션만으로는 반올림 오차가 지수적으로 확대되어 개별 궤도를 장시간 정확히 추적할 수 없다는 점도 이 계에서 처음 널리 주목받았다.

8.6 연습문제와 해설

연습문제 8.4 $f(x) = x^2 - 2$의 고정점과 주기 2 궤도를 구하고 안정성을 판정하라.

풀이. 고정점은 $x^2 - x - 2 = (x-2)(x+1) = 0$에서 $x = 2, -1$이다. $f'(x) = 2x$이므로 $f'(2) = 4$, $f'(-1) = -2$이고 둘 다 절댓값이 1보다 크므로 불안정하다.

주기 2 궤도를 구하려면 $f(f(x)) = x$를 풀고 고정점의 인수 $x^2 - x - 2$를 나눈다. $f(f(x)) - x = (x^2-2)^2 - 2 - x = x^4 - 4x^2 - x + 2$이고, 이를 $x^2 - x - 2$로 나누면 몫 $x^2 + x - 1$, 나머지 0을 얻는다.

따라서 주기 2 궤도는 $x^2 + x - 1 = 0$의 해 $x_{0,1} = \dfrac{-1 \pm \sqrt{5}}{2}$이다. 근과 계수의 관계로 $x_0 x_1 = -1$이므로

$$(f^2)'(x_0) = f'(x_0) f'(x_1) = 4 x_0 x_1 = 4 \cdot (-1) = -4$$

이고 절댓값이 1보다 크므로 이 주기 2 궤도는 불안정하다. 이 사상은 $x = 2\cos\theta$로 치환하면 $\theta \mapsto 2\theta$와 반공액이며($f(2\cos\theta) = 2\cos 2\theta$) 구간 $[-2, 2]$에서 혼돈적이다.

연습문제 8.5 로지스틱 사상의 주기 2 궤도가 $r > 3$에서 존재함을 보이고 그 점을 구하라.

풀이. $f_r^2(x) - x$를 고정점의 인수 $f_r(x) - x$로 나누면

$$r^2 x^2 - r(r+1)x + (r+1) = 0$$

이 남는다. 이 이차방정식의 판별식은

$$r^2(r+1)^2 - 4r^2(r+1) = r^2(r+1)(r-3)$$

이고 $r > 3$에서 양이므로, 두 실근

$$x = \frac{(r+1) \pm \sqrt{(r+1)(r-3)}}{2r}$$

이 존재하며 이 두 점이 주기 2 궤도를 이룬다. $r \to 3^+$에서 판별식이 0으로 가며 두 점이 고정점 $x^* = 1 - 1/r \to 2/3$으로 합쳐지는 것이 주기배가 분기의 모습이다.

연습문제 8.6 $\theta \mapsto 2\theta \bmod 1$의 주기 3인 점을 모두 구하라.

풀이. 주기 3인 점은 $f^3(\theta) = 8\theta \bmod 1 = \theta$, 즉 $7\theta \in \mathbb{Z}$를 만족해야 한다. $\theta \in [0, 1)$에서 이를 만족하는 점은 $\theta = k/7$ $(k = 0, 1, \dots, 6)$이다. $\theta = 0$은 고정점(주기 1)이므로 제외하면, 남은 여섯 점은 사상 아래에서 두 궤도

$$\{1/7,\ 2/7,\ 4/7\}, \qquad \{3/7,\ 6/7,\ 5/7\}$$

를 이룬다(각 괄호 안에서 2를 곱하고 1을 법으로 줄이면 다음 원소로 옮겨 간다).

참고 (다음 연결). 이 권은 1계 방정식에서 시작해 극한주기·분기·혼돈까지 비선형 동역학계의 정성적 이론을 훑었다. 편미분방정식으로의 확장과 그 해석학적 기초는 제13권에서, 수치 적분과 분기 추적의 계산 기법은 제25권에서, Markov 연쇄로 추상화된 확률적 이산 동역학은 제21권에서 이어진다.

제12권의 범위와 다음 읽기

제12권은 1계 방정식의 언어와 풀이, 해의 존재·유일성·연장과 매개변수 의존성, 고계 선형 방정식과 급수해, 선형계와 행렬지수·상평면, Laplace 변환과 전달함수, 비선형계의 평형점과 안정성, 극한주기와 분기, 이산 동역학과 혼돈을 다루었다. 앞 여섯 장에서 선형·비선형 상미분방정식의 풀이와 정성적 분석(안정성, 상평면)의 기본 도구를 세운 뒤, 제7 8장에서는 그 도구를 극한주기의 존재·부재 판정과 매개변수에 따른 평형점·주기궤도의 분기, 그리고 이산시간 사상의 혼돈적 거동으로 확장하였다. 편미분방정식과 Sturm–Liouville 이론은 제13권, 미분방정식의 수치해법과

분기 추적은 제25권, 확률미분방정식은 제21권으로 이어진다. 또한 선형대수의 고유값·대각화(제7권)가 제4장의 행렬지수와 상평면 분류의 기초가 되고, 다변수 미적분의 임계점·Hessian 판정(제9권)이 제6장의 Lyapunov 함수 구성과 직접 연결된다.

표준 참고서로 W. E. Boyce and R. C. DiPrima, *Elementary Differential Equations and Boundary Value Problems*; M. W. Hirsch, S. Smale and R. L. Devaney, *Differential Equations, Dynamical Systems, and an Introduction to Chaos*; S. H. Strogatz, *Nonlinear Dynamics and Chaos*; L. Perko, *Differential Equations and Dynamical Systems*가 있다.

참고 자료의 사용 방식

본문의 설명과 문제는 이 참고서를 위해 새로 작성했다. 아래 목록은 관련 주제를 더 넓은 교재와 대조해 읽기 위한 안내이며, 이 원고 전체가 해당 기관이나 저자의 검토를 받았다는 뜻은 아니다. 개별 정리의 정확한 가정과 기호 약속은 자료마다 다를 수 있으므로, 독자는 다른 자료를 참고할 때마다 그 자료의 정의를 먼저 확인해야 한다.

- MIT OpenCourseWare, 18.03SC *Differential Equations*: 선형 방정식, Laplace 변환, 상평면 분석의 강의와 연습.
- OpenStax, *Calculus Volume 3*: 2계 선형 미분방정식 장의 계산 연습.

제 13 권

함수해석 · 편미분방정식

제13권은 함수 전체의 모임을 무한차원 벡터공간으로 다루는 함수해석학과, 그 도구를 편미분방정식에 적용하는 방법을 다룬다. 제1–4장은 노름공간과 유계 선형 작용소, Hilbert 공간과 Fourier 급수, Hahn–Banach 정리 · 균등유계원리 · 열린사상 정리의 세 기둥, 스펙트럼과 콤팩트 작용소를 차례로 세운다. 제5–7장은 편미분방정식의 분류와 특성곡선, 파동방정식, 변수분리와 Sturm–Liouville 문제, Laplace 방정식과 Green 함수와 Fourier 변환을 다룬다. 제8장은 약해와 Sobolev 공간, Lax–Milgram 정리로 고전적 미분가능성을 요구하지 않는 해의 이론을 세워, 앞의 두 부분을 하나로 잇는다.

제 1 장

노름공간과 유계 선형 작용소

개요 노름공간은 거리와 완비성의 개념을 갖춘 벡터공간이며, **함수해석학**(*functional analysis*)은 함수 전체의 모임을 이러한 "무한차원 벡터공간"으로 다루어 미분방정식·적분방정식을 선형대수의 언어로 재구성하는 분야이다. 이 권은 함수해석학의 기본 정리를 세운 뒤 그 언어로 편미분방정식을 정리한다. 첫 장에서는 노름공간의 기본 예, 유계 선형 작용소와 그 노름, 쌍대공간을 정의하고, 유한차원 선형대수의 친숙한 사실 가운데 무한차원에서 실패하는 것들을 정리한다. 선행 지식: 제7권의 벡터공간과 선형사상, 제10권 제7장의 L^p 공간과 완비성(제10권 제7장).

1.1 노름공간과 Banach 공간

정의 1.1 (**노름공간과 Banach 공간**) 실수 또는 복소수체 $\mathbb{F}$ 위의 벡터공간 X에 **노름**(*norm*) $\|\cdot\|$이 주어지면 $d(x,y)=\|x-y\|$로 거리공간이 된다. 이 거리에 대해 완비이면 X를 **Banach 공간**이라고 한다.

기본 예는 다음과 같다.

- $\mathbb{R}^n$, $\mathbb{C}^n$(임의의 노름). 유한차원 노름공간은 어떤 노름을 주어도 항상 완비이다.
- ℓ^p $(1\le p<\infty)$: $\sum_{k} |x_k|^p<\infty$인 수열 전체, $\|x\|_p=\left(\sum_k |x_k|^p\right)^{1/p}$. ℓ^∞: 유계 수열 전체, 상한 노름 $\|x\|_\infty=\sup_k |x_k|$.
- $C(K)$: 콤팩트 거리공간 K 위의 연속함수 전체, 균등노름 $\|f\|_\infty=\max_K |f|$. 연속함수의 균등극한이 다시 연속이므로 완비이다.
- $L^p(\mu)$ $(1\le p\le\infty)$: 제10권의 Riesz–Fischer 정리(제10권 제7장)로 완비이다.
- $C^k[a,b]$: 노름 $\sum_{j\le k}\|f^{(j)}\|_\infty$에 대해 완비이다.

예제 1.2 (**완비가 아닌 노름공간**) $C[0,1]$에 L^1 노름 $\|f\|_1=\int_0^1|f|$를 준 공간은 완비가 아니다. 예컨대 $1/2$ 근처에서 가파르게 0에서 1로 바뀌는 연속함수열은 L^1에서 계단함수(불연속함수)로 수렴하는데, 그 극한은 $C[0,1]$에 속하지 않기 때문이다. 같은 집합 $C[0,1]$이라도 어떤 노름을 주는지에 따라 완비성이 달라진다는 것이 중요하다.

1.2 유계 선형 작용소

명제 1.3 노름공간 사이의 선형사상 $T:X\to Y$에 대해 다음은 동치이다.
(1) T는 (노름 위상에서) 연속이다.
(2) T는 0에서 연속이다.
(3) $\|Tx\|\le C\|x\|$인 상수 $C\ge 0$이 있다(**유계**).

증명. (1)⇒(2)는 자명하다. (2)⇒(3): 0에서의 연속성으로 $\|x\| \le \delta$이면 $\|Tx\| \le 1$인 $\delta > 0$가 있다. 임의의 $x \neq 0$에 대해 $\delta x/\|x\|$에 T의 선형성을 적용하면 $\|T(\delta x/\|x\|)\| \le 1$, 즉 $\|Tx\| \le \|x\|/\delta$이므로 $C = 1/\delta$가 된다. (3)⇒(1): T의 선형성으로 $\|Tx - Ty\| = \|T(x-y)\| \le C\|x-y\|$이므로 T는 (C를 Lipschitz 상수로 갖는) 연속사상이다. □

명제 1.3의 (3)을 만족하는 최소의 C를 **작용소 노름** $\|T\| = \sup_{\|x\|\le 1}\|Tx\|$라고 한다. 유계 작용소 전체의 공간 $B(X,Y)$는 이 노름에 대해 노름공간이며, Y가 완비이면 $B(X,Y)$도 완비이다(유계 작용소의 Cauchy열은 각 점에서 극한을 갖고, 그 극한사상이 선형이며 유계임을 확인하면 된다). 합성에 대해서는 $\|ST\| \le \|S\|\,\|T\|$가 성립한다.

예제 1.4

- 연속인 핵 k를 갖는 적분 작용소 $(Kf)(x) = \int_0^1 k(x,y)f(y)\,dy$는 $C[0,1]$에서 유계이고 $\|K\| = \max_x \int_0^1 |k(x,y)|\,dy$이다.
- 오른쪽 이동 사상 $S(x_1,x_2,\dots) = (0,x_1,x_2,\dots)$는 ℓ^2의 등거리 사상($\|Sx\| = \|x\|$)이지만 전사가 아니다(첫 성분이 항상 0). 유한차원에서는 단사인 선형사상이 자동으로 전사이지만, 무한차원에서는 그렇지 않다는 것을 보여 주는 표준적인 예이다.
- 미분 작용소 $Df = f'$은 $C^1[0,1]$(자신의 노름 $\|f\|_{C^1} = \|f\|_\infty + \|f'\|_\infty$)에서 $C[0,1]$로는 유계이지만, $C[0,1]$의 부분공간인 $C^1[0,1]$에 균등노름 $\|\cdot\|_\infty$을 그대로 주면 비유계이다. $f_n(x) = \sin(nx)$는 $\|f_n\|_\infty \le 1$이지만 $\|Df_n\|_\infty = n \to \infty$이기 때문이다.

참고 (양자역학의 비유계 작용소). 양자역학의 운동량 연산자 $-i\hbar\,d/dx$와 위치 연산자는 $L^2(\mathbb{R})$ 전체에서 비유계이다. 비유계 작용소는 공간 전체가 아니라 조밀한 부분공간(정의역)에서만 정의되며, 자기수반성 같은 개념에는 유계 작용소보다 훨씬 세심한 정의가 필요하다(제13권 제4장 끝).

1.3 쌍대공간

정의 1.5 (쌍대공간) 노름공간 X에서 스칼라체 $\mathbb{F}$로 가는 유계 선형 범함수 전체 $X^* = B(X,\mathbb{F})$를 **쌍대공간**(*dual space*)이라고 한다. 스칼라체 $\mathbb{F}$ 자신이 완비이므로 X^*는 (X가 완비가 아니어도) 항상 Banach 공간이다.

- $1 < p < \infty$, $1/p + 1/q = 1$이면 $(L^p)^* \cong L^q$이다. $g \in L^q$가 $f \mapsto \int fg$로 작용하며 Hölder 부등식으로 유계임이 확인된다. (σ-유한 측도에서는 $(L^1)^* \cong L^\infty$도 성립한다.)
- $(L^\infty)^*$는 L^1을 진부분공간으로 포함할 만큼 더 크다. $(\ell^\infty)^*$에는 수열의 통상적 극한을 모든 유계수열로 확장하는 Banach 극한 같은, ℓ^1에 대응하지 않는 원소가 있다.
- $C[a,b]^*$는 $[a,b]$ 위의 유한 부호 Borel 측도들의 공간이다(Riesz 표현정리). 점 평가 $f \mapsto f(c)$는 Dirac 측도 δ_c에 해당한다.

1.4 무한차원에서 달라지는 것

정리 1.6 (Riesz 보조정리의 결과) 노름공간의 닫힌 단위공이 콤팩트일 필요충분조건은 그 공간이 유한차원인 것이다.

증명. 유한차원이면 Heine–Borel 정리로 닫힌 유계집합이 콤팩트이다. 역으로 무한차원 공간에서 닫힌 단위공이 콤팩트가 아님을 보인다. ℓ^2의 경우 표준 단위벡터 e_k는 단위공 안에 있고 $\|e_j - e_k\| = \sqrt{2}$ $(j \neq k)$이므로 어떤 부분수열도 Cauchy가 될 수 없어 수렴하지 않는다. 일반 노름공간에서는 **Riesz 보조정리**(닫힌 진부분공간 M과 $\varepsilon \in (0,1)$에 대해 $\|x\| = 1$, $\operatorname{dist}(x, M) \geq 1 - \varepsilon$인 x가 있다)를 반복 적용하여, 서로 거리가 $1-\varepsilon$ 이상인 단위벡터열을 만들어 같은 결론을 얻는다. $\square$

정리 1.6 때문에 무한차원에서는 유한차원 선형대수와 해석학의 기본 도구인 "유계 수열은 수렴하는 부분수열을 갖는다"(Bolzano–Weierstrass)를 그대로 쓸 수 없다. 대신 다음 세 대체물을 쓴다.

(1) 약수렴과 약*-콤팩트성(Banach–Alaoglu 정리, 제13권 제3장).

(2) 작용소의 콤팩트성(제13권 제4장).

(3) 함수공간의 콤팩트 매장(Arzelà–Ascoli 정리, Rellich 정리).

변분법과 편미분방정식의 해 존재 증명 대부분이 이 세 도구 가운데 하나에 의존한다.

또 다른 차이로, 무한차원 노름공간에서는 노름들이 서로 동치일 필요가 없고(유한차원에서는 모든 노름이 동치이다), 정의역 전체에서 정의된 선형 범함수가 연속이 아닐 수 있다(이런 불연속 범함수는 Hamel 기저와 선택공리를 이용해 구성한다). 실제 해석학에서 다루는 범함수는 언제나 연속인 것들이다.

1.5 고정점 정리의 응용

제9권의 **축약사상 원리**(제9권 제4장)는 완비 거리공간이기만 하면 성립하므로 Banach 공간 어디에서나 적용된다. 예를 들어 적분방정식

$$f(x) = g(x) + \lambda \int_0^1 k(x,y) f(y)\, \mathrm{d}y \tag{1.1}$$

은 $|\lambda|\,\|K\| < 1$이면 $C[0,1]$에서 유일한 해를 가지며, 그 해는 **Neumann 급수**

$$f = \sum_{n \geq 0} (\lambda K)^n g \tag{1.2}$$

로 주어진다. 일반적으로 $\|A\| < 1$이면 $I - A$는 가역이고

$$(I-A)^{-1} = \sum_{n \geq 0} A^n, \qquad \|(I-A)^{-1}\| \leq \frac{1}{1 - \|A\|} \tag{1.3}$$

이다(부분합이 $B(X)$에서 Cauchy열을 이루고, $B(X)$의 완비성으로 수렴하며, 그 극한이 $I-A$의 역임을 직접 확인한다). 식 (1.3)로부터, 가역 작용소의 집합은 $B(X)$의 열린부분집합임을 알 수 있다. T_0가 가역이고 $\|T - T_0\| < 1/\|T_0^{-1}\|$이면 $T = T_0(I - T_0^{-1}(T_0 - T))$에서 $\|T_0^{-1}(T_0 - T)\| < 1$이기 때문이다.

1.6 연습문제와 해설

연습문제 1.7 $\ell^1 \subsetneq \ell^2 \subsetneq \ell^\infty$임을 보이고 각 포함이 진부분임을 예로 확인하라.

풀이. $x \in \ell^1$이면 $|x_k| \to 0$이므로 충분히 큰 k에서 $|x_k| \le 1$이고, 따라서 $|x_k|^2 \le |x_k|$이므로 $x \in \ell^2$이다. ℓ^2의 원소는 성분이 0으로 가므로 유계수열이고 ℓ^∞에 속한다. 포함이 진부분임은 $(1/k)_{k\ge 1} \in \ell^2 \setminus \ell^1$(조화급수의 제곱합은 수렴하지만 조화급수 자체는 발산)과 $(1, 1, 1, \dots) \in \ell^\infty \setminus \ell^2$로 확인된다. 이는 $L^p(0,1)$의 포함 방향($L^\infty \subset L^2 \subset L^1$, 유한측도 공간에서 지수가 클수록 작은 공간)과 정반대임에 주의해야 한다. ℓ^p에서는 꼬리가 느리게 줄어드는 수열이 지수가 큰 공간에만 속하므로, 큰 지수가 더 큰 공간을 준다.

연습문제 1.8 $(Tf)(x) = \int_0^x f(t)\,dt$를 $C[0,1]$ 위의 작용소로 볼 때 $\|T\|$를 구하라.

풀이. $|Tf(x)| \le x\,\|f\|_\infty \le \|f\|_\infty$이므로 $\|T\| \le 1$이고, $f \equiv 1$에서 $\|Tf\|_\infty = 1$이므로 $\|T\| = 1$이다. 한편 반복 적용하면 $T^n f(x) = \int_0^x \frac{(x-t)^{n-1}}{(n-1)!} f(t)\,dt$이므로 $\|T^n\| \le 1/n!$이다. 따라서 $\|T^n\|^{1/n} \to 0$이며, 이는 T의 스펙트럼반지름이 0임을 뜻한다(제13권 제4장). 작용소 노름이 1이어도 반복에 따른 "평균적 크기"는 0으로 줄어든다는 점에서, 작용소 노름과 스펙트럼반지름이 서로 다른 양임을 보여 주는 예이다.

연습문제 1.9 ℓ^2에서 $\|A\| < 1$이면 $I - A$가 가역임을 보이고, 오른쪽 이동 S에 대해 $I - S/2$의 역을 급수로 써라.

풀이. 부분합 $\sum_{n\le N} A^n$은 $\sum_n \|A\|^n < \infty$(등비급수, 공비 $\|A\| < 1$)이므로 $B(\ell^2)$에서 Cauchy열이고 완비성으로 수렴한다. $(I - A)\sum_{n\le N} A^n = I - A^{N+1} \to I$이므로 그 극한이 $(I - A)^{-1}$이다. 오른쪽 이동 S는 등거리 사상이므로 $\|S/2\| = 1/2 < 1$이고

$$(I - S/2)^{-1} = \sum_{n\ge 0} 2^{-n} S^n,$$

즉 $(y_k)_{k\ge 0} \mapsto \left(\sum_{j\le k} 2^{-(k-j)} y_j\right)_{k\ge 0}$이다.

연습문제 1.10 $C[0,1]$에서 점 평가 $\delta_{1/2}(f) = f(1/2)$는 유계 범함수인가? $L^2[0,1]$에서는 어떠한가?

풀이. $C[0,1]$에서는 $|f(1/2)| \le \|f\|_\infty$이므로 유계이며 그 노름은 1이다(자명한 함수 $f \equiv 1$로 달성). $L^2[0,1]$에서는 원소가 거의 모든 점에서 같은 함수들의 동치류이므로 애초에 한 점에서의 값이 정의되지 않는다. 연속함수에만 정의역을 한정해도 f_n을 $1/2$ 근처에 너비 $1/n$, 높이 1인 좁은 봉우리로 두면 $\|f_n\|_2 \to 0$이지만 $f_n(1/2) = 1$이므로 유계가 아니다. 이것이 양자역학에서 "한 점에서의 파동함수 값"이 위치 고유상태로 정의되지 않는 수학적 이유이다($\delta_{1/2}$ 자체가 L^2 위의 유계 범함수가 아니기 때문).

참고 (다음 연결). 내적이 있으면 직교와 사영을 쓸 수 있어, 무한차원에서도 유한차원과 거의 같은 기하가 성립한다. 다음 장에서는 Hilbert 공간과 Fourier 급수를 다룬다(제13권 제2장).

제 2 장

Hilbert 공간과 Fourier 급수

개요 **Hilbert 공간**은 내적으로부터 나온 노름에 대해 완비인 벡터공간이며, 내적이 주는 직교 개념 덕분에 일반 Banach 공간보다 훨씬 유한차원에 가까운 기하를 갖는다. 이 장은 완비 내적공간에서 최근접점의 존재와 직교사영을 증명하고, 그로부터 Riesz 표현정리를 얻은 뒤, 정규직교기저에 의한 전개를 Fourier 급수로 구체화한다. 선행 지식: 앞 장의 노름공간(제13권 제1장), 제7권 제8장의 내적과 직교사영(제7권 제8장).

2.1 내적공간과 Hilbert 공간

정의 2.1 (내적공간과 Hilbert 공간) 복소 벡터공간 X 위의 **내적** $\langle x, y\rangle$은 첫 변수에 선형, 둘째 변수에 켤레선형이고 $\langle y, x\rangle = \overline{\langle x, y\rangle}$, $x \neq 0 \Rightarrow \langle x, x\rangle > 0$을 만족하는 함수이다. $\|x\| = \sqrt{\langle x, x\rangle}$가 노름이 되며, 이 노름에 대해 완비이면 X를 **Hilbert 공간**이라고 한다. ℓ^2와 $L^2(\mu)$가 기본 예이다.

주의 (켤레선형 자리의 규약). 이 권은 함수해석학의 관례, 곧 첫 변수에 선형·둘째 변수에 켤레선형인 규약을 따른다. 제7권 (제7권 제8장)과 양자역학 문헌은 첫 변수에 켤레선형인 반대 규약을 쓰므로, 그 쪽 자료의 공식을 이 권의 표기로 옮길 때는 두 변수의 순서를 바꾸어 읽어야 한다.

명제 2.2 (평행사변형 법칙) 내적에서 나온 노름은

$$\|x+y\|^2 + \|x-y\|^2 = 2\|x\|^2 + 2\|y\|^2 \tag{2.1}$$

을 만족한다. 역으로 식 (2.1)을 만족하는 노름은 (편극 항등식으로 복원되는) 어떤 내적에서 나온다.

L^p $(p \neq 2)$와 $C[0,1]$의 균등노름은 식 (2.1)을 만족하지 않으므로 (예컨대 $[0,1]$에서 $x(t)=1$, $y(t)=2t-1$을 L^∞에 넣으면 등식이 깨진다) 내적에서 나올 수 없고, 따라서 이 노름을 준 공간은 Hilbert 공간이 아니다.

2.2 최근접점과 직교사영

정리 2.3 (사영 정리) Hilbert 공간 H의 공집합이 아닌 닫힌 볼록집합 K와 점 $x \in H$에 대해, $\|x-y\|$를 최소로 하는 $y \in K$가 유일하게 존재한다. 특히 K가 닫힌 부분공간 M이면 그 최근접점 Px는 $x - Px \perp M$으로 특징지어지고, $H = M \oplus M^{\perp}$이다.

증명. $d = \inf_{y\in K}\|x-y\|$라 하고 $\|x-y_n\| \to d$인 수열 $(y_n) \subset K$를 잡는다. 평행사변형 법칙 (2.1)을 $x-y_n$, $x-y_m$에 적용하면

$$\|y_n - y_m\|^2 = 2\|x-y_n\|^2 + 2\|x-y_m\|^2 - 4\left\|x - \frac{y_n+y_m}{2}\right\|^2 \le 2\|x-y_n\|^2 + 2\|x-y_m\|^2 - 4d^2 \to 0$$

이다(마지막 부등식은 K의 볼록성으로 중점 $(y_n+y_m)/2$가 K에 속해 $\|x-(y_n+y_m)/2\|\ge d$이기 때문이다). 따라서 (y_n)은 Cauchy열이고, H의 완비성으로 $y_n\to y\in K$(K가 닫혀 있으므로)이며 $\|x-y\|=d$이다. 유일성도 두 최소점에 같은 부등식을 적용하면 나온다.

$K=M$이 부분공간인 경우, 임의의 $m\in M$, $t\in\mathbb{R}$에 대해 $\|x-y-tm\|^2$이 $t=0$에서 최소이므로 그 t에 대한 미분이 0, 즉 $\operatorname{Re}\langle x-y,m\rangle=0$이다. m을 im으로 바꾸면 허수부도 0이 되어 $\langle x-y,m\rangle=0$, 곧 $x-y\perp M$을 얻는다. $x=y+(x-y)\in M+M^{\perp}$이고 $M\cap M^{\perp}=\{0\}$이므로 $H=M\oplus M^{\perp}$이다. $\square$

완비성과 볼록성이 모두 꼭 필요한 가정이다(완비성 없이는 극한 y가 K 안에 있다고 보장할 수 없고, 볼록성 없이는 중점 논법이 성립하지 않는다). 유한차원 **최소제곱법**(제7권, 제23권)은 정리 2.3의 M이 유한차원 부분공간인 특수한 경우이다.

2.3 Riesz 표현정리

정리 2.4 (Riesz 표현정리) Hilbert 공간 H 위의 유계 선형 범함수 φ에 대해 $\varphi(x)=\langle x,y\rangle$인 $y\in H$가 유일하게 존재하고 $\|\varphi\|=\|y\|$이다.

증명. $\varphi=0$이면 $y=0$으로 자명하다. $\varphi\neq 0$이면 $M=\ker\varphi$는 닫힌 진부분공간이므로 정리 2.3로 $M^{\perp}\neq\{0\}$이고 $\|z\|=1$인 $z\in M^{\perp}$를 고를 수 있다. 임의의 $x\in H$에 대해 $\varphi(x)z-\varphi(z)x$는 φ로 보내면 0이 되므로 M에 속하고, 따라서 z와의 내적이 0이다: $\langle \varphi(x)z-\varphi(z)x,z\rangle=0$, 즉 $\varphi(x)\|z\|^2=\varphi(z)\langle x,z\rangle$. $\|z\|=1$이므로 정리하면 $\varphi(x)=\langle x,\overline{\varphi(z)}z\rangle$이다. $y=\overline{\varphi(z)}z$로 두면 되고, 유일성과 $\|\varphi\|=\|y\|$는 Cauchy–Schwarz 부등식으로 확인된다. $\square$

정리 2.4로 Hilbert 공간은 (켤레선형 사상을 통해) 자기 쌍대공간과 동일시된다. 이것이 Dirac의 bra-ket 표기에서 bra $\langle\psi|$를 ket $|\psi\rangle$와 짝지어 $\varphi(x)=\langle\psi|x\rangle$ 로 쓰는 근거이다. 제8장(제13권 제8장)에서는 이 정리를 쌍선형형식으로 일반화한 Lax–Milgram 정리로 편미분방정식의 약해를 얻는다.

2.4 정규직교기저

정규직교 집합 $\{e_k\}$에 대해 **Bessel 부등식**

$$\sum_{k}|\langle x,e_k\rangle|^2\le\|x\|^2 \tag{2.2}$$

이 성립한다. 유한 부분합에서 $x-\sum_{k\le n}\langle x,e_k\rangle e_k$가 각 e_j $(j\le n)$와 직교함을 확인하고 피타고라스 정리를 적용하면 $\|x\|^2=\bigl\|x-\sum_{k\le n}\langle x,e_k\rangle e_k\bigr\|^2+\sum_{k\le n}|\langle x,e_k\rangle|^2\ge\sum_{k\le n}|\langle x,e_k\rangle|^2$이고, $n\to\infty$에서 식 (2.2)을 얻는다.

정리 2.5 가산 정규직교 집합 $\{e_k\}$에 대해 다음은 동치이다.

(1) $\{e_k\}$의 유한 일차결합들이 H에서 조밀하다(**완비성**).

(2) 모든 $x\in H$에서 $x=\sum_k\langle x,e_k\rangle e_k$(노름 수렴).

(3) Parseval 등식 $\|x\|^2=\sum_k|\langle x,e_k\rangle|^2$가 모든 x에서 성립한다.

(4) $\langle x, e_k\rangle = 0$이 모든 k에서 성립하면 $x = 0$.

이 네 조건 가운데 하나(따라서 모두)를 만족하는 집합을 **정규직교기저**(완비 정규직교계)라고 한다. 정규직교기저가 가산인 Hilbert 공간을 **가분**(*separable*)이라고 하며, 무한차원 가분 Hilbert 공간은 모두 ℓ^2와 등거리 동형이다. 이 "기저"는 (가산) 무한 합을 노름 수렴의 의미로 허용하므로, 유한 일차결합만 허용하는 대수적 기저(Hamel 기저)와는 전혀 다른 개념이다.

Gram–Schmidt 과정으로 일차독립인 수열에서 정규직교계를 만들 수 있다. $L^2[-1,1]$에서 $1, x, x^2, \dots$에 이 과정을 적용하면, 정규화를 제외하고 **Legendre 다항식** $P_0 = 1$, $P_1 = x$, $P_2 = \tfrac{1}{2}(3x^2 - 1)$, … 를 얻는다. 구간 전체에서 가중치 e^{-x^2}을 주고 같은 과정을 적용하면 **Hermite 다항식**이 나오며, 이는 양자 조화진동자의 고유함수에 나타난다.

2.5 Fourier 급수

$L^2[-\pi,\pi]$에 내적 $\langle f, g\rangle = \dfrac{1}{2\pi}\displaystyle\int_{-\pi}^{\pi} f\bar{g}$를 주면, $e_k = e^{ikx}$ $(k \in \mathbb{Z})$는 정규직교이다.

정리 2.6 $\{e^{ikx}\}_{k\in\mathbb{Z}}$는 $L^2[-\pi,\pi]$의 정규직교기저이다. 따라서

$$\hat{f}(k) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)e^{-ikx}\,\mathrm{d}x \tag{2.3}$$

에 대해 $\sum_{|k|\le N}\hat{f}(k)e^{ikx} \to f$ (L^2에서)이고 $\dfrac{1}{2\pi}\displaystyle\int |f|^2 = \sum_{k}\left|\hat{f}(k)\right|^2$(Parseval 등식)이다.

완비성(정리 2.5의 조건 1)은 삼각다항식이 연속 주기함수 공간에서 균등 조밀하다는 사실(Stone–Weierstrass 정리, 또는 Fejér 정리로 직접)과, 연속함수가 L^2에서 조밀하다는 사실을 합쳐서 얻는다.

예제 2.7 (Basel 문제) $f(x) = x$ $(-\pi < x < \pi)$이면 식 (2.3)에서 $\hat{f}(k) = i(-1)^k/k$ $(k \neq 0)$, $\hat{f}(0) = 0$이다. Parseval 등식은

$$\frac{1}{2\pi}\int_{-\pi}^{\pi} x^2\,\mathrm{d}x = \frac{\pi^2}{3} = \sum_{k\neq 0}\frac{1}{k^2} = 2\sum_{k\ge 1}\frac{1}{k^2}$$

을 주므로 $\displaystyle\sum_{k\ge 1}k^{-2} = \pi^2/6$이다.

L^2 수렴은 점별수렴을 뜻하지 않는다. 연속함수의 Fourier 급수도 어떤 점에서 발산할 수 있다(제3장, 제13권 제3장). 그러나 조각마다 C^1인 함수의 Fourier 급수는 각 점에서 좌우극한의 평균 $\tfrac{1}{2}(f(x^+)+f(x^-))$로 (점별로) 수렴한다(**Dirichlet 정리**). 불연속점 근처에서는 부분합이 점프 크기의 약 9% 만큼 넘쳐 오르며, 이 넘침은 $N \to \infty$에서도 사라지지 않고 다만 폭이 좁아지기만 한다(**Gibbs 현상**). **Carleson 정리**는 L^2 함수의 Fourier 급수가 거의 모든 점에서(측도 0인 예외 집합을 제외하고) 수렴함을 보였다.

2.6 연습문제와 해설

연습문제 2.8 $L^2[-1,1]$에서 x^2에 가장 가까운 일차식 $a+bx$를 구하라.

풀이. 직교사영의 문제이다. 정규화된 Legendre 다항식 $q_0 = 1/\sqrt{2}$, $q_1 = \sqrt{3/2}\,x$에 대해 $\langle x^2, q_0\rangle = \int_{-1}^{1} x^2/\sqrt{2}\,dx = \dfrac{2}{3\sqrt{2}}$, $\langle x^2, q_1\rangle = 0$ (피적분함수가 기함수)이므로, x^2을 $\operatorname{span}\{q_0, q_1\}$(곧 모든 일차식의 공간)에 사영한 것은 $\dfrac{2}{3\sqrt{2}}\cdot\dfrac{1}{\sqrt{2}} = \dfrac{1}{3}$뿐이다. 따라서 답은 상수 $1/3$이다($b=0$은 x^2이 우함수라는 대칭성에서도 바로 나온다).

연습문제 2.9 $f(x)=|x|$의 $[-\pi,\pi]$ Fourier 급수를 구하고 Parseval 등식으로 $\sum_{k\ \text{홀수}} k^{-4}$를 계산하라.

풀이. f가 짝함수이므로

$$|x| = \frac{\pi}{2} - \frac{4}{\pi}\sum_{k\ \text{홀수}} \frac{\cos kx}{k^2}$$

이다(사인 계수는 모두 0이고, $a_0 = \pi$, 짝수 코사인 계수는 0). 실수 형식의 Parseval 등식 $\dfrac{1}{\pi}\displaystyle\int_{-\pi}^{\pi} f^2 = \frac{a_0^2}{2} + \sum_{k\ge 1} a_k^2$에서

$$\frac{2\pi^2}{3} = \frac{\pi^2}{2} + \frac{16}{\pi^2}\sum_{k\ \text{홀수}} k^{-4}$$

이므로 $\sum_{k\ \text{홀수}} k^{-4} = \pi^4/96$이다. 홀수 지수만의 합과 전체 합 사이에는 $\sum_{k\ \text{홀수}} k^{-4} = (1-2^{-4})\sum_{k\ge1} k^{-4} = \frac{15}{16}\zeta(4)$의 관계가 있으므로

$$\zeta(4) = \sum_{k\ge1} k^{-4} = \frac{16}{15}\cdot\frac{\pi^4}{96} = \frac{\pi^4}{90}$$

이다.

연습문제 2.10 ℓ^2에서 $e_n \to 0$이 약수렴(모든 $y\in\ell^2$에서 $\langle e_n, y\rangle \to 0$)함을 보이되, 노름 수렴은 아님을 보여라.

풀이. $\langle e_n, y\rangle = \overline{y_n} \to 0$이다. $\sum_k |y_k|^2 < \infty$인 급수의 항은 0으로 가야 하기 때문이다. 그러나 $\|e_n\| = 1$이 모든 n에서 일정하므로 e_n은 (노름의 뜻으로는) 0에 수렴하지 않는다. 무한차원 Hilbert 공간의 유계 수열은 약수렴하는 부분수열을 갖는다는 사실 (Banach–Alaoglu 정리의 결과)이, 제1장에서 말한 콤팩트성의 대체물 가운데 하나이다(제13권 제1장).

참고 (다음 연결). 완비성은 무한차원 해석학에서 매우 강력한 도구가 된다. 다음 장에서는 Baire 범주 정리에 기초한 세 정리—Hahn–Banach 정리, 균등유계원리, 열린사상 정리—를 다룬다(제13권 제3장).

제 3 장

Banach 공간의 세 기둥

개요 이 장은 함수해석학의 세 기본정리—Hahn–Banach 정리, 균등유계원리(Banach–Steinhaus 정리), 열린사상 정리(및 닫힌 그래프 정리)—를 세운다. 이들은 각각 무한차원에서 "선형 범함수가 충분히 많다", "점별 유계이면 균등 유계이다", "연속인 전단사 선형사상의 역은 자동으로 연속이다"를 보장하며, 세 정리 모두 완비성(Banach 공간, 또는 Baire 범주 정리가 적용되는 완비 거리공간)을 결정적인 가정으로 쓴다. 선행 지식: 앞 두 장(제13권 제1장, 제13권 제2장), 제5권의 선택공리와 Zorn 보조정리 (제5권 제6장), 제10권 제1장의 완비성(제10권 제1장).

3.1 Hahn–Banach 정리

정리 3.1 (Hahn–Banach 정리, 노름 형태) 노름공간 X의 부분공간 M 위의 유계 선형 범함수 φ는 노름을 보존하며 X 전체로 확장된다. 즉 $\Phi|_M = \varphi$, $\|\Phi\| = \|\varphi\|$인 $\Phi \in X^*$가 존재한다.

증명은 M에 속하지 않는 한 점을 더해 차원을 하나씩 늘려 가며, 각 단계에서 노름을 보존하는 확장이 가능함을 부등식 논법으로 보이고(실수 스칼라에서는 Hahn의 부등식 논법, 복소수에서는 실수부만 다루고 허수부를 복원), 그 과정을 Zorn 보조정리로 극대까지 밀어붙여 X 전체에 이르는 것이다. X가 가분 공간이면 가산 조밀부분집합을 하나씩 추가하는 수학적 귀납법만으로 충분하고 선택공리(Zorn 보조정리)가 필요 없다.

따름정리 3.2 $x \neq 0$이면 $\|\Phi\| = 1$, $\Phi(x) = \|x\|$인 $\Phi \in X^*$가 있다. 따라서 $\|x\| = \max_{\|\Phi\|\le 1} |\Phi(x)|$이고, 쌍대공간의 범함수들은 X의 점을 분리한다(서로 다른 두 점 $x \neq y$에 대해 $\Phi(x) \neq \Phi(y)$인 $\Phi \in X^*$가 있다).

정리 3.1의 기하적 형태는 **분리 정리**이다: 실 노름공간에서 서로소인 두 볼록집합 A(열린집합)와 B는 닫힌 초평면으로 분리된다. 즉 $\Phi(a) < c \le \Phi(b)$가 모든 $a \in A$, $b \in B$에서 성립하는 $\Phi \in X^* \setminus \{0\}$와 상수 c가 있다. 볼록 최적화의 쌍대성(제25권)과 경제학의 (균형) 가격 존재 정리가 이 분리 정리의 형태를 쓴다.

3.2 Baire 범주 정리

정리 3.3 (Baire) 완비 거리공간은 내부가 빈 닫힌집합들의 가산 합집합으로 쓸 수 없다. 동치로, 조밀한 열린집합들의 가산 교집합은 (공집합이 아니라) 조밀하다.

증명의 뼈대. 조밀한 열린집합 $U_1, U_2, \dots$와 임의의 열린 공 B_0가 주어졌다고 하자. U_1이 조밀하므로 $\overline{B_1} \subseteq B_0 \cap U_1$이고 반지름이 1보다 작은 닫힌 공 $\overline{B_1}$을 고를 수 있다. 이를 반복해, $\overline{B_k} \subseteq B_{k-1} \cap U_k$이고 반지름이 $1/k$보다 작은 공들의 감소하는 사슬 $B_0 \supset \overline{B_1} \supset B_1 \supset \overline{B_2} \supset \cdots$를

얻는다. 중심들은 반지름이 0으로 가므로 Cauchy 점열이고, 완비성으로 어떤 점에 수렴하며, 그 극한은 모든 $\overline{B_k}$에 (따라서 모든 U_k와 B_0에) 속한다. $\square$

응용 예: $\mathbb{R}$은 가산 개의 점만으로 쓸 수 없으므로(각 점은 내부가 빈 닫힌집합이다) 비가산집합이다. $C[0,1]$에서 어떤 점에서도 미분가능하지 않은 함수들의 여집합, 곧 "적어도 한 점에서 미분가능한 함수"들의 집합은 (내부가 빈 닫힌집합들의 가산 합집합에 포함되는) 범주론적 뜻에서 "작은" 집합임이 알려져 있다. 즉 범주의 의미에서 대부분의 연속함수는 어디서도 미분가능하지 않다. 제10권의 **Weierstrass 함수**는 예외적인 병리가 아니라 전형적인 연속함수의 모습이라는 뜻이다.

3.3 균등유계원리

정리 3.4 (Banach–Steinhaus) X가 Banach 공간이고 $\{T_\alpha\} \subseteq B(X,Y)$가 모든 $x \in X$에서 $\sup_\alpha \|T_\alpha x\| < \infty$(점별 유계)이면, $\sup_\alpha \|T_\alpha\| < \infty$(균등 유계)이다.

증명. $E_n = \{x \in X : \sup_\alpha \|T_\alpha x\| \le n\}$은 (각 T_α의 연속성으로) 닫힌집합이고, 점별 유계 가정으로 $\bigcup_n E_n = X$이다. X는 완비이므로 Baire 정리(정리 3.3)에 의해 어떤 E_n은 공집합이 아닌 내부, 곧 어떤 공 $B(x_0, r)$을 포함한다. $\|z\| < r$이면 $x_0 + z \in B(x_0,r) \subseteq E_n$이므로 $T_\alpha z = T_\alpha(x_0+z) - T_\alpha x_0$에서 $\|T_\alpha z\| \le \|T_\alpha(x_0+z)\| + \|T_\alpha x_0\| \le n + n = 2n$이다. 따라서 $\|T_\alpha\| \le 2n/r$이 모든 α에서 성립한다. $\square$

예제 3.5 (연속함수의 Fourier 급수가 발산할 수 있다) $S_N f(0) = \dfrac{1}{2\pi}\displaystyle\int_{-\pi}^{\pi} f(t) D_N(t)\,\mathrm{d}t$는 $C(\mathbb{T})$(주기 2π 연속함수 공간, 균등노름) 위의 유계 선형 범함수이고, 그 노름은 **Lebesgue 상수** $L_N = \dfrac{1}{2\pi}\displaystyle\int |D_N|$이다. 여기서

$$D_N(t) = \frac{\sin\!\left(\left(N+\tfrac{1}{2}\right)t\right)}{\sin(t/2)}$$

은 **Dirichlet 핵**이다. $L_N \sim \dfrac{4}{\pi^2}\log N \to \infty$이므로, 정리 3.4의 대우로 $\sup_N |S_N f(0)| = \infty$인 연속함수 f가 (구체적으로 무엇인지 지정하지 않고도) 존재해야 한다. 이러한 함수의 구체적인 예는 du Bois-Reymond가 1873년에 처음 만들었다.

같은 논법으로, 보간 노드의 배열을 어떻게 고르더라도 모든 연속함수에서 균등수렴하는 다항식 보간법은 없다는 **Faber 정리**도 얻는다. 등간격 노드에서 나타나는 **Runge 현상**(제25권)은 이 사실의 대표적인 사례이다.

3.4 열린사상 정리와 닫힌 그래프 정리

정리 3.6 (열린사상 정리) Banach 공간 사이의 전사 유계 선형사상은 열린사상이다. 따라서 전단사 유계 선형사상의 역사상도 유계이다(**유계역정리**).

정리 3.7 (닫힌 그래프 정리) Banach 공간 X, Y 사이의 선형사상 $T : X \to Y$의 그래프 $\{(x, Tx) : x \in X\}$가 $X \times Y$에서 닫혀 있으면, T는 유계이다.

닫힌 그래프 조건은 "$x_n \to x$이고 $Tx_n \to y$이면 $y = Tx$"이고, 연속성 자체의 조건인 "$x_n \to x$이면 Tx_n이 (어딘가로) 수렴한다"보다 확인하기 쉽다. 정리 3.7는 완비성(열린사상 정리와 Baire 범주 정리)을 이용해 그 수렴 자체를 거저 얻게 해 준다.

> **예제 3.8 (완비성이 없으면 실패한다)** $C^1[0,1]$에 (고유 노름 $\|f\|_{C^1}$ 대신) 균등노름 $\|\cdot\|_\infty$을 그대로 주면 완비가 아니다(연속이지만 미분불가능한 함수로 수렴하는 C^1 함수열이 있다). 이 공간에서 미분 작용소 $D : C^1 \to C[0,1]$은 그래프가 닫혀 있다(균등수렴 $f_n \to f$와 도함수의 균등수렴 $f_n' \to g$가 동시에 있으면 극한의 도함수가 g와 일치한다는 해석학의 표준 정리). 그러나 D는 (정의역에 균등노름을 준 이 설정에서는) 유계가 아니다(예제 1.4 참조). 이는 닫힌 그래프 정리의 완비성 가정이 실제로 필요함을 보여 준다: 정의역 $C^1[0,1]$에 균등노름이 아니라 제 노름(이 노름에서는 완비이다)을 주어야만 정리가 적용된다.

3.5 응용: 노름의 비교와 안정성

같은 벡터공간 위의 두 노름 $\|\cdot\|_1$, $\|\cdot\|_2$가 모두 완비이고 $\|x\|_2 \le C\,\|x\|_1$ (모든 x에서)이면, 항등사상 $(X,\|\cdot\|_1) \to (X,\|\cdot\|_2)$은 전단사 유계 선형사상이므로 유계역정리(정리 3.6)를 적용해 그 역도 유계이고, 두 노름은 동치이다. 즉 완비인 두 노름은 한쪽이 다른 쪽을 지배하기만 하면(한 방향 부등식만 성립해도) 자동으로 서로 동치이다.

수치해석에서 **Lax 동치정리**("일관된 선형 차분법은 안정할 때 그리고 오직 그때에만 수렴한다")의 증명에도 균등유계원리가 핵심적으로 쓰인다. 안정성이 바로 그 차분법이 만드는 작용소 열의 균등 유계성을 뜻하기 때문이다(제25권).

3.6 연습문제와 해설

> **연습문제 3.9** c_0(0으로 수렴하는 수열의 공간, 상한 노름)에서 $T_n(x) = \sum_{k\le n} x_k$는 각 x에서 유계 수열 $(T_n(x))_n$을 주는가? $\|T_n\|$은 얼마인가?

풀이. $\|T_n\| = n$이다. $x = (1,\dots,1,0,0,\dots)$($1$이 n개)이면 $\|x\|_\infty = 1$이고 $T_n(x) = n$이므로 $\|T_n\| \ge n$이며, $|T_n(x)| \le n\,\|x\|_\infty$로 $\|T_n\| \le n$이다. 균등유계원리 (정리 3.4)의 대우로, $\|T_n\| \to \infty$이므로 $\sup_n |T_n(x)| = \infty$인 $x \in c_0$가 존재해야 한다. 실제로 $x_k = 1/k$이면 $x \in c_0$이지만 $T_n(x)$는 조화급수의 부분합이라 발산한다.

> **연습문제 3.10 (Hellinger–Toeplitz 정리)** Hilbert 공간에서 $\langle Tx, y\rangle = \langle x, Ty\rangle$가 모든 x, y에서 성립하는 선형사상 $T : H \to H$는 유계임을 보여라.

풀이. $x_n \to x$, $Tx_n \to z$라 하자. 모든 $y \in H$에서

$$\langle z, y\rangle = \lim_n \langle Tx_n, y\rangle = \lim_n \langle x_n, Ty\rangle = \langle x, Ty\rangle = \langle Tx, y\rangle$$

이므로 $z - Tx$가 모든 y와 직교하고, 따라서 $z = Tx$이다. 즉 T의 그래프는 닫혀 있고, 닫힌 그래프 정리(정리 3.7)로 T는 유계이다. 따라서 양자역학의 비유계 자기수반 연산자(해밀토니안 등)는 이 성질(대칭성 $\langle Tx, y\rangle = \langle x, Ty\rangle$)을 공간 전체에서 가질 수 없고, 반드시 조밀한 진부분공간에서만 정의되어야 한다.

연습문제 3.11 Baire 정리를 이용하여 무한차원 Banach 공간은 가산 Hamel 기저를 가질 수 없음을 보여라.

풀이. 가산 Hamel 기저 $\{b_k\}_{k\ge 1}$가 있다고 가정하면, $X = \bigcup_{n} F_n$, $F_n = \operatorname{span}\{b_1, \dots, b_n\}$ 이다. 각 F_n은 유한차원이므로 (완비 부분공간이라) X에서 닫혀 있고, X 자신과 같지 않은 진부분공간이므로 (기저가 무한히 많은 벡터를 필요로 하므로) 내부가 비어 있다. 그러면 X는 내부가 빈 닫힌집합들의 가산 합집합이 되어 Baire 정리(정리 3.3)에 모순된다. 그러므로 ℓ^2와 같은 무한차원 Hilbert(또는 Banach) 공간에서 "기저"란 항상 무한 합을 허용하는 정규직교기저 (제13권 제2장)를 뜻하며, 대수적 Hamel 기저가 아니다.

참고 (다음 연결). 무한차원 작용소 가운데 유한차원 행렬과 가장 비슷하게 행동하는 것이 콤팩트 작용소이다. 다음 장에서는 그 스펙트럼 이론을 다룬다(제13권 제4장).

제 4 장

스펙트럼과 콤팩트 작용소

개요 작용소의 **스펙트럼**(*spectrum*)은 유한차원 선형대수의 고유값 개념을 무한차원 Banach·Hilbert 공간으로 확장한 것으로, 고유값 집합을 포함하되 일반적으로 그보다 크다. 이 장은 유계 작용소의 스펙트럼을 해집합의 여집합으로 정의하고 점·연속·잉여 스펙트럼으로 분류한 뒤, 콤팩트 자기수반 작용소에 대해서는 유한차원과 거의 같은 꼴의 스펙트럼 정리(고유값과 고유벡터로의 전개)가 성립함을 증명한다. 이어서 콤팩트 작용소가 섞인 방정식의 가해성을 다루는 Fredholm 대안을 소개하고, 비유계 작용소에서는 대칭성과 자기수반성이 서로 다른 개념임을 짚는다. 이 정리들은 제6장의 Sturm–Liouville 이론과 양자역학의 고유함수 전개가 성립하는 이유를 제공한다. 선행 지식: 이 책 앞부분의 노름공간, 유계 선형작용소, Hilbert 공간과 Riesz 표현정리(제13권 제1장, 제13권 제2장), 열린사상 정리(제13권 제3장), 대칭행렬의 스펙트럼 정리(제7권 제7장).

4.1 스펙트럼

Banach 공간 X 위의 유계 작용소 T에 대해 $T-\lambda I$가 유계인 역을 갖는 $\lambda \in \mathbb{C}$들의 집합을 **해집합**(*resolvent set*) $\rho(T)$라 하고, 그 여집합을 **스펙트럼**(*spectrum*) $\sigma(T)$라 한다(이하 X는 복소 Banach 공간이다). 유한차원에서는 $\sigma(T)$가 바로 고유값의 집합이지만, 무한차원에서는 $T-\lambda I$가 단사이면서도 전사가 아닐 수 있으므로 스펙트럼이 고유값의 집합보다 크다. 스펙트럼은 성질에 따라 다음 세 가지로 나뉜다.

- **점 스펙트럼**(*point spectrum*): $T-\lambda I$가 단사가 아니다(즉 λ가 고유값이다).
- **연속 스펙트럼**(*continuous spectrum*): $T-\lambda I$가 단사이고 치역이 조밀하지만 전사가 아니다.
- **잉여 스펙트럼**(*residual spectrum*): $T-\lambda I$가 단사이지만 치역이 조밀하지 않다.

정리 4.1 (스펙트럼의 콤팩트성과 스펙트럼반지름) $\sigma(T)$는 공집합이 아닌 콤팩트 집합이고 $\sigma(T)\subseteq\{\lambda : |\lambda|\le \|T\|\}$이다. **스펙트럼반지름**(*spectral radius*)은

$$r(T)=\max_{\lambda\in\sigma(T)}|\lambda|=\lim_{n\to\infty}\|T^n\|^{1/n} \tag{4.1}$$

이다(Gelfand 공식).

증명. $|\lambda|>\|T\|$이면 $T-\lambda I=-\lambda(I-T/\lambda)$이고 $\|T/\lambda\|<1$이므로 Neumann 급수 $(T-\lambda I)^{-1}=-\lambda^{-1}\sum_{n\ge 0}(T/\lambda)^n$이 (작용소 노름에 대해) 수렴하여 가역이다. 따라서 $\sigma(T)\subseteq\{|\lambda|\le\|T\|\}$이고 유계이다. 가역 작용소의 집합이 (같은 Neumann 급수 논법으로) 열려 있으므로 $\rho(T)$도 열려 있고, $\sigma(T)$는 그 여집합이므로 닫혀 있다. 유계이고 닫힌 집합이므로 $\sigma(T)$는 콤팩트이다. $\sigma(T)$가 공집합이 아님은 해석함수 $\lambda\mapsto(T-\lambda I)^{-1}$(정의역 $\rho(T)$)에 Liouville 정리를 적용하여 보인다(제11권 제4장): $\sigma(T)=\emptyset$이면 이 함수가 $\mathbb{C}$ 전체에서 정의된 해석함수가 되고, $|\lambda|\to\infty$에서 Neumann

급수로 0에 수렴하므로 유계이기도 하다. Liouville 정리로 상수함수, 그것도 0이어야 하는데 이는 $(T-\lambda I)^{-1}$이 가역 작용소라는 사실과 모순이다. Gelfand 공식의 증명은 복소함수론의 Laurent 급수 전개(레졸벤트의 멱급수 전개)에 의존하므로 생략한다. □

예제 4.2 (적분 작용소의 스펙트럼) 제1장 연습문제의 적분 작용소(Volterra 작용소) $(Tf)(x)=\int_0^x f$는 $r(T)=0$, 즉 $\sigma(T)=\{0\}$이지만 0은 고유값이 아니다. $Tf=0$이면 양변을 미분하여 $f=0$을 얻기 때문이다.

예제 4.3 (곱셈 작용소) $L^2[0,1]$에서 $(Mf)(x)=xf(x)$의 스펙트럼은 $[0,1]$이지만 고유값은 없다. $xf=\lambda f$가 a.e.로 성립하면 $(x-\lambda)f(x)=0$이 a.e.에서 성립하므로, $x\neq\lambda$인 거의 모든 점에서 $f=0$이고 결국 $f=0$ a.e.이기 때문이다. 양자역학의 위치 연산자처럼 연속 스펙트럼만 갖는 예이다.

4.2 수반 작용소와 자기수반성

Hilbert 공간에서 유계 작용소 T의 **수반**(*adjoint*) T^{*}를 $\langle Tx,y\rangle=\langle x,T^{*}y\rangle$ $(x,y\in H)$로 정의한다. 각 고정된 y에 대해 $x\mapsto\langle Tx,y\rangle$가 유계 선형범함수이므로 Riesz 표현정리에 의해 그러한 $T^{*}y$가 유일하게 존재한다. $T=T^{*}$이면 T를 **자기수반**(*self-adjoint*)이라 한다.

명제 4.4 (자기수반 작용소의 기본 성질) 자기수반 작용소 T에 대해 다음이 성립한다.

(1) 고유값은 모두 실수이다.

(2) 서로 다른 고유값에 대응하는 고유벡터는 직교한다.

(3) $\sigma(T)\subseteq\mathbb{R}$이고 $\|T\|=\sup_{\|x\|=1}|\langle Tx,x\rangle|$이다.

증명. (1) $Tx=\lambda x$, $x\neq0$이라 하면 $\langle Tx,x\rangle=\lambda\|x\|^2$이고, 자기수반성과 내적의 켤레대칭성으로

$$\langle Tx,x\rangle=\langle x,Tx\rangle=\overline{\langle Tx,x\rangle}$$

이므로 $\langle Tx,x\rangle$는 실수이다. $\|x\|^2>0$이 실수이므로 $\lambda=\langle Tx,x\rangle/\|x\|^2\in\mathbb{R}$이다.

(2) $Tx=\lambda x$, $Ty=\mu y$, $\lambda\neq\mu$($\lambda,\mu\in\mathbb{R}$, (1)에 의해)라 하면

$$\lambda\langle x,y\rangle=\langle Tx,y\rangle=\langle x,Ty\rangle=\mu\langle x,y\rangle$$

이므로 $(\lambda-\mu)\langle x,y\rangle=0$이고, $\lambda\neq\mu$에서 $\langle x,y\rangle=0$이다.

(3) $M=\sup_{\|x\|=1}|\langle Tx,x\rangle|$로 두면 Cauchy–Schwarz 부등식으로 $M\le\|T\|$이다. 역부등식은 편극항등식에서 얻는다. 단위벡터 x,y에 대해

$$\langle T(x+y),x+y\rangle-\langle T(x-y),x-y\rangle=4\,\mathrm{Re}\langle Tx,y\rangle$$

이고 평행사변형 법칙 $\|x+y\|^2+\|x-y\|^2=2\|x\|^2+2\|y\|^2=4$로

$$4\,|\mathrm{Re}\langle Tx,y\rangle|\le M\bigl(\|x+y\|^2+\|x-y\|^2\bigr)=4M$$

이다. y를 적절한 위상 $e^{i\theta}y$로 바꾸어 $\langle Tx,y\rangle$가 음이 아닌 실수가 되게 하면 $|\langle Tx,y\rangle|\le M$을 모든 단위벡터 x,y에 대해 얻고, y에 대해 상한을 취하면 $\|Tx\|\le M$, 즉 $\|T\|\le M$이다. 따라서 $\|T\|=M$이다.

$\sigma(T)\subseteq\mathbb{R}$을 보이기 위해 $\lambda=a+ib$ $(a,b\in\mathbb{R})$로 쓰고 $S=T-aI$(자기수반)로 둔다. 모든 $x\in H$에 대해

$$\|(T-\lambda I)x\|^2=\|Sx-ibx\|^2=\|Sx\|^2+b^2\|x\|^2\geq b^2\|x\|^2$$

이다(전개하면 교차항이 $ib\langle Sx,x\rangle-ib\langle x,Sx\rangle$인데 $\langle Sx,x\rangle\in\mathbb{R}$이므로 $\langle x,Sx\rangle=\overline{\langle Sx,x\rangle}=\langle Sx,x\rangle$이어서 두 항이 상쇄된다). $b\neq0$이면 이 부등식은 $T-\lambda I$가 단사이고 치역이 닫혀 있음을 보여 준다(치역 위에서 역이 노름 $1/|b|$ 이하로 유계). 같은 부등식을 $T-\bar\lambda I=T^*-\bar\lambda I=(T-\lambda I)^*$에 적용하면 이것도 단사이므로, $\operatorname{ran}(T-\lambda I)^\perp=\ker(T-\lambda I)^*=\ker(T-\bar\lambda I)=\{0\}$, 즉 치역이 조밀하다. 닫혀 있고 조밀한 부분공간은 전체 공간이므로 $T-\lambda I$는 전단사이고 (열린사상정리로) 역도 유계, 곧 $\lambda\in\rho(T)$이다. 따라서 $b\neq0$이면 $\lambda\notin\sigma(T)$이고, 결국 $\sigma(T)\subseteq\mathbb{R}$이다. □

4.3 콤팩트 작용소

정의 4.5 (콤팩트 작용소) Banach 공간 X,Y 사이의 선형사상 T가 X의 모든 유계 집합을 Y의 상대 콤팩트 집합(폐포가 콤팩트인 집합)으로 보내면 T를 **콤팩트 작용소**(*compact operator*)라 한다.

유한 계수 작용소(*finite-rank operator*, 치역이 유한차원인 유계 작용소)는 콤팩트이다. 치역이 유한차원이면 유계 집합의 상이 유계인 유한차원 집합이고, 유한차원 공간에서는 유계 닫힌 집합이 콤팩트(Heine–Borel 성질)이기 때문이다. 콤팩트 작용소의 노름 극한도 콤팩트이다. Hilbert 공간에서는 역으로 모든 콤팩트 작용소가 유한 계수 작용소의 노름 극한이다(정규직교기저로 만든 사영 P_N에 대해 $\|TP_N-T\|\to0$). 무한차원에서 항등 작용소는 콤팩트가 아니다(Riesz 정리, 제13권 제1장): 닫힌 단위구가 콤팩트가 아니기 때문이다.

예제 4.6 (Hilbert–Schmidt 적분 작용소) $k\in L^2([a,b]^2)$이면 $(Kf)(x)=\int_a^b k(x,y)f(y)\,dy$는 $L^2[a,b]$에서 콤팩트이며 $\|K\|\leq\|k\|_{L^2}$이다. k를 정규직교기저 $\{e_i(x)\overline{e_j(y)}\}$로 전개하여 부분합으로 유한 계수 근사 K_N을 만들면, 버려진 항들의 계수 제곱합이 $\|k\|_{L^2}^2$로 수렴하므로 $\|K-K_N\|\to0$이고 콤팩트성이 나온다. $k(x,y)=\overline{k(y,x)}$이면 K는 자기수반이다.

4.4 콤팩트 자기수반 작용소의 스펙트럼 정리

정리 4.7 (콤팩트 자기수반 작용소의 스펙트럼 정리) T가 Hilbert 공간 H 위의 콤팩트 자기수반 작용소이면, 0이 아닌 실수 고유값들 $\lambda_1,\lambda_2,\dots$(유한개이거나 0으로 수렴하는 수열)과 정규직교 고유벡터 $e_1,e_2,\dots$가 존재하여

$$Tx=\sum_{k}\lambda_k\langle x,e_k\rangle e_k\qquad(x\in H)\tag{4.2}$$

이다. 0이 아닌 각 고유값의 고유공간은 유한차원이고, $\{e_k\}$에 $\ker T$의 정규직교기저를 더하면 H의 정규직교기저가 된다.

증명의 뼈대. $\|T\|=\sup_{\|x\|=1}|\langle Tx,x\rangle|$(명제 4.4(3))를 달성하는 단위벡터가 콤팩트성으로 존재하고, 그것이 고유값 $\pm\|T\|$의 고유벡터임을 보인다(Rayleigh 몫의 최대화). 그 고유벡터의 직교여공간은 T-불변이므로 같은 논법을 반복하여 다음으로 큰(절댓값) 고유값과 고유벡터를 얻는다.

고유값이 0으로 수렴하는 것은 콤팩트성 때문이다: 직교하는 단위 고유벡터들의 상 $\lambda_k e_k$가 (콤팩트 작용소는 유계열을 상대 콤팩트 집합으로 보내므로) 수렴하는 부분수열을 가져야 하는데, $k \neq l$이면 $\|\lambda_k e_k - \lambda_l e_l\|^2 = \lambda_k^2 + \lambda_l^2$이므로 이 수열이 코시 부분수열을 가지려면 $\lambda_k \to 0$이어야 한다. $\square$

고유값의 변분 특성(최소최대 원리)도 유한차원과 같다. 양의 고유값을 큰 순서로 $\lambda_1 \geq \lambda_2 \geq \cdots$라 하면

$$\lambda_k = \max_{\dim V = k} \; \min_{x \in V,\, \|x\|=1} \langle Tx, x \rangle. \tag{4.3}$$

이 공식은 수치계산(Rayleigh–Ritz 방법)과 고유값의 비교 정리에 쓰인다.

4.5 Fredholm 대안

> **정리 4.8 (Fredholm 대안)** K가 콤팩트 작용소이고 $\lambda \neq 0$이면 다음 중 정확히 하나가 성립한다.
>
> (1) $(K - \lambda I)x = y$가 모든 y에 대해 유일한 해를 갖는다.
>
> (2) $(K - \lambda I)x = 0$이 0이 아닌 해를 갖는다.
>
> (2)의 경우 $(K - \lambda I)x = y$가 해를 가질 필요충분조건은 $y \perp \ker(K^* - \bar{\lambda} I)$이다.

유한차원의 "정사각행렬은 단사이면 전사이다"라는 명제가 $\lambda I -$ (콤팩트) 꼴의 작용소에서도 살아남는다는 정리이다. 경계값 문제의 해가 존재할 조건(공명 조건)이 이 대안으로 표현된다.

> **예제 4.9 (공명 조건)** $-u'' - \pi^2 u = f$, $u(0) = u(1) = 0$은 $\sin \pi x$가 동차방정식의 0이 아닌 해이므로(즉 $\lambda = \pi^2$이 대응하는 콤팩트 적분 작용소의 고유값이므로) $\int_0^1 f(x) \sin \pi x \, dx = 0$일 때만 해를 갖는다.

4.6 비유계 작용소에 대한 주석

양자역학의 해밀토니안이나 미분 작용소 $-\dfrac{d^2}{dx^2}$는 비유계이며 조밀한 정의역 $D(A) \subsetneq H$에서만 정의된다. 이때 **대칭성**(*symmetry*, $\langle Ax, y\rangle = \langle x, Ay\rangle$, $x, y \in D(A)$)과 **자기수반성**(*self-adjointness*, $A = A^*$이고 정의역까지 $D(A) = D(A^*)$)은 서로 다르다. 관측가능량이 실수 스펙트럼과 스펙트럼 분해를 가지려면 자기수반이어야 하며, 대칭이기만 한 작용소는 경계조건을 추가로 정해야 비로소 자기수반이 된다.

주의 (대칭성과 자기수반성의 차이). $-i\frac{d}{dx}$를 $[0,1]$ 위에서 정의할 때, 경계조건 $f(1) = e^{i\theta} f(0)$마다 서로 다른 자기수반 확장이 존재한다($\theta \in [0, 2\pi)$마다 하나씩, 무한히 많은 확장). 서로 다른 θ에 대응하는 작용소는 정의역부터 다른, 서로 다른(그러나 각각 자기수반인) 연산자이다. 무한우물에서 운동량 연산자의 자기수반 확장이 미묘한 이유이다.

4.7 연습문제와 해설

연습문제 4.10 ℓ^2에서 $T(x_1, x_2, \dots) = (x_1, x_2/2, x_3/3, \dots)$가 콤팩트 자기수반임을 보이고 스펙트럼을 구하라.

풀이. 유한 계수 작용소 T_N(처음 N개 성분만 남기고 나머지를 0으로 둠)에 대해 $\|T - T_N\| = 1/(N+1) \to 0$이므로 T는 콤팩트이다. T는 실수 대각 작용소이므로 자기수반이다. 고유값은 $1/k$ $(k \ge 1)$이고 그 극한 0을 더하여 $\sigma(T) = \{0\} \cup \{1/k : k \ge 1\}$이며, 0은 고유값이 아니다($Tx = 0$이면 모든 성분이 0이다).

연습문제 4.11 $L^2[0,1]$에서 $(Kf)(x) = \int_0^1 \min(x,y) f(y)\,dy$의 고유값을 구하라.

풀이. $u = Kf$로 두면 $u(x) = \int_0^x y f(y)\,dy + x\int_x^1 f(y)\,dy$이고, 미분하면 $u'(x) = \int_x^1 f(y)\,dy$, $u''(x) = -f(x)$이다. 또한 $u(0) = 0$, $u'(1) = 0$이다. $Kf = \lambda f$에서 $f = u/\lambda$이므로 $u'' = -u/\lambda$, 즉 $u = \sin(x/\sqrt{\lambda})$ 꼴(경계조건 $u(0)=0$을 만족하는 해)이고, 경계조건 $u'(1) = 0$에서 $\cos(1/\sqrt{\lambda}) = 0$, 즉 $1/\sqrt{\lambda} = (k - \tfrac{1}{2})\pi$이다. 따라서

$$\lambda_k = \frac{1}{(k-\tfrac{1}{2})^2 \pi^2}, \qquad (k = 1, 2, \dots).$$

이 핵은 Brown 운동의 공분산 함수이며, Karhunen–Loève 전개의 계수가 여기서 나온다.

연습문제 4.12 K가 콤팩트이고 $\|Kx_n\| \to \|K\|$, $\|x_n\| = 1$일 때 x_n의 약수렴 부분수열에 대해 무엇을 말할 수 있는가?

풀이. Hilbert 공간의 닫힌 단위구는 약콤팩트이므로 $x_{n_j} \rightharpoonup x$인 부분수열이 있다. 콤팩트 작용소는 약수렴 수열을 노름수렴 수열로 보내므로 $Kx_{n_j} \to Kx$이고, 노름의 연속성으로 $\|Kx\| = \|K\|$이다. 따라서 $x \neq 0$이다. 또한 약하한 반연속성으로 $\|x\| \le \liminf \|x_{n_j}\| = 1$이고, $\|Kx\| \le \|K\|\,\|x\| \le \|K\|$에서 등호가 성립하려면 $\|x\| = 1$이어야 한다. 즉 $\|T\|$를 달성하는 상한이 실제로 어떤 단위벡터에서 이루어지며, 이것이 정리 4.7의 증명에서 쓰는 단계이다.

다음 연결. 이제 미분방정식으로 돌아간다. 다음 장(제13권 제5장)에서는 편미분방정식의 분류와 1계 방정식의 특성곡선, 파동방정식의 d'Alembert 공식을 다룬다.

제 5 장

편미분방정식의 분류, 특성곡선, 파동방정식

개요 **편미분방정식**(*partial differential equation*)은 여러 변수에 대한 함수와 그 편도함수 사이의 관계식이다. 이 장은 2계 선형 편미분방정식을 판별식의 부호에 따라 포물형·쌍곡형·타원형 세 유형으로 분류하고, 1계 방정식을 **특성곡선**(*characteristic curve*)을 따라 상미분방정식으로 바꾸는 방법을 설명한 뒤, 1차원 파동방정식의 d'Alembert 공식과 고차원에서의 Kirchhoff 공식을 유도한다. 유형에 따라 문제 설정(초기값·경계값)이 근본적으로 달라진다는 사실과, 해가 자료에 연속적으로 의존하는 잘 정립된 문제의 개념이 이 장의 중심이다. 선행 지식: 다변수 함수와 연쇄법칙(제9권 제2장), 제12권(미분방정식·동역학)의 1계 상미분방정식.

5.1 세 가지 원형

편미분방정식의 가장 기본적인 세 가지 원형은 다음과 같다.

- **열방정식**(*heat equation*) $u_t = k\nabla^2 u$ (포물형): 확산, 열전도, 확률밀도의 시간 진화.
- **파동방정식**(*wave equation*) $u_{tt} = c^2\nabla^2 u$ (쌍곡형): 현의 진동, 음파, 전자기파.
- **Laplace 방정식** $\nabla^2 u = 0$ (타원형): 정전기 퍼텐셜, 정상 열분포, 비압축 퍼텐셜 흐름.

2변수 2계 선형 방정식

$$a u_{xx} + 2b u_{xy} + c u_{yy} + (\text{저차항}) = 0 \tag{5.1}$$

은 판별식 $b^2 - ac$의 부호로 **쌍곡형**($b^2 - ac > 0$), **포물형**($b^2 - ac = 0$), **타원형**($b^2 - ac < 0$)으로 나뉜다. 원뿔곡선 $ax^2 + 2bxy + cy^2 =$ 상수의 분류와 같은 대수적 구조이다. 계수 a, b, c가 영역에 따라 변하면 한 방정식이 영역에 따라 유형을 바꿀 수 있다. Tricomi 방정식 $y u_{xx} + u_{yy} = 0$은 $y > 0$에서 타원형($b^2 - ac = -y < 0$), $y < 0$에서 쌍곡형이며 천음속 흐름의 모형이다.

이 분류가 상수계수인 경우에 실제로 쓸모 있는 이유는 다음과 같다. 식 (5.1)에 $u = F(y - \lambda x)$ 꼴을 대입하면 $u_{xx} = \lambda^2 F''$, $u_{xy} = -\lambda F''$, $u_{yy} = F''$이므로 $(a\lambda^2 - 2b\lambda + c)F'' = 0$을 얻고, $F'' \not\equiv 0$인 한 λ는 2차방정식 $a\lambda^2 - 2b\lambda + c = 0$의 근이어야 한다. 이 방정식의 판별식은 $4(b^2 - ac)$로 분류 판별식과 같은 부호를 가지므로, 쌍곡형이면 서로 다른 두 실근 λ_1, λ_2가 있어 일반해가 $u = F(y - \lambda_1 x) + G(y - \lambda_2 x)$ 꼴이 된다(F, G는 임의의 두 번 미분가능한 함수). 연습문제 5.3이 이 계산의 예이다.

유형마다 적절한 문제 설정이 다르다. 쌍곡형은 초기값(위치와 속도), 포물형은 초기값 하나와 경계값, 타원형은 경계값이 자연스럽다. 해가 존재하고 유일하며 자료에 연속적으로 의존하는 문제를 **잘 정립된**(*well-posed*) 문제라 한다(Hadamard).

> **예제 5.1 (잘 정립되지 않은 문제)** Laplace 방정식의 초기값 문제 $u_{xx} + u_{yy} = 0$, $u(x,0) = 0$, $u_y(x,0) = \frac{1}{n}\sin(nx)$의 해는 $u = \frac{1}{n^2}\sin(nx)\sinh(ny)$이다. 자료는 $n \to \infty$에서 0으로 가지

만($\sup_x |u_y(x,0)| = 1/n \to 0$), 고정된 $y>0$에서 해는 $n\to\infty$일 때 지수적으로 커진다($\sinh(ny)\sim e^{ny}/2$). 타원형 방정식에 초기값 문제를 주면 연속 의존성이 깨진다.

5.2 1계 선형 방정식과 특성곡선

수송방정식 $u_t + c u_x = 0$은 직선 $x - ct =$ 상수를 따라 u가 상수임을 뜻한다. 실제로 $\frac{\mathrm{d}}{\mathrm{d}t}u(x_0+ct,t) = u_t + c u_x = 0$이다. 따라서 $u(x,t) = f(x-ct)$, 즉 초기 모양이 속도 c로 그대로 이동한다. 일반적으로 1계 선형(또는 준선형) 방정식 $a(x,y)u_x + b(x,y)u_y = g(x,y,u)$에서 **특성곡선**(*characteristic curve*)

$$\frac{\mathrm{d}x}{\mathrm{d}s} = a, \qquad \frac{\mathrm{d}y}{\mathrm{d}s} = b \tag{5.2}$$

을 따라 $\frac{\mathrm{d}u}{\mathrm{d}s} = g$이다. 편미분방정식이 특성곡선 위에서의 상미분방정식들의 모임으로 분해되는 것이다.

예제 5.2 $u_x + 2xu_y = 0$, $u(0,y) = e^{-y^2}$를 생각한다. 특성곡선은 $\frac{\mathrm{d}y}{\mathrm{d}x} = 2x$, 즉 $y - x^2 =$ 상수이고 그 위에서 u는 상수이다. $x=0$에서 이 상수선은 $y = y_0$를 지나므로 $u = e^{-y_0^2} = e^{-(y-x^2)^2}$이다. 따라서

$$u(x,y) = e^{-(y-x^2)^2}.$$

5.3 비선형 수송과 충격파

Burgers 방정식 $u_t + u u_x = 0$에서는 특성곡선의 속도가 해 자신이다. 초기값 $u(x,0)=u_0(x)$에서 특성곡선은 $x = x_0 + u_0(x_0)t$이고 그 위에서 $u = u_0(x_0)$로 일정하다. u_0가 감소하는 구간이 있으면 왼쪽의 빠른 특성곡선이 오른쪽의 느린 것을 따라잡아 교차하고, 시각

$$t^{*} = -\frac{1}{\min_x u_0'(x)} \tag{5.3}$$

에 해의 기울기가 무한대가 된다. 그 뒤에는 고전해가 존재하지 않고, 보존 형태 $u_t + (u^2/2)_x = 0$의 **약해**(*weak solution*)로 불연속(**충격파**, *shock wave*)을 허용한다. 충격파의 속도는 **Rankine–Hugoniot 조건**

$$s = \frac{[u^2/2]}{[u]} = \frac{u_L + u_R}{2} \tag{5.4}$$

($[\cdot]$는 불연속면 양쪽 값의 차, u_L, u_R은 불연속의 좌우 극한값)이며, 물리적으로 의미 있는 해를 고르려면 **엔트로피 조건**(*entropy condition*) $u_L > u_R$이 추가로 필요하다(그렇지 않으면 특성곡선이 불연속에서 멀어지는 방향이 되어 약해가 유일하지 않다). 기체역학의 충격파와 교통 흐름의 정체 파가 같은 수학 구조를 갖는다.

5.4 d’Alembert 공식

$u_{tt} = c^2 u_{xx}$, $x\in\mathbb{R}$을 특성좌표 $\xi = x-ct$, $\eta = x+ct$로 바꾸면 연쇄법칙으로 $u_{\xi\eta} = 0$이 되므로 u_ξ가 η에 무관하고, 적분하면 $u = F(\xi) + G(\eta) = F(x-ct) + G(x+ct)$이다. 초기조건 $u(x,0)=f(x)$, $u_t(x,0)=g(x)$를 대입하면 $F+G=f$, $-cF' + cG' = g$를 얻고, 이를 F, G에 대해 풀어 적분하면

$$u(x,t) = \frac{f(x-ct)+f(x+ct)}{2} + \frac{1}{2c}\int_{x-ct}^{x+ct} g(s)\,\mathrm{d}s. \tag{5.5}$$

- **유한 전파 속도**: $u(x,t)$는 구간 $[x-ct, x+ct]$의 초기 자료에만 의존한다(**의존 영역**, *domain of dependence*). 역으로 한 점의 자료는 $|x-x_0| \le ct$ 안에만 영향을 준다(**영향 영역**, *domain of influence*).
- 특이성은 특성선을 따라 전파된다. f에 꺾인 점이 있으면 해에도 그 점이 속도 $\pm c$로 이동한다. 열방정식은 즉시 매끄러워지는 것과 대조적이다.
- 에너지 $E = \frac{1}{2}\int (u_t^2 + c^2 u_x^2)\,\mathrm{d}x$는 시간에 무관하게 보존된다($u_{tt} = c^2 u_{xx}$에 u_t를 곱해 x에 대해 적분하고 부분적분하면 $\frac{\mathrm{d}E}{\mathrm{d}t} = 0$을 얻는다).

5.5 반직선과 반사

$x \ge 0$에서 $u(0,t) = 0$(고정단)이면 초기 자료를 홀함수로 확장($\tilde f(-x) = -f(x)$, $\tilde g(-x) = -g(x)$)하여 전체 직선의 d'Alembert 공식(식 (5.5))을 적용한다. 그러면 경계에서 반사파가 부호를 바꾸어 돌아온다. 자유단 $u_x(0,t) = 0$이면 짝함수로 확장하며 반사파의 부호가 유지된다. 전송선에서 단락된 끝(전압 0)과 개방된 끝(전류 0)의 반사계수가 각각 -1, $+1$인 것과 같은 구조이다.

5.6 고차원 파동과 Huygens 원리

3차원에서 $u_{tt} = c^2 \nabla^2 u$의 해는 Kirchhoff 공식으로 구면 평균

$$u(\mathbf{x},t) = \partial_t \big(t\, M_{ct}[f](\mathbf{x}) \big) + t\, M_{ct}[g](\mathbf{x}) \tag{5.6}$$

으로 주어진다. 여기서 $M_r[h](\mathbf{x})$는 $\mathbf{x}$를 중심으로 반지름 r인 구면 위의 h의 평균이다. 해가 구면 $\{|\mathbf{y}-\mathbf{x}| = ct\}$ 위의 자료에만 의존하고 그 내부의 자료에는 의존하지 않으므로, 국소적인 소리는 지나간 뒤 깨끗이 사라진다(**강한 Huygens 원리**, *strong Huygens' principle*). 2차원에서는 해가 원판 $\{|\mathbf{y}-\mathbf{x}| \le ct\}$ 안의 자료에 의존하므로 파동의 꼬리가 남는다. 강한 Huygens 원리는 홀수 차원 $n \ge 3$에서 성립한다.

5.7 연습문제와 해설

연습문제 5.3 $u_{xx} + 4u_{xy} + 3u_{yy} = 0$의 유형을 판정하고 일반해를 구하라.

풀이. $a = 1, b = 2, c = 3$이므로 $b^2 - ac = 4 - 3 = 1 > 0$으로 쌍곡형이다. $u = F(y - \lambda x)$를 넣으면 $u_{xx} = \lambda^2 F''$, $u_{xy} = -\lambda F''$, $u_{yy} = F''$이므로 $\lambda^2 - 4\lambda + 3 = 0$, 즉 $\lambda = 1, 3$이다. 일반해는 $u = F(y-x) + G(y-3x)$이다. 예를 들어 $(y-3x)^2$을 넣으면 $u_{xx} = 18$, $u_{xy} = -6$, $u_{yy} = 2$이므로 $18 + 4(-6) + 3\cdot 2 = 18 - 24 + 6 = 0$으로 확인된다.

연습문제 5.4 $u_{tt} = u_{xx}$, $u(x,0) = 0$, $u_t(x,0) = \dfrac{1}{1+x^2}$의 해를 구하라.

풀이. d'Alembert 공식(식 (5.5), $c = 1$, $f = 0$)으로

$$u(x,t) = \frac{1}{2}\int_{x-t}^{x+t} \frac{\mathrm{d}s}{1+s^2} = \frac{1}{2}\big[\arctan(x+t) - \arctan(x-t)\big]$$

이다. $t \to \infty$에서 고정된 x의 값은 $\tfrac{1}{2}\big(\tfrac{\pi}{2} - (-\tfrac{\pi}{2})\big) = \dfrac{\pi}{2}$로 간다. 초기 속도 분포의 총량 $\int_{-\infty}^{\infty} g = \pi$가 남긴 영구 변위이다.

연습문제 5.5 Burgers 방정식에서 $u_0(x) = -\tanh x$이면 충격파가 생기는 시각은?

풀이. $u_0'(x) = -\operatorname{sech}^2 x$이고 이 함수의 최솟값은 $x = 0$에서 -1이므로 식 (5.3)에서 $t^{*} = -1/(-1) = 1$이다. 원점 근방의 특성곡선들이 $t = 1$에 처음 교차한다. u_0가 기함수이므로 대칭성으로 충격파는 $x = 0$에 머물며, $u_L = \lim_{x\to-\infty} u_0(x) = 1$, $u_R = \lim_{x\to\infty} u_0(x) = -1$에서 식 (5.4)로 $s = (1 + (-1))/2 = 0$이다.

다음 연결. 경계가 있는 유한 구간에서는 해를 고유함수의 급수로 전개한다. 다음 장(제13권 제6장)에서는 변수분리법과 Sturm–Liouville 이론으로 열방정식과 파동방정식을 푼다.

제 6 장

변수분리와 Sturm–Liouville 문제

개요 **변수분리법**(*separation of variables*)은 유한 구간에서 경계조건을 만족하는 열방정식·파동방정식의 해를 고유함수의 급수로 전개하는 방법이다. 이 장은 먼저 Dirichlet 경계조건을 갖는 열방정식과 파동방정식에 변수분리를 적용하고, 경계조건의 종류에 따라 고유함수족이 바뀜을 보인 뒤, 이러한 전개가 항상 성립하는 이유를 **Sturm–Liouville 이론**으로 설명한다. Sturm–Liouville 작용소의 역(Green 함수를 핵으로 하는 적분 작용소)이 콤팩트 자기수반 작용소라는 사실이 제4장의 스펙트럼 정리와 이 장을 잇는 다리이다. 선행 지식: 정규직교기저와 Fourier 급수(제13권 제2장), 콤팩트 자기수반 작용소의 스펙트럼 정리(제13권 제4장), 2계 선형 상미분방정식(제12권 제3장).

6.1 열방정식의 변수분리

$u_t = k u_{xx}$ $(0 < x < L,\, t > 0)$, $u(0,t) = u(L,t) = 0$, $u(x,0) = f(x)$를 생각한다. $u = X(x)T(t)$ 꼴의 해를 넣으면 변수가 분리되어

$$\frac{T'}{kT} = \frac{X''}{X} = -\lambda$$

가 (좌변은 t만의 함수, 가운데는 x만의 함수이므로) 상수여야 한다. 경계조건 $X(0) = X(L) = 0$과 $X'' + \lambda X = 0$을 동시에 만족하는 0이 아닌 해는

$$\lambda_n = \left(\frac{n\pi}{L}\right)^2, \qquad X_n = \sin\frac{n\pi x}{L} \qquad (n \ge 1)$$

일 때만 존재한다. $\lambda \le 0$이면 $X'' + \lambda X = 0$의 일반해가 지수함수 또는 일차함수이고, 경계조건 $X(0) = X(L) = 0$을 넣으면 $X \equiv 0$이 강제된다. 각 n에 대해 $T_n(t) = e^{-k(n\pi/L)^2 t}$가 $T_n' = -k(n\pi/L)^2 T_n$을 만족하므로, 중첩으로

$$u(x,t) = \sum_{n \ge 1} b_n e^{-k(n\pi/L)^2 t} \sin\frac{n\pi x}{L}, \qquad b_n = \frac{2}{L}\int_0^L f(x)\sin\frac{n\pi x}{L}\,dx. \tag{6.1}$$

$t > 0$이면 지수인자가 고차 모드를 급격히 감쇠시키므로 해는 f가 불연속이어도 즉시 C^∞가 된다 (**평활화 효과**, *smoothing effect*). 긴 시간에는 첫 모드 $b_1 e^{-k\pi^2 t/L^2}\sin(\pi x/L)$가 지배한다. 역방향(과거로) 풀면 지수인자가 커지므로 후방 열방정식은 잘 정립되지 않는다.

6.2 파동방정식과 정상파

$u_{tt} = c^2 u_{xx}$, 양 끝 고정, $u(x,0) = f$, $u_t(x,0) = g$이면

$$u = \sum_{n \ge 1}\left(a_n \cos\frac{n\pi c t}{L} + b_n \sin\frac{n\pi c t}{L}\right)\sin\frac{n\pi x}{L} \tag{6.2}$$

이며 a_n은 f의, $\frac{n\pi c}{L}b_n$은 g의 사인 계수이다. 진동수 $\omega_n = n\pi c/L$은 기본 진동수 ω_1의 정수배이다(**배음**, *harmonic*). 북의 막처럼 2차원 원판에서는 고유진동수가 Bessel 함수의 영점에 비례하여 정수배가 아니며, 그래서 북소리는 현악기처럼 뚜렷한 음높이를 갖지 않는다.

6.3 비동차 경계조건과 정상상태

$u(0,t) = A$, $u(L,t) = B$이면 **정상상태**(*steady state*) $v(x) = A + (B-A)x/L$($v'' = 0$이고 두 경계값을 만족)을 빼서 $w = u - v$가 동차 경계조건을 만족하게 한다. 원천항이 있는 $u_t = ku_{xx} + q(x)$도 정상상태 $kv'' + q = 0$을 먼저 풀고 나머지를 고유함수로 전개한다. 경계조건의 종류에 따라 고유함수가 바뀐다.

- 양끝 Dirichlet: $\sin(n\pi x/L)$, $n \ge 1$.
- 양끝 Neumann($u_x = 0$, 단열): $\cos(n\pi x/L)$, $n \ge 0$. $n=0$ 모드(평균온도)는 보존된다.
- 주기 조건: $e^{2\pi i n x/L}$, $n \in \mathbb{Z}$(Fourier 급수).
- 혼합 조건 $u(0)=0$, $u_x(L) + hu(L) = 0$(대류 냉각): $\tan(\mu L) = -\mu/h$의 근 μ_n에 대해 $\sin \mu_n x$. 고유값을 수치로 구해야 한다.

6.4 Sturm–Liouville 문제

정의 6.1 (**정칙 Sturm–Liouville 문제**) 구간 $[a,b]$에서 $p > 0$과 $w > 0$가 연속이고 p'과 q가 연속인 실함수일 때,

$$-(py')' + qy = \lambda w y, \qquad \alpha_1 y(a) + \alpha_2 y'(a) = 0, \qquad \beta_1 y(b) + \beta_2 y'(b) = 0 \tag{6.3}$$

($(\alpha_1,\alpha_2) \neq (0,0)$, $(\beta_1,\beta_2) \neq (0,0)$인 실수)을 **정칙 Sturm–Liouville 문제**라 한다. q에는 부호 조건이 없다.

정리 6.2 (**Sturm–Liouville**) 정칙 Sturm–Liouville 문제에 대해 다음이 성립한다.

(1) 고유값은 모두 실수이고 단순(고유공간이 1차원)하며 $\lambda_1 < \lambda_2 < \cdots \to \infty$로 나열된다.
(2) 고유함수들은 가중 내적 $\langle f, g\rangle_w = \int_a^b fgw\,dx$에 대해 직교한다.
(3) n번째 고유함수는 (a,b) 안에 정확히 $n-1$개의 영점을 갖는다.
(4) 정규화한 고유함수들은 $L^2_w[a,b]$의 정규직교기저이다.

증명의 개요. (1)과 (2)는 작용소 $\mathcal{L}y = \frac{1}{w}\big(-(py')' + qy\big)$가 경계조건 아래 **대칭**(자기수반)이라는 Green 항등식

$$\int_a^b (\mathcal{L}f)g\,w\,dx - \int_a^b f(\mathcal{L}g)w\,dx = \Big[p(fg' - f'g)\Big]_a^b = 0$$

(경계조건 때문에 우변이 0이다)에서 나온다. 명제 4.4의 증명과 같은 논법으로 (1)의 고유값이 실수임과 (2)의 직교성을 얻는다. (4)는 $\mathcal{L}$의 역(Green 함수를 핵으로 하는 적분 작용소)이 가중 Hilbert 공간 $L^2_w[a,b]$ 위의 콤팩트 자기수반 작용소이므로, 제4장의 스펙트럼 정리(정리 4.7)를 적용하여 얻는다. (3)의 영점 개수는 Sturm 비교정리에 의존하므로 증명을 생략한다. $\square$

특이 Sturm–Liouville 문제(끝점에서 $p=0$이거나 구간이 무한)에서도 Legendre, Bessel, Hermite, Laguerre 함수들이 같은 역할을 하며, 수소 원자와 조화진동자의 고유함수가 여기서 나온다. 이들 특이 문제의 q 역시 부호가 정해져 있지 않다. 예를 들어 Legendre 방정식은 $q\equiv 0$이다.

참고 (고유함수의 정규화). 정리 6.2의 고유함수 y_n은 상수배까지만 정해지므로, $\int_a^b y_n^2 w\,dx=1$이 되도록 적절한 상수를 곱하여 **정규화**한다. 전개 계수는 이 정규화된 고유함수에 대한 가중 내적 $c_n=\langle f,y_n\rangle_w$으로 주어진다. 식 (6.1)의 b_n은 이 일반 공식에서 $p=1$, $q=0$, $w=1$인 특수한 경우이며, 가중치가 상수이므로 보통 내적과 일치한다.

6.5 Rayleigh 몫과 고유값 추정

최소 고유값은

$$\lambda_1=\min_{y\neq 0}\frac{\int_a^b \left(p\,|y'|^2+q\,|y|^2\right)\,dx}{\int_a^b w\,|y|^2\,dx}. \tag{6.4}$$

이다(경계조건이 Dirichlet 조건이면 부분적분의 경계항이 사라진다). 시험함수를 넣으면 상계를 얻는다. 예를 들어 $-y''=\lambda y$, $y(0)=y(1)=0$에서 시험함수 $y=x(1-x)$를 넣으면

$$\frac{\int_0^1 (1-2x)^2\,dx}{\int_0^1 x^2(1-x)^2\,dx}=\frac{1/3}{1/30}=10$$

이고 실제 $\lambda_1=\pi^2\approx 9.87$이다. 시험함수가 실제 고유함수에 가까울수록 상계가 정확해지며, 이것이 Rayleigh–Ritz 방법과 유한요소법(제8장, 제25권)의 원리이다.

6.6 수렴과 Gibbs 현상

f가 L^2이면 고유함수 전개는 L^2에서 수렴한다. f가 조각마다 C^1이면 점별로 좌우극한의 평균에 수렴한다. 균등수렴은 f가 연속이고 경계조건과 양립할 때 기대할 수 있다. 예를 들어 Dirichlet 문제의 사인 급수로 $f(x)=1$을 전개하면 끝점에서 $f\neq 0$(경계조건과 불일치)이므로 끝점 근처에서 **Gibbs 현상**(*Gibbs phenomenon*)이 생긴다. 열방정식에서는 $t>0$이면 지수 감쇠가 이 문제를 사라지게 하지만, 파동방정식에서는 불연속이 특성선을 따라 영원히 전파된다.

6.7 연습문제와 해설

> **연습문제 6.3** $u_t=u_{xx}$, $0<x<\pi$, $u_x(0,t)=u_x(\pi,t)=0$, $u(x,0)=x$를 풀고 $t\to\infty$의 극한을 구하라.

풀이. 코사인 전개 $x=\dfrac{\pi}{2}-\dfrac{4}{\pi}\displaystyle\sum_{n\ \text{홀수}}\frac{\cos nx}{n^2}$이므로

$$u=\frac{\pi}{2}-\frac{4}{\pi}\sum_{n\ \text{홀수}}\frac{e^{-n^2t}\cos nx}{n^2}$$

이다. $t \to \infty$에서 지수항이 모두 사라지므로 평균값 $\pi/2$로 간다. 단열 경계에서 총 열량이 보존되기 때문이다.

> **연습문제 6.4** $-y'' = \lambda y$, $y(0) = 0$, $y'(1) = 0$의 고유값과 고유함수를 구하고 직교성을 확인하라.

풀이. $y(0) = 0$에서 $y = \sin(\mu x)$ 꼴이고, $y'(1) = 0$에서 $\mu \cos \mu = 0$, 즉 $\cos \mu = 0$이므로 $\mu_n = (n - \tfrac{1}{2})\pi$, $\lambda_n = \mu_n^2$이다.

$$\int_0^1 \sin \mu_m x \sin \mu_n x \, dx = \frac{1}{2}\int_0^1 \left[\cos(\mu_m - \mu_n)x - \cos(\mu_m + \mu_n)x\right] dx.$$

$m \neq n$이면 $\mu_m - \mu_n = (m-n)\pi$와 $\mu_m + \mu_n = (m+n-1)\pi$가 모두 0이 아닌 π의 정수배이므로 (피적분함수가 주기 2π의 코사인이고 적분 구간의 길이 1이 반주기의 정수배이다), 각 항의 적분이 0이다. 제4장 연습문제 4.11의 핵 $\min(x,y)$의 고유값 $1/((k-\tfrac{1}{2})^2\pi^2)$이 이 λ_n들의 역수였다.

> **연습문제 6.5** 길이 L인 현의 중앙을 높이 h만큼 당겼다 놓았다(삼각형 초기 모양, 초기속도 0). 짝수 배음이 들리지 않는 이유를 설명하라.

풀이. 초기 모양이 중앙($x = L/2$)에 대해 대칭이고 $\sin(n\pi x/L)$은 n이 짝수일 때 중앙에 대해 반대칭이므로, 삼각형 모양을 사인 급수로 전개하면 n이 짝수인 계수가 0이 된다. 실제로 계산하면 $a_n = \dfrac{8h}{n^2\pi^2}\sin\dfrac{n\pi}{2}$이며, n이 짝수이면 $\sin(n\pi/2) = 0$이다. 현을 뜯는 위치에 따라 음색이 바뀌는 수학적 이유이다.

다음 연결. 시간에 의존하지 않는 문제는 Laplace·Poisson 방정식이 된다. 다음 장(제13권 제7장)에서는 조화함수의 성질과 Green 함수를 다룬다.

제 7 장

Laplace 방정식, Green 함수, Fourier 변환

개요 **조화함수**(*harmonic function*)는 Laplace 방정식 $\nabla^2 u = 0$을 만족하는 C^2 함수이며, 평균값 성질과 최대원리라는 강한 제약을 받는다. 이 장은 조화함수의 기본 성질을 일반 차원 $\mathbb{R}^n$에서 정리하고, 점원에 대한 기본해로부터 Green 함수를 구성하여 Poisson 방정식의 Dirichlet 문제를 풀며, Fourier 변환으로 무한 영역의 열방정식을 풀고 선형 방정식의 분산관계를 소개한다. 선행 지식: 발산 정리와 Green 항등식(제9권 제7장), 제11권(복소해석)에서 다룬 조화함수(해석함수의 실수부·허수부)와 Poisson 공식.

7.1 평균값 성질과 최대원리

$\nabla^2 u = 0$인 C^2 함수 u를 **조화함수**라 한다.

> **정리 7.1 (평균값 성질)** u가 닫힌 공 $\overline{B(x,r)}$의 근방에서 조화이면 $u(x)$는 구면 $\partial B(x,r)$ 위의 평균값과 같고, 공 $B(x,r)$ 위의 평균값과도 같다.

증명. $\phi(r)$을 구면 평균이라 하면 ϕ를 반지름에 대해 미분하고 발산 정리를 쓰면

$$\phi'(r) = \frac{1}{|\partial B(x,r)|}\int_{\partial B(x,r)} \partial_n u \, \mathrm{d}S = \frac{1}{|\partial B(x,r)|}\int_{B(x,r)} \nabla^2 u \, \mathrm{d}V = 0$$

이다. 따라서 ϕ는 상수이며, $r \to 0$에서 $\phi(r) \to u(x)$(연속성)이므로 $\phi(r) \equiv u(x)$이다. 공 평균은 구면 평균을 반지름에 대해 (부피 가중으로) 적분하여 얻으며, 모든 반지름에서 구면 평균이 같은 값 $u(x)$이므로 공 평균도 $u(x)$이다. $\square$

> **정리 7.2 (강최대원리)** 연결된 열린 영역에서 조화함수가 내부에서 최댓값을 가지면 그 함수는 상수이다. 따라서 유계 영역 U에서 $u \in C^2(U)\cap C(\overline{U})$가 조화이면 $\max_{\overline{U}} u = \max_{\partial U} u$이다.

최댓값을 갖는 점들의 집합이 평균값 성질에 의해 열려 있고(최댓값 M을 갖는 점 주변의 작은 공에서 평균값 성질과 연속성으로 그 공 전체가 M이어야 한다) 연속성으로 닫혀 있으므로, 연결성에 의해 그 집합이 영역 전체이거나 공집합이다. 결과로 Dirichlet 문제 $\nabla^2 u = f$ (U), $u = g$ (∂U)의 해는 유일하고, 경계값에 연속적으로 의존한다($\max|u_1 - u_2| \le \max_{\partial U}|g_1 - g_2|$, 두 해의 차에 최대원리를 적용하여 얻는다). 온도 분포의 최고점이 (정상상태에서) 내부에 있을 수 없다는 물리적 직관과 같다.

7.2 기본해

$\mathbb{R}^n$에서 $\nabla^2 \Phi = \delta$를 만족하는 방사 대칭 함수(**기본해**, *fundamental solution*)는

$$\Phi(x) = \frac{1}{2\pi}\log|x| \quad (n=2), \qquad \Phi(x) = -\frac{1}{(n-2)\omega_n |x|^{n-2}} \quad (n \ge 3) \tag{7.1}$$

이다. ω_n은 $\mathbb{R}^n$의 단위구면 S^{n-1}의 $(n-1)$차원 넓이이며 $\omega_n = 2\pi^{n/2}/\Gamma(n/2)$($\Gamma$는 감마함수)로 주어진다. $n=3$이면 $\omega_3 = 4\pi$이므로 $\Phi = -1/(4\pi|x|)$이다. 부호 관례는 책마다 다르다(물리학에서는 $-\nabla^2 G = \delta$로 $G = 1/(4\pi|x|)$를 많이 쓴다; 제9권 제7장). 그러면 적절히 감소하는(예를 들어 콤팩트 지지를 갖는) f에 대해 $u = \Phi * f$, 즉 $n=3$에서

$$u(x) = -\frac{1}{4\pi}\int_{\mathbb{R}^3} \frac{f(y)}{|x-y|}\,\mathrm{d}y \tag{7.2}$$

가 $\nabla^2 u = f$의 해이다. 전하분포 ρ의 정전 퍼텐셜 $V = \dfrac{1}{4\pi\varepsilon_0}\displaystyle\int \frac{\rho(y)}{|x-y|}\,\mathrm{d}y$는 $\nabla^2 V = -\rho/\varepsilon_0$의 해로, 부호와 상수 $4\pi\varepsilon_0$만 다를 뿐 같은 공식이다.

7.3 Green 함수

유계 영역 U의 Dirichlet 문제를 위해 $G(x,y) = \Phi(x-y) - h_y(x)$로 두되, h_y는 U에서 (변수 x에 대해) 조화이고 경계에서 $\Phi(x-y)$와 같게 정한다. 그러면 $G(\cdot,y)$는 경계에서 0이고 $\nabla_x^2 G = \delta_y$이다. Green의 제2항등식으로

$$u(y) = \int_U G(x,y)\nabla^2 u(x)\,\mathrm{d}x + \int_{\partial U} u(x)\,\partial_{n_x} G(x,y)\,\mathrm{d}S_x. \tag{7.3}$$

$\partial_n G$가 경계값을 영역 내부로 옮기는 **Poisson 핵**(*Poisson kernel*)이 된다. Green 함수는 대칭 $G(x,y) = G(y,x)$이며, 보정함수 h_y를 구하는 것이 핵심 작업이다.

> **예제 7.3 (반공간과 영상법)** $U = \{x_3 > 0\}$이면 점 $y = (y_1,y_2,y_3)(y_3>0)$의 거울상 $y^* = (y_1,y_2,-y_3)$에 대해
> $$G(x,y) = \Phi(x-y) - \Phi(x-y^*)$$
> 이다. 경계 $x_3 = 0$ 위에서는 $|x-y| = |x-y^*|$이므로 두 항이 상쇄되어 $G=0$이다. 접지된 도체 평면 앞의 점전하 문제를 영상전하로 푸는 방법(전자기학 마스터 레퍼런스의 영상법)과 정확히 같다. 공 영역에서는 반전 $y^* = R^2 y/|y|^2$(R은 공의 반지름)과 크기 보정으로 Green 함수를 만들며, 그 결과가 Poisson 공식이다.

7.4 열핵과 Fourier 변환

$f \in L^1(\mathbb{R}^n)$의 **Fourier 변환**(*Fourier transform*)을 $\hat f(\xi) = \int f(x) e^{-ix\cdot\xi}\,\mathrm{d}x$로 정의한다. 미분이 곱셈 $\widehat{\partial_j f} = i\xi_j \hat f$로, 합성곱이 곱 $\widehat{f * g} = \hat f \hat g$로 바뀐다. **Plancherel 정리** $\int |f|^2 = (2\pi)^{-n}\int |\hat f|^2$로 L^2까지 확장되며, 역변환은 $f(x) = (2\pi)^{-n}\int \hat f(\xi) e^{ix\cdot\xi}\,\mathrm{d}\xi$이다. 신호처리에서는 2π를 지수 안에 넣는 관례($e^{-2\pi i x\cdot\xi}$)를 써서 역변환에 별도의 상수가 붙지 않게 하므로, 다른 책의 공식을 옮길 때는 어느 관례인지 반드시 확인해야 한다.

$u_t = k\nabla^2 u$, $u(x,0) = f$를 x에 대해 Fourier 변환하면 $\hat u_t = -k|\xi|^2 \hat u$(각 ξ에 대한 상수계수 1계 상미분방정식)이므로 $\hat u(\xi,t) = e^{-k|\xi|^2 t}\hat f(\xi)$이다. Gauss 함수의 Fourier 변환은 다시 Gauss 함수이므로 역변환하면

$$u(x,t) = \int_{\mathbb{R}^n} K_t(x-y) f(y)\,\mathrm{d}y, \qquad K_t(x) = \frac{1}{(4\pi k t)^{n/2}} e^{-|x|^2/(4kt)}. \tag{7.4}$$

K_t는 평균 0, (각 좌표의) 분산 $2kt$인 정규분포의 밀도이다. 열확산과 Brown 운동(제21권)이 같은 수학이라는 사실이 여기서 드러난다. $f \geq 0$이고 $f \not\equiv 0$이면(콤팩트 지지를 가져도) $t > 0$에서 $u(x,t) = \int K_t(x-y) f(y)\,\mathrm{d}y > 0$이 모든 x에서 성립한다($K_t > 0$이 $\mathbb{R}^n$ 전체에서 성립하기 때문이다). 열방정식의 전파 속도가 무한대라는 뜻이며, 파동방정식의 유한 전파 속도(식 (5.5))와 대조적이다.

7.5 분산관계와 파동의 분산

선형 방정식에 평면파 $e^{i(kx-\omega t)}$를 넣으면 ω와 k의 관계(**분산관계**, *dispersion relation*)를 얻는다. 파동방정식은 $\omega = \pm ck$로 모든 파수가 같은 속도로 움직인다(**비분산**, *non-dispersive*). Klein–Gordon 방정식 $u_{tt} - c^2 u_{xx} + m^2 u = 0$은 $\omega^2 = c^2k^2 + m^2$으로, **위상속도** ω/k와 **군속도** $\mathrm{d}\omega/\mathrm{d}k$가 서로 다르고 파속(波束)이 퍼진다. 자유 Schrödinger 방정식 $i\psi_t = -\psi_{xx}$은 $\omega = k^2$이고, 초기 파동함수 $\psi(x,0) = e^{-x^2/(2\sigma^2)}$의 폭 매개변수가 시간 t에서 $\sigma\sqrt{1 + 4t^2/\sigma^4}$로 퍼진다.

7.6 연습문제와 해설

연습문제 7.4 $\mathbb{R}^3 \setminus \{0\}$에서 방사 대칭 조화함수를 모두 구하라.

풀이. $u = u(r)$이면 구면좌표의 Laplacian(제9권 제7장)으로 $\nabla^2 u = \dfrac{1}{r^2}(r^2 u')' = 0$이므로 $r^2 u' = A$(상수), $u' = A/r^2$이고 적분하면 $u = -A/r + B$이다.

연습문제 7.5 $x^2 - y^2$이 단위원판에서 조화임을 확인하고 최대원리로 원판에서의 최댓값을 구하라.

풀이. $\nabla^2(x^2 - y^2) = 2 - 2 = 0$이다. 최대원리로 최댓값은 경계에서 달성되며, $x = \cos\theta$, $y = \sin\theta$에서 $x^2 - y^2 = \cos 2\theta$이다. 이 함수의 최댓값은 1이고 $\theta = 0, \pi$, 즉 $(\pm 1, 0)$에서 달성된다.

연습문제 7.6 열핵 K_t가 $\int K_t = 1$이고 $t \to 0^+$에서 δ로 수렴함을 설명하라.

풀이. K_t가 정규분포의 밀도이므로 적분이 1이다. 분산 $2kt \to 0$이므로 질량이 원점 근처로 몰리고, 연속이고 유계인 f에 대해 $\int K_t(x-y) f(y)\,\mathrm{d}y \to f(x)$이다(Chebyshev 부등식으로 K_t 질량의 대부분이 원점의 임의로 작은 근방에 모여 있음을 보이고, f의 균등연속성으로 그 근방에서 $f(y) \approx f(x)$임을 이용하는 근사항등함수 논법).

다음 연결. 고전해가 없거나 증명이 어려운 경우를 위해 해의 개념 자체를 넓혀야 한다. 마지막 장(제13권 제8장)에서는 약미분, Sobolev 공간, Lax–Milgram 정리로 약해를 정의한다.

제 8 장

약해, Sobolev 공간, Lax–Milgram 정리

개요 **약해**(*weak solution*)는 미분방정식을 부분적분으로 적분 형태로 바꾸어, 고전적인 의미의 미분가능성을 요구하지 않고도 정의한 해이다. 이 장은 먼저 부분적분을 거꾸로 이용하여 **약미분**(*weak derivative*)을 정의하고 이를 **Sobolev 공간**(*Sobolev space*) $W^{k,p}$로 조직한다. 그 뒤 Poincaré 부등식으로 H^1_0 위에서 기울기의 노름이 동치인 노름임을 보이고, Lax–Milgram 정리로 타원형 경계값 문제의 약해가 유일하게 존재함을 증명한다. 이 틀은 유한요소법의 수학적 기초이기도 하다. 선행 지식: Riesz 표현정리(제13권 제2장), L^p 공간(제10권 제7장)과 절대연속함수(제10권 제8장), Green 항등식(제9권 제7장).

8.1 시험함수와 약미분

$C_c^\infty(U)$의 원소(콤팩트 지지를 갖는 매끄러운 함수)를 **시험함수**(*test function*)라 한다. $u \in C^1(U)$이면 부분적분으로 모든 시험함수 φ에 대해 $\int_U \partial_i u\,\varphi = -\int_U u\,\partial_i \varphi$이다. 경계항은 φ의 지지가 U 안의 콤팩트 집합이라 사라진다.

정의 8.1 (약미분) 국소 적분가능 함수 u에 대해 모든 시험함수 φ에서 $\int_U v\varphi = -\int_U u\,\partial_i\varphi$가 성립하는 국소 적분가능 함수 v가 있으면 v를 u의 **약미분** $\partial_i u$라 한다.

약미분은 존재하면 거의 모든 곳에서 유일하다(두 후보의 차가 모든 시험함수와의 적분이 0이므로 거의 모든 곳에서 0이다). $u(x) = |x|$($x \in \mathbb{R}$)의 약미분은 $\operatorname{sgn} x$이다. $\operatorname{sgn} x$의 약미분은 존재하지 않는다. 형식적으로는 2δ인데, 이는 δ가 국소 적분가능 함수가 아니기 때문이다.

이를 더 일반화한 것이 **분포**(*distribution*)이다. 시험함수 공간 위의 연속 선형범함수를 분포라 하고, 분포 T의 미분을 $(\partial_i T)(\varphi) = -T(\partial_i \varphi)$로 정의한다. 그러면 모든 분포가 무한 번 미분가능하며, $\delta(\varphi) = \varphi(0)$도 분포이고 $H' = \delta$(**Heaviside 함수**)가 정확한 문장이 된다.

8.2 Sobolev 공간

정의 8.2 (Sobolev 공간) $1 \le p \le \infty$, $k \ge 0$에 대해 $W^{k,p}(U)$는 차수 k 이하의 모든 약미분이 $L^p(U)$에 속하는 함수들의 공간이고, 노름은

$$\|u\|_{W^{k,p}} = \left(\sum_{|\alpha| \le k} \|\partial^\alpha u\|_p^p \right)^{1/p}$$

이다. $H^k = W^{k,2}$이며, H^1은 내적 $\langle u, v\rangle_{H^1} = \int (uv + \nabla u \cdot \nabla v)$를 갖는 Hilbert 공간이다.

$W^{k,p}$는 Banach 공간이다(제10권 제7장의 L^p 완비성). $C_c^\infty(U)$의 H^1 폐포를 $H^1_0(U)$라 하며, 이는 "경계에서 0"인 함수들의 공간을 대신한다. H^1 함수는 경계에서 각 점의 값을 갖지 않지만 **대각합**(*trace*)으로 $L^2(\partial U)$의 경계값을 갖는다(경계가 충분히 매끄러울 때).

예제 8.3 (Sobolev 함수는 연속이 아닐 수 있다) $\mathbb{R}^2$의 단위원판에서 $u(x) = \log\log(1+1/|x|)$는 원점에서 무한대로 가지만 $\int |\nabla u|^2 < \infty$이므로 H^1에 속한다. 2차원에서 H^1은 연속함수의 공간에 포함되지 않는다. 일반적으로 Sobolev 매장 정리에 의해 $kp > n$이면 $W^{k,p}(U) \subseteq C(\overline{U})$(경계의 적절한 정칙성 아래)이다. 1차원에서는 H^1 함수가 연속(실제로 1/2-Hölder)이며 제10권 제8장의 절대연속 함수와 같은 대상이다.

8.3 Poincaré 부등식

정리 8.4 (Poincaré 부등식) 유계 영역 U에서 상수 $C = C(U)$가 있어 모든 $u \in H^1_0(U)$에 대해 $\|u\|_{L^2} \le C\,\|\nabla u\|_{L^2}$이다.

1차원의 증명. $U = (0, L)$, $u(0) = 0$이면 $u(x) = \int_0^x u'$이고 Cauchy–Schwarz 부등식으로

$$|u(x)|^2 \le x \int_0^L |u'|^2 .$$

양변을 $[0, L]$에서 x에 대해 적분하면 $\|u\|_2^2 \le \dfrac{L^2}{2}\,\|u'\|_2^2$이다. □

최적 상수는 $1/\sqrt{\lambda_1}$이며 λ_1은 Dirichlet Laplacian의 최소 고유값이다(제6장의 Rayleigh 몫, 식 (6.4)). 이 부등식으로 H^1_0에서 $\|\nabla u\|_2$ 자체가 (원래의 H^1 노름과) 동치인 노름이 된다. 경계값 0 조건이 없으면 상수함수가 반례이다($\nabla u = 0$이지만 $u \neq 0$).

8.4 약해와 Lax–Milgram 정리

Dirichlet 문제 $-\nabla^2 u = f$ (U), $u = 0$ (∂U)의 고전해에 시험함수 v를 곱하고 Green 항등식을 쓰면

$$\int_U \nabla u \cdot \nabla v \,\mathrm{d}x = \int_U f v \,\mathrm{d}x \qquad (\text{모든 } v \in H^1_0(U)). \tag{8.1}$$

이 식을 만족하는 $u \in H^1_0(U)$를 **약해**라 한다. 미분을 한 번만 요구하고 $f \in L^2$(또는 더 약한 H^{-1})이면 충분하다.

정리 8.5 (Lax–Milgram) Hilbert 공간 H 위의 쌍선형형식 $a(u,v)$가 **유계**($|a(u,v)| \le M\,\|u\|\,\|v\|$)이고 **강제적**(*coercive*, $a(u,u) \ge \alpha\,\|u\|^2$, $\alpha > 0$)이면, 모든 $\ell \in H^*$에 대해 $a(u,v) = \ell(v)$ $(v \in H)$인 u가 유일하게 존재하며 $\|u\| \le \|\ell\|/\alpha$이다.

역사 (Lax–Milgram 정리). 이 정리는 1954년 Peter Lax와 Arthur Milgram이 포물형 편미분방정식에 대한 연구에서 증명하였으며, 대칭이 아닌 쌍선형형식에도 적용할 수 있어 Riesz 표현정리의 비대칭 확장으로 널리 쓰인다.

증명의 개요. a가 대칭이면 a 자체가 ($\|\cdot\|$과 동치인 노름을 주는) 내적이므로 Riesz 표현정리를 그대로 적용하면 된다. 일반적으로는 고정된 u에 대해 $v \mapsto a(u,v)$가 유계 선형범함수이므로 Riesz 표현정리로 $a(u,v) = \langle Au, v\rangle$인 유계 작용소 $A : H \to H$를 얻는다. 강제성 $\langle Au, u\rangle \ge \alpha\,\|u\|^2$은 A가 아래로 유계이고(단사이고 치역이 닫혀 있음을 뜻한다) 유계성 $\|Au\| \le M\,\|u\|$와 함께 쓰면 A의 치역이 조밀함도 보일 수 있어(A^*에 같은 강제성 부등식을 적용), A가 전단사이고

$\|A^{-1}\| \le 1/\alpha$임을 얻는다. $u = A^{-1}\ell^\sharp$(여기서 $\ell^\sharp$는 Riesz 표현정리로 얻은 ℓ의 표현 벡터)로 해를 얻고, $\alpha\|u\|^2 \le a(u,u) = \ell(u) \le \|\ell\|\,\|u\|$에서 $\|u\| \le \|\ell\|/\alpha$를 얻는다. □

Dirichlet 문제에서 $a(u,v) = \int \nabla u \cdot \nabla v$의 강제성은 Poincaré 부등식(정리 8.4)에서 나온다. 따라서 모든 $f \in L^2$에 대해 약해가 유일하게 존재한다. a가 대칭인 이 경우, 약해는 에너지

$$E(v) = \frac{1}{2}\int_U |\nabla v|^2 - \int_U f v \tag{8.2}$$

의 유일한 최소점이기도 하다(**Dirichlet 원리**, *Dirichlet principle*).

8.5 정칙성과 유한요소법

약해가 실제로 매끄러운지(고전해인지)는 별도의 **정칙성 이론**(*regularity theory*)이 답한다. 경계가 매끄럽고 $f \in H^k$이면 $u \in H^{k+2}$이며(**타원형 정칙성**, *elliptic regularity*), f가 매끄러우면 u도 매끄럽다. 구석이 있는 영역(예: L자 영역의 오목한 모서리)에서는 f가 매끄러워도 해가 H^2에 속하지 않을 수 있다.

유한요소법(*finite element method*)은 H^1_0을 조각마다 일차인 함수들의 유한차원 부분공간 V_h로 바꾸어 같은 약형식을 푼다. Galerkin 직교성 $a(u - u_h, v_h) = 0$ ($v_h \in V_h$, 참해와 근사해의 차가 a에 대해 V_h와 직교한다는 뜻)으로 **Céa 보조정리**

$$\|u - u_h\| \le \frac{M}{\alpha}\,\min_{v_h \in V_h}\|u - v_h\| \tag{8.3}$$

를 얻는다. 근사해의 오차가 부분공간의 최선 근사 오차의 상수배라는 뜻이며, 오차 분석이 근사 이론 문제로 바뀐다(제25권).

8.6 연습문제와 해설

연습문제 8.6 $u(x) = |x|^a$가 $(-1,1)$에서 H^1에 속하는 a의 범위를 구하라.

풀이. $u' = a\,|x|^{a-1}\operatorname{sgn} x$(약미분, $a > 0$일 때 원점의 특이성은 적분가능)이고

$$\int_{-1}^{1} |x|^{2a-2}\,\mathrm{d}x < \infty \iff 2a - 2 > -1 \iff a > \frac{1}{2}$$

이다. 따라서 $a > 1/2$이다(상수함수인 $a = 0$은 자명하게 H^1에 속하므로 제외한다). 이 함수들은 모두 연속이며 1차원 Sobolev 매장과 일치한다.

연습문제 8.7 $-u'' = 1$, $u(0) = u(1) = 0$의 약형식을 쓰고 해를 구하라.

풀이. 약형식은 $\displaystyle\int_0^1 u'v' = \int_0^1 v$ ($v \in H^1_0$)이다. 고전해 $u(x) = \dfrac{x(1-x)}{2}$는 $u'' = -1$을 직접 만족하고 경계값도 0이므로 이 약형식을 만족하는 약해이다(정칙성에 의해 매끄러운 약해는 고전해이기도 하며, 해의 유일성으로 이것이 유일한 약해이다).

연습문제 8.8 분포의 의미에서 $\dfrac{\mathrm{d}^2}{\mathrm{d}x^2}|x| = 2\delta$임을 보여라.

풀이. 시험함수 φ에 대해

$$\int_{-\infty}^{\infty} |x|\,\varphi''\,\mathrm{d}x = \int_{0}^{\infty} x\varphi''\,\mathrm{d}x - \int_{-\infty}^{0} x\varphi''\,\mathrm{d}x$$

이다. 각 항을 두 번 부분적분하면(경계에서 φ와 φ'이 0이므로 경계항이 사라진다)

$$\int_{0}^{\infty} x\varphi''\,\mathrm{d}x = \Big[x\varphi'\Big]_{0}^{\infty} - \int_{0}^{\infty} \varphi'\,\mathrm{d}x = -\big[\varphi\big]_{0}^{\infty} = \varphi(0),$$

$$-\int_{-\infty}^{0} x\varphi''\,\mathrm{d}x = -\Big[x\varphi'\Big]_{-\infty}^{0} + \int_{-\infty}^{0} \varphi'\,\mathrm{d}x = \big[\varphi\big]_{-\infty}^{0} = \varphi(0)$$

이므로 합은 $2\varphi(0) = (2\delta)(\varphi)$이다. 즉 $|x|$의 분포 의미의 2계 도함수는 2δ이다.

제13권의 범위와 다음 읽기

이 권은 노름공간과 유계 선형작용소, Hilbert 공간과 Fourier 급수, Banach 공간의 세 기둥(균등유계성 원리·열린사상정리·폐그래프 정리), 콤팩트 작용소의 스펙트럼, 편미분방정식의 분류와 특성곡선 및 파동방정식, 변수분리와 Sturm–Liouville 이론, Laplace 방정식과 Green 함수 및 Fourier 변환, 약해와 Sobolev 공간 및 Lax–Milgram 정리를 다루었다. 표준 참고서로 E. Kreyszig, *Introductory Functional Analysis with Applications*(Wiley, 1978); H. Brezis, *Functional Analysis, Sobolev Spaces and Partial Differential Equations*(Springer, 2011); L. C. Evans, *Partial Differential Equations*, 2판(American Mathematical Society, 2010); W. A. Strauss, *Partial Differential Equations: An Introduction*, 2판(Wiley, 2008); M. Reed and B. Simon, *Methods of Modern Mathematical Physics I: Functional Analysis*, 개정판(Academic Press, 1980)이 있다.

함수해석의 작용소 이론은 양자역학의 수학적 구조(관측가능량과 자기수반 작용소, 스펙트럼과 측정값)로 바로 이어지고, Sturm–Liouville 이론의 고유함수 전개는 분리형 좌표계에서의 특수함수(Legendre, Bessel, Hermite, Laguerre)로 확장된다. 약해와 Sobolev 공간의 틀은 제17권(미분기하·다양체, 아직 집필되지 않음)에서 다양체 위의 타원형 작용소로, 제25권(수치해석·최적화, 아직 집필되지 않음)에서 유한요소법의 수렴 이론으로 각각 이어진다. Brown 운동과 열핵의 관계(제7장)는 제21권(확률과정)에서 확률미분방정식으로 정식화되며, Hilbert 공간의 기하(제2장)는 제22권(수리통계·추론)의 최소제곱·최대우도 이론에서 다시 쓰인다.

참고 자료의 사용 방식

본문의 설명과 문제는 이 참고서를 위해 새로 작성했다. 아래 목록은 관련 주제를 더 넓은 교재와 대조해 읽기 위한 안내이며, 이 원고 전체가 해당 기관이나 저자의 검토를 받았다는 뜻은 아니다. 개별 정리의 정확한 가정과 기호 약속은 자료마다 다를 수 있으므로, 독자는 다른 자료를 참고할 때마다 그 자료의 정의를 먼저 확인해야 한다.

- MIT OpenCourseWare, 18.102 *Introduction to Functional Analysis*: Banach·Hilbert 공간과 작용소의 강의노트.
- MIT OpenCourseWare, 18.152 *Introduction to PDEs*: 열·파동·Laplace 방정식의 고전 이론.
- J. K. Hunter & B. Nachtergaele, *Applied Analysis*: Hilbert 공간, Fourier 급수, 약해의 응용해석.

제 14 권

군·환·체·갈루아 이론

제14권은 대칭과 산술의 구조를 군, 환, 체라는 세 가지 대수구조로 추상화하여 다루는 현대 대수학이다. 제1–3장은 군의 정의와 Lagrange 정리, 정규부분군·몫군·동형정리, 군의 작용과 Sylow 정리를 다룬다. 제4–6장은 환·아이디얼·몫환에서 출발하여 다항식환과 주아이디얼정역, 유일인수분해를 거쳐 가군과 PID 위의 유한생성 가군의 구조정리에 이른다. 제7–8장은 체의 확대, 분해체, 유한체, 작도 문제를 다룬 뒤 Galois 이론으로 다항방정식의 근의 공식이 존재할 조건을 군의 성질로 번역한다.

제 1 장

군의 정의, 부분군, 순환군, Lagrange 정리

개요 군(*group*)은 결합법칙을 만족하는 하나의 이항연산과 항등원, 역원을 갖춘 집합이며, 대칭을 수를 다루지 않고 그 자체로 다루기 위한 대수학의 기본 언어이다. 이 장은 군을 정의하고, 부분군·생성된 부분군·순환군·원소의 위수 개념을 세운 다음, 잉여류로 군을 분할하여 유한군론 전체의 출발점이 되는 Lagrange 정리를 증명한다. 끝으로 대칭군 S_n의 순환 표기와 순열의 부호를 다룬다. 제14권은 이처럼 연산의 구조만을 추상하여 연구하는 군·환·체·갈루아 이론을 다루며, 이 장의 결과는 뒤따르는 모든 장이 쓰는 공통 언어이다. 선행 지식: 제4권의 관계와 동치류, 제1권의 합동식, 제7권의 행렬.

1.1 군의 정의

정의 1.1 (군) 집합 G와 이항연산 $G \times G \to G$, $(a,b) \mapsto ab$가 다음을 만족하면 G를 **군**이라 한다.

(1) **결합법칙**: 모든 $a,b,c \in G$에 대하여 $(ab)c = a(bc)$이다.

(2) **항등원**: 모든 $a \in G$에 대해 $ea = ae = a$인 $e \in G$가 있다.

(3) **역원**: 각 $a \in G$에 대해 $aa^{-1} = a^{-1}a = e$인 $a^{-1} \in G$가 있다.

모든 $a,b \in G$에서 $ab = ba$이면 G를 **가환군**(*abelian group*, 아벨군)이라 한다.

연산이 집합 $G \times G$에서 G로 가는 사상이라는 조건, 곧 두 원소를 연산한 결과가 다시 G 안에 있다는 **닫혀 있음**(*closure*) 조건은 정의에 이미 포함되어 있지만, 실제로 어떤 구조가 군인지 확인할 때 가장 먼저 점검해야 하는 조건이다. 홀수 전체의 집합은 덧셈에 닫혀 있지 않으므로(홀수+홀수=짝수) 이 조건부터 어긋난다.

명제 1.2 (항등원·역원의 유일성과 소거법칙) 군 G에서 항등원은 유일하고, 각 원소의 역원도 유일하며 $(ab)^{-1} = b^{-1}a^{-1}$이다. 또한 소거법칙

$$ab = ac \implies b = c, \qquad ba = ca \implies b = c$$

가 성립한다.

증명. e, e'이 둘 다 항등원이면 $e = ee' = e'$이다. a의 역원이 b, c 두 개 있다면 $b = be = b(ac) = (ba)c = ec = c$이므로 유일하다. $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$이고 같은 방식으로 $(b^{-1}a^{-1})(ab) = e$이므로 $(ab)^{-1} = b^{-1}a^{-1}$이다. $ab = ac$이면 양변에 왼쪽에서 a^{-1}을 곱해 $b = a^{-1}ab = a^{-1}ac = c$를 얻고, 오른쪽 소거법칙도 같은 방식으로 얻는다. □

원소의 개수 $|G|$를 군의 **위수**(*order*)라 한다. $|G|$가 유한이면 G를 유한군, 그렇지 않으면 무한군이라 한다.

예제 1.3 다음은 모두 군의 예이다.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}^\times, \cdot)$, 단위원의 집합 $\{z \in \mathbb{C} : |z| = 1\}$의 곱셈: 모두 가환군이다.
- $\mathbb{Z}/n\mathbb{Z}$ (덧셈), $(\mathbb{Z}/n\mathbb{Z})^\times$ (n과 서로소인 잉여류 전체의 곱셈, 위수 $\varphi(n)$).
- 대칭군 S_n: $\{1, \dots, n\}$의 전단사 전체가 함수의 합성으로 이루는 군. 위수 $n!$이고, $n \geq 3$이면 비가환이다.
- 정이면체군 D_n: 정n각형의 대칭(회전 n개, 뒤집기 n개) 전체, 위수 $2n$. 생성원 r(회전), s(뒤집기)가
$$r^n = s^2 = e, \qquad srs^{-1} = r^{-1} \tag{1.1}$$
를 만족한다.
- 일반선형군 $GL_n(\mathbb{R})$: 가역인 $n \times n$ 실행렬 전체, 행렬곱. $SO(3)$은 3차원 회전군이다.

$(\mathbb{Z}, \cdot)$이나 $(\mathbb{R}, \cdot)$은 군이 아니다. 0을 포함한 대부분의 원소에 곱셈 역원이 없기 때문이다.

역사 (추상적 정의의 등장). 군의 공리를 현재와 같은 형태로 집합과 연산만으로 서술한 것은 Arthur Cayley(1821–1895)의 1854년 논문이다. 그 이전에도 Lagrange는 다항식의 근을 치환하는 순열들의 모임을 연구하였고, Galois는 그러한 모임에 **정규부분군**이라는 개념을 실질적으로 사용하였다(제2장, 제8장). 이 장의 Lagrange 정리라는 이름은 그가 증명한 당시의 결과를 후대에 추상적인 군 언어로 다시 쓴 것이다.

1.2 부분군

정의 1.4 (부분군) 군 G의 부분집합 H가 G와 같은 연산으로 그 자체로 군이 되면 H를 G의 **부분군**(*subgroup*)이라 하고 $H \leq G$로 쓴다.

명제 1.5 (부분군 판정법) 공집합이 아닌 $H \subseteq G$가 부분군일 필요충분조건은
$$a, b \in H \implies ab^{-1} \in H$$
이다. H가 유한집합이면 곱셈에 닫혀 있다는 조건(모든 $a, b \in H$에 $ab \in H$)만으로 충분하다.

증명. $H \leq G$이면 $a, b \in H$에서 $b^{-1} \in H$이고 닫혀 있으므로 $ab^{-1} \in H$이다. 역으로 조건이 성립한다고 하자. $H \neq \emptyset$이므로 $a \in H$를 하나 잡으면 $aa^{-1} = e \in H$이다. $a \in H$에는 $ea^{-1} = a^{-1} \in H$이고, $a, b \in H$이면 $b^{-1} \in H$에서 $a(b^{-1})^{-1} = ab \in H$이다. 결합법칙은 G에서 물려받으므로 H는 부분군이다.

H가 유한이고 곱셈에 닫혀 있다고 하자. $a \in H$의 거듭제곱 $a, a^2, a^3, \dots$은 모두 H에 속하는데 H가 유한이므로 $a^i = a^j$ $(i < j)$인 쌍이 있고, 소거법칙으로 $a^{j-i} = e$를 얻는다. $m = j - i \geq 1$이라 하면 $a^{-1} = a^{m-1} \in H$이므로 역원 조건도 저절로 성립한다. □

유한 조건이 없으면 두 번째 주장은 실패한다. $\mathbb{N} \subseteq \mathbb{Z}$는 덧셈에 닫혀 있지만, $1 \in \mathbb{N}$의 거듭제곱 $1, 2, 3, \dots$이 모두 다르므로 위 논증이 멈추지 않고, 실제로 $\mathbb{N}$에는 역원이 없어 부분군이 아니다.

명제 1.6 (교집합과 생성된 부분군) 부분군들의 모임 $\{H_i\}_{i \in I}$의 교집합 $\bigcap_i H_i$는 부분군이다.

증명. 각 H_i가 e를 포함하므로 교집합도 e를 포함해 공집합이 아니다. $a, b \in \bigcap_i H_i$이면 모든 i에서 $a, b \in H_i$이므로 명제 1.5에 의해 $ab^{-1} \in H_i$이고, 이것이 모든 i에서 성립하므로 $ab^{-1} \in \bigcap_i H_i$이다. □

이 사실로 부분집합 $S \subseteq G$를 포함하는 모든 부분군의 교집합을 생각할 수 있고, 이것이 S를 포함하는 가장 작은 부분군이다. 이를 S가 **생성하는 부분군** $\langle S \rangle$이라 한다.

두 부분군의 합집합은 일반적으로 부분군이 아니다. $2\mathbb{Z} \cup 3\mathbb{Z}$는 2와 3을 포함하지만 $2+3=5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$이므로 덧셈에 닫혀 있지 않다.

1.3 순환군과 원소의 위수

정의 1.7 (순환 부분군과 원소의 위수) 군 G의 한 원소 a가 생성하는 부분군은

$$\langle a \rangle = \{ a^k : k \in \mathbb{Z} \}$$

이며 이를 **순환 부분군**이라 한다. $a^k = e$를 만족하는 최소 양의 정수 k를 a의 **위수** $\operatorname{ord}(a)$라 하며, 그런 정수가 없으면 $\operatorname{ord}(a) = \infty$라 한다. $G = \langle a \rangle$인 어떤 a가 있으면 G를 **순환군**(*cyclic group*)이라 한다.

명제 1.8 $\operatorname{ord}(a) = n < \infty$이면 다음이 성립한다.

(1) $a^k = e \iff n \mid k$이다.

(2) $|\langle a \rangle| = n$이다.

(3) $\operatorname{ord}(a^k) = n / \gcd(n, k)$이다.

증명. (1) $k = nq + r$ $(0 \le r < n)$로 나누면 $a^k = (a^n)^q a^r = a^r$이므로 $a^k = e \iff a^r = e$이고, $\operatorname{ord}(a) = n$의 최소성으로 $a^r = e$는 $r = 0$과 동치, 곧 $n \mid k$와 동치이다. (2) $a^i = a^j$ $(0 \le i < j < n)$이면 $a^{j-i} = e$이고 $0 < j - i < n$이 되어 $\operatorname{ord}(a) = n$의 최소성에 모순이므로 $e, a, \dots, a^{n-1}$은 서로 다르다. (1)에 의해 임의의 a^k는 이 n개 가운데 하나와 같으므로 $|\langle a \rangle| = n$이다. (3) $d = \gcd(n, k)$라 하면 $(a^k)^m = e \iff n \mid km \iff (n/d) \mid (k/d)m$이고 $\gcd(n/d, k/d) = 1$이므로 이는 $(n/d) \mid m$과 동치이다. 따라서 $\operatorname{ord}(a^k) = n/d$이다. □

정리 1.9 순환군의 부분군은 순환군이다. 위수 n인 순환군 $\langle a \rangle$은 n의 각 양의 약수 d에 대하여 위수 d인 부분군을 정확히 하나 갖는다.

증명. $H \le \langle a \rangle$이고 $H \neq \{e\}$라 하자. $a^k \in H$인 최소 양의 정수 k를 잡는다. $a^m \in H$이면 나눗셈 $m = qk + r$ $(0 \le r < k)$에서 $a^r = a^m (a^k)^{-q} \in H$이므로 k의 최소성에 의해 $r = 0$이다. 따라서 $H = \langle a^k \rangle$이다.

위수 d인 부분군이 존재하는지 보자. $n = dk$라 하면 명제 1.8(3)에 의해 $\operatorname{ord}(a^k) = n/\gcd(n,k) = n/k = d$이므로 $\langle a^k \rangle$은 위수 d인 부분군이다. 유일성은 위 문단에서 보였듯 임의의 부분군이 $\langle a^j \rangle$ 꼴이고, $\left|\langle a^j \rangle\right| = n/\gcd(n,j) = d$이려면 $\gcd(n,j) = n/d = k$여야 하는데, 이는 j가 k의 배수이면서 $\gcd(j/k, n/k) = 1$인 것과 같다. 그런 $j \pmod n$ 가운데 $\langle a^j \rangle = \langle a^k \rangle$을 만족하는 것은 $j \equiv k \pmod n$일 때뿐만 아니라 a^j가 $\langle a^k \rangle = \langle a^{n/d} \rangle$의 생성원일 때 모두이므로, 부분군 자체는 $\langle a^{n/d} \rangle$ 하나로 유일하다. □

참고 (순환군의 분류). 모든 순환군은 $\mathbb{Z}$ 또는 어떤 $\mathbb{Z}/n\mathbb{Z}$와 동형이다. 위수가 무한이면 $k \mapsto a^k$가 $\mathbb{Z}$에서 $\langle a\rangle$로의 동형사상이고(명제 1.8(1)에서 $a^k = e$가 $k = 0$뿐임을 뜻한다), 위수가 n이면 같은 사상이 $\mathbb{Z}/n\mathbb{Z}$에서의 동형사상이다. $\mathbb{Z}/n\mathbb{Z}$의 생성원은 n과 서로소인 잉여류이며 그 개수는 Euler 함수값 $\varphi(n)$이다(제1권). 위수 n인 순환군에서 각 원소는 정확히 하나의 순환 부분군을 생성하고, 정리 1.9에 의해 약수 $d \mid n$마다 위수 d인 원소가 정확히 $\varphi(d)$개 있으므로, 이를 더하면

$$\sum_{d \mid n} \varphi(d) = n \tag{1.2}$$

이라는 항등식을 얻는다.

1.4 잉여류와 Lagrange 정리

정의 1.10 (잉여류) $H \le G$와 $a \in G$에 대해 $aH = \{ah : h \in H\}$를 a의 **좌잉여류**(*left coset*)라 한다.

관계 $a \sim b \iff a^{-1}b \in H$는 동치관계이고($a^{-1}a = e \in H$로 반사성, $a^{-1}b \in H \Rightarrow b^{-1}a = (a^{-1}b)^{-1} \in H$로 대칭성, $a^{-1}b, b^{-1}c \in H \Rightarrow a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$로 추이성), 그 동치류가 바로 좌잉여류 aH이다. 따라서 서로 다른 좌잉여류들은 G 전체를 분할한다. 또한 $h \mapsto ah$는 H에서 aH로 가는 전단사이므로(역사상은 $x \mapsto a^{-1}x$) 모든 좌잉여류의 크기는 $|H|$로 같다.

정리 1.11 (Lagrange 정리) G가 유한군이고 $H \le G$이면 $|H|$는 $|G|$를 나누며

$$|G| = [G : H]\ |H|$$

이다. 여기서 $[G : H]$는 서로 다른 좌잉여류의 개수이며 이를 H의 **지표**(*index*)라 한다.

증명. 좌잉여류들은 G를 서로소인 부분집합들로 분할하고 그 개수가 $[G : H]$이며, 각 잉여류의 크기는 $|H|$로 모두 같다. 유한집합을 크기가 같은 $[G : H]$개의 서로소인 조각으로 나눈 것이므로 $|G| = [G : H]\,|H|$이고, 특히 $|H|$는 $|G|$를 나눈다. □

따름정리 1.12 유한군 G에서 원소 a의 위수는 $|G|$를 나누고, $a^{|G|} = e$이다. 위수가 소수인 군은 순환군이다.

증명. $\operatorname{ord}(a) = |\langle a\rangle|$이므로 정리 1.11에 의해 $\operatorname{ord}(a) \mid |G|$이고, $a^{|G|} = (a^{\operatorname{ord}(a)})^{|G|/\operatorname{ord}(a)} = e$이다. $|G| = p$가 소수이면 e가 아닌 임의의 $a \in G$의 위수는 1이 아니면서 p를 나누므로 $\operatorname{ord}(a) = p = |G|$, 곧 $G = \langle a\rangle$이다. □

따름정리 1.12를 $(\mathbb{Z}/n\mathbb{Z})^\times$ (위수 $\varphi(n)$)에 적용하면 Euler 정리

$$a^{\varphi(n)} \equiv 1 \pmod{n} \qquad (\gcd(a, n) = 1)$$

를 얻고, $n = p$가 소수이면 Fermat 소정리 $a^{p-1} \equiv 1 \pmod{p}$ $(p \nmid a)$이다. 제1권에서 합동식으로 따로 증명했던 이 결과들이 이 장에서는 Lagrange 정리의 한 줄 따름정리가 된다.

흔한 오류 (Lagrange 정리의 역은 성립하지 않는다). $|H|$가 $|G|$를 나눈다고 해서 그 위수를 갖는 부분군이 항상 존재하지는 않는다. 교대군 A_4(위수 12)는 위수 6인 부분군을 갖지 않는다. 약수마

다 부분군이 존재한다는 보장은 순환군(정리 1.9)과, 소수의 거듭제곱 위수에 대해서는 제3장의 Sylow 정리가 준다.

1.5 대칭군과 순열의 부호

표기 (순환 표기). 서로 다른 원소 $i_1, \dots, i_k \in \{1, \dots, n\}$에 대해 $i_1 \mapsto i_2 \mapsto \cdots \mapsto i_k \mapsto i_1$이고 나머지는 고정하는 순열을 길이 k인 **순환**(*cycle*) $(i_1\, i_2\, \cdots\, i_k)$이라 쓴다. 공통된 원소가 없는 두 순환은 **서로소**라 하며, 서로소인 순환은 합성 순서를 바꾸어도 같은 순열을 준다.

S_n의 원소는 서로소인 순환들의 곱으로 (순서를 제외하고) 유일하게 쓰인다. 예를 들어 $1 \mapsto 3, 3 \mapsto 5, 5 \mapsto 1, 2 \mapsto 4, 4 \mapsto 2$인 순열은 $(1\,3\,5)(2\,4)$이다. 이러한 표현을 **순환형**이라 하며, 순환형의 위수는 순환 길이들의 최소공배수이다. 모든 순열은 **호환**(길이 2인 순환)의 곱으로 쓸 수 있으며, 그 표현에 쓰인 호환 개수의 홀짝은 표현 방법과 무관하게 정해진다.

순열의 **부호** $\operatorname{sgn} : S_n \to \{\pm 1\}$은 곱을 보존하는 준동형사상이며$(\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$, 제2장에서 자세히 다룬다), 짝순열(부호 1인 순열) 전체가 **교대군** A_n(위수 $n!/2$, $n \geq 2$)을 이룬다. 행렬식의 정의

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} a_{i\,\sigma(i)}$$

에 나타나는 부호가 바로 이것이다(제7권).

1.6 연습문제와 해설

연습문제 1.13 $(\mathbb{Z}/12\mathbb{Z}, +)$의 모든 부분군을 나열하라.

풀이. 12의 양의 약수 $d = 1, 2, 3, 4, 6, 12$에 대해 정리 1.9로 위수 d인 부분군이 하나씩 있다. 생성원으로 적으면 $\langle 0\rangle$(위수 1), $\langle 6\rangle$(위수 2), $\langle 4\rangle$(위수 3), $\langle 3\rangle$(위수 4), $\langle 2\rangle$(위수 6), $\langle 1\rangle$(위수 12)이다.

연습문제 1.14 $(1\,2\,3\,4)(5\,6)$의 위수와 부호를 구하라.

풀이. 길이 4와 길이 2인 두 서로소 순환의 곱이므로 위수는 $\operatorname{lcm}(4, 2) = 4$이다. 길이 k인 순환은 호환 $k-1$개의 곱으로 쓸 수 있으므로 부호는 $(-1)^3(-1)^1 = 1$이고, 짝순열이다.

연습문제 1.15 위수가 짝수인 유한군에는 위수 2인 원소가 있음을 보여라.

풀이. $a \neq a^{-1}$인 원소들은 서로 다른 쌍 $\{a, a^{-1}\}$으로 묶이므로 그런 원소의 개수는 짝수이다. 따라서 $a = a^{-1}$인 원소의 개수는 $|G|$에서 짝수를 뺀 것으로 역시 짝수이고, 그중 e가 하나 있으므로 $a = a^{-1} \neq e$인 원소, 곧 위수 2인 원소가 적어도 하나 있다. 이는 Cauchy 정리(소수 p가 $|G|$를 나누면 위수 p인 원소가 있다는 정리, 제3장에서 일반적으로 증명한다)의 $p = 2$인 경우이다.

연습문제 1.16 2^{100}을 13으로 나눈 나머지를 구하라.

풀이. Fermat 소정리로 $2^{12} \equiv 1 \pmod{13}$이다. $100 = 8 \cdot 12 + 4$이므로

$$2^{100} = (2^{12})^8 \cdot 2^4 \equiv 2^4 = 16 \equiv 3 \pmod{13}$$

이다.

연습문제 1.17 D_4(정사각형의 대칭군)의 원소 위수를 모두 구하라.

풀이. 식 (1.1)의 회전 e, r, r^2, r^3의 위수는 각각 $1, 4, 2, 4$이고, 뒤집기 4개는 모두 위수 2이다($s^2 = e$이고 각 뒤집기가 항등원이 아니므로). 따라서 위수 2인 원소가 5개이며, 위수 8인 원소가 없으므로(위수 8인 군이려면 $|D_4| = 8$과 같아야 하는데 그런 원소가 없다) D_4는 순환군이 아니다.

참고 (다음 연결). 부분군 가운데 좌잉여류 전체가 자연스럽게 다시 군을 이루는 특별한 것이 정규부분군이다. 제14권 제2장에서는 몫군과 준동형사상, 세 가지 동형정리를 다룬다.

제 2 장

정규부분군, 몫군, 동형정리

개요 이 장은 잉여류들 사이에 연산을 자연스럽게 줄 수 있는 조건을 찾아 **몫군**을 구성하고, 준동형사상의 핵과 상으로 두 군의 구조를 비교하는 세 가지 **동형정리**를 증명한다. 직접곱과 위수가 작은 군의 분류, 그리고 단순군과 합성열까지 다루어 유한군의 전체적인 그림을 완성한다. 선행 지식: 앞 장의 부분군과 잉여류, 제4권의 몫집합과 잘 정의된 함수.

2.1 준동형사상

정의 2.1 (준동형사상) 군 G, G' 사이의 사상 $\varphi : G \to G'$이 모든 $a, b \in G$에 대해 $\varphi(ab) = \varphi(a)\varphi(b)$를 만족하면 φ를 **준동형사상**(*homomorphism*)이라 한다. 전단사인 준동형사상을 **동형사상**(*isomorphism*)이라 하고, 그런 사상이 존재하면 $G \cong G'$로 쓴다.

명제 2.2 준동형사상 $\varphi : G \to G'$은 $\varphi(e) = e'$, $\varphi(a^{-1}) = \varphi(a)^{-1}$을 만족한다. 핵 $\ker\varphi = \{a \in G : \varphi(a) = e'\}$와 상 $\varphi(G)$는 각각 G, G'의 부분군이며, φ가 단사일 필요충분조건은 $\ker\varphi = \{e\}$이다.

증명. $\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$이므로 양변에 $\varphi(e)^{-1}$을 곱하면 $\varphi(e) = e'$이다. $e' = \varphi(e) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$이므로 $\varphi(a^{-1}) = \varphi(a)^{-1}$이다. $a, b \in \ker\varphi$이면 $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = e'e'^{-1} = e'$이므로 명제 1.5에 의해 $\ker\varphi$는 부분군이다. 같은 판정법으로 $\varphi(G)$도 부분군임을 바로 확인한다. φ가 단사이면 $\varphi(a) = e' = \varphi(e)$인 a는 $a = e$뿐이므로 $\ker\varphi = \{e\}$이다. 역으로 $\ker\varphi = \{e\}$이고 $\varphi(a) = \varphi(b)$이면 $\varphi(ab^{-1}) = e'$에서 $ab^{-1} \in \ker\varphi = \{e\}$, 곧 $a = b$이다. □

예제 2.3

- $\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$는 준동형사상이고 핵은 특수선형군 $SL_n(\mathbb{R})$이다.
- $\mathrm{sgn} : S_n \to \{\pm 1\}$은 준동형사상이고 핵은 교대군 A_n이다.
- $\exp : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$는 동형사상이다. 덧셈 구조와 곱셈 구조가 본질적으로 같은 군이라는 뜻이며, 로그표로 곱셈을 덧셈으로 바꾸어 계산하던 방법의 원리이기도 하다.
- $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $k \mapsto k \bmod n$은 준동형사상이고 핵은 $n\mathbb{Z}$이다.
- $\mathbb{R} \to S^1 = \{z \in \mathbb{C} : |z| = 1\}$, $t \mapsto e^{2\pi i t}$는 준동형사상이고 핵은 $\mathbb{Z}$이다($e^{2\pi i t} = 1 \iff t \in \mathbb{Z}$).

2.2 정규부분군

좌잉여류의 집합에 $(aH)(bH) = abH$로 연산을 정의하려면, 그 값이 대표원 선택과 무관해야 한다. 곧 $aH = a'H$, $bH = b'H$일 때 항상 $abH = a'b'H$가 성립할 조건을 찾는 것이 자연스러운 출발점이며, 이 조건이 다음 정의로 이어진다.

정의 2.4 (정규부분군) 부분군 $N \le G$가 모든 $g \in G$에 대해

$$gNg^{-1} = N$$

을 만족하면(동치로 모든 g에서 좌잉여류와 우잉여류가 같아 $gN = Ng$이면) N을 G의 **정규부분군**(*normal subgroup*)이라 하고 $N \trianglelefteq G$로 쓴다.

명제 2.5 다음은 모두 정규부분군이다.

(1) 가환군의 모든 부분군.

(2) 준동형사상 $\varphi : G \to G'$의 핵 $\ker\varphi$.

(3) G에서 지표가 2인 부분군.

증명. (1) 가환군에서는 $gng^{-1} = gg^{-1}n = n$이다. (2) $n \in \ker\varphi$이면 $\varphi(gng^{-1}) = \varphi(g)e'\varphi(g)^{-1} = e'$이므로 $gng^{-1} \in \ker\varphi$이다. (3) $[G : H] = 2$이면 H가 아닌 좌잉여류는 $G \setminus H$ 하나뿐이고, 우잉여류도 마찬가지로 H와 $G \setminus H$ 둘뿐이다. $g \in H$이면 $gH = H = Hg$이고, $g \notin H$이면 $gH = G \setminus H = Hg$이므로 모든 g에서 $gH = Hg$, 곧 $H \trianglelefteq G$이다. □

(3)에 의해 $A_n \trianglelefteq S_n$이다($[S_n : A_n] = 2$).

예제 2.6 (정규가 아닌 부분군) S_3의 부분군 $H = \{e, (1\,2)\}$는 정규가 아니다. 순환 $(1\,2)$를 $(1\,3)$으로 켤레하면 $(1\,3)(1\,2)(1\,3)^{-1} = (2\,3) \notin H$이기 때문이다. 실제로 $(1\,3)H = \{(1\,3), (1\,3)(1\,2)\} = \{(1\,3), (1\,2\,3)\}$이지만 $H(1\,3) = \{(1\,3), (1\,2)(1\,3)\} = \{(1\,3), (1\,3\,2)\}$로 서로 다르다. 이처럼 좌잉여류와 우잉여류가 일치하지 않는 경우에는 잉여류의 곱이 대표원 선택에 따라 달라져 잘 정의되지 않는다.

2.3 몫군

정리 2.7 $N \trianglelefteq G$이면 잉여류 전체의 집합 G/N은

$$(aN)(bN) = abN$$

으로 군이 되고, 사영 $\pi : G \to G/N,\ a \mapsto aN$은 핵이 N인 전사 준동형사상이다. G가 유한이면 $|G/N| = |G|\,/|N|$이다.

증명. 연산이 대표원 선택과 무관함을 먼저 보인다. $aN = a'N$, $bN = b'N$이면 $a' = an_1$, $b' = bn_2$ $(n_1, n_2 \in N)$이고

$$a'b' = an_1bn_2 = ab(b^{-1}n_1b)n_2.$$

N이 정규이므로 $b^{-1}n_1b \in N$이고, 따라서 $a'b' \in abN$, 곧 $a'b'N = abN$이다. 결합법칙은 G의 결합법칙에서 바로 물려받고, 항등원은 $N = eN$이며, aN의 역원은 $a^{-1}N$이다. $\pi(ab) = abN = (aN)(bN) = \pi(a)\pi(b)$이므로 π는 준동형사상이고 분명히 전사이며, $\pi(a) = N \iff a \in N$이므로 $\ker\pi = N$이다. 유한일 때의 크기 공식은 Lagrange 정리(정리 1.11)에서 $|G/N| = [G : N] = |G|\,/|N|$으로 바로 나온다. □

몫군 G/N은 직관적으로 "N의 원소를 항등원으로 간주한" 군이다. $\mathbb{Z}/n\mathbb{Z}$는 n의 배수를 모두 0으로 보는 군이고, $\mathbb{R}/\mathbb{Z}$는 정수만큼의 차이를 무시한 실수, 즉 원 위의 각도를 나타내는 군이다.

2.4 동형정리

정리 2.8 (제1동형정리) 준동형사상 $\varphi : G \to G'$에 대해

$$G/\ker\varphi \;\cong\; \varphi(G)$$

이며, 동형사상은 $a\ker\varphi \mapsto \varphi(a)$로 주어진다.

증명. 명제 2.2에 의해 $\ker\varphi \trianglelefteq G$이므로(핵이 정규부분군임은 명제 2.5(2)) 몫군 $G/\ker\varphi$가 정의된다. $\bar\varphi(a\ker\varphi) = \varphi(a)$라 하면

$$a\ker\varphi = b\ker\varphi \iff a^{-1}b \in \ker\varphi \iff \varphi(a^{-1}b) = e' \iff \varphi(a) = \varphi(b)$$

이므로 $\bar\varphi$는 잘 정의되고(첫 번째 동치는 좌잉여류가 같을 조건, 가운데는 핵의 정의, 마지막은 준동형사상의 성질에서 나온다) 동시에 단사이다. $\bar\varphi(a\ker\varphi \cdot b\ker\varphi) = \bar\varphi(ab\ker\varphi) = \varphi(ab) = \varphi(a)\varphi(b) = \bar\varphi(a\ker\varphi)\bar\varphi(b\ker\varphi)$이므로 준동형이고, 상이 $\varphi(G)$ 전체이므로 전사이다. 따라서 $\bar\varphi$는 $G/\ker\varphi$에서 $\varphi(G)$로의 동형사상이다. □

예제 2.9 $GL_n/SL_n \cong \mathbb{R}^\times$, $S_n/A_n \cong \{\pm 1\}$, $\mathbb{R}/\mathbb{Z} \cong S^1$, $\mathbb{C}^\times/S^1 \cong \mathbb{R}_{>0}$ $(z \mapsto |z|)$이다.

정리 2.10 (제2동형정리와 제3동형정리)

(1) $H \le G$, $N \trianglelefteq G$이면 $HN = \{hn : h \in H, n \in N\}$은 G의 부분군이고 $H \cap N \trianglelefteq H$이며

$$HN/N \;\cong\; H/(H \cap N)$$

이다.

(2) $N \le K \le G$이고 N, K가 모두 G에서 정규이면

$$(G/N)/(K/N) \;\cong\; G/K$$

이다.

증명. (1) 먼저 HN이 부분군임을 보인다. $h_1n_1, h_2n_2 \in HN$에 대해 $(h_1n_1)(h_2n_2)^{-1} = h_1n_1n_2^{-1}h_2^{-1} = h_1h_2^{-1}(h_2n_1n_2^{-1}h_2^{-1})$인데, N이 정규이므로 괄호 안의 원소가 N에 속하고 전체가 HN에 속한다. 포함 사상 $H \hookrightarrow HN$ 뒤에 사영 $\pi : HN \to HN/N$을 합성한 $\varphi : H \to HN/N$, $h \mapsto hN$은 전사 준동형사상이다. $\ker\varphi = \{h \in H : hN = N\} = H \cap N$이므로 $H \cap N \trianglelefteq H$이고, 제1동형정리(정리 2.8)에 의해 $H/(H\cap N) \cong HN/N$이다.

(2) 사영 $\pi : G \to G/N$을 다시 $G/N \to (G/N)/(K/N)$에 합성한 사상 $\psi : G \to (G/N)/(K/N)$을 생각하면 ψ는 전사 준동형사상이고, $\psi(g)$가 항등원일 조건은 $gN \in K/N$, 곧 $g \in K$이므로 $\ker\psi = K$이다. 제1동형정리에 의해 $G/K \cong (G/N)/(K/N)$이다. □

정리 2.11 (대응정리) $N \trianglelefteq G$일 때, N을 포함하는 G의 부분군들과 G/N의 부분군들은

$$H \;\longmapsto\; H/N$$

으로 일대일 대응하며, 이 대응은 포함관계와 정규성을 모두 보존한다.

2.5 직접곱과 작은 군의 분류

군 G, H의 곱집합 $G \times H$에 성분별 연산 $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$를 주면 **직접곱군**이 된다.

명제 2.12 (순환군의 직접곱) $\gcd(m, n) = 1$이면 $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$이다(제1권 중국인의 나머지 정리의 군론적 형태). $\gcd(m, n) > 1$이면 이 동형은 성립하지 않는다.

증명. $k \mapsto (k \bmod m,\ k \bmod n)$은 준동형사상이고, 핵은 $m \mid k$이면서 $n \mid k$인 k, 곧 $\operatorname{lcm}(m, n) = mn$ (서로소이므로)의 배수이다. 따라서 핵은 $mn\mathbb{Z}$뿐이고 사상은 단사이며, 정의역과 공역의 크기가 같은 mn이므로 전사이기도 하다. $\gcd(m, n) = d > 1$이면 $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$의 모든 원소 (a, b)의 위수는 $\operatorname{lcm}(\operatorname{ord} a, \operatorname{ord} b)$이며 이는 $\operatorname{lcm}(m, n) = mn/d < mn$을 넘지 못하므로, 위수 mn인 원소가 없어 순환군이 아니다. □

클라인 4군 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$는 위수 4인 원소가 없으므로(모든 원소의 위수가 1 또는 2) $\mathbb{Z}/4\mathbb{Z}$와 동형이 아니다. 이는 명제 2.12에서 $\gcd(2, 2) = 2 > 1$인 경우에 해당한다.

위수가 작은 군은 동형을 제외하고 표 2.1와 같다.

표 2.1 위수 8 이하인 군의 분류(동형을 제외)

위수	군
p (소수)	$\mathbb{Z}/p\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z}$, $S_3 \cong D_3$
8	$\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^3$, D_4, 사원수군 Q_8
p^2	$\mathbb{Z}/p^2\mathbb{Z}$, $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ (모두 가환)

사원수군 $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$은 $i^2 = j^2 = k^2 = ijk = -1$로 정의되며, 모든 부분군이 정규이지만 군 자체는 가환이 아니다. (위수 p^2인 군이 항상 가환임은 제3장의 류 방정식으로 증명한다.)

2.6 단순군과 합성열

정의 2.13 (단순군) $\{e\}$와 자기 자신 이외의 정규부분군이 없는 군을 **단순군**(*simple group*)이라 한다.

가환 단순군은 소수 위수의 순환군뿐이다(가환군의 모든 부분군이 정규이므로, 비자명한 진부분군이 있으면 그것이 비자명한 정규부분군이 되어 단순성에 어긋난다. 소수 위수이면 따름정리 1.12로 자명한 부분군뿐이다). 교대군 A_n $(n \geq 5)$은 단순군이며, 이 사실은 제8장에서 5차 이상의 일반 다항식에 근의 공식이 없음을 보이는 Galois 이론적 증명의 핵심이 된다.

핵심 (Jordan–Hölder 정리). 모든 유한군은 유한 개의 단순군을 "벽돌"로 쌓아 만들어진다. 정확히는, $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_k = G$이고 각 몫 G_{i+1}/G_i가 단순군인 **합성열**이 존재하며, 그

몫 단순군들은 순서를 제외하고 유일하게 정해진다. 유한 단순군의 분류는 순환군, 교대군, Lie형 군의 족, 그리고 26개의 산재군으로 완성되었으며, 증명은 수많은 논문에 걸쳐 있다.

2.7 연습문제와 해설

> **연습문제 2.14** $\varphi : \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$, $\varphi(k) = k \bmod 4$가 잘 정의된 준동형사상임을 보이고 핵을 구하라.

풀이. $4 \mid 12$이므로 $k \equiv k' \pmod{12}$이면 $k \equiv k' \pmod{4}$가 성립해 φ는 잘 정의된다. 준동형임은 나머지 연산의 정의에서 바로 나온다. 핵은 $\{0, 4, 8\} = \langle 4 \rangle$이고, 제1동형정리로 $(\mathbb{Z}/12\mathbb{Z})/\langle 4\rangle \cong \mathbb{Z}/4\mathbb{Z}$이다. 반대 방향의 $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z}$, $k \mapsto k$는 잘 정의되지 않는다. $4 \equiv 0 \pmod 4$이지만 $4 \not\equiv 0 \pmod{12}$이기 때문이다.

> **연습문제 2.15** 군 G의 중심 $Z(G) = \{z \in G : zg = gz \ \forall g \in G\}$가 정규부분군임을 보이고, $G/Z(G)$가 순환군이면 G가 가환임을 보여라.

풀이. $z \in Z(G)$이면 모든 g에서 $gzg^{-1} = z$이므로 $Z(G)$는 정규부분군이다(부분군임은 정의에서 바로 확인된다). $G/Z = \langle aZ \rangle$라 하면 임의의 원소는 $a^m z$, $a^n z'$ $(z, z' \in Z)$ 꼴이고

$$(a^m z)(a^n z') = a^{m+n} z z' = a^{n+m} z' z = (a^n z')(a^m z)$$

이므로(지수의 덧셈은 가환이고 $z, z' \in Z(G)$이므로 a의 거듭제곱과도 교환된다) G는 가환이다.

> **연습문제 2.16** $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$에서 원소의 최대 위수를 구하고 이 군이 순환군인지 판정하라.

풀이. (a, b)의 위수는 $\operatorname{lcm}(\operatorname{ord} a, \operatorname{ord} b) \le \operatorname{lcm}(6, 4) = 12$이고, $(1, 1)$의 위수가 실제로 12이다. 군의 위수는 24인데 최대 원소 위수가 $12 < 24$이므로 순환군이 아니다. 불변인자 형태로 다시 쓰면 $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$이다(제6장).

참고 (다음 연결). 군은 집합 위에 작용할 때 그 구조가 가장 잘 드러난다. 제14권 제3장에서는 군의 작용, 궤도-안정자 정리, 류 방정식, Sylow 정리를 다룬다.

제 3 장

군의 작용과 Sylow 정리

개요 이 장은 군이 집합 위에 **작용**한다는 관점을 세워, 셈 문제와 군의 구조를 연결한다. 궤도-안정자 정리로 작용의 크기를 재고, Burnside 보조정리로 대칭을 허용한 셈을 하고, 류 방정식으로 p-군의 중심이 자명하지 않음을 보인 다음, 이 모든 도구를 합쳐 임의의 유한군 안에서 소수 거듭제곱 위수의 부분군이 존재함을 보장하는 Sylow 정리에 이른다. 선행 지식: 앞 두 장의 잉여류, 정규부분군, 동형정리.

3.1 군의 작용

정의 3.1 (군의 작용) 군 G가 집합 X 위에 **작용**(*action*)한다는 것은 사상 $G \times X \to X$, $(g, x) \mapsto g \cdot x$가

$$e \cdot x = x, \qquad g \cdot (h \cdot x) = (gh) \cdot x$$

를 만족하는 것이다.

이는 준동형사상 $G \to \mathrm{Sym}(X)$($\mathrm{Sym}(X)$는 X의 전단사 전체가 합성으로 이루는 군)를 주는 것과 동치이다. $g \cdot (g^{-1} \cdot x) = x$이므로 각 g가 주는 사상 $x \mapsto g \cdot x$는 전단사이기 때문이다.

정의 3.2 (궤도와 안정자) 점 $x \in X$에 대해 $G \cdot x = \{ g \cdot x : g \in G \}$를 x의 **궤도**(*orbit*)라 하고, $G_x = \{ g \in G : g \cdot x = x \}$를 x의 **안정자**(*stabilizer*)라 한다.

G_x는 부분군이다. $g, h \in G_x$이면 $(gh^{-1}) \cdot x = g \cdot (h^{-1} \cdot x) = g \cdot x = x$이기 때문이다. 관계 $x \sim y \iff y \in G \cdot x$는 동치관계이므로 궤도들은 X를 분할한다.

예제 3.3

- $SO(3)$이 $\mathbb{R}^3$에 회전으로 작용한다. 궤도는 원점을 중심으로 하는 구면들이고, $x \neq 0$의 안정자는 x축 둘레의 회전으로 이루어진 군(동형으로 $SO(2)$)이다.
- G가 자기 자신에 켤레로 작용한다: $g \cdot x = g x g^{-1}$. 이때 궤도는 **켤레류**, 안정자는 **중심화군** $C_G(x) = \{ g \in G : gx = xg \}$이다.
- G가 부분군 H의 좌잉여류 집합 G/H에 왼쪽 곱으로 작용한다: $g \cdot (aH) = (ga)H$.

3.2 궤도-안정자 정리

정리 3.4 (궤도-안정자 정리) 유한군 G가 집합 X에 작용하면 임의의 $x \in X$에 대해

$$|G \cdot x| = [G : G_x] = \frac{|G|}{|G_x|}$$

이다.

증명. 좌잉여류 gG_x에 $g\cdot x$를 대응시키는 사상이 잘 정의되고 전단사임을 보인다. $g\cdot x = h\cdot x \iff g^{-1}h\cdot x = x \iff g^{-1}h \in G_x \iff gG_x = hG_x$이므로, 이 대응은 서로 다른 좌잉여류를 서로 다른 궤도의 점으로 보내는 단사이며(잘 정의됨도 같은 동치에서 나온다), 정의에 의해 궤도 위로의 전사이다. 따라서 좌잉여류 전체의 집합(크기 $[G:G_x]$)과 궤도(크기 $|G\cdot x|$) 사이에 전단사가 있고, Lagrange 정리(정리 1.11)로 $[G:G_x] = |G|/|G_x|$이다. □

> **예제 3.5 (정육면체의 회전군)** 정육면체의 회전은 정육면체의 6개 면에 추이적으로(궤도가 하나로) 작용한다. 한 면의 안정자는 그 면의 중심을 지나는 축에 대한 회전 4개($0°, 90°, 180°, 270°$)로 이루어지므로, 궤도-안정자 정리에 의해 회전군의 위수는 $6\cdot 4 = 24$이다. 실제로 이 군은 정육면체의 네 개의 대각선을 치환하는 작용을 통해 S_4와 동형임을 보일 수 있다.

3.3 Burnside 보조정리와 셈

> **정리 3.6 (Burnside 보조정리)** 유한군 G가 유한집합 X에 작용하면 궤도의 개수는
>
> $$\frac{1}{|G|}\sum_{g\in G}|X^g|, \qquad X^g = \{x\in X : g\cdot x = x\}$$
>
> 이다.

증명. 집합 $\{(g,x)\in G\times X : g\cdot x = x\}$의 크기를 두 가지 방법으로 센다. g를 고정하고 세면 $\sum_{g\in G}|X^g|$이고, x를 고정하고 세면 $\sum_{x\in X}|G_x|$이다. 궤도-안정자 정리로 $|G_x| = |G|/|G\cdot x|$이므로

$$\sum_{x\in X}|G_x| = \sum_{x\in X}\frac{|G|}{|G\cdot x|}.$$

같은 궤도에 속한 점들은 모두 같은 항 $|G|/\big|(\text{그 궤도의 크기})\big|$을 주며 그 궤도의 크기만큼 여러 번 더해지므로, 한 궤도의 기여는 정확히 $|G|$이다. 궤도가 모두 N개이면 이 합은 $N|G|$이고, 따라서 $\sum_g |X^g| = N|G|$에서 $N = \frac{1}{|G|}\sum_g |X^g|$를 얻는다. □

주의 (이름에 대하여). 이 보조정리는 관습적으로 Burnside의 이름을 따르지만, 역사적으로는 그보다 앞서 Cauchy와 Frobenius가 사실상 같은 결과를 알고 있었다. 그래서 *Cauchy–Frobenius lemma*라는 이름도 함께 쓰인다.

> **예제 3.7 (목걸이 세기)** 구슬 4개를 원형으로 꿰고 각 구슬을 두 색 중 하나로 칠할 때, 회전으로 겹치는 색칠을 같게 본다면 몇 가지인가?
>
> 회전군은 $\mathbb{Z}/4\mathbb{Z} = \{e, r, r^2, r^3\}$이며 ($r$은 $90°$ 회전), 각 원소가 고정하는 색칠의 수는 다음과 같다. e는 모든 색칠 $2^4 = 16$가지를 고정한다. r, r^3($90°, 270°$ 회전)은 네 구슬이 한 순환으로 옮겨 다니므로 모두 같은 색이어야 고정되며 2가지이다. r^2($180°$ 회전)은 마주보는 두 쌍이 각각 같은 색이면 되므로 $2^2 = 4$가지이다. Burnside 보조정리로
>
> $$\frac{16+2+4+2}{4} = \frac{24}{4} = 6$$
>
> 가지이다. 뒤집기까지 같게 보아 정이면체군 D_4(위수 8)를 쓰면, 꼭짓점을 지나는 두 뒤집기는 $2^3 = 8$가지씩, 변의 중점을 지나는 두 뒤집기는 $2^2 = 4$가지씩을 고정하므로
>
> $$\frac{16+2+4+2+8+8+4+4}{8} = \frac{48}{8} = 6$$

가지로 역시 6가지이다. 구슬이 4개인 이 경우에는 두 답이 우연히 같다.

3.4 류 방정식과 p-군

켤레 작용(예 3.3)에 궤도-안정자 정리를 적용하면, 원소 x의 켤레류의 크기는 $[G : C_G(x)]$이고, 크기가 1인 켤레류는 $C_G(x) = G$인 원소, 곧 중심 $Z(G)$의 원소이다. 켤레류들이 G를 분할하므로

$$|G| = |Z(G)| + \sum_{i} [G : C_G(x_i)] \tag{3.1}$$

를 얻는다. 이 합은 크기가 1보다 큰 켤레류에서 대표원 x_i 하나씩을 뽑아 취하며, 이를 **류 방정식**(*class equation*)이라 한다.

정리 3.8 p가 소수이고 $|G| = p^n$ $(n \geq 1)$이면 $Z(G) \neq \{e\}$이다. 따라서 위수 p^2인 군은 가환이다.

증명. 식 (3.1)의 각 항 $[G : C_G(x_i)] > 1$은 $|G| = p^n$의 약수이면서 1보다 크므로 p의 배수이다. 따라서 $|G| = |Z(G)| + (p$의 배수들의 합$)$에서 $|Z(G)|$도 p의 배수이고, $e \in Z(G)$이므로 $|Z(G)| \geq 1$이니 $|Z(G)|$는 0이 아닌 p의 배수, 곧 $Z(G) \neq \{e\}$이다.

$|G| = p^2$이면 $|Z(G)| \in \{p, p^2\}$이다. $|Z(G)| = p^2$이면 $G = Z(G)$로 가환이다. $|Z(G)| = p$이면 $|G/Z(G)| = p$로 소수이므로 따름정리 1.12에 의해 $G/Z(G)$는 순환군이고, 연습문제 2.15에 의해 G는 가환이다. 그런데 G가 가환이면 $Z(G) = G$이므로 $|Z(G)| = p$라는 가정에 모순이다. 따라서 $|Z(G)| = p^2$인 경우만 가능하고 G는 가환이다. □

3.5 Sylow 정리

정리 3.9 (Sylow) $|G| = p^a m$이고 $p \nmid m$이라 하자(p는 소수).

(1) 위수 p^a인 부분군(**Sylow p-부분군**)이 존재한다.

(2) 모든 Sylow p-부분군은 서로 켤레이다. 모든 p-부분군(위수가 p의 거듭제곱인 부분군)은 어떤 Sylow p-부분군에 포함된다.

(3) Sylow p-부분군의 개수 n_p는

$$n_p \equiv 1 \pmod{p}, \qquad n_p \mid m$$

을 만족한다.

존재(1)는 크기 p^a인 부분집합들 전체 위의 G의 작용과, 이항계수 $\binom{p^a m}{p^a} \not\equiv 0 \pmod{p}$라는 사실을 쓰는 Wielandt의 증명이 짧다. (2)와 (3)은 하나의 Sylow p-부분군 P를 다른 모든 Sylow p-부분군의 집합, 또는 잉여류 집합 G/Q 위에 켤레 작용 또는 곱셈 작용으로 작용시키고 그 고정점을 세어 얻는다. 특히 $n_p = 1$이면 그 Sylow p-부분군은 유일하므로 모든 켤레에 대해 자기 자신과 같고, 따라서 정규이다.

예제 3.10 (위수 15인 군) $|G| = 15 = 3 \cdot 5$라 하자. $n_3 \equiv 1 \pmod 3$이고 $n_3 \mid 5$이므로 $n_3 \in \{1, 5\} \cap \{1, 4, 7, \dots\} = \{1\}$, 곧 $n_3 = 1$이다. $n_5 \equiv 1 \pmod 5$이고 $n_5 \mid 3$이므로 마찬가지로 $n_5 = 1$이다. 따라서 Sylow 3-부분군 P_3과 Sylow 5-부분군 P_5는 모두 정규이고, $P_3 \cap P_5 = \{e\}$이며

($|P_3 \cap P_5|$가 3과 5를 모두 나누어야 하므로 1), $|P_3P_5| = |P_3|\,|P_5|\,/|P_3 \cap P_5| = 15 = |G|$이므로 $G = P_3P_5$이다. 두 정규부분군의 교집합이 자명하므로 $G \cong P_3 \times P_5 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/15\mathbb{Z}$(명제 2.12). 위수 15인 군은 순환군뿐이다.

예제 3.11 (위수 12인 군은 단순군이 아니다) $|G| = 12 = 2^2 \cdot 3$이라 하자. $n_3 \equiv 1 \pmod 3$이고 $n_3 \mid 4$이므로 $n_3 \in \{1, 4\}$이다. $n_3 = 4$이면 Sylow 3-부분군 4개가 각각 위수 3이고 서로 다른 두 Sylow 3-부분군의 교집합은 자명하므로(교집합의 크기가 3을 나누고 3보다 작아야 한다), 위수 3인 원소가 $4 \cdot 2 = 8$개 있다. 나머지 원소는 $12 - 8 = 4$개이고, 이들이 위수 4인 유일한 부분군을 이루므로 $n_2 = 1$이다. $n_3 = 1$인 경우에는 그 자체로 정규 Sylow 3-부분군이 있다. 어느 경우든 정규인 Sylow 부분군이 존재하므로 G는 단순군이 아니다.

3.6 연습문제와 해설

연습문제 3.12 정사면체의 회전군의 위수를 궤도-안정자 정리로 구하라.

풀이. 회전군은 정사면체의 4개 꼭짓점에 추이적으로 작용하고, 한 꼭짓점의 안정자는 그 꼭짓점과 마주한 면의 중심을 지나는 축에 대한 회전 3개$(0^\circ, 120^\circ, 240^\circ)$이다. 궤도-안정자 정리로 위수는 $4 \cdot 3 = 12$이며, 이 군은 교대군 A_4와 동형임을 보일 수 있다.

연습문제 3.13 3가지 색으로 정사각형의 네 꼭짓점을 칠하는 방법을, 회전으로 겹치는 것을 같게 보아 세어라.

풀이. 회전군 $\mathbb{Z}/4\mathbb{Z}$의 각 원소가 고정하는 색칠의 수는 e: 3^4, $90^\circ, 270^\circ$ 회전: 3 (네 꼭짓점이 한 순환이므로), 180° 회전: 3^2 (마주보는 두 쌍)이다. Burnside 보조정리로

$$\frac{1}{4}\left(3^4 + 3 + 3^2 + 3\right) = \frac{81 + 3 + 9 + 3}{4} = \frac{96}{4} = 24$$

가지이다.

연습문제 3.14 위수 35인 군이 순환군임을 보여라.

풀이. $|G| = 35 = 5 \cdot 7$이다. $n_5 \mid 7$이고 $n_5 \equiv 1 \pmod 5$이므로 $n_5 = 1$이고, $n_7 \mid 5$이고 $n_7 \equiv 1 \pmod 7$이므로 $n_7 = 1$이다. 예 3.10와 같은 논법으로 $G \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \cong \mathbb{Z}/35\mathbb{Z}$이다. 일반적으로 $p < q$가 소수이고 $p \nmid q - 1$이면, $n_q \mid p$이고 $n_q \equiv 1 \pmod q$인데 $p < q$이므로 $n_q = 1$이며, $n_p \mid q$이고 $n_p \equiv 1 \pmod p$인 $n_p \in \{1, q\}$ 가운데 $q \equiv 1 \pmod p$가 가정$(p \nmid q - 1)$에 의해 성립하지 않으므로 $n_p = 1$이다. 따라서 위수 pq인 군은 모두 순환군이다.

연습문제 3.15 S_4의 켤레류와 각 류의 크기를 구하고 류 방정식을 확인하라.

풀이. S_n에서 두 순열이 켤레일 필요충분조건은 순환형이 같은 것이다. S_4의 순환형과 각 류의 크기는 항등원 1개, 호환(길이 2) $\binom{4}{2} = 6$개, 길이 3인 순환 $\binom{4}{3} \cdot 2 = 8$개(원소 3개를 고르고 그 순환 방향을 2가지로 정한다), 길이 4인 순환 $4!/4 = 6$개, $(2,2)$형(서로소인 두 호환의 곱) 3개이다. 합을 확인하면 $1 + 6 + 8 + 6 + 3 = 24 = 4! = |S_4|$이다. S_4의 중심은 자명하므로($n \geq 3$에서 S_n의 중심은 자명하다) 류 방정식 (3.1)은 $24 = 1 + 6 + 8 + 6 + 3$으로 확인된다.

참고 (다음 연결). 덧셈과 곱셈이라는 두 연산을 함께 갖춘 구조가 **환**이다. 제14권 제4장에서는 환, 아이디얼, 몫환을 다룬다.

제 4 장

환, 아이디얼, 몫환

개요 **환**(*ring*)은 덧셈과 곱셈이라는 두 연산을 함께 갖춘 대수구조이며, 정수의 산술을 추상화한 것이다. 이 장은 환을 정의하고, 영인자가 없는 정역과 모든 원소가 가역인 체를 구분한 다음, 몫군을 만드는 정규부분군에 대응하는 개념인 **아이디얼**로 몫환을 구성한다. 소 아이디얼과 극대 아이디얼이 각각 몫환의 정역성·체 됨과 어떻게 대응하는지 보이고, 중국인의 나머지 정리와 환의 표수로 장을 마친다. 선행 지식: 앞 장들의 군과 몫군, 제1권의 정수와 합동식.

4.1 환의 정의와 예

정의 4.1 (환) 집합 R에 덧셈과 곱셈이 있어 $(R,+)$가 가환군이고, 곱셈이 결합적이며 분배법칙

$$a(b+c)=ab+ac, \qquad (a+b)c=ac+bc$$

이 성립하면 R을 **환**이라 한다. 이 권에서는 곱셈 항등원 1을 가진 환만 다루며, 곱셈이 가환이면 R을 **가환환**이라 한다.

예: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}/n\mathbb{Z}$, 다항식환 $R[x]$, 행렬환 $M_n(\mathbb{R})$(비가환), 구간 $[0,1]$ 위의 연속함수 전체인 함수환 $C[0,1]$, Gauss 정수 $\mathbb{Z}[i]=\{a+bi : a,b\in\mathbb{Z}\}$.

곱셈 역원을 갖는 원소를 **단원**(*unit*)이라 하고, 단원 전체 $R^\times$는 곱셈에 대한 군을 이룬다(결합법칙은 환에서 물려받고, 1이 항등원이며, 단원의 정의로 역원이 존재하고, 두 단원의 곱도 단원이다). $\mathbb{Z}^\times=\{\pm1\}$, $\mathbb{Z}[i]^\times=\{\pm1,\pm i\}$, $(\mathbb{Z}/n\mathbb{Z})^\times$는 n과 서로소인 잉여류 전체이다. 0이 아닌 모든 원소가 단원인 가환환을 **체**(*field*)라 한다.

4.2 정역과 영인자

정의 4.2 (영인자와 정역) 가환환 R에서 $a\neq0$, $b\neq0$인데 $ab=0$이면 a,b를 **영인자**(*zero divisor*)라 한다. 영인자가 없고 $1\neq0$인 가환환을 **정역**(*integral domain*)이라 한다.

정역에서는 곱셈 소거법칙 $ab=ac,\ a\neq0\Rightarrow b=c$가 성립한다. $ab=ac$이면 $a(b-c)=0$이고 $a\neq0$이므로(영인자가 없으므로) $b-c=0$이기 때문이다.

- $\mathbb{Z}/6\mathbb{Z}$에서 $2\cdot3=0$이므로 정역이 아니다. $\mathbb{Z}/n\mathbb{Z}$가 정역일 필요충분조건은 n이 소수인 것이며, 그때 $\mathbb{Z}/n\mathbb{Z}$는 체이다.
- 유한 정역은 체이다. $a\neq0$이면 $x\mapsto ax$는 단사이고(소거법칙), 유한집합 위의 단사사상은 전사이므로 $ax=1$인 x가 있다.
- 정역 D에서 분수 a/b $(b\neq0)$를 형식적으로 만들어 **분수체**(*field of fractions*)를 얻는다. $\mathbb{Z}$의 분수체가 $\mathbb{Q}$이다(제5권에서 구성한다).

4.3 아이디얼과 몫환

정의 4.3 (아이디얼) 가환환 R의 덧셈 부분군 I가 $r \in R,\ a \in I \Rightarrow ra \in I$를 만족하면 I를 **아이디얼**(*ideal*)이라 한다.

아이디얼은 몫환을 만들 수 있는 정확한 조건이다. R/I의 원소는 잉여류 $a+I$이고, $(a+I)(b+I) = ab+I$가 대표원 선택과 무관하게 잘 정의되려면 바로 이 흡수 조건이 필요하다. 실제로 $a+I = a'+I$, $b+I = b'+I$이면 $a' = a+i_1$, $b' = b+i_2$ $(i_1, i_2 \in I)$이고

$$a'b' = ab + ai_2 + i_1 b + i_1 i_2$$

에서 오른쪽의 뒤 세 항이 모두 I에 속하므로(첫째와 둘째는 아이디얼의 흡수 조건, 셋째는 I가 부분군이라 $i_1 i_2$도 흡수 조건으로 I에 속한다) $a'b'+I = ab+I$이다.

환 준동형사상 $\varphi : R \to R'$의 핵 $\ker\varphi = \{a \in R : \varphi(a) = 0\}$은 아이디얼이고 제1동형정리 $R/\ker\varphi \cong \varphi(R)$가 성립한다(군의 경우와 같은 논증이 각 연산에 대해 그대로 적용된다).

원소 하나가 생성하는 아이디얼 $(a) = aR$를 **주아이디얼**(*principal ideal*)이라 한다. $\mathbb{Z}$의 아이디얼은 모두 $n\mathbb{Z}$ 꼴이다. 나눗셈 알고리즘으로, 아이디얼의 0이 아닌 원소 가운데 절댓값이 가장 작은 원소가 그 아이디얼의 모든 원소를 나누기 때문이다(제1장에서 순환 부분군이 $\langle a^k\rangle$ 꼴임을 보인 논증과 완전히 같은 구조이다).

예제 4.4

- $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$: $\mathbb{R}[x] \to \mathbb{C}$, $p \mapsto p(i)$는 전사이고 핵이 (x^2+1)이다. 복소수는 "$x^2+1=0$으로 강제한 실계수 다항식"으로 볼 수 있다.
- $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ (상수항만 남는다), $\mathbb{Z}[x]/(2,x) \cong \mathbb{Z}/2\mathbb{Z}$.
- $C[0,1]$에서 $I_c = \{f : f(c) = 0\}$은 아이디얼이고 $C[0,1]/I_c \cong \mathbb{R}$이다(평가 사상 $f \mapsto f(c)$의 핵이 I_c).

4.4 소 아이디얼과 극대 아이디얼

정의 4.5 (소 아이디얼과 극대 아이디얼) 진아이디얼(자기 자신이 아닌 아이디얼) P가 $ab \in P \Rightarrow a \in P$ 또는 $b \in P$를 만족하면 **소 아이디얼**(*prime ideal*)이라 한다. 진아이디얼 M을 포함하는 아이디얼이 M과 R뿐이면 M을 **극대 아이디얼**(*maximal ideal*)이라 한다.

정리 4.6 가환환 R에서 다음이 성립한다.

(1) P가 소 아이디얼이다 $\iff$ R/P가 정역이다.

(2) M이 극대 아이디얼이다 $\iff$ R/M이 체이다.

따라서 극대 아이디얼은 소 아이디얼이다(체는 영인자를 갖지 않으므로 정역이기 때문이다).

증명. (1) R/P의 원소 $a+P \neq 0,\ b+P \neq 0$은 각각 $a \notin P,\ b \notin P$를 뜻한다. $(a+P)(b+P) = ab+P = 0$은 $ab \in P$를 뜻하므로, P가 소 아이디얼이라는 조건은 정확히 "$a, b \notin P \Rightarrow ab \notin P$", 곧 그 대우인 "$R/P$에 영인자가 없다"는 것과 같다. $P \neq R$이므로 R/P에서 $1 \neq 0$이다.

(2) $a \notin M$이면 M과 a를 모두 포함하는 아이디얼 $M+(a)$는 M보다 진짜로 크므로 극대성에 의해 R이다. 따라서 $1 = m+ra$인 $m \in M,\ r \in R$가 있고, 이는 $(a+M)(r+M) = 1+M$을 뜻하므로

$a+M$이 R/M에서 가역이다. $a \notin M$은 $a+M \neq 0$과 같으므로, 0이 아닌 모든 원소가 가역이어서 R/M은 체이다. 역으로 R/M이 체라 하자. M을 진짜로 포함하는 아이디얼 J가 있으면, $a \in J \setminus M$에 대해 $a+M \neq 0$이 R/M에서 가역이므로 $(a+M)(b+M) = 1+M$인 b가 있고, $ab-1 \in M \subseteq J$이다. $a \in J$이므로 $ab \in J$이고 따라서 $1 = ab-(ab-1) \in J$, 곧 $J = R$이다. 그러므로 M은 극대 아이디얼이다. □

$\mathbb{Z}$에서 소 아이디얼은 (0)과 (p)(p는 소수)이고, 극대 아이디얼은 (p)뿐이다((0)은 $\mathbb{Z}/(0) = \mathbb{Z}$가 정역이지만 체가 아니므로 극대가 아니다). $\mathbb{Z}[x]$에서 (x)는 소 아이디얼이지만 극대가 아니다($\mathbb{Z}[x]/(x) \cong \mathbb{Z}$는 정역이지만 체가 아니다). 실제로 $(x) \subsetneq (2,x)$이고 $\mathbb{Z}[x]/(2,x) \cong \mathbb{Z}/2\mathbb{Z}$는 체이므로 $(2,x)$가 극대 아이디얼이다.

핵심 (극대 아이디얼의 존재). Zorn 보조정리를 아이디얼들의 포함관계에 적용하면, $1 \neq 0$인 환의 모든 진아이디얼은 (자기 자신을 포함하여) 어떤 극대 아이디얼에 포함된다. 임의의 사슬(전순서로 늘어선 아이디얼들)의 합집합이 다시 아이디얼이면서 진아이디얼이라는 점이 핵심이며(1을 포함하면 어느 한 아이디얼이 이미 1을 포함해야 하는데 각각이 진아이디얼이므로 불가능하다), Zorn 보조정리가 극대 원소의 존재를 보장한다.

4.5 중국인의 나머지 정리

정리 4.7 (중국인의 나머지 정리, 환론적 형태) 가환환 R의 아이디얼 $I_1, \dots, I_k$가 쌍마다 서로소($I_i + I_j = R,\ i \neq j$)이면

$$R/(I_1 \cap \cdots \cap I_k) \;\cong\; R/I_1 \times \cdots \times R/I_k$$

이다.

$R = \mathbb{Z}$, $I_j = (n_j)$(쌍마다 서로소, 곧 $\gcd(n_i, n_j) = 1$)이면 이는 제1권의 중국인의 나머지 정리와 같다. 다항식환에서는 Lagrange 보간이 된다. R이 체이고 $a_1, \dots, a_k \in R$가 서로 다른 점이면(일반적으로는 $a_i - a_j$가 모두 단원이면) $R[x]/\left(\prod_j (x-a_j)\right) \cong R^k$이며, 이 동형사상의 역사상이 "주어진 k개의 점에서 지정된 값을 갖는 다항식"을 만들어 준다.

4.6 환의 표수

정의 4.8 (표수) $\underbrace{1+1+\cdots+1}_{n\text{번}} = 0$을 만족하는 최소 양의 정수 n을 환의 **표수**(*characteristic*)라 하고, 그런 n이 없으면 표수가 0이라 한다.

정역의 표수는 0이거나 소수이다. 표수가 합성수 $n = ab$ $(1 < a, b < n)$라면, 1을 a번 더한 것과 b번 더한 것의 곱이 1을 n번 더한 것과 같아 0이 되는데, n이 최소라는 가정으로 두 인수는 모두 0이 아니어서 영인자가 생기기 때문이다.

표수 p인 가환환에서는

$$(a+b)^p = a^p + b^p$$

가 성립한다. 이항정리로 전개한 $\binom{p}{k}a^k b^{p-k}$ $(0<k<p)$ 항의 이항계수 $\binom{p}{k}=\frac{p!}{k!(p-k)!}$의 분자에는 p가 있지만 분모의 $k!,(p-k)!$에는 $k, p-k<p$이므로 p가 나타나지 않아, $\binom{p}{k}$ 자체가 p의 배수이고 표수 p인 환에서 그 항이 소거되기 때문이다. 이 성질을 흔히 "신입생의 꿈(*freshman's dream*)"이라 부르며, 유한체 이론(제7장)과 현대 암호학의 기초가 되는 사실이다.

4.7 연습문제와 해설

연습문제 4.9 $\mathbb{Z}/12\mathbb{Z}$의 단원, 영인자, 멱영원($a^k=0$인 $k\geq 1$이 있는 원소)을 모두 구하라.

풀이. 단원은 12와 서로소인 $1,5,7,11$이다. 0이 아닌 나머지 원소 $2,3,4,6,8,9,10$은 각각 적당한 비영 원소와 곱해 0이 되므로(예: $2\cdot 6=12\equiv 0$, $3\cdot 4=12\equiv 0$, $8\cdot 3=24\equiv 0$) 영인자이다. 멱영원은 0과 6이다($6^2=36\equiv 0 \pmod{12}$이고, 다른 원소의 거듭제곱은 결코 0이 되지 않음을 직접 확인할 수 있다). 유한 가환환에서는 모든 원소가 단원이거나 영인자이다. a가 단원이 아니면 $x\mapsto ax$가 단사가 아니므로(단사이면 유한집합에서 전사가 되어 $ax=1$인 x가 생겨 단원이 된다) $ab=ac$, $b\neq c$인 b,c가 있고 $a(b-c)=0$, $b-c\neq 0$에서 a는 영인자이다.

연습문제 4.10 $\mathbb{Z}[x]/(x^2-2)$와 $\mathbb{Z}[\sqrt{2}]$가 동형임을 보여라.

풀이. 사상 $p(x)\mapsto p(\sqrt{2})$는 전사 환 준동형사상이다($\mathbb{Z}[\sqrt{2}]$의 모든 원소가 $a+b\sqrt{2}$ 꼴이고 이는 $p(x)=a+bx$의 상이다). 핵은 $\sqrt{2}$를 근으로 갖는 정수계수 다항식 전체이며, x^2-2가 모닉(최고차 계수가 1)이므로 나눗셈 알고리즘으로 그런 다항식은 모두 x^2-2의 배수이다. 실제로 $p(x)=(x^2-2)q(x)+(a+bx)$로 나누면 $p(\sqrt{2})=0$은 $a+b\sqrt{2}=0$을 뜻하는데, $\sqrt{2}$가 무리수이므로 $a=b=0$이어야 하기 때문이다. 제1동형정리로 $\mathbb{Z}[x]/(x^2-2)\cong\mathbb{Z}[\sqrt{2}]$이다.

연습문제 4.11 $\mathbb{Z}/2\mathbb{Z}[x]/(x^2+x+1)$이 원소 4개인 체임을 보여라.

풀이. $\mathbb{Z}/2\mathbb{Z}$에서 x^2+x+1의 값은 $x=0$일 때 1, $x=1$일 때 $1+1+1=1$이므로 근이 없고, 2차 다항식이 근을 갖지 않으면 기약이다(제5장). 기약다항식이 생성하는 아이디얼은 극대이므로(제5장에서 증명한다) 몫환은 체이다. 원소는 잉여류의 대표원 $0,1,\alpha,\alpha+1$ 넷이며(α는 x의 상, $\alpha^2=\alpha+1$), $\alpha(\alpha+1)=\alpha^2+\alpha=(\alpha+1)+\alpha=2\alpha+1=1$(표수 2이므로 $2\alpha=0$)이므로 α와 $\alpha+1$이 서로 역원이고, 1은 자기 자신이 역원이다. 모든 비영 원소가 역원을 가지므로 체이다.

연습문제 4.12 $C[0,1]$의 극대 아이디얼은 모두 $I_c=\{f : f(c)=0\}$ 꼴임을 보여라.

풀이. 극대 아이디얼 M이 어떤 I_c에도 포함되지 않는다고 가정하자. 각 $c\in[0,1]$마다 $f_c(c)\neq 0$인 $f_c\in M$이 있다(그렇지 않으면 $M\subseteq I_c$). 연속성으로 f_c는 c 근방에서도 0이 아니고, $[0,1]$의 콤팩트성으로 유한개의 점 $c_1,\dots,c_n$의 근방들이 $[0,1]$을 덮는다. $g=\sum_{j} f_{c_j}^2\in M$(각 $f_{c_j}^2\in M$이고 M이 덧셈 부분군이므로)은 모든 점에서 양수이므로 $[0,1]$에서 연속인 역함수 $1/g$가 있어 단원이고, 단원을 포함하는 아이디얼은 전체 환이므로 $M=C[0,1]$이 되어 진아이디얼이라는 가정에 모순이다. 따라서 $M\subseteq I_c$인 c가 있고, M의 극대성과 $I_c\neq C[0,1]$(I_c는 상수함수 1을 포함하지 않는다)로 $M=I_c$이다. 공간의 점과 함수환의 극대 아이디얼이 일대일로 대응한다는 이 관찰이 대수기하학(제18권)의 출발점이다.

참고 (다음 연결). 정수에서 성립하는 소인수분해의 유일성은 어떤 환에서 일반적으로 성립하는가? 제14권 제5장에서는 다항식환, 주아이디얼정역, 유일인수분해정역을 다룬다.

제 5 장

다항식환, 주아이디얼정역, 유일인수분해

개요 정수에서는 나눗셈 알고리즘, 최대공약수, 소인수분해의 유일성이 모두 성립한다. 이 장은 이러한 성질이 일반적으로 성립하는 환의 부류, 곧 Euclid 정역 · 주아이디얼정역(PID) · 유일인수분해정역(UFD)을 정의하고 그 포함관계를 밝힌다. Gauss 보조정리와 Eisenstein 판정법 등 다항식의 기약성을 판정하는 표준 방법을 다루고, 체 위의 다항식환이 PID라는 사실로부터 유한체의 곱셈군이 순환군임을 보인다. 선행 지식: 앞 장의 아이디얼과 몫환, 제2권의 다항식 나눗셈, 제1권의 산술의 기본정리.

5.1 Euclid 정역과 주아이디얼정역

정역 D에서 $a \mid b$는 $b = ac$인 $c \in D$가 있다는 뜻이다. 0이 아니고 단원도 아닌 원소 p가

$$p = ab \implies a \text{ 또는 } b\text{가 단원}$$

을 만족하면 p를 **기약원**(*irreducible*)이라 하고,

$$p \mid ab \implies p \mid a \text{ 또는 } p \mid b$$

를 만족하면 p를 **소원**(*prime element*)이라 한다. 소원은 항상 기약원이지만($p = ab$이면 $p \mid ab$에서 $p \mid a$ 또는 $p \mid b$이고, 가령 $p \mid a$이면 $a = pc$에서 $p = pcb$, 소거법칙으로 $cb = 1$이 되어 b가 단원이다), 그 역은 일반적으로 성립하지 않는다(예 5.6).

정의 5.1 (Euclid 정역과 PID) 정역 D에 함수 $N : D \setminus \{0\} \to \mathbb{N}$이 있어, 모든 $a \in D$와 $b \in D \setminus \{0\}$에 대해

$$a = qb + r, \qquad r = 0 \text{ 또는 } N(r) < N(b)$$

인 $q, r \in D$가 존재하면 D를 **Euclid 정역**(*Euclidean domain*)이라 한다. 모든 아이디얼이 주아이디얼인 정역을 **주아이디얼정역**(*principal ideal domain*, PID)이라 한다.

예: $\mathbb{Z}$ ($N = |\cdot|$), 체 $\mathbb{F}$ 위의 다항식환 $\mathbb{F}[x]$ ($N = \deg$), Gauss 정수 $\mathbb{Z}[i]$ ($N(a+bi) = a^2 + b^2$).

명제 5.2 Euclid 정역은 PID이다. PID에서는 임의의 두 원소에 최대공약수가 존재하고 Bézout 항등식 $\gcd(a,b) = ax + by$가 성립하며, 기약원과 소원이 일치한다.

증명. $I \neq \{0\}$이 Euclid 정역 D의 아이디얼이라 하자. $I \setminus \{0\}$에서 N값이 최소인 원소 d를 잡으면, 임의의 $a \in I$를 $a = qd + r$로 나눌 때 $r = a - qd \in I$이고 $r = 0$ 또는 $N(r) < N(d)$인데 후자는 d의 최소성에 모순이므로 $r = 0$, 곧 $a \in (d)$이다. 따라서 $I = (d)$는 주아이디얼이다. D가 PID이면 $(a,b) = (a) + (b)$도 주아이디얼이므로 $(a,b) = (d)$인 d가 있다. $a, b \in (d)$이므로 d는 a, b의 공약수이고, $d \in (a,b)$이므로 $d = ax + by$인 x, y가 있다. 임의의 공약수 e는 a, b를 나누므로 $ax + by = d$도 나누어, d가 최대공약수이다. 기약원 p가 소원임을 보인다. $p \mid ab$라 하고 $p \nmid a$라

하면 $\gcd(p, a) = 1$이다(p의 약수는 단원 또는 p의 단원배수뿐이고, $p \nmid a$이므로 후자는 공약수가 아니다). Bézout로 $px + ay = 1$이고 양변에 b를 곱하면 $pxb + aby = b$인데, 왼쪽 두 항 모두 p로 나누어지므로 $(p \mid ab)$ $p \mid b$이다. □

예제 5.3 $\mathbb{Z}[x]$는 PID가 아니다. 아이디얼 $(2, x)$가 하나의 원소 d로 생성된다면 d는 2와 x를 모두 나누어야 한다. $d \mid 2$이므로 d는 상수이고, x를 나누는 상수는 ± 1뿐이므로 d는 단원, 곧 $d = \pm 1$이어야 한다. 그런데 $(2, x)$의 원소는 모두 상수항이 짝수인 다항식이므로 $1 \notin (2, x)$이다. 마찬가지로 체 $\mathbb{F}$ 위의 이변수 다항식환 $\mathbb{F}[x, y]$의 아이디얼 (x, y)도 주아이디얼이 아니다.

5.2 유일인수분해정역

정의 5.4 (유일인수분해정역) 정역 D에서 0도 단원도 아닌 모든 원소가 기약원들의 곱으로 쓰이고, 그 표현이 인수의 순서와 단원 배수의 차이를 제외하고 유일하면 D를 **유일인수분해정역**(*unique factorization domain*, UFD)이라 한다.

정리 5.5 PID는 UFD이다.

존재(모든 원소가 기약원들의 곱으로 쓰임)는 아이디얼의 증가열이 결국 멈춘다는 사실(**Noether 성질**: $(a_1) \subsetneq (a_2) \subsetneq \cdots$ 꼴의 무한히 진짜로 증가하는 아이디얼열이 없다는 성질이며, 그 합집합도 아이디얼이고 PID에서는 다시 주아이디얼이므로 어느 한 항에서 이미 전체와 같아져야 한다는 데서 나온다)에서 얻는다. 유일성은 명제 5.2에서 보인 "기약원은 소원이다"라는 사실에서 나온다(소원으로 분해하면 산술의 기본정리(제1권)의 증명과 똑같은 귀납 논증으로 유일성을 얻는다).

예제 5.6 (유일인수분해가 실패하는 환) $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$에서

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

이다. 노름 $N(a + b\sqrt{-5}) = a^2 + 5b^2$은 곱셈적이고$(N(zw) = N(z)N(w))$ $N(2) = 4$, $N(3) = 9$, $N(1 \pm \sqrt{-5}) = 1 + 5 = 6$이다. 노름이 2나 3인 원소는 없다($a^2 + 5b^2 = 2$ 또는 3은 정수해가 없다). 따라서 네 인수 $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$는 모두 기약원이고(더 작은 노름의 비단원 곱으로 분해될 수 없다), 서로 단원의 배수도 아니다($\mathbb{Z}[\sqrt{-5}]^\times = \{\pm 1\}$이고, $2, 3, 1+\sqrt{-5}$는 노름이 서로 다르며, 노름이 같은 $1+\sqrt{-5}$와 $1-\sqrt{-5}$는 부호만 바꾼다고 서로 같아지지 않는다). 그러므로 두 분해는 본질적으로 다르며, $\mathbb{Z}[\sqrt{-5}]$는 UFD가 아니다. 이 현상을 원소 대신 아이디얼의 분해로 복구하는 것이 Dedekind 정역의 이데알 이론이다(제15권).

정리 5.7 (Gauss) D가 UFD이면 $D[x]$도 UFD이다. 따라서 $\mathbb{Z}[x]$와 $\mathbb{F}[x_1, \ldots, x_n]$($\mathbb{F}$는 체)은 모두 UFD이다.

$\mathbb{Z}[x]$는 PID가 아니지만(예 5.3) UFD이므로, UFD와 PID는 서로 다른 개념이다. 포함관계는

$$\text{UFD} \supsetneq \text{PID} \supsetneq \text{Euclid 정역}$$

이며 각 포함이 진부분이다.

5.3 Gauss 보조정리

정수계수 다항식의 계수 전체의 최대공약수가 1이면 그 다항식을 **원시다항식**(*primitive polynomial*)이라 한다.

보조정리 5.8 (Gauss 보조정리) 원시다항식들의 곱은 원시다항식이다. 따라서 정수계수 다항식이 $\mathbb{Q}[x]$에서 인수분해되면 $\mathbb{Z}[x]$에서도 같은 차수의 인수들로 인수분해된다.

증명. 원시다항식 f, g의 곱 fg가 원시다항식이 아니라면 어떤 소수 p가 fg의 모든 계수를 나눈다. 법 p로 환원하면 $\mathbb{Z}/p\mathbb{Z}[x]$에서 $\bar{f}\bar{g} = \overline{fg} = 0$인데, $\mathbb{Z}/p\mathbb{Z}$가 정역이므로 $\mathbb{Z}/p\mathbb{Z}[x]$도 정역이고(다항식환이 정역 위에 있으면 정역이다. 최고차항끼리의 곱이 영인자가 될 수 없기 때문이다) $\bar{f} = 0$ 또는 $\bar{g} = 0$이어야 한다. 이는 f 또는 g의 모든 계수가 p의 배수라는 뜻이 되어 원시성에 모순이다.

두 번째 주장은, $f \in \mathbb{Z}[x]$가 $\mathbb{Q}[x]$에서 $f = gh$로 인수분해되면 분모를 모두 걷어내어 $f = \frac{a}{b} g_1 h_1$ ($g_1, h_1 \in \mathbb{Z}[x]$는 원시다항식, a/b는 기약분수)로 쓸 수 있고, 첫 부분에 의해 $g_1 h_1$도 원시다항식이므로 f의 계수들의 최대공약수를 비교하면 $b = \pm 1$이어야 함을 보여 얻는다. □

5.4 기약성 판정

- 차수 2 또는 3인 다항식은 체 $\mathbb{F}$ 위에서 근이 없을 때 그리고 그때에만 기약이다(차수가 2나 3이면 비자명한 인수분해에 반드시 일차식이 나타나야 하기 때문이다). 차수 4 이상에서는 근이 없어도 두 이차식의 곱으로 인수분해될 수 있다: $x^4+4 = (x^2+2x+2)(x^2-2x+2)$ (Sophie Germain 항등식).
- 유리근 정리: $a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$의 유리근 p/q(기약분수)는 $p \mid a_0$, $q \mid a_n$을 만족한다.
- 법 p 환원: 최고차 계수를 소수 p가 나누지 않을 때, 법 p로 환원한 $\bar{f} \in \mathbb{Z}/p\mathbb{Z}[x]$가 기약이면 f는 $\mathbb{Q}[x]$에서 기약이다(역은 성립하지 않는다. 연습문제 5.11을 보라).

정리 5.9 (Eisenstein 판정법) $f = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$와 소수 p에 대해

$$p \nmid a_n, \qquad p \mid a_i \ (0 \le i < n), \qquad p^2 \nmid a_0$$

이면 f는 $\mathbb{Q}[x]$에서 기약이다.

증명. Gauss 보조정리에 의해 $\mathbb{Q}[x]$에서의 기약성은 $\mathbb{Z}[x]$에서의 기약성과 같으므로, $f = gh$ ($g, h \in \mathbb{Z}[x]$, 차수 모두 ≥ 1)라 가정하고 모순을 보인다. 법 p로 환원하면 $\bar{f} = \bar{a}_n x^n = \bar{g}\bar{h}$인데 $\mathbb{Z}/p\mathbb{Z}[x]$가 UFD이고 $\bar{a}_n \neq 0$이므로, $\bar{g} = b x^k$, $\bar{h} = c x^{n-k}$ ($k, n-k \ge 1$, $b, c \in (\mathbb{Z}/p\mathbb{Z})^\times$) 꼴이어야 한다. 이는 g, h의 상수항이 모두 p의 배수임을 뜻하므로, $a_0 = g(0)h(0)$이 p^2의 배수가 되어 가정에 모순이다. □

예제 5.10 (원분다항식) p가 소수이면 p번째 **원분다항식**

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1}$$

은 $\mathbb{Q}[x]$에서 기약이다. $x \mapsto x+1$을 대입하면

$$\frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{p-1}$$

이고, $0 < k < p$인 모든 $\binom{p}{k}$가 p의 배수이며 상수항 $\binom{p}{p-1} = p$는 p^2의 배수가 아니므로 Eisenstein 판정법을 적용할 수 있다. 다항식의 치환 $x \mapsto x+1$은 가역한 변수변환이므로 기약성을 보존한다.

5.5 다항식의 근과 체 위의 다항식

체 $\mathbb{F}$ 위에서 $f(a) = 0 \iff (x-a) \mid f$(인수정리, 나눗셈 $f = (x-a)q + r$에서 $r = f(a)$인 상수이기 때문이다)이므로, 차수 n인 다항식은 근을 많아야 n개 갖는다(근마다 일차 인수가 하나씩 떨어져 나가고, 전체 차수가 n을 넘을 수 없기 때문이다).

주의 (정역이 아니면 실패한다). $\mathbb{Z}/8\mathbb{Z}$에서 $x^2 - 1$은 근 $1, 3, 5, 7$ 네 개를 갖는다($\mathbb{Z}/8\mathbb{Z}$가 정역이 아니므로 인수정리의 논증이 깨진다).

이 사실(근의 개수가 차수를 넘지 않음)을 이용해 유한체의 곱셈군이 순환군임을 보일 수 있다. 유한체 $\mathbb{F}$의 곱셈군 $\mathbb{F}^\times$에서 위수 d인 원소 a가 있다면 $\langle a \rangle$의 d개 원소가 모두 $x^d - 1 = 0$의 근이므로 $x^d - 1$의 근은 정확히 $\langle a \rangle$의 원소들이고, 위수 d인 원소는 그 가운데 생성원인 $\varphi(d)$개뿐이다. 따라서 $n = |\mathbb{F}^\times|$의 각 약수 d에 대해 위수 d인 원소는 0개 또는 $\varphi(d)$개이며, 이를 모두 더하면 n이어야 하므로 제1장의 항등식 $\sum_{d \mid n} \varphi(d) = n$과 비교하여 모든 d에서 정확히 $\varphi(d)$개이다. 특히 위수 n인 원소, 곧 생성원이 반드시 존재한다. $(\mathbb{Z}/p\mathbb{Z})^\times$의 생성원을 법 p의 **원시근**이라 한다(제15권에서 자세히 다룬다).

$\mathbb{F}[x]$가 PID이므로(명제 5.2, $N = \deg$인 Euclid 정역이기 때문이다), f가 기약일 필요충분조건은 (f)가 극대 아이디얼인 것, 곧 $\mathbb{F}[x]/(f)$가 체인 것이다(정리 4.6). 이것이 다음 두 장에서 체의 확대를 구성하는 기본 방법이다.

5.6 연습문제와 해설

연습문제 5.11 $x^4 + 1$이 $\mathbb{Q}[x]$에서 기약임을 보이고, 모든 소수 p에 대해 $\mathbb{Z}/p\mathbb{Z}[x]$에서는 가약임을 참고로 말하라.

풀이. $x \mapsto x+1$을 대입하면

$$(x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$$

이고 $p = 2$에서 Eisenstein 조건$(2 \nmid 1,\ 2 \mid 4, 6, 4, 2,\ 4 \nmid 2)$을 만족하므로 $x^4 + 1$은 기약이다. 그런데 모든 소수 p에서 $x^4 + 1$은 $\mathbb{Z}/p\mathbb{Z}[x]$에서 가약이다(법 p 환원이 기약성의 충분조건일 뿐 필요조건은 아님을 보여 주는 표준적인 예이다). 따라서 이 다항식에 대해서는 법 p 판정으로 기약성을 증명할 수 없다.

연습문제 5.12 $\mathbb{Z}[i]$에서 $\gcd(11 + 3i,\ 1 + 8i)$를 Euclid 알고리즘으로 구하라.

풀이.

$$\frac{11+3i}{1+8i} = \frac{(11+3i)(1-8i)}{65} = \frac{35-85i}{65} \approx 0.54 - 1.31i$$

이므로 가장 가까운 Gauss 정수 $q = 1 - i$로 나눈다.

$$r = (11+3i) - (1-i)(1+8i) = (11+3i) - (9+7i) = 2 - 4i.$$

다음으로

$$\frac{1+8i}{2-4i} = \frac{(1+8i)(2+4i)}{20} = \frac{-30+20i}{20} = -1.5 + i$$

이므로 $q = -1 + i$로 둔다(실수부가 -1.5여서 $-2 + i$를 택해도 된다).

$$r = (1+8i) - (-1+i)(2-4i) = (1+8i) - (2+6i) = -1 + 2i.$$

마지막으로 $\dfrac{2-4i}{-1+2i} = \dfrac{(2-4i)(-1-2i)}{5} = \dfrac{-10}{5} = -2$로 나누어떨어지므로, $\gcd(11+3i, 1+8i) = -1+2i$이다(단원 $\pm 1, \pm i$ 배수 차이를 제외하면 유일하며, 노름은 5이다).

연습문제 5.13 $x^3 - 3x - 1$이 $\mathbb{Q}$ 위에서 기약임을 보여라.

풀이. 3차 다항식은 유리근이 없으면 기약이다. 유리근 정리로 후보는 ± 1뿐이고, $1-3-1 = -3 \neq 0$, $-1+3-1 = 1 \neq 0$이므로 유리근이 없다. 이 다항식의 근 $2\cos(\pi/9) = 2\cos 20^\circ$는 제7장에서 60°를 삼등분할 수 없다는 증명에 쓰인다. 삼배각 공식 $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$에 $\theta = 20^\circ$를 대입하면 $\cos 60^\circ = \tfrac{1}{2}$에서 $4\cos^3 20^\circ - 3\cos 20^\circ = \tfrac{1}{2}$이고, $y = 2\cos 20^\circ$로 치환하면 $y^3 - 3y - 1 = 0$을 얻는다.

참고 (다음 연결). PID 위의 다항식환에 대한 이 장의 결과는 선형대수와도 깊이 연결된다. 제14권 제6장에서는 **가군**을 도입하고, PID 위의 유한생성 가군의 구조정리로 유한생성 아벨군의 분류와 행렬의 Jordan 표준형을 함께 얻는다.

제 6 장

가군과 PID 위의 유한생성 가군

개요 이 장은 체 위의 벡터공간을 일반적인 환 위로 넓힌 개념인 **가군**을 정의하고, 주아이디얼정역(PID) 위의 유한생성 가군에 대한 구조정리를 소개한다. 이 하나의 정리에서 유한생성 아벨군의 완전한 분류와 행렬의 Jordan 표준형·유리 표준형이 동시에 나온다는 점에서, 이 장은 군론과 환론을 선형대수와 잇는 다리 역할을 한다. 선행 지식: 앞 장의 PID, 제7권의 벡터공간·선형사상·고유값.

6.1 가군

정의 6.1 (가군) 가환환 R 위의 **가군**(*module*) M은 가환군 $(M, +)$과 스칼라곱 $R \times M \to M$의 쌍으로, 벡터공간의 공리와 같은 다음 성질을 만족하는 것이다. 모든 $r, s \in R$, $m, n \in M$에 대해

$$r(m+n) = rm + rn, \quad (r+s)m = rm + sm, \quad (rs)m = r(sm), \quad 1m = m.$$

예제 6.2

- R이 체이면 R-가군은 바로 R 위의 벡터공간이다.
- $\mathbb{Z}$-가군은 가환군과 같은 개념이다. $nm = \underbrace{m + \cdots + m}_{n}$ ($n \geq 0$, $n < 0$이면 $-(-n)m$)으로 스칼라곱이 가환군 구조만으로 자동으로 정해지기 때문이다.
- 유한차원 벡터공간 V와 선형사상 $T : V \to V$가 주어지면 $p(x) \cdot v = p(T)v$로 V는 $\mathbb{F}[x]$-가군이 된다(여기서 $p(T)$는 p에 x 대신 T를 대입하고 상수항은 $T^0 = \mathrm{id}$의 배수로 보는 선형사상이다). 하나의 선형사상을 연구하는 것은 그에 대응하는 $\mathbb{F}[x]$-가군 하나를 연구하는 것과 같다.
- 환 R의 아이디얼은 R-부분가군이다(흡수 조건 $rI \subseteq I$가 바로 가군의 스칼라곱이 닫혀 있다는 조건이다).

벡터공간과 달리 가군에는 **기저**가 없을 수 있다. $\mathbb{Z}/2\mathbb{Z}$를 $\mathbb{Z}$-가군으로 보면, 어떤 원소 m에 대해서도 $2m = 0$이므로 $\{m\}$조차 일차독립이 아니다(계수 $2 \neq 0$인데 $2m = 0$이기 때문이다). 기저를 갖는 가군을 **자유가군**이라 하며, 기저의 크기가 n이면 R^n과 동형이다.

6.2 꼬임과 생성

정의 6.3 (꼬임 원소와 유한생성) $rm = 0$인 0이 아닌 $r \in R$이 존재하는 원소 $m \in M$을 **꼬임 원소**(*torsion element*)라 한다. 유한 개의 원소 $m_1, \dots, m_k$로 $M = Rm_1 + \cdots + Rm_k$와 같이 생성되는 가군을 **유한생성**이라 한다.

정역 R 위의 가군에서 꼬임 원소 전체는 부분가군 M_{tors}를 이룬다($rm = 0$, $sn = 0$이면 $(rs)(m+n) = s(rm) + r(sn) = 0$이고 정역이므로 $r \neq 0, s \neq 0 \Rightarrow rs \neq 0$이기 때문이다).

PID 위에서는 유한생성 자유가군의 부분가군이 다시 자유가군이고, 그 계수(기저의 크기)가 원래보다 커지지 않는다는 사실이 구조정리의 증명에서 결정적인 역할을 한다. 일반적인 환에서는 이 사실이 실패한다. $\mathbb{Z}[x]$ 위의 아이디얼 $(2, x)$는 $\mathbb{Z}[x]$-가군으로서 자유가군이 아니다(두 생성원 $2, x$ 사이에 $x \cdot 2 - 2 \cdot x = 0$이라는 자명하지 않은 관계가 있어 일차독립인 기저를 이루지 못한다).

6.3 구조정리

정리 6.4 (PID 위의 유한생성 가군의 구조정리) R이 PID이고 M이 유한생성 R-가군이면

$$M \;\cong\; R^{r} \oplus R/(d_1) \oplus \cdots \oplus R/(d_k), \qquad d_1 \mid d_2 \mid \cdots \mid d_k \tag{6.1}$$

이다. 여기서 d_i는 0도 단원도 아니며, 음이 아닌 정수 r(가군의 **계수**, *rank*)과 아이디얼 $(d_1), \dots, (d_k)$는 M에 의해 유일하게 결정된다(**불변인자 형태**). 동치로, M은 R^{r}과 $R/(p^{e})$(p는 기약원, $e \geq 1$) 꼴의 가군들의 직합으로도 쓸 수 있다(**기본인자 형태**).

증명의 핵심은 행렬의 **Smith 표준형**이다. PID 위의 행렬은 가역인 행·열 기본연산(두 행을 바꾸기, 한 행에 원소를 곱해 다른 행에 더하기, 한 행에 단원을 곱하기 및 그 열에 대한 연산)으로 대각행렬 $\mathrm{diag}(d_1, \dots, d_k, 0, \dots, 0)$, $d_1 \mid d_2 \mid \cdots$ 꼴로 바꿀 수 있다. 유한생성 가군 M을 생성원 n개와 그 사이의 관계식들로 서술하면 $M \cong R^{n}/K$ (여기서 K는 생성원들 사이의 관계가 생성하는 부분가군)로 쓸 수 있고, 관계식을 나타내는 행렬을 Smith 표준형으로 바꾸면 식 (6.1)의 구조가 그대로 드러난다. 이는 제1권에서 다룬 연립 일차 디오판토스 방정식을 푸는 방법을 일반적인 PID로 확장한 것이다.

6.4 유한생성 가환군

$R = \mathbb{Z}$에 정리 6.4를 적용하면 다음을 얻는다.

따름정리 6.5 유한생성 가환군은

$$\mathbb{Z}^{r} \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_k\mathbb{Z}, \qquad d_1 \mid \cdots \mid d_k,\ d_i > 1$$

와 유일하게 동형이다. 특히 유한 가환군($r = 0$인 경우)은 순환군들의 직접곱이다.

예제 6.6 (위수 72인 가환군의 분류) $72 = 2^{3} \cdot 3^{2}$이므로, 기본인자 형태에서 2-부분은 분할 $3, 2+1, 1+1+1$에 대응해 $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z})^{3}$ 가운데 하나이고, 3-부분은 분할 $2, 1+1$에 대응해 $\mathbb{Z}/9\mathbb{Z}$, $(\mathbb{Z}/3\mathbb{Z})^{2}$ 가운데 하나이다. 서로 독립적으로 고를 수 있으므로 $3 \cdot 2 = 6$개의 동형류가 있다. 예를 들어 기본인자가 $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z}$인 경우, 불변인자 형태로 고쳐 쓰면 각 소수에서 가장 큰 기본인자들을 모아 $d_k = \mathrm{lcm}(4, 9) = 36$을 만들고 남은 $\mathbb{Z}/2\mathbb{Z}$를 $d_{k-1} = 2$로 두어 $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/36\mathbb{Z}$가 된다($2 \cdot 36 = 72$로 위수가 일치하고 $2 \mid 36$으로 나눗셈 사슬도 성립한다).

예제 6.7 (관계식으로 주어진 군의 계산) 생성원 a, b와 관계식 $6a + 4b = 0$, $2a + 2b = 0$으로 정의된 가환군을 생각하자. 관계 행렬은

$$\begin{pmatrix} 6 & 4 \\ 2 & 2 \end{pmatrix}$$

이며, 이 행렬의 Smith 표준형은 $\operatorname{diag}(2, 2)$이다(행렬식이 $6\cdot 2 - 4\cdot 2 = 4$이고 성분들의 최대공약수가 2이므로, 불변인자는 $d_1 = 2$, $d_1 d_2 = 4$에서 $d_2 = 2$이다). 따라서 이 군은 $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$이다.

6.5 선형사상의 표준형

$R = \mathbb{F}[x]$, $M = V$(유한차원 $\mathbb{F}$-벡터공간), x의 작용을 선형사상 T로 둔 경우에 구조정리를 적용한다. V가 유한차원이므로 특성다항식 p_T에 대해 $p_T(T) = 0$(Cayley–Hamilton 정리, 제7권)이 되어 V 전체가 꼬임 가군이고, 정리 6.4에 의해

$$V \;\cong\; \mathbb{F}[x]/(d_1(x)) \oplus \cdots \oplus \mathbb{F}[x]/(d_k(x)), \qquad d_1 \mid \cdots \mid d_k$$

로 분해된다.

- 각 성분 $\mathbb{F}[x]/(d)$는 기저 $1, x, \dots, x^{m-1}$($m = \deg d$)에서 d의 **동반행렬**(*companion matrix*)로 표현된다. 이것이 **유리 표준형**이며 체가 어떤 것이든(대수적으로 닫혀 있지 않아도) 성립한다.
- d_k는 T의 최소다항식이고 $d_1 \cdots d_k$는 특성다항식이다. Cayley–Hamilton 정리는 (d_k가 특성다항식을 나누므로) 이 분해의 따름정리이다.
- 특성다항식이 일차식들의 곱으로 완전히 분해되면(예: $\mathbb{F} = \mathbb{C}$), 기본인자 $(x-\lambda)^e$에 대응하는 성분 $\mathbb{F}[x]/((x-\lambda)^e)$는 기저 $(x-\lambda)^{e-1}, \dots, (x-\lambda), 1$에서 **Jordan 블록** $J_e(\lambda)$로 표현된다. 이것이 **Jordan 표준형**이다.

T가 대각화 가능할 필요충분조건은 최소다항식이 서로 다른 일차인수들의 곱인 것이다(기본인자가 모두 $e = 1$이어야 Jordan 블록이 전부 1×1이 되기 때문이다). 두 행렬이 닮음일 필요충분조건은 불변인자들이 모두 같은 것이며, 이는 $xI - A$를 PID $\mathbb{F}[x]$ 위의 행렬로 보아 그 Smith 표준형을 계산해서 얻는다.

예제 6.8 $A = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$의 특성다항식은 $(x-2)^3$이다. $A - 2I = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$이고 $(A-2I)^2 = 0$이지만 $A - 2I \neq 0$이므로 최소다항식은 $(x-2)^2$이다. 불변인자는 $x-2$와 $(x-2)^2$이고(곱이 특성다항식 $(x-2)^3$과 같고 $d_k = (x-2)^2$이 최소다항식이어야 하므로 $d_1 = x-2$), Jordan 형은 $J_1(2) \oplus J_2(2)$이다. 같은 특성다항식 $(x-2)^3$을 가진 $2I$(불변인자가 $x-2$ 세 개, 모두 1×1 블록)와 $J_3(2)$(단일 Jordan 블록, 불변인자 $(x-2)^3$ 하나)는 A와 불변인자가 서로 다르므로 A와 닮음이 아니며, 세 행렬은 서로 다른 세 닮음류를 이룬다.

6.6 연습문제와 해설

연습문제 6.9 위수 100인 가환군의 동형류는 몇 개인가?

풀이. $100 = 2^2 \cdot 5^2$이다. 각 소수의 지수 2에 대응하는 분할은 2와 $1+1$ 두 가지($\mathbb{Z}/p^2\mathbb{Z}$ 또는 $(\mathbb{Z}/p\mathbb{Z})^2$)이므로, 2-부분과 5-부분을 독립적으로 고르면 $2 \cdot 2 = 4$개의 동형류가 있다.

연습문제 6.10 $(\mathbb{Z}/15\mathbb{Z})^\times$를 순환군들의 곱으로 나타내어라.

풀이. 중국인의 나머지 정리(정리 4.7)로

$$(\mathbb{Z}/15\mathbb{Z})^\times \;\cong\; (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \;\cong\; \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

이다($\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$과 위수가 일치한다). $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$에는 위수 8인 원소가 없으므로(최대 위수는 $\operatorname{lcm}(2,4) = 4$) 순환군이 아니며, 따라서 법 15의 원시근은 존재하지 않는다.

연습문제 6.11 특성다항식이 $(x-1)^4$인 4×4 복소행렬의 닮음류는 몇 개인가?

풀이. Jordan 블록들의 크기는 4를 몇 개의 양의 정수의 합으로 나누는 분할에 대응하므로, 닮음류의 개수는 분할수 $p(4) = 5$개이다: 4, $3+1$, $2+2$, $2+1+1$, $1+1+1+1$.

참고 (다음 연결). 이제 체 자체의 구조로 넘어간다. 제14권 제7장에서는 체의 확대와 차수, 분해체, 유한체, 그리고 자와 컴퍼스만으로 하는 고대 작도 문제의 해결을 다룬다.

제 7 장

체의 확대, 분해체, 유한체, 작도 문제

개요 체 F를 더 큰 체 K 안에 포함시키는 것을 체의 **확대**(*field extension*)라 하고, K를 F 위의 벡터공간으로 보아 그 차원으로 확대의 크기를 잰다. 이 장은 확대의 차수와 탑 법칙에서 출발하여, 다항식의 근을 체에 추가하는 대수적 확대와 최소다항식, 다항식의 모든 근을 모은 분해체, 원소 개수가 유한인 체의 완전한 분류를 차례로 세운다. 이 도구들을 모아 자와 컴퍼스로 무엇을 작도할 수 있는지를 체의 차수 문제로 바꾸어, 정육면체의 배적·각의 삼등분·원적문제가 일반적으로 불가능함과 정다각형의 작도가능성을 판정하는 Gauss–Wantzel 정리를 증명과 함께 얻는다. 선행 지식: 앞 장들의 환, 아이디얼, 몫환과 다항식환, 주아이디얼정역, 유일인수분해(제14권 제4장, 제14권 제5장), 제7권의 벡터공간·기저·차원(제7권 제3장).

7.1 확대와 차수

정의 7.1 체 $F \subseteq K$에서 K를 F의 **확대**라 하고 K/F로 쓴다. K는 F 위의 벡터공간이며, 그 차원 $[K:F]$를 확대의 **차수**(*degree*)라 한다. $[K:F] < \infty$이면 K/F를 **유한 확대**라 한다.

$[\mathbb{C}:\mathbb{R}] = 2$이고(기저 $1, i$), $[\mathbb{R}:\mathbb{Q}] = \infty$이다(가산집합인 $\mathbb{Q}$ 위의 유한 차원 벡터공간은 가산이지만 $\mathbb{R}$은 비가산이므로).

정리 7.2 (탑 법칙) $F \subseteq K \subseteq L$이면

$$[L:F] = [L:K]\,[K:F] \tag{7.1}$$

이다. 한쪽이 무한이면 다른 쪽도 무한이다.

증명. K/F의 기저를 $\{a_i\}_{i\in I}$, L/K의 기저를 $\{b_j\}_{j\in J}$라 하면 $\{a_i b_j\}_{(i,j)\in I\times J}$가 L/F의 기저임을 보이면 된다. 생성: 임의의 $x \in L$은 $x = \sum_j c_j b_j$ ($c_j \in K$, 유한합)로 쓰이고, 각 $c_j = \sum_i d_{ij} a_i$ ($d_{ij} \in F$)이므로 $x = \sum_{i,j} d_{ij} a_i b_j$이다. 일차독립: $\sum_{i,j} d_{ij} a_i b_j = 0$이면 이를 $\sum_j \left(\sum_i d_{ij} a_i\right) b_j = 0$으로 묶고, $\{b_j\}$가 L/K 위에서 일차독립이므로 각 j에서 $\sum_i d_{ij} a_i = 0$이며, $\{a_i\}$가 K/F 위에서 일차독립이므로 모든 $d_{ij} = 0$이다. $\square$

이 곱셈 법칙은 간단하지만, §7.3에서 작도 문제를 해결하는 열쇠가 된다. $[K:F]$가 유한이면 $[L:F]$가 유한일 필요충분조건이 $[L:K]$가 유한인 것이라는 점도 식 (7.1)에서 바로 나온다.

7.2 대수적 원소와 최소다항식

정의 7.3 확대 K/F에서 $\alpha \in K$가 F 계수의 0이 아닌 다항식의 근이면 α는 F 위에서 **대수적**(*algebraic*)이라 하고, 그렇지 않으면 **초월적**(*transcendental*)이라 한다. 대수적 원소 α에 대하여 α를 근으로 갖는 최소 차수의 모닉 다항식 $m_\alpha \in F[x]$를 α의 **최소다항식**이라 한다.

$F[x] \to K$, $p \mapsto p(\alpha)$의 핵은 α를 근으로 갖는 다항식 전체이고, $F[x]$는 주아이디얼정역이므로 이 핵은 (m_α) 꼴이다. 핵이 극대인 것과 m_α가 기약인 것이 동치이므로(제5장), 최소다항식은 기약이고 α를 근으로 갖는 모든 다항식을 나눈다.

정리 7.4 α가 F 위에서 대수적이고 최소다항식 m_α의 차수가 n이면

$$F(\alpha) \cong F[x]/(m_\alpha), \qquad [F(\alpha) : F] = n,$$

이며 $1, \alpha, \dots, \alpha^{n-1}$이 $F(\alpha)$의 F 위 기저이다.

증명. 준동형사상 $F[x] \to F(\alpha)$, $p \mapsto p(\alpha)$의 핵이 (m_α)이고 m_α가 기약이므로 (m_α)는 극대아이디얼이고, 몫환 $F[x]/(m_\alpha)$는 체이다. 이 사상의 상은 α를 포함하는 $F(\alpha)$ 안의 부분환이면서 체이므로 $F(\alpha)$ 전체와 같다. 따라서 동형 $F(\alpha) \cong F[x]/(m_\alpha)$를 얻는다. 나눗셈 정리로 모든 $p \in F[x]$는 $p = q m_\alpha + r$, $\deg r < n$(또는 $r = 0$) 꼴로 쓰이므로 $F[x]/(m_\alpha)$의 원소는 $1, x, \dots, x^{n-1}$의 F 계수 일차결합으로 유일하게 표현되고, 이는 $F(\alpha)$에서 $1, \alpha, \dots, \alpha^{n-1}$이 기저임을 뜻한다. $\square$

예를 들어 $\mathbb{Q}(\sqrt[3]{2})$의 최소다항식은 $x^3 - 2$(차수 3, Eisenstein 판정으로 기약)이므로, $\mathbb{Q}(\sqrt[3]{2})$의 원소는 $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ $(a, b, c \in \mathbb{Q})$ 꼴로 유일하게 쓰이고 역원도 이 꼴로 표현된다.

명제 7.5 유한 확대는 대수적 확대이다. 즉 $[K : F] = n < \infty$이면 K의 모든 원소는 F 위에서 대수적이다.

증명. $\alpha \in K$에 대해 $1, \alpha, \dots, \alpha^n$은 $n+1$개의 원소인데 K는 F 위 n차원이므로 일차종속이다. $\sum_{k=0}^{n} c_k \alpha^k = 0$ $(c_k \in F$, 모두 0은 아님)이 성립하므로 α는 0이 아닌 다항식 $\sum c_k x^k$의 근이다. $\square$

참고 (대수적 수 전체와 초월수). 복소수 가운데 $\mathbb{Q}$ 위에서 대수적인 것 전체 $\overline{\mathbb{Q}} = \overline{\mathbb{Q}} \cap \mathbb{C}$는 체를 이루지만(두 대수적 수의 합·곱은 그 둘을 포함하는 유한 확대 안에 있으므로 명제 7.5에 의해 대수적이다), $\mathbb{Q}$ 위의 확대로는 무한 차수를 갖는다. π와 e는 초월수이다(Hermite 1873, Lindemann 1882). 뒤의 사실이 §7.3의 원적문제 불가능성을 준다.

7.3 작도 문제

정의 7.6 눈금 없는 자와 컴퍼스만으로, 길이 1인 선분에서 시작하여 유한 번의 작도로 얻을 수 있는 길이의 실수를 **작도가능수**라 한다.

좌표평면에서 이미 작도된 점들로 그은 두 직선, 직선과 원, 두 원의 교점을 구하는 일은 각각 일차방정식이나 이차방정식을 푸는 일과 같다. 교점의 좌표는 이전 단계까지 작도된 수들이 생성하는 체의 원소들의 사칙연산과 제곱근으로 표현되므로 다음이 성립한다.

정리 7.7 실수 α가 작도가능하면 $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_k$, $[F_{i+1} : F_i] = 2$, $\alpha \in F_k$인 체의 탑이 존재한다. 탑 법칙(정리 7.2)에 의해 $[\mathbb{Q}(\alpha) : \mathbb{Q}]$는 $[F_k : \mathbb{Q}] = 2^k$의 약수이므로 2의 거듭제곱이다.

이 정리는 필요조건만을 준다(역은 일반적으로 성립하지 않는다). 그래도 차수가 2의 거듭제곱이 아니면 작도 불가능하다는 결론을 얻기에는 충분하며, 이것으로 고대 그리스의 세 작도 문제가 해결된다.

- **정육면체 배적**: 부피가 2배인 정육면체의 한 변을 구하는 문제는 $\sqrt[3]{2}$의 작도를 요구한다. 최소다항식 $x^3 - 2$(Eisenstein, $p = 2$)의 차수가 3이어서 2의 거듭제곱이 아니므로 작도 불가능하다.
- **각의 삼등분**(60°의 경우): 삼배각 공식 $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$에 $\theta = 20^\circ$를 넣으면 $\cos 20^\circ$는 $8x^3 - 6x - 1 = 0$의 근이다. $y = 2x$로 바꾸면 $y^3 - 3y - 1 = 0$을 얻는데, 유리근 정리의 후보 ± 1을 대입하면 각각 $-3, 1$이 되어 근이 아니므로 이 삼차식은 $\mathbb{Q}$ 위에서 기약이다. 따라서 $[\mathbb{Q}(\cos 20^\circ) : \mathbb{Q}] = 3$이 2의 거듭제곱이 아니어서, 일반적인 각의 삼등분은 자와 컴퍼스로 불가능하다.
- **원적문제**: 넓이가 같은 정사각형의 변을 구하려면 $\sqrt{\pi}$를 작도해야 한다. π가 초월수이므로 $\sqrt{\pi}$도 초월수이고(대수적이면 $\pi = (\sqrt{\pi})^2$도 대수적이어야 하므로), 작도 불가능하다.
- **정n각형**(Gauss–Wantzel 정리): 정n각형이 작도가능할 필요충분조건은 $n = 2^k p_1 \cdots p_m$($k \geq 0$, p_i는 서로 다른 Fermat 소수 $2^{2^j}+1$)인 것이다. 정17각형은 $17 = 2^{2^2}+1$이 Fermat 소수이므로 작도가능하고, 정7각형과 정9각형은(7이 Fermat 소수가 아니고 $9 = 3^2$에서 3이 중복되므로) 불가능하다.

역사 (세 고대 작도 문제). 정육면체의 배적(*doubling the cube*, 델로스 문제), 각의 삼등분, 원적문제는 고대 그리스 기하학에서 자와 컴퍼스만을 허용하여 제기된 세 작도 문제이다. 정육면체 배적과 임의각 삼등분의 불가능성은 Pierre Wantzel이 1837년에 체의 차수 논법으로 증명하였고, 원적문제의 불가능성은 Lindemann이 1882년에 π의 초월성을 증명함으로써 완성되었다. 정n각형의 작도가능성은 Gauss가 1796년에 정17각형의 작도를 발견하고 충분조건을 제시하였으며, Wantzel이 1837년에 필요조건까지 증명하여 정리를 완성하였다.

7.4 분해체

정의 7.8 다항식 $f \in F[x]$의 모든 근 $\alpha_1, \ldots, \alpha_n$을 포함하는 가장 작은 확대 $K = F(\alpha_1, \ldots, \alpha_n)$을 f의 F 위 **분해체**(*splitting field*)라 한다.

분해체는 항상 존재한다. f가 F 위에서 완전히 일차식으로 분해되지 않으면 기약인수 하나를 골라 그 근을 추가한 체 $F_1 = F[x]/(p(x))$를 만들고, f가 완전히 분해될 때까지 이 과정을 반복하면 된다. 또한 분해체는 동형을 제외하고 유일하다(기약인수를 어떤 순서로 추가하든 동형인 체를 얻는다).

예제 7.9 $x^3 - 2$의 $\mathbb{Q}$ 위 분해체는 $\mathbb{Q}(\sqrt[3]{2}, \omega)$이다. 여기서 $\omega = e^{2\pi i/3}$이다. $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$이고 ω는 실수가 아니므로 $\mathbb{Q}(\sqrt[3]{2})$(실수체)에는 없으며, ω는 $x^2 + x + 1$의 근이다. 탑 법칙으로

분해체의 차수는 $3\cdot 2=6$이다. 실수체 $\mathbb{Q}(\sqrt[3]{2})$에는 x^3-2의 다른 두 근 $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$가 없으므로, 이 확대 하나만으로는 분해체가 되지 않는다.

7.5 유한체

정리 7.10

(1) 유한체의 원소 개수는 소수의 거듭제곱 $q=p^n$이다.

(2) 각 소수거듭제곱 $q=p^n$에 대하여 원소 q개인 체 $\mathbb{F}_q$가 동형을 제외하고 정확히 하나 존재하며, 그것은 x^q-x의 $\mathbb{F}_p$ 위 분해체이다.

(3) $\mathbb{F}_q^\times$는 위수 $q-1$인 순환군이다.

(4) $\mathbb{F}_{p^m}\subseteq\mathbb{F}_{p^n}\iff m\mid n$.

설명. (i) 유한체 K의 표수는 영환이 아니므로 소수 p이고(1을 p번 더하면 처음으로 0이 되는 p가 소수가 아니면 K에 영인자가 생긴다), K는 소체 $\mathbb{F}_p$ 위의 유한 차원 벡터공간이다. $[K:\mathbb{F}_p]=n$이면 $|K|=p^n$이다.

(ii) x^q-x의 도함수는 $qx^{q-1}-1=-1$(표수 p이고 $p\mid q$)이므로 x^q-x와 서로소이고, 따라서 x^q-x는 중근이 없이 정확히 q개의 서로 다른 근을 갖는다. 이 근들의 집합이 Frobenius 사상 $\phi(a)=a^p$의 체 자기동형사상 성질(덧셈과 곱셈을 보존함은 이항정리와 표수 p에서 $\binom{p}{k}\equiv 0\ (1\le k\le p-1)$이기 때문이다)에 의해 덧셈·곱셈에 닫혀 있어 체를 이루고, 이것이 $\mathbb{F}_q$이다. 서로 다른 q에 대한 $\mathbb{F}_q$가 동형이 아님은 원소 개수가 다르기 때문이다.

(iii) 체의 유한 곱셈부분군은 순환군이라는 사실의 특수한 경우이다: F_p 위에서 차수 d인 다항식은 근을 많아야 d개 가지므로(제5장), $\mathbb{F}_q^\times$의 위수 $q-1$의 각 약수 d에 대해 $x^d=1$의 해가 많아야 d개이고, 이로부터 위수 d인 원소가 0개이거나 정확히 $\varphi(d)$개임을 보일 수 있다(제15권 제1장). 모든 약수를 더하면 $q-1$이 되므로($\sum_{d\mid q-1}\varphi(d)=q-1$) 위수 $q-1$인 원소, 곧 생성원이 반드시 존재한다.

(iv) $\mathbb{F}_{p^m}\subseteq\mathbb{F}_{p^n}$이면 $\mathbb{F}_{p^n}$은 $\mathbb{F}_{p^m}$ 위의 벡터공간이므로 탑 법칙으로 $p^n=(p^m)^{[\mathbb{F}_{p^n}:\mathbb{F}_{p^m}]}$, 곧 $m\mid n$이다. 역으로 $m\mid n$이면 $(x^{p^m}-x)\mid(x^{p^n}-x)$이므로($a^{p^m}=a\Rightarrow a^{p^n}=a$를 거듭제곱으로 확인) $\mathbb{F}_{p^m}$의 모든 원소가 $\mathbb{F}_{p^n}$에 속한다. □

$\mathbb{F}_q$는 $\mathbb{F}_p[x]/(f)$(f는 n차 기약다항식)로 구체적으로 만든다. 예를 들어 $\mathbb{F}_8=\mathbb{F}_2[x]/(x^3+x+1)$이다($x^3+x+1$은 $\mathbb{F}_2$에서 0, 1 모두 근이 아니므로 기약이다). 유한체는 오류정정부호(Reed–Solomon 부호, CD·QR 코드), 암호(AES의 $\mathbb{F}_{2^8}$, 타원곡선 암호), 의사난수 생성의 기초이다.

7.6 연습문제와 해설

연습문제 7.11 $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]$를 구하고 $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$임을 보여라.

풀이. $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$이다($(a+b\sqrt{2})^2=3$이면 $2ab\sqrt{2}$ 항이 없어야 하므로 $ab=0$인데, $a=0$이면 $2b^2=3$, $b=0$이면 $a^2=3$이어서 모두 유리수 해가 없어 모순). 탑 법칙으로 $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=2\cdot 2=4$이다. $\beta=\sqrt{2}+\sqrt{3}$이라 하면 $\beta^{-1}=\sqrt{3}-\sqrt{2}$이므로($\beta(\sqrt{3}-\sqrt{2})=3-2=1$)

$\sqrt{3} = (\beta + \beta^{-1})/2$, $\sqrt{2} = (\beta - \beta^{-1})/2 \in \mathbb{Q}(\beta)$이다. 따라서 $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$이고 등호가 성립한다. β의 최소다항식은 $x^4 - 10x^2 + 1$이다($\beta^2 = 5 + 2\sqrt{6}$, $(\beta^2 - 5)^2 = 24$에서 전개).

연습문제 7.12 $\mathbb{F}_9$를 $\mathbb{F}_3[x]/(x^2+1)$로 만들 수 있음을 보이고 곱셈군의 생성원을 하나 찾아라.

풀이. $x^2 + 1$은 $\mathbb{F}_3$에서 근이 없으므로($0, 1, 2$에서 값 $1, 2, 2$) 기약이다. $i^2 = -1$로 쓰면 i의 위수는 4($i, -1, -i, 1$을 순환)이므로 생성원이 아니다. $1+i$는 $(1+i)^2 = 2i$, $(1+i)^4 = (2i)^2 = 4\cdot(-1) = -4 \equiv -1 \pmod 3$이므로 위수가 4가 아니고, $\left|\mathbb{F}_9^\times\right| = 8$의 약수 가운데 $1, 2, 4$가 모두 아니므로 위수는 8이다. 따라서 $1 + i$가 생성원이다.

연습문제 7.13 정5각형이 작도가능한 이유를 $\cos 72^\circ$의 최소다항식으로 설명하라.

풀이. $\cos 72^\circ = \dfrac{\sqrt{5}-1}{4}$은 $4x^2 + 2x - 1 = 0$의 근이므로 $\mathbb{Q}$ 위의 차수가 2이다. 이차확대 하나로 얻어지므로 정리 7.7의 역방향 구성(이차방정식의 해는 제곱근으로 표현되므로 작도가능)에 의해 작도가능하다. $5 = 2^{2^1} + 1$이 Fermat 소수라는 사실과 일치한다.

참고 (다음 연결). 분해체의 대칭, 즉 근들을 섞는 자기동형사상들의 군이 Galois 군이다. 다음 장에서는 확대체와 부분군의 대응, 그리고 5차 이상의 방정식에는 근의 공식이 없다는 정리를 다룬다.

제 8 장

Galois 이론과 근의 공식

개요 체의 확대 K/F에서 F의 원소를 고정하는 K의 체 자기동형사상 전체가 이루는 군을 Galois 군이라 하며, 분해체의 Galois 군은 그 다항식의 근들을 섞는 치환군으로 나타난다. 이 장은 Galois 군의 정의와 예로 시작하여, 확대의 차수와 군의 위수가 일치하는 Galois 확대를 특징짓고, Galois 대응(중간체와 부분군 사이의 포함 반전 일대일 대응)을 진술한다. 이 대응을 유한체와 원분체에 적용한 뒤, 가해군의 개념으로 거듭제곱근에 의한 해법을 번역하여 5차 이상의 일반 다항식에는 근의 공식이 없다는 Abel–Ruffini 정리를 Galois 군이 S_5인 구체적인 오차방정식으로 증명한다. 선행 지식: 앞 장의 분해체와 확대 차수(제14권 제7장), 제3장의 군의 작용과 Sylow 정리(제14권 제3장), 제2장의 정규부분군·몫군·단순군(제14권 제2장).

8.1 Galois 군

정의 8.1 확대 K/F에서 F의 원소를 모두 고정하는 K의 체 자기동형사상 전체를 $\mathrm{Gal}(K/F)$로 쓰고 K/F의 **Galois 군**이라 한다. 합성에 대해 군을 이룬다.

$\sigma \in \mathrm{Gal}(K/F)$이고 $f \in F[x]$의 근이 α이면 $f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0$이므로(계수가 F에 있어 σ가 고정함), σ는 f의 근을 f의 또 다른 근으로 보낸다. 따라서 f의 분해체의 Galois 군은 근들의 치환군, 즉 근이 n개이면 대칭군 S_n의 부분군으로 볼 수 있다.

예제 8.2

- $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id},\ z \mapsto \bar{z}\} \cong \mathbb{Z}/2$이다.
- $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$이다: $\sqrt{2} \mapsto \pm\sqrt{2}$, $\sqrt{3} \mapsto \pm\sqrt{3}$을 독립적으로 고를 수 있다.
- $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{id}\}$이다: $x^3 - 2$의 다른 두 근 $\omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$가 실수체 $\mathbb{Q}(\sqrt[3]{2})$에는 없으므로 자명한 자기동형사상만 있다.

8.2 Galois 확대

정의 8.3 유한 확대 K/F가 $|\mathrm{Gal}(K/F)| = [K:F]$를 만족하면 K/F를 **Galois 확대**라 한다.

동치로, K가 F 위의 **분리가능**(*separable*) 다항식(중근이 없는 다항식)의 분해체일 때 그리고 그때에만 K/F는 Galois 확대이다. 표수 0인 체(예: $\mathbb{Q}$)와 유한체에서는 모든 기약다항식이 분리가능하므로, 이런 체 위에서는 단지 "분해체"이기만 하면 Galois 확대이다. 반면 표수 $p > 0$인 체에서는 분리가능하지 않은 기약다항식(예: $\mathbb{F}_p(t)$ 위의 $x^p - t$)이 있을 수 있어 사정이 다르지만, 이 책에서 다루는 체는 모두 표수 0이거나 유한체이다.

예제 8.2의 세 번째 예 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$는 차수가 3인데 Galois 군이 자명하므로 Galois 확대가 아니다. 분해체 $\mathbb{Q}(\sqrt[3]{2}, \omega)$는 Galois 확대이며 Galois 군은 세 근의 모든 치환 S_3이다(위수 6 = 차수).

8.3 Galois 기본정리

정리 8.4 (Galois 대응) K/F가 유한 Galois 확대이고 $G = \mathrm{Gal}(K/F)$라 하자. 중간체 $F \subseteq E \subseteq K$와 부분군 $H \le G$ 사이에

$$E \mapsto \mathrm{Gal}(K/E), \qquad H \mapsto K^H = \{a \in K : \sigma(a) = a \ \forall \sigma \in H\}$$

가 서로 역인 포함 반전 대응을 준다. 또한 $[K:E] = |\mathrm{Gal}(K/E)|$, $[E:F] = [G : \mathrm{Gal}(K/E)]$이며, E/F가 Galois 확대일 필요충분조건은 $\mathrm{Gal}(K/E)$가 G의 정규부분군인 것이고 그때 $\mathrm{Gal}(E/F) \cong G/\mathrm{Gal}(K/E)$이다.

예제 8.5 ($x^3 - 2$) $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$, $G \cong S_3$이다. 부분군은 $\{e\}$, 위수 2인 세 개($\langle(12)\rangle$ 꼴, 서로 다른 근을 고정), A_3, S_3이다. 대응하는 중간체는 K, 세 근 각각을 붙인 $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\omega\sqrt[3]{2})$, $\mathbb{Q}(\omega^2\sqrt[3]{2})$(차수 3), $\mathbb{Q}(\omega)$(차수 2, A_3의 고정체), $\mathbb{Q}$이다. A_3만이 비자명한 정규 진부분군이므로 $\mathbb{Q}(\omega)/\mathbb{Q}$만이 Galois인 중간 확대이고, 세 차수 3 확대는 Galois가 아니다(A_3 이외의 위수 2 부분군은 정규가 아니다. S_3에서 전치는 서로 켤레이기 때문이다).

8.4 유한체와 원분체의 Galois 군

$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$는 Frobenius 사상 $\phi(a) = a^p$가 생성하는 위수 n인 순환군이다(정리 7.10(iv)에서 $\phi^n = \mathrm{id}$이고 $\phi^m \neq \mathrm{id}$, $m < n$, 이는 $|\mathbb{F}_{p^m}| < p^n$이기 때문). 중간체는 $\mathbb{F}_{p^m}$($m \mid n$)이며 $\langle\phi^m\rangle$의 고정체이다.

원분체 $\mathbb{Q}(\zeta_n)$, $\zeta_n = e^{2\pi i/n}$의 Galois 군은 $(\mathbb{Z}/n\mathbb{Z})^\times$이다. $\sigma_a(\zeta_n) = \zeta_n^a$가 그 대응이다. 이는 원분다항식 Φ_n이 기약이라는 사실(소수 n의 경우는 제5장)에 기초한다. Galois 군이 가환이므로 모든 중간체가 Galois 확대이다. 정17각형의 작도가능성은 $(\mathbb{Z}/17\mathbb{Z})^\times \cong \mathbb{Z}/16$의 부분군 사슬 $16 \supset 8 \supset 4 \supset 2 \supset 1$이 각 단계 차수 2인 확대들의 탑을 준다는 사실로 설명된다.

8.5 가해군과 거듭제곱근에 의한 풀이

정의 8.6 거듭제곱근을 차례로 붙이는 확대 $F = F_0 \subseteq F_1 = F_0(\sqrt[n]{a_1}) \subseteq \cdots \subseteq F_k = F_0(\sqrt[n]{a_1}, \dots)$로 다항식의 근에 도달할 수 있으면 그 다항식은 **거듭제곱근으로 풀린다**(*solvable by radicals*)고 한다.

2차, 3차(Cardano), 4차(Ferrari) 방정식에는 그런 공식이 있다.

정의 8.7 (가해군) 부분군 사슬 $G = G_0 \rhd G_1 \rhd \cdots \rhd G_k = \{e\}$에서 각 몫 G_i/G_{i+1}이 가환군이면 G를 **가해군**(*solvable group*)이라 한다.

$S_3 (\supset A_3 \supset \{e\}$, 몫 $\mathbb{Z}/2, \mathbb{Z}/3)$와 $S_4 (\supset A_4 \supset V_4 \supset \{e\}$, 몫 $\mathbb{Z}/2, \mathbb{Z}/3, \mathbb{Z}/2 \times \mathbb{Z}/2)$는 가해군이다. $n \ge 5$이면 A_n이 비가환 단순군이므로(제14권 제2장) $A_n/\{e\} = A_n$ 자체가 가환이 아니어서 $S_n \supset A_n \supset \{e\}$를 더 세분할 수 없고, S_n은 가해군이 아니다.

정리 8.8 (Galois) 표수 0인 체에서 다항식이 거듭제곱근으로 풀릴 필요충분조건은 그 분해체의 Galois 군이 가해군인 것이다.

거듭제곱근 $\sqrt[n]{a}$를 붙이는 확대는(필요한 단위근을 미리 붙여 두면) 순환 Galois 군을 갖는다. 따라서 거듭제곱근 탑의 Galois 군은 가환 몫들의 사슬을 갖고, 그 몫군은 분해체의 Galois 군도 가해군의 몫이어서(Galois 대응의 정규부분군 성질로) 가해이다. 역방향은 순환 확대가 거듭제곱근 확대임을 보이는 Kummer 이론을 쓴다.

> **예제 8.9 (풀리지 않는 5차 방정식)** $f(x)=x^5-4x+2$는 Eisenstein 판정($p=2$: $-4,0,0,0$은 2로 나누어지고 상수항 2는 4로 나누어지지 않음)으로 기약이다. 미분 $f'(x)=5x^4-4$는 실근을 $x=\pm(4/5)^{1/4}$ 두 개만 가지며, 그 극값은 $f(-(4/5)^{1/4})\approx 5.03>0$, $f((4/5)^{1/4})\approx -1.03<0$으로 부호가 반대이다. 따라서 f는 실근을 정확히 3개 갖는다(f는 $-\infty$ 쪽에서 음수, 극대점에서 양수, 극소점에서 음수, $+\infty$ 쪽에서 양수이므로 중간값 정리에 의해 세 구간에 각각 근이 하나 이상 있고, 극값이 두 개뿐이어서 f가 각 구간에서 단조이므로 정확히 하나씩이다). 기약인 5차 다항식의 분해체의 Galois 군은 추이적인 S_5의 부분군이고 그 위수는 5로 나누어지므로(Cauchy 정리) 5-순환을 포함한다. 복소켤레는 두 허근을 서로 바꾸고 나머지 세 실근을 고정하므로 전치(transposition) 하나를 준다. 5-순환과 전치 하나로 생성되는 S_5의 부분군은 S_5 전체이므로 Galois 군은 S_5이고, A_5가 단순군이어서 가해가 아니다. 정리 8.8에 의해 이 방정식의 근은 계수에서 사칙연산과 거듭제곱근만으로 표현할 수 없다.

흔한 오류 ("5차방정식은 풀 수 없다"의 뜻). 이 말은 "근이 존재하지 않는다"가 아니라 "근을 계수로부터 사칙연산과 거듭제곱근의 유한한 조합(공식)으로 표현할 수 없다"는 뜻이다. 근은 대수학의 기본정리로 존재하고, 수치적으로는 얼마든지 원하는 정확도로 계산할 수 있으며, 타원모듈러 함수를 쓰는 공식(Hermite, 1858)도 있다. 또한 모든 5차 방정식이 안 풀리는 것은 아니다: x^5-2처럼 Galois 군이 가해군(이 경우 위수 20)인 특수한 5차 방정식은 거듭제곱근으로 풀린다.

8.6 연습문제와 해설

> **연습문제 8.10** $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$의 부분군과 대응하는 중간체를 모두 구하라.

풀이. $\sigma:\sqrt{2}\mapsto-\sqrt{2}$(그리고 $\sqrt{3}$ 고정), $\tau:\sqrt{3}\mapsto-\sqrt{3}$(그리고 $\sqrt{2}$ 고정)이라 하면 위수 2인 부분군 $\langle\sigma\rangle,\langle\tau\rangle,\langle\sigma\tau\rangle$의 고정체는 각각 $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{6})$이다. 자명군과 전체 군은 각각 $K=\mathbb{Q}(\sqrt{2},\sqrt{3})$와 $\mathbb{Q}$에 대응한다(군이 가환이므로 다섯 중간체 모두 $\mathbb{Q}$ 위 Galois 확대이다).

> **연습문제 8.11** $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$를 구하고 $\sqrt{2}\in\mathbb{Q}(\zeta_8)$임을 보여라.

풀이. $(\mathbb{Z}/8\mathbb{Z})^\times=\{1,3,5,7\}\cong\mathbb{Z}/2\times\mathbb{Z}/2$이다. $\zeta_8+\zeta_8^{-1}=2\cos(\pi/4)=\sqrt{2}$이므로 $\sqrt{2}\in\mathbb{Q}(\zeta_8)$이다. 마찬가지로 $\zeta_8^2=i$이므로 $\mathbb{Q}(\zeta_8)=\mathbb{Q}(\sqrt{2},i)$이다.

> **연습문제 8.12** x^4-2의 분해체의 차수와 Galois 군을 구하라.

풀이. 근은 $\pm\sqrt[4]{2},\pm i\sqrt[4]{2}$이고 분해체는 $\mathbb{Q}(\sqrt[4]{2},i)$이다. $[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}]=4$(Eisenstein, $p=2$)이고 i는 실수체 $\mathbb{Q}(\sqrt[4]{2})$에 없으므로 탑 법칙으로 차수는 8이다. Galois 군은 $\sqrt[4]{2}\mapsto i^k\sqrt[4]{2}$, $i\mapsto\pm i$로 정해지는 위수 8의 군으로, 네 근을 정사각형의 꼭짓점으로 보았을 때의 대칭군 D_4와 동형이다.

제14권의 범위와 다음 읽기

이 권은 군과 부분군, 몫군과 동형정리, 군의 작용과 Sylow 정리, 환과 아이디얼, 다항식환·주아이디얼정역·유일인수분해, 가군과 주아이디얼정역 위의 유한생성 가군의 구조정리, 체의 확대와 유한체, Galois 이론을 다루었다. 앞 여섯 장에서 군·환·가군이라는 세 가지 대수 구조를 각각의 부분구조·몫구조·분류 정리로 세운 뒤, 제7 8장에서는 체의 확대를 벡터공간의 차원으로 재고 그 대칭을 군으로 번역하는 Galois 대응을 얻어, 작도 문제와 근의 공식이라는 두 고전적인 질문을 대수적으로 완결하였다. 대수적 정수론과 유한체 위의 해석적 정수론은 제15권으로, 가환대수와 대수기하는 제18권으로, 군의 표현론과 양자역학의 대칭은 양자역학 마스터 레퍼런스로 이어진다.

표준 참고서로 D. S. Dummit and R. M. Foote, *Abstract Algebra*; M. Artin, *Algebra*; J. A. Gallian, *Contemporary Abstract Algebra*; S. Lang, *Algebra*; I. Stewart, *Galois Theory*가 있다.

참고 자료의 사용 방식

본문의 설명과 문제는 이 참고서를 위해 새로 작성했다. 아래 목록은 관련 주제를 더 넓은 교재와 대조해 읽기 위한 안내이며, 이 원고 전체가 해당 기관이나 저자의 검토를 받았다는 뜻은 아니다. 개별 정리의 정확한 가정과 기호 약속은 자료마다 다를 수 있으므로, 독자는 다른 자료를 참고할 때마다 그 자료의 정의를 먼저 확인해야 한다.

- MIT OpenCourseWare, 18.701 *Algebra I*: 군과 군의 작용, 대칭.
- MIT OpenCourseWare, 18.702 *Algebra II*: 환, 체의 확대, Galois 이론.

제 15 권

정수론 · 대수적 정수론

제15권은 정수의 성질을 초등적 방법에서 대수적·해석적 방법까지 단계적으로 다루는 정수론이다. 제1–3장은 합동과 Euler 함수, 원시근, 이차잉여와 이차상호법칙, 산술함수와 Dirichlet 합성곱, Möbius 반전을 다룬다. 제4–5장은 연분수와 Diophantus 근사, Pell 방정식, 소수의 분포와 Riemann zeta 함수를 다룬다. 제6–8장은 대수적 정수와 수체의 정수환, Dedekind 정역과 아이디얼 분해, 이데알류군, p 진수와 국소–대역 원리로 대수적 정수론의 입구를 보인다.

제 1 장

합동, Euler 함수, 원시근

개요 정수론은 정수의 성질, 특히 나눗셈·약수·소수에 관한 성질을 다루며, 초등적 합동식 계산에서 출발하여 대수적·해석적 방법으로 확장된다. 이 장은 법 n의 기약잉여류가 이루는 곱셈군 $(\mathbb{Z}/n\mathbb{Z})^\times$와 그 위수인 Euler 함수 $\varphi(n)$을 군론의 언어로 다시 세우고, 이 군이 순환군이 되는 법 n(원시근이 존재하는 경우)을 완전히 분류한다. 이어 Wilson 정리와 Fermat 소정리의 역이 소수 판정에 쓰이는 방식, 그리고 소인수분해의 계산 어려움에 기초한 RSA 공개키 암호를 정리한다. 선행 지식: 제1권의 합동식과 중국인의 나머지 정리(제1권 제9장), 제14권의 군·순환군·Lagrange 정리(제14권 제1장).

1.1 법 n의 곱셈군

n과 서로소인 법 n의 잉여류 전체 $(\mathbb{Z}/n\mathbb{Z})^\times$는 곱셈에 대해 군을 이루며, 그 위수를 **Euler 함수**(*Euler's totient function*) $\varphi(n)$이라 한다. Lagrange 정리(제14권 제1장)로 Euler 정리

$$a^{\varphi(n)} \equiv 1 \pmod{n} \qquad (\gcd(a,n)=1) \tag{1.1}$$

가 성립한다. 중국인의 나머지 정리로 $n = \prod_{i} p_i^{e_i}$이면

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_i (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times, \qquad \varphi(n) = \prod_i p_i^{e_i-1}(p_i-1) = n\prod_{p\mid n}\left(1-\frac{1}{p}\right)$$

이다.

φ는 **곱셈적 함수**이다: $\gcd(m,n)=1 \Rightarrow \varphi(mn)=\varphi(m)\varphi(n)$. 서로소 조건 없이 모든 m,n에서 곱셈성이 성립하는 **완전 곱셈적 함수**와 구분해야 한다. $\varphi(4)=2\neq\varphi(2)^2=1$이 그 예이다(2와 2는 서로소가 아니다).

> **예제 1.1** $\varphi(360)=\varphi(2^3)\varphi(3^2)\varphi(5)=4\cdot 6\cdot 4=96$이다. $\gcd(7,360)=1$이므로 식 (1.1)에 의해 $7^{96}\equiv 1 \pmod{360}$이고, $7^{98}=7^{96}\cdot 7^2\equiv 7^2=49 \pmod{360}$이다.

1.2 위수와 원시근

> **정의 1.2** $\gcd(a,n)=1$일 때 $a^k\equiv 1 \pmod{n}$인 최소 양의 정수 k를 법 n에 대한 a의 **위수** $\operatorname{ord}_n(a)$라 한다.

위수는 $\varphi(n)$을 나누고, $a^m\equiv 1 \iff \operatorname{ord}_n(a)\mid m$이다(정리 1.9와 같은 논법). 위수가 $\varphi(n)$인 a를 **원시근**(*primitive root*)이라 하며, 원시근이 있다는 것은 $(\mathbb{Z}/n\mathbb{Z})^\times$가 순환군이라는 뜻이다.

> **정리 1.3 (원시근의 존재, Gauss)** 법 n의 원시근이 존재할 필요충분조건은 $n=1,2,4,p^k,2p^k$(p는 홀수 소수, $k\ge 1$)인 것이다.

증명의 뼈대. 소수 p에 대해서는 유한체의 곱셈군이 순환군이다(제14권 제5장). g가 법 p의 원시근이면 g 또는 $g+p$가 법 p^2의 원시근이고, 그것은 귀납적으로 모든 p^k에서 원시근이다(p 홀수). $2p^k$는 $(\mathbb{Z}/2\mathbb{Z})^\times$가 자명하므로 중국인의 나머지 정리로 $(\mathbb{Z}/2p^k\mathbb{Z})^\times \cong (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/p^k\mathbb{Z})^\times \cong (\mathbb{Z}/p^k\mathbb{Z})^\times$가 되어 p^k와 같은 경우로 환원된다. 그 밖의 n은 서로소인 두 인수 $m_1, m_2 > 2$로 나뉘어 $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/m_1\mathbb{Z})^\times \times (\mathbb{Z}/m_2\mathbb{Z})^\times$인데, $m_i > 2$이면 $\varphi(m_i)$가 짝수이므로 두 성분 모두 위수가 짝수인 원소를 가져 곱의 지수(모든 원소의 위수의 최소공배수)가 전체 위수 $\varphi(m_1)\varphi(m_2)$보다 작아 순환군이 아니다. $2^k (k \ge 3)$에서는 $(\mathbb{Z}/2^k\mathbb{Z})^\times \cong \mathbb{Z}/2 \times \mathbb{Z}/2^{k-2}$이어서 역시 순환군이 아니다. $\square$

> **예제 1.4** 법 7에서 3의 거듭제곱은 $3, 2, 6, 4, 5, 1$이므로($3^1=3$, $3^2=9\equiv 2$, $3^3\equiv 6$, $3^4\equiv 4$, $3^5\equiv 5$, $3^6\equiv 1$) 위수가 $6=\varphi(7)$인 3은 원시근이다. 2는 $2, 4, 1$로 위수 3이어서 원시근이 아니다. 법 8에서는 모든 홀수의 제곱이 1이므로($1^2, 3^2, 5^2, 7^2 \equiv 1 \pmod 8$) 원시근이 없다. $8 = 2^3$이 정리 1.3의 예외 꼴에 들지 않는 것과 일치한다.

원시근 g의 개수는 $\varphi(\varphi(n))$이다(식 (1.1)와 같은 순환군의 생성원 개수 공식, 제14권 제1장). 원시근 g에 대해 $a \equiv g^k$인 k(법 $\varphi(n)$에서 유일)를 **이산로그**(*discrete logarithm*)라 한다. 큰 소수에서 이산로그를 계산하는 효율적인 고전 알고리즘은 알려져 있지 않으며, Diffie–Hellman 키 교환의 안전성이 이에 기초한다. Shor 알고리즘은 양자 컴퓨터에서 이산로그와 소인수분해를 다항식 시간에 푼다.

1.3 k차 잉여와 거듭제곱근

원시근 g가 있는 법 n에서 $x^k \equiv a \pmod n$의 해의 개수는 이산로그로 쓴 일차 합동식 $k \cdot \operatorname{ind}(x) \equiv \operatorname{ind}(a) \pmod{\varphi(n)}$의 해의 개수와 같다. 따라서 $d = \gcd(k, \varphi(n))$에 대해 해가 있을 필요충분조건은 $a^{\varphi(n)/d} \equiv 1$이고, 있으면 정확히 d개이다. $k=2$, $n=p$가 홀수 소수인 경우가 다음 장의 Euler 판정법이다.

1.4 Wilson 정리

> **정리 1.5 (Wilson)** p가 소수이면 $(p-1)! \equiv -1 \pmod p$이다. 역으로 $n > 1$이 이 합동식을 만족하면 n은 소수이다.

증명. $\mathbb{F}_p^\times$의 원소를 각자의 역원과 짝지으면, 자기 자신이 역원인 $x^2 = 1$의 해 ± 1만 남는다. 따라서 곱은 $1 \cdot (-1) = -1$이다. 합성수 $n > 1$이면 n의 진약수 $d (1 < d < n)$가 $(n-1)!$을 나누므로 $(d \le n-1)$ $(n-1)! \equiv -1 \pmod d$가 될 수 없다($(n-1)! \equiv 0 \pmod d$인데 $-1 \not\equiv 0 \pmod d$, $d > 1$). $\square$

Wilson 정리는 소수 판정의 필요충분조건이지만 계승의 계산이 비싸 실용적이지 않다.

1.5 소수 판정과 RSA

Fermat 소정리의 대우로, $a^{n-1} \not\equiv 1 \pmod n$이면 n은 합성수이다. 역은 성립하지 않는다. $561 = 3 \cdot 11 \cdot 17$은 모든 서로소 a에서 $a^{560} \equiv 1$을 만족하는 **Carmichael** 수이다($2, 10, 16$이 모두 560을 나누므로 Korselt 판정법, 곧 n이 제곱인수가 없고 모든 소인수 p에서 $p-1 \mid n-1$이라는 조건을 만족한다). Miller–Rabin 판정법은 $n-1 = 2^s d$로 쓰고 $a^d, a^{2d}, \dots$를 확인하여 Carmichael 수도 높은 확률로 걸러낸다. 결정론적 다항식 시간 판정법(AKS, 2002)도 존재한다.

핵심 (RSA 암호). 큰 소수 p, q로 $N = pq$를 공개하고 $ed \equiv 1 \pmod{\varphi(N)}$인 e를 공개키, d를 비밀키로 한다. 평문 m의 암호문은 $c = m^e \bmod N$이고 복호는 $c^d \equiv m^{ed} \equiv m \pmod N$이다(Euler 정리, 중국인의 나머지 정리로 $\gcd(m, N) \neq 1$인 경우도 성립). N을 소인수분해할 수 있으면 $\varphi(N) = (p-1)(q-1)$과 d를 알 수 있으므로, 안전성은 N의 인수분해의 어려움에 기댄다.

1.6 연습문제와 해설

연습문제 1.6 법 11의 원시근을 모두 구하라.

풀이. $\varphi(10) = 4$개가 있다. 2의 거듭제곱은 $2, 4, 8, 5, 10, 9, 7, 3, 6, 1$로 위수 10이므로 2는 원시근이다. 나머지는 $2^k (\gcd(k, 10) = 1)$이므로 $2^1, 2^3, 2^7, 2^9 = 2, 8, 7, 6$이다.

연습문제 1.7 $x^3 \equiv 5 \pmod{13}$의 해의 개수를 구하라.

풀이. $\varphi(13) = 12$, $d = \gcd(3, 12) = 3$이다. $5^4 = 625 = 48 \cdot 13 + 1 \equiv 1 \pmod{13}$이므로 해가 있고 정확히 3개이다. 실제로 $7^3 = 343 = 26 \cdot 13 + 5$이므로 7이 해이고, 1의 세제곱근 $1, 3, 9$를 곱한 $7, 21, 63 \equiv 7, 8, 11 \pmod{13}$이 세 해이다.

연습문제 1.8 $p = 11$, $q = 13$, $e = 7$인 RSA에서 비밀키 d를 구하라.

풀이. $\varphi(N) = 10 \cdot 12 = 120$이고 $7d \equiv 1 \pmod{120}$이다. $7 \cdot 103 = 721 = 6 \cdot 120 + 1$이므로 $d = 103$이다.

연습문제 1.9 $p \equiv 1 \pmod 4$인 소수에서 $\left(\frac{p-1}{2}\right)!^2 \equiv -1 \pmod p$임을 보여라.

풀이. Wilson 정리에서 $(p-1)! = \prod_{k=1}^{(p-1)/2} k(p-k) \equiv \prod (-k^2) = (-1)^{(p-1)/2} \left(\frac{p-1}{2}\right)!^2$이다. $(p-1)/2$가 짝수이므로 $\left(\frac{p-1}{2}\right)!^2 \equiv -1$이다. 따라서 $p \equiv 1 \pmod 4$이면 -1은 법 p의 제곱잉여이다.

참고 (다음 연결). 마지막 연습문제처럼 "어떤 수가 법 p의 제곱수인가"는 정수론의 중심 질문 가운데 하나이다. 다음 장에서는 Legendre 기호와 이차상호법칙을 다룬다.

제 2 장

이차잉여와 이차상호법칙

개요 홀수 소수 p와 p로 나누어떨어지지 않는 정수 a에 대해, $x^2 \equiv a \pmod p$가 풀리는지를 판정하는 문제는 정수론에서 가장 오래되고 가장 영향력이 큰 질문 가운데 하나이다. 이 장은 그 판정을 부호 하나로 기록하는 Legendre 기호를 정의하고, Euler 판정법과 두 보충법칙을 거쳐 서로 다른 두 홀수 소수 p, q에 대한 $\left(\frac{p}{q}\right)$과 $\left(\frac{q}{p}\right)$의 관계를 주는 이차상호법칙(정수론의 "황금 정리")을 증명과 함께 제시한다. 응용으로 큰 수의 이차잉여 여부를 빠르게 계산하는 방법과, 두 제곱수의 합으로 표현되는 소수를 판정하는 Fermat의 정리를 다룬다. 선행 지식: 앞 장의 원시근과 Wilson 정리(제15권 제1장).

2.1 Legendre 기호

정의 2.1 홀수 소수 p와 $p \nmid a$에 대해 $x^2 \equiv a \pmod p$가 해를 가지면 a를 **이차잉여**(*quadratic residue*), 아니면 **이차비잉여**(*quadratic nonresidue*)라 한다. **Legendre 기호**(*Legendre symbol*)를

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a\text{가 이차잉여}, \\ -1 & a\text{가 이차비잉여}, \\ 0 & p \mid a \end{cases}$$

로 정의한다.

법 p에서 0이 아닌 제곱수는 $1^2, \dots, \left(\frac{p-1}{2}\right)^2$로 정확히 $(p-1)/2$개이다. x와 $-x$가 같은 제곱을 주므로 $1 \le x \le (p-1)/2$만 살피면 충분하고, 이 범위의 서로 다른 x, y는 서로 다른 제곱을 준다. $x^2 \equiv y^2$이면 $p \mid (x-y)(x+y)$인데 $0 < x+y < p$이므로 $p \mid x-y$여야 하고, $|x-y| < p$이므로 $x = y$이기 때문이다. 따라서 $1, \dots, p-1$ 가운데 이차잉여와 이차비잉여는 각각 $(p-1)/2$개이다.

정리 2.2 (Euler 판정법) p가 홀수 소수이고 $p \nmid a$이면 $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$이다. 이 합동식은 $p \mid a$일 때도 성립한다. 따라서 Legendre 기호는 완전 곱셈적이다:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

증명. 원시근 g(제15권 제1장)로 $a \equiv g^k$라 하면 a가 이차잉여일 필요충분조건은 k가 짝수인 것이다. $k = 2j$이면 $x = g^j$가 해를 주고, 역으로 $x \equiv g^j$가 해이면 $g^{2j} \equiv g^k$에서 $2j \equiv k \pmod{p-1}$이며 $p-1$이 짝수이므로 k도 짝수이다. 한편 $g^{(p-1)/2} \equiv -1$이다. g의 위수가 $p-1$이므로 $g^{(p-1)/2} \not\equiv 1$이고, $(g^{(p-1)/2})^2 \equiv 1$인데 $\mathbb{F}_p$에서 $x^2 = 1$의 해는 ± 1뿐이기 때문이다. 따라서 $a^{(p-1)/2} \equiv (g^{(p-1)/2})^k \equiv (-1)^k$이고, 이것이 $\left(\frac{a}{p}\right)$와 같다. 곱셈성은 $(ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2}$이고 $p \ge 3$에서 $1 \not\equiv -1 \pmod p$이므로 합동식의 양변이 $\pm 1, 0$으로 일치하는 데서 나온다. $\square$

따름정리 2.3 (제1보충법칙) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, 즉 -1은 $p \equiv 1 \pmod 4$일 때 그리고 그때에만 이차잉여이다.

이 따름정리에서 $4k+1$ 꼴의 소수가 무한히 많음을 얻는다. $p_1, \dots, p_m$이 $4k+1$ 꼴의 소수들이라 하고 $N = (2p_1 \cdots p_m)^2 + 1$이라 하면, N은 홀수이고 N의 임의의 소인수 q에 대해 $-1 \equiv (2p_1 \cdots p_m)^2 \pmod q$이므로 -1이 법 q의 이차잉여, 곧 따름정리 2.3에 의해 $q \equiv 1 \pmod 4$이다. 또한 q는 어떤 p_i와도 다르다($p_i \mid N$이면 $p_i \mid 1$이 되어 모순). 따라서 $4k+1$ 꼴의 소수는 그 유한 목록 밖에도 하나 더 존재하며, 귀납적으로 무한히 많다.

2.2 Gauss 보조정리와 제2보충법칙

보조정리 2.4 (Gauss) p가 홀수 소수이고 $p \nmid a$일 때, $a, 2a, \dots, \frac{p-1}{2}a$를 법 p로 $(-p/2, p/2)$ 범위의 대표원으로 놓았을 때 음수가 되는 것의 개수를 μ라 하면 $\left(\frac{a}{p}\right) = (-1)^{\mu}$이다.

증명. 각 ka의 대표원이 음수이면 -1을 곱해 양수로 바꾼다. 그러면 얻어지는 $(p-1)/2$개의 수는 모두 $1, \dots, (p-1)/2$ 안에 있고 서로 다르다. 실제로 서로 다른 $k, k' \le (p-1)/2$에서 $ka \equiv \pm k'a$이면 $p \nmid a$이므로 $k \equiv \pm k'$인데, $2 \le k + k' \le p-1$이고 $|k - k'| < p$이므로 $k = k'$뿐이다. 따라서 이 수들은 $1, \dots, (p-1)/2$의 재배열이다. 모든 ka의 곱을 비교하면

$$a^{(p-1)/2}\left(\frac{p-1}{2}\right)! \equiv (-1)^{\mu}\left(\frac{p-1}{2}\right)! \pmod p,$$

$\left(\frac{p-1}{2}\right)!$이 p와 서로소이므로 양변을 나누면 $a^{(p-1)/2} \equiv (-1)^{\mu}$이고, Euler 판정법(정리 2.2)과 비교하여 $\left(\frac{a}{p}\right) = (-1)^{\mu}$를 얻는다. □

따름정리 2.5 (제2보충법칙) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$, 즉 2는 $p \equiv \pm 1 \pmod 8$일 때 이차잉여이고 $p \equiv \pm 3 \pmod 8$일 때 이차비잉여이다.

증명. $a = 2$이면 $2, 4, \dots, p-1$ 가운데 $p/2$보다 큰 것의 개수가 μ이다. $2k > p/2$는 $k > p/4$와 같으므로

$$\mu = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor.$$

$p = 8m + r (r \in \{1,3,5,7\})$로 쓰면 μ는 $r = 1, 3, 5, 7$에서 차례로 $2m,\ 2m+1,\ 2m+1,\ 2m+2$이므로 μ가 짝수일 필요충분조건은 $r = 1, 7$, 곧 $p \equiv \pm 1 \pmod 8$이다. 같은 네 경우에 $(p^2-1)/8 = \big((p-1)/2\big)\big((p+1)/2\big)/2$는 $8m^2+2m,\ 8m^2+6m+1,\ 8m^2+10m+3,\ 8m^2+14m+6$이어서 그 홀짝도 같다. □

예를 들어 $17 \equiv 1 \pmod 8$이므로 2는 법 17의 이차잉여이며, 실제로 $6^2 = 36 \equiv 2 \pmod{17}$이다. $11 \equiv 3 \pmod 8$이므로 2는 법 11의 이차비잉여이다.

2.3 이차상호법칙

정리 2.6 (이차상호법칙, Gauss) 서로 다른 홀수 소수 p, q에 대해

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \tag{2.1}$$

즉 p, q 중 하나라도 $4k+1$ 꼴이면 $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$이고, 둘 다 $4k+3$ 꼴이면 부호가 반대이다.

격자점 증명. 먼저 $\left(\frac{q}{p}\right) = (-1)^{S(q,p)}$, $S(q,p) = \sum_{k=1}^{(p-1)/2} \lfloor kq/p \rfloor$임을 보인다($p, q$ 홀수). $m = (p-1)/2$로 놓고 $kq = p\lfloor kq/p \rfloor + r_k$, $0 < r_k < p$라 쓴다. $r_k < p/2$인 것을 $e_1, \dots, e_s$, $r_k > p/2$인 것을 $f_1, \dots, f_\mu$라 하면, 보조정리 2.4의 증명에서 $\{e_i\} \cup \{p - f_j\} = \{1, \dots, m\}$이므로

$$\sum_{k=1}^{m} k = \sum e_i + \mu p - \sum f_j.$$

한편 $q\sum_{k=1}^{m} k = pS(q,p) + \sum e_i + \sum f_j$이다. 두 식을 빼면

$$(q-1)\sum_{k=1}^{m} k = p\bigl(S(q,p) - \mu\bigr) + 2\sum f_j$$

이다. q가 홀수이므로 좌변이 짝수이고 p가 홀수이므로 $S(q,p) \equiv \mu \pmod 2$이다. 보조정리 2.4에 의해 $\left(\frac{q}{p}\right) = (-1)^{\mu} = (-1)^{S(q,p)}$이다.

이제 $S(q,p)$는 직사각형 $0 < x < p/2$, $0 < y < q/2$ 안의 격자점 가운데 대각선 $y = qx/p$ 아래에 있는 것의 수이다. 각 x에서 $y < qx/p$인 정수 y는 $\lfloor qx/p \rfloor$개이고 $qx/p < q/2$이므로 모두 직사각형 안에 있다. 마찬가지로 $S(p,q) = \sum_{y=1}^{(q-1)/2} \lfloor py/q \rfloor$는 같은 직사각형 안에서 대각선 위쪽($x < py/q$)의 격자점 수이다. 대각선 위에는 격자점이 없다($py = qx$이면 $p \mid x$인데 $0 < x < p/2$이므로 불가능). 직사각형 안의 격자점은 모두 $\frac{p-1}{2}\cdot\frac{q-1}{2}$개이므로

$$S(q,p) + S(p,q) = \frac{p-1}{2}\cdot\frac{q-1}{2}$$

이다. 따라서 $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{S(p,q)+S(q,p)} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$이다. □

역사 ("황금 정리"). 이차상호법칙은 Euler와 Legendre가 먼저 진술했으나 완전한 증명은 Gauss가 1796년에 처음 얻었고, 1801년의 *Disquisitiones Arithmeticae*에 실렸다. Gauss는 이 정리를 *theorema aureum*(황금 정리)이라 부르며 생전에 여러 가지 증명을 남겼다. 오늘날에는 Gauss 합, 원분체의 Galois 이론, 유체론 등 수백 가지 증명이 알려져 있으며, 이 법칙을 일반 수체로 확장하려는 시도가 대수적 정수론과 Langlands 프로그램(제28권 제3장)으로 이어졌다.

2.4 계산 예

상호법칙과 두 보충법칙, 곱셈성으로 큰 Legendre 기호도 인수분해 없이(Jacobi 기호를 쓰면) 빠르게 계산된다.

예제 2.7 $\left(\frac{219}{383}\right)$을 구하자(383은 소수). $219 = 3 \cdot 73$이다.

- $\left(\frac{3}{383}\right)$: $3 \equiv 383 \equiv 3 \pmod 4$ 이므로 상호법칙에서 부호가 바뀌어 $= -\left(\frac{383}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1$.
- $\left(\frac{73}{383}\right)$: $73 \equiv 1 \pmod 4$ 이므로 $= \left(\frac{383}{73}\right) = \left(\frac{18}{73}\right) = \left(\frac{2}{73}\right)\left(\frac{9}{73}\right) = 1 \cdot 1 = 1$ ($73 \equiv 1 \pmod 8$).

따라서 $\left(\frac{219}{383}\right) = 1$, 즉 219는 법 383의 이차잉여이다.

Jacobi 기호(*Jacobi symbol*) $\left(\frac{a}{n}\right) = \prod_i \left(\frac{a}{p_i}\right)^{e_i}$ ($n = \prod p_i^{e_i}$ 홀수)도 같은 상호법칙을 만족하므로 소인수분해 없이 계산할 수 있다.

흔한 오류 (Jacobi 기호와 이차잉여). Jacobi 기호가 1이라고 해서 a가 법 n의 이차잉여인 것은 아니다. $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$이지만, 2는 법 3에서도 법 5에서도 제곱수가 아니다. Solovay–Strassen 소수 판정법은 Euler 판정법과 Jacobi 기호의 이러한 차이(Jacobi 기호가 합성수 n에서는 $a^{(n-1)/2}$와 어긋날 수 있다는 점)를 이용한다.

2.5 두 제곱수의 합

정리 2.8 (Fermat) 홀수 소수 p가 $p = a^2 + b^2$으로 쓰일 필요충분조건은 $p \equiv 1 \pmod 4$이다.

증명. 필요성: 정수의 제곱은 법 4로 0 또는 1이므로 $a^2 + b^2$은 법 4로 $0, 1, 2$ 중 하나이며 3일 수 없다. 홀수 소수 p는 법 4로 1 또는 3이므로 $p \equiv 1 \pmod 4$이다.

충분성: $p \equiv 1 \pmod 4$이면 따름정리 2.3로 -1이 법 p의 이차잉여이므로 $p \mid x^2+1 = (x+i)(x-i)$인 정수 x가 있다. Gauss 정수환 $\mathbb{Z}[i]$는 Euclid 정역(제14권 제5장)이므로 주아이디얼정역이고, 여기서는 기약원이 곧 소원이다. p가 $\mathbb{Z}[i]$에서 소원이면 $p \mid x+i$ 또는 $p \mid x-i$여야 하는데, 이는 $x/p \pm i/p$가 Gauss 정수가 아니므로 불가능하다. 따라서 p는 기약원이 아니어서 $p = \alpha\beta$(α, β는 단위원이 아님)로 쓰인다. 노름 $N(a+bi) = a^2 + b^2$은 곱셈적이고 단위원의 노름이 1이므로 $N(\alpha)N(\beta) = p^2$에서 $N(\alpha) = N(\beta) = p$이다. $\alpha = a + bi$라 하면 $p = a^2 + b^2$이다. □

일반적으로 양의 정수가 두 제곱수의 합일 필요충분조건은 소인수분해에서 $4k+3$ 꼴 소인수의 지수가 모두 짝수인 것이다.

2.6 연습문제와 해설

연습문제 2.9 $x^2 \equiv 3 \pmod{13}$의 해가 있는지 판정하고 있으면 구하라.

풀이. $13 \equiv 1 \pmod 4$이므로 $\left(\frac{3}{13}\right) = \left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$이다. $4^2 = 16 \equiv 3$이므로 해는 $x \equiv \pm 4$이다.

연습문제 2.10 3이 이차잉여인 소수 $p > 3$을 법 12로 분류하라.

풀이. 상호법칙으로 $\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right)$이다. $p \equiv 1 \pmod 4$이면 $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$이므로 $\left(\frac{3}{p}\right) = 1 \iff p \equiv 1 \pmod 3$이다. $p \equiv 3 \pmod 4$이면 $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$이므로 $\left(\frac{3}{p}\right) = 1 \iff \left(\frac{p}{3}\right) = -1 \iff p \equiv 2 \pmod 3$이다. 중국인의 나머지 정리로 합치면 $p \equiv 1 \pmod{12}$ 또는 $p \equiv 11 \pmod{12}$, 곧 $p \equiv \pm 1 \pmod{12}$이다. 검산: 13에서 $4^2 \equiv 3$, 11에서 $5^2 = 25 \equiv 3$이고, $5 \equiv 5 \pmod{12}$인 소수 5에서는 3이 제곱수가 아니다.

연습문제 2.11 $13 = a^2 + b^2$, $29 = a^2 + b^2$의 해를 찾고, $13 \cdot 29 = 377$을 두 제곱수의 합으로 두 가지 방법으로 나타내어라.

풀이. $13 = 3^2 + 2^2$, $29 = 5^2 + 2^2$이다. $(3 + 2i)(5 + 2i) = 11 + 16i$, $(3 + 2i)(5 - 2i) = 19 + 4i$이므로 $377 = 11^2 + 16^2 = 19^2 + 4^2$이다. Gauss 정수의 곱셈이 Brahmagupta–Fibonacci 항등식 $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 = (ac + bd)^2 + (ad - bc)^2$을 준다.

참고 (다음 연결). 이차잉여는 곱셈적 함수의 한 예였다. 다음 장에서는 약수에 대한 합으로 정의되는 산술함수와 그 반전 공식을 다룬다.

제 3 장

산술함수, Dirichlet 합성곱, Möbius 반전

개요 산술함수는 양의 정수에서 정의된 복소값 함수이며, 약수의 개수·약수의 합·Euler 함수처럼 정수의 약수 구조를 기록하는 함수들이 그 대표적인 예이다. 이 장은 산술함수의 곱셈성을 정의하고, 약수에 대한 합으로 두 산술함수를 결합하는 Dirichlet 합성곱이 항등원을 가진 가환 결합 연산임을 보인다. 이를 바탕으로 Möbius 함수와 Möbius 반전 공식을 증명하고, 유한체 위의 기약다항식의 개수와 완전수의 분류에 적용한다. 끝으로 Dirichlet 급수와 Euler 곱, 산술함수의 평균 크기를 통해 해석적 정수론으로 가는 다리를 놓는다. 선행 지식: 제1권의 약수의 개수와 합, 앞 장들의 곱셈적 함수(Euler 함수 φ, Legendre 기호).

3.1 산술함수와 곱셈성

정의 3.1 양의 정수 전체에서 정의된 복소값 함수 $f : \mathbb{N}_{>0} \to \mathbb{C}$를 **산술함수**(*arithmetic function*)라 한다. 산술함수 f가 $f(1) = 1$이고 $\gcd(m,n) = 1$일 때 $f(mn) = f(m)f(n)$이면 f를 **곱셈적**(*multiplicative*)이라 하고, $f(1) = 1$이고 모든 m, n에 대해 $f(mn) = f(m)f(n)$이면 **완전 곱셈적**이라 한다.

곱셈적 함수는 소수 거듭제곱에서의 값으로 완전히 결정된다. $n = \prod p_i^{e_i}$이면 $f(n) = \prod_i f(p_i^{e_i})$이기 때문이다. 대표적인 예는 다음과 같다.

- $\tau(n) = \sum_{d \mid n} 1$(약수의 개수), $\sigma(n) = \sum_{d \mid n} d$(약수의 합), $\varphi(n)$(Euler 함수). 모두 곱셈적이지만 완전 곱셈적은 아니다.
- $\mu(n)$(**Möbius 함수**): $\mu(1) = 1$, n이 서로 다른 소수 k개의 곱이면 $\mu(n) = (-1)^k$, n이 제곱인 수를 가지면 $\mu(n) = 0$.
- $\mathbf{1}(n) = 1$, $\mathrm{id}(n) = n$, $\varepsilon(n) = [n = 1]$(완전 곱셈적). 여기서 $[P]$는 명제 P가 참이면 1, 거짓이면 0이다.

von Mangoldt 함수 $\Lambda(n)$은 $n = p^k$(p 소수, $k \geq 1$)이면 $\log p$, 그 밖에는 0으로 정의한다. $\Lambda(6) = 0$이지만 $\Lambda(2)\Lambda(3) \neq 0$이므로 Λ는 곱셈적이 아니지만, 소수 분포 연구의 핵심이다.

곱셈적 함수의 값은 소수 거듭제곱에서 정해진다. 예를 들어 $\tau(p^k) = k+1$, $\sigma(p^k) = 1+p+\cdots+p^k$, $\varphi(p^k) = p^{k-1}(p-1)$, $\mu(p) = -1$이고 $k \geq 2$이면 $\mu(p^k) = 0$이다. $n = 12 = 2^2 \cdot 3$에서는 $\tau(12) = 3 \cdot 2 = 6$, $\sigma(12) = 7 \cdot 4 = 28$, $\varphi(12) = 2 \cdot 2 = 4$, $\mu(12) = 0$이다.

3.2 Dirichlet 합성곱

정의 3.2 산술함수 f, g의 **Dirichlet 합성곱**(*Dirichlet convolution*)을

$$(f * g)(n) = \sum_{d \mid n} f(d)\, g\!\left(\frac{n}{d}\right)$$

로 정의한다. 합은 n의 양의 약수 d 전체에 대해 취한다.

정리 3.3 Dirichlet 합성곱은 가환이고 결합적이며 항등원은 ε이다. $f(1) \neq 0$인 산술함수는 합성곱에 대한 역원을 갖는다. 두 곱셈적 함수의 합성곱은 곱셈적이다.

증명. $(f*g)(n) = \sum_{ab=n} f(a)g(b)$로 쓰면 a, b의 역할을 바꾸어 가환성이 나온다. 결합성: $((f*g)*h)(n)$과 $(f*(g*h))(n)$은 모두 $\sum_{abc=n} f(a)g(b)h(c)$이다. 항등원: $(f*\varepsilon)(n) = \sum_{d\mid n} f(d)\varepsilon(n/d) = f(n)$이다. 역원: $f(1)\neq 0$일 때 $g(1) = 1/f(1)$, $n>1$에서

$$g(n) = -\frac{1}{f(1)} \sum_{\substack{d \mid n \\ d < n}} g(d)\, f\!\left(\frac{n}{d}\right)$$

로 귀납적으로 정의하면 $(f*g)(1) = 1$이고, $n>1$에서 $(g*f)(n) = \sum_{d\mid n} g(d) f(n/d) = 0 = \varepsilon(n)$이다. 곱셈성: f, g가 곱셈적이고 $\gcd(m,n)=1$이면 mn의 약수는 m의 약수 d_1과 n의 약수 d_2의 곱 $d_1 d_2$로 유일하게 쓰이고 $\gcd(d_1, d_2) = \gcd(m/d_1, n/d_2) = 1$이므로

$$(f*g)(mn) = \sum_{d_1\mid m}\sum_{d_2\mid n} f(d_1)f(d_2)\, g\!\left(\frac{m}{d_1}\right) g\!\left(\frac{n}{d_2}\right) = (f*g)(m)\,(f*g)(n)$$

이다. $(f*g)(1) = f(1)g(1) = 1$이다. □

두 곱셈적 함수의 합성곱은 곱셈적이지만 완전 곱셈적이라고는 할 수 없다. 예를 들어 $\tau = \mathbf{1}*\mathbf{1}$에서 $\tau(4) = 3 \neq \tau(2)^2 = 4$이다. 이 언어로 다음 네 항등식이 성립한다.

$$\tau = \mathbf{1}*\mathbf{1}, \qquad \sigma = \mathrm{id}*\mathbf{1}, \qquad \mathrm{id} = \varphi*\mathbf{1}, \qquad \log = \Lambda*\mathbf{1}. \tag{3.1}$$

처음 두 식은 정의 자체이다. 셋째 식은 제14권(제14권 제1장)의 $\sum_{d\mid n}\varphi(d) = n$이고, 넷째 식은 산술의 기본정리 $n = \prod p^{a_p}$에서 얻는 $\log n = \sum_{p^k \mid n} \log p$이다. $p^k \mid n$인 $(p,k)(k\geq 1)$마다 $\Lambda(p^k) = \log p$가 한 번씩 더해지기 때문이다.

3.3 Möbius 반전 공식

명제 3.4 $\mu * \mathbf{1} = \varepsilon$, 즉 $\sum_{d\mid n}\mu(d) = [n=1]$이다.

증명. 양변이 곱셈적이므로(정리 3.3) $n = p^k (k\geq 1)$에서 확인하면 된다. $\sum_{j=0}^{k}\mu(p^j) = \mu(1) + \mu(p) = 1 - 1 = 0$이다. □

정리 3.5 (Möbius 반전) 산술함수 F가 $F(n) = \sum_{d\mid n} f(d)$이면

$$f(n) = \sum_{d\mid n} \mu(d)\, F\!\left(\frac{n}{d}\right) \tag{3.2}$$

이다. 역으로 식 (3.2)이 성립하면 $F(n)=\sum_{d\mid n} f(d)$ 이다.

증명. $F=f*\mathbf{1}$의 양변에 μ를 합성곱하면 합성곱의 결합성과 명제 3.4에 의해 $\mu*F=\mu*(\mathbf{1}*f)=(\mu*\mathbf{1})*f=\varepsilon*f=f$이다. 역으로 $f=\mu*F$이면 $\mathbf{1}*f=(\mathbf{1}*\mu)*F=F$이다. □

예를 들어 $\mathrm{id}=\varphi*\mathbf{1}$에 반전을 적용하면

$$\varphi(n)=\sum_{d\mid n}\mu(d)\frac{n}{d}=n\prod_{p\mid n}\Bigl(1-\frac{1}{p}\Bigr)$$

를 다시 얻는다. 둘째 등호는 $\mu(d)\neq 0$인 d가 n의 서로 다른 소인수들의 곱(제곱인수 없는 약수)이라는 사실에서 곱 $\prod_{p\mid n}(1-1/p)$를 전개한 항과 일대일로 대응하기 때문이다. 이는 포함-배제 원리(제19권)의 정수론적 형태이다. $n=12$이면 $12-6-4+2=4=\varphi(12)$이다. 또 $\sigma=\mathrm{id}*\mathbf{1}$에서 $\sum_{d\mid 12}\mu(d)\sigma(12/d)=\sigma(12)-\sigma(6)-\sigma(4)+\sigma(2)=28-12-7+3=12=\mathrm{id}(12)$이다.

예제 3.6 (기약다항식의 개수) $\mathbb{F}_q$ 위의 차수 n인 모닉 기약다항식의 개수를 N_n이라 하면, $\mathbb{F}_{q^n}$의 원소를 $\mathbb{F}_q$ 위의 최소다항식별로 세어 $q^n=\sum_{d\mid n} dN_d$이다. 이는 $\mathbb{F}_{q^n}$의 각 원소의 최소다항식 차수 d가 n의 약수이고(정리 7.10), 차수가 d인 기약다항식은 $\mathbb{F}_{q^n}$ 안에 근을 정확히 d개 가지기 때문이다. Möbius 반전을 적용하면

$$N_n=\frac{1}{n}\sum_{d\mid n}\mu(d)\,q^{n/d}$$

이다. $q=2$, $n=4$이면 $\frac{1}{4}(16-4)=3$개$(x^4+x+1,\ x^4+x^3+1,\ x^4+x^3+x^2+x+1)$이다.

3.4 완전수와 σ

$\sigma(n)=2n$인 n을 **완전수**(*perfect number*)라 한다. Euclid는 2^p-1이 소수(Mersenne 소수)이면 $2^{p-1}(2^p-1)$이 완전수임을 보였고, Euler는 짝수 완전수가 모두 이 꼴임을 증명했다. σ의 곱셈성으로 $\sigma\bigl(2^{p-1}(2^p-1)\bigr)=(2^p-1)\cdot 2^p$이다. $\sigma(2^{p-1})=2^p-1$이고 소수 2^p-1에서 $\sigma(2^p-1)=2^p$이기 때문이다.

정리 3.7 (Euclid–Euler) 짝수 n이 완전수일 필요충분조건은 $n=2^{p-1}(2^p-1)$이고 2^p-1이 소수인 것이다.

증명. 충분성은 위에서 보였다. 필요성: $n=2^k m$($k\ge 1$, m 홀수)이 완전수이면 $\sigma(n)=(2^{k+1}-1)\sigma(m)=2^{k+1}m$이다. $2^{k+1}-1$은 2^{k+1}과 서로소이므로 $(2^{k+1}-1)\mid m$이다. $m=(2^{k+1}-1)t$라 하면 $\sigma(m)=2^{k+1}t=m+t$이다. $k\ge 1$이므로 $2^{k+1}-1\ge 3$이어서 $t<m$이고, t, m은 모두 m의 약수이다. $t\neq 1$이면 $1, t, m$이 서로 다른 약수이므로 $\sigma(m)\ge 1+t+m>m+t$가 되어 모순이다. 따라서 $t=1$이고 $m=2^{k+1}-1$이며 $\sigma(m)=m+1$이므로 m의 약수는 1과 m뿐, 곧 m은 소수이다. $p=k+1$로 놓으면 된다. □

홀수 완전수가 존재하는지는 아직 알려져 있지 않다. 알려진 Mersenne 소수는 대규모 분산 계산 프로젝트로 찾은 것을 포함해 수십 개이며, 무한히 많은지도 미해결이다.

3.5 Dirichlet 급수와 Euler 곱

산술함수 f에 Dirichlet 급수 $D_f(s)=\sum_{n\ge 1} f(n)n^{-s}$를 대응시키면 합성곱이 곱이 된다.

$$D_{f*g}=D_f D_g \qquad \text{(두 급수가 절대수렴하는 곳에서)}. \tag{3.3}$$

두 절대수렴 급수의 곱을 $n=ab$로 묶으면 $\sum_{a,b} f(a)g(b)(ab)^{-s}=\sum_n\big(\sum_{ab=n} f(a)g(b)\big)n^{-s}$이기 때문이다. $f=\mathbf{1}$이면 **Riemann zeta 함수**

$$\zeta(s)=\sum_{n\ge 1}\frac{1}{n^s}\qquad(\operatorname{Re} s>1)$$

이다. 곱셈적 f에 대해서는 산술의 기본정리가 **Euler 곱**으로 표현된다. 절대수렴하는 영역에서 $D_f(s)=\prod_p\sum_{k\ge 0} f(p^k)p^{-ks}$이고, 특히

$$\zeta(s)=\prod_{p}\frac{1}{1-p^{-s}},\qquad \frac{1}{\zeta(s)}=\sum_{n\ge1}\frac{\mu(n)}{n^s},\qquad -\frac{\zeta'(s)}{\zeta(s)}=\sum_{n\ge1}\frac{\Lambda(n)}{n^s} \tag{3.4}$$

이다. 둘째 식은 $\mu*\mathbf{1}=\varepsilon$에 식 (3.3)를 적용한 $D_\mu\zeta=1$이다. 셋째 식은 $\zeta'(s)=-\sum_n(\log n)n^{-s}$와 $\log=\Lambda*\mathbf{1}$(식 (3.1))에서 $-\zeta'=D_\Lambda\,\zeta$로 나온다.

$s\to 1^+$에서 $\zeta(s)\to\infty$이므로(조화급수의 발산) Euler 곱의 인수가 무한히 많아야 하고, 따라서 소수가 무한히 많다. 더 정확하게는 $\sum_p 1/p=\infty$이다(Euler).

$\sum_p 1/p=\infty$의 증명. Euler 곱의 로그를 취하면 $\log\zeta(s)=\sum_p\sum_{k\ge1}\frac{1}{kp^{ks}}\ge\sum_p p^{-s}$이다$(s>1)$. $s\to1^+$에서 $\log\zeta(s)\to\infty$이므로 $\sum_p p^{-s}\to\infty$이다. 만약 $\sum_p 1/p$가 수렴하면 $p^{-s}<p^{-1}$이므로 $\sum_p p^{-s}$가 유계여서 모순이다. $\square$

다음 장들의 소수 분포 이론은 이 함수들의 해석적 성질을 연구한다.

3.6 평균 크기

산술함수는 개별 값이 불규칙해도 평균은 규칙적이다.

$$\sum_{n\le x}\tau(n)=x\log x+(2\gamma-1)x+O(\sqrt{x}),\qquad \sum_{n\le x}\varphi(n)=\frac{3}{\pi^2}x^2+O(x\log x). \tag{3.5}$$

첫 식은 Dirichlet의 쌍곡선 방법으로 얻으며 $\gamma\approx 0.5772$는 Euler–Mascheroni 상수이다. 둘째 식에서 두 정수가 서로소일 "확률"이 $6/\pi^2=1/\zeta(2)$임이 따라 나온다. 이는 각 소수 p가 두 수를 동시에 나누지 않을 확률 $1-p^{-2}$들의 곱이 $1/\zeta(2)$인 것과 일치한다.

식 (3.5)의 증명 개요. $\varphi=\mu*\mathrm{id}$이므로

$$\sum_{n\le x}\varphi(n)=\sum_{d\le x}\mu(d)\sum_{m\le x/d} m=\sum_{d\le x}\mu(d)\Big(\frac{x^2}{2d^2}+O\Big(\frac{x}{d}\Big)\Big)=\frac{x^2}{2}\sum_{d\le x}\frac{\mu(d)}{d^2}+O(x\log x).$$

$\sum_{d>x} d^{-2}=O(1/x)$이므로 $\sum_{d\le x}\mu(d)d^{-2}=1/\zeta(2)+O(1/x)$이고, 이 오차가 $x^2\cdot O(1/x)=O(x)$를 준다. $1/\zeta(2)=6/\pi^2$이므로 둘째 식을 얻는다. τ에 대해서는 $\sum_{n\le x}\tau(n)=\#\{(a,b):ab\le x\}$를 $a\le\sqrt{x}$ 또는 $b\le\sqrt{x}$로 나누어 $2\sum_{a\le\sqrt{x}}\lfloor x/a\rfloor-\lfloor\sqrt{x}\rfloor^2$로 쓴다. $\sum_{a\le y}1/a=\log y+\gamma+O(1/y)$를 $y=\sqrt{x}$에 쓰면 $2x(\tfrac12\log x+\gamma)-x+O(\sqrt{x})$를 얻는다. $\square$

3.7 연습문제와 해설

연습문제 3.8 $\sigma(n)$이 홀수일 필요충분조건을 구하라.

풀이. 곱셈성으로 각 $\sigma(p^k) = 1 + p + \cdots + p^k$의 홀짝을 본다. $p = 2$이면 항상 홀수이고, p가 홀수이면 $k+1$개의 홀수의 합이므로 k가 짝수일 때 홀수이다. 따라서 n이 제곱수이거나 제곱수의 두 배일 때이다.

연습문제 3.9 $\sum_{d \mid n} \mu(d)\tau(d) = (-1)^{\omega(n)}$임을 보여라($\omega(n)$은 서로 다른 소인수의 개수).

풀이. 좌변은 곱셈적이고 $n = p^k (k \ge 1)$에서 $\mu(1)\tau(1) + \mu(p)\tau(p) = 1 - 2 = -1$이다. 따라서 n의 서로 다른 소인수마다 -1이 곱해진다.

연습문제 3.10 $\mathbb{F}_3$ 위의 차수 2 모닉 기약다항식의 개수를 공식과 직접 셈으로 확인하라.

풀이. 공식으로 $\frac{1}{2}(9-3) = 3$이다. 모닉 이차식 9개 중 근이 있는 것은 $(x-a)(x-b)$ 꼴로 $\binom{3}{2}+3 = 6$개이므로 기약은 3개$(x^2+1,\ x^2+x+2,\ x^2+2x+2)$이다.

참고 (다음 연결). Dirichlet 급수의 해석적 성질은 소수의 분포를 결정한다. 그 전에 다음 장에서는 무리수를 유리수로 근사하는 연분수와 Pell 방정식을 다룬다.

제 4 장

연분수, Diophantus 근사, Pell 방정식

개요 **연분수**(*continued fraction*)는 실수를 $a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}$ 꼴로 전개하여 유리수로 가장 효율적으로 근사하는 방법이다. 이 장은 단순 연분수의 구성과 그 근사분수(수렴분수)의 성질을 정리하고, 수렴분수가 Dirichlet 의미에서 최선의 근사임을 보인 뒤, 이차 무리수의 연분수가 결국 주기적이라는 Lagrange 정리를 거쳐 Pell 방정식 $x^2 - dy^2 = 1$의 완전한 해법에 적용한다. 선행 지식: 제1권 제2장의 나눗셈 알고리즘과 유클리드 알고리즘, 제1권 제6장의 무리수, 제14권 제4장의 단원군.

4.1 단순 연분수

실수 α에 대해

$$a_0 = \lfloor \alpha \rfloor, \qquad \alpha_1 = \frac{1}{\alpha - a_0} \ (\alpha \neq a_0), \qquad a_1 = \lfloor \alpha_1 \rfloor, \qquad \alpha_2 = \frac{1}{\alpha_1 - a_1}, \ \dots$$

을 반복하여 정수열 $a_0, a_1, a_2, \dots$ (**부분몫**, *partial quotient*)를 얻는다. $a_0 \in \mathbb{Z}$이고 $k \geq 1$에서 α_k는 성질상 1보다 크므로 $a_k \geq 1$이다. 이 과정으로

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}} = [a_0; a_1, a_2, \dots] \tag{4.1}$$

라고 쓴다. α가 유리수이면 과정이 유한 번에 끝나며, 이는 유클리드 알고리즘(제1권 제2장)과 같은 계산이다. 실제로 $\alpha = p/q$ $(q > 0)$에서 $a_0 = \lfloor p/q \rfloor$를 빼고 역수를 취하는 것은 나눗셈 정리 $p = a_0 q + r$에서 q/r로 넘어가는 것과 같은 재귀이므로, 나머지가 0이 될 때 연분수가 끝난다.

> **예제 4.1** $\frac{43}{19} = [2; 3, 1, 4]$이다. 유클리드 알고리즘의 각 단계
>
> $$43 = 2 \cdot 19 + 5, \qquad 19 = 3 \cdot 5 + 4, \qquad 5 = 1 \cdot 4 + 1, \qquad 4 = 4 \cdot 1$$
>
> 에서 몫 $2, 3, 1, 4$가 그대로 부분몫이 된다. 마지막 나머지가 0이 되는 순간 전개가 끝난다.

α가 무리수이면 α_k가 모든 k에서 정의되고 정수가 될 수 없으므로 과정은 무한히 계속되며, 이때 식 (4.1)의 우변은 무한 연분수의 극한(다음 절의 수렴분수의 극한)으로 이해한다.

4.2 수렴분수

$[a_0; a_1, \dots, a_n]$을 유한 번째에서 끊어 얻은 기약분수를 p_n/q_n으로 쓰고 n번째 **수렴분수**(*convergent*)라 한다. 다음 점화식으로 계산한다.

$$p_n = a_n p_{n-1} + p_{n-2}, \qquad q_n = a_n q_{n-1} + q_{n-2} \qquad (p_{-1}=1,\ q_{-1}=0,\ p_{-2}=0,\ q_{-2}=1). \tag{4.2}$$

명제 4.2 (점화식의 타당성과 기약성) 식 (4.2)으로 정의된 p_n, q_n은 실제로 $[a_0; a_1, \dots, a_n] = p_n/q_n$을 만족하며,

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1} \tag{4.3}$$

이다. 따라서 p_n/q_n은 기약분수이다.

증명. $n = 0$에서 $p_0/q_0 = a_0/1$로 성립한다(약속 $p_{-1}=1, q_{-1}=0$ 아래 식 (4.2)이 $p_0 = a_0, q_0 = 1$을 준다). 귀납적으로 $[a_0; \dots, a_{n-1}, a_n]$은 $[a_0; \dots, a_{n-2}, a_{n-1} + 1/a_n]$과 같은 분수이므로, a_{n-1} 자리에 $a_{n-1} + 1/a_n$을 넣은 $(n-1)$단계 점화식

$$\frac{(a_{n-1} + 1/a_n)p_{n-2} + p_{n-3}}{(a_{n-1} + 1/a_n)q_{n-2} + q_{n-3}} = \frac{a_n(a_{n-1}p_{n-2} + p_{n-3}) + p_{n-2}}{a_n(a_{n-1}q_{n-2} + q_{n-3}) + q_{n-2}} = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}}$$

를 주며, 이것이 바로 식 (4.2)의 p_n/q_n이다. 식 (4.3)은 귀납법으로 보인다. $n = 0$에서 $p_0 q_{-1} - p_{-1} q_0 = a_0 \cdot 0 - 1 \cdot 1 = -1 = (-1)^{-1}$이다. 귀납 단계는

$$\begin{aligned} p_n q_{n-1} - p_{n-1} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-1} - p_{n-1}(a_n q_{n-1} + q_{n-2}) \\ &= -(p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) = -(-1)^{n-2} = (-1)^{n-1} \end{aligned}$$

이다. 식 (4.3)에서 p_n, q_n의 공약수는 $(-1)^{n-1}$을 나누므로 1뿐이다. □

수렴분수는 α의 양쪽에서 번갈아 접근한다. 짝수 번째 수렴분수는 아래에서, 홀수 번째는 위에서 접근하며, 다음 오차 평가가 성립한다.

$$\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}} \le \frac{1}{q_n^2}. \tag{4.4}$$

예제 4.3 (원주율과 황금비의 연분수) $\pi = [3; 7, 15, 1, 292, \dots]$의 수렴분수는 $3, 22/7, 333/106, 355/113, \dots$이다. $355/113$은 다음 부분몫 292가 매우 크기 때문에 분모의 크기에 비해 이례적으로 정확하다($|\pi - 355/113| \approx 2.7 \times 10^{-7}$, 식 (4.4)의 상계 $1/q_3^2 \approx 7.8 \times 10^{-5}$보다도 훨씬 작다). 황금비 $\phi = \frac{1+\sqrt{5}}{2} = [1; 1, 1, 1, \dots]$는 모든 부분몫이 1이라 수렴분수(연속한 Fibonacci 수의 비)가 가장 느리게 수렴하는, 유리수로 "가장 근사하기 어려운" 무리수이다.

4.3 최선 근사와 Dirichlet 정리

정리 4.4 (Dirichlet 근사정리) 무리수 α에 대해 $|\alpha - p/q| < 1/q^2$을 만족하는 기약분수 p/q가 무한히 많다.

수렴분수가 바로 그런 분수들이다(식 (4.4)). 이 정리는 비둘기집 원리로도 독립적으로 증명된다. 양의 정수 Q를 고정하고 $\{\cdot\}$을 소수부분 기호라 하면, $Q+1$개의 수 $0, \{\alpha\}, \{2\alpha\}, \dots, \{Q\alpha\}$를 길이

$1/Q$인 구간 Q개 $[0,1/Q),[1/Q,2/Q),\dots$에 넣으면 비둘기집 원리에 의해 적어도 두 개가 같은 구간에 들어가므로, 그 둘에 대응하는 정수 $0\le i<j\le Q$에서 $|\{j\alpha\}-\{i\alpha\}|<1/Q$이다. $q=j-i$, $p=\lfloor j\alpha\rfloor-\lfloor i\alpha\rfloor$로 두면 $|q\alpha-p|<1/Q\le 1/q$이고 $1\le q\le Q$이므로 $|\alpha-p/q|<1/(qQ)\le 1/q^2$이다. $Q\to\infty$로 보내면 서로 다른 p/q가 무한히 나온다(그렇지 않으면 어떤 고정된 p/q에서 $|\alpha-p/q|$가 임의로 작은 $1/(qQ)$보다 작아야 하는데 $\alpha\neq p/q$이므로 모순).

수렴분수는 다음 의미에서 **최선 근사**이다: $q<q_{n+1}$이면 $|q\alpha-p|\ge|q_n\alpha-p_n|$이 모든 정수 p에 대해 성립한다. 역으로 $|\alpha-p/q|<\frac{1}{2q^2}$이면 p/q는 반드시 어떤 수렴분수이다(Legendre). 상수 1을 $1/\sqrt{5}$까지는 줄일 수 있지만 그보다 작은 상수로는 모든 무리수에 대해 정리가 성립하지 않는다(Hurwitz; 극단적인 경우가 황금비이다). 반면 대수적 무리수 α에 대해 $|\alpha-p/q|<q^{-2-\varepsilon}$ $(\varepsilon>0)$을 만족하는 기약분수 p/q는 유한 개뿐이다(Roth 정리, 1955).

4.4 이차 무리수와 주기 연분수

정리 4.5 (Lagrange) 무리수 α의 연분수가 결국 주기적일 필요충분조건은 α가 **이차 무리수**(*quadratic irrational*, 정수 계수 이차방정식의 무리근)인 것이다.

예제 4.6 $\sqrt{2}=[1;\overline{2}]$, $\sqrt{3}=[1;\overline{1,2}]$, $\sqrt{7}=[2;\overline{1,1,1,4}]$이다(막대는 반복되는 주기 부분을 뜻한다). 제곱수가 아닌 양의 정수 d에 대해 $\sqrt{d}=[a_0;\overline{a_1,\dots,a_{r-1},2a_0}]$ 꼴이며, 주기 부분 $a_1,\dots,a_{r-1}$은 좌우대칭이다(즉 $a_i=a_{r-i}$).

4.5 Pell 방정식

제곱수가 아닌 양의 정수 d에 대해 $x^2-dy^2=1$을 **Pell 방정식**이라 한다.

정리 4.7 Pell 방정식은 자명해 $(\pm1,0)$ 외의 정수해를 가지며, 양의 해 (x,y) $(x,y>0)$ 중 가장 작은 것 (x_1,y_1)(**기본해**, *fundamental solution*)에 대해 모든 양의 해는

$$x_n+y_n\sqrt{d}=(x_1+y_1\sqrt{d})^n\qquad(n\ge1)\tag{4.5}$$

로 완전히 주어진다. 기본해는 $\sqrt{d}$의 연분수 주기의 길이를 r이라 할 때, r이 짝수이면 수렴분수 p_{r-1}/q_{r-1}에서, r이 홀수이면 p_{2r-1}/q_{2r-1}에서 얻는다.

대수적으로는 환 $\mathbb{Z}[\sqrt{d}]$에서 **노름** $N(x+y\sqrt{d})=x^2-dy^2$가 곱셈적$(N(\xi\eta)=N(\xi)N(\eta))$이므로, 노름이 1인 원소들이 곱셈에 대해 군을 이루고, 정리 4.7은 그 군이 $\{\pm1\}\times\mathbb{Z}$와 동형(한 원소 $x_1+y_1\sqrt{d}$로 생성)이라는 진술이다. 이는 제14권 제4장의 단원군 개념을 실이차수체의 정수환에 적용한 것이고, 제6장(제6장)에서 다룰 실이차체의 단원군에 대한 Dirichlet 단원정리의 특수한 경우이다.

예제 4.8 (기본해의 계산) $x^2-2y^2=1$: $\sqrt{2}=[1;\overline{2}]$, 주기 길이 $r=1$(홀수)이므로 $p_1/q_1=3/2$에서 기본해 $(3,2)$를 얻는다 $(3^2-2\cdot2^2=9-8=1)$. 다음 해는 $(3+2\sqrt{2})^2=17+12\sqrt{2}$로 $(17,12)$이다 $(17^2-2\cdot12^2=289-288=1)$. 수렴분수 $p_0/q_0=1/1$은 $1^2-2\cdot1^2=-1$이므로 음의 Pell 방정식 $x^2-2y^2=-1$의 해 $(1,1)$이다.

예제 4.9 (작은 d에서도 큰 기본해) $x^2 - 61y^2 = 1$의 기본해는 $(1766319049,\ 226153980)$이다. Fermat가 1657년에 도전 문제로 낸 예이며, $\sqrt{61}$의 연분수 주기 길이가 11로 길기 때문에 해가 매우 크다. 기본해의 크기는 d에 대해 매우 불규칙하게 변한다.

4.6 연습문제와 해설

연습문제 4.10 $\sqrt{3}$의 연분수와 처음 네 수렴분수를 구하라.

풀이. $\sqrt{3} = 1 + (\sqrt{3}-1)$이고 $\frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2} = 1 + \frac{\sqrt{3}-1}{2}$, $\frac{2}{\sqrt{3}-1} = \sqrt{3}+1 = 2+(\sqrt{3}-1)$이므로 연분수는 $[1;\overline{1,2}]$이다. 수렴분수는 $1, 2, \frac{5}{3}, \frac{7}{4}$이다. $7^2 - 3\cdot 4^2 = 1$이다.

연습문제 4.11 $x^2 - 3y^2 = 1$의 기본해를 찾고 다음 두 해를 구하라.

풀이. 주기 길이 $r = 2$(짝수)이므로 $p_1/q_1 = 2/1$, 기본해 $(2,1)$이다. $(2+\sqrt{3})^2 = 7 + 4\sqrt{3}$, $(2+\sqrt{3})^3 = 26 + 15\sqrt{3}$이므로 다음 두 해는 $(7,4)$, $(26,15)$이다.

연습문제 4.12 $x^2 - 3y^2 = -1$은 정수해가 없음을 보여라.

풀이. 법 3으로 보면 $x^2 \equiv -1 \equiv 2 \pmod 3$인데 법 3의 제곱수는 $0, 1$뿐이므로 해가 없다. 같은 결론은 연분수로도 설명된다. 음의 Pell 방정식 $x^2 - dy^2 = -1$은 $\sqrt{d}$의 연분수 주기 길이가 홀수일 때에만 해를 가지는데, $\sqrt{3}$의 주기 길이는 $r = 2$로 짝수이다.

다음 연결. 정수론의 많은 질문은 소수가 얼마나 많고 어떻게 분포하는지로 귀착된다. 다음 장(제5장)에서는 소수정리와 Riemann zeta 함수를 다룬다.

제 5 장

소수의 분포와 Riemann zeta 함수

개요 소수의 개수 함수 $\pi(x)$(x 이하 소수의 개수)의 크기는 산술적 대상인 소수의 분포를 해석적 방법으로 다루게 하는 핵심 질문이다. 이 장은 소수가 무한히 많다는 사실을 넘어 $\pi(x)$의 크기를 재는 초등적 결과(Chebyshev 부등식)에서 출발하여, 깊은 해석적 정리인 소수정리와 그 증명의 핵심 도구인 Riemann zeta 함수의 해석적 연속, 함수방정식, 영점 분포(Riemann 가설)를 정리하고, 등차수열의 소수(Dirichlet 정리)와 소수 사이의 간격에 관한 최근 결과로 맺는다. 선행 지식: 제3장의 Dirichlet 급수와 Euler 곱, 제11권 제1장과 제11권 제6장의 해석함수와 유수. 제28권의 연구 동향 장에서 다룬 최근 결과들의 배경이다.

5.1 소수의 무한성과 크기

$\pi(x)$를 x 이하의 소수의 개수라 한다. Euclid의 논증(제1장)은 소수가 무한히 많다는 것만 보여 주고, 크기에 대한 정보는 거의 주지 않는다. Euler 곱에서 $\sum_{p \le x} 1/p = \log\log x + O(1)$이므로 소수는 제곱수의 역수의 합($\sum 1/n^2 < \infty$)보다 훨씬 조밀하게 분포한다.

정리 5.1 (Chebyshev) 충분히 큰 x에서 $c_1 \dfrac{x}{\log x} \le \pi(x) \le c_2 \dfrac{x}{\log x}$인 양의 상수 $c_1 < c_2$가 있다.

증명의 핵심은 중앙 이항계수 $\binom{2n}{n}$이다. $\dfrac{4^n}{2n+1} \le \binom{2n}{n} \le 4^n$이고, $n < p \le 2n$인 모든 소수가 $\binom{2n}{n} = \dfrac{(2n)!}{(n!)^2}$를 나누며(분자 $(2n)!$에 정확히 한 번 나타나고 분모 $(n!)^2$에는 나타나지 않는다), 각 소수의 거듭제곱 인수는 $2n$ 이하이다. 이로부터 상계 $\prod_{n<p\le 2n} p \le \binom{2n}{n} \le 4^n$과 하계 $\binom{2n}{n} \le (2n)^{\pi(2n)}$을 얻고, 이를 $x = 2, 4, 8, \dots$에 걸쳐 정밀화하면 정리의 양쪽 부등식이 나온다. 같은 방법의 정밀화로 Bertrand 가설(모든 $n \ge 1$에 대해 $n < p \le 2n$인 소수가 존재한다)도 증명된다.

5.2 소수정리

정리 5.2 (소수정리, Hadamard–de la Vallée Poussin, 1896)

$$\pi(x) \sim \frac{x}{\log x}, \qquad \text{더 정확히} \qquad \pi(x) \sim \operatorname{Li}(x) = \int_2^x \frac{\mathrm{d}t}{\log t}.$$

동치인 형태는 $\psi(x) = \sum_{n \le x} \Lambda(n) \sim x$이다(여기서 Λ는 von Mangoldt 함수, 제3장). Gauss는 소수표를 보고 "x 근처에서 소수의 밀도는 약 $1/\log x$"라고 추측했다. $\operatorname{Li}(x)$가 $x/\log x$보다 훨씬 좋은 근사이다. 예를 들어 $x = 10^9$에서 $\pi(x) = 50\,847\,534$이고 $x/\log x \approx 48\,254\,942$, $\operatorname{Li}(x) \approx 50\,849\,234$이다.

증명은 $\zeta(s)$가 직선 $\operatorname{Re} s = 1$ 위에서 0이 되지 않는다는 사실에 결정적으로 의존한다. Selberg와 Erdős(1949)는 복소해석을 쓰지 않는 "초등적" 증명을 찾았지만 길고 복잡하다. Newman(1980)의 Tauberian 논법은 비교적 짧은 복소해석적 증명을 준다.

5.3 Riemann zeta 함수의 해석적 성질

$\zeta(s) = \sum_{n \ge 1} n^{-s}$는 $\operatorname{Re} s > 1$에서 정칙이다. Riemann(1859)은 다음을 보였다.

- ζ는 $s = 1$의 단순극(유수 1)을 제외하고 복소평면 전체로 해석적으로 연장된다.
- 함수방정식: $\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$에 대해 $\xi(s) = \xi(1-s)$이다.
- 자명한 영점 $s = -2, -4, -6, \dots$ 외의 영점(비자명 영점)은 띠 $0 < \operatorname{Re} s < 1$ 안에 있다.

특수값으로 $\zeta(2) = \pi^2/6$, $\zeta(4) = \pi^4/90$이고, 일반적으로 $\zeta(2k)$($k \ge 1$)는 Bernoulli 수로 표현되는 π^{2k}의 유리수 배이다. $\zeta(3)$은 무리수임이 알려져 있지만(Apéry, 1978), 홀수 값들의 닫힌 형태는 알려져 있지 않다. 해석적 연장으로 $\zeta(-1) = -\tfrac{1}{12}$이지만, 이는 발산급수 $1 + 2 + 3 + \cdots$의 "합"이 아니라 연장된 함수의 값이다.

5.4 명시적 공식과 Riemann 가설

von Mangoldt의 명시적 공식은 소수의 분포를 영점들로 정확히 표현한다(x가 소수의 거듭제곱이 아닐 때).

$$\psi(x) = x - \sum_{\rho} \frac{x^{\rho}}{\rho} - \log(2\pi) - \frac{1}{2}\log\!\left(1 - x^{-2}\right). \tag{5.1}$$

합은 비자명 영점 ρ에 대해 허수부의 절댓값 순서로 취한다. 각 영점 $\rho = \beta + i\gamma$는 크기 x^{β}인 진동을 기여하므로, 오차항의 크기는 영점의 실수부가 얼마나 큰지로 결정된다.

핵심 (Riemann 가설). 모든 비자명 영점은 직선 $\operatorname{Re} s = \tfrac{1}{2}$ 위에 있다.

Riemann 가설은 $\pi(x) = \operatorname{Li}(x) + O(\sqrt{x}\log x)$와 동치이다. 2026년 현재 미해결이며 Clay 수학연구소의 밀레니엄 문제 중 하나이다. 처음 10^{13}개 이상의 영점이 직선 위에 있음이 수치적으로 확인되었고, 영점의 양의 비율(40% 이상)이 직선 위에 있음이 증명되어 있다(Conrey). 영점이 없는 영역으로 현재 증명된 가장 좋은 것은 $\operatorname{Re} s = 1$ 근처의 좁은 영역(Vinogradov–Korobov 형태)이다.

5.5 등차수열의 소수

> **정리 5.3 (Dirichlet, 1837)** $\gcd(a, q) = 1$이면 $p \equiv a \pmod q$인 소수가 무한히 많다. 더 정확히 이런 소수들은 $\varphi(q)$개의 잉여류에 균등하게 분포한다: $\pi(x; q, a) \sim \dfrac{1}{\varphi(q)} \dfrac{x}{\log x}$.

증명은 Dirichlet 지표 $\chi : (\mathbb{Z}/q\mathbb{Z})^{\times} \to \mathbb{C}^{\times}$와 L-함수 $L(s, \chi) = \sum \chi(n) n^{-s}$를 쓰며, 핵심은 비자명 지표에 대해 $L(1, \chi) \neq 0$임을 보이는 것이다. 지표의 직교성으로 한 잉여류만 골라내는 방법은 유한 Fourier 분석이며, Dirichlet가 해석적 정수론을 창시한 결과이다. 제2장에서 $4k + 1$

꼴 소수의 무한성을 초등적으로 보였지만, 일반 등차수열에는 이런 초등적 증명이 알려진 경우가 제한적이다.

5.6 소수 사이의 간격

소수정리에 따르면 x 근처 소수 사이의 평균 간격은 $\log x$이다. 쌍둥이 소수 추측(간격 2인 소수쌍이 무한히 많다)은 미해결이지만, Zhang(2013)은 간격 7×10^7 이하인 소수쌍이 무한히 많음을 증명했고 Maynard–Tao의 방법과 Polymath 프로젝트로 그 상계가 246까지 줄었다. 반대로 Green–Tao 정리(2004)는 소수 집합이 임의의 길이의 등차수열을 포함함을 보였다. 이 결과들의 최근 상황은 제28권 제2장에서 다룬다.

5.7 연습문제와 해설

연습문제 5.4 $\zeta(2) = \pi^2/6$을 이용하여 $\sum_{n \text{ 홀수}} 1/n^2$을 구하라.

풀이. 짝수 항의 합은 $\sum_{n \ge 1} \frac{1}{(2n)^2} = \frac{1}{4}\zeta(2)$이므로 홀수 항의 합은 $\zeta(2) - \frac{1}{4}\zeta(2) = \frac{3}{4}\zeta(2) = \frac{3}{4}\cdot\frac{\pi^2}{6} = \frac{\pi^2}{8}$이다. 제13권의 $|x|$ Fourier 급수에서도 같은 값이 나온다.

연습문제 5.5 $\binom{2n}{n}$이 $n < p \le 2n$인 모든 소수 p로 나누어떨어지는 이유와, $\frac{2}{3}n < p \le n$인 소수($n \ge 3$)로는 나누어떨어지지 않는 이유를 설명하라.

풀이. 첫째: p는 분자 $(2n)!$에 정확히 한 번 나타나고($\lfloor 2n/p \rfloor = 1$, $n < p \le 2n$이므로 $p^2 > 2n$이기도 하다) 분모 $(n!)^2$에는 나타나지 않는다($p > n$). 둘째: $\frac{2}{3}n < p \le n$이면 $2p \le 2n < 3p$이고, $n \ge 3$에서 $p^2 > 2n$이므로 p의 더 높은 거듭제곱은 $(2n)!$에 나타나지 않는다. 따라서 p는 $(2n)!$에 정확히 두 번(p와 $2p$의 인수로), $(n!)^2$에도 정확히 두 번($n!$ 안의 p 한 번이 제곱되어) 나타나 지수가 0이 된다. Bertrand 가설의 Erdős 증명에서 쓰는 관찰이다.

연습문제 5.6 소수정리를 이용하여 n번째 소수 p_n이 $p_n \sim n \log n$임을 보여라.

풀이. $\pi(p_n) = n$이고 $\pi(x) \sim x/\log x$이므로 $n \sim p_n/\log p_n$이다. 양변에 로그를 취하면 $\log n \sim \log p_n - \log\log p_n \sim \log p_n$이고, 이를 원래 관계에 대입하면 $p_n \sim n \log p_n \sim n \log n$이다.

다음 연결. 정수의 성질을 더 큰 수 체계에서 보면 새로운 구조가 드러난다. 다음 장에서는 대수적 정수와 수체의 정수환을 다룬다.

제 6 장

대수적 정수와 수체의 정수환

개요 **대수적 정수**(*algebraic integer*)는 정수 $\mathbb{Z}$의 원소 개념을 유리수체의 유한 확대인 **수체**(*number field*)로 일반화한 것이다. 이 장은 대수적 정수의 정의와 그 전체가 환을 이룬다는 사실에서 출발하여, 이차체를 주된 예로 정수환 O_K의 구조를 노름·대각합·판별식으로 계산하는 방법을 정리하고, 정수환을 격자로 보는 기하적 관점과 단원군에 대한 Dirichlet 단원정리로 맺는다. 선행 지식: 제14권 제7장의 체의 확대와 최소다항식, 제14권 제6장의 가군과 PID.

6.1 대수적 정수

정의 6.1 복소수 α가 정수계수 모닉 다항식의 근이면 **대수적 정수**라 한다. 유리수체 위의 유한 확대 K(수체) 안의 대수적 정수 전체를 O_K로 쓴다.

α가 대수적 정수일 필요충분조건은 $\mathbb{Q}$ 위의 최소다항식의 계수가 모두 정수인 것이다(Gauss 보조정리에 근거한다: 유리수 계수 모닉 다항식이 정수계수 모닉 다항식을 나누면 그 계수도 정수이다). 유리수 중 대수적 정수는 정수뿐이다. 따라서 $O_{\mathbb{Q}} = \mathbb{Z}$이다.

정리 6.2 대수적 정수들의 합과 곱은 대수적 정수이다. 따라서 O_K는 환이다.

α가 대수적 정수일 필요충분조건은 $\mathbb{Z}[\alpha]$가 유한생성 $\mathbb{Z}$-가군인 것이다(제14권 제6장). $\mathbb{Z}[\alpha,\beta]$가 유한생성이면 그 원소 $\alpha+\beta$, $\alpha\beta$도 같은 성질을 가진다. 행렬식 기법(Cayley–Hamilton 정리: 곱셈 사상 $x \mapsto \alpha x$를 $\mathbb{Z}[\alpha,\beta]$ 위의 $\mathbb{Z}$-선형사상으로 보고 그 행렬의 특성다항식이 모닉 정수계수임을 이용)으로 증명한다.

6.2 이차체의 정수환

제곱인수가 없는 정수 $d \neq 0, 1$에 대해 $K = \mathbb{Q}(\sqrt{d})$의 원소 $\alpha = a + b\sqrt{d}$ $(a, b \in \mathbb{Q},\ b \neq 0)$의 최소다항식은 $x^2 - 2ax + (a^2 - db^2)$이다. 대수적 정수가 되려면 $2a \in \mathbb{Z}$, $a^2 - db^2 \in \mathbb{Z}$이어야 하고, 이를 정리하면

$$O_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \pmod 4, \\ \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right] & d \equiv 1 \pmod 4. \end{cases} \tag{6.1}$$

예를 들어 $\frac{1+\sqrt{5}}{2}$(황금비)는 $x^2 - x - 1$의 근이므로 대수적 정수이고, $\mathbb{Z}[\sqrt{5}]$는 $\mathbb{Q}(\sqrt{5})$의 정수환 전체가 아니다 ($5 \equiv 1 \pmod 4$이므로 식 (6.1)의 둘째 경우에 해당한다). $d = -1$이면 Gauss 정수 $\mathbb{Z}[i]$, $d = -3$이면 Eisenstein 정수 $\mathbb{Z}[\omega]$($\omega = \frac{-1+\sqrt{-3}}{2}$, $-3 \equiv 1 \pmod 4$이므로 둘째 경우)이다.

6.3 노름, 대각합, 판별식

$[K:\mathbb{Q}]=n$이면 K에서 $\mathbb{C}$로 가는 체 매장이 정확히 n개 있다($\sigma_1,\dots,\sigma_n$). 원소 $\alpha\in K$의 **노름**과 **대각합**을

$$N(\alpha)=\prod_{i}\sigma_i(\alpha),\qquad \mathrm{Tr}(\alpha)=\sum_{i}\sigma_i(\alpha) \tag{6.2}$$

로 정의한다. 이는 곱셈사상 $x\mapsto \alpha x$(K를 $\mathbb{Q}$ 위의 벡터공간으로 볼 때)의 행렬식과 대각합과 같다. $\alpha\in\mathcal{O}_K$이면 $N(\alpha),\mathrm{Tr}(\alpha)\in\mathbb{Z}$이고, α가 $\mathcal{O}_K$의 **단원**(*unit*)일 필요충분조건은 $N(\alpha)=\pm1$이다. 이차체에서 $N(a+b\sqrt{d})=a^2-db^2$이다.

$\mathcal{O}_K$는 계수 n인 자유 $\mathbb{Z}$-가군이며 그 기저를 **정수 기저**라 한다. 정수 기저 $\omega_1,\dots,\omega_n$의 **판별식** $d_K=\det(\sigma_i(\omega_j))^2$은 기저 선택과 무관한 정수이다. 이차체의 판별식은 $d\equiv 1\pmod 4$이면 d, 아니면 $4d$이다. 판별식은 다음 장에서 어떤 소수가 분기하는지를 결정한다.

6.4 단원과 Dirichlet 단원정리

> **정리 6.3 (Dirichlet 단원정리)** 수체 K가 실매장 r_1개와 복소매장 쌍 r_2개를 가지면($r_1+2r_2=n$) 단원군은
>
> $$\mathcal{O}_K^{\times}\cong \mu_K\times\mathbb{Z}^{r_1+r_2-1} \tag{6.3}$$
>
> 이다. 여기서 μ_K는 K에 속한 단위근들의 유한 순환군이다.

- 허이차체($d<0$): $r_1=0$, $r_2=1$이므로 $r_1+r_2-1=0$이고 단원군은 유한하다. $\mathbb{Z}[i]^\times=\{\pm1,\pm i\}$, $\mathbb{Z}[\omega]^\times$는 6개의 단위근, 나머지 $d<0$은 $\{\pm1\}$뿐이다.
- 실이차체($d>0$): $r_1=2, r_2=0$이므로 $r_1+r_2-1=1$이고 단원군은 $\{\pm1\}\times\mathbb{Z}$이다. 기본단원은 Pell 방정식 (제4장)의 기본해로 얻는다. $\mathbb{Q}(\sqrt{2})$의 기본단원은 $1+\sqrt{2}$(노름 -1)이다.

6.5 기하적 관점: 격자로서의 정수환

$\sigma=(\sigma_1,\dots,\sigma_{r_1},\mathrm{Re}\,\sigma_{r_1+1},\mathrm{Im}\,\sigma_{r_1+1},\dots)$로 K를 $\mathbb{R}^n$에 넣으면 $\mathcal{O}_K$는 격자가 되고 그 기본영역의 부피는 $2^{-r_2}\sqrt{|d_K|}$이다. Minkowski의 볼록체 정리(원점에 대칭인 볼록집합의 부피가 $2^n\cdot$(격자의 부피)보다 크면 원점이 아닌 격자점을 포함한다)를 이 격자에 적용하는 것이 기하적 수론이다. 다음 장의 이데알류군의 유한성과 단원정리가 모두 이 방법으로 증명된다. 또 $|d_K|>1$ ($K\neq\mathbb{Q}$)이라는 결과, 즉 $\mathbb{Q}$의 진확대에서는 어떤 소수가 반드시 분기한다는 결과도 같은 기하적 방법에서 나온다.

6.6 연습문제와 해설

> **연습문제 6.4** $\dfrac{1+\sqrt{-7}}{2}$가 대수적 정수인지 판정하라.

풀이. 최소다항식은 x^2-x+2이다(두 근의 합 1, 곱 $\frac{1+7}{4}=2$). 정수계수 모닉이므로 대수적 정수이다. $-7\equiv 1\pmod 4$인 경우의 정수환 공식과 일치한다.

연습문제 6.5 $\mathbb{Z}[\sqrt{-2}]$의 단원을 모두 구하라.

풀이. $N(a+b\sqrt{-2}) = a^2+2b^2 = 1$의 정수해는 $(\pm 1, 0)$뿐이므로 단원은 ± 1이다.

연습문제 6.6 $\mathbb{Q}(\sqrt{3})$에서 $2+\sqrt{3}$이 단원임을 보이고 그 역원을 구하라.

풀이. $N(2+\sqrt{3}) = 4-3 = 1$이므로 단원이고 역원은 켤레 $2-\sqrt{3}$이다. $x^2-3y^2=1$의 기본해 $(2,1)$(제4장)에 대응하는 기본단원이다(노름 -1인 단원은 없다).

다음 연결. $\mathbb{Z}[\sqrt{-5}]$에서 보았듯이 정수환에서 원소의 인수분해는 유일하지 않을 수 있다. 다음 장에서는 원소 대신 아이디얼을 분해하여 유일성을 되찾는 Dedekind의 이론과 이데알류군을 다룬다.

제 7 장

Dedekind 정역, 아이디얼 분해, 이데알류군

개요 수체의 정수환에서는 원소의 인수분해가 유일하지 않을 수 있지만, 아이디얼의 수준에서는 유일한 분해가 항상 성립한다. 이 장은 **Dedekind 정역**을 정의하고 그 안에서 영이 아닌 아이디얼이 소 아이디얼들의 곱으로 유일하게 분해됨을 정리한 뒤, 유리수 소수가 정수환에서 어떻게 분해되는지(분해·관성·분기)를 다루고, 원소의 유일인수분해가 얼마나 실패하는지를 재는 **이데알류군**을 정의한다. 선행 지식: 제6장의 정수환과 노름, 제14권 제4장의 아이디얼과 몫환, 제14권 제5장의 PID와 UFD.

7.1 Dedekind 정역

정의 7.1 Noether 정역 D가 정수적으로 닫혀 있고(분수체의 원소 중 D 위에서 정수인 것은 D에 속함) 0이 아닌 모든 소 아이디얼이 극대 아이디얼이면 **Dedekind 정역**이라 한다.

수체의 정수환 $\mathcal{O}_K$는 Dedekind 정역이다. PID도 Dedekind 정역이다. 그러나 $\mathbb{Z}[\sqrt{-3}]$은 정수적으로 닫혀 있지 않으므로($\omega = \frac{-1+\sqrt{-3}}{2}$를 포함하지 않음) Dedekind 정역이 아니다.

정리 7.2 (아이디얼의 유일 분해) Dedekind 정역에서 0이 아닌 진아이디얼은 소 아이디얼들의 곱으로 순서를 제외하고 유일하게 분해된다.

아이디얼의 곱은 $IJ = \{\sum a_i b_i : a_i \in I, b_i \in J\}$이다. 증명의 핵심은 분수 아이디얼들이 곱셈에 대해 군을 이룬다는 것, 즉 모든 0이 아닌 아이디얼이 역을 갖는다는 것이다. 아이디얼에서는 "나눈다"와 "포함된다"가 같다($I \mid J \iff J \subseteq I$).

예제 7.3 ($\mathbb{Z}[\sqrt{-5}]$에서 6의 분해) $\mathfrak{p}_2 = (2, 1+\sqrt{-5})$, $\mathfrak{p}_3 = (3, 1+\sqrt{-5})$, $\mathfrak{p}_3' = (3, 1-\sqrt{-5})$로 두면

$$(2) = \mathfrak{p}_2^2, \qquad (3) = \mathfrak{p}_3\mathfrak{p}_3', \qquad (1+\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_3, \qquad (1-\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_3' \tag{7.1}$$

이다. 따라서 $(6) = \mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}_3'$로 유일하게 분해되고, 원소의 두 분해 $2\cdot 3$과 $(1+\sqrt{-5})(1-\sqrt{-5})$는 같은 소 아이디얼들을 다르게 묶은 것이다. $\mathfrak{p}_2$는 주아이디얼이 아니다(노름 2인 원소가 없다: $a^2+5b^2=2$는 정수해가 없다).

7.2 소수의 분해

유리수 소수 p가 생성하는 아이디얼 $p\mathcal{O}_K$는 $\mathcal{O}_K$에서 $\prod \mathfrak{p}_i^{e_i}$로 분해되고, $\mathcal{O}_K/\mathfrak{p}_i$는 원소 p^{f_i}개인 유한체이며 $\sum e_i f_i = n = [K:\mathbb{Q}]$이다. $e_i > 1$인 경우를 **분기** (*ramification*)라 한다. 이차체($n=2$)에서는 세 가지 경우뿐이다.

- **분해**(*split*): $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$ ($\mathfrak{p} \neq \mathfrak{p}'$).
- **관성**(*inert*): $p\mathcal{O}_K$가 소 아이디얼 그대로($f = 2$).

- **분기**: $pO_K = \mathfrak{p}^2$.

홀수 소수 $p \nmid d$에 대해 p가 $\mathbb{Q}(\sqrt{d})$에서 분해될 필요충분조건은 $\left(\frac{d}{p}\right) = 1$이고, 관성이면 $\left(\frac{d}{p}\right) = -1$이다. 분기하는 소수는 정확히 판별식 d_K를 나누는 소수이다. 제2장의 Legendre 기호가 소수의 분해 법칙이 되며, 이차상호법칙은 분해 법칙이 p의 법 $|d_K|$ 잉여류로만 결정된다는 문장으로 바뀐다. 이 관찰의 일반화가 유체론이다.

> **예제 7.4** $\mathbb{Z}[i]$$(d_K = -4)$에서 $2 = -i(1+i)^2$로 분기, $p \equiv 1 \pmod 4$이면 $p = (a+bi)(a-bi)$로 분해, $p \equiv 3 \pmod 4$이면 관성이다. 제2장의 두 제곱수 정리가 분해 법칙의 한 예이다.

7.3 이데알류군과 유수

분수 아이디얼들의 군을 주 분수 아이디얼들의 부분군으로 나눈 몫을 **이데알류군** $\mathrm{Cl}(K)$라 하고, 그 위수를 **유수** h_K라 한다.

> **정리 7.5** 이데알류군은 유한군이다. 또한 각 아이디얼류는 노름이 **Minkowski 상수**
>
> $$M_K = \sqrt{|d_K|}\left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n} \tag{7.2}$$
>
> 이하인 아이디얼을 포함한다.

$h_K = 1$일 필요충분조건은 O_K가 PID, 동치로 UFD인 것이다(Dedekind 정역에서는 PID와 UFD가 같은 조건이다). 이데알류군은 유일인수분해가 실패하는 정도를 측정한다.

> **예제 7.6** ($\mathbb{Q}(\sqrt{-5})$**의 유수**) $d_K = -20$, $n = 2$, $r_2 = 1$이므로 $M_K = \sqrt{20}\cdot\frac{4}{\pi}\cdot\frac{2}{4} \approx 2.85$이다. 노름 2 이하의 아이디얼만 보면 되고, 그것은 (1)과 $\mathfrak{p}_2$이다. $\mathfrak{p}_2$는 주아이디얼이 아니고 $\mathfrak{p}_2^2 = (2)$는 주아이디얼이므로 $h_K = 2$이다.

허이차체 중 유수가 1인 것은 정확히 $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$의 아홉 개이다(Baker, Heegner, Stark). $e^{\pi\sqrt{163}} = 262537412640768743.99999999999925\ldots$가 거의 정수인 현상이 $d = -163$의 유수 1과 관련된다. 실이차체 중 유수 1인 것이 무한히 많은지는 미해결이다(Gauss 추측).

7.4 Fermat의 마지막 정리와 이데알 이론의 탄생

$x^p + y^p = z^p$을 원분체 $\mathbb{Q}(\zeta_p)$에서 $\prod_{k}(x + \zeta_p^k y) = z^p$로 분해하는 접근은 $\mathbb{Z}[\zeta_p]$가 UFD라면 성공한다. 그러나 $p = 23$부터 UFD가 아니다. Kummer는 이상수(ideal number)를 도입하여 p가 $\mathbb{Q}(\zeta_p)$의 유수를 나누지 않는 소수(정칙 소수)에 대해 정리를 증명했고, 이것이 Dedekind의 아이디얼 이론으로 이어졌다. 정리의 완전한 증명은 Wiles(1995, Taylor–Wiles의 보완)가 타원곡선과 모듈러 형식의 대응으로 완성했다. 이 증명을 증명 보조기로 형식화하는 작업의 현황은 제28권에서 다룬다.

7.5 연습문제와 해설

연습문제 7.7 $\mathbb{Z}[i]$에서 5와 13의 소인수분해를 구하라.

풀이. $5 = (2+i)(2-i)$, $13 = (3+2i)(3-2i)$이다. 두 수 모두 $1 \pmod 4$이므로 분해된다. 인수들은 노름이 소수이므로 기약원이다.

연습문제 7.8 $\mathbb{Q}(\sqrt{-5})$에서 7이 분해되는지 판정하고, 분해된다면 소 아이디얼을 써라.

풀이. $\left(\frac{-5}{7}\right) = \left(\frac{2}{7}\right) = 1$ ($7 \equiv -1 \pmod 8$)이므로 분해된다. $x^2 \equiv -5 \equiv 2 \pmod 7$의 해는 $x \equiv \pm 3$이므로 $(7) = (7, 3+\sqrt{-5})(7, 3-\sqrt{-5})$이다. 노름 7인 원소가 없으므로($a^2+5b^2 = 7$의 해 없음) 두 인수는 주아이디얼이 아니다.

연습문제 7.9 $\mathbb{Q}(\sqrt{-3})$에서 Minkowski 상수를 계산하여 유수가 1임을 보여라.

풀이. $d_K = -3$이므로 $M_K = \sqrt{3} \cdot \frac{4}{\pi} \cdot \frac{1}{2} \approx 1.10 < 2$이다. 노름 1인 아이디얼은 (1)뿐이므로 모든 아이디얼류가 자명하고 $h_K = 1$이다.

다음 연결. 소수 p에서의 분해는 "p 근처"만 보는 국소적 정보이다. 마지막 장에서는 그 국소적 정보를 완비화한 p진수와, 국소적 해에서 대역적 해를 얻는 원리를 다룬다.

제 8 장

p 진수와 국소–대역 원리

개요 p 진수는 소수 p에 대한 모든 법 $(\bmod p, p^2, p^3, \dots)$의 합동 정보를 하나의 체 $\mathbb{Q}_p$로 묶은 것이다. 이 장은 p진 절댓값과 그로부터 얻는 비아르키메데스적 거리를 정의하고, 완비화 $\mathbb{Q}_p$와 그 안의 정수환 $\mathbb{Z}_p$의 구조, 법 p의 단순근을 끌어올리는 Hensel 보조정리, 절댓값을 분류하는 Ostrowski 정리를 차례로 다룬 뒤, 방정식의 해가 "모든 국소체에서" 존재하는 것과 "$\mathbb{Q}$에서" 존재하는 것이 언제 같은지를 다루는 국소–대역 원리(Hasse–Minkowski 정리)로 맺는다. 선행 지식: 제1장의 합동식, 제2장의 이차잉여, 제6장의 이차체, 제10권 제1장의 거리공간과 완비성.

정수 방정식에 해가 있는지 판정할 때 가장 먼저 하는 일은 법 $p, p^2, \dots$ 에서 해가 있는지와 실수 해가 있는지를 확인하는 것이다. 어느 하나라도 실패하면 정수해는 없다. 법 p^k $(k = 1, 2, \dots)$의 해들이 서로 호환되도록 고른 정보를 하나의 수로 보면 p진 정수가 된다. 이 관점은 대수적 정수론 전체의 기본 언어이다.

8.1 p진 절댓값은 큰 거듭제곱을 작게 잰다

정의 8.1 소수 p와 0이 아닌 유리수 x를 $x = p^v a/b$ $(a, b \in \mathbb{Z},\ p \nmid ab)$로 쓸 때 $v_p(x) = v$를 p**진 지수**라 하고, $|x|_p = p^{-v_p(x)}$, $|0|_p = 0$으로 정의한다. 보통의 절댓값은 $|\cdot|_\infty$로 쓴다.

$v_p(xy) = v_p(x) + v_p(y)$이므로 $|xy|_p = |x|_p\,|y|_p$이다. 예를 들어 $|12|_2 = 1/4$, $|12|_3 = 1/3$, $|12|_5 = 1$, $|5^n|_5 = 5^{-n} \to 0$이다. p진 거리에서는 p로 많이 나누어지는 수가 작다.

명제 8.2 (강삼각부등식) 모든 $x, y \in \mathbb{Q}$에 대해 $|x+y|_p \le \max(|x|_p, |y|_p)$이다. 특히 $|x|_p \neq |y|_p$이면 등호 $|x+y|_p = \max(|x|_p, |y|_p)$가 성립한다.

증명. $x, y \neq 0, x+y \neq 0$이라 하고 $v_p(x) \le v_p(y)$라 하자. $x = p^{v_p(x)} a/b$, $y = p^{v_p(x)} c/d$ $(p \nmid bd)$로 쓰면 $x + y = p^{v_p(x)}(ad + bc)/(bd)$이므로 $v_p(x+y) \ge v_p(x)$이다. $v_p(x) < v_p(y)$이면 $p \mid c$이고 $p \nmid ad$이므로 $p \nmid ad + bc$, 따라서 $v_p(x+y) = v_p(x)$이다. □

이런 절댓값을 **비아르키메데스적**(*non-archimedean*)이라 한다. 둘째 문장은 "모든 삼각형이 이등변"이라는 뜻이다. 또한 급수 $\sum x_k$가 p진 거리에서 수렴할 필요충분조건은 $|x_k|_p \to 0$이다(완비성 아래에서). 실수에서는 $\sum 1/k$처럼 항이 0으로 가도 발산할 수 있으므로 이 판정은 p진 세계에만 있는 단순함이다.

흔한 오류. $|x|_p$를 "p진법으로 쓴 수의 크기"로 생각하면 안 된다. $|1000|_5 = |5^3 \cdot 8|_5 = 1/125$이고 $|1/1000|_5 = 125$이다. 크기는 자릿수가 아니라 p로 나누어지는 횟수로 정해진다.

8.2 $\mathbb{Q}_p$와 $\mathbb{Z}_p$: 완비화와 p진 전개

$\mathbb{Q}$를 $|\cdot|_p$에 대해 완비화한 체를 $\mathbb{Q}_p$라 한다. 즉 p진 Cauchy 수열의 동치류들로 $\mathbb{Q}_p$를 만들고, 절댓값과 사칙연산을 극한으로 확장한다(제10권 제1장의 실수 구성과 같은 방법이다). $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \le 1\}$은 강삼각부등식에 의해 덧셈과 곱셈에 닫힌 환이며 **p진 정수환**이라 한다.

명제 8.3

(1) $\mathbb{Z}_p^\times = \{x : |x|_p = 1\}$이고, 0이 아닌 모든 $x \in \mathbb{Q}_p$는 $x = p^n u$ $(n \in \mathbb{Z},\, u \in \mathbb{Z}_p^\times)$로 유일하게 쓸 수 있다.

(2) 모든 $x \in \mathbb{Z}_p$는 $x = \sum_{k \ge 0} a_k p^k$, $a_k \in \{0, 1, \dots, p-1\}$로 유일하게 전개된다.

(3) 절단 사상은 동형 $\mathbb{Z}_p / p^k\mathbb{Z}_p \cong \mathbb{Z}/p^k\mathbb{Z}$를 준다. 특히 $\mathbb{Z}$는 $\mathbb{Z}_p$에서 조밀하다.

증명 개요. (1) $|x|_p = 1$이면 $|x^{-1}|_p = 1$이므로 $x^{-1} \in \mathbb{Z}_p$이다. $|x|_p = p^{-n}$이면 $u = p^{-n}x$의 절댓값이 1이다. (2) $x \in \mathbb{Z}_p$에 대해 $|x - m|_p < 1$인 정수 m을 고르고($\mathbb{Z}$의 조밀성, $\mathbb{Q}$에서 분모가 p와 서로소인 수는 법 p에서 정수와 합동) $a_0 \equiv m \pmod p$를 $0 \le a_0 < p$로 정한다. $(x - a_0)/p \in \mathbb{Z}_p$에 같은 과정을 반복한다. 항 $a_k p^k$의 절댓값이 0으로 가므로 급수가 x로 수렴한다. 유일성은 법 p^k에서 자릿수를 차례로 비교하면 된다. (3) $\sum a_k p^k \mapsto \sum_{k<n} a_k p^k \bmod p^n$이 전사 준동형이고 핵이 $p^n\mathbb{Z}_p$이다. $\square$

예제 8.4 (-1과 $1/3$의 전개) $\mathbb{Z}_p$에서

$$-1 = \sum_{k \ge 0} (p-1) p^k \tag{8.1}$$

이다. $(p-1)\sum_{k<n} p^k = p^n - 1 \equiv -1 \pmod{p^n}$이기 때문이다. $\mathbb{Z}_2$에서 $1/3$은 자릿수 $1, 1, 0, 1, 0, 1, 0, \dots$를 가진다. 즉

$$\frac{1}{3} = 1 + 2 + 2^3 + 2^5 + 2^7 + \cdots. \tag{8.2}$$

검산: $3 \cdot (1 + 2 + 2^3 + \cdots + 2^{2m+1}) = 1 + 2^{2m+3} \equiv 1 \pmod{2^{2m+3}}$이다.

$\mathbb{Z}_p$는 법 p^k의 정보를 모든 k에 대해 동시에 기억하는 대상이다. 방정식 $f(x) = 0$ $(f \in \mathbb{Z}[x])$이 $\mathbb{Z}_p$에서 해를 가지면 모든 k에 대해 $f(x) \equiv 0 \pmod{p^k}$가 풀린다. 역도 성립한다($\mathbb{Z}_p$의 콤팩트성). $\mathbb{Z}_p$는 p진 거리에서 콤팩트하며(완비이고 전체유계), 실수의 $[0,1]$과 같은 역할을 한다.

8.3 Hensel 보조정리: 법 p의 단순근은 끌어올려진다

정리 8.5 (**Hensel 보조정리**) $f \in \mathbb{Z}_p[x]$이고 $a \in \mathbb{Z}_p$가 $f(a) \equiv 0 \pmod p$, $f'(a) \not\equiv 0 \pmod p$를 만족하면 $\alpha \equiv a \pmod p$이고 $f(\alpha) = 0$인 $\alpha \in \mathbb{Z}_p$가 유일하게 존재한다.

증명. 다항식의 Taylor 전개 $f(x+h) = f(x) + f'(x)h + h^2 g(x,h)$에서 g는 $\mathbb{Z}_p$ 계수 다항식이다. $a_0 = a$에서 Newton 반복 $a_{n+1} = a_n - f(a_n)/f'(a_n)$을 정의한다. 귀납 가정을 $f(a_n) \equiv 0 \pmod{p^{2^n}}$, $a_n \equiv a \pmod p$로 두면 $f'(a_n) \equiv f'(a) \not\equiv 0 \pmod p$이므로 $f'(a_n) \in \mathbb{Z}_p^\times$이고

$h_n = -f(a_n)/f'(a_n)$은 p^{2^n}의 배수이다. 그러면

$$f(a_{n+1}) = f(a_n) + f'(a_n)h_n + h_n^2 g(a_n, h_n) = h_n^2 g(a_n, h_n) \equiv 0 \pmod{p^{2^{n+1}}}.$$

$|a_{n+1} - a_n|_p = |h_n|_p \le p^{-2^n} \to 0$이므로 (a_n)은 Cauchy 수열이고 극한 α에서 $f(\alpha) = 0$이다. 유일성: $\beta \equiv a$도 근이면 $0 = f(\beta) - f(\alpha) = (\beta - \alpha)\big(f'(\alpha) + (\beta-\alpha)g(\alpha,\beta-\alpha)\big)$이고 둘째 인수는 단원이므로 $\beta = \alpha$이다. □

Newton 방법이 실수에서는 초기값이 가까워야 수렴하지만, 여기서는 "$f'(a)$가 단원"이라는 한 조건이 수렴을 보장한다. 더 일반적으로 $|f(a)|_p < |f'(a)|_p^2$이면 $|\alpha - a|_p < |f'(a)|_p$인 근이 유일하게 존재한다(같은 증명).

> **예제 8.6** ($\sqrt{2} \in \mathbb{Q}_7$, $\sqrt{-1} \in \mathbb{Q}_5$) $f(x) = x^2 - 2$, $a = 3$이면 $f(3) = 7 \equiv 0$, $f'(3) = 6 \not\equiv 0 \pmod 7$이므로 $\mathbb{Q}_7$에 $\sqrt{2}$가 있고 $\sqrt{2} \equiv 3 \pmod 7$이다. 법 49로 올리면 $(3+7t)^2 \equiv 9 + 42t \equiv 2 \pmod{49}$에서 $6t \equiv -1 \pmod 7$, $t = 1$이므로 $\sqrt{2} \equiv 10 \pmod{49}$이다 ($10^2 = 100 = 2\cdot 49 + 2$). 마찬가지로 $x^2 + 1$은 $a = 2$에서 법 5의 단순근을 가지므로 $\sqrt{-1} \in \mathbb{Q}_5$이고 $\sqrt{-1} \equiv 2 \pmod 5$, $\equiv 7 \pmod{25}$이다($7^2 + 1 = 50$).

> **예제 8.7** (2는 $\mathbb{Q}_3$의 제곱수가 아니다) $x^2 = 2$인 $x \in \mathbb{Q}_3$이 있으면 $2v_3(x) = v_3(2) = 0$이므로 $x \in \mathbb{Z}_3^\times$이고 $x^2 \equiv 2 \pmod 3$이다. 그러나 법 3의 제곱은 $0, 1$뿐이다. 따라서 $\mathbb{Q}_3$에는 $\sqrt{2}$가 없다. 실수에서는 $\sqrt{2}$가 있으므로 "어느 체에서 푸는가"가 답을 바꾼다.

> **명제 8.8** ($\mathbb{Q}_p^\times$의 제곱 판정) p가 홀수 소수이면 $x = p^n u \in \mathbb{Q}_p^\times$ ($u \in \mathbb{Z}_p^\times$)가 제곱수일 필요충분조건은 n이 짝수이고 $u \bmod p$가 이차잉여인 것이다. $p = 2$이면 $u \in \mathbb{Z}_2^\times$가 제곱수일 필요충분조건은 $u \equiv 1 \pmod 8$이다.

증명. 홀수 p: 필요성은 위 예제와 같은 계산이다. 충분성은 $x^2 - u$에 Hensel 보조정리를 쓰면 된다 ($f'(a) = 2a$가 단원). $p = 2$: 홀수의 제곱은 법 8로 1이므로 필요하다. 역으로 $u \equiv 1 \pmod 8$이면 $f(x) = x^2 - u$, $a = 1$에서 $|f(1)|_2 \le 2^{-3} < |f'(1)|_2^2 = 2^{-2}$이므로 일반형 Hensel 보조정리로 근이 있다. □

주의. 법 p에서 풀린다고 p진 해가 있는 것은 아니다. $x^2 \equiv 3 \pmod 2$는 $x = 1$로 풀리지만 $3 \not\equiv 1 \pmod 8$이므로 $\mathbb{Q}_2$에 $\sqrt{3}$은 없다(이미 법 4에서 $x^2 \equiv 3$이 불가능하다). Hensel 보조정리의 조건 $f'(a) \not\equiv 0 \pmod p$가 깨지는 경우 ($p = 2$의 제곱근, 중근)에는 더 높은 법까지 확인해야 한다.

8.4 Ostrowski 정리와 곱 공식

$\mathbb{Q}$ 위의 절댓값(곱셈적, 삼각부등식, $|x| = 0 \iff x = 0$)은 $|\cdot|_\infty$와 $|\cdot|_p$ 말고도 이들의 거듭제곱 $|\cdot|^c$ ($0 < c \le 1$) 등이 있지만, 위상까지 같으면 같은 것으로 본다.

> **정리 8.9 (Ostrowski)** $\mathbb{Q}$ 위의 자명하지 않은 절댓값은 $|\cdot|_\infty$ 또는 어떤 소수 p에 대한 $|\cdot|_p$와 동치이다. 즉 어떤 $c > 0$에 대해 $|\cdot| = |\cdot|_v^c$ 꼴이다.

증명은 정수 n의 절댓값이 1보다 큰 경우(아르키메데스적)와 모든 정수에서 1 이하인 경우로 나누어 진행하며, F. Q. Gouvêa, *p-adic Numbers*에 표준적인 증명이 있다. 따라서 $\mathbb{Q}$의 완비화는 $\mathbb{R}$과 $\mathbb{Q}_p$ 들뿐이다. 이들을 묶어 $\mathbb{Q}$의 "자리" (*place*) $v \in \{\infty, 2, 3, 5, \dots\}$라 부른다.

명제 8.10 (곱 공식) $x \in \mathbb{Q}^\times$이면 $\prod_{v} |x|_v = |x|_\infty \prod_{p} |x|_p = 1$이다(유한 개를 제외한 모든 인수는 1이다).

증명. $x = \pm \prod_p p^{v_p(x)}$이면 $|x|_\infty = \prod_p p^{v_p(x)}$이고 $|x|_p = p^{-v_p(x)}$이다. 곱하면 1이다. □

예를 들어 $x = -12/35$에 대해 $|x|_\infty = 12/35$, $|x|_2 = 1/4$, $|x|_3 = 1/3$, $|x|_5 = 5$, $|x|_7 = 7$이고 곱은 1이다. 곱 공식은 "0이 아닌 유리수는 모든 자리에서 동시에 작을 수 없다"는 뜻이며, 이 장의 마지막 절과 해석적 정수론(제28권 제2장)에서 반복된다.

8.5 이차형식의 Hasse–Minkowski 정리

정리 8.11 (Hasse–Minkowski) $\mathbb{Q}$ 계수의 비퇴화 이차형식 $Q(x_1, \dots, x_n)$이 $\mathbb{Q}^n$에서 자명하지 않은 영점을 가질 필요충분조건은 $\mathbb{R}^n$과 모든 소수 p에 대한 $\mathbb{Q}_p^n$에서 자명하지 않은 영점을 가지는 것이다.

증명은 J.-P. Serre, *A Course in Arithmetic*에 있다. 대각형식 $\sum a_i x_i^2$ ($a_i \in \mathbb{Z}$, $n \ge 3$)에서는 $p \nmid 2a_1 \cdots a_n$인 p에 대해 $\mathbb{Q}_p$ 조건이 자동으로 성립하므로(법 p의 해가 Chevalley–Warning 정리로 존재하고 Hensel 보조정리로 올라간다) 실제로 확인할 자리는 유한 개이다.

예제 8.12 ($x^2+y^2=3z^2$에는 유리해가 없다) 자명하지 않은 해가 있으면 서로소 정수해 (x, y, z)가 있다. 법 3에서 $x^2 + y^2 \equiv 0$인데 -1은 법 3의 이차잉여가 아니므로 $3 \mid x$, $3 \mid y$이다. 그러면 $9 \mid 3z^2$, $3 \mid z$가 되어 서로소 조건에 모순이다. 같은 논증은 $\mathbb{Q}_3$에서 v_3을 쓰면 그대로 성립하므로 $\mathbb{Q}_3$에도 해가 없다. 실수 해는 있으므로 장애는 자리 3에서 온다. 반면 $x^2 + y^2 = 5z^2$은 $(1, 2, 1)$, $x^2 + y^2 = 2z^2$은 $(1, 1, 1)$을 해로 가진다.

따름정리 8.13 (Meyer) $n \ge 5$인 부정부호(*indefinite*) 비퇴화 유리 이차형식은 자명하지 않은 유리 영점을 가진다.

이는 $n \ge 5$인 모든 비퇴화 형식이 모든 $\mathbb{Q}_p$에서 영점을 가진다는 국소적 사실과 부정부호 조건(실수 영점)에 Hasse–Minkowski 정리를 적용한 결과이다. 양의 정부호 형식 $x_1^2 + \cdots + x_5^2$는 실수 영점이 없으므로 제외된다.

8.6 국소–대역 원리가 실패하는 경우

Hasse–Minkowski 정리는 이차형식에 대한 정리이다. 차수가 높거나 방정식이 여러 개이면 "모든 자리에서 풀리지만 $\mathbb{Q}$에서는 풀리지 않는" 경우가 생긴다.

예제 8.14 (모든 자리에서 근이 있는 다항식) $f(x) = (x^2 - 2)(x^2 - 17)(x^2 - 34)$는 $\mathbb{Q}$에서 근이 없다($\sqrt{2}, \sqrt{17}, \sqrt{34}$는 무리수). 그러나 $\mathbb{R}$과 모든 $\mathbb{Q}_p$에서 근이 있다.

- $\mathbb{R}$: $\sqrt{2}$.
- $p = 2$: $17 \equiv 1 \pmod 8$이므로 17은 $\mathbb{Q}_2$의 제곱수이다.
- $p = 17$: $6^2 = 36 \equiv 2 \pmod{17}$이므로 Hensel 보조정리로 $\sqrt{2} \in \mathbb{Q}_{17}$이다.

- 그 밖의 홀수 소수 p: Legendre 기호의 곱셈성으로 $\left(\frac{34}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{17}{p}\right)$이므로 셋 중 적어도 하나는 $+1$이고, 그 수의 제곱근이 Hensel 보조정리로 $\mathbb{Q}_p$에 있다.

이보다 깊은 예로 Selmer의 3차 곡선 $3x^3+4y^3+5z^3=0$은 $\mathbb{R}$과 모든 $\mathbb{Q}_p$에서 자명하지 않은 해를 가지지만 $\mathbb{Q}$에서는 자명하지 않은 해가 없다. 이 사실의 증명은 이 권의 범위를 넘으며, 타원곡선의 Selmer 군과 Tate–Shafarevich 군이 이러한 실패를 측정한다. 국소 정보는 필요조건을 빠짐없이 주지만, 충분조건이 되는지는 대상의 종류에 따라 다르다.

8.7 연습문제와 해설

연습문제 8.15 $x = 360/7$에 대해 $|x|_v$ $(v = \infty, 2, 3, 5, 7)$를 구하고 곱 공식을 확인하라.

풀이. $360 = 2^3 \cdot 3^2 \cdot 5$이므로 $|x|_2 = 1/8$, $|x|_3 = 1/9$, $|x|_5 = 1/5$, $|x|_7 = 7$, $|x|_\infty = 360/7$이다. 곱은 $\frac{360}{7} \cdot \frac{1}{360} \cdot 7 = 1$이고 나머지 소수에서는 1이다.

연습문제 8.16 $\mathbb{Z}_5$에서 $-1/4$의 5진 전개를 구하라.

풀이. $|5|_5 < 1$이므로 등비급수 $\sum_{k\ge 0} 5^k$는 $\mathbb{Z}_5$에서 $1/(1-5) = -1/4$로 수렴한다. 따라서 $-1/4 = 1+5+5^2+\cdots$ 이고 모든 자릿수가 1이다. 검산: $4(1+5+\cdots+5^{n-1}) = 5^n - 1 \equiv -1 \pmod{5^n}$이다.

연습문제 8.17 $\mathbb{Q}_3$에 $\sqrt{7}$이 있는지 판정하고, 있다면 법 9에서의 값을 구하라.

풀이. $7 \equiv 1 \pmod 3$은 이차잉여이고 $f(x) = x^2 - 7$, $a = 1$에서 $f'(1) = 2 \not\equiv 0 \pmod 3$이므로 Hensel 보조정리로 존재한다. $(1+3t)^2 \equiv 1 + 6t \equiv 7 \pmod 9$에서 $t \equiv 1 \pmod 3$이므로 $\sqrt{7} \equiv 4 \pmod 9$이다$(16 \equiv 7)$. 다른 근은 $-4 \equiv 5 \pmod 9$이다.

연습문제 8.18 $x^2 + y^2 + z^2 = 7w^2$이 자명하지 않은 유리해를 갖지 않음을 보여라.

풀이. 서로소 정수해 (x, y, z, w)가 있다고 하자. 제곱수는 법 8로 $0, 1, 4$이다. w가 홀수이면 우변은 $7 \pmod 8$인데 $\{0, 1, 4\}$의 세 원소의 합은 7이 될 수 없다. w가 짝수이면 $x^2 + y^2 + z^2 \equiv 0 \pmod 4$이고, 법 4의 제곱은 $0, 1$이므로 x, y, z가 모두 짝수이다. 그러면 네 수가 모두 짝수가 되어 모순이다. 장애는 자리 2에서 온다($\mathbb{Q}_2$에서 같은 논증이 성립한다).

연습문제 8.19 $f(x) = x^2 - 17$과 $a = 1$에 기본형 Hensel 보조정리를 쓸 수 없는 이유와, 그럼에도 $\mathbb{Q}_2$에 $\sqrt{17}$이 있는 이유를 설명하라.

풀이. $f'(1) = 2 \equiv 0 \pmod 2$이므로 기본형의 조건이 깨진다. 그러나 $|f(1)|_2 = |-16|_2 = 2^{-4} < |f'(1)|_2^2 = 2^{-2}$이므로 일반형 Hensel 보조정리가 적용되어 $|\alpha - 1|_2 < 1/2$인 근이 있다. 이는 $17 \equiv 1 \pmod 8$이라는 제곱 판정과 일치한다.

다음 연결. $\mathbb{Q}_p$들과 $\mathbb{R}$을 한꺼번에 다루는 아델환, 이차형식의 국소 불변량(Hilbert 기호), 타원곡선의 Selmer 군은 이 장의 언어를 그대로 확장한다. 대수기하의 관점은 제18권, 현대 정수론의 대응 이론은 제28권 제3장에서 이어진다.

제15권의 범위와 다음 읽기

이 권은 합동과 원시근, 이차잉여와 이차상호법칙, 산술함수와 Möbius 반전, 연분수와 Pell 방정식, 소수의 분포와 zeta 함수, 대수적 정수와 수체의 정수환, Dedekind 정역과 이데알류군, p 진수와 국소–대역 원리를 다루었다. 제1권의 나눗셈·합동 계산에서 출발하여 현대 정수론의 기본 대상까지 이어지도록 구성했다.

다음 읽기로는 군·환·체와 Galois 이론(제14권)으로 대수적 배경을 보강하고, 대수기하(제18권)에서 방정식의 해집합을 기하적으로 다루며, 소수 분포와 Langlands 대응의 현재 연구 지도는 제28권에서 확인할 수 있다. 표준 참고서로 K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*; I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*; D. A. Marcus, *Number Fields*; J.-P. Serre, *A Course in Arithmetic*가 있다.

참고자료의 사용방식. 본문의 설명과 문제는 이 참고서를 위해 새로 작성했다. 아래 링크는 관련 주제를 더 넓은 교재와 대조해 읽기 위한 안내이며, 이 원고 전체가 해당 기관이나 저자의 검토를 받았다는 뜻은 아니다. 개별 정리의 정확한 가정과 기호 약속이 다를 수 있으므로 독자는 자료를 바꿀 때 정의를 확인해야 한다.

- MIT OpenCourseWare, *18.781 Theory of Numbers*: 합동, 이차상호법칙, 연분수, 이차형식의 강의와 문제.
- American Institute of Mathematics, *Open Textbook Initiative*: 정수론을 포함한 공개 교재 목록.

제 19 권

조합론 · 그래프 · 이산수학

제19권은 유한한 대상의 개수와 이산적 구조를 다루는 조합론과 그래프 이론이다. 제1–3장은 세는 대상의 정확한 정의와 일대일 대응, 포함배제 원리와 대칭을 가진 계수, 점화식과 생성함수를 다룬다. 제4–6장은 그래프의 연결 · 나무 · 순회, 이분 그래프와 색칠과 평면성, 매칭과 네트워크 흐름을 다루며, 그래프 위의 최적화 문제로 이어지는 결과를 증명한다.

제 1 장

세는 대상과 일대일 대응

개요 조합론(*combinatorics*)은 유한하거나 가산적인 대상의 개수를 세는 수학 분야이다. 이 장은 센다는 것이 무엇을 뜻하는지, 곧 세려는 대상의 집합을 정확히 정의하고 그 집합과 이미 개수를 아는 집합 사이에 일대일 대응(*bijection*)을 세우는 절차로 조합론의 계산을 정당화하는 데서 출발한다. 합의 법칙과 곱의 법칙으로 기본적인 선택의 개수를 세고, 순서를 두거나 잊는 선택인 순열과 조합, 반복을 허용하는 다중집합과 중복조합의 공식을 유도한다. 하나의 집합을 두 가지 방법으로 세어 항등식을 얻는 이중 계수의 기법과 그 대표적 결과인 이항정리, 그리고 존재를 보장하는 비둘기집 원리를 다룬다. 선행 지식: 유한 집합, 함수, 자연수와 이항계수의 기초.

1.1 합의 법칙과 곱의 법칙

조합론의 계산은 대개 두 가지 기본 규칙으로 환원된다. 서로소인 유한 집합 $A_1, \dots, A_r$의 합집합 크기는

$$|A_1 \cup \cdots \cup A_r| = \sum_{i} |A_i|$$

이다. 이를 **합의 법칙**(*sum rule*)이라 한다. 서로소 조건이 없으면 겹치는 원소를 중복해서 세므로 따로 처리해야 하며, 이 조정은 제19권 제2장의 포함배제 원리로 일반화된다. 순서쌍의 집합 $A \times B$는 $|A|\,|B|$개 원소를 가지므로, 첫 선택이 a가지이고 그 각각에 대해 둘째 선택이 항상 b가지이면 전체 선택은 ab가지다. 이를 **곱의 법칙**(*product rule*)이라 한다. 둘째 선택지의 구체적인 내용이 첫 선택에 따라 달라도 그 가짓수가 항상 같기만 하면 곱의 법칙을 적용할 수 있다.

> **예제 1.1** 숫자 $0, 1, \dots, 9$로 중복 없이 세 자리 양의 정수를 만들면 첫 자리는 0을 제외한 9가지, 둘째 자리는 이미 쓴 숫자를 제외한 9가지, 셋째 자리는 8가지이므로 $9 \cdot 9 \cdot 8 = 648$개다. 첫 자리까지 10가지로 세면 맨 앞이 0인 문자열, 곧 실제로는 두 자리 이하인 수까지 포함하게 되므로 틀린다.

> **명제 1.2 (섬유를 이용한 계수)** 유한 집합 사이의 함수 $f\colon A \to B$가 전사이고 모든 $b \in B$에 대하여 $\left|f^{-1}(\{b\})\right| = k$이면 $|A| = k\,|B|$이다.

증명. 각 원소 $a \in A$는 정확히 하나의 **섬유**(*fiber*) $f^{-1}(\{f(a)\})$에 속한다. 따라서 섬유들이 A를 서로소인 $|B|$개의 집합으로 나누고 각 크기가 k이므로 $|A| = k\,|B|$이다. □

참고. 명제 1.2는 "대칭이 있으니 대칭의 개수로 나눈다"는 계산의 정확한 근거다. 모든 섬유(동치류)의 크기가 같다는 확인 없이 대칭의 개수로 나눌 수는 없다. 회전시켜도 같은 목걸이처럼 일부 배열이 대칭 변환에 그대로 고정되는 문제는 섬유의 크기가 고르지 않으므로 명제 1.2를 직접 쓸 수 없고, 제19권 제2장의 Burnside 보조정리가 필요하다.

1.2 순열, 조합, 다중집합

정의 1.3 (순열과 조합) n개의 서로 다른 원소 중 순서를 두어 k개를 중복 없이 나열한 것을 **순열**(*permutation*)이라 하고, 순서를 잊고 k개를 중복 없이 고른 것을 **조합**(*combination*)이라 한다.

n개의 원소에서 순서 있게 k개를 고르는 순열의 수는 각 자리를 차례로 채우는 곱의 법칙으로

$$n(n-1)\cdots(n-k+1)$$

이다. 순서를 잊는 함수(순열을 조합으로 보내는 사상)의 각 섬유는 명제 1.2에 의해 $k!$개의 순열로 이루어지므로, 조합의 수 곧 **이항계수**(*binomial coefficient*) $\binom{n}{k}$는

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \qquad (0 \le k \le n) \tag{1.1}$$

이다. 범위 밖의 정수 k에는 $\binom{n}{k} = 0$으로 놓으면 여러 항등식을 간결하게 쓸 수 있다. $\binom{n}{0} = 1$은 공집합이라는 선택이 하나뿐이라는 뜻이다.

정리 1.4 (Pascal 항등식) $n \ge 1$일 때

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

이다.

증명. 특정 원소 하나를 고정한다. k원소 부분집합은 그 원소를 포함하지 않는 경우와 포함하는 경우로 나뉜다. 전자는 나머지 $n-1$개에서 k개를, 후자는 나머지 $n-1$개에서 $k-1$개를 고르는 것과 일대일 대응한다. □

역사. 식 (1.1)의 계수를 삼각형으로 배열한 이른바 Pascal의 삼각형은 Blaise Pascal이 1654년 논고에서 체계적으로 다루기 여러 세기 앞서 인도의 Pingala, 페르시아의 Omar Khayyam, 중국의 Yang Hui(13세기) 등이 이미 알고 있었다.

정리 1.5 (중복조합: 별과 막대) $n \ge 0$, $r \ge 1$인 정수에 대하여

$$x_1 + \cdots + x_r = n, \qquad x_i \in \mathbb{N}$$

의 해의 개수는 $\binom{n+r-1}{r-1}$이다. 이 수를 **중복조합**(*combination with repetition*)이라고도 한다.

증명. n개의 별과 $r-1$개의 막대를 일렬로 배치한다. 첫 막대 앞의 별 수를 x_1, 연속한 두 막대 사이의 별 수를 해당 x_i, 마지막 막대 뒤의 별 수를 x_r로 읽는다. 막대가 나란히 있으면 해당 값이 0이다. 이 대응은 역변환(별·막대의 배열에서 각 x_i를 도로 읽어내는 과정)이 있는 일대일 대응이므로, 전체 $n+r-1$자리에서 막대의 위치 $r-1$개를 고르는 것과 해의 개수가 같다. □

예제 1.6 서로 구별하지 않는 사탕 10개를 이름이 다른 아이 4명에게 각자 적어도 하나씩 주는 방법의 수를 구한다. $y_i = x_i - 1 \ge 0$로 바꾸면 $\sum_i y_i = 6$을 세는 문제가 되므로 정리 1.5에 의해 답은 $\binom{9}{3} = 84$다. 사탕이 서로 구별되면 이 답은 달라진다.

다중집합에서 종류 i가 n_i번 나오는 길이 $n = \sum_i n_i$인 문자열의 수는

$$\frac{n!}{n_1! \cdots n_r!}$$

이다. 같은 종류의 사본에 임시로 서로 다른 이름을 붙여 모두 순열로 센 뒤, 이름을 잊는 섬유의 크기 $n_1! \cdots n_r!$로 나누면 명제 1.2에 의해 증명된다. 이 수를 **다중집합**(*multiset*) 순열의 수 또는 다항계수라 한다.

1.3 이중 계수와 이항정리

같은 집합을 두 가지 방법으로 세면 이항계수에 관한 항등식을 얻는다. 이를 **이중 계수**(*double counting*)라 한다. n원소 집합에서 부분집합 S와 그 안의 표시된 원소 $s \in S$를 고르는 순서쌍을 생각하자. $|S| = k$로 나누어 세면 $\sum_{k=0}^{n} k\binom{n}{k}$이고, 표시할 원소를 먼저 고르고 나머지 $n-1$개 원소 각각의 포함 여부를 정하면 $n2^{n-1}$이다. 두 셈이 같은 대상을 센 것이므로 $n \ge 1$에 대해

$$\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1} \tag{1.2}$$

이다.

명제 1.7 (Vandermonde 항등식) 음이 아닌 정수 m, n, r에 대하여

$$\sum_{k} \binom{m}{k}\binom{n}{r-k} = \binom{m+n}{r}$$

이다. 범위 밖의 이항계수는 0으로 해석한다.

증명. 크기 m, n인 서로소 두 집합의 합집합에서 r개를 고른다. 첫 집합에서 고른 개수가 k인 경우로 나누어 세면 왼쪽이고, 합친 집합에서 한꺼번에 고르면 오른쪽이다. □

가환환의 원소 x, y에 대하여 n개의 인자 $(x+y)$를 곱할 때, y를 택하는 위치가 k개인 항은 $\binom{n}{k}x^{n-k}y^{k}$이다. 모든 k에 대해 이 항들을 더하면 **이항정리**(*binomial theorem*)

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^{k} \tag{1.3}$$

를 조합적으로 얻는다. 행렬처럼 $xy \neq yx$이면 전개의 항들을 이렇게 모을 수 없다. $n = 2$에서는 이미

$$(x+y)^2 = x^2 + xy + yx + y^2$$

이고, $xy = yx$를 가정해야 $x^2 + 2xy + y^2$으로 줄어든다.

1.4 비둘기집 원리와 존재 증명

정리 1.8 (비둘기집 원리) N개 대상을 $r \ge 1$개 상자에 넣으면 어떤 상자에는 적어도 $\lceil N/r \rceil$개가 들어 있다.

증명. 모든 상자의 크기가 $\lceil N/r \rceil - 1 < N/r$이면 전체 합이 N보다 작아 모순이다. □

예제 1.9 임의의 정수 $a_1, \dots, a_n$에서 합이 n의 배수인 비어 있지 않은 연속 부분열이 존재한다. 부분합 $s_k = \sum_{i=1}^{k} a_i$를 본다. 어떤 s_k가 0과 합동이면 끝이다. 그렇지 않으면 n개의 나머지가 $n-1$개의 비영 나머지 중 하나이므로, 정리 1.8에 의해 $s_i \equiv s_j \pmod n$인 $i < j$가 있다. 그러면 $a_{i+1} + \cdots + a_j = s_j - s_i$가 원하는 합이다.

예제 1.10 $1, 2, \dots, 2n$에서 $n+1$개의 수를 고르면 하나가 다른 하나를 나누는 두 수가 있다. 각 수를 $2^k q$로 쓰되 q는 홀수로 둔다. 가능한 홀수 부분 q는 $1, 3, \dots, 2n-1$의 n가지다. 고른 수가 $n+1$개이므로 정리 1.8에 의해 같은 q를 가진 두 수가 있고, 이 둘은 2의 지수만 다르므로 작은 수가 큰 수를 나눈다.

흔한 오류. 비둘기집 원리는 어떤 쌍이 존재한다는 사실을 주지만 반드시 그 쌍을 즉시 구성해 주지는 않는다. 상자를 어떻게 정하느냐가 증명의 핵심이며, 예제 1.9에서는 나머지를, 예제 1.10에서는 홀수 부분을 상자로 삼았다.

1.5 연습문제와 해설

연습문제 1.11 길이 8의 이진 문자열 중 1이 정확히 3개인 것과 적어도 하나인 것의 수를 각각 구하라.

풀이. 첫째는 1의 위치를 고르므로 $\binom{8}{3} = 56$이다. 둘째는 전체 2^8개에서 0만 있는 하나를 빼서 255개다.

연습문제 1.12 $x + y + z = 12$를 만족하는 양의 정수해 중 $x \ge 3$인 것의 수를 구하라.

풀이. $u = x - 3 \ge 0$, $v = y - 1 \ge 0$, $w = z - 1 \ge 0$으로 두면 음이 아닌 해 $u + v + w = 7$과 일대일 대응한다. 정리 1.5에 의해 답은 $\binom{9}{2} = 36$이다.

연습문제 1.13 $n \ge 2$일 때 $\displaystyle\sum_{k} k(k-1)\binom{n}{k} = n(n-1)2^{n-2}$를 계수로 증명하라.

풀이. 부분집합 하나와 그 안의 서로 다른 두 표시 원소를 순서 있게 고르는 삼중항을 센다. 부분집합의 크기를 먼저 정하면 왼쪽이다. 표시 원소를 먼저 고르는 $n(n-1)$가지와, 나머지 $n-2$개 원소 각각의 포함 여부 2^{n-2}가지를 곱하면 오른쪽이다.

연습문제 1.14 정수 6개 중 차이가 5의 배수인 두 수가 반드시 있는 이유를 설명하라.

풀이. 5로 나눈 나머지는 5가지뿐이므로, 정리 1.8을 $N = 6$, $r = 5$에 적용하면 같은 나머지 상자에 적어도 두 수가 들어간다. 같은 나머지 상자에 있는 서로 다른 두 입력의 차이는 5의 배수이고, 두 입력의 값이 같은 경우에도 차이 0은 5의 배수다.

제 2 장

포함과 배제, 대칭을 가진 계수

개요 포함배제 원리(*inclusion–exclusion principle*)는 여러 조건을 동시에 만족하는 대상의 개수를, 각 조건과 그 교집합들의 크기를 번갈아 더하고 빼어 구하는 계산 규칙이다. 이 장은 포함배제 원리로 완전순열과 전사 함수의 수, 상한이 있는 정수해의 개수를 구하고, 유한 군의 작용으로 생기는 대칭을 Burnside 보조정리로 올바르게 세는 방법을 다룬다. 두 원리 모두 제1장의 섬유를 이용한 계수(명제 1.2)를 일반화한다. 선행 지식: 유한 집합의 합집합·교집합, 순열, 함수의 합성.

2.1 포함배제 원리

두 집합에서는 $|A \cup B| = |A| + |B| - |A \cap B|$이다. 세 집합에서는 두 번 겹친 부분을 빼다가 세 집합 모두에 속한 원소를 과하게 빼므로 마지막에 다시 더한다. 이를 일반화하면 다음과 같다.

정리 2.1 (포함배제 원리) 유한 집합 $A_1, \dots, A_r$에 대하여

$$\left| \bigcup_{i=1}^{r} A_i \right| = \sum_{\emptyset \neq I \subseteq \{1,\dots,r\}} (-1)^{|I|+1} \left| \bigcap_{i \in I} A_i \right| \tag{2.1}$$

이다.

증명. 어떤 원소가 정확히 $k \geq 1$개의 집합에 속한다고 하자. 식 (2.1)의 오른쪽에서 그 원소가 받는 계수는

$$\sum_{j=1}^{k} (-1)^{j+1} \binom{k}{j} = 1$$

이다. 이는 $(1-1)^k = \sum_{j=0}^{k} (-1)^j \binom{k}{j} = 0$에서 $j = 0$인 상수항 1을 반대편으로 옮긴 것과 같다. 아무 집합에도 속하지 않는 원소의 계수는 0이다. 원소별 기여가 양쪽에서 일치하므로 전체 합도 같다. $\square$

예제 2.2 1부터 100까지 중 2 또는 3 또는 5의 배수는

$$50 + 33 + 20 - 16 - 10 - 6 + 3 = 74$$

개다. 교집합을 셀 때 2와 3의 공배수는 6의 배수, 세 수 모두의 공배수는 30의 배수라는 점을 쓴다.

참고. 확률에서도 지표함수(사건이 일어나면 1, 아니면 0인 함수)에 대한 같은 증명을 기댓값에 적용하면 포함배제 공식을 얻는다. 집합의 크기를 사건의 확률로 바꾸면 되며, 기댓값의 선형성만 쓰므로 사건들이 서로 독립일 필요는 없다.

2.2 완전순열과 전사 함수

정의 2.3 (완전순열) $\{1,\dots,n\}$의 순열 σ에서 모든 i에 대해 $\sigma(i)\neq i$이면 σ를 **완전순열**(*derangement*)이라 한다. 완전순열의 개수를 D_n으로 쓴다.

위치 i가 고정되는 사건 $A_i=\{\sigma:\sigma(i)=i\}$를 모두 피해야 한다. 정해진 k개 위치가 고정되는 순열은 나머지 $n-k$개 자리의 임의 순열이므로 $(n-k)!$개다. 정리 2.1에서 $|I|=k$인 항이 $\binom{n}{k}$개씩 같은 값을 가지므로

$$D_n=\sum_{k=0}^{n}(-1)^k\binom{n}{k}(n-k)!=n!\sum_{k=0}^{n}\frac{(-1)^k}{k!} \tag{2.2}$$

이다. 작은 값은 $D_0=1$, $D_1=0$, $D_2=1$, $D_3=2$, $D_4=9$이다. 지수함수의 Maclaurin 급수 $e^{-1}=\sum_{k\ge 0}(-1)^k/k!$의 교대급수 나머지 추정을 쓰면 $|D_n-n!/e|<1/(n+1)$이고, $n\ge 1$에서 D_n은 $n!/e$에 가장 가까운 정수다. 이 근사는 급수의 수렴을 다루는 제8권 제6장에서 정당화한다.

예제 2.4 크기 m의 집합에서 크기 r의 집합으로 가는 전사 함수의 수는

$$\sum_{k=0}^{r}(-1)^k\binom{r}{k}(r-k)^m$$

이다. 여기서는 $m\ge 1$로 두어 $0^m=0$이 명확하다. 공역 원소 가운데 상이 비는 집합을 포함배제한다. $m=4$, $r=3$이면 $3^4-3\cdot 2^4+3\cdot 1^4=81-48+3=36$이다.

$m<r$이면 전사 함수가 없어 위 합은 0이다. 공식을 그대로 계산하기 전에 이 구조적 사실을 알면 검산에 도움이 된다. 빈 정의역의 유일한 함수(공집합에서 가는 함수)는 공역도 비어 있을 때에만 전사다.

2.3 상한이 있는 정수해

$x_1+\cdots+x_r=n$, $0\le x_i\le b$를 세려면 상한을 위반하는 사건 $A_i=\{x_i\ge b+1\}$를 제거한다. 지정된 k개의 변수를 각각 $b+1$만큼 내리면 합이 $n-k(b+1)$인 음이 아닌 해로 바뀌므로, 정리 2.1와 정리 1.5에 의해

$$\sum_{k=0}^{r}(-1)^k\binom{r}{k}\binom{n-k(b+1)+r-1}{r-1} \tag{2.3}$$

이 답이다. 이 식에서 $n-k(b+1)<0$인 항은 0으로 정의한다. 위 지수가 음수가 된 이항계수를 일반화된 이항계수로 해석하는 것은 이 계수 문제와는 다른 규약이다.

예제 2.5 $x+y+z=8$, $0\le x,y,z\le 4$의 해는 $\binom{10}{2}-3\binom{5}{2}=45-30=15$개다. 두 변수가 동시에 5 이상이면 합이 10 이상이 되어 8을 넘으므로 두 겹 교집합의 항은 없다.

2.4 군 작용과 궤도

유한 군 G가 유한 집합 X에 **작용**(*group action*)한다는 것은 각 $g\in G$가 X의 순열로 작용하고 $ex=x$, $(gh)x=g(hx)$를 만족한다는 뜻이다. 군의 공리를 아직 배우지 않았어도 회전의 합성과 항등 회전을 생각하면 충분히 예를 다룰 수 있다(군의 정식 정의는 제14권 제1장에서 다룬다).

정의 2.6 (궤도와 안정자군) $x \in X$의 **궤도**(*orbit*)는 $Gx = \{gx : g \in G\}$이고, **안정자군**(*stabilizer*)은 $G_x = \{g \in G : gx = x\}$이다. 원소 $g \in G$가 고정하는 대상의 집합은 $\mathrm{Fix}(g) = \{x \in X : gx = x\}$이다.

보조정리 2.7 (궤도와 안정자) $|Gx| = |G| / |G_x|$이다.

증명. 함수 $g \mapsto gx$의 같은 섬유에 속한다는 조건, 곧 $gx = hx$는 $h^{-1}g \in G_x$와 같다. 따라서 각 섬유는 어떤 h에 대해 hG_x 꼴이고 크기가 $|G_x|$로 모두 같다. 명제 1.2(섬유 계수 법칙)를 치역 Gx에 적용하면 $|G| = |G_x|\,|Gx|$이다. □

정리 2.8 (Burnside 보조정리) 궤도의 개수는

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$$

이다.

증명. 쌍 (g, x) 중 $gx = x$인 것의 수를 센다. g를 먼저 고르면 정리의 오른쪽에 있는 합이다. x를 먼저 고르면 $\sum_x |G_x|$이다. 하나의 궤도 O에서는 모든 $x \in O$에 대해 보조정리 2.7에 의해 $|G_x| = |G| / |O|$이므로 그 궤도의 기여는 $|O| \cdot |G| / |O| = |G|$이다. 따라서 전체 합은 궤도 개수의 $|G|$배이고, 양변을 $|G|$로 나누면 원하는 식을 얻는다. □

역사. 정리 2.8는 William Burnside의 1897년 저서 *Theory of Groups of Finite Order*에 실려 그 이름이 붙었지만, 핵심 계산은 그보다 앞서 1845년 Augustin-Louis Cauchy가, 1887년 Ferdinand Georg Frobenius가 이미 증명했다. 이 때문에 Cauchy–Frobenius 보조정리라고도 부른다.

예제 2.9 네 꼭짓점이 있는 정사각형의 각 꼭짓점을 두 색 중 하나로 칠하되, 회전으로 일치하는 것은 같게 보고 반사는 허용하지 않는다. 회전군은 항등, 90도, 180도, 270도 회전으로 이루어진 크기 4의 군이다. 항등 회전은 $2^4 = 16$개의 배열을 고정하고, 90도와 270도 회전은 네 꼭짓점을 하나의 순환으로 옮기므로 같은 색이어야 고정되어 각각 2개를, 180도 회전은 두 쌍의 꼭짓점을 바꾸므로 $2^2 = 4$개를 고정한다. 정리 2.8에 의해 서로 다른 색칠은

$$\frac{16 + 2 + 4 + 2}{4} = 6$$

가지다. 단순히 $16/4 = 4$로 나누면 회전 대칭을 가진 배열(예컨대 네 꼭짓점이 모두 같은 색인 배열)을 중복해서 빼는 셈이 되어 잘못 센다.

흔한 오류. 회전만 같게 보는지 반사도 같게 보는지에 따라 작용하는 군 G가 달라지고, 이에 따라 $\mathrm{Fix}(g)$도 달라진다. 예제 2.9는 이름이 붙은 꼭짓점의 색칠을 먼저 세고 회전으로 묶은 것일 뿐, 반사를 포함하는 정이면체군을 쓰면 답이 달라진다.

2.5 연습문제와 해설

연습문제 2.10 1부터 60까지 중 4 또는 6의 배수인 수는 몇 개인가?

풀이. 각각 15개, 10개이고 공배수는 4, 6의 최소공배수인 12의 배수 5개다. 정리 2.1에 의해 답은 $15 + 10 - 5 = 20$개다. 4와 6의 곱 24의 배수를 빼면 최소공배수가 아니어서 틀린다.

연습문제 2.11 D_5를 구하고 $n \ge 2$에서 $D_n = (n-1)(D_{n-1} + D_{n-2})$인 이유를 설명하라.

풀이. 식 (2.2)에서 $D_5 = 120 - 120 + 60 - 20 + 5 - 1 = 44$이다. 완전순열 σ에서 $\sigma(1) = j \neq 1$을 먼저 정한다. $\sigma(j) = 1$이면 $1, j$의 2-순환을 지우고 나머지 $n-2$개 원소를 완전순열로 만들면 되므로 D_{n-2}가지다. $\sigma(j) \neq 1$이면 순환 표기에서 1을 지우고 $\sigma(j)$를 그 자리로 당기면 나머지 $n-1$개 원소의 완전순열과 대응하며, 역으로 j 바로 앞에 1을 삽입하면 원래의 완전순열을 복원하므로 D_{n-1}가지다. j의 선택은 $n-1$가지이므로 두 경우를 더하면 $D_n = (n-1)(D_{n-1} + D_{n-2})$이다.

연습문제 2.12 삼각형의 꼭짓점을 세 색으로 칠하되 회전만 같은 것으로 보면 몇 종류인가?

풀이. 회전군의 크기는 3이다. 항등 회전은 $3^3 = 27$개를 고정하고, 두 개의 120도 회전은 세 꼭짓점을 하나의 순환으로 옮기므로 세 꼭짓점이 모두 같은 색인 3개씩을 고정한다. 정리 2.8에 의해 답은 $(27 + 3 + 3)/3 = 11$이다.

연습문제 2.13 $x_1 + x_2 + x_3 + x_4 = 6$, $0 \le x_i \le 2$의 해의 수를 구하라.

풀이. 식 (2.3)에 $n = 6$, $b = 2$, $r = 4$를 대입하면 $\binom{9}{3} - 4\binom{6}{3} + 6\binom{3}{3} = 84 - 80 + 6 = 10$이다. 검산으로 $y_i = 2 - x_i$를 두면 $\sum y_i = 2$인 음이 아닌 4변수 해를 세는 문제가 되고, 그 수는 $\binom{5}{3} = 10$으로 일치한다. 합이 2이므로 각 $y_i \le 2$는 자동으로 성립한다.

제 3 장

점화식과 생성함수

개요 점화식(*recurrence relation*)은 수열의 뒤 항을 앞 항들로 정의하는 규칙이고, 생성함수(*generating function*)는 수열의 모든 항을 하나의 형식적 멱급수의 계수로 부호화하여 대수 연산으로 다루는 도구다. 이 장은 초기값 없이는 점화식이 수열을 정하지 못한다는 사실에서 출발하여, 상수계수 선형 점화식의 특성방정식 풀이법, 형식적 멱급수의 엄밀한 정의와 연산, Fibonacci 수열과 Catalan 수의 생성함수를 통한 닫힌 식 유도, 선택을 인자의 곱으로 바꾸는 생성함수의 계수 추출 기법을 다룬다. 선행 지식: 수열, 다항식, 유한 합. 해석적 수렴은 필요한 곳에서 별도로 가정한다.

3.1 점화식에는 초기값이 필요하다

점화식은 앞 항으로 뒤 항을 정하는 규칙이다. $a_{n+1} = 2a_n$만으로는 수열을 하나로 정하지 못하며, a_0를 주어야 $a_n = 2^n a_0$로 유일하게 결정된다. 더 높은 차수의 점화식은 그에 맞는 개수의 초기 자료가 필요하다.

> **예제 3.1 (하노이 탑)** 기둥 세 개를 사용하는 하노이 탑에서, 한 기둥에 크기순으로 쌓인 n개의 원판을 다른 지정된 기둥으로 옮기는 최소 횟수를 T_n이라 하자. 한 번에 원판 하나만 옮기고, 큰 원판을 작은 원판 위에 놓지 않는다. 가장 큰 원판을 처음 옮기기 전에는 작은 $n-1$개를 남은 한 기둥에 모두 모아야 하고, 가장 큰 원판을 마지막으로 목표 기둥에 옮긴 뒤에는 작은 원판들을 다시 그 위로 옮겨야 한다. 두 과정은 각각 최소 T_{n-1}번이 필요하고, 가장 큰 원판의 이동도 적어도 한 번 필요하다. 이 하한은 큰 원판을 정확히 한 번만 옮기는 재귀적 절차로 실제로 달성되므로
>
> $$T_n = 2T_{n-1} + 1, \qquad T_0 = 0$$
>
> 이고, 귀납적으로 $T_n = 2^n - 1$이다. 이러한 횟수로 옮기는 절차를 하나 제시하는 것만으로는 그보다 적은 횟수로 옮기는 절차가 없다는 최소성까지 증명되지 않으므로, 앞의 하한 논증이 반드시 필요하다.

> **정리 3.2 (이차 선형 점화식의 일반해)** 상수 p, q에 대한 점화식 $a_{n+2} = pa_{n+1} + qa_n$ $(q \neq 0)$에서 $a_n = r^n$을 대입하면 특성방정식 $r^2 - pr - q = 0$을 얻는다. 이 방정식이 서로 다른 두 근 r_1, r_2를 가지면 점화식의 모든 해는 $Ar_1^n + Br_2^n$ 꼴이고, 중근 $r \neq 0$을 가지면 모든 해는 $(A + Bn)r^n$ 꼴이다.

증명. $a_n = Ar_1^n + Br_2^n$이 점화식을 만족함은 직접 대입하면 확인된다. 임의의 초기값 a_0, a_1에 대해 $A + B = a_0$, $Ar_1 + Br_2 = a_1$을 A, B에 대해 풀면, 두 식에서 $A + B = a_0$를 r_1배 하여 빼면 $B(r_2 - r_1) = a_1 - a_0 r_1$을 얻고 $r_1 \neq r_2$이므로 B가, 이어서 A가 유일하게 정해지며, 점화식 자체가 초기값으로 수열을 유일하게 결정하므로 이것이 유일한 해다. 중근 r인 경우에는 $(A + Bn)r^n$

도 점화식을 만족함을 대입으로 확인하고, 마찬가지로 A, B를 초기값에서 유일하게 결정할 수 있다. $\square$

근이 0인 퇴화 경우($q = 0$)는 $a_{n+2} = p a_{n+1}$이 되어 등비수열로 직접 확인한다.

3.2 형식적 멱급수의 뜻

정의 3.3 (형식적 멱급수) 체 K 위의 **형식적 멱급수**(*formal power series*) $A(x) = \sum_{n \ge 0} a_n x^n$은 계수열 $(a_0, a_1, \dots)$을 기록하는 기호다. 이 단계에서 x는 실수로 대입하는 변수가 아니다. 두 급수의 곱은

$$[x^n](A(x)B(x)) = \sum_{k=0}^{n} a_k b_{n-k} \tag{3.1}$$

로 정의한다. $[x^n]$은 x^n의 계수를 뽑는 기호다.

각 계수의 계산에 유한 합만 필요하므로 수렴 반경 없이도 곱셈을 정의할 수 있다. 상수항이 0이 아닌 급수는 곱셈 역원을 가진다. $a_0 b_0 = 1$로 b_0를 정하고, $n \ge 1$에서 $\sum_{k=0}^{n} a_k b_{n-k} = 0$으로 b_n을 차례로 정하면(이 조건이 b_n을 $a_0, \dots, a_n$과 $b_0, \dots, b_{n-1}$만으로 유일하게 결정한다) 역원의 존재가 증명된다.

$$\frac{1}{1 - x} = \sum_{n \ge 0} x^n, \qquad \frac{1}{1 - cx} = \sum_{n \ge 0} c^n x^n$$

은 형식적 항등식이다. 이를 수치 함수의 등식으로 읽으려면 각각 $|x| < 1$, $|cx| < 1$처럼 수렴 조건을 확인해야 한다. 형식적 합성이나 무한 합을 다룰 때에도 매 계수에 유한하게만 기여한다는 조건을 확인해야 한다.

3.3 Fibonacci 수열과 계수 추출

$F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$의 생성함수 $F(x) = \sum_{n \ge 0} F_n x^n$는

$$F(x) - x = x F(x) + x^2 F(x), \qquad F(x) = \frac{x}{1 - x - x^2}$$

를 만족한다. 첫 등식은 점화식 $F_{n+2} = F_{n+1} + F_n$ $(n \ge 0)$이 양변에서 차수가 2 이상인 항들의 계수를 맞춘 것과 같다는 사실에서 나온다. $\alpha = (1 + \sqrt{5})/2$, $\beta = (1 - \sqrt{5})/2$라 두면 α, β는 $r^2 - r - 1 = 0$의 두 근이므로 $1 - x - x^2 = (1 - \alpha x)(1 - \beta x)$이고, 부분분수 분해로

$$\frac{x}{1 - x - x^2} = \frac{1}{\sqrt{5}} \left(\frac{1}{1 - \alpha x} - \frac{1}{1 - \beta x} \right)$$

이므로

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}} \tag{3.2}$$

을 얻는다(Binet 공식).

예제 3.4 길이 n인 이진 문자열 중 1이 연속해서 나오지 않는 것의 수를 b_n이라 하자. 마지막 문자가 0이면 앞부분은 b_{n-1}가지이다. 마지막 문자가 1이면 바로 앞은 0이어야 하므로 $n \ge 2$에서 앞의 $n - 2$자리는 b_{n-2}가지다. $b_0 = 1$(빈 문자열), $b_1 = 2$이므로 $b_n = F_{n+2}$이다. 빈 문자

열을 하나로 세어야 이 초기값이 Fibonacci 수열과 어긋나지 않는다.

3.4 선택을 곱셈으로 바꾸기

음이 아닌 정수해 $x_1 + \cdots + x_r = n$에서 각 x_i의 선택은 인자 $1 + x + x^2 + \cdots$의 항 선택으로 나타낼 수 있다. 합계 n은 r개 인자를 곱한 급수에서 x^n의 계수다. 상한 b_i가 있으면 해당 인자는 $1 + x + \cdots + x^{b_i}$로 바뀐다.

예제 3.5 1, 2, 5 단위 동전을 각각 제한 없이 써서 7을 만드는 방법의 수는

$$[x^7]\frac{1}{(1-x)(1-x^2)(1-x^5)} = 6$$

이다. 5단위 동전을 쓰지 않으면 2단위 동전이 $0, 1, 2, 3$개인 4가지, 5단위 동전을 하나 쓰면 남은 2를 만드는 2가지이므로 합이 6이다. 동전을 나열하는 순서는 세지 않는다.

지수생성함수(*exponential generating function*)에서는 $\mathbb{Q}, \mathbb{R}$ 등 특성 0인 체를 써서 모든 항을 $n!$으로 나눌 수 있게 한다. 이때 $\sum_{n\ge 0} a_n x^n/n!$을 사용한다. 두 지수생성함수의 곱에서 $x^n/n!$의 계수는 $\sum_k \binom{n}{k} a_k b_{n-k}$이다. 이름이 붙은 n개의 원소를 두 구조에 나누어 배정하는 문제에서 이항계수가 자연스럽게 나타나는 이유다. 일반생성함수와 지수생성함수는 계수 추출 규칙이 다르므로 (식 (3.1)와 비교) 서로 바꾸어 쓸 수 없다.

3.5 Catalan 수와 경로의 반사

격자에서 오른쪽 $(1,0)$과 위쪽 $(0,1)$으로만 움직여 $(0,0)$에서 (n,n)까지 가되 항상 $y \le x$를 지키는 경로의 수를 C_n이라 하자. 전체 경로는 $\binom{2n}{n}$개다. 금지선을 처음 넘어 $y = x+1$에 도달하는 경로의 그 지점까지의 앞부분에서 오른쪽과 위쪽 이동을 서로 바꾸면, 끝점이 $(n+1, n-1)$인 경로와 일대일로 대응한다(역변환은 $x = y+1$에 처음 도달하는 앞부분을 다시 반사하면 된다). 따라서 $n \ge 1$에서

$$C_n = \binom{2n}{n} - \binom{2n}{n-1} = \frac{1}{n+1}\binom{2n}{n}, \qquad C_0 = 1 \tag{3.3}$$

이다.

명제 3.6 $C_{n+1} = \sum_{k=0}^{n} C_k C_{n-k}$이다.

증명. 허용 경로는 첫 오른쪽 이동 뒤 처음으로 대각선에 돌아올 때까지의 작은 허용 경로 하나와, 그 뒤를 잇는 또 하나의 작은 허용 경로를 담고 있다. 첫 블록 내부의 크기를 k로 두면 나머지 블록의 크기는 $n-k$다. 첫 귀환 위치가 유일하게 정해지므로 이 분해는 중복이 없고, $k = 0, \dots, n$에 대해 합하면 된다. 같은 논증을 올바른 괄호열에서 첫 여는 괄호와 그 짝이 되는 닫는 괄호의 안쪽·바깥쪽 분해로 읽어도 동일하다. □

생성함수 $C(x) = \sum_{n\ge 0} C_n x^n$는 명제 3.6와 식 (3.1)에 의해

$$C(x) = 1 + xC(x)^2$$

를 만족한다. 이 식은 계수를 차례로 유일하게 정하므로 수열 (C_n)을 결정한다. 이차방정식 $xt^2 - t + 1 = 0$의 두 대수적 가지 $t = (1 \pm \sqrt{1-4x})/(2x)$ 중, 형식적 멱급수로서 상수항이 1인 가지(곧 $\sqrt{1-4x}$의 전개에서 $-$ 부호를 택한 가지)를 골라야 한다.

흔한 오류. 생성함수의 분모를 대수적으로 푸는 일과, 계수 수열의 확률적·해석적 성질을 증명하는 일은 다른 작업이다. 특이점 $x = 1/4$ 근방에서 C_n의 점근식을 얻으려면 별도의 해석적 정리(특이점 분석)가 필요하며, 이는 이 장의 형식적 대수 범위를 넘어선다.

3.6 연습문제와 해설

연습문제 3.7 $a_0 = 2$, $a_{n+1} = 3a_n + 4$의 일반항을 구하라.

풀이. $a_{n+1} + 2 = 3(a_n + 2)$이므로 $a_n + 2 = 4 \cdot 3^n$, 즉 $a_n = 4 \cdot 3^n - 2$이다. $n = 0$과 점화식에 대입해 검산한다.

연습문제 3.8 $[x^n](1-x)^{-2}$를 구하라.

풀이. 식 (3.1)로 두 기하급수를 곱하면 x^n에 기여하는 순서쌍 $(k, n-k)$가 $k = 0, \dots, n$의 $n+1$가지이므로 계수는 $n+1$이다. 해석적 미분 없이 형식적 곱만으로 얻었다.

연습문제 3.9 1이 연속하지 않는 길이 5 이진 문자열과, 올바른 세 쌍 괄호열의 개수를 각각 구하라.

풀이. 예제 3.4와 식 (3.3)에 의해 각각 $F_7 = 13$, $C_3 = \binom{6}{3}/4 = 5$이다. 괄호열은 $((()))$, $(()())$, $(())()$, $()(())$, $()()()$이다.

연습문제 3.10 상수항이 0인 형식적 멱급수 x에는 왜 멱급수 역원이 없는가?

풀이. 어떤 멱급수 $B(x)$와 곱해도 $xB(x)$의 상수항은 0이다. 따라서 상수항이 1인 곱셈 항등원과 같을 수 없다. x^{-1}은 음의 차수를 허용하는 Laurent 급수의 원소이며, 정의 3.3의 형식적 멱급수환의 원소는 아니다.

제 4 장

그래프, 연결, 나무와 순회

개요 그래프(*graph*)는 대상들 사이의 두 자리 관계를 꼭짓점과 간선으로 나타내는 구조다. 이 장은 유한 단순 무향 그래프를 정의하고 차수와 손잡기 정리, 인접행렬을 소개한 뒤, 보행·트레일·경로·순환의 용어를 구분하고 연결 성분을 정의한다. 이어서 순환이 없는 그래프인 나무의 여러 동치 조건을 증명하고, 모든 간선을 한 번씩 지나는 Euler 순회의 존재 조건을 다룬다. 선행 지식: 유한 집합, 관계, 수학적 귀납법.

4.1 그래프의 모형을 먼저 정하기

정의 4.1 (단순 그래프) 유한 **단순 무향 그래프**(*simple undirected graph*) $G = (V, E)$에서 V는 **꼭짓점**(*vertex*) 집합이고, E는 서로 다른 두 꼭짓점의 순서 없는 쌍들의 집합으로 **간선**(*edge*)이라 한다. 자기 자신을 잇는 고리와, 같은 쌍을 중복해서 잇는 간선은 허용하지 않는다. 간선에 방향이 있는 그래프를 방향 그래프라 하고, 중복 간선을 허용하는 그래프를 다중 그래프라 하며 둘 다 별도의 모형이다.

꼭짓점 v의 **차수**(*degree*) $\deg(v)$는 그 꼭짓점에 닿는 간선의 수다. 이웃 집합을 $N(v)$로 쓴다. 단순 그래프에서는 $\deg(v) = |N(v)|$이지만, 고리나 중복 간선이 있으면 같은 식으로 정의할 수 없다. 고리가 있는 무향 그래프에서 아래의 손잡기 정리를 유지하려면 고리는 차수에 두 번 기여한다고 정한다.

정리 4.2 (손잡기 정리) 유한 무향 그래프에서

$$\sum_{v \in V} \deg(v) = 2\,|E|$$

이다. 따라서 홀수 차수를 가진 꼭짓점의 개수는 짝수다.

증명. 각 간선은 양 끝에서 한 번씩 세어지므로 차수의 합은 간선 수의 두 배다. 차수 합에서 짝수인 항들을 모두 빼면 남는 것은 홀수 차수 꼭짓점들의 차수의 합이고, 이것이 짝수(전체 합이 짝수이므로)여야 하므로 홀수 항의 개수도 짝수여야 한다. □

예제 4.3 차수열 $(3, 3, 2, 2, 2)$의 합은 12이므로 이를 가진 그래프가 있다면 간선은 6개다. 다만 합이 짝수라는 조건만으로 차수열이 항상 실현되는 것은 아니다. 단순 그래프의 차수열 $(3, 3, 1, 1)$은 불가능하다. 차수가 3인 처음 두 꼭짓점은 나머지 모든 꼭짓점과 연결되어야 하는데, 꼭짓점이 모두 넷뿐이므로 이 두 꼭짓점은 나머지 두 꼭짓점 각각과도 연결되어야 하고, 따라서 마지막 두 꼭짓점의 차수가 적어도 2가 되어 모순이다.

모든 두 꼭짓점이 간선으로 이어진 n개 꼭짓점의 단순 그래프를 **완전 그래프**(*complete graph*) K_n이라 한다.

인접행렬(*adjacency matrix*) A는 꼭짓점에 번호를 붙인 뒤, i, j 사이에 간선이 있으면 $A_{ij} = 1$, 없으면 0으로 놓은 행렬이다. 단순 무향 그래프에서는 A가 대칭이고 대각 성분이 0이다. 번호를 바꾸면 행렬은 바뀌어도(동시에 행과 열에 같은 치환을 적용한 것과 같다) 그래프의 연결 구조 자체는 바뀌지 않는다.

4.2 보행, 경로, 연결 성분

보행(*walk*)은 연속한 꼭짓점들이 간선으로 이어지는 꼭짓점의 열이다. 간선을 반복하지 않는 보행을 **트레일**(*trail*)이라 하고, 꼭짓점을 반복하지 않는 것을 **단순 경로**(*path*)라 한다. 단순 무향 그래프에서 길이가 3 이상이고 시작과 끝만 같으며 나머지 꼭짓점은 서로 다른 닫힌 보행을 **순환**(*cycle*)이라 한다. 이 용어들은 문헌마다 정의가 약간씩 달라서 조건을 직접 확인하는 습관이 필요하다. 두 꼭짓점을 잇는 보행이 있으면 반복되는 구간을 지워 단순 경로를 얻을 수 있다. "단순 경로로 연결된다"는 관계는 동치관계이며 그 동치류를 **연결 성분**(*connected component*)이라 한다. 모든 꼭짓점이 하나의 성분에 속하면 연결 그래프라 한다.

> **명제 4.4** 인접행렬 A의 (i, j) 성분 $(A^k)_{ij}$는 i에서 j로 가는 길이 k의 보행 수다. $k = 0$에서는 $A^0 = I$로 해석한다.

증명. $k = 1$은 정의와 같다. 길이 $k+1$인 보행을 마지막 직전 꼭짓점 ℓ로 나누면, i에서 ℓ까지 길이 k인 보행과 ℓ에서 j로 가는 간선의 짝의 수인 $\sum_{\ell} (A^k)_{i\ell} A_{\ell j}$개다. 이는 행렬곱 $A^{k+1} = A^k A$의 정의와 같으므로, k에 대한 귀납법이 적용된다. $\square$

이 값은 일반적으로 단순 경로의 수가 아니다. 보행은 같은 꼭짓점이나 간선을 여러 번 지날 수 있기 때문이다. 완전 그래프 K_3에서 $(A^2)_{11} = 2$는 출발점으로 되돌아오는 두 가지 길이 2의 보행(이웃 두 곳을 거쳐 돌아오는 두 경로)을 센 것이다.

4.3 나무의 동치 조건

> **정의 4.5 (나무와 숲)** 연결되고 순환이 없는 유한 단순 그래프를 **나무**(*tree*)라고 한다. 순환이 없는 그래프는 연결 여부와 무관하게 **숲**(*forest*)이라 한다. 꼭짓점 하나와 간선이 없는 그래프도 나무다.

> **보조정리 4.6** 꼭짓점이 둘 이상인 유한 나무에는 차수가 1인 **잎**(*leaf*)이 적어도 둘 있다.

증명. 길이가 최대인 단순 경로를 하나 고른다. 양 끝점 중 하나에 경로 밖의 이웃이 있으면 그 이웃을 덧붙여 경로를 늘릴 수 있어 최대성에 모순이다. 경로 안의 다른 꼭짓점에 끝점이 추가로 연결되면 그 끝점에서 경로를 따라가다 그 연결로 되돌아오는 순환이 생겨 나무라는 가정에 모순이다. 따라서 경로의 양 끝점은 경로 위의 이웃 하나만을 가지므로 차수가 1이다. $\square$

> **정리 4.7 (나무의 동치 조건)** $n \geq 1$개 꼭짓점을 가진 유한 단순 그래프 G에 대하여 다음은 동치다.
>
> (1) G는 나무이다.
>
> (2) 임의의 두 꼭짓점 사이에 단순 경로가 정확히 하나 있다.

(3) G는 연결되어 있고 간선 수가 $n-1$이다.
(4) G는 순환이 없고 간선 수가 $n-1$이다.

증명. (1)⇒(2). 나무에서는 연결성에 의해 경로가 존재한다. 서로 다른 두 경로가 있으면 처음 갈라졌다가 다시 만나는 구간에서 순환이 생기므로 유일하다.

(2)⇒(1). 유일한 경로가 있다는 조건은 연결성을 주고, 두 경로가 있으면 순환이 생기므로 순환의 존재를 배제한다.

(1)⇒(3). 나무에서 잎 하나(보조정리 4.6로 존재)와 그 간선을 지우면 남은 그래프도 나무다. n에 대한 귀납법으로, $n=1$이면 간선이 $0=n-1$개이고, $n>1$이면 귀납 가정에 의해 지운 뒤의 나무는 간선이 $(n-1)-1$개이므로 원래 나무는 $n-1$개다.

(3)⇒(4). 연결 그래프가 간선 수 $n-1$보다 많은 간선을 가지면 순환이 있고, 그 순환의 간선 하나를 지워도 연결성이 유지된다(연습문제 4.12). 이를 반복해 순환이 없는 연결 그래프, 곧 나무로 만들 수 있으므로 원래 그래프는 적어도 $n-1$개의 간선을 가진다. 연결 그래프가 이미 간선을 $n-1$개 가지면 더 지울 여유가 없으므로 순환이 없다.

(4)⇒(3). 순환이 없는 그래프의 연결 성분 수를 c라 하자. (1)⇒(3)에 의해 각 성분은 나무이므로 간선 수는 성분별 n_i-1을 합한 $n-c$이다. 이것이 $n-1$이면 $c=1$이어서 연결이다. □

연결 그래프의 모든 꼭짓점을 포함하는 나무 부분그래프를 **신장 나무**(*spanning tree*)라 한다. 간선을 추가해도 연결성은 유지되지만, 나무에 간선을 하나 더하면 정리 4.7의 (2)에 의해 정확히 하나의 순환이 생긴다. 새 간선의 양 끝을 잇는 기존의 유일한 경로가 그 순환의 나머지 부분을 이룬다.

4.4 Euler 순회: 간선을 한 번씩

Euler 트레일(*Eulerian trail*)은 모든 간선을 정확히 한 번 지나는 트레일이고, 시작과 끝이 같은 경우 **Euler 회로**(*Eulerian circuit*)라 한다. 꼭짓점을 한 번씩 방문하는 Hamilton 경로와는 다른 문제다.

정리 4.8 (Euler 순회의 존재 조건) 간선이 적어도 하나 있는 유한 무향 그래프에서, 차수가 양수인 모든 꼭짓점이 같은 연결 성분에 있다고 하자. Euler 회로가 존재할 필요충분조건은 모든 차수가 짝수인 것이다. 서로 다른 끝점을 가진 Euler 트레일이 존재할 필요충분조건은 홀수 차수의 꼭짓점이 정확히 둘인 것이고, 그 두 끝점이 바로 그 홀수 차수 꼭짓점이다.

증명. 필요성. 순회 중 중간 꼭짓점을 지날 때마다 들어온 간선과 나간 간선이 짝을 이룬다. 닫힌 순회에서는 시작점(끝점과 같다)도 마찬가지이므로 모든 차수가 짝수다. 열린 순회에서는 양 끝에서만 짝이 하나씩 남으므로 그 두 꼭짓점만 홀수 차수다.

충분성(회로). 모든 차수가 짝수라고 하자. 임의의 비고립 꼭짓점에서 시작해, 미사용 간선을 따라 더 갈 수 없을 때까지 간선을 반복하지 않고 걷는다. 시작점이 아닌 곳에서 멈춘다면 그곳에 들어올 때와 나갈 때 쓴 간선의 수가 홀수이면서도 그 꼭짓점의 전체 차수는 짝수이므로, 미사용 간선이 적어도 하나 남아야 하므로 모순이다. 따라서 시작점에서 멈추어 닫힌 트레일을 얻는다. 아직 미사용 간선이 있으면 연결성 때문에 현재 트레일 위의 어떤 꼭짓점에서 미사용 간선으로 나갈 수 있다. 그 미사용 간선들만으로 그 꼭짓점을 시작점·끝점으로 하는 닫힌 트레일을 다시

만들고, 기존 트레일에 그 꼭짓점에서 끼워 넣는다. 간선이 유한하므로 이 절차는 모든 간선을 쓸 때 끝난다.

충분성(트레일). 홀수 차수 꼭짓점이 둘이면 그 둘 사이에 임시 간선을 하나 추가한다. 중복 간선이 생겨도 앞의 회로 논증은 다중 그래프에도 그대로 적용된다. 모든 차수가 짝수가 된 새 그래프에서 Euler 회로를 얻고, 그 회로에서 임시 간선을 지우면 원래 그래프의 열린 Euler 트레일을 얻는다. □

흔한 오류. 차수 조건만 맞고 비고립 연결 성분이 여러 개이면 한 번의 보행으로 모든 간선을 방문할 수 없다. 정리 4.8에서 "차수가 양수인 모든 꼭짓점이 같은 연결 성분에 있다"는 가정이 바로 이를 배제한다. 고립 꼭짓점 자체는 간선 순회에 영향을 주지 않는다.

4.5 연습문제와 해설

연습문제 4.9 간선이 11개인 숲에 꼭짓점이 15개 있다. 연결 성분은 몇 개인가?

풀이. 정리 4.7의 증명에서 쓴 숲의 간선 수 공식 $m = n - c$에 $n = 15$, $m = 11$을 대입하면 $c = 15 - 11 = 4$이다. 고립 꼭짓점도 하나의 성분으로 센다.

연습문제 4.10 완전 그래프 K_n에서 Euler 회로가 존재하는 $n \geq 2$를 판정하라.

풀이. K_n의 모든 차수는 $n-1$이고 그래프는 연결되어 있다. 정리 4.8에 의해 $n-1$이 짝수일 때, 곧 n이 홀수일 때, 그리고 그때에만 Euler 회로가 있다. $n = 2$에서는 두 꼭짓점의 차수가 모두 1(홀수가 둘)이므로 열린 Euler 트레일만 있다.

연습문제 4.11 나무에서 차수가 1인 꼭짓점의 수를 L, 차수가 3인 꼭짓점의 수를 B라 하자. 다른 차수를 가진 꼭짓점이 없고 꼭짓점이 둘 이상이면 $L = B + 2$임을 보여라.

풀이. 정리 4.2(손잡기 정리)에서 차수의 합은 $L \cdot 1 + B \cdot 3 = L + 3B$이고, 이는 간선 수 $L + B - 1$(정리 4.7)의 두 배인 $2(L + B - 1)$과 같다. $L + 3B = 2L + 2B - 2$를 정리하면 $L = B + 2$가 된다. 이 증명은 가능한 차수가 오직 1과 3뿐이라는 가정에 의존한다.

연습문제 4.12 연결 그래프에서 순환 위의 간선 하나를 지워도 연결인 이유와, 나무에서는 어떤 간선을 지워도 연결이 끊기는 이유를 설명하라.

풀이. 첫 경우에는 지운 간선을 쓰던 경로를 그 순환의 반대쪽 우회로로 바꿀 수 있으므로 모든 꼭짓점 쌍이 여전히 경로로 이어진다. 둘째 경우에 간선을 지운 뒤에도 연결이 유지된다면, 지운 간선의 두 끝 사이에 그 간선 말고 다른 경로가 있었다는 뜻이고, 그 경로와 지운 간선을 합치면 원래 그래프에 순환이 생겨 나무라는 가정(정리 4.7)에 모순이다.

제 5 장

이분 그래프, 색칠과 평면성

개요 이분 그래프(*bipartite graph*)는 꼭짓점을 두 그룹으로 나누어 모든 간선이 그룹 사이만 잇도록 할 수 있는 그래프이고, 평면 그래프(*planar graph*)는 간선이 서로 교차하지 않게 평면에 그릴 수 있는 그래프다. 이 장은 이분 그래프를 홀수 길이 순환의 유무로 특징짓고, 꼭짓점 색칠과 색칠수를 정의하여 최대 차수에 의한 상한을 증명한다. 평면 그래프에서는 Euler 공식 $n - m + f = 2$를 유도하고 이로부터 간선 수의 상한과 K_5, $K_{3,3}$의 비평면성을 보인 뒤, 평면 그래프의 여섯 색 정리를 증명한다. 이분 그래프에서의 매칭과 흐름 이론은 제19권 제6장에서 다룬다. 선행 지식: 경로, 순환, 연결 성분, 손잡기 정리.

5.1 이분성과 홀수 순환

정의 5.1 (이분 그래프) 꼭짓점을 서로소인 두 집합 U, W로 나누어 모든 간선이 U와 W 사이를 이으면 **이분 그래프**(*bipartite graph*)라 한다. 어느 한쪽 집합 안에는 간선이 없다. 이러한 분할 (U, W) 자체는 유일하지 않을 수 있다.

정리 5.2 유한 단순 무향 그래프가 이분 그래프일 필요충분조건은 홀수 길이 순환이 없는 것이다.

증명. 필요성. 이분 그래프의 보행은 U와 W를 번갈아 방문하므로, 시작점으로 되돌아오는 순환의 길이는 짝수다.

충분성. 각 연결 성분에서 뿌리를 하나 정하고, 뿌리에서 최단 경로의 길이가 짝수인 꼭짓점의 집합과 홀수인 꼭짓점의 집합으로 나눈다. 같은 짝홀성을 가진 두 꼭짓점이 간선으로 이어진다면, 각 꼭짓점까지의 뿌리 경로 둘과 그 간선을 합쳐 길이가 홀수인 닫힌 보행을 얻는다. 홀수 길이의 닫힌 보행에서 내부 꼭짓점이 반복되면 두 개의 더 짧은 닫힌 보행으로 자를 수 있고, 둘의 길이의 합이 홀수이므로 그중 하나는 홀수 길이다. 이를 반복하면 결국 홀수 길이 순환을 얻어 가정에 모순이다. 따라서 모든 간선은 짝홀성이 다른 두 부분을 잇고, 이 두 부분이 이분 그래프의 분할을 이룬다. □

이 증명은 너비 우선 탐색(*breadth-first search*)의 거리 짝홀성을 이용해 실제로 두 색으로 분할하거나, 충돌이 생기는 지점에서 홀수 순환을 찾아내는 알고리즘으로 바뀐다. 깊이 우선 탐색으로도 같은 문제를 해결할 수 있지만, 방문 순서 자체와 뿌리로부터의 거리를 혼동해서는 안 된다.

5.2 꼭짓점 색칠

정의 5.3 (꼭짓점 색칠과 색칠수) 인접한 꼭짓점들이 서로 다른 색을 갖도록 색을 배정하는 것을 **적절한 꼭짓점 색칠**(*proper vertex coloring*)이라 한다. 적절한 색칠에 필요한 최소 색 수를 **색칠수**(*chromatic number*) $\chi(G)$라 한다. 빈 그래프(꼭짓점도 없는 그래프)의 색칠수는 0으로 정하고, 꼭짓점은 있지만 간선이 없는 그래프는 1이다.

완전 그래프 K_n은 모든 두 꼭짓점이 인접하므로 n색이 필요하다. 길이 n인 **순환 그래프**(*cycle graph*) C_n은 n이 짝수면 2색으로 충분하고, n이 홀수면 3색이 필요하다. 홀수 순환에서 2색으로는 정리 5.2에 의해 불가능하지만, 번갈아 2색을 칠하다 마지막 꼭짓점에 세 번째 색을 쓰면 충분하다.

명제 5.4 (탐욕 색칠의 상한) 비어 있지 않은 유한 단순 그래프의 최대 차수를 Δ라 하면 $\chi(G) \le \Delta + 1$이다.

증명. 꼭짓점을 임의의 순서로 하나씩 색칠한다. 어떤 꼭짓점을 칠할 차례에 이미 색칠된 이웃은 많아야 Δ개이므로, 가능한 $\Delta + 1$개의 색 중 적어도 하나는 금지되지 않는다. 그 색을 쓰면 이미 색칠된 어떤 이웃과도 충돌하지 않는다. $\square$

이 상한은 항상 최소 색 수를 주는 것은 아니다. 가운데 꼭짓점 하나에 나머지 모든 꼭짓점이 연결된 별 그래프는 가운데 차수가 매우 커도 두 색이면 충분하다. 또한 색칠 순서에 따라 탐욕 알고리즘이 실제로 쓰는 색 수가 달라질 수 있다. 간선에 색을 칠하는 간선 색칠이나 지도의 영역을 칠하는 문제는 대상이 달라 이 절의 결과를 그대로 적용할 수 없고 추가 변환이 필요하다.

5.3 평면 그래프와 Euler 공식

정의 5.5 (평면 그래프) 간선이 끝점 이외에서 서로 교차하지 않게 평면에 그릴 수 있는 그래프를 **평면 그래프**(*planar graph*)라 한다. 이미 그러한 그림 하나를 고정한 것을 평면에 매장된 그래프로 구분해서 부르기도 한다. 그 그림이 평면을 나누는 각 영역을 **면**(*face*)이라 하며, 무한히 넓은 바깥 영역도 하나의 면으로 센다.

정리 5.6 (평면 Euler 공식) 유한 연결 평면 그래프의 꼭짓점, 간선, 면의 수를 각각 n, m, f라 하면

$$n - m + f = 2 \tag{5.1}$$

이다.

증명의 핵심. 나무이면 정리 4.7에 의해 $m = n - 1$이고 면은 바깥 영역 하나뿐이어서 $f = 1$이므로 식 (5.1)이 성립한다. 순환이 있으면 그 위의 간선을 하나 지운다. 이 간선은 두 개의 서로 다른 면의 경계를 이루고 있었으므로(평면의 단순 닫힌 곡선이 안과 밖을 나눈다는 위상적 성질에 의해, 순환은 평면을 적어도 두 면으로 나눈다), 간선을 지우면 그 두 면이 하나로 합쳐져 연결성을 유지하면서 m과 f가 각각 1씩 줄어든다. 따라서 $n - m + f$의 값은 변하지 않는다. 이를 반복해 순환을 모두 없애 나무로 만들면 앞의 경우로 환원되어 결과를 얻는다. 여기서 쓴 평면의 위상적 성질(Jordan 곡선 정리)의 완전한 증명은 이 초등적인 장의 범위를 벗어난다. $\square$

연결 성분이 c개인 평면 그래프에서는 $n - m + f = 1 + c$이다. 서로 떨어진 성분들을 교차 없는 $c - 1$개의 간선으로 이으면 면의 수가 변하지 않으면서 연결 그래프가 되므로 연결인 경우로 환원된다.

명제 5.7 $n \geq 3$인 유한 단순 연결 평면 그래프는 $m \leq 3n - 6$을 만족한다. 삼각형이 없으면 $m \leq 2n - 4$이다.

증명. 각 면의 경계 길이를, 그 면에 인접한 간선의 출현 횟수로 센다(다리, 곧 지우면 그래프를 끊는 간선은 양쪽에서 같은 면에 속해 같은 면의 경계에 두 번 나올 수 있다). 모든 간선은 정확히 두 면(또는 한 면에 두 번)의 경계에 기여하므로 경계 길이의 전체 합은 $2m$이다. 단순 연결 그래프에서 $n \geq 3$이면 각 면의 경계 길이가 적어도 3이므로 $3f \leq 2m$이다. Euler 공식 (5.1)의 $f = 2 - n + m$을 대입하면 $3(2 - n + m) \leq 2m$, 곧 $m \leq 3n - 6$을 얻는다. 삼각형이 없으면 각 면의 경계 길이가 적어도 4이므로 $4f \leq 2m$이고, 같은 방식으로 $m \leq 2n - 4$를 얻는다. □

예제 5.8 K_5는 $n = 5$, $m = 10$인데 $10 > 3 \cdot 5 - 6 = 9$이므로 명제 5.7에 의해 평면 그래프가 아니다. 두 꼭짓점 집합의 크기가 각각 p, q이고 모든 간선이 두 집합 사이를 잇는 **완전 이분 그래프**(*complete bipartite graph*) $K_{p,q}$ 가운데, $K_{3,3}$은 삼각형이 없고(이분 그래프이므로 정리 5.2에 의해 홀수 순환이 없다) $n = 6$, $m = 9$인데 $9 > 2 \cdot 6 - 4 = 8$이므로 평면 그래프가 아니다.

명제 5.7의 간선 수 조건은 필요조건일 뿐 충분조건은 아니다. 조건을 만족한다고 반드시 평면 그래프인 것은 아니다. 예를 들어 $K_{3,3}$의 간선마다 중간 꼭짓점을 하나씩 넣으면 $n = 15$, $m = 18$이 되어 두 상한을 모두 만족하지만, 원래의 교차 장애는 사라지지 않으므로 여전히 평면 그래프가 아니다. 중간 꼭짓점들을 없애고 간선을 다시 이어 붙이면 원래 그래프의 평면 그림이 생겨야 하는데, $K_{3,3}$ 자체가 평면 그래프가 아니기 때문이다.

5.4 평면 그래프의 여섯 색 정리

정리 5.9 (여섯 색 정리) 유한 단순 평면 그래프는 6색으로 적절하게 색칠할 수 있다.

증명. 꼭짓점 수에 대한 귀납법을 쓴다. $n \leq 2$이면 명백하다. 각 연결 성분을 따로 색칠할 수 있으므로 연결인 경우를 보면 충분하다. 명제 5.7에 의해 $2m \leq 6n - 12 < 6n$이므로 손잡기 정리(정리 4.2)에서 평균 차수는 6보다 작다. 따라서 차수가 5 이하인 꼭짓점 v가 존재한다. v를 지운 평면 그래프는 꼭짓점이 하나 적으므로 귀납 가정에 의해 6색으로 색칠된다. v의 이웃은 많아야 5개이므로 금지되는 색도 많아야 5개이고, 남은 색 중 하나로 v를 색칠하면 전체가 적절한 6색 색칠이 된다. □

역사. 더 강한 네 색 정리(모든 단순 평면 그래프가 4색으로 적절하게 색칠된다는 명제)가 성립하지만, 그 증명은 정리 5.9와 같은 짧은 평균 차수 논증만으로는 나오지 않는다. 네 색 정리는 1976년 Kenneth Appel과 Wolfgang Haken이 컴퓨터로 천 개가 넘는 환원 가능한 배치(모든 평면 그래프가 반드시 포함하는 불가피 집합)를 일일이 검사하여 증명했으며, 사람이 손으로 모두 검증할 수 없는 분량의 경우 나누기를 쓴 최초의 주요 정리로 꼽힌다. 여기서 증명한 결과가 어디까지나 여섯 색 상한이라는 점을 분명히 해야 한다. 그래프의 정확한 색칠수를 계산하는 문제, 어떤 상한을 증명하는 문제, 특정한 색칠을 실제로 구성하는 문제는 서로 연결되지만 같은 과제는 아니다.

5.5 연습문제와 해설

연습문제 5.10 순환이 없는 그래프는 왜 이분 그래프인가? 고립 꼭짓점은 어떻게 처리하는가?

풀이. 순환이 없으면 홀수 길이 순환도 없으므로 정리 5.2를 적용하면 이분 그래프다. 직접 구성하려면 각 나무 성분에서 뿌리로부터의 거리의 짝홀성으로 나누어도 된다. 고립 꼭짓점은 간선이 없어 어느 쪽에 넣어도 이분 조건을 깨지 않으므로 두 부분 중 아무 쪽에 넣어도 된다.

연습문제 5.11 단순 연결 평면 그래프가 꼭짓점 8개, 간선 15개를 가지면 면은 몇 개인가? 이 계산만으로 그러한 그래프가 존재함을 알 수 있는가?

풀이. 존재한다면 식 (5.1)에 의해 $f = 2 - 8 + 15 = 9$이다. 이 관계는 평면 그래프라는 모형에서의 필요조건이므로, 숫자를 대입해 식이 성립한다는 사실만으로 그러한 그래프의 존재가 증명되지는 않는다 (명제 5.7로 $m \le 3 \cdot 8 - 6 = 18$이라는 필요조건은 만족하지만, 이 역시 충분조건은 아니다). 실제 존재를 보이려면 별도의 구성이나 존재 정리가 필요하다.

연습문제 5.12 $K_{2,5}$가 이분 그래프라는 사실만으로 평면 여부를 결론 내릴 수 있는가?

풀이. 그럴 수 없다. 이분 그래프 가운데에는 예제 5.8의 $K_{3,3}$처럼 평면이 아닌 것도 있다. $K_{2,5}$ 자체는 두 꼭짓점 사이에 서로 교차하지 않는 다섯 개의 곡선을 그리고 각 곡선에 중간 꼭짓점을 하나씩 넣으면 평면에 그릴 수 있다. 중요한 것은 이분성과는 별개인 구체적인 구성이다.

연습문제 5.13 최소 차수가 6인 유한 단순 평면 그래프가 존재할 수 없는 이유를 설명하라.

풀이. 그러한 그래프의 각 연결 성분은 최소 차수가 6이므로 꼭짓점이 적어도 7개다. 한 연결 성분에 대해 손잡기 정리(정리 4.2)는 $2m \ge 6n$을 주지만, 명제 5.7의 평면 상한은 $2m \le 6n - 12$를 준다. 두 부등식을 함께 쓰면 $6n \le 2m \le 6n - 12$가 되어 모순이므로 그러한 평면 그래프는 존재하지 않는다.

제 6 장

매칭과 네트워크 흐름

개요 매칭(*matching*)은 그래프에서 어떤 두 간선도 끝점을 공유하지 않도록 고른 간선의 집합이고, 네트워크 흐름(*network flow*)은 방향 그래프의 각 간선에 정해진 용량 아래에서 출발점에서 도착점으로 보낼 수 있는 흐름을 다루는 틀이다. 이 장은 교대 경로와 증대 경로로 매칭의 최대성을 특징짓는 데서 출발하여, 이분 그래프에서 한쪽을 모두 포화하는 매칭이 존재할 조건을 Hall의 결혼 정리로 서술하고, 흐름·용량·절단의 개념을 세운 뒤 최대 흐름이 최소 절단의 용량과 같다는 정리를 증명한다. 마지막으로 이분 그래프의 매칭 문제를 네트워크 흐름 문제로 바꾸는 표준적인 방법을 설명한다. 선행 지식: 이분 그래프, 유한 집합, 선형 부등식.

6.1 매칭과 교대 경로

정의 6.1 (매칭과 포화) 그래프 G에서 **매칭**(*matching*)은 어떤 두 간선도 끝점을 공유하지 않는 간선의 집합이다. 매칭 M의 간선에 닿은 꼭짓점을 M에 **포화**되었다고 한다. 이분 그래프의 한쪽 U를 모두 포화하는 매칭은 U의 각 원소에 서로 다른 이웃을 하나씩 배정한다.

극대 매칭(*maximal matching*)은 간선을 하나 더 추가할 수 없는 매칭이고, **최대 매칭**(*maximum matching*)은 모든 매칭 가운데 간선 수가 가장 많은 것이다. 최대이면 극대이지만 역은 성립하지 않는다. 네 꼭짓점을 잇는 경로 1–2–3–4에서 가운데 간선 $\{2,3\}$ 하나만 고른 매칭은 간선을 더 추가할 수 없으므로 극대이지만, 양 끝의 두 간선 $\{1,2\},\{3,4\}$를 고른 매칭보다 크기가 작다. 주어진 매칭 M에 대해 M 밖의 간선과 안의 간선을 번갈아 지나는 경로를 **교대 경로**(*alternating path*)라 한다. 양 끝이 포화되지 않고 첫 간선과 마지막 간선이 M 밖에 있는 단순 교대 경로는 **증대 경로**(*augmenting path*)다. 증대 경로 위에서 M 안팎을 서로 바꾸면(M 안의 간선은 빼고 밖의 간선은 더하면) 매칭 크기가 1 증가한다.

명제 6.2 (증대 경로 판정) 유한 그래프에서 매칭 M이 최대일 필요충분조건은 M에 대한 증대 경로가 없는 것이다.

증명. 증대 경로가 있으면 매칭을 늘릴 수 있으므로 M은 최대가 아니다. 반대로 M보다 큰 매칭 M'이 있다고 하면, 대칭차 $M \triangle M'$만 남긴 부분그래프에서 각 꼭짓점의 차수는 많아야 2이고 각 간선은 두 매칭 M, M'에서 번갈아 나온다. 따라서 이 부분그래프의 비자명한 연결성분은 모두 경로이거나 짝수 길이의 순환이다. 전체에서 M'의 간선이 더 많으므로, 어느 경로 성분은 M'의 간선을 M의 간선보다 하나 더 가진다. 그 경로의 양 끝은 M에 포화되지 않으므로, 그 경로는 M의 증대 경로다. □

6.2 Hall 결혼 정리

이분 그래프 $G = (U, W; E)$에서 $S \subseteq U$의 모든 이웃의 집합을 $N(S)$로 쓴다.

정리 6.3 (Hall) 유한 이분 그래프에서 U 전체를 포화하는 매칭이 존재할 필요충분조건은 모든 $S \subseteq U$에 대해

$$|N(S)| \geq |S| \tag{6.1}$$

인 것이다. 이 조건을 **Hall 조건**이라 한다.

증명. 매칭이 있으면 S의 서로 다른 꼭짓점들이 서로 다른 이웃을 받으므로 조건의 필요성은 자명하다.

조건이 성립한다고 가정하고 크기가 최대인 매칭 M을 고른다. 포화되지 않은 $u_0 \in U$가 있다면, u_0에서 M 밖의 간선으로 W에 가고 M의 간선으로 U에 돌아오는 교대 경로로 도달 가능한 꼭짓점들을 조사한다. 이렇게 도달한 U의 꼭짓점들의 집합을 S, W의 꼭짓점들의 집합을 T라 한다. S의 모든 이웃은 T에 속한다. 매칭 간선으로 연결된 이웃은 해당 꼭짓점에 도착할 때 이미 거친 것이고, 그 밖의 이웃은 다음 단계에서 도달하기 때문이다. 따라서 $N(S) = T$다.

도달한 W의 꼭짓점 가운데 포화되지 않은 것이 있으면 증대 경로를 얻어 M의 최대성에 모순이다. 그러므로 T의 모든 꼭짓점은 포화되어 있고 그 짝은 $S \setminus \{u_0\}$에 속한다. 반대로 S의 u_0 이외의 꼭짓점은 모두 이런 매칭 간선으로 T에서 도달한다. 따라서 $|T| = |S| - 1$이다. 이는 $N(S) = T$와 식 (6.1)에 모순이다. 결국 미포화된 u_0는 존재하지 않으므로 U 전체가 포화된다. □

예제 6.4 작업자 $1, 2, 3$은 작업 a, b만 할 수 있고 작업자 4는 c, d를 할 수 있다고 한다. 양쪽 원소가 각각 네 개이고 모든 작업자에게 이웃(할 수 있는 작업)이 있지만, 완전 배정은 불가능하다. $S = \{1, 2, 3\}$에서 $N(S) = \{a, b\}$이므로 $|N(S)| = 2 < 3 = |S|$이기 때문이다. 한 사람씩의 선택지만 검사하면 이런 집단 전체의 부족을 놓치므로, Hall 조건은 반드시 모든 부분집합 S에 대해 검사해야 한다.

따름정리 6.5 (정규 이분 그래프의 완전 매칭) 유한 이분 그래프 $G = (U, W; E)$가 d-**정규**(d-*regular*)라는 것은 U와 W의 모든 꼭짓점의 차수가 d로 같다는 뜻이다. $d \geq 1$인 유한 d-정규 이분 그래프는 양쪽을 모두 포화하는 매칭을 가진다.

증명. 전체 간선 수를 양쪽에서 세면 $d|U| = d|W|$이므로 두 부분의 크기가 같다. $S \subseteq U$에서 나오는 간선은 $d|S|$개이고 모두 $N(S)$로 들어간다. $N(S)$로 들어갈 수 있는 전체 간선 수는 $N(S)$의 각 꼭짓점의 차수가 d이므로 많아야 $d|N(S)|$다. 따라서 $d|S| \leq d|N(S)|$, 곧 $|S| \leq |N(S)|$이고 모든 $S \subseteq U$에 대해 Hall 조건이 성립하여 정리 6.3을 적용한다. 대칭적인 논증(또는 U, W를 바꾼 같은 정리의 적용)으로 W 쪽도 포화됨을 얻는다. □

역사 (이름의 유래). Hall의 결혼 정리는 Philip Hall이 1935년에 증명하였다. "결혼 정리"라는 이름은 이 정리를, 여러 명의 남자 각각을 자신이 아는 여자들 가운데 한 명과 서로 다르게 결혼시킬 수 있는 조건을 묻는 문제로 서술한 데서 비롯한다.

6.3 흐름, 용량, 절단

유한 방향 네트워크에 서로 다른 출발점 s와 도착점 t를 정하고, 각 간선 e에 유한한 **용량**(*capacity*) $c_e \geq 0$을 준다. **흐름**(*flow*) f는 각 간선에 $0 \leq f_e \leq c_e$를 배정하면서 s, t가 아닌 모든 중간 꼭짓점에서 유입량과 유출량이 같다는 조건(흐름 보존)을 만족하는 것이다. 흐름의 **값** $|f|$는 s에서

나가는 양에서 s로 들어오는 양을 뺀 값이다. 출발점 s를 포함하고 도착점 t를 포함하지 않는 꼭짓점 집합 S가 **절단**(*cut*)을 정한다. 절단의 용량 $c(S, S^c)$는 S에서 바깥(S^c)으로 나가는 간선들의 용량의 합이다. 반대 방향(바깥에서 S로 들어오는) 간선의 용량은 이 합에 넣지 않는다.

보조정리 6.6 (약한 쌍대성) 임의의 가능한 흐름의 값은 임의의 절단의 용량 이하이다.

증명. S 안의 꼭짓점들에서 유출량에서 유입량을 뺀 값을 모두 합하면, S 내부를 잇는 간선의 기여는 서로 상쇄되고 중간 꼭짓점 각각의 보존식의 기여도 0이므로, 남는 것은 S의 경계를 지나는 간선들뿐이다. 따라서

$$|f| = \sum_{e:\, S \to S^c} f_e \;-\; \sum_{e:\, S^c \to S} f_e \;\le\; \sum_{e:\, S \to S^c} c_e = c(S, S^c) \tag{6.2}$$

이다. 둘째 부등식에서 두 번째 합의 비음성과, 첫째 합의 각 항에서 $f_e \le c_e$라는 사실을 썼다. □

흐름 f를 더 보낼 수 있는지를 따지는 **잔여 네트워크**(*residual network*)는 원래 간선마다 **정방향 용량** $c_e - f_e$와 **역방향 용량** f_e를 가진다. 역방향 간선은 이미 보낸 흐름을 취소하고 다른 경로로 재배정하는 기능을 한다. 원래 네트워크에 반대 방향의 간선이 이미 있으면, 잔여 간선들을 서로 다른 간선으로 따로 관리하거나 같은 방향의 용량을 정확히 합쳐서 관리한다.

6.4 최대 흐름과 최소 절단

핵심 수식

Hall 조건:
$$|N(S)| \ge |S| \quad (\forall S \subseteq U), \tag{6.3}$$

최대 흐름 최소 절단:
$$\max_{f} |f| = \min_{S} c(S, S^c). \tag{6.4}$$

정리 6.7 (최대 흐름 최소 절단) 유한 방향 네트워크의 유한하고 비음인 실수 용량에 대해, 최대 흐름의 값은 최소 절단의 용량과 같다. 모든 용량이 정수이면 정수값을 갖는 간선 흐름으로 최대값을 달성할 수 있다.

증명. 먼저 최대 흐름이 존재함을 보인다. 가능한 흐름들의 집합은, 각 간선의 흐름값을 닫힌 유계 구간 $[0, c_e]$에 가두고 흐름 보존이라는 선형 등식들을 추가로 만족하는 유한 차원 공간의 부분집합이므로 닫히고 유계이며, 영 흐름을 포함해 공집합이 아니다. 따라서 이 집합은 콤팩트하고, 흐름 값은 연속함수이므로 콤팩트 집합 위에서 최댓값을 가진다(유한 차원 해석학의 최대값 정리).

최대 흐름 f의 잔여 네트워크에 s에서 t로 가는 양의 잔여 용량을 가진 경로가 있다면, 그 경로의 최소 잔여 용량만큼 흐름을 늘릴 수 있어 f가 최대라는 가정에 모순이다. s에서 잔여 경로로 도달 가능한 꼭짓점의 집합을 S라 하면 $t \notin S$이고, S에서 바깥으로 나가는 원래 간선은 모두 포화되어 있다(그렇지 않으면 정방향 잔여 간선으로 더 멀리 도달할 수 있다). 바깥에서 S로 들어오는 원래 간선에는 흐름이 0이다(그렇지 않으면 그 역방향 잔여 간선으로 바깥에서 S에 도달할 수 있어 S의 정의에 어긋난다). 따라서 식 (6.2)의 두 부등식이 모두 등식이 되어 $|f| = c(S, S^c)$를 얻는다. 보조정리 6.6의 약한 쌍대성과 합치면, 이 흐름의 값과 이 절단의 용량이 각각 최댓값과 최솟값이며 서로 같다.

용량이 모두 정수이면, 영 흐름에서 시작해 잔여 s–t 경로를 하나씩 고르고 그 경로의 최소 잔여 용량만큼 흐름을 증가시킨다. 용량이 모두 정수이므로 이 과정에서 모든 흐름과 잔여 용량은 정수로 유지되고, 매번 흐름의 값이 적어도 1 증가한다. 흐름의 값은 s의 총 유출 용량 이하이므로 유한 번 뒤에는 더 이상 증대 경로가 남지 않는다. 앞의 도달 가능 집합을 이용한 논증을 이 시점의 정수 흐름에 적용하면, 그 흐름이 최대임을 알 수 있다. □

흔한 오류. 임의의 실수 용량 네트워크에서 아무 증대 경로나 골라 흐름을 늘려 가는 절차가 유한 번에 끝난다는 것을, 위 증명은 보장하지 않는다. (실제로 증대 경로를 나쁘게 고르면 무한히 계속되면서 최댓값에 수렴조차 하지 않는 예가 있다.) 최대 흐름 최소 절단 정리 자체의 성립과, 그 최댓값을 찾는 특정 알고리즘의 종료 여부·속도는 별개의 문제로 구분해야 한다.

> **예제 6.8** 간선의 용량이 $s \to a : 3$, $s \to b : 2$, $a \to t : 2$, $b \to t : 3$, $a \to b : 1$이라고 한다. 경로 $s \to a \to t$에 2, $s \to b \to t$에 2, $s \to a \to b \to t$에 1을 보내면 흐름의 값은 5다 (간선 $s \to a$에는 $2+1=3$, 간선 $b \to t$에는 $2+1=3$이 흐르고, 나머지 간선은 모두 포화된다). 절단 $S = \{s\}$의 용량도 $3+2=5$이므로, 이 흐름이 최대 흐름이고 이 절단이 최소 절단임이 즉시 인증된다. 가능한 흐름 하나는 최대값의 하한 증거이고, 절단 하나는 최솟값의 상한 증거의 역할을 한다.

6.5 매칭을 흐름으로 바꾸기

이분 그래프 $G = (U, W; E)$에서 $s \to U$, $U \to W$(E의 각 간선을 그대로), $W \to t$의 간선을 새로 만들고 모든 용량을 1로 놓는다. 정수 흐름에서는 각 U와 W의 꼭짓점이 많아야 한 단위의 흐름만 전달한다(모든 간선 용량이 1이기 때문이다). 따라서 값이 k인 정수 흐름은 크기 k의 매칭과 일대일로 대응한다. 역으로 매칭의 각 간선에 대해 s에서 t까지 한 단위를 흘리면 그 매칭에 대응하는 정수 흐름을 얻는다. 실수 흐름 하나의 간선값이 모두 0 또는 1인 것은 일반적으로 아니지만, 정리 6.7의 정수 용량에 대한 부분에 의해 최댓값을 달성하는 정수 흐름이 적어도 하나 존재한다. “모든 최적해가 정수다”와 “정수인 최적해가 존재한다”는 서로 다른 주장이므로 이 둘을 구분해야 한다.

6.6 연습문제와 해설

> **연습문제 6.9** $U = \{1, 2, 3\}$, $W = \{a, b, c\}$이고 이웃이 $N(1) = \{a, b\}$, $N(2) = \{b\}$, $N(3) = \{a, c\}$일 때, U를 포화하는 매칭을 구하라.

풀이. 2에는 b, 1에는 a, 3에는 c를 배정한다. 모든 이웃 부분집합을 검사해 Hall 조건을 확인할 수도 있지만, 실제로 매칭 하나를 제시하면 이 사례에서 완전 매칭이 존재한다는 증명으로 충분하다.

> **연습문제 6.10** 네 꼭짓점을 잇는 경로에서 극대 매칭이 최대가 아닐 수 있음을 증대 경로로 설명하라.

풀이. 꼭짓점을 순서대로 $1, 2, 3, 4$라 하고 $M = \{\{2, 3\}\}$로 둔다. M은 간선을 더 추가할 수 없으므로 극대 매칭이다. 전체 경로 1–2–3–4의 간선은 (M) 밖, 안, 밖의 순서로 교대하고 양 끝 $1, 4$가

미포화이므로 이 경로는 증대 경로다. 경로 위에서 안팎을 뒤집으면 $\{\{1,2\},\{3,4\}\}$가 되어 매칭 크기가 1에서 2로 증가한다.

연습문제 6.11 예제 6.8의 흐름 예에서 간선 $a \to b$를 지우면 최대값은 얼마인가?

풀이. 두 경로 $s \to a \to t$와 $s \to b \to t$에 각각 2를 보내 값 4를 만든다. 절단 $S = \{s, a\}$에서 바깥으로 나가는 간선은 $s \to b$와 $a \to t$뿐이고 그 용량의 합이 $2 + 2 = 4$다. 정리 6.7에 의해 흐름 값과 절단 용량이 모두 4로 일치하므로, 이 흐름이 최대이고 최대값은 정확히 4다.

연습문제 6.12 실수 용량의 최대 흐름 존재 증명에서 유한한 간선 수와 유한한 용량을 사용한 위치를 설명하라.

풀이. 흐름의 변수들을 유한 차원 유클리드 공간(차원이 간선의 개수)의 한 점으로 두고, 각 좌표를 닫힌 유계 구간 $[0, c_e]$에 제한하였다. 간선 수가 유한해야 이 공간의 차원이 유한하고, 각 용량 c_e가 유한해야 그 구간이 유계가 된다. 흐름 보존식은 선형 등식이므로 닫힌 부분집합을 정하고, 그 결과 가능한 흐름들의 집합이 콤팩트해진다. 무한 네트워크(꼭짓점이나 간선이 무한히 많은 경우)에는 이 유한 차원 논증을 그대로 적용할 수 없다.

추가 읽기

MIT의 공개강의 *Mathematics for Computer Science* 자료는 그래프, 계수, 점화식, 생성함수를 다루는 장을 제공하며, 이 장의 설명과 예제는 그 자료의 본문을 그대로 옮기지 않고 독자적으로 구성하였다. 이후의 주제로는 그래프 알고리즘의 실행 시간 분석, Ramsey 이론, 극값 조합론, 확률적 방법, 매트로이드와 조합적 최적화가 있다.

제 20 권

확률론

제20권은 불확실성을 측도론에 기초한 확률공간으로 다루는 확률론이다. 제1–3장은 표본공간·사건·확률의 공리, 계수법과 유한 확률모형, 조건부 확률과 Bayes 공식과 독립성을 다루고, 제4–7장은 확률변수와 분포함수, 기댓값·분산·공분산, 핵심 확률분포와 변환 도구, 결합분포와 다변수 변환을 다룬다. 제8–9장은 조건부 기댓값과 정보의 수학, 변환함수와 분포의 식별, 모멘트를 다루고, 제10–12장은 확률변수열의 여러 수렴 개념과 반례, 큰수법칙·중심극한정리·델타 방법, 확률 부등식과 집중으로 극한 이론을 정리한다.

제 1 장

표본공간, 사건, 확률의 공리

개요 확률공간(*probability space*)은 무작위 현상에서 나올 수 있는 결과와 그 결과들에 부여할 확률을 공리적으로 규정하는 세 쌍 $(\Omega, \mathcal{F}, \mathbb{P})$이다. 이 장은 표본공간과 사건의 언어를 세우는 데서 출발하여, 사건의 합집합·교집합·여집합·대칭차 연산과 σ-대수의 공리를 정의하고, Kolmogorov의 확률 공리로부터 기본 계산 규칙, 포함배제 공식, 가산가법성의 결과인 합집합 상계와 확률의 연속성 정리를 유도한다. 마지막으로 "확률이 0이다"라는 말이 뜻하는 바를 가산 무한 표본공간과 비가산 무한 표본공간에서 대비하여 설명한다. 선행 지식: 집합의 합집합과 교집합, 유한합, 수열의 극한. 측도론의 전문 용어는 필요한 곳에서만 도입한다.

1.1 무엇을 무작위라고 모델링하는가

확률 모형은 관찰하기 전의 불확실성을 수학적으로 표현한다. 동전을 던지면 실제 결과는 앞면 또는 뒷면 하나이지만, 결과를 보기 전에는 가능한 결과들의 모임과 그 각각에 부여할 확률을 정해야 한다. 이때 "가능하다"와 "같은 확률로 일어난다"는 서로 다른 주장이다. 동전의 모양이 두 면을 가진다는 사실만으로 앞면의 확률이 $1/2$이라는 결론이 나오지는 않는다. 대칭성, 실험 조건, 반복 관찰 또는 별도의 가정을 통해 그 값을 정한다.

확률 문제를 풀 때에는 먼저 세 가지를 분리한다. 무엇을 한 번의 실험으로 보는가, 어떤 결과를 서로 다른 것으로 구별하는가, 어떤 사건의 확률을 구하는가이다. 두 주사위를 던지는 실험에서 첫째 주사위와 둘째 주사위를 구별하면 $(1,2)$와 $(2,1)$은 다른 결과다. 반면 합만 기록하면 두 결과 모두 3으로 관찰된다. 기록을 거칠게 만든다고 해서 새로운 기록값들이 같은 확률을 갖는 것은 아니다.

정의 1.1 (확률공간) **확률공간**(*probability space*)은 세 대상 $(\Omega, \mathcal{F}, \mathbb{P})$으로 이루어진다. Ω는 **표본공간**(*sample space*)이고, $\mathcal{F}$는 확률을 부여할 **사건**(*event*)들의 모임이며, $\mathbb{P} : \mathcal{F} \to [0,1]$은 **확률측도**(*probability measure*)다. 사건 A가 일어났다는 것은 실제 결과 ω가 A에 속한다는 뜻이다.

유한 표본공간에서는 보통 모든 부분집합을 사건으로 허용한다. 곧 $\mathcal{F} = 2^{\Omega}$로 둔다. 연속적인 표본공간에서는 모든 부분집합에 일관된 길이나 확률을 부여할 수 있는지에 별도의 문제가 생기므로, 사건의 모임을 따로 지정한다. 초급 계산에서 나타나는 구간과 그 가산 합집합 등은 뒤에서 정의할 Borel 사건에 들어가므로 일반적인 계산을 하는 데 지장이 없다.

예제 1.2 (두 주사위의 표본공간) 공정하고 서로 독립인 두 주사위를 구별해서 던진다. 표본공간은

$$\Omega = \{(i,j) : i, j \in \{1,2,3,4,5,6\}\}$$

이며 36개의 결과가 각각 확률 $1/36$을 갖는다. 합이 7인 사건은

$$A = \{(1,6),(2,5),(3,4),(4,3),(5,2),(6,1)\}$$

이므로 $\mathbb{P}(A) = 1/6$이다. 합이 2인 사건에는 $(1,1)$ 하나만 있으므로 그 확률은 $1/36$이다. 가능한 합은 2부터 12까지 11개지만, 각각의 합이 확률 $1/11$을 갖는 것은 아니다.

1.2 사건의 논리와 집합 연산

사건 $A \cup B$는 적어도 하나가 일어나는 사건, $A \cap B$는 둘 다 일어나는 사건이다. $A^c = \Omega \setminus A$는 A가 일어나지 않는 사건이다. "또는"은 별도의 언급이 없으면 둘 다 일어나는 경우도 포함한다. 정확히 하나만 일어나는 사건은 **대칭차**(*symmetric difference*)

$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$

로 표현한다. **서로 배반**(*mutually exclusive*)인 사건은 $A \cap B = \emptyset$을 만족하는 사건이다. 배반은 동시에 일어날 수 없다는 뜻이고, *independent*(독립)은 한 사건의 정보를 알아도 다른 사건의 확률이 바뀌지 않는다는 뜻이다. 두 개념은 제20권 제3장에서 엄밀하게 구별한다.

드모르간 법칙은 복잡한 사건을 여사건으로 바꿀 때 유용하다.

$$(A \cup B)^c = A^c \cap B^c, \qquad \left(\bigcap_{k=1}^{\infty} A_k\right)^c = \bigcup_{k=1}^{\infty} A_k^c.$$

예를 들어 "열 번 중 적어도 한 번 성공"의 여사건은 "열 번 모두 실패"다. 성공 횟수를 하나씩 나누어 더하는 것보다 여사건 하나를 계산하는 편이 쉬울 수 있다.

정의 1.3 (**σ-대수**) $\mathcal{F} \subseteq 2^{\Omega}$가 다음 조건을 만족하면 **$\sigma$-대수**($\sigma$-*algebra*)라 한다.

(1) $\Omega \in \mathcal{F}$.

(2) $A \in \mathcal{F}$이면 $A^c \in \mathcal{F}$.

(3) $A_1, A_2, \dots \in \mathcal{F}$이면 $\bigcup_{n=1}^{\infty} A_n \in \mathcal{F}$.

이 조건들로부터 $\emptyset \in \mathcal{F}$와, 드모르간 법칙을 통한 가산 교집합에 대한 닫힘도 따라온다.

가산(*countable*)이라는 말은 사건들을 자연수로 나열할 수 있다는 뜻이다. 이 조건은 무한히 반복되는 실험이나 수열의 극한을 사건으로 다루는 데 필요하다. 유한집합의 모든 부분집합, 실수축의 Borel 집합족, $\{\emptyset, \Omega\}$는 각각 σ-대수의 예다. 마지막 예는 관찰 가능한 정보가 전혀 없는 가장 거친 사건 체계다.

1.3 세 공리와 그 즉각적인 결과

정의 1.4 (**확률의 공리**) 확률측도 $\mathbb{P}$는 다음을 만족한다.

$$\mathbb{P}(A) \geq 0 \qquad (A \in \mathcal{F}), \tag{1.1}$$

$$\mathbb{P}(\Omega) = 1, \tag{1.2}$$

$$\mathbb{P}\left(\bigcup_{n=1}^{\infty} A_n\right) = \sum_{n=1}^{\infty} \mathbb{P}(A_n) \qquad \text{서로 배반인 } A_n \text{에 대하여.} \tag{1.3}$$

식 (1.3)의 성질을 **가산가법성**(*countable additivity*)이라 한다. 서로 겹치는 사건에는 이 식을 그대로 적용할 수 없다.

역사 (공리화의 역사). 확률의 공리적 정식화는 Andrey Kolmogorov가 1933년 저서 *Grundbegriffe der Wahrscheinlichkeitsrechnung*에서 측도론을 바탕으로 제시하였다. 그 이전에도 Blaise Pascal과 Pierre de Fermat은 1654년 도박 문제를 주고받은 편지에서 유한 표본공간의 확률 계산을 체계화하였고, Pierre-Simon Laplace는 1812년 저서 *Théorie analytique des probabilités*에서 확률을 "같은 정도로 가능한 경우의 수의 비"로 정의하였다. Kolmogorov의 공리는 이 고전적 정의가 다루지 못하는 연속적 표본공간과 무한한 사건열을 하나의 틀로 통합한다.

명제 1.5 (기본 계산 규칙) 확률공간의 사건 A, B에 대해 다음이 성립한다.

$$\mathbb{P}(\emptyset) = 0, \qquad \mathbb{P}(A^c) = 1 - \mathbb{P}(A),$$
$$A \subseteq B \implies \mathbb{P}(A) \le \mathbb{P}(B), \qquad \mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B).$$

증명. $A_1 = \Omega$, $A_2 = A_3 = \cdots = \emptyset$에 가산가법성을 적용하면 $1 = 1 + \sum_{n=2}^{\infty} \mathbb{P}(\emptyset)$을 얻으므로, 급수가 수렴하려면 $\mathbb{P}(\emptyset) = 0$이어야 한다. 비음수성과 함께 이 등식은 $\mathbb{P}(\emptyset) \ge 0$과 모순되지 않는 유일한 값이 0임을 보여 준다. 이제 유한한 배반 사건 $B_1, \dots, B_k$ 뒤에 빈 집합 $\emptyset, \emptyset, \dots$를 붙여 가산가법성을 적용하면 $\mathbb{P}(B_1 \cup \cdots \cup B_k) = \mathbb{P}(B_1) + \cdots + \mathbb{P}(B_k)$라는 유한가법성도 얻는다. A와 A^c는 Ω를 두 배반 사건으로 분할하므로, 유한가법성에 의해 $\mathbb{P}(A) + \mathbb{P}(A^c) = \mathbb{P}(\Omega) = 1$이고 여사건 공식이 성립한다. $A \subseteq B$이면 $B = A \cup (B \setminus A)$가 배반 분해이므로 $\mathbb{P}(B) = \mathbb{P}(A) + \mathbb{P}(B \setminus A) \ge \mathbb{P}(A)$, 곧 단조성이 성립한다. 마지막으로 $A \cup B$를 $A \setminus B$, $B \setminus A$, $A \cap B$의 세 배반 사건으로 나누면 $\mathbb{P}(A \cup B) = \mathbb{P}(A \setminus B) + \mathbb{P}(B \setminus A) + \mathbb{P}(A \cap B)$이고, $\mathbb{P}(A) + \mathbb{P}(B)$에는 $A \cap B$의 확률이 두 번 들어 있음을 알 수 있다. 그중 한 번을 빼면 구하는 식을 얻는다. $\square$

두 사건의 확률만 알려져 있으면 교집합의 확률은 일반적으로 결정되지 않는다. 단조성과 합집합의 확률이 1 이하라는 사실을 함께 사용하면

$$\max\{0, \mathbb{P}(A) + \mathbb{P}(B) - 1\} \le \mathbb{P}(A \cap B) \le \min\{\mathbb{P}(A), \mathbb{P}(B)\}$$

를 얻는다. 이 범위는 독립을 가정하지 않아도 성립한다.

예제 1.6 (겹치는 장애 사건) 어떤 시스템의 두 장애 사건을 A, B라 한다. $\mathbb{P}(A) = 0.08$, $\mathbb{P}(B) = 0.05$, $\mathbb{P}(A \cap B) = 0.02$이면 적어도 하나의 장애가 날 확률은

$$\mathbb{P}(A \cup B) = 0.08 + 0.05 - 0.02 = 0.11$$

이다. 정확히 하나의 장애가 날 확률은 $0.08 + 0.05 - 2(0.02) = 0.09$이며, 둘 다 발생하지 않을 확률은 0.89다. 두 개의 주변확률만 알고 있었다면, 적어도 하나의 장애가 날 확률은 0.08 이상 0.13 이하라고만 말할 수 있다.

1.4 합집합의 상계와 포함배제

정리 1.7 (합집합 상계) 임의의 사건열 $A_1, A_2, \dots$ 에 대해

$$\mathbb{P}\left(\bigcup_{n=1}^{\infty} A_n\right) \le \sum_{n=1}^{\infty} \mathbb{P}(A_n) \tag{1.4}$$

이 성립한다. 우변이 무한대인 경우에도 이 부등식은 참이지만 유용한 수치 상계를 주지는 않는다.

증명. $B_1 = A_1$, $B_n = A_n \setminus \bigcup_{j<n} A_j$ 로 둔다. B_n 들은 서로 배반이고 그 합집합은 A_n 들의 합집합과 같다. 또한 $B_n \subseteq A_n$ 이므로 $\mathbb{P}(B_n) \le \mathbb{P}(A_n)$ 이다. 가산가법성과 단조성을 차례로 적용하면 결론을 얻는다. $\square$

이 부등식을 **합집합 상계**(*union bound*)라 한다. 서로의 의존 관계를 모르는 여러 실패 사건을 묶을 때 특히 유용하다. 다만 중복이 많으면 매우 느슨해진다. 열 가지 경보가 모두 같은 사건을 가리킨다면 경보 중 하나가 울릴 확률은 개별 경보의 확률과 같지만, 합집합 상계는 그 열 배를 제시한다.

세 사건의 정확한 포함배제 공식은

$$\begin{aligned}\mathbb{P}(A \cup B \cup C) = {} & \mathbb{P}(A) + \mathbb{P}(B) + \mathbb{P}(C) \\ & - \mathbb{P}(A \cap B) - \mathbb{P}(A \cap C) - \mathbb{P}(B \cap C) \\ & + \mathbb{P}(A \cap B \cap C)\end{aligned} \tag{1.5}$$

이다. 세 사건에 모두 속한 결과는 식 (1.5)의 첫 줄에서 세 번 더해지고 둘째 줄에서 세 번 빠지므로, 마지막 줄에서 한 번 되살려야 한다. 이처럼 한 결과가 몇 번 세어지는지를 확인하는 방법은 유한 포함배제 원리의 일반적인 증명으로 이어진다.

1.5 사건열과 확률의 연속성

무한히 많은 사건의 확률을 계산할 때에는 가산가법성이 극한과 연결된다. $A_n \uparrow A$ 는 $A_1 \subseteq A_2 \subseteq \cdots$ 이고 $A = \bigcup_n A_n$ 이라는 뜻이다. $A_n \downarrow A$ 는 감소하는 사건열의 교집합이 A 라는 뜻이다.

정리 1.8 (아래와 위로부터의 연속성) 확률측도에 대해

$$A_n \uparrow A \implies \mathbb{P}(A_n) \to \mathbb{P}(A), \qquad A_n \downarrow A \implies \mathbb{P}(A_n) \to \mathbb{P}(A)$$

가 성립한다.

증명. 증가하는 경우, $B_1 = A_1$, $B_n = A_n \setminus A_{n-1}$ 로 두면 B_n 들은 배반이다. 따라서

$$\mathbb{P}(A) = \sum_{n=1}^{\infty} \mathbb{P}(B_n) = \lim_{N\to\infty} \sum_{n=1}^{N} \mathbb{P}(B_n) = \lim_{N\to\infty} \mathbb{P}(A_N).$$

감소하는 경우에는 $A_n^{c} \uparrow A^{c}$ 에 방금 증명한 결과를 적용하고 여사건 공식을 사용한다. 일반적인 무한 측도에서는 위로부터의 연속성에 측도가 유한하다는 조건이 필요하지만, 확률측도에서는 전체 질량이 1 이므로 이 조건이 자동으로 충족된다. $\square$

예제 1.9 (언젠가 앞면이 나오는가) 각 던지기가 독립이고 앞면 확률이 $p \in (0,1]$인 무한 동전 던지기 모형을 생각한다. A_n을 처음 n번 모두 뒷면인 사건으로 두면 $A_n \downarrow A$이고, 여기서 A는 영원히 앞면이 나오지 않는 사건이다. 유한 독립성으로 $\mathbb{P}(A_n) = (1-p)^n$이므로

$$\mathbb{P}(A) = \lim_{n\to\infty} (1-p)^n = 0.$$

따라서 언젠가 앞면이 나올 확률은 1이다. 이 계산은 무한 실험 모형이 주어졌다는 전제 아래 이루어진다. 무한 곱 확률공간의 존재 정리는 확률론의 후속 과정에서 다룬다.

1.6 확률이 영이라는 말의 의미

유한 균등모형에서는 확률이 영인 사건이 빈집합뿐이다. 이 직관을 모든 확률공간에 그대로 적용하면 오류가 생긴다. $[0,1]$에서 길이에 비례하여 점 하나를 고르는 균등모형에서는 모든 고정된 x에 대해 $\mathbb{P}(\{x\}) = 0$이다. 그럼에도 표본점은 반드시 어느 한 점으로 실현된다.

정의 1.10 (거의 확실) 어떤 명제가 성립하는 사건의 확률이 1이면, 그 명제가 **거의 확실**(*almost surely*)하게 성립한다고 말한다. 성립하지 않는 결과가 집합으로 존재할 수 있으나, 그 결과들 전체의 확률이 0이라는 뜻이다.

서로 다른 명제들이 각각 거의 확실하다고 해서, 비가산 개의 명제를 동시에 만족할 확률이 반드시 1인 것은 아니다. U가 $[0,1]$ 위의 균등변수이면 고정된 x마다 $\mathbb{P}(U \neq x) = 1$이지만, 모든 $x \in [0,1]$에 대하여 동시에 $U \neq x$일 수는 없다. 반면 가산 개의 확률 1 사건의 교집합은 확률이 1이다. 여사건들의 확률을 합집합 상계로 묶으면 이를 곧바로 증명할 수 있다.

주의 (가산 무한집합의 균등확률은 존재하지 않는다). $\Omega = \{1,2,3,\dots\}$의 모든 한 점 사건에 같은 확률 c를 부여한다고 하면, $c > 0$일 때 처음 n개 점의 확률 nc가 충분히 큰 n에서 1을 초과한다. $c = 0$이면 가산가법성 때문에 전체 확률도 0이 된다. 따라서 자연수 전체에 대한 균등확률이라는 표현은 이 의미로는 정의될 수 없다. 유한 구간에서 균등하게 고른 뒤 극한을 취하는 절차가 있더라도, 그 극한이 자연수 위의 균등확률이 된다고 단정할 수 없다.

1.7 연습문제와 해설

연습문제 1.11 $\mathbb{P}(A) = 0.6$, $\mathbb{P}(B) = 0.5$, $\mathbb{P}(A \cap B) = 0.3$이다. $A \cup B$, $A \setminus B$, $A \triangle B$, $(A \cup B)^c$의 확률을 각각 구하라.

풀이. 차례로 $0.8, 0.3, 0.5, 0.2$이다. 정확히 하나가 일어나는 사건 $A \triangle B$의 확률에서는 교집합의 확률을 두 번 빼야 한다는 점을 확인한다(곧 $\mathbb{P}(A\triangle B) = \mathbb{P}(A)+\mathbb{P}(B)-2\mathbb{P}(A\cap B) = 0.6+0.5-0.6 = 0.5$).

연습문제 1.12 $A \subseteq B$이고 $\mathbb{P}(A) = \mathbb{P}(B)$이면 $A = B$인가?

풀이. 반드시 같지는 않다. 가법성은 $\mathbb{P}(B \setminus A) = 0$만 보장한다. $[0,1]$ 균등모형에서 $A = (0,1)$, $B = [0,1]$로 두면 두 확률은 모두 1이지만 집합은 다르다.

연습문제 1.13 $\mathbb{P}(A_n) = 1$인 사건열에 대해 $\mathbb{P}\left(\bigcap_{n=1}^{\infty} A_n\right) = 1$임을 증명하라.

풀이. 드모르간 법칙과 합집합 상계에 의해

$$\mathbb{P}\left(\left(\bigcap_{n} A_n\right)^{c}\right) = \mathbb{P}\left(\bigcup_{n} A_n^{c}\right) \le \sum_{n} \mathbb{P}(A_n^{c}) = 0.$$

따라서 여사건의 확률이 0이고, $\mathbb{P}\left(\bigcap_n A_n\right) = 1 - 0 = 1$이다.

> **연습문제 1.14** 두 사건의 확률이 각각 0.7, 0.8일 때 교집합 확률의 가능한 범위를 구하라. 두 끝값을 실제로 달성할 수 있는가?

풀이. 범위는 $[0.5, 0.7]$이다. $[0,1]$ 균등모형에서 $A = [0, 0.7]$로 둔다. $B = [0.2, 1]$이면 교집합의 길이가 0.5이고, $B = [0, 0.8]$이면 0.7이다. 따라서 주어진 주변확률만으로는 이보다 좁은 일반 범위를 주장할 수 없고, 두 끝값은 모두 달성된다.

> **연습문제 1.15** 서로 배반인 A_n에 대해 $\mathbb{P}(A_n)$이 0으로 수렴함을 보여라. 배반 조건을 없애면 결론이 유지되는가?

풀이. $\sum_n \mathbb{P}(A_n) = \mathbb{P}\left(\bigcup_n A_n\right) \le 1$이므로, 수렴하는 비음수 급수의 일반항은 0으로 수렴한다. 배반 조건을 없애고 모든 $A_n = \Omega$로 두면 확률은 항상 1이므로 결론이 실패한다.

참고 (다음 연결). 유한 균등모형에서 확률은 사건의 크기와 표본공간의 크기의 비율이다. 제20권 제2장에서는 그 크기를 정확하게 세는 방법과, 균등하게 세어도 되는 대상을 식별하는 방법을 다룬다.

제 2 장

계수법과 유한 확률모형

개요 유한 확률모형은 표본공간 Ω가 유한집합이고 모든 결과가 같은 확률을 가지는 모형이며, 이 모형에서 사건 A의 확률은 $|A|/|\Omega|$라는 비율로 정해진다. 이 장은 그러한 비율을 계산하는 데 필요한 **계수법**(*enumerative combinatorics*)을 정리한다. 곱의 법칙에서 출발하여 순열과 조합, 복원·비복원추출, 다항계수, 중복조합(별과 막대)을 차례로 세우고, 이를 생일 문제·완전순열(교란순열)·초기하분포 같은 대표적인 계산에 적용한다. 각 절에서 가장 중요한 것은 공식 자체가 아니라 그 공식이 어떤 표본공간을 균등하게 센 결과인지 식별하는 일이다. 같은 대상이라도 순서를 구별하는지, 복원을 허용하는지에 따라 분모가 달라지며, 이를 혼동하는 것이 유한 확률에서 가장 흔한 오류이다. 선행 지식: 곱셈·팩토리얼·집합 연산, 그리고 제20권 제1장의 확률의 공리와 가법성. 이 장에서 n, k는 별도 언급이 없으면 비음수 정수이다.

2.1 같은 가능성의 결과를 먼저 정한다

유한집합 Ω의 모든 결과가 같은 확률이면 가법성과 정규화에 의해

$$\mathbb{P}(A) = \frac{|A|}{|\Omega|} \tag{2.1}$$

이다. 이러한 모형을 **유한 균등모형**(*uniform probability model*)이라고 한다. 여기서 가장 중요한 조건은 유한성보다 균등성이다. 추첨기에서 각 표본이 같은 확률로 나오는지, 먼저 순서를 구별한 다음 순서를 잊는지, 복원을 하는지에 따라 분모가 달라진다.

공정한 주사위 두 개의 눈을 순서 없이 기록할 때 가능한 쌍은 $\binom{6}{2} + 6 = 21$개다. 그러나 $\{1,1\}$은 순서 있는 결과 하나에 대응하고 $\{1,2\}$는 두 개에 대응하므로, 이 21개를 같은 확률로 세면 안 된다. 순서를 잊는 사상에서 각 기록값의 원상이 같은 크기인지 확인하는 습관이 유한 확률의 많은 오류를 막아 준다.

흔한 오류 (눈에 보이는 결과와 균등한 결과). "가능한 결과의 수가 m개이므로 각 확률은 $1/m$이다"라는 추론은 그 m개의 결과가 실제로 같은 확률을 가질 때만 성립한다. 위의 21가지 순서 없는 쌍이 바로 이 추론이 깨지는 예이다.

2.2 곱의 법칙, 순열, 조합

첫 단계에 a가지 선택이 있고 그 각각에 대해 둘째 단계에 정확히 b가지 선택이 있으면 전체 선택은 ab가지다. 이를 **곱의 법칙**(*multiplication principle*)이라고 한다. 단계별 선택 수가 이전 결과에 따라 달라지면 각 가지의 수를 합해야 하며 단순 곱으로 처리할 수 없다.

서로 다른 n개 중 k개를 중복 없이 순서 있게 고르는 것을 **순열**(*permutation*)이라고 하며, 그 경우의 수는

$$(n)_k = n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!}, \qquad 0 \le k \le n \tag{2.2}$$

이다. $(n)_k$를 **하강계승**(*falling factorial*)이라고 부른다.

순서를 구별하지 않고 k개를 고르는 것을 **조합**(*combination*)이라고 한다. 각 k원소 부분집합이 $k!$개의 순열에 대응하므로 식 (2.2)을 $k!$로 나누어

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{2.3}$$

를 얻는다. $\binom{n}{k} = 0$을 $k < 0$ 또는 $k > n$에 대한 관례로 사용하면 합의 범위를 쓰기 편하다. 특히 $0! = 1$이고 빈 부분집합은 하나이므로 $\binom{n}{0} = 1$이다.

참고 (이항계수의 대칭성). k개를 고르는 것과 고르지 않는 나머지 $n-k$개를 고르는 것은 같은 선택이므로

$$\binom{n}{k} = \binom{n}{n-k} \tag{2.4}$$

이다. 식 (2.3)에서 분모의 두 인자 $k!(n-k)!$가 k와 $n-k$에 대해 대칭이라는 점으로도 확인된다.

명제 2.1 (Pascal 항등식) $1 \le k \le n$이면

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}. \tag{2.5}$$

증명. n개 원소 중 하나를 특별한 원소로 지정한다. k개를 고른 집합은 그 원소를 포함하지 않는 경우와 포함하는 경우로 나뉜다. 첫 경우에는 나머지 $n-1$개에서 k개를 고르고, 둘째 경우에는 나머지에서 $k-1$개를 고른다. 두 경우가 배반이고 모든 선택을 덮는다. □

이 증명은 식을 팩토리얼로 전개하는 계산보다 더 많은 정보를 준다. 어떤 사건을 두 개의 배반 경우로 나누는지가 보이므로, 비슷한 계수 문제에서 같은 분할을 다시 사용할 수 있다.

예제 2.2 (위원회 구성) 서로 다른 8명 중 3명을 뽑되 특정 두 사람 u, v가 함께 뽑히지 않게 하자. 전체는 $\binom{8}{3} = 56$가지다. 두 사람이 모두 뽑히는 경우에는 나머지 6명 중 한 명을 추가하면 되므로 6가지다. 따라서 허용되는 위원회는 $56 - 6 = 50$가지다. 모든 3인 위원회를 균등하게 뽑았다면 조건을 만족할 확률은 $50/56 = 25/28$이다.

2.3 복원추출과 비복원추출

복원추출(*sampling with replacement*)에서는 한 번 뽑은 대상을 다시 넣으므로 같은 대상이 다시 나올 수 있다. N개의 대상을 매번 균등하고 독립적으로 k번 뽑으면 순서 있는 표본은 N^k개다. **비복원추출**(*sampling without replacement*)에서는 다시 넣지 않으므로 순서 있는 표본은 $(N)_k$개다. 비복원추출의 서로 다른 단계들은 일반적으로 독립이 아니다.

빨간 공이 r개, 파란 공이 b개 있는 주머니에서 두 개를 뽑자. 복원하면 두 개 모두 빨간 공일 확률은 $(r/(r+b))^2$다. 비복원이면

$$\frac{r}{r+b} \cdot \frac{r-1}{r+b-1} = \frac{\binom{r}{2}}{\binom{r+b}{2}}$$

이다. 왼쪽은 순서 있는 실험으로, 오른쪽은 순서 없는 표본으로 계산한다. 두 식이 같은 것은 같은 사건을 일관된 표본공간 두 가지로 센 결과다.

예제 2.3 (작은 로트의 불량 검사) 10개 제품 중 3개가 불량이며, 서로 다른 4개를 균등하게 검사한다. 불량이 정확히 2개일 확률은

$$\frac{\binom{3}{2}\binom{7}{2}}{\binom{10}{4}} = \frac{63}{210} = 0.3.$$

불량이 하나도 없을 확률은 $\binom{7}{4}/\binom{10}{4} = 35/210 = 1/6$이므로, 적어도 하나를 발견할 확률은 $5/6$이다. 추출 비율이 $4/10$으로 작지 않으므로 각 검사를 독립인 불량 확률 0.3의 시행으로 근사하면 정확한 답과 차이가 날 수 있다.

2.4 다항계수와 순서의 중복

n개의 위치에 종류가 m개인 기호를 놓되 종류별 개수가 $n_1, \dots, n_m$이고 합이 n이라고 하자. 같은 종류의 기호는 서로 구별하지 않는다. 서로 다른 배열의 수를 **다항계수**(*multinomial coefficient*)라고 하며

$$\binom{n}{n_1, \dots, n_m} = \frac{n!}{n_1! \cdots n_m!} \tag{2.6}$$

이다. 처음에는 모든 기호에 개별 이름을 붙여 $n!$가지로 배열한 뒤, 이름을 지웠을 때 동일해지는 $n_1! \cdots n_m!$개의 배열을 한 묶음으로 나누면 된다. $m = 2$이면 식 (2.6)은 이항계수 $\binom{n}{n_1}$로 돌아간다.

예제 2.4 (세 범주의 관측 순서) 6번의 관측에서 A가 3번, B가 2번, C가 1번 나오는 순서는 $6!/(3!2!1!) = 60$개다. 시행들이 독립이고 각 시행의 범주확률이 p_A, p_B, p_C이면, 이 빈도 벡터의 확률은

$$60\, p_A^3 p_B^2 p_C.$$

범주확률의 합은 1이어야 한다. 범주 이름이 세 가지라고 해서 $p_A = p_B = p_C$를 자동으로 가정해서는 안 된다.

2.5 중복조합과 별과 막대

비음수 정수해

$$x_1 + \cdots + x_m = n$$

의 개수를 **중복조합**(*combination with repetition*)이라고 하며, 그 개수는 $\binom{n+m-1}{m-1}$이다. 이를 세는 표준적인 방법이 **별과 막대**(*stars and bars*) 논법이다. n개의 별을 일렬로 놓고 $m-1$개의 막대로 구분하면 각 구획의 별 개수가 x_i가 된다. 끝이나 막대 사이에 별이 없을 수도 있으므로 0도 허용된다. 양의 정수해를 요구하면 $y_i = x_i - 1$을 대입하여 $n \ge m$일 때 $\binom{n-1}{m-1}$을 얻는다.

흔한 오류 (점유 벡터와 균등성). 별과 막대로 센 **점유 벡터**(*occupancy vector*)가 자동으로 균등해지는 것은 아니다. 공을 독립적으로 상자에 넣는 모형에서는 같은 점유 벡터를 만드는 공의 배치 수가 다르다.

예제 2.5 (점유 벡터의 확률) 구별되는 공 3개를 각자 독립적으로 두 상자 중 하나에 확률 $1/2$로 넣는다. 점유 벡터는 $(3,0), (2,1), (1,2), (0,3)$의 네 가지다. 하지만 확률은 순서대로 $1/8, 3/8, 3/8, 1/8$이다. 첫 상자에 들어갈 공들의 부분집합을 고르는 방법이 각각 $1, 3, 3, 1$가지

이기 때문이다. 점유 벡터 네 개에 1/4씩 주는 것은 별개의 확률모형이다.

2.6 충돌 확률과 포함배제의 계산

예제 2.6 (생일 충돌) 한 해를 d개의 날로 모델링하고 n명의 생일을 독립·균등하게 가정한다. 윤년과 계절적 출생 편차는 이 모형에서 제외한다. $n \le d$이면 모두 다른 날에 태어날 확률은

$$\frac{(d)_n}{d^n} = \prod_{j=0}^{n-1}\left(1 - \frac{j}{d}\right),$$

따라서 적어도 한 쌍이 같은 생일을 가질 확률은 이 값의 여사건이다. $d = 365$, $n = 23$이면

$$1 - \prod_{j=0}^{22}\left(1 - \frac{j}{365}\right) \approx 0.507297.$$

이는 "누군가가 특정 한 사람과 생일이 같다"는 사건의 확률과 다르다. 후자는 나머지 22명만 비교하므로 $1 - (364/365)^{22}$이다.

쌍별 충돌 사건에 합집합 상계를 적용하면

$$\mathbb{P}(\text{충돌}) \le \binom{n}{2}\frac{1}{d} \tag{2.7}$$

를 얻는다. 이 값은 1을 넘을 수도 있으므로 필요하면 1과의 최솟값을 취한다. 드문 충돌 영역에서는 크기의 규모를 빠르게 파악하는 데 도움이 되지만, 정확한 확률이라고 사용하면 안 된다.

예제 2.7 (잘못 배달된 편지) n개의 서로 다른 편지를 n개의 주소에 무작위 순열로 배달한다. 어느 편지도 제 주소에 도착하지 않을 확률을 구하자. A_i를 편지 i가 제 주소에 도착하는 사건으로 두면, 지정한 k개의 편지가 모두 맞게 배달되는 순열은 $(n-k)!$개다. 포함배제로 아무것도 맞지 않는 순열의 수는

$$D_n = \sum_{k=0}^{n}(-1)^k\binom{n}{k}(n-k)! = n!\sum_{k=0}^{n}\frac{(-1)^k}{k!}$$

이다. D_n을 **교란순열**(*derangement*)의 수라고 한다. 따라서 $n = 4$일 때 $D_4 = 24(1 - 1 + 1/2 - 1/6 + 1/24) = 9$이고 확률은 $9/24 = 3/8$이다. $n \to \infty$이면 지수함수의 급수에 의해 이 확률은 e^{-1}로 수렴한다. 이 극한은 유한 n에서의 정확한 값과 구별해야 한다.

2.7 초기하분포의 정규화가 주는 항등식

N개 중 표시된 대상이 K개이고, 크기 n의 부분집합을 균등하게 고르자. 표시된 대상의 개수를 X라 하면 X가 따르는 분포를 **초기하분포**(*hypergeometric distribution*)라고 하며

$$\mathbb{P}(X = k) = \frac{\binom{K}{k}\binom{N-K}{n-k}}{\binom{N}{n}}, \qquad \max(0, n - N + K) \le k \le \min(n, K). \tag{2.8}$$

분자가 모든 n원소 부분집합을 표시 개수에 따라 분할하므로

$$\sum_{k} \binom{K}{k}\binom{N-K}{n-k} = \binom{N}{n} \tag{2.9}$$

이다. 이를 **Vandermonde 항등식**이라 한다. 분포를 제시할 때에는 허용 범위와 합이 1이라는 사실을 함께 확인해야 한다. 범위를 잘못 쓰면 음수 팩토리얼처럼 정의되지 않은 식이 생기거나 가능한 결과를 누락한다.

역사 (Pascal 삼각형의 기원). 식 (2.5)의 계수를 삼각형으로 배열한 표는 Pascal보다 앞서 여러 문화권에서 연구되었다. 중국의 Yang Hui(楊輝, 13세기)와 페르시아의 Omar Khayyam이 이미 이항계수의 삼각 배열을 다루었으며, Pascal의 1654년 *Traité du triangle arithmétique*는 이를 확률 계산과 체계적으로 연결한 저작으로 평가된다.

핵심 식

$$(n)_k = \frac{n!}{(n-k)!}, \qquad \binom{n}{k} = \frac{n!}{k!(n-k)!}, \tag{2.10}$$

$$\binom{n}{n_1,\dots,n_m} = \frac{n!}{n_1!\cdots n_m!}, \qquad \binom{n+m-1}{m-1} \ \text{(비음수 정수해의 수)}, \tag{2.11}$$

$$D_n = n!\sum_{k=0}^{n}\frac{(-1)^k}{k!}, \qquad \mathbb{P}(X=k) = \frac{\binom{K}{k}\binom{N-K}{n-k}}{\binom{N}{n}}. \tag{2.12}$$

2.8 연습문제와 해설

연습문제 2.8 0부터 9까지의 숫자로 길이 4의 문자열을 만든다. 첫 자리의 0도 허용한다. 반복을 허용할 때와 금지할 때의 경우의 수를 구하라. 반복 허용 균등모형에서 네 숫자가 모두 다를 확률은?

풀이. 각각 $10^4 = 10000$, $10\cdot 9\cdot 8\cdot 7 = 5040$이다. 확률은 $5040/10000 = 0.504$이다. "네 자리 자연수"였다면 첫 자리의 0을 제외해야 하므로 표본공간이 바뀐다.

연습문제 2.9 빨간 공 4개와 파란 공 5개에서 비복원으로 3개를 균등 추출한다. 빨간 공이 적어도 하나 있을 확률을 구하라.

풀이. 모두 파란 공인 여사건을 사용하면 $1-\binom{5}{3}/\binom{9}{3} = 1-10/84 = 37/42$이다. 순서 있게 계산해도 $1-(5/9)(4/8)(3/7)$로 같은 값을 얻는다.

연습문제 2.10 비음수 정수 x, y, z가 $x+y+z=7$을 만족하는 해의 수를 구하라. 셋 모두 양수일 때는?

풀이. 비음수 해는 $\binom{9}{2} = 36$개, 양의 해는 각 변수에서 1씩 뺀 뒤 $\binom{6}{2} = 15$개다. 정수해를 균등하게 고르는 모형과 일곱 공을 독립적으로 상자에 넣는 모형의 차이를 다시 확인하자.

연습문제 2.11 5개 대상의 무작위 순열에서 적어도 하나가 원래 위치에 있을 확률을 정확한 분수로 구하라.

풀이. $D_5 = 5!\sum_{k=0}^{5}(-1)^k/k! = 44$이므로 확률은 $1 - 44/120 = 19/30$이다. 서로 다른 대상의 제자리 사건들은 독립이 아니다.

연습문제 2.12 $\displaystyle\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$을 계수 논증으로 증명하라.

풀이. n명 중 비어 있지 않은 팀을 고르고 그 안에서 대표 한 명을 고르는 방법을 센다. 팀 크기 k를 먼저 고르면 왼쪽이다. 대표를 먼저 고르면 n가지이며 나머지 $n-1$명은 각각 참여 여부를 자유롭게 정하므로 $n2^{n-1}$가지다. $n=0$은 별도로 양변을 0으로 해석한다.

계수법은 균등한 원시 결과의 수를 계산한다. 관측 정보가 주어져 표본공간이 좁아졌을 때 확률을 어떻게 갱신하는지는 조건부 확률의 문제이며, 제20권 제3장에서 다룬다.

제 3 장

조건부 확률, 베이즈 공식, 독립성

개요 조건부 확률은 어떤 사건이 참이라고 알려졌을 때 확률을 다시 정규화하는 연산이며, 이 장은 그 정의에서 출발하여 곱셈법칙(연쇄법칙), 전확률 공식, 베이즈 공식을 차례로 세우고 가능도비를 이용한 갱신을 설명한다. 이어서 사건의 독립성과 상호독립을 정의하고, 쌍별독립이 상호독립을 함의하지 않는 예와 조건을 걸면 독립성이 생기거나 깨지는 예를 통해 두 개념을 구별한다. 마지막으로 부분집단의 가중평균이 뒤집히는 Simpson 역설과 영확률 사건에 조건을 거는 문제의 한계를 다룬다. 선행 지식: 제20권 제1장의 확률의 가법성과 배반 사건에 의한 분할, 제20권 제2장의 기본적인 계수법. 모든 조건부 확률은 분모가 양수일 때에만 정의된다.

3.1 정보가 주어졌을 때의 확률

정의 3.1 (사건에 대한 조건부 확률) $\mathbb{P}(B) > 0$일 때 사건 A의 B에 대한 **조건부 확률**(*conditional probability*)을

$$\mathbb{P}(A \mid B) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)} \tag{3.1}$$

로 정의한다. B는 관측되어 참이라고 알려진 사건이며, 분자는 그중에서도 A가 참인 부분의 확률이다.

조건부 확률은 단순히 B 바깥의 결과를 버리는 것만으로 끝나지 않는다. 남은 전체 확률이 1이 되도록 $\mathbb{P}(B)$로 나누어 정규화한다. 유한 균등모형에서는 $\mathbb{P}(A \mid B) = |A \cap B| \,/\, |B|$이지만, 원래 결과들이 비균등했다면 조건을 걸어도 일반적으로 균등해지지 않는다.

고정된 B에 대해 $A \mapsto \mathbb{P}(A \mid B)$는 다시 확률측도이다. 비음수성과 전체 질량 1은 정의에서 확인된다. 배반인 A_n에 대해서는 $A_n \cap B$도 배반이므로 가산가법성이 유지된다. 따라서 여사건 공식, 합집합 상계 등 제20권 제1장의 계산 규칙을 모두 조건부 확률 안에서 사용할 수 있다.

예제 3.2 (주사위의 합을 안 뒤의 확률) 독립인 공정한 두 주사위에서 $B = \{\text{합이 } 8\}$, $A = \{\text{첫째 눈이 } 3\}$라 하자. B의 가능한 결과는 $(2,6), (3,5), (4,4), (5,3), (6,2)$의 다섯 개다. 따라서 $\mathbb{P}(A \mid B) = 1/5$이다. 반대로 첫째 눈이 3이라고 알려졌다면 둘째 눈이 5일 확률은 $1/6$이므로 $\mathbb{P}(B \mid A) = 1/6$이다. 조건과 목표를 바꾸는 것은 같은 계산이 아니다.

3.2 곱셈법칙과 순차 계산

정의 3.1의 분모를 곱하면

$$\mathbb{P}(A \cap B) = \mathbb{P}(B)\mathbb{P}(A \mid B) \tag{3.2}$$

를 얻는다. 여러 사건에 대해 중간 교집합의 확률이 양수이면

$$\begin{aligned}\mathbb{P}(A_1 \cap \cdots \cap A_n) = \mathbb{P}(A_1)\mathbb{P}(A_2 \mid A_1) \\ \cdot \mathbb{P}(A_3 \mid A_1 \cap A_2) \cdots \mathbb{P}(A_n \mid A_1 \cap \cdots \cap A_{n-1}).\end{aligned} \tag{3.3}$$

이것을 **연쇄법칙**(*chain rule*)이라 한다. 사건들이 독립이라는 가정은 필요하지 않다. 오히려 의존성을 조건부 확률에 정확히 반영하는 식이다. 중간 교집합이 영확률이면 최종 교집합도 영확률이지만, 정의되지 않은 조건부 확률들을 억지로 곱해서 표현하지 않는다.

예제 3.3 (비복원추출의 순서) 빨간 공 3개와 파란 공 2개에서 세 개를 비복원으로 뽑을 때, 색이 빨강–파랑–빨강 순서일 확률은

$$\frac{3}{5} \cdot \frac{2}{4} \cdot \frac{2}{3} = \frac{1}{5}$$

이다. 각 단계의 분모와 분자가 이전 결과를 반영한다. “빨간 공 두 개와 파란 공 한 개”라는 순서 없는 사건은 가능한 세 색 순서를 모두 포함하며, 각 순서의 확률이 $1/5$이므로 전체 확률은 $3/5$이다. 초기하 공식 $\binom{3}{2}\binom{2}{1}/\binom{5}{3}$도 같은 답을 준다.

3.3 전확률 공식

정리 3.4 (전확률 공식) $B_1, B_2, \ldots$가 Ω의 가산 분할이고 각 $\mathbb{P}(B_i) > 0$이면

$$\mathbb{P}(A) = \sum_{i} \mathbb{P}(A \mid B_i)\mathbb{P}(B_i). \tag{3.4}$$

영확률인 분할 조각이 있으면 해당 항은 교집합 확률 0으로 처리하고, 정의되지 않은 조건부 확률을 평가하지 않는다.

증명. $A = \bigcup_i (A \cap B_i)$는 서로 배반인 분해이다. 따라서 $\mathbb{P}(A) = \sum_i \mathbb{P}(A \cap B_i)$이고 각 항에 조건부 확률의 정의를 적용하면 된다. $\square$

전확률 공식은 서로 다른 환경에서의 확률을 환경의 발생 비율로 가중평균한다. 단순 산술평균이 되는 것은 모든 환경의 가중치가 같을 때뿐이다.

예제 3.5 (두 생산 경로) 전체 부품의 60%가 경로 B_1, 나머지 40%가 경로 B_2에서 온다. 각 경로의 불량률을 $0.02, 0.05$로 가정하면 전체 불량률은

$$0.6(0.02) + 0.4(0.05) = 0.032.$$

0.02와 0.05의 산술평균 0.035는 경로 비중을 무시한 값이다. 여기서 경로와 불량 여부가 독립이라면 두 경로의 조건부 불량률이 전체 불량률과 같아야 하는데, 주어진 모형에서는 그렇지 않다.

3.4 베이즈 공식과 가능도비

정리 3.6 (베이즈 공식) 전확률 공식의 가정 아래 $\mathbb{P}(A) > 0$이면

$$\mathbb{P}(B_j \mid A) = \frac{\mathbb{P}(A \mid B_j)\mathbb{P}(B_j)}{\sum_i \mathbb{P}(A \mid B_i)\mathbb{P}(B_i)}. \tag{3.5}$$

증명. 분자는 $\mathbb{P}(A \cap B_j)$이고 분모는 $\mathbb{P}(A)$다. 따라서 식은 조건부 확률의 정의이며, 분모를 전확률 공식으로 전개했을 뿐이다. □

관측 전의 $\mathbb{P}(B_j)$를 **사전확률**(*prior probability*), 관측 후의 $\mathbb{P}(B_j \mid A)$를 **사후확률** (*posterior probability*)이라 한다. $\mathbb{P}(A \mid B_j)$는 B_j가 참일 때 지금의 관측이 얼마나 잘 설명되는지 나타내는 **가능도**(*likelihood*) 역할을 한다. 가능도는 원인을 고정한 조건부 확률이므로 사후확률과 구별해야 한다.

두 가설 H, H^c의 사전확률과 필요한 조건부 확률이 모두 양수이면

$$\frac{\mathbb{P}(H \mid A)}{\mathbb{P}(H^c \mid A)} = \frac{\mathbb{P}(A \mid H)}{\mathbb{P}(A \mid H^c)} \cdot \frac{\mathbb{P}(H)}{\mathbb{P}(H^c)}. \tag{3.6}$$

즉 사후 **오즈**(*odds*)는 **가능도비**(*likelihood ratio*)와 사전 오즈의 곱이다. 새로운 증거가 들어왔을 때 그 증거의 효과를 곱셈 인자로 해석할 수 있다.

예제 3.7 (희귀 결함과 경보) 가상의 검사 모형에서 결함 확률이 0.01, 결함품에 경보가 울릴 확률이 0.9, 정상품에 경보가 울릴 확률이 0.05라고 하자. 경보 A를 관측했을 때 결함 H의 사후확률은

$$\mathbb{P}(H \mid A) = \frac{0.9(0.01)}{0.9(0.01) + 0.05(0.99)} = \frac{2}{13} \approx 0.153846.$$

90%라는 검출률과 경보 뒤의 결함확률을 혼동하면 큰 오차가 생긴다. 예를 들어 가상 부품 10000개를 생각하면 기대 개수 기준으로 결함품 경보가 90개, 정상품 경보가 495개이므로 $90/(90+495)$로 같은 값을 확인할 수 있다.

두 번 경보를 확인했을 때 앞의 가능도비를 단순히 두 번 곱하려면, 두 경보가 결함 여부를 조건으로 독립이라는 추가 가정이 필요하다. 그 가정 아래에는

$$\mathbb{P}(H \mid A_1 \cap A_2) = \frac{0.9^2(0.01)}{0.9^2(0.01) + 0.05^2(0.99)} = \frac{36}{47} \approx 0.765957.$$

같은 고장 원인으로 두 검사가 동시에 오작동한다면 이 계산은 적용할 수 없다. 반복 측정이 있다는 사실만으로 독립된 증거 두 개를 얻은 것은 아니다.

3.5 독립의 정확한 정의

정의 3.8 (사건의 독립) 사건 A, B가 **독립**(*independence*)이라는 것은

$$\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B) \tag{3.7}$$

라는 뜻이다. $\mathbb{P}(B) > 0$이면 이는 $\mathbb{P}(A \mid B) = \mathbb{P}(A)$와 동치이다.

교집합 형태의 정의는 영확률 사건에도 그대로 적용할 수 있다. 예를 들어 영확률 사건은 모든 사건과 독립이다. 그러나 그 영확률 사건을 조건으로 하는 비율식은 정의되지 않을 수 있다.

독립인 A, B에 대해 A^c, B도 독립이다. 실제로

$$\mathbb{P}(A^c \cap B) = \mathbb{P}(B) - \mathbb{P}(A \cap B) = (1 - \mathbb{P}(A))\mathbb{P}(B).$$

같은 논법으로 여사건을 취한 나머지 조합도 독립임을 알 수 있다.

주의 (배반과 독립). A, B가 배반이고 두 확률이 모두 양수라면 독립일 수 없다. 교집합 확률은 0이지만 주변확률의 곱은 양수이기 때문이다. A가 일어났다는 정보는 배반인 B가 일어나지 않았음을 완전히 알려 준다.

정의 3.9 (상호독립) 사건 $A_1, \dots, A_n$이 **상호독립**(*mutual independence*)이면 모든 비어 있지 않은 지표 부분집합 $I \subseteq \{1, \dots, n\}$에 대해

$$\mathbb{P}\left(\bigcap_{i \in I} A_i\right) = \prod_{i \in I} \mathbb{P}(A_i) \tag{3.8}$$

가 성립한다. 크기가 2인 부분집합에 대해서만 성립하면 **쌍별독립**(*pairwise independence*)이라 한다.

예제 3.10 (쌍별독립이지만 상호독립은 아닌 경우) 독립인 공정한 비트 $X, Y \in \{0, 1\}$를 고르고 Z를 두 비트가 다르면 1, 같으면 0으로 둔다. $A = \{X = 0\}$, $B = \{Y = 0\}$, $C = \{Z = 0\}$는 각각 확률 $1/2$이다. 각 두 사건의 교집합 확률은 $1/4$이므로 쌍별독립이다. 하지만 세 사건의 교집합은 $(X, Y) = (0, 0)$ 하나이므로 확률 $1/4$이며 $(1/2)^3 = 1/8$과 다르다. 전체 교집합 하나만 검사하거나 쌍만 검사하는 것으로 상호독립을 판정해서는 안 된다.

3.6 조건부 독립과 주변 독립

$\mathbb{P}(C) > 0$일 때 A, B가 C를 조건으로 **조건부 독립**(*conditional independence*)이라는 말은

$$\mathbb{P}(A \cap B \mid C) = \mathbb{P}(A \mid C)\mathbb{P}(B \mid C) \tag{3.9}$$

라는 뜻이다. 조건부 독립과 조건 없는 독립 사이에는 일반적인 함의가 없다.

예제 3.11 (혼합은 의존성을 만든다) 앞면 확률이 0.9인 동전과 0.1인 동전 중 하나를 확률 $1/2$로 고른 뒤, 고른 동전을 두 번 독립적으로 던진다. 동전 종류가 주어졌을 때 두 결과는 독립이다. 그러나 동전 종류를 모르면 각 던지기의 앞면 확률은 0.5이고 두 번 모두 앞면일 확률은

$$\frac{1}{2}(0.9^2) + \frac{1}{2}(0.1^2) = 0.41 \neq 0.25.$$

첫 번째 앞면을 보고 나면 0.9 동전을 골랐을 가능성이 올라가므로 두 번째 앞면도 더 기대하게 된다. 공통의 숨은 환경이 주변 의존성을 만든 것이다.

예제 3.12 (조건을 걸어 의존성이 생기는 경우) 독립인 공정한 비트 X, Y에 대해 적어도 하나가 1이라는 조건 C를 걸자. 남는 결과는 $(1,0), (0,1), (1,1)$이며 각각 조건부 확률 $1/3$이다. 따라서

$$\mathbb{P}(X = 1 \mid C) = \mathbb{P}(Y = 1 \mid C) = \frac{2}{3}, \qquad \mathbb{P}(X = Y = 1 \mid C) = \frac{1}{3} \neq \frac{4}{9}.$$

조건 전의 독립성이 조건 후에도 유지된다고 생각하면 안 된다.

3.7 서로 다른 집단을 합칠 때의 역전

예제 3.13 (가중평균과 Simpson 역설) 두 알고리즘 A, B를 쉬운 문제와 어려운 문제에서 평가했다고 하자.

표 3.1 쉬운 문제와 어려운 문제에서의 성공/전체

	쉬운 문제의 성공/전체	어려운 문제의 성공/전체
A	80/100	1/10
B	9/10	20/100

쉬운 문제에서는 $0.8 < 0.9$, 어려운 문제에서는 $0.1 < 0.2$로 B의 성공률이 높다. 그런데 전체 성공률은 A가 $81/110$, B가 $29/110$이어서 순서가 뒤집힌다. 이는 수학적 모순이 아니다. A는 주로 쉬운 문제를, B는 주로 어려운 문제를 풀었으므로 서로 다른 가중치의 평균을 비교했기 때문이다. 공정한 비교를 원하면 공통된 문제 분포에서의 목표 성공률을 먼저 정해야 한다. 이 현상을 **Simpson 역설**(*Simpson's paradox*)이라 한다.

역사 (Simpson 역설의 이름). 이 역전 현상은 Udny Yule이 20세기 초에 이미 보고하였으나, 1951년 Edward Simpson의 논문을 통해 널리 알려져 그의 이름이 붙었다. 세 범주 이상의 분할표에서도 같은 방식으로 나타날 수 있다.

3.8 영확률 사건에 조건을 걸 때

연속형 변수에서 $\mathbb{P}(X = x) = 0$인 경우 $\mathbb{P}(A \cap \{X = x\})/\mathbb{P}(X = x)$는 $0/0$이어서 의미가 없다. 이후 사용하는 $\mathbb{P}(Y \le y \mid X = x)$는 조건부 밀도나 정규 조건부분포 같은 별도 구성으로 정의된다. "아주 좁은 구간으로 조건을 걸고 극한을 취하면 언제나 유일하다"고 가정해서도 안 된다. 어떤 방식으로 조건을 좁히는지와 정규성 조건이 중요하다. 초급 단계에서는 양의 확률 사건에 대한 조건부 확률과 연속형 조건부분포를 분리하여 다루는 것이 안전하다.

핵심 식

$$\mathbb{P}(A \mid B) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)}, \qquad \mathbb{P}(A) = \sum_i \mathbb{P}(A \mid B_i)\mathbb{P}(B_i), \tag{3.10}$$

$$\mathbb{P}(B_j \mid A) = \frac{\mathbb{P}(A \mid B_j)\mathbb{P}(B_j)}{\sum_i \mathbb{P}(A \mid B_i)\mathbb{P}(B_i)}, \qquad \mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B) \ \text{(독립)}. \tag{3.11}$$

3.9 연습문제와 해설

연습문제 3.14 두 생산 경로의 비중과 불량률이 각각 $(0.6, 0.02)$, $(0.4, 0.05)$이다. 불량품이 나왔을 때 둘째 경로에서 왔을 확률은?

풀이. 전체 불량률은 0.032이고 둘째 경로이면서 불량일 확률은 0.02이므로 $0.02/0.032 = 5/8$이다. 사전 경로확률 0.4와 사후확률 0.625를 구별하자.

연습문제 3.15 $\mathbb{P}(A) = 1/3$, $\mathbb{P}(B) = 1/2$이며 두 사건이 독립이다. $\mathbb{P}(A \cup B)$와 $\mathbb{P}(A^c \mid B)$를 구하라.

풀이. 교집합은 $1/6$이므로 합집합은 $2/3$이다. 독립성이 여사건에도 유지되므로 둘째 답은 $2/3$이다.

연습문제 3.16 $\mathbb{P}(A), \mathbb{P}(B) > 0$이고 $\mathbb{P}(A \mid B) = \mathbb{P}(B \mid A)$이다. $\mathbb{P}(A) = \mathbb{P}(B)$가 반드시 성립하는가?

풀이. 교집합 확률이 양수이면 공통 분자를 약분하여 두 주변확률이 같음을 얻는다. 교집합 확률이 0이면 두 조건부 확률이 모두 0이므로 결론이 나오지 않는다. 서로 배반인 사건에 확률 $1/4$, $1/2$를 주면 반례가 된다.

연습문제 3.17 $\mathbb{P}(B) = 0.4$, $\mathbb{P}(A \mid B) = 0.7$, $\mathbb{P}(A \mid B^c) = 0.2$이다. $\mathbb{P}(A)$와 $\mathbb{P}(B \mid A)$를 구하라.

풀이. 전확률 공식으로 $0.7(0.4) + 0.2(0.6) = 0.4$다. 베이즈 공식으로 $\mathbb{P}(B \mid A) = 0.28/0.4 = 0.7$이다. 우연히 같은 수가 나타났지만 분자와 분모의 의미는 서로 다르다.

연습문제 3.18 독립인 공정한 동전을 세 번 던진다. A는 첫째와 둘째가 같은 사건, B는 둘째와 셋째가 같은 사건이다. A, B의 독립성을 판정하라.

풀이. 각 확률은 $1/2$이고 교집합은 세 번 모두 앞면 또는 모두 뒷면인 두 결과이므로 확률 $2/8 = 1/4$다. 따라서 독립이다. 두 사건의 서술에 둘째 던지기가 공통으로 나타난다는 사실만으로 의존이라고 결론 내릴 수 없다.

다음 장에서는 사건의 참/거짓만 기록하는 대신 결과에 수치를 부여한다. 확률변수는 확률을 가진 수 자체가 아니라 표본공간에서 수의 공간으로 가는 함수이며, 이는 제20권 제4장의 주제이다.

제 4 장

확률변수, 분포함수, 확률질량과 밀도

개요 **확률변수**(*random variable*)는 확률공간의 결과마다 실수를 대응시키는 가측함수이고, 확률변수가 결정하는 **분포**는 그 대응을 통해 원래 확률측도를 실수선 위로 옮겨 놓은 것이다. 이 장은 가측성의 정의에서 출발하여 분포 전체를 기술하는 **누적분포함수**의 단조성·오른쪽 연속성·극한값을 증명하고, 이산형 분포의 **확률질량함수**와 절대연속형 분포의 **확률밀도함수**를 구별하여 정의한 뒤 두 성질이 섞인 혼합분포를 다룬다. 이어서 분포함수의 일반화된 역함수인 **분위수함수**와 이를 이용한 역변환 표본생성, 확률변수의 함수(변환)의 분포를 구하는 방법, 끝으로 두 확률변수의 결합분포·주변분포·독립성을 차례로 세운다. 선행 지식: 함수와 역상, 미적분의 기본정리, 조건부 확률. 연속형 분포의 적분은 우선 Riemann 적분으로 이해해도 좋다.

4.1 확률변수는 가측함수이다

정의 4.1 (실수값 확률변수) 확률공간 $(\Omega, \mathcal{F}, \mathbb{P})$에서 실수값 **확률변수** X는 모든 $x \in \mathbb{R}$에 대해

$$\{\omega : X(\omega) \le x\} \in \mathcal{F}$$

를 만족하는 함수 $X : \Omega \to \mathbb{R}$이다. 이 조건을 **가측성**(*measurability*)이라 한다.

가측성은 X에 관한 확률 질문이 원래 확률공간의 사건으로 번역될 수 있게 한다. $\mathbb{P}(X \le x)$는 약식 표기이며, 엄밀하게는 $\mathbb{P}(\{\omega : X(\omega) \le x\})$이다. 유한 표본공간에서 모든 부분집합이 사건이면, 곧 $\mathcal{F}$가 Ω의 멱집합이면 모든 실수값 함수가 확률변수다.

표기 (Borel 집합과 가측성의 확장). 실수선의 **Borel 집합**(*Borel set*)은 모든 반직선 $(-\infty, x]\,(x \in \mathbb{R})$를 포함하고 가산 합집합·가산 교집합·여집합을 취하는 데 닫혀 있는 가장 작은 집합족, 곧 이 반직선들이 생성하는 σ-대수의 원소이다. 열린구간·닫힌구간·가산집합을 비롯하여 실제 계산에서 만나는 거의 모든 실수 부분집합이 Borel 집합이며, σ-대수의 일반론과 Borel 집합의 구성은 제10권 제3장에서 다룬다. 정의 4.1의 조건은 $(-\infty, x]$ 꼴의 특수한 Borel 집합에 대한 가측성만 요구하지만, $\{B \subseteq \mathbb{R} : \{X \in B\} \in \mathcal{F}\}$는 그 자체로 하나의 σ-대수이고 모든 $(-\infty, x]$를 포함하므로 Borel 집합 전체를 포함한다. 따라서 $\{X \in B\} \in \mathcal{F}$는 임의의 Borel 집합 B에 대해 자동으로 성립하며, 아래 정의 4.2의 $\mathbb{P}_X(B)$가 모든 Borel B에서 뜻을 가진다.

두 주사위의 합 $X(i,j) = i + j$, 큰 눈 $M(i,j) = \max(i,j)$, 두 눈이 같은지 나타내는 $I(i,j) = \mathbf{1}_{\{i=j\}}$는 같은 확률공간 위의 서로 다른 확률변수다. 같은 변수라도 표본공간의 확률측도를 바꾸면 분포가 바뀐다. 반대로 서로 다른 확률공간에 정의된 변수들이 같은 분포를 가질 수도 있다.

정의 4.2 (분포) X의 **분포**(*distribution*, *law*)는 실수의 Borel 집합 B에 대해

$$\mathbb{P}_X(B) = \mathbb{P}(X \in B) \tag{4.1}$$

로 정한 확률측도이다. X와 Y가 같은 분포라는 것은 모든 Borel 집합에서 이 확률이 같다는 뜻이며, $X = Y$가 표본별로 성립한다는 뜻은 아니다.

4.2 누적분포함수의 성질

정의 4.3 (**누적분포함수**) 확률변수 X의 **누적분포함수**(*cumulative distribution function*)는 $F_X(x) = \mathbb{P}(X \le x)$이다. 문맥이 분명하면 F로 줄여 쓴다.

정리 4.4 (**분포함수의 기본 성질**) F는 비감소 함수이고 오른쪽 연속이며

$$\lim_{x \to -\infty} F(x) = 0, \qquad \lim_{x \to \infty} F(x) = 1.$$

또한 $a < b$일 때 $\mathbb{P}(a < X \le b) = F(b) - F(a)$이다.

증명. $x \le y$이면 $\{X \le x\} \subseteq \{X \le y\}$이므로 비감소한다. $x_n \downarrow x$이면 $\{X \le x_n\} \downarrow \{X \le x\}$이므로 확률의 위로부터의 연속성에서 $F(x_n) \to F(x)$를 얻는다. $\{X \le n\} \uparrow \Omega$, $\{X \le -n\} \downarrow \varnothing$에 연속성을 적용하면 양 끝의 극한이 성립한다. 마지막 식은 $\{X \le b\}$를 $\{X \le a\}$와 $\{a < X \le b\}$로 배반 분해하여 얻는다. $\square$

왼쪽 극한을 $F(x-) = \lim_{t \uparrow x} F(t)$라 하면

$$\mathbb{P}(X < x) = F(x-), \qquad \mathbb{P}(X = x) = F(x) - F(x-). \tag{4.2}$$

따라서 분포함수의 점프 크기가 그 점의 확률이다. 부등호에 등호가 있는지 없는지를 무심코 바꾸어도 되는 것은 해당 경계점의 확률이 0일 때다.

예제 4.5 (**계단형 분포함수**) X가 $-1, 0, 2$를 각각 확률 $1/4, 1/2, 1/4$로 가지면

$$F(x) = \begin{cases} 0, & x < -1, \\ 1/4, & -1 \le x < 0, \\ 3/4, & 0 \le x < 2, \\ 1, & x \ge 2. \end{cases}$$

$\mathbb{P}(0 < X \le 2) = 1/4$지만 $\mathbb{P}(0 \le X \le 2) = 3/4$이다. $x = 0$에서의 점프 $1/2$가 두 값의 차이다.

4.3 확률질량함수와 이산형 분포

정의 4.6 (**확률질량함수**) X가 유한 또는 가산 집합 S에서 확률 1로 값을 가지면 **이산형**이라 한다. 그 **확률질량함수**(*probability mass function*)는

$$p_X(x) = \mathbb{P}(X = x), \qquad x \in S$$

이며 $p_X(x) \ge 0$, $\sum_{x \in S} p_X(x) = 1$을 만족한다.

질량함수의 합은 확률 그 자체를 더한다. 반면 뒤에서 볼 밀도함수는 구간에 걸쳐 적분해야 확률을 얻는다. 이 둘을 같은 기호 f로 쓰는 책도 있지만 이 원고에서는 이산형에는 p, 밀도에는 f를 우선 사용한다.

예제 4.7 (두 주사위 합의 질량함수) S를 독립인 공정한 두 주사위의 합이라 하면

$$p_S(s) = \begin{cases} (s-1)/36, & s = 2,3,\dots,7, \\ (13-s)/36, & s = 8,9,\dots,12, \\ 0, & \text{그 밖의 값}. \end{cases}$$

분자의 합은 $1+2+\cdots+6+5+\cdots+1 = 36$이므로 정규화된다. 합이 서로 다른 결과를 구별하지 않는다는 점을 앞 장의 계수법과 연결해 볼 수 있다.

4.4 밀도는 확률이 아니라 단위 길이당 질량이다

정의 4.8 (확률밀도함수) 비음수 가측함수 f가 $\int_{\mathbb{R}} f(x)\,dx = 1$을 만족하고 모든 Borel 집합 B에 대해

$$\mathbb{P}(X \in B) = \int_B f(x)\,dx$$

이면 f를 X의 **확률밀도함수**(*probability density function*)라 한다. 이런 분포를 Lebesgue 측도에 대해 **절대연속**(*absolutely continuous*)이라고 한다.

밀도 $f(x)$는 1보다 클 수 있다. 예를 들어 $[0, 1/4]$의 균등분포는 밀도가 4다. 이 값은 한 점의 확률이 아니라 작은 길이 구간의 확률을 근사하는 비율이다. x가 밀도의 연속점이면 작은 $h>0$에 대해 $\mathbb{P}(x < X \le x+h) \approx f(x)h$다. X의 단위가 초이면 밀도의 단위는 초의 역수이므로 적분한 확률은 무차원이다. 절대연속인 경우

$$F(x) = \int_{-\infty}^{x} f(t)\,dt \tag{4.3}$$

이며 적당한 미적분 의미에서 $F' = f$가 거의 모든 점에서 성립한다. 밀도의 한 점에서의 값을 바꾸어도 적분은 바뀌지 않으므로 분포는 같을 수 있다. 그러므로 밀도는 점별로 유일하다고 말하기보다 거의 모든 곳에서 유일하다고 말한다.

예제 4.9 (정규화 상수) $f(x) = cx$를 $0 < x < 2$에서 정의하고 그 밖에서는 0으로 두자. 밀도가 되려면

$$1 = \int_0^2 cx\,dx = 2c$$

이므로 $c = 1/2$다. 이때 $0 \le x \le 2$에서 $F(x) = x^2/4$이고 $\mathbb{P}(1 < X < 2) = 1 - F(1) = 3/4$다. 끝점들의 확률은 영이므로 이 예제에서는 열린 구간과 닫힌 구간의 선택이 확률을 바꾸지 않는다.

흔한 오류. 분포함수가 연속이라는 조건만으로 밀도가 존재한다고 결론 내릴 수 없다. Cantor 분포처럼 연속이지만 절대연속이 아닌 분포가 있다. 여기서는 존재를 경고하는 데 그치고 그 구성은 측도확률론에서 다룬다.

4.5 이산과 연속이 섞인 분포

현실의 모형에는 특정 값에 양의 질량이 있으면서 나머지는 연속적인 경우가 많다. 예를 들어 대기시간이 0인 경우와 양수인 경우가 섞이거나, 측정기가 검출 한계 아래 값을 모두 0으로 기록할 수 있다.

> **예제 4.10 (영점 질량을 가진 혼합모형)** 확률 $1/3$로 $X = 0$이고, 나머지 확률 $2/3$로 $[0,1]$ 균등값을 고른다고 하자. 그러면
>
> $$F_X(x) = \begin{cases} 0, & x < 0, \\ 1/3 + (2/3)x, & 0 \le x < 1, \\ 1, & x \ge 1. \end{cases}$$
>
> $\mathbb{P}(X = 0) = 1/3$이고 $\mathbb{P}(0 < X \le 1/2) = 1/3$이다. 양의 구간에서의 밀도 $2/3$만 적분하면 전체 질량이 $2/3$이므로, 영점의 질량을 별도로 넣어야 한다. 이 분포 전체를 보통 함수 하나의 Lebesgue 밀도로 표현할 수는 없다.

4.6 분위수와 역변환 표본생성

분포함수는 평평한 구간이나 점프를 가질 수 있으므로 일반적인 역함수가 존재하지 않을 수 있다. 이를 위해 $0 < u < 1$에서 일반화된 역함수

$$Q(u) = \inf\{x \in \mathbb{R} : F(x) \ge u\} \tag{4.4}$$

를 정의한다. $Q(u)$는 u-**분위수**(*quantile*)의 한 표준적인 선택이다. 표본 분위수의 보간법은 소프트웨어마다 다를 수 있으므로 그 정의를 별도로 확인해야 한다.

> **명제 4.11 (역변환법)** U가 $(0,1)$ 균등분포를 가지면 $Q(U)$의 분포함수는 F다.

증명. 분포함수의 단조성과 오른쪽 연속성을 이용하면 $Q(u) \le x$와 $u \le F(x)$가 동치임을 확인할 수 있다. 따라서

$$\mathbb{P}(Q(U) \le x) = \mathbb{P}(U \le F(x)) = F(x). \qquad \square$$

예를 들어 $F(x) = 1 - e^{-\lambda x}$, $x \ge 0$, $\lambda > 0$이면 $Q(u) = -\log(1-u)/\lambda$다. 구현에서는 u가 정확히 1이 되지 않게 하고, 작은 u에서 $\log(1-u)$를 안정적으로 평가하는 함수를 사용한다. 수학적으로 같은 공식도 부동소수점 계산에서는 서로 다른 정확도를 가질 수 있다.

역사 (역변환법과 표본생성). 명제 4.11의 변환은 *probability integral transform*이라고도 불리며, F가 연속이면 $F(X)$가 $(0,1)$ 균등분포를 가진다는 역방향의 사실(Nikolai Smirnov, 1939년경 정리됨)과 짝을 이룬다. 일반화된 역함수 Q를 쓰면 F가 평평한 구간이나 점프를 가지는 이산형·혼합형 분포에서도 같은 방법으로 균등난수로부터 원하는 분포의 표본을 생성할 수 있다.

4.7 확률변수의 변환

$Y = g(X)$의 분포를 구하는 가장 안전한 출발점은

$$F_Y(y) = \mathbb{P}(g(X) \le y)$$

이다. 이 사건을 X에 관한 사건으로 다시 쓰고, 원래 분포로 계산한다.

정리 4.12 (일대일 미분가능 변환) 구간 I에서 X가 밀도 f_X를 가지고, $g : I \to J$가 엄격히 단조이며 역함수 $h = g^{-1}$가 미분가능하다고 하자. 해당 변환에서 변수변환 정리가 적용되면

$$f_Y(y) = f_X(h(y))\,|h'(y)|, \qquad y \in J.$$

구간 밖에서는 밀도가 0이다. 끝점이나 미분 불가능한 유한 개 점의 밀도값은 확률을 바꾸지 않는다.

절댓값은 감소함수에서 방향이 뒤집히는 것을 보정한다. $Y = aX + b$, $a \neq 0$이면

$$f_Y(y) = \frac{1}{|a|} f_X\!\left(\frac{y-b}{a}\right).$$

가로축을 $|a|$배 늘리면 밀도의 높이가 그 역수로 줄어 전체 면적 1이 보존된다.

예제 4.13 (제곱변환과 여러 원상) X가 $[-1,1]$ 균등분포이고 $Y = X^2$라 하자. $0 \le y \le 1$에서

$$F_Y(y) = \mathbb{P}(-\sqrt{y} \le X \le \sqrt{y}) = \sqrt{y}.$$

따라서 $0 < y < 1$에서 $f_Y(y) = 1/(2\sqrt{y})$다. 이 밀도는 0 근처에서 무한히 커지지만 적분은 1이다. $x \mapsto x^2$는 일대일이 아니므로 양의 제곱근만 사용하면 질량의 절반을 빠뜨린다.

4.8 결합분포와 주변분포

두 변수의 결합분포는 두 값을 함께 관찰할 때의 확률을 나타낸다. 이산형이면 $p_{X,Y}(x,y) = \mathbb{P}(X = x, Y = y)$이고

$$p_X(x) = \sum_{y} p_{X,Y}(x,y), \qquad p_Y(y) = \sum_{x} p_{X,Y}(x,y).$$

결합밀도가 존재하면 합 대신 적분하여

$$f_X(x) = \int_{\mathbb{R}} f_{X,Y}(x,y)\,\mathrm{d}y$$

를 얻는다. 주변분포만으로 결합분포는 일반적으로 결정되지 않는다. 예를 들어 공정한 비트 X에 대해 $Y = X$인 모형과 독립인 공정한 비트 Y를 새로 고르는 모형은 두 주변분포가 같지만 결합분포가 다르다.

정의 4.14 (확률변수의 독립) X, Y가 **독립**(*independent*)이라는 것은 모든 Borel 집합 A, B에 대해

$$\mathbb{P}(X \in A,\, Y \in B) = \mathbb{P}(X \in A)\mathbb{P}(Y \in B)$$

가 성립한다는 뜻이다. 이산형에서는 질량함수의 곱 분해와 동치이고, 결합밀도가 존재할 때에는 거의 모든 (x,y)에서의 밀도 곱 분해와 동치이다.

예제 4.15 (삼각형 영역의 결합밀도) $f_{X,Y}(x,y) = 2$를 $0 < x < y < 1$에서, 그 밖에서는 0으로 두자. 삼각형 넓이가 $1/2$이므로 정규화된다. 주변밀도는

$$f_X(x) = 2(1-x), \quad 0<x<1, \qquad f_Y(y) = 2y, \quad 0<y<1.$$

주변밀도의 곱은 삼각형 밖의 일부 점에서도 양수이므로 결합밀도와 다르다. 따라서 독립이 아니다. $f_Y(y) > 0$인 $0<y<1$에서 조건부 밀도는

$$f_{X\mid Y}(x\mid y) = \frac{f_{X,Y}(x,y)}{f_Y(y)} = \frac{1}{y}\mathbf{1}_{(0,y)}(x),$$

즉 $Y=y$가 주어졌을 때 X는 $(0,y)$에서 균등하다. 이 식은 영확률 사건의 단순 비율을 계산한 것이 아니라 밀도에 의한 조건부분포의 표현이다.

4.9 연습문제와 해설

연습문제 4.16 X의 질량함수가 $p(k) = ck$ $(k=1,2,3)$이다. c와 $\mathbb{P}(X>1)$을 구하라.

풀이. $c(1+2+3)=1$에서 $c=1/6$, 확률은 $5/6$이다. 질량함수는 모든 실수에서 정의할 수도 있으나 나머지 값에서는 0이다.

연습문제 4.17 $f(x) = c(1-x)$ $(0<x<1)$가 밀도일 때 c와 중앙값 m을 구하라.

풀이. 정규화에서 $c=2$다. $F(x) = 2x - x^2$이므로 $F(m)=1/2$의 구간 안 해는 $m = 1 - 1/\sqrt{2}$이다. 중앙값은 평균과 같은 개념이 아니다.

연습문제 4.18 $X \sim \mathrm{Unif}(0,1)$이고 $Y = -\log X$이다. Y의 분포함수와 밀도를 구하라.

풀이. $y<0$이면 $F_Y(y)=0$이다. $y\ge 0$이면 $\mathbb{P}(-\log X \le y) = \mathbb{P}(X \ge e^{-y}) = 1 - e^{-y}$다. 따라서 $y>0$에서 밀도는 e^{-y}이며 rate 1인 지수분포이다.

연습문제 4.19 앞의 영점 혼합모형에서 $\mathbb{P}(X \le 1/2)$와 $\mathbb{P}(X < 1/2)$가 같은가? $\mathbb{P}(X \le 0)$와 $\mathbb{P}(X<0)$는 같은가?

풀이. $1/2$에는 점질량이 없으므로 두 확률은 모두 $2/3$이다. 0에서는 두 확률이 각각 $1/3$과 0으로 다르다. 경계점의 점프를 직접 확인하면 된다.

연습문제 4.20 X, Y가 독립이고 g, h가 Borel 가측함수이면 $g(X), h(Y)$도 독립임을 설명하라.

풀이. $\{g(X)\in A\} = \{X \in g^{-1}(A)\}$이고 역상은 Borel 집합이다. Y에도 같은 표현을 적용한 뒤 X, Y의 독립성을 사용하면 원하는 곱 분해를 얻는다.

참고 (다음 연결). 분포는 변수의 모든 확률적 정보를 담는다. 다음 장의 기댓값과 분산은 그 분포를 각각 중심과 퍼짐이라는 수치로 요약한다. 이 요약값이 존재하려면 적분가능성 조건을 확인해야 한다.

제 5 장

기댓값, 분산, 공분산

개요 분포함수는 모든 구간 확률을 알려 주지만 실제 계산에서는 몇 개의 대표 수치가 필요하다. **기댓값**은 확률에 따라 가중한 중심이며, **분산**은 그 중심으로부터의 제곱거리 평균이다. 두 변수의 **공분산**은 함께 증가하거나 감소하는 선형적 경향을 나타낸다. 이 장은 기댓값의 정의와 존재 조건에서 출발하여 선형성·지시변수·꼬리합 공식, 분산·공분산의 계산법칙, Cauchy–Schwarz 부등식에 근거한 상관계수의 범위, Jensen·Markov·Chebyshev 부등식과 약한 큰수법칙, 끝으로 조건부 기댓값과 전체 분산의 분해를 차례로 세운다. 이 수치들이 같아도 분포 전체가 같지는 않으며, 어느 분포에는 평균이나 분산이 존재하지 않는다. 공식을 적용하기 전에 존재 조건을 살피는 습관이 계산 자체만큼 중요하다. 선행 지식: 확률변수의 분포, 합과 적분, 이차식의 완전제곱. 이 장의 등식은 기댓값의 존재 조건까지 함께 읽는다.

5.1 기댓값의 정의와 존재 조건

정의 5.1 (비음수 변수와 적분가능한 변수) $X \ge 0$인 이산 확률변수의 **기댓값**(*expectation*)은

$$\mathbb{E}X = \sum_{x} x P(X = x) \in [0, \infty]$$

이다. 비음수이고 밀도가 있는 경우에는 $\mathbb{E}X = \int_0^\infty x f_X(x)\,dx$이다. 일반적인 실수 확률변수에서는 $X^+ = \max(X, 0)$, $X^- = \max(-X, 0)$로 놓고

$$\mathbb{E}X = \mathbb{E}X^+ - \mathbb{E}X^-$$

로 정의하되, 우변이 $\infty - \infty$이면 정의하지 않는다. $\mathbb{E}\,|X| < \infty$인 변수를 **적분가능**하다고 하며, 이때 기댓값은 유한한 실수이다.

이 장에서 별도 언급 없이 기댓값의 선형성을 쓰면 관련 변수들이 적분가능하다고 가정한다. 비음수 변수에는 무한대 값을 허용한 등식도 유용하지만, 무한대끼리 빼는 연산을 만들면 안 된다. 혼합분포에서는 점질량의 합과 연속부분의 적분을 모두 더한다. 앞 장의 영점 질량 $1/3$과 균등분포 성분 $2/3$인 변수는 평균이 $(1/3)\cdot 0 + (2/3)\cdot(1/2) = 1/3$이다.

정리 5.2 (분포를 통한 기댓값 계산) Borel 가측함수 g에 대하여 $g(X) \ge 0$이거나 $\mathbb{E}\,|g(X)| < \infty$이면

$$\mathbb{E}[g(X)] = \sum_{x} g(x) p_X(x) \quad \text{또는} \quad \mathbb{E}[g(X)] = \int_{-\infty}^{\infty} g(x) f_X(x)\,dx$$

이다. 각각 이산분포와 밀도가 있는 분포에 대한 식이다.

이 원리는 $Y = g(X)$의 분포를 먼저 구하지 않고 평균을 계산하게 해 준다. 이산형에서는 같은 $g(x)$ 값을 갖는 원래 결과들을 모아서 더하면 증명된다. 일반형은 지시함수에 대해 성립하는

분포의 정의에서 출발하여 비음수 단순함수, 비음수 가측함수, 적분가능 함수 순서로 확장된다. 이 단계의 극한 교환을 정당화하는 단조수렴정리는 측도론적 확률론에서 다룬다.

예제 5.3 (변환의 평균) $X \sim \mathrm{Unif}(-1,1)$이면

$$\mathbb{E}X = \frac{1}{2}\int_{-1}^{1} x\,\mathrm{d}x = 0, \qquad \mathbb{E}X^2 = \frac{1}{2}\int_{-1}^{1} x^2\,\mathrm{d}x = \frac{1}{3}.$$

따라서 $\mathbb{E}[X^2] \neq (\mathbb{E}X)^2$이다. 평균에 함수를 취하는 일과 함수를 취한 뒤 평균을 내는 일은 일반적으로 교환되지 않는다.

예제 5.4 (대칭이 있어도 평균이 존재하지 않을 수 있다) 표준 Cauchy 밀도는 $f(x) = 1/[\pi(1+x^2)]$이다. 양의 부분에 대한 적분은

$$\int_0^{R} \frac{x}{\pi(1+x^2)}\,\mathrm{d}x = \frac{\log(1+R^2)}{2\pi} \longrightarrow \infty.$$

음의 부분의 절댓값 적분도 발산하므로 $\mathbb{E}X$는 정의되지 않는다. 대칭 절단 적분 $\int_{-R}^{R} x f(x)\,\mathrm{d}x = 0$은 Cauchy 주값이며 확률론의 기댓값과 다른 개념이다. 대칭인 그래프라는 이유만으로 평균을 0이라고 적으면 안 된다.

5.2 선형성, 지시변수, 꼬리합

정리 5.5 (기댓값의 선형성) $X_1, \dots, X_n$이 적분가능하고 $a_1, \dots, a_n$이 실수이면

$$\mathbb{E}\left[\sum_{i=1}^{n} a_i X_i\right] = \sum_{i=1}^{n} a_i \mathbb{E}X_i.$$

여기에는 독립성 가정이 없다. 또한 $X \le Y$가 거의 확실히 성립하면 $\mathbb{E}X \le \mathbb{E}Y$이다.

증명. 유한한 합의 선형성은 적분의 선형성에서 따른다. 단조성은 $Y - X \ge 0$의 기댓값이 비음수라는 사실을 사용한다. 이산형에서는 합의 순서를 정리하는 것만으로도 확인할 수 있다. 무한급수로 바꿀 때에는 별도의 수렴 조건이 필요하다. $\square$

사건 A의 지시변수 $\mathbf{1}_A$는 A에서 1, 그 밖에서 0이며

$$\mathbb{E}\mathbf{1}_A = \mathbb{P}(A).$$

개수를 구하는 문제를 지시변수의 합으로 바꾸면 결합분포 전체를 열거하지 않고 평균을 구할 수 있다. 특히 변수들이 서로 의존하더라도 선형성은 그대로 작동한다.

예제 5.6 (비복원 추출의 성공 개수) N개 중 K개가 성공 항목이고, 순서대로 n개를 비복원 균등추출한다. I_j를 j번째 추출이 성공인지 나타내는 지시변수라 하면 각 위치의 주변 성공확률은 K/N이다. 따라서 성공 개수 X는

$$X = \sum_{j=1}^{n} I_j, \qquad \mathbb{E}X = \frac{nK}{N}.$$

예를 들어 $N = 10$, $K = 3$, $n = 4$이면 평균 불량 개수는 1.2다. 개별 시행에서는 정수만 관측되어도 기댓값은 정수일 필요가 없다.

예제 5.7 (고정점의 평균) n개의 물건을 균등하게 순열로 재배치한다. 원래 자리에 남은 물건의 수를 F라 하자. 각 물건이 제자리에 있을 확률은 $1/n$이므로 $\mathbb{E}F = 1$이다. n이 커져도 평균은 그대로지만, 분포 전체가 같은 것은 아니다. 예를 들어 $n = 1$에서는 반드시 하나가 남고 $n = 2$에서는 0개 또는 2개가 각각 확률 $1/2$로 남는다.

명제 5.8 (꼬리합과 꼬리적분) X가 음이 아닌 정수값 변수이면, 무한대를 허용하여

$$\mathbb{E}X = \sum_{k=1}^{\infty} \mathbb{P}(X \geq k).$$

일반적인 비음수 실수값 변수이면

$$\mathbb{E}X = \int_0^{\infty} \mathbb{P}(X > t)\, \mathrm{d}t.$$

증명. 정수값 변수는 점별로 $X = \sum_{k \geq 1} \mathbf{1}_{\{X \geq k\}}$이다. 비음수 항이므로 부분합에 단조수렴을 적용하면 첫 번째 식을 얻는다. 두 번째 식은 각 $x \geq 0$에 대해 $x = \int_0^{\infty} \mathbf{1}_{\{x > t\}}\, \mathrm{d}t$인 사실과 비음수 함수에 대한 적분 순서 교환으로 얻는다. 이 비음수 조건 덕분에 유한한 평균을 미리 가정할 필요가 없다. □

흔한 오류. $\mathbb{E}(XY) = \mathbb{E}X\mathbb{E}Y$는 선형성이 아니다. X, Y가 독립이고 각각 적분가능하면 성립하지만, 일반적인 의존 변수에는 성립하지 않는다. 예를 들어 $Y = X$인 공정한 Bernoulli 변수에서는 $\mathbb{E}(XY) = 1/2$이지만 $\mathbb{E}X\mathbb{E}Y = 1/4$이다.

5.3 분산과 공분산의 계산법

정의 5.9 $\mathbb{E}X^2 < \infty$인 변수의 **분산**(*variance*)과 **표준편차**(*standard deviation*)를

$$\operatorname{Var}(X) = \mathbb{E}[(X - \mathbb{E}X)^2], \qquad \sigma_X = \sqrt{\operatorname{Var}(X)}$$

로 정의한다. 두 변수의 이차 모멘트가 유한하면 **공분산**(*covariance*)은

$$\operatorname{Cov}(X, Y) = \mathbb{E}[(X - \mathbb{E}X)(Y - \mathbb{E}Y)]$$

이다. 두 분산이 모두 양수일 때 **상관계수**(*correlation coefficient*)는

$$\rho_{X,Y} = \frac{\operatorname{Cov}(X, Y)}{\sigma_X \sigma_Y}$$

로 정의한다.

분산의 단위는 원래 변수 단위의 제곱이다. 표준편차는 원래 단위를 갖고, 상관계수는 단위가 없다. 상수인 변수는 표준편차가 0이므로 위 식으로 상관계수를 정의할 수 없다. 계산 도구가 이런 상황에서 결측값을 반환하는 것은 단순한 수치 오차가 아니다.

명제 5.10 (분산과 공분산의 항등식) 유한한 이차 모멘트 아래에서

$$\operatorname{Var}(X) = \mathbb{E}X^2 - (\mathbb{E}X)^2, \tag{5.1}$$

$$\operatorname{Var}(aX+b) = a^2 \operatorname{Var}(X), \tag{5.2}$$

$$\operatorname{Cov}(X,Y) = \mathbb{E}(XY) - \mathbb{E}X\mathbb{E}Y, \tag{5.3}$$

$$\operatorname{Var}\left(\sum_{i=1}^{n} a_i X_i\right) = \sum_{i=1}^{n} a_i^2 \operatorname{Var}(X_i) + 2\sum_{i<j} a_i a_j \operatorname{Cov}(X_i, X_j). \tag{5.4}$$

증명. 중심화한 변수 $X_i - \mathbb{E}X_i$를 사용하여 제곱을 전개하고 기댓값의 선형성을 적용한다. 첫 번째 식에서는 $\mathbb{E}[X\mathbb{E}X] = (\mathbb{E}X)^2$이고, 마지막 식에서는 모든 교차항이 두 번씩 나타난다. 제곱의 기댓값이 존재하므로 필요한 곱의 적분가능성은 아래 Cauchy–Schwarz 부등식으로 보장된다. □

독립인 두 변수의 공분산은 0이다. 식 (5.3)에서 독립이면 $\mathbb{E}(XY) = \mathbb{E}X\mathbb{E}Y$이므로 바로 따른다. 따라서 독립인 변수들의 합에서는 분산을 더할 수 있다. 그러나 합의 평균과 달리 합의 분산에는 의존성이 직접 들어간다. 같은 변수를 두 번 더한 $X+X$의 분산은 $4\operatorname{Var}(X)$이며 $2\operatorname{Var}(X)$가 아니다.

예제 5.11 (가중합과 측정 오차) $\mathbb{E}X = 2$, $\mathbb{E}Y = 5$, $\operatorname{Var}(X) = 4$, $\operatorname{Var}(Y) = 9$, $\operatorname{Cov}(X,Y) = 1$이라 하자. $Z = 3X - 2Y + 7$이면

$$\mathbb{E}Z = 3, \qquad \operatorname{Var}(Z) = 9\cdot 4 + 4\cdot 9 - 12\cdot 1 = 60.$$

평균을 계산할 때 공분산은 필요 없지만, 분산을 계산할 때에는 필요하다. 모든 수치가 유효한 결합분포에서 나온 값인지도 확인해야 한다. 여기서는 $|1| \le \sqrt{4\cdot 9} = 6$이므로 공분산의 기본 필요조건에 어긋나지 않는다.

명제 5.12 (비복원 추출의 분산) $N > 1$, $0 \le K \le N$, $0 \le n \le N$이고 X가 비복원 추출 성공 개수라 하자. $p = K/N$이면

$$\operatorname{Var}(X) = np(1-p)\frac{N-n}{N-1}.$$

증명. 앞의 지시변수에서 $\operatorname{Var}(I_j) = p(1-p)$이다. 서로 다른 위치 i, j에 대해서는

$$\mathbb{E}(I_i I_j) = \frac{K(K-1)}{N(N-1)}, \qquad \operatorname{Cov}(I_i, I_j) = -\frac{p(1-p)}{N-1}.$$

분산의 합 공식에 n개의 대각항과 $n(n-1)$개의 순서 있는 교차항을 넣으면

$$np(1-p) - n(n-1)\frac{p(1-p)}{N-1} = np(1-p)\frac{N-n}{N-1}$$

이다. □

$N = 10$, $K = 3$, $n = 4$이면 분산은 $4(0.3)(0.7)(6/9) = 0.56$이다. 같은 성공확률로 독립 복원 추출했다면 분산은 0.84였을 것이다. 비복원 추출에서 한 항목을 얻는 일이 다음 성공 가능성을 줄이는 음의 의존성이 차이를 만든다. $n = N$이면 성공 개수가 항상 K이므로 분산이 0인 것도 식에서 확인된다.

5.4 상관관계의 범위와 한계

정리 5.13 (Cauchy–Schwarz와 상관계수) $\mathbb{E}U^2, \mathbb{E}V^2 < \infty$이면

$$|\mathbb{E}(UV)|^2 \le \mathbb{E}U^2 \mathbb{E}V^2.$$

따라서 상관계수가 정의될 때 $-1 \le \rho_{X,Y} \le 1$이다. $|\rho_{X,Y}| = 1$인 것은 어떤 상수 $a \neq 0$, b에 대해 $Y = aX + b$가 거의 확실히 성립하는 것과 동치이다.

증명. 먼저 $2|UV| \le U^2 + V^2$이므로 곱은 적분가능하다. $\mathbb{E}V^2 > 0$일 때 $\mathbb{E}(U - tV)^2 \ge 0$에 $t = \mathbb{E}(UV)/\mathbb{E}V^2$를 대입하면 부등식을 얻는다. $\mathbb{E}V^2 = 0$이면 $V = 0$이 거의 확실히 성립하여 자명하다. 중심화한 $U = X - \mathbb{E}X$, $V = Y - \mathbb{E}Y$를 대입하면 상관계수의 범위가 나온다. 등호일 때 최소 제곱값이 0이므로 $U = tV$가 거의 확실히 성립한다. 양의 분산 조건 아래에서는 비례상수가 0일 수 없다. 역은 직접 계산으로 확인된다. □

여기서 비음수 변수 W에 대해 $\mathbb{E}W = 0$이면 $W = 0$이 거의 확실하다는 사실을 사용했다. 실제로 $\mathbb{P}(W \ge 1/m) \le m\mathbb{E}W = 0$이고, $\{W > 0\}$는 이 사건들의 가산 합집합이다. 특히 $\operatorname{Var}(X) = 0$이면 $X = \mathbb{E}X$가 거의 확실히 성립한다.

예제 5.14 (무상관이지만 의존하는 변수) $X \sim \mathrm{Unif}(-1, 1)$이고 $Y = X^2$라 하자. 대칭성으로 $\mathbb{E}X = \mathbb{E}X^3 = 0$이므로 $\operatorname{Cov}(X, Y) = 0$이다. 하지만 Y는 X로 완전히 결정되므로 독립이 아니다. 확률로도 확인할 수 있다.

$$\mathbb{P}(|X| \le 1/2) = \frac{1}{2}, \qquad \mathbb{P}(Y \le 1/4) = \frac{1}{2},$$

두 사건은 같은 사건이어서 교집합 확률이 $1/2$이며 주변 확률의 곱 $1/4$와 다르다. 상관계수 0은 이 예의 곡선 형태 의존성을 감지하지 못한다.

흔한 오류. 상관관계는 인과관계의 정의가 아니다. 공통 원인, 선택 과정, 시간 순서 등으로 상관이 생길 수 있다. 반대로 상관계수 0도 관계가 없다는 뜻은 아니다. 공동 정규분포처럼 추가 구조가 있을 때에만 무상관으로부터 독립을 결론낼 수 있다. 각 주변분포가 따로 정규라는 조건만으로는 충분하지 않다.

5.5 볼록성과 확률 부등식

정리 5.15 (Jensen 부등식) X가 적분가능하고 볼록함수 φ의 정의역인 구간에 거의 확실히 속한다고 하자. 필요한 기댓값이 잘 정의되면

$$\varphi(\mathbb{E}X) \le \mathbb{E}[\varphi(X)].$$

우변이 유한하지 않은 경우에도 $+\infty$를 허용하는 형태로 읽을 수 있다.

미분가능한 경우의 증명. $m = \mathbb{E}X$가 정의역 내부에 있고 φ가 m에서 미분가능하면 볼록성에 의해 $\varphi(x) \ge \varphi(m) + \varphi'(m)(x - m)$이다. 기댓값을 취하면 오른쪽 선형항의 평균이 0이 되어 결론을

얻는다. 일반적인 내부점에서는 미분계수 대신 지지직선의 기울기를 사용한다. m이 정의역의 끝점인 경우에는 $X = m$이 거의 확실히 성립하거나 구간을 축소하여 같은 결론을 얻는다. □

$\varphi(x) = x^2$이면 $(\mathbb{E}X)^2 \le \mathbb{E}X^2$이다. $X > 0$이고 관련 평균이 존재하면 $-\log x$의 볼록성으로 $\mathbb{E}\log X \le \log \mathbb{E}X$를 얻는다. 평균 수익률의 로그와 로그 수익률의 평균을 혼동해서는 안 되는 이유도 여기에 있다. φ가 오목하면 부등식의 방향이 반대이다.

역사 (Jensen, Markov, Chebyshev). 정리 5.15은 덴마크의 Johan Jensen이 1906년에 일반적인 형태로 발표하였다. 정리 5.16의 두 부등식은 러시아 St. Petersburg 학파에서 비롯한다. 부등식 $\mathbb{P}(X \ge a) \le \mathbb{E}X/a$는 Andrei Markov의 이름을 따르지만 그의 스승 Pafnuty Chebyshev가 1867년에 이미 쓴 형태에 가깝고, $\mathbb{P}(|X-\mu| \ge t) \le \sigma^2/t^2$가 오늘날 Chebyshev 부등식으로 불린다. 두 부등식은 분포의 구체적인 형태를 모를 때에도 적분가능성과 유한 분산만으로 꼬리확률의 상한을 준다는 공통점이 있다.

정리 5.16 (Markov 부등식과 Chebyshev 부등식) $X \ge 0$, $a > 0$이면

$$\mathbb{P}(X \ge a) \le \frac{\mathbb{E}X}{a}.$$

$\mu = \mathbb{E}X$, $\sigma^2 = \mathrm{Var}(X) < \infty$, $t > 0$이면

$$\mathbb{P}(|X-\mu| \ge t) \le \frac{\sigma^2}{t^2}.$$

증명. $X \ge a\mathbf{1}_{\{X \ge a\}}$의 기댓값을 취하면 Markov 부등식을 얻는다. 여기에 비음수 변수 $(X-\mu)^2$와 문턱 t^2를 넣으면 Chebyshev 부등식이 된다. □

예제 5.17 (평균만으로 얻는 상한) 비음수 대기시간 T의 평균이 3분이라고 하자. 분포를 더 모르더라도 $\mathbb{P}(T \ge 15) \le 1/5$이다. 이를 정확한 확률 0.2라고 해석하면 안 된다. 또한 음수가 가능한 오차 변수에 비음수 조건 확인 없이 Markov 부등식을 직접 적용할 수 없다. 필요하면 절댓값이나 제곱을 사용한다.

명제 5.18 (유한 분산 아래의 약한 큰수법칙) $X_1, X_2, \dots$가 서로 독립이고 공통 평균 μ, 공통 유한 분산 σ^2를 가지면, $\overline{X}_n = n^{-1}\sum_{i=1}^{n} X_i$에 대해 모든 $\varepsilon > 0$에서

$$\mathbb{P}\left(\left|\overline{X}_n - \mu\right| \ge \varepsilon\right) \le \frac{\sigma^2}{n\varepsilon^2} \longrightarrow 0.$$

증명. 선형성으로 평균은 μ이며, 독립성과 분산의 합 공식으로 분산은 σ^2/n이다. Chebyshev 부등식을 적용하면 된다. □

이 결론은 확률수렴이다. "모든 표본에서 결국 오차가 0"이라는 주장도, 유한한 n에서 오차가 절대로 일정 값을 넘지 않는다는 주장도 아니다. 거의 확실한 수렴, 중심극한정리, 종속 자료의 큰수법칙은 이후의 심화 장에서 각각 구별한다. 위 증명에서는 실제로 쌍별 무상관과 공통 유한 분산만으로도 같은 결론이 성립한다.

5.6 조건부 기댓값과 전체 분산

조건부 기댓값은 관측한 정보에 따라 달라지는 예측값이다. Y가 이산형이고 $\mathbb{P}(Y=y)>0$이면

$$m(y)=\mathbb{E}[X\mid Y=y]=\sum_{x} x\,\mathbb{P}(X=x\mid Y=y)$$

이며, 결합밀도가 있는 경우에는 조건부 밀도를 적분하여 정의한다. $\mathbb{E}[X\mid Y]$는 함수 m을 확률변수 Y에 적용한 $m(Y)$이다. 따라서 보통 하나의 상수가 아니라 확률변수이다. 확률 0인 y에서 선택한 버전은 달라도 거의 확실한 의미에서 같은 조건부 기댓값을 나타낼 수 있다.

정리 5.19 (전체 기댓값과 전체 분산) X가 적분가능하면

$$\mathbb{E}\{\mathbb{E}[X\mid Y]\}=\mathbb{E}X.$$

X가 제곱적분가능하면

$$\operatorname{Var}(X)=\mathbb{E}\{\operatorname{Var}(X\mid Y)\}+\operatorname{Var}\{\mathbb{E}[X\mid Y]\}.$$

여기서 $\operatorname{Var}(X\mid Y)=\mathbb{E}[(X-\mathbb{E}[X\mid Y])^2\mid Y]$이다.

이산 조건변수의 경우. 첫 번째 식은

$$\sum_{y}\left[\sum_{x} x\,\mathbb{P}(X=x\mid Y=y)\right]\mathbb{P}(Y=y)=\sum_{x} x\,\mathbb{P}(X=x)$$

로 확인한다. 적분가능성이 합의 교환을 보장한다. 둘째 식은 $m(Y)=\mathbb{E}[X\mid Y]$로 쓰고

$$X-\mathbb{E}X=(X-m(Y))+(m(Y)-\mathbb{E}X)$$

를 제곱한다. 교차항의 기댓값은 Y를 고정할 때 $\mathbb{E}[X-m(Y)\mid Y]=0$이므로 0이다. 두 제곱항의 기댓값이 각각 조건부 분산의 평균과 조건부 평균의 분산이다. 밀도형에서도 같은 계산을 적분으로 바꾸면 된다. 일반적인 정보에 대한 정의와 증명은 조건부 기댓값의 측도론적 성질로 확장된다. □

첫 번째 분산항은 정보를 알아도 남는 내부 변동이고, 두 번째 분산항은 조건별 평균이 달라서 생기는 변동이다. 둘 다 비음수이므로 평균적인 조건부 분산은 전체 분산보다 클 수 없다. 다만 어떤 특정 조건 $Y=y$ 아래의 분산이 전체 분산보다 항상 작다는 주장은 별개이며 일반적으로 거짓이다.

예제 5.20 (성공확률이 다른 집단의 혼합) 먼저 Θ를 0.1 또는 0.9 중 같은 확률로 선택하고, 그 값을 고정한 뒤 독립 Bernoulli 시행 10번을 한다. 성공 개수를 X라 하면

$$\mathbb{E}[X\mid\Theta]=10\Theta,\qquad \operatorname{Var}(X\mid\Theta)=10\Theta(1-\Theta)=0.9.$$

따라서 $\mathbb{E}X=5$이며

$$\operatorname{Var}(X)=0.9+100\operatorname{Var}(\Theta)=0.9+100(0.16)=16.9.$$

주변 성공확률이 $1/2$라는 이유로 $X\sim\mathrm{Bin}(10,1/2)$라고 생각하면 분산을 2.5로 잘못 계산한다. 같은 Θ를 공유하는 시행들은 조건부로는 독립이지만 주변적으로는 양의 의존성을 갖는다.

명제 5.21 (평균제곱오차와 조건부 평균) $\mathbb{E}X^2 < \infty$이고 $g(Y)$도 제곱적분가능하면

$$\mathbb{E}[(X - g(Y))^2] = \mathbb{E}[(X - \mathbb{E}[X \mid Y])^2] + \mathbb{E}[(\mathbb{E}[X \mid Y] - g(Y))^2].$$

따라서 조건부 평균은 Y의 함수들 가운데 평균제곱오차를 최소화한다.

증명은 전체 분산의 증명과 같은 중심화 및 교차항 소거이다. 이 결과는 회귀분석의 목표를 설명하지만, 조건부 평균이 반드시 직선이라는 뜻은 아니다. 선형회귀는 후보 함수를 직선 또는 지정한 선형 결합으로 제한한 별도의 근사 문제이다.

5.7 연습문제와 해설

연습문제 5.22 X가 $0, 1, 2$를 각각 확률 $1/4, 1/2, 1/4$로 갖는다. 평균, 분산, $3X - 1$의 분산을 구하라.

풀이. $\mathbb{E}X = 1$, $\mathbb{E}X^2 = 3/2$이므로 $\operatorname{Var}(X) = 1/2$이다. 마지막 분산은 $9/2$이다. 상수 -1은 퍼짐을 바꾸지 않는다.

연습문제 5.23 공정한 주사위를 20번 던진다. 여섯 눈이 모두 적어도 한 번 나올 확률을 계산하지 말고, 관측된 서로 다른 눈의 개수의 기댓값을 구하라.

풀이. 각 눈이 한 번 이상 나왔는지 나타내는 지시변수를 더한다. 특정 눈이 한 번도 나오지 않을 확률은 $(5/6)^{20}$이므로 기댓값은 $6[1 - (5/6)^{20}] \approx 5.84350$이다. 여섯 지시변수의 독립성은 필요 없다.

연습문제 5.24 독립이고 분산이 모두 σ^2인 $X_1, \dots, X_n$을 가중 평균 $T = \sum_i w_i X_i$로 결합한다. $\sum_i w_i = 1$일 때 분산의 최솟값과 달성하는 가중치를 구하라.

풀이. $\operatorname{Var}(T) = \sigma^2 \sum_i w_i^2$이다. $1 = (\sum_i w_i)^2 \le n \sum_i w_i^2$이므로 최솟값은 σ^2/n이며 $w_i = 1/n$에서 달성된다. $\sigma^2 > 0$이면 이 가중치가 유일하다. 분산이 서로 다르거나 공분산이 존재하면 결론이 달라진다.

연습문제 5.25 X의 평균이 10, 분산이 4일 때 $\mathbb{P}(|X - 10| \ge 6)$의 상한을 구하라. 정규분포를 가정해도 되는가?

풀이. Chebyshev 부등식으로 $4/36 = 1/9$이다. 두 모멘트만으로 정규성을 결론낼 수 없다. 상한은 분포 정보가 제한된 상황에서 유효한 보장이지 실제 꼬리확률의 정확한 값이 아니다.

연습문제 5.26 Y가 공정한 0–1 변수이다. $Y = 0$일 때 X의 조건부 평균과 분산이 $1, 2$이고, $Y = 1$일 때 각각 $3, 6$이다. X의 평균과 분산을 구하라.

풀이. 평균은 $(1 + 3)/2 = 2$이다. 조건부 분산의 평균은 4, 조건부 평균의 분산은 1이므로 전체 분산은 5이다. $Y = 1$에서의 조건부 분산 6은 전체 분산보다 크다. 평균적인 감소와 모든 조건에서의 감소를 구별하는 반례이다.

연습문제 5.27 $\mathbb{E}X^2 < \infty$일 때 상수 a로 예측하는 평균제곱오차가 $\mathbb{E}[(X - a)^2] = \operatorname{Var}(X) + (a - \mathbb{E}X)^2$임을 보이고 최적 상수를 구하라.

풀이. $X-a=(X-\mathbb{E}X)+(\mathbb{E}X-a)$를 제곱하면 교차항의 평균이 0이 된다. 따라서 $a=\mathbb{E}X$에서 최소이고 최솟값은 분산이다. 절대오차의 평균을 최소화하는 상수는 중앙값이며 목적함수가 바뀌면 대표값도 바뀐다.

참고 (다음 연결). 평균과 분산은 계산 원리가 단순하지만 존재 조건과 의존성에 민감하다. 다음 장에서는 자주 사용하는 분포를 지원집합, 모수화, 모멘트, 생성함수와 함께 정리한다. 분포의 이름보다 그 분포를 도입하는 가정을 먼저 확인한다.

제 6 장

핵심 확률분포와 변환 도구

개요 이 장은 확률론과 통계학에서 가장 자주 쓰이는 분포를 지원집합, 모수 범위, 질량함수 또는 밀도, 기댓값과 분산을 함께 고정하여 정의하고, 분포 사이의 정확한 관계와 극한 관계를 구별하여 증명한다. 이산 분포로 **Bernoulli 분포**, **이항분포**, **기하분포**, **음이항분포**, **초기하분포**, **Poisson 분포**를, 연속 분포로 **균등분포**, **지수분포**, **감마분포**, **베타분포**, **정규분포**, 그리고 정규분포에서 파생되는 **카이제곱분포**, t **분포**, F **분포**를 다룬다. 이어서 **확률생성함수**, **적률생성함수**, **특성함수**를 정의하고 독립합의 분포, 합성곱, 최댓값과 최솟값, 균등표본의 순서통계량을 계산한다. 선행 지식: 지수함수와 로그, 이항정리, 적분과 기본 급수, 앞 장의 기댓값과 분산(제20권 제5장). 감마함수는 이 장에서 필요한 만큼 정의한다.

분포표는 공식을 찾는 도구이지 모형을 정당화하는 도구는 아니다. 시행들이 독립인지, 성공확률이 일정한지, 추출이 복원인지, 시간의 단위가 무엇인지를 먼저 확인해야 한다. 같은 분포 이름도 모수화나 지원집합의 관례가 다를 수 있다. 이 장에서는 각 분포의 지원집합과 모수 범위를 고정하고, 정확한 등식과 근사를 구별한다. 마지막에는 확률생성함수, 적률생성함수, 특성함수를 연결하여 합과 변환을 다룬다.

6.1 Bernoulli와 이항분포

정의 6.1 (Bernoulli 분포와 이항분포) $0 \le p \le 1$일 때 $X \sim \mathrm{Bern}(p)$는

$$\mathbb{P}(X = 1) = p, \qquad \mathbb{P}(X = 0) = 1 - p$$

인 분포이다. 서로 독립이고 같은 성공확률 p인 **Bernoulli 변수** $X_1, \dots, X_n$의 합 S_n은 **이항분포**(*binomial distribution*) $\mathrm{Bin}(n, p)$를 따르며

$$\mathbb{P}(S_n = k) = \binom{n}{k} p^k (1-p)^{n-k}, \qquad k = 0, 1, \dots, n. \tag{6.1}$$

끝점 모수 $p = 0, 1$에서는 각각 0, n에 집중된 분포로 해석한다.

한 Bernoulli 변수는 $X^2 = X$이므로 $\mathbb{E}X = p$, $\mathrm{Var}(X) = p(1-p)$이다. 독립인 합에 대해

$$\mathbb{E}S_n = np, \qquad \mathrm{Var}(S_n) = np(1-p)$$

를 얻는다. 질량함수의 이항계수는 성공 위치를 고르는 수이다. 각 특정 배열의 확률이 독립성과 동일한 성공확률 때문에 $p^k(1-p)^{n-k}$로 같아진다. 독립이더라도 성공확률이 서로 다르면 일반적인 이항분포가 아니며, 그 합을 **Poisson binomial 분포**라고 부른다.

예제 6.2 (이항 확률의 직접 계산) 다섯 번의 독립 시행에서 성공확률이 0.2일 때 정확히 두 번

성공할 확률은

$$\binom{5}{2}(0.2)^2(0.8)^3 = 10 \cdot 0.04 \cdot 0.512 = 0.2048$$

이다. 한 번 이상 성공할 확률은 $1-(0.8)^5 = 0.67232$이다. 두 결과는 서로 다른 사건이다. 평균 성공 횟수는 1, 분산은 0.8이다. 평균이 1이라고 해서 정확히 한 번 성공할 확률이 1이 되는 것은 아니다.

6.2 기하분포와 음이항분포

정의 6.3 (첫 성공까지의 시행 수) $0 < p \le 1$에 대해 독립 Bernoulli 시행에서 첫 성공이 나오는 시행 번호 T는

$$\mathbb{P}(T = k) = (1-p)^{k-1}p, \qquad k = 1, 2, \dots$$

인 **기하분포**(*geometric distribution*)를 따른다. 이 장에서는 $T \sim \mathrm{Geom}(p)$라고 쓴다. 실패 횟수 $F = T - 1$을 기하분포라고 정의하는 문헌도 있으므로 지원집합을 반드시 확인한다.

$q = 1-p$라 하면 $\mathbb{P}(T > m) = q^m$ $(m = 0, 1, \dots)$이다. 앞 장의 꼬리합으로

$$\mathbb{E}T = \sum_{k=1}^{\infty} \mathbb{P}(T \ge k) = \sum_{k=1}^{\infty} q^{k-1} = \frac{1}{p}$$

를 얻는다. 급수를 미분하거나 생성함수를 사용하면

$$\mathrm{Var}(T) = \frac{1-p}{p^2}, \qquad \mathbb{E}F = \frac{1-p}{p}, \qquad \mathrm{Var}(F) = \frac{1-p}{p^2}$$

를 얻는다. $p = 0$이면 첫 성공 시간이 유한하지 않으므로 위 실수값 분포의 모수 범위에서 제외했다. 확률생성함수를 이용한 분산의 유도는 6.8절에서 보인다.

명제 6.4 (기하분포의 무기억성) $0 < p < 1$이고 음이 아닌 정수 m, n에 대해

$$\mathbb{P}(T > m + n \mid T > m) = \mathbb{P}(T > n) = q^n.$$

증명. 조건 사건의 확률은 $q^m > 0$이며 두 꼬리확률의 비는 $q^{m+n}/q^m = q^n$이다. □

이 성질은 “실패를 오래 했으니 다음 성공이 더 가까워졌다”는 직관이 일정 성공확률의 독립 시행에는 적용되지 않음을 뜻한다. 시행의 성공확률이 변하거나 시행들이 의존하면 이 모형의 무기억성을 사용할 수 없다. $p = 1$에서는 $m \ge 1$의 조건 사건 확률이 0이므로 같은 조건부 식을 쓰지 않는다.

정의 6.5 (음이항분포의 두 관례) r이 양의 정수이고 $0 < p < 1$일 때 r번째 성공까지의 전체 시행 수 T_r는

$$\mathbb{P}(T_r = k) = \binom{k-1}{r-1} p^r (1-p)^{k-r}, \qquad k = r, r+1, \dots$$

인 **음이항분포**(*negative binomial distribution*)를 따른다. 실패 개수 $F_r = T_r - r$로 쓰면

$$\mathbb{P}(F_r = f) = \binom{f+r-1}{r-1} p^r (1-p)^f, \qquad f = 0, 1, 2, \dots.$$

마지막 시행은 성공이어야 하고, 그 이전 $k-1$개 중 성공 위치 $r-1$개를 고르면 질량함수가 나온다. 서로 겹치지 않는 연속 성공 사이의 대기시간들은 독립인 기하분포이므로 T_r는 r개의 독립인 $\mathrm{Geom}(p)$의 합이고,

$$\mathbb{E}T_r = \frac{r}{p}, \qquad \mathrm{Var}(T_r) = \frac{r(1-p)}{p^2}, \qquad \mathbb{E}F_r = \frac{r(1-p)}{p}$$

이다. 통계 모형에서는 감마함수로 계수를 확장하여 양의 실수 r을 쓰는 음이항분포도 사용한다. 이때에는 정수 번째 성공이라는 문자 그대로의 시행 해석을 그대로 적용하지 않는다.

예제 6.6 성공확률 $1/4$인 독립 시행에서 세 번째 성공이 정확히 여덟 번째에 나올 확률은

$$\binom{7}{2}\left(\frac{1}{4}\right)^3\left(\frac{3}{4}\right)^5 = \frac{21\cdot 243}{4^3\cdot 4^5} = \frac{5103}{65536} \approx 0.0778656$$

이다. 평균 대기 시행 수는 $3/(1/4) = 12$이다. 평균이 12여도 여덟 번째에 종료될 가능성은 양수이다.

6.3 초기하분포와 Poisson 분포

정의 6.7 (초기하분포) N개 중 성공 항목이 K개이고 n개를 비복원 균등 추출할 때 성공 개수 X는

$$\mathbb{P}(X=k) = \frac{\binom{K}{k}\binom{N-K}{n-k}}{\binom{N}{n}}, \qquad \max(0, n-N+K) \le k \le \min(n, K)$$

인 **초기하분포**(*hypergeometric distribution*)를 따른다. 모든 모수는 정수이며 $0 \le K, n \le N$이다.

평균은 nK/N이고 $N>1$일 때 분산은 앞 장에서 구한

$$n\frac{K}{N}\left(1-\frac{K}{N}\right)\frac{N-n}{N-1}$$

이다. $N=1$인 경우는 직접 가능한 결과를 확인한다. 표본 크기가 모집단 크기에 비해 작을 때 이항분포 근사가 유용할 수 있지만, 유한 모집단 보정 $(N-n)/(N-1)$이 언제나 1인 것은 아니다. 특히 전수 추출 $n=N$에서는 초기하분포의 분산이 0이므로 독립 이항모형과 큰 차이가 난다.

정의 6.8 (Poisson 분포) $\lambda > 0$일 때 $X \sim \mathrm{Pois}(\lambda)$는

$$\mathbb{P}(X=k) = e^{-\lambda}\frac{\lambda^k}{k!}, \qquad k = 0, 1, 2, \dots$$

인 **Poisson 분포**(*Poisson distribution*)이다. $\lambda = 0$도 $X=0$인 퇴화분포로 포함할 수 있다.

지수함수의 급수 $e^{\lambda} = \sum_{k\ge 0}\lambda^k/k!$로 질량합이 1임을 확인한다. $k/k! = 1/(k-1)!$을 사용하면

$$\mathbb{E}X = \sum_{k\ge 1} e^{-\lambda}\frac{\lambda^k}{(k-1)!} = \lambda, \qquad \mathbb{E}[X(X-1)] = \sum_{k\ge 2} e^{-\lambda}\frac{\lambda^k}{(k-2)!} = \lambda^2, \qquad \mathrm{Var}(X) = \lambda^2 + \lambda - \lambda^2 = \lambda$$

이다. 평균과 분산이 같다는 성질은 Poisson 모형의 진단 단서가 될 수 있지만, 두 모멘트가 같다는 사실만으로 이 분포를 판정할 수는 없다.

예제 6.9 (구간당 사건 수) 어떤 고정 구간의 사건 수를 평균 3인 Poisson 변수로 모형화하면 사건이 한 번도 없을 확률은 $e^{-3} \approx 0.0497871$이고, 한 번 이상은 약 0.950213이다. 이 모형에는 적절한 사건 발생 가정이 필요하다. 실제 자료에 군집 발생이나 시간에 따른 강도 변화가 있으면 단순한 동일 강도 Poisson 모형이 맞지 않을 수 있다. "평균이 3"이라는 정보만으로 위 확률을 결정할 수는 없다.

정리 6.10 (희박 사건의 이항 극한) $X_n \sim \mathrm{Bin}(n, \lambda/n)$이고 $\lambda > 0$가 고정되어 있다고 하자. 충분히 큰 $n (n > \lambda)$에서 모수가 유효하며, 고정된 음이 아닌 정수 k에 대해

$$\mathbb{P}(X_n = k) \longrightarrow e^{-\lambda}\frac{\lambda^k}{k!}.$$

증명. $n \geq k$에서

$$\binom{n}{k}\left(\frac{\lambda}{n}\right)^k = \frac{\lambda^k}{k!}\prod_{j=0}^{k-1}\left(1 - \frac{j}{n}\right) \longrightarrow \frac{\lambda^k}{k!}.$$

또한 $(1-\lambda/n)^{n-k} \to e^{-\lambda}$이므로 두 인자의 곱이 결론이다. $k = 0$의 빈 곱은 1로 정의한다. □

이 정리는 극한 명제이다. 유한한 n에서 이항 확률이 Poisson 확률과 정확히 같다는 뜻은 아니다. 실제 근사 오차가 중요한 계산에서는 이항 확률을 직접 계산하거나 별도의 오차 한계를 사용한다.

예제 6.11 (근사의 크기) $\mathrm{Bin}(100, 0.03)$에서 $\mathbb{P}(X = 2) = \binom{100}{2}(0.03)^2(0.97)^{98} \approx 0.225153$이고, 같은 평균 $\lambda = 3$인 Poisson 확률은 $e^{-3} \cdot 9/2 \approx 0.224042$이다. 상대 차이는 약 0.5%이지만 두 값은 같지 않다. 평균이 같아도 분산은 $np(1-p) = 2.91$과 3으로 다르다.

역사 (Poisson 분포의 이름). Siméon Denis Poisson은 1837년의 저서에서 이 분포를 판결의 확률에 관한 극한 형태로 다루었다. 이 분포가 드문 사건의 횟수를 나타내는 모형으로 널리 알려진 것은 이후의 응용을 통해서이다.

6.4 균등분포와 지수분포

정의 6.12 (연속 균등분포) $a < b$일 때 **연속 균등분포**(*uniform distribution*) $\mathrm{Unif}(a, b)$의 밀도는

$$f(x) = \frac{1}{b-a}\mathbf{1}_{(a,b)}(x)$$

이다. 기댓값과 분산은

$$\mathbb{E}X = \frac{a+b}{2}, \qquad \mathrm{Var}(X) = \frac{(b-a)^2}{12}$$

이다. 밀도의 경계점 값은 분포를 바꾸지 않는다.

$U \sim \mathrm{Unif}(0,1)$에 $X = a + (b-a)U$를 적용하면 모멘트도 쉽게 얻는다. $\mathbb{E}U = 1/2$, $\mathbb{E}U^2 = 1/3$이므로 $\mathrm{Var}(U) = 1/12$이고 $\mathrm{Var}(X) = (b-a)^2/12$이다. 균등하다는 주장은 선택한 좌표에 의존한다. 예를 들어 U가 균등해도 U^2는 균등하지 않다. 측정 척도를 바꿀 때 밀도가 야코비안과 함께 변하는 이유이다.

정의 6.13 (지수분포의 rate 모수) $\lambda > 0$일 때 $T \sim \mathrm{Exp}(\lambda)$는

$$f_T(t) = \lambda e^{-\lambda t}\mathbf{1}_{(0,\infty)}(t), \qquad \mathbb{P}(T > t) = e^{-\lambda t} \quad (t \geq 0)$$

인 **지수분포**(*exponential distribution*)이다. 이 장에서 λ는 **rate**이며

$$\mathbb{E}T = \frac{1}{\lambda}, \qquad \operatorname{Var}(T) = \frac{1}{\lambda^2}.$$

시간의 단위가 분이면 rate의 단위는 분의 역수이다. **scale** $\theta = 1/\lambda$를 쓰는 자료에서는 밀도가 $\theta^{-1}e^{-t/\theta}$이다. 숫자만 보고 rate와 scale을 서로 바꾸어 넣으면 평균이 역수로 달라진다.

명제 6.14 (지수분포의 무기억성) $s, t \geq 0$이면

$$\mathbb{P}(T > s + t \mid T > s) = e^{-\lambda t} = \mathbb{P}(T > t).$$

반대로 비음수 실수값 변수의 생존함수 $S(t)$가 모든 $t \geq 0$에서 양수이고, $S(0) = 1$, $S(t) \to 0$이며 이 무기억성을 가지면 어떤 $\lambda > 0$에 대해 $S(t) = e^{-\lambda t}$이다.

증명. 첫 번째 식은 꼬리확률의 비로 계산한다. 역방향에서 무기억성은 $S(s+t) = S(s)S(t)$이다. $g(t) = -\log S(t)$는 비감소이고 $g(s+t) = g(s) + g(t)$를 만족한다. 먼저 유리수 $t \geq 0$에 대해 $g(t) = t g(1)$을 얻고, 단조성을 이용하여 유리수로 실수를 아래위에서 근사하면 모든 t에 성립한다. 극한 $S(t) \to 0$이므로 $g(1) > 0$이다. □

예제 6.15 rate가 시간당 2이면 30분을 넘길 확률은 $e^{-2 \cdot 0.5} = e^{-1} \approx 0.367879$이다. 이미 한 시간을 기다렸다는 조건에서 추가로 30분 이상 기다릴 확률도 같다. 이는 지수분포 모형의 결과이다. 부품의 노화나 대기열의 혼잡 변화가 있는 실제 상황에 자동으로 적용되는 물리 법칙은 아니다.

6.5 감마분포와 베타분포

정의 6.16 (감마함수와 감마분포) $\alpha > 0$에 대해

$$\Gamma(\alpha) = \int_0^\infty x^{\alpha - 1} e^{-x} \, \mathrm{d}x$$

를 **감마함수**(*gamma function*)라 한다. 부분적분으로 $\Gamma(\alpha + 1) = \alpha \Gamma(\alpha)$이고 $\Gamma(1) = 1$이다. 따라서 양의 정수 m에 대해 $\Gamma(m) = (m-1)!$이다. shape $\alpha > 0$, rate $\beta > 0$인 **감마분포**(*gamma distribution*)는

$$f(x) = \frac{\beta^\alpha}{\Gamma(\alpha)} x^{\alpha - 1} e^{-\beta x} \mathbf{1}_{(0,\infty)}(x)$$

이며 $X \sim \operatorname{Gamma}(\alpha, \beta)$라고 쓴다.

치환 $u = \beta x$로 정규화를 확인한다. 같은 치환과 감마함수의 재귀식으로, r이 실수이고 $\alpha + r > 0$이면

$$\mathbb{E}X^r = \frac{\beta^\alpha}{\Gamma(\alpha)} \int_0^\infty x^{\alpha + r - 1} e^{-\beta x} \, \mathrm{d}x = \frac{\Gamma(\alpha + r)}{\beta^r \Gamma(\alpha)}. \tag{6.2}$$

따라서 평균은 α/β, 분산은 $\alpha(\alpha+1)/\beta^2 - \alpha^2/\beta^2 = \alpha/\beta^2$이다. 특히 shape 1은 rate β의 지수분포이다. scale θ를 쓰는 관례에서는 $\theta = 1/\beta$이고 평균과 분산은 $\alpha\theta$, $\alpha\theta^2$이다.

예제 6.17 (정수 shape의 대기시간) 독립인 rate β 지수변수 m개의 합은 $\operatorname{Gamma}(m, \beta)$를 따른다. 이 성질은 뒤의 적률생성함수로 확인한다. 독립인 동일 rate 대기시간을 연속해서 더한

총시간 모형이며, $m=2$, $\beta=3$이면 평균은 $2/3$, 분산은 $2/9$이다. 서로 다른 rate의 지수변수 합은 일반적으로 이 형태의 단일 감마분포가 아니다.

정의 6.18 (베타함수와 베타분포) $\alpha,\beta>0$에 대해

$$B(\alpha,\beta)=\int_0^1 x^{\alpha-1}(1-x)^{\beta-1}\,\mathrm{d}x=\frac{\Gamma(\alpha)\Gamma(\beta)}{\Gamma(\alpha+\beta)}$$

를 **베타함수**라 한다. **베타분포** $\mathrm{Beta}(\alpha,\beta)$의 밀도는

$$f(x)=\frac{x^{\alpha-1}(1-x)^{\beta-1}}{B(\alpha,\beta)}\mathbf{1}_{(0,1)}(x).$$

감마함수와 베타함수의 관계는 양의 사분면에서 $\Gamma(\alpha)\Gamma(\beta)$를 이중적분으로 쓰고 $s=u+v$, $z=u/(u+v)$로 치환하면 얻는다. 역변환은 $u=sz$, $v=s(1-z)$이며 야코비안의 절댓값은 s다. 적분이 $\Gamma(\alpha+\beta)B(\alpha,\beta)$로 분리된다. 비음수 적분이므로 순서 교환도 정당하다.

베타함수 비율로 모멘트를 계산하면, $\mathbb{E}X=B(\alpha+1,\beta)/B(\alpha,\beta)$ 등으로부터

$$\mathbb{E}X=\frac{\alpha}{\alpha+\beta},\qquad \mathrm{Var}(X)=\frac{\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)}$$

이다. $(0,1)$의 비율이나 미지의 성공확률을 모형화할 때 자주 사용하지만, 관측된 비율이 반드시 베타분포여야 하는 것은 아니다. $\alpha=\beta=1$이면 균등분포다. 두 shape가 모두 1보다 작으면 밀도가 경계 근처에서 발산할 수 있어도 적분은 유한하다.

예제 6.19 $X\sim\mathrm{Beta}(2,3)$이면 $B(2,3)=\Gamma(2)\Gamma(3)/\Gamma(5)=1/12$이므로 $f(x)=12x(1-x)^2$이다. 평균은 $2/5$, 분산은 $1/25$이며

$$\mathbb{P}(X>1/2)=1-\left(6(1/2)^2-8(1/2)^3+3(1/2)^4\right)=\frac{5}{16}.$$

여기서는 $0<x<1$에서 $F(x)=6x^2-8x^3+3x^4$인 누적분포함수를 사용했다.

6.6 정규분포와 표준화

정의 6.20 (정규분포) $\mu\in\mathbb{R}$, $\sigma>0$일 때 **정규분포**(*normal distribution*) $N(\mu,\sigma^2)$의 밀도는

$$f(x)=\frac{1}{\sigma\sqrt{2\pi}}\exp\!\left[-\frac{(x-\mu)^2}{2\sigma^2}\right],\qquad x\in\mathbb{R}.$$

평균과 분산은 각각 μ,σ^2이다. **표준정규분포**는 $N(0,1)$이며 밀도와 분포함수를 ϕ,Φ로 쓴다.

정규화의 핵심 적분을 $I=\int_{-\infty}^{\infty}e^{-x^2/2}\,\mathrm{d}x$라 하자. 양의 함수이므로 이중적분으로 제곱한 뒤 평면의 극좌표를 사용하면

$$I^2=\int_0^{2\pi}\int_0^{\infty}e^{-r^2/2}r\,\mathrm{d}r\,\mathrm{d}\theta=2\pi.$$

$I>0$이므로 $I=\sqrt{2\pi}$이다. 대칭성으로 표준정규 평균은 0이고, 부분적분으로 이차 모멘트는 1이다. 일반 정규변수는 $X=\mu+\sigma Z$로 표현하여 모멘트를 얻는다.

명제 6.21 (정규변수의 선형 변환) $X \sim N(\mu, \sigma^2)$이면

$$Z = \frac{X - \mu}{\sigma} \sim N(0, 1).$$

$a \neq 0$에 대해 $aX + b \sim N(a\mu + b, a^2\sigma^2)$이다. 독립인 정규변수들의 선형 결합도 정규분포이며 평균과 분산은 선형성 및 분산의 합 공식으로 계산한다. 결합의 분산이 0이면 상수인 퇴화분포이다.

예제 6.22 (정규모형 안에서의 구간 확률) $X \sim N(100, 15^2)$이라면

$$\mathbb{P}(85 \le X \le 115) = \Phi(1) - \Phi(-1) \approx 0.682689.$$

단위가 있는 85, 115를 표준화할 때 표준편차 15로 나누며 분산 225로 나누지 않는다. 임의의 평균 100, 표준편차 15인 분포에서 이 숫자가 보장되는 것은 아니다. 정규분포 가정이 없으면 같은 구간의 확률이 크게 달라질 수 있다.

흔한 오류. 표준화는 중심을 0, 분산을 1로 만드는 연산이다. 임의의 변수를 표준화한다고 정규분포가 되지는 않는다. 독립인 변수의 합이 정규분포에 가까워지는 중심극한정리도 조건과 극한의 의미를 갖는 별도의 정리이다(제20권 제11장).

예제 6.23 (로그정규분포) $Z \sim N(\mu, \sigma^2)$이고 $X = e^Z$이면 X는 양수인 **로그정규변수**이다. 단조변환 공식으로

$$f_X(x) = \frac{1}{x\sigma\sqrt{2\pi}} \exp\!\left[-\frac{(\log x - \mu)^2}{2\sigma^2}\right], \qquad x > 0.$$

정규 적률생성함수를 사용하면

$$\mathbb{E}X = e^{\mu + \sigma^2/2}, \qquad \operatorname{Var}(X) = e^{2\mu + \sigma^2}\left(e^{\sigma^2} - 1\right).$$

$e^{\mathbb{E}Z} = e^{\mu}$는 X의 중앙값이며 평균은 아니다. 양의 모든 정수차 모멘트가 존재해도 X의 적률생성함수는 $t > 0$에서 발산한다. 모멘트의 존재와 영점 주변의 적률생성함수 존재는 서로 다른 조건이다.

6.7 표본분포에 자주 등장하는 세 분포

이 절의 분포들은 통계학에서 신뢰구간과 검정통계량을 구성할 때 다시 등장한다. 지금은 정의, 자유도, 모멘트 존재 조건을 구별해 둔다. 표본이 정규모형을 따른다는 등의 조건 없이 모든 자료의 통계량이 이 분포들을 따른다고 결론내릴 수는 없다.

정의 6.24 (카이제곱분포) 양의 실수 ν에 대해 **카이제곱분포** χ^2_ν는 $\mathrm{Gamma}(\nu/2, 1/2)$이다. 양의 정수 ν와 독립인 $Z_i \sim N(0,1)$에 대해서는

$$\sum_{i=1}^{\nu} Z_i^2 \sim \chi^2_\nu.$$

평균은 ν, 분산은 2ν이다.

하나의 표준정규변수를 제곱한 밀도를 두 역상으로 변환하면 shape $1/2$, rate $1/2$의 감마밀도가 나온다. 독립합에 대한 감마분포의 닫힘 성질로 정수 자유도의 표현을 얻는다. 실수 자유도에서는 감마밀도 자체가 정의이며 "실수 개의 정규변수를 더한다"는 뜻이 아니다. 평균과 분산은 식 (6.2)에서 $\alpha = \nu/2$, $\beta = 1/2$를 대입하여 평균 $\alpha/\beta = \nu$, 분산 $\alpha/\beta^2 = 2\nu$로 얻는다.

정의 6.25 (Student의 t 분포) $Z \sim N(0,1)$과 $V \sim \chi^2_\nu$가 독립이고 $\nu > 0$일 때

$$T = \frac{Z}{\sqrt{V/\nu}}$$

의 분포를 **Student의 t 분포** t_ν라고 한다. 밀도는

$$f_T(t) = \frac{\Gamma((\nu+1)/2)}{\sqrt{\nu\pi}\,\Gamma(\nu/2)}\left(1 + \frac{t^2}{\nu}\right)^{-(\nu+1)/2}.$$

평균은 $\nu > 1$일 때 0이고, 분산은 $\nu > 2$일 때 $\nu/(\nu-2)$이다.

$0 < \nu \le 1$에서는 평균이 정의되지 않는다. $1 < \nu \le 2$에서는 평균은 존재하지만 분산은 무한하다. $\nu = 1$은 표준 **Cauchy 분포**이다. 대칭인 밀도라는 사실이 평균 존재 조건을 대신하지 않는 예가 다시 나타난다. t 분포의 꼬리는 정규분포보다 느리게 감소한다.

역사 (Student의 필명). t 분포는 William Sealy Gosset이 "Student"라는 필명으로 1908년에 발표한 소표본의 평균 추론에서 유래한다.

정의 6.26 (F 분포) 독립인 $U \sim \chi^2_{d_1}$, $V \sim \chi^2_{d_2}$ $(d_1, d_2 > 0)$에 대해

$$F = \frac{U/d_1}{V/d_2}$$

의 분포를 **F 분포** F_{d_1,d_2}라고 한다. $d_2 > 2$이면 평균은 $d_2/(d_2-2)$이며, $d_2 > 4$이면

$$\operatorname{Var}(F) = \frac{2d_2^2(d_1 + d_2 - 2)}{d_1(d_2-2)^2(d_2-4)}.$$

분모 자유도가 평균과 분산의 존재를 좌우한다. 정의에서 바로 $T^2 \sim F_{1,\nu}$ $(T \sim t_\nu)$, $1/F \sim F_{d_2,d_1}$이라는 관계를 얻는다. 자유도의 순서를 바꾸면 분포가 달라지므로 첨자의 순서를 유지해야 한다.

6.8 확률생성함수와 적률생성함수

정의 6.27 (확률생성함수와 적률생성함수) 음이 아닌 정수값 변수 X의 **확률생성함수**(*probability generating function*)는

$$G_X(z) = \mathbb{E}[z^X] = \sum_{k=0}^{\infty} \mathbb{P}(X = k) z^k, \qquad 0 \le z \le 1$$

이다. $z = 0$에서는 $0^0 = 1$로 해석하여 $G_X(0) = \mathbb{P}(X = 0)$이다. 실수값 변수의 **적률생성함수**(*moment generating function*)는

$$M_X(t) = \mathbb{E}[e^{tX}]$$

이며 그 값이 유한한 t에서 사용한다. 모든 t에서 존재할 필요는 없고, 특히 0의 열린 근방에서 유한한지가 중요하다.

G_X는 $[0,1]$에서 항상 유한하다. 내부에서 급수를 미분하면 계수를 복원할 수 있으므로 분포를 결정한다. 첫 두 모멘트가 유한하면 $z \uparrow 1$인 왼쪽 극한의 의미로

$$G_X'(1) = \mathbb{E}X, \qquad G_X''(1) = \mathbb{E}[X(X-1)], \qquad \operatorname{Var}(X) = G_X''(1) + G_X'(1) - [G_X'(1)]^2.$$

$G_X''(1)$은 $\mathbb{E}X^2$ 자체가 아니라 이차 계승모멘트이다. 이 차이를 놓치면 분산식의 $G_X'(1)$ 항이 사라진다.

$M_X(t)$가 0을 포함하는 열린 구간에서 유한하면 모든 정수차 절대모멘트가 유한하고, 적분 안에서 미분할 수 있어

$$M_X^{(r)}(0) = \mathbb{E}X^r, \qquad r = 1, 2, \dots$$

이다. 이 조건 아래에서 적률생성함수는 분포를 유일하게 결정한다. 정리의 증명은 변환의 유일성 이론에 속하며 여기서는 계산 도구로 사용한다(제20권 제9장). $t = 0$에서 $M_X(0) = 1$이라는 한 점의 존재만으로 이 미분법을 정당화할 수 없다.

표 6.1 기본 분포의 생성함수

분포	$G_X(z)$	$M_X(t)$
$\operatorname{Bern}(p)$	$1 - p + pz$	$1 - p + pe^t$
$\operatorname{Bin}(n,p)$	$(1 - p + pz)^n$	$(1 - p + pe^t)^n$
$\operatorname{Pois}(\lambda)$	$e^{\lambda(z-1)}$	$e^{\lambda(e^t-1)}$

표의 세 적률생성함수는 모든 실수 t에서 유한하다. 기하분포의 경우에는 지원집합 관련과 수렴 범위를 함께 적어야 한다. T가 첫 성공까지의 시행 수이고 $q = 1-p$, $0 < p < 1$이면

$$G_T(z) = \frac{pz}{1 - qz}, \qquad M_T(t) = \frac{pe^t}{1 - qe^t} \quad (t < -\log q).$$

z 식은 적어도 $0 \le z \le 1$에서 유효하다. 실패 횟수 $F = T - 1$의 생성함수에는 분자의 z 또는 e^t가 없다.

예제 6.28 (기하분포의 분산) $G_T'(z) = p/(1-qz)^2$, $G_T''(z) = 2pq/(1-qz)^3$이므로 $G_T'(1) = 1/p$, $G_T''(1) = 2q/p^2$이다. 따라서

$$\operatorname{Var}(T) = \frac{2q}{p^2} + \frac{1}{p} - \frac{1}{p^2} = \frac{2q + p - 1}{p^2} = \frac{q}{p^2} = \frac{1-p}{p^2}$$

이며, 앞에서 인용한 값과 일치한다.

명제 6.29 (독립합의 생성함수) X, Y가 독립이면, 비음수 정수값 변수의 확률생성함수는

$$G_{X+Y}(z) = G_X(z) G_Y(z).$$

두 적률생성함수가 유한한 t에서는

$$M_{X+Y}(t) = M_X(t) M_Y(t).$$

증명. $z^{X+Y} = z^X z^Y$ 또는 $e^{t(X+Y)} = e^{tX}e^{tY}$를 사용한다. 독립성과 적분가능성에 의해 곱의 기댓값을 두 기댓값의 곱으로 분리한다. □

이에 따라 독립인 $\mathrm{Pois}(\lambda_1)$, $\mathrm{Pois}(\lambda_2)$의 합은 $\mathrm{Pois}(\lambda_1+\lambda_2)$이다. 독립 이항변수도 성공확률 p가 같으면 시행 수를 더할 수 있지만, 성공확률이 다르면 같은 결론을 쓸 수 없다. 독립성 없이 주변 생성함수만 곱하는 것도 잘못이다.

6.9 연속분포의 적률생성함수와 특성함수

감마밀도를 적분하면

$$M_X(t) = \left(\frac{\beta}{\beta - t}\right)^{\alpha}, \qquad t < \beta, \qquad X \sim \mathrm{Gamma}(\alpha, \beta).$$

따라서 같은 rate β의 독립 감마변수들을 더하면 shape를 더한 감마분포가 된다. 지수분포는 $\alpha = 1$인 특별한 경우다. 서로 다른 rate에서는 생성함수의 곱이 일반적으로 하나의 같은 꼴 감마식으로 정리되지 않는다.

정규분포에서는 지수의 완전제곱을 사용한다.

$$M_X(t) = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{\infty} \exp\!\left(tx - \frac{(x-\mu)^2}{2\sigma^2}\right) \mathrm{d}x = e^{\mu t + \sigma^2 t^2/2}.$$

남은 적분은 평균이 $\mu + \sigma^2 t$인 정규밀도의 적분이므로 1이다. 독립 정규합의 적률생성함수를 곱하면 같은 형태가 되어 정규합 성질이 증명된다. 이 계산은 $\mathbb{E}e^{rZ}$를 바로 주기 때문에 로그정규 모멘트에도 사용된다.

정의 6.30 (특성함수) 실수값 확률변수 X의 **특성함수**(*characteristic function*)는

$$\varphi_X(t) = \mathbb{E}[e^{itX}], \qquad t \in \mathbb{R}$$

이다. 여기서 $i^2 = -1$이며 실수부와 허수부의 기댓값으로 정의한다.

$|e^{itX}| = 1$이므로 특성함수는 모든 실수값 분포에 대해 모든 실수 t에서 존재한다. 항상 $\varphi_X(0) = 1$, $|\varphi_X(t)| \le 1$, $\varphi_X(-t) = \overline{\varphi_X(t)}$이며 t에 대해 연속이다. 연속성은 $e^{it_nX} \to e^{itX}$와 상계 1에 지배수렴을 적용하면 얻는다. 독립합에서는 역시 곱이 된다.

표 6.2 기본 분포의 특성함수

분포	특성함수
$N(\mu, \sigma^2)$	$e^{i\mu t - \sigma^2 t^2/2}$
$\mathrm{Pois}(\lambda)$	$e^{\lambda(e^{it}-1)}$
$\mathrm{Unif}(-a, a)$, $a > 0$	$\sin(at)/(at)$, $t \neq 0$

균등분포의 특성함수는 $t = 0$에서 연속적으로 1로 정의한다. 특성함수도 분포를 유일하게 결정하며, 적률생성함수가 없는 경우의 극한정리에도 핵심 도구가 된다. 다만 복소함수이므로

일반적인 확률이나 밀도처럼 비음수일 필요는 없다. 그 절댓값이 1 이하라는 성질과 함수 자체가 양수라는 주장은 다르다.

흔한 오류. 특성함수의 존재에는 모멘트가 필요 없지만, 원점에서 미분하여 모멘트를 얻으려면 조건을 확인해야 한다. $\mathbb{E}\,|X|^r < \infty$이면 $\varphi_X^{(r)}(0) = i^r \mathbb{E}X^r$이다. 형식적으로 t에 it를 대입하는 조작만으로 모든 적률생성함수와 특성함수의 관계를 정당화하지 않는다.

6.10 합성곱, 최댓값과 최솟값

명제 6.31 (독립합의 합성곱) 독립인 이산 변수 X, Y의 합 $S = X + Y$에 대해

$$\mathbb{P}(S = s) = \sum_{x} p_X(x)\, p_Y(s - x).$$

독립이고 밀도가 있는 경우에는 거의 모든 s에서

$$f_S(s) = \int_{-\infty}^{\infty} f_X(x)\, f_Y(s - x)\, \mathrm{d}x.$$

증명. 첫 식은 $X = x$로 사건을 분할한 뒤 독립성을 사용한다. 두 번째 식은 결합밀도 $f_X(x) f_Y(y)$를 $(x, s = x + y)$ 좌표로 바꾸고 x에 대해 적분하면 얻는다. □

의존하는 경우에는 주변밀도의 곱 대신 실제 결합밀도를 사용해야 한다.

예제 6.32 (두 균등변수의 합) 독립인 $U, V \sim \mathrm{Unif}(0,1)$에 대해 적분 구간은 $0 < u < 1$과 $0 < s - u < 1$을 동시에 만족해야 한다. 교집합 구간의 길이를 계산하면

$$f_{U+V}(s) = \begin{cases} s, & 0 < s < 1, \\ 2 - s, & 1 \le s < 2, \\ 0, & \text{그 밖}. \end{cases}$$

합이 균등하다는 추측은 틀리다. 가운데 합을 만드는 조합이 많기 때문에 삼각형 밀도가 된다. 평균은 1, 분산은 $1/6$이며 밀도를 직접 적분한 결과와 독립합 공식이 일치한다.

독립이고 동일한 분포함수 F를 갖는 $X_1, \dots, X_n$에 대해 $M_n = \max_i X_i$, $L_n = \min_i X_i$라 하면

$$\mathbb{P}(M_n \le x) = F(x)^n, \qquad \mathbb{P}(L_n > x) = [1 - F(x)]^n.$$

최댓값이 x 이하라는 것은 모든 값이 x 이하라는 뜻이므로 독립성을 적용한다. 동일분포를 가정하지 않으면 각 $F_i(x)$ 또는 $1 - F_i(x)$의 곱을 사용한다. 밀도가 있고 미분이 가능한 점에서는

$$f_{M_n}(x) = n f(x) F(x)^{n-1}, \qquad f_{L_n}(x) = n f(x) [1 - F(x)]^{n-1}.$$

예제 6.33 (지수변수 중 최초 사건) 서로 독립이고 $T_i \sim \mathrm{Exp}(\lambda_i)$이면 $t \ge 0$에서

$$\mathbb{P}\big(\min_i T_i > t\big) = \prod_i e^{-\lambda_i t} = e^{-t \sum_i \lambda_i}.$$

따라서 최솟값은 rate $\sum_i \lambda_i$인 지수분포이다. $\lambda_i = 2$인 변수 세 개라면 첫 사건까지 평균 대기시간은 $1/6$이다. 여기에서도 독립성이 핵심이며, 같은 사건 시계를 복제한 변수들에는 이 곱셈을

쓸 수 없다.

명제 6.34 (균등표본의 순서통계량) $U_1, \dots, U_n$이 독립인 $\mathrm{Unif}(0,1)$이고 $U_{(k)}$가 작은 순서로 k번째 값이면

$$U_{(k)} \sim \mathrm{Beta}(k, n+1-k), \qquad \mathbb{E}U_{(k)} = \frac{k}{n+1}.$$

증명. $U_{(k)} \le u$는 u 이하인 관측값의 개수가 적어도 k라는 사건이다. 그 개수는 $\mathrm{Bin}(n,u)$이므로 이항 꼬리확률을 미분하면

$$f_{U_{(k)}}(u) = \frac{n!}{(k-1)!(n-k)!} u^{k-1}(1-u)^{n-k}, \qquad 0<u<1$$

을 얻는다. 이것은 $\mathrm{Beta}(k, n+1-k)$의 밀도이다. 상수 $n!/((k-1)!(n-k)!) = 1/B(k,n+1-k)$이기 때문이다. □

최솟값과 최댓값은 각각 $k=1, n$인 경우다. 표본 분위수의 분포와 신뢰구간을 다룰 때 이 결과가 연결된다.

6.11 분포 선택과 계산을 점검하는 순서

실무 계산에서 다음 네 질문을 순서대로 확인하면 여러 오류를 막을 수 있다. 첫째, 변수는 횟수인지, 대기시간인지, 비율인지, 양방향 오차인지 확인한다. 둘째, 지지하는 값의 범위와 경계에서의 점질량을 확인한다. 셋째, 독립성, 동일 성공확률, 비복원 여부처럼 분포를 만드는 조건을 적는다. 넷째, 정규화, 단위, 극한 모수에서의 결과를 검산한다.

예를 들어 $\mathrm{Bin}(n,p)$에서 $p \to 0$이면 평균과 분산이 0으로 가고 질량이 0에 집중된다. n을 동시에 늘려 $np=\lambda$를 고정하면 Poisson 극한이 된다. 두 극한은 조건이 다르다. 지수분포에서는 rate를 두 배로 하면 평균이 절반이 되고, scale을 두 배로 하면 평균이 두 배가 된다. 초기하분포에서는 $n=N$일 때 분산이 0이어야 한다. 이렇게 간단한 경계 검사만으로도 모수의 역수 오류와 누락된 보정계수를 찾을 수 있다.

6.12 연습문제와 해설

연습문제 6.35 $X \sim \mathrm{Bin}(8, 1/4)$일 때 평균, 분산, 성공이 전혀 없을 확률을 구하라.

풀이. 평균은 2, 분산은 $3/2$이며 $\mathbb{P}(X=0) = (3/4)^8 = 6561/65536 \approx 0.100113$이다. 마지막 계산은 독립인 여덟 번 모두 실패할 확률이다.

연습문제 6.36 첫 성공까지의 시행 수가 $T \sim \mathrm{Geom}(1/5)$일 때 $\mathbb{P}(T>7 \mid T>4)$와 $\mathbb{E}(T-1)$을 구하라.

풀이. 무기억성으로 조건부 확률은 $(4/5)^3 = 64/125$이다. 실패 횟수의 평균은 $(1-p)/p = 4$다. T의 평균은 5이며 두 지원집합의 차이를 유지한다.

연습문제 6.37 독립인 $X \sim \mathrm{Pois}(2)$, $Y \sim \mathrm{Pois}(3)$에 대해 $X+Y$의 분포와 $\mathbb{P}(X=1 \mid X+Y=2)$를 구하라.

풀이. 합은 $\mathrm{Pois}(5)$이다. 조건부 확률은

$$\frac{\mathbb{P}(X=1,Y=1)}{\mathbb{P}(X+Y=2)} = \frac{(2e^{-2})(3e^{-3})}{e^{-5}5^2/2} = \frac{12}{25}.$$

일반적으로 합 n이 주어졌을 때 X는 $\mathrm{Bin}(n, 2/5)$를 따른다. 두 Poisson 질량함수의 곱을 합의 질량으로 나누면 이항계수가 나타난다.

> **연습문제 6.38** 독립인 $X_1 \sim \mathrm{Gamma}(2,3)$, $X_2 \sim \mathrm{Gamma}(4,3)$의 합의 분포와 평균을 구하라. 두 번째 변수의 rate가 5로 바뀌면 같은 방식으로 shape만 더할 수 있는가?

풀이. 같은 rate이므로 합은 $\mathrm{Gamma}(6,3)$이며 평균은 2이다. rate가 달라지면 적률생성함수의 곱은 $(3/(3-t))^2(5/(5-t))^4$이므로 일반적으로 단일 감마 형태가 아니다. 평균은 여전히 선형성으로 $2/3 + 4/5 = 22/15$이다.

> **연습문제 6.39** 독립인 표준정규변수 Z_1, Z_2에 대해 $3Z_1 - 4Z_2$의 분포를 구하라. $Z_2 = Z_1$로 바뀌면 어떻게 되는가?

풀이. 독립이면 평균 0, 분산 $9+16=25$인 $N(0,25)$이다. 같은 변수이면 $-Z_1$이므로 $N(0,1)$이다. 주변분포만으로 합의 분포가 정해지는 것은 아니다.

> **연습문제 6.40** 독립인 균등변수 세 개 $U_i \sim \mathrm{Unif}(0,1)$의 최댓값 M에 대해 $\mathbb{P}(M \le 1/2)$와 $\mathbb{E}M$을 구하라.

풀이. 분포함수는 $F_M(x) = x^3$ $(0 \le x \le 1)$이므로 확률은 $1/8$이다. 밀도는 $3x^2$이며 평균은 $\int_0^1 3x^3\,dx = 3/4$이다. 베타분포 $\mathrm{Beta}(3,1)$의 평균으로도 검산한다.

> **연습문제 6.41** $G_X(z) = (1+z+z^2)/3$인 변수의 분포, 평균, 분산을 구하라.

풀이. $0,1,2$에 각각 질량 $1/3$인 분포이다. $G_X'(1) = 1$, $G_X''(1) = 2/3$이므로 분산은 $2/3+1-1 = 2/3$이다. 직접 모멘트로 계산하면 $\mathbb{E}X^2 = 5/3$이어서 같은 결과를 얻는다.

> **연습문제 6.42** $T \sim t_3$이면 평균과 분산은 얼마인가? $T \sim t_1$일 때 대칭성을 근거로 평균을 0이라고 둘 수 있는가?

풀이. t_3의 평균은 0, 분산은 3이다. t_1은 Cauchy 분포여서 평균이 정의되지 않는다. 분포의 대칭 중심과 기댓값은 존재 조건을 확인한 뒤에만 같은 수치로 연결할 수 있다.

참고 (다음 연결). 이 여섯 장은 확률 모형을 읽고 기본 계산을 수행하는 출발점이다. 다음 확률론 묶음에서는 확률수렴과 거의 확실한 수렴, 큰수법칙과 중심극한정리의 정확한 가정, 조건부 기댓값의 일반 정의, 마팅게일과 확률과정으로 범위를 넓힌다. 통계학에서는 모수를 모르는 상황에서 자료로 추론한다는 별도의 문제를 이 확률 언어 위에 세운다.

제 7 장

결합분포와 다변수 변환

개요 **결합분포**(*joint distribution*)는 여러 확률변수를 한 벡터로 묶어 그 벡터가 놓이는 영역의 확률을 지정하는 분포이다. 한 변수의 분포만 알면 그 변수에 관한 확률은 계산할 수 있으나, 여러 변수의 합·차·비율·최댓값은 변수들이 함께 움직이는 방식에 달려 있고 주변분포는 이 정보를 담지 않는다. 이 장은 결합분포함수·결합질량·결합밀도와 지원집합, 공분산 행렬과 다변량 정규분포, 일대일 좌표변환에 따른 밀도 변환 공식(야코비안), 극좌표 변환과 감마–베타 분해, 최솟값과 최댓값의 결합밀도를 차례로 세우고, 좌표를 바꿀 때 확률 질량이 어떻게 보존되는지를 계산으로 보인다. 선행 지식: 주변분포와 독립성, 이중적분, 행렬식과 야코비안, 제20권 제6장의 밀도 변환. 이 장에서는 결합분포의 기하와 좌표변환을 중심으로 다룬다.

7.1 결합분포, 주변분포, 지원집합

정의 7.1 (결합분포함수) 실수값 **확률벡터**(*random vector*) (X, Y)의 **결합분포함수**는

$$F_{X,Y}(x, y) = \mathbb{P}(X \le x,\, Y \le y), \qquad (x, y) \in \mathbb{R}^2$$

이다. 직사각형의 확률은 네 모서리의 값을 포함배제하여 얻는다.

$$\mathbb{P}(a < X \le b,\, c < Y \le d) = F(b,d) - F(a,d) - F(b,c) + F(a,c), \qquad a < b,\ c < d. \tag{7.1}$$

결합분포함수는 각 좌표에 대해 비감소이고 오른쪽 연속이며, 두 좌표가 모두 $+\infty$로 가면 1로, 어느 한 좌표가 $-\infty$로 가면 0으로 수렴한다. 그러나 두 좌표 각각에서 비감소라는 성질만으로 유효한 결합분포함수가 되는 것은 아니다. 식 (7.1)의 직사각형 증가량이 항상 비음수여야 한다. 예를 들어 $F(x,y) = \mathbf{1}\{x + y \ge 0\}$은 각 좌표에서 비감소이고 극한 조건도 만족하지만, $a = c = -1$, $b = d = 1$이면 직사각형 증가량이 $F(1,1) - F(-1,1) - F(1,-1) + F(-1,-1) = 1 - 1 - 1 + 0 = -1 < 0$이어서 결합분포함수가 아니다. 이 때문에 유효한 주변분포 두 개를 아무 방식으로 조합해도 결합분포가 되지는 않는다.

이산형 **결합질량** $p(x,y)$는 비음수이며 전체 합이 1이다. **주변질량**은 행 또는 열에 해당하는 값을 더하여 얻는다. 밀도형에서는

$$f_X(x) = \int_{\mathbb{R}} f_{X,Y}(x,y)\, \mathrm{d}y, \qquad f_Y(y) = \int_{\mathbb{R}} f_{X,Y}(x,y)\, \mathrm{d}x \tag{7.2}$$

이다. 적분의 실제 범위는 **지원집합**(*support*)과 함께 결정된다. 삼각형 지원집합을 직사각형인 것처럼 독립적인 적분 구간으로 바꾸면 정규화부터 틀릴 수 있다. 두 변수가 독립이면 결합밀도는 주변밀도의 곱이므로 지원집합은 반드시 직사각형(의 거의 모든 점)이어야 한다. 이 사실이 독립성의 가장 빠른 반증 수단이다.

예제 7.2 (지원집합부터 확인하기) $f_{X,Y}(x,y) = c$가 $0 < x < y < 2$에서만 양수라고 하자. 삼각형의 면적이 2이므로 $c = 1/2$이다. 주변밀도는

$$f_X(x) = \frac{2-x}{2}\,\mathbf{1}_{(0,2)}(x), \qquad f_Y(y) = \frac{y}{2}\,\mathbf{1}_{(0,2)}(y)$$

이다. 따라서

$$\mathbb{E}X = \int_0^2 x\,\frac{2-x}{2}\,dx = \frac{2}{3}, \qquad \mathbb{E}Y = \int_0^2 \frac{y^2}{2}\,dy = \frac{4}{3}, \qquad \mathbb{E}(XY) = \frac{1}{2}\int_0^2\int_0^y xy\,dx\,dy = 1$$

이고, $\operatorname{Cov}(X,Y) = 1 - \tfrac{2}{3}\cdot\tfrac{4}{3} = \tfrac{1}{9}$이다. 독립이라면 결합밀도가 주변밀도의 곱이어야 하지만, 곱은 $x > y$인 일부 점에서도 양수이므로 독립일 수 없다.

7.2 공분산 행렬과 다변량 정규분포

정의 7.3 (평균벡터와 공분산 행렬) $X = (X_1,\dots,X_d)^{\top}$의 각 성분이 제곱적분가능하면 **평균벡터**와 **공분산 행렬**(*covariance matrix*)을

$$\mu = \mathbb{E}X, \qquad \Sigma = \mathbb{E}\big[(X-\mu)(X-\mu)^{\top}\big]$$

로 정의한다. (i,j) 성분은 $\operatorname{Cov}(X_i,X_j)$이다.

모든 $a \in \mathbb{R}^d$에 대해

$$a^{\top}\Sigma a = \operatorname{Var}(a^{\top}X) \ge 0$$

이므로 Σ는 대칭 양의 준정부호 행렬이다. 따라서 임의의 숫자들을 대칭으로 배치했다고 해서 공분산 행렬이 되는 것은 아니다. 선형변환 $Y = AX + b$에서는

$$\mathbb{E}Y = A\mu + b, \qquad \operatorname{Cov}(Y) = A\Sigma A^{\top}$$

이다. 행렬의 곱 순서와 전치는 차원 확인만으로도 자주 검산할 수 있다. A가 $k\times d$ 행렬이면 $A\Sigma A^{\top}$는 $k\times k$이다.

정의 7.4 (다변량 정규분포) 확률벡터 X의 모든 선형 결합 $a^{\top}X$가 정규분포 또는 상수인 퇴화분포이면 X를 **다변량 정규벡터**(*multivariate normal vector*)라고 한다. 평균 μ, 공분산 Σ인 경우 $N_d(\mu,\Sigma)$로 쓴다. Σ가 양의 정부호이면 밀도는

$$f(x) = \frac{\exp\!\big[-(x-\mu)^{\top}\Sigma^{-1}(x-\mu)/2\big]}{(2\pi)^{d/2}(\det\Sigma)^{1/2}}, \qquad x \in \mathbb{R}^d \tag{7.3}$$

이다.

Σ가 특이하면 $\mathbb{R}^d$의 Lebesgue 측도에 대한 위 밀도는 존재하지 않는다. 그렇다고 정규분포 자체가 정의되지 않는 것은 아니다. 예를 들어 (Z,Z)는 직선 $y=x$ 위에 지지된 정규벡터이며 공분산 행렬 $\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}$의 행렬식은 0이다. 행렬식을 분포에 넣기 전에 비특이성을 확인해야 한다. 특이한 경우까지 포함하는 일반 정의는 특성함수 $\exp(it^{\top}\mu - t^{\top}\Sigma t/2)$로 주어진다(제20권 제9장).

명제 7.5 (공동 정규성 아래의 독립) 공동 정규벡터의 두 성분이 무상관이면 독립이다. 더 일반적으로 두 부분벡터 사이의 모든 교차 공분산이 0이면 두 부분벡터는 독립이다.

비특이한 경우에는 블록 대각 공분산 행렬의 밀도 (7.3)이 두 밀도의 곱으로 분리됨을 보면 된다. (Σ가 블록 대각이면 $\det\Sigma$는 블록 행렬식의 곱이고 이차형식 $(x-\mu)^{\top}\Sigma^{-1}(x-\mu)$는 두 이차형식의 합이다.) 특이한 경우까지 포함하려면 특성함수 $\exp(it^{\top}\mu - t^{\top}\Sigma t/2)$의 곱 분해와 유일성을 사용한다. 이 정리에는 공동 정규성이 필요하다. 성분들이 각각 정규라는 조건은 더 약하다.

예제 7.6 (정규 주변분포만으로는 부족하다) $Z \sim N(0,1)$이고, 독립인 부호 S가 ± 1을 같은 확률로 갖는다고 하자. $X = Z$, $Y = SZ$이면 각각 표준정규이며

$$\mathbb{E}(XY) = \mathbb{E}(SZ^2) = \mathbb{E}S\,\mathbb{E}Z^2 = 0$$

이다. 하지만 $|X| = |Y|$가 항상 성립하므로 독립이 아니다. 또한 $X+Y$는 확률 $1/2$로 정확히 0이 되고 나머지에서는 $2Z$이므로 일반적인 정규분포도, 상수분포도 아니다. 따라서 (X,Y)는 공동 정규벡터가 아니다. 무상관인 두 정규변수가 독립이 아닐 수 있다는 점에서 명제 7.5의 "공동"이라는 조건은 생략할 수 없다.

7.3 일대일 좌표변환과 야코비안

정리 7.7 (다변수 밀도 변환) X가 열린집합 $D \subset \mathbb{R}^d$ 위에 밀도 f_X를 가지고 $(\mathbb{P}(X \in D) = 1)$, $h : D \to E$가 열린집합 E 위로의 일대일 대응이며 h와 역함수가 연속 미분가능하고 역변환의 야코비안 행렬식이 영이 아니라고 하자. $Y = h(X)$의 밀도는

$$f_Y(y) = f_X\big(h^{-1}(y)\big)\,\big|\det Dh^{-1}(y)\big|, \qquad y \in E \tag{7.4}$$

이며 E 밖에서는 0이다. 영확률 경계나 제외집합은 별도로 처리할 수 있다.

증명. $B \subseteq E$가 보렐 집합이면 $\mathbb{P}(Y \in B) = \mathbb{P}(X \in h^{-1}(B)) = \int_{h^{-1}(B)} f_X(x)\,\mathrm{d}x$이다. 다변수 적분의 변수변환 정리 $(x = h^{-1}(y))$로 이를 B 위의 적분 $\int_B f_X(h^{-1}(y))\,\big|\det Dh^{-1}(y)\big|\,\mathrm{d}y$로 바꾸면 제시한 밀도가 나온다. 역변환의 행렬식이 등장하는 이유는 원래 확률 질량을 새로운 좌표의 부피로 나누기 때문이다. □

변환이 여러 대 일이라면 역상의 가지들을 나누어 밀도 기여를 더해야 한다. 야코비안의 부호도 확률의 부호가 될 수 없으므로 절댓값을 취한다. 실전에서는 원래 영역, 역변환, 새 영역, 행렬식, 정규화의 순서로 적는 것이 안전하다.

예제 7.8 (합과 차) 독립인 $X, Y \sim N(0,1)$에 대해 $U = X+Y$, $V = X-Y$로 놓는다. 역변환은

$$X = \frac{U+V}{2}, \qquad Y = \frac{U-V}{2}, \qquad \left|\det \frac{\partial(x,y)}{\partial(u,v)}\right| = \frac{1}{2}$$

이다. $x^2 + y^2 = (u^2+v^2)/2$이므로

$$f_{U,V}(u,v) = \frac{1}{2\pi}\,e^{-(u^2+v^2)/4}\cdot\frac{1}{2} = \frac{1}{4\pi}\exp\!\left(-\frac{u^2+v^2}{4}\right)$$

이다. 이 식은 $N(0,2)$ 밀도 둘의 곱이므로 U, V는 독립이고 각각 분산이 2이다. 정규변수가 아닌 경우에는 합과 차가 무상관이더라도 독립일 필요가 없다. 동일분포인 독립 변수 X, Y에서

$\operatorname{Cov}(X+Y, X-Y) = \operatorname{Var} X - \operatorname{Var} Y = 0$이지만, 예컨대 X, Y가 독립인 $\mathrm{Bern}(1/2)$이면 $X+Y=0$이거나 2일 때 $X-Y=0$이 되어 독립이 아니다.

7.4 극좌표와 반지름의 분포

독립 표준정규 X, Y에 대해

$$X = R\cos\Theta, \qquad Y = R\sin\Theta, \qquad R>0, \quad 0 \le \Theta < 2\pi$$

로 쓴다. 원점과 각도의 경계는 확률 0이므로 적절한 열린 영역들로 나누어 변환한다. 역방향, 즉 (r,θ)에서 (x,y)로 가는 야코비안의 절댓값은 r이다. 그러므로

$$f_{R,\Theta}(r,\theta) = \frac{1}{2\pi}\, r e^{-r^2/2}\, \mathbf{1}_{(0,\infty)}(r)\, \mathbf{1}_{[0,2\pi)}(\theta) \tag{7.5}$$

이다. 밀도가 곱으로 분리되므로 반지름과 각도는 독립이다. 각도는 균등하고 반지름은 **Rayleigh 밀도** $r e^{-r^2/2}$를 갖는다. 원래 평면의 정규밀도를 그대로 r의 밀도로 쓰면 원둘레 방향으로 축적되는 부피 인자 r을 잃는다.

예제 7.9 (정규 난수의 좌표 구성) 독립 $U, V \sim \mathrm{Unif}(0,1)$이면

$$R = \sqrt{-2\log U}, \qquad \Theta = 2\pi V, \qquad X = R\cos\Theta, \qquad Y = R\sin\Theta$$

로 만든 X, Y는 독립 표준정규이다. 실제로 $\mathbb{P}(R>r) = \mathbb{P}(U < e^{-r^2/2}) = e^{-r^2/2}$이고 R, Θ는 독립이므로 식 (7.5)의 결합밀도를 역으로 따른다. 이 구성은 Box–Muller 변환으로 알려져 있다. 유한 정밀도 난수 구현에서는 $U=0$을 넣으면 로그가 정의되지 않으므로 생성기의 끝점 규약을 확인해야 한다. 수학적 연속 균등모형에서는 그 사건의 확률이 0이다.

7.5 감마변수의 합과 비율

정리 7.10 (감마–베타 분해) $X \sim \mathrm{Gamma}(\alpha,\lambda)$, $Y \sim \mathrm{Gamma}(\beta,\lambda)$가 독립이고 $\alpha,\beta,\lambda>0$이라 하자. 같은 *rate* λ를 사용한다. 그러면

$$S = X+Y, \qquad Z = \frac{X}{X+Y}$$

는 서로 독립이고

$$S \sim \mathrm{Gamma}(\alpha+\beta,\lambda), \qquad Z \sim \mathrm{Beta}(\alpha,\beta)$$

이다.

증명. 역변환은 $X = SZ$, $Y = S(1-Z)$이고 새 영역은 $s>0$, $0<z<1$이다. 역변환 야코비안 $\det \frac{\partial(x,y)}{\partial(s,z)} = \det\begin{pmatrix} z & s \\ 1-z & -s \end{pmatrix} = -s$의 절댓값은 s이다. 원래 밀도 곱 $\dfrac{\lambda^{\alpha+\beta}}{\Gamma(\alpha)\Gamma(\beta)} x^{\alpha-1}y^{\beta-1}e^{-\lambda(x+y)}$에 이를 곱하면

$$\begin{aligned} f_{S,Z}(s,z) &= \frac{\lambda^{\alpha+\beta}}{\Gamma(\alpha)\Gamma(\beta)}\, s^{\alpha+\beta-2} z^{\alpha-1}(1-z)^{\beta-1} e^{-\lambda s}\cdot s \\ &= \frac{\lambda^{\alpha+\beta}}{\Gamma(\alpha+\beta)}\, s^{\alpha+\beta-1}e^{-\lambda s} \;\times\; \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}\, z^{\alpha-1}(1-z)^{\beta-1} \end{aligned}$$

이다. 두 인수는 각각 감마밀도와 베타밀도이며 영역도 곱집합이다. 따라서 두 분포와 독립성을 모두 얻는다. □

예제 7.11 독립인 동일 *rate* 지수변수 X, Y는 $\alpha = \beta = 1$인 경우이므로 $X/(X+Y) \sim \mathrm{Beta}(1,1)$, 곧 $(0,1)$에서 균등하다. 두 양의 대기시간의 합이 주어져도 그 합에서 첫 변수가 차지하는 비율의 조건부분포는 그대로이다. *rate*가 다르면 지수항이 $e^{-s[\lambda_1 z + \lambda_2(1-z)]}$가 되어 s와 z에 대한 곱분해가 되지 않는다. 동일 *rate* 조건이 독립성 결론에서 중요한 역할을 한다.

7.6 최솟값과 최댓값의 결합분포

앞 묶음에서는 순서통계량 하나의 분포를 구했다. 여기서는 독립 균등표본 $U_1, \dots, U_n$ $(n \ge 2)$의 최솟값 L, 최댓값 M을 함께 다룬다. 이들은 당연히 $L < M$(거의 확실히)을 만족하므로 독립일 수 없다. $0 < l < m < 1$에서 결합밀도는

$$f_{L,M}(l,m) = n(n-1)(m-l)^{n-2} \tag{7.6}$$

이다. 작은 구간 $[l, l+\mathrm{d}l]$에 최솟값을 맡을 관측을 고르는 방법이 n개이고, $[m, m+\mathrm{d}m]$에 최댓값을 맡을 관측이 $n-1$개이다. 나머지 $n-2$개가 사이에 있을 확률이 $(m-l)^{n-2}$인 것이 식의 구조이다. 엄밀하게는 $\mathbb{P}(L > l, M \le m) = (m-l)^n$ $(l < m)$을 두 경계에 대해 미분하여, 곧 $f_{L,M} = -\partial_l \partial_m \mathbb{P}(L > l, M \le m)$로 같은 식을 얻는다.

범위 $R = M - L$과 L로 변환하면 야코비안은 1이고 $0 < r < 1$, $0 < l < 1 - r$이다. 따라서

$$f_R(r) = \int_0^{1-r} n(n-1) r^{n-2} \, \mathrm{d}l = n(n-1) r^{n-2}(1-r)\, \mathbf{1}_{(0,1)}(r),$$

즉 $R \sim \mathrm{Beta}(n-1, 2)$이며 $\mathbb{E}R = (n-1)/(n+1)$이다. 표본이 커질수록 범위가 1에 가까워지는 방향과 평균식이 일치한다. $n = 1$이면 범위는 항상 0이므로 위 밀도식의 가정에서 제외했다.

7.7 연습문제와 해설

연습문제 7.12 $f(x,y) = cxy$가 $0 < x < 1$, $0 < y < 2$에서의 밀도이다. c와 독립 여부를 구하라.

풀이. $\int_0^1 x\,\mathrm{d}x \int_0^2 y\,\mathrm{d}y = \tfrac{1}{2} \cdot 2 = 1$이므로 $c = 1$이다. 주변밀도는 $2x$와 $y/2$이며 곱이 xy이므로 독립이다. 영역이 직사각형이라는 조건까지 함께 사용했다.

연습문제 7.13 $\mathrm{Var}(X) = 1$, $\mathrm{Var}(Y) = 4$, $\mathrm{Cov}(X,Y) = 3$인 확률벡터가 존재하는가?

풀이. 존재하지 않는다. 공분산 행렬의 행렬식이 $4 - 9 = -5$여서 양의 준정부호가 아니며, Cauchy–Schwarz의 $|\mathrm{Cov}(X,Y)| \le 2$에도 어긋난다.

연습문제 7.14 독립 표준정규 X, Y에 대해 $R = \sqrt{X^2 + Y^2}$일 때 $\mathbb{P}(R > 2)$를 구하라.

풀이. Rayleigh 생존함수로 $\mathbb{P}(R > 2) = e^{-2} \approx 0.135335$이다. $R^2 \sim \chi^2_2 = \mathrm{Gamma}(1, 1/2)$를 사용해도 같은 결과를 얻는다.

연습문제 7.15 동일 *rate*인 독립 감마변수의 *shape*가 $2, 3$일 때 $Z = X/(X+Y)$의 평균과 $\mathbb{P}(Z > 1/2)$를 구하라.

풀이. $Z \sim \mathrm{Beta}(2,3)$이므로 평균은 $2/5$이고, 밀도 $12z(1-z)^2$를 $[0,1/2]$에서 적분하면 $\mathbb{P}(Z \le 1/2) = 12\left(\frac{1}{8} - \frac{1}{12} + \frac{1}{64}\right) = \frac{11}{16}$이므로 $\mathbb{P}(Z > 1/2) = 5/16$이다. 공통 *rate*는 비율의 분포에서 사라지지만 두 *rate*가 같다는 조건 자체는 필요하다.

연습문제 7.16 독립 균등표본 네 개의 범위 R에 대해 $\mathbb{E}R$과 $\mathbb{P}(R \le 1/2)$를 구하라.

풀이. $n = 4$이므로 평균은 $3/5$이다. 밀도는 $12r^2(1-r)$이므로 누적분포는 $4r^3 - 3r^4$이며 $r = 1/2$에서 $\frac{1}{2} - \frac{3}{16} = \frac{5}{16}$이다.

다음 연결. 변환 문제에서 지원집합과 야코비안은 계산의 부속 조건이 아니라 밀도 자체의 일부이다. 다음 장은 같은 결합분포를 관측한 정보에 따라 다시 정리하는 조건부 기댓값을 다룬다(제20권 제8장).

제 8 장

조건부 기댓값과 정보의 수학

개요 **조건부 기댓값**(*conditional expectation*)은 관측된 정보 $\mathcal{G}$로 구별할 수 있는 사건들 위에서 원래 변수와 평균이 일치하는 $\mathcal{G}$-가측 변수이다. 양의 확률인 사건을 조건으로 하는 분모 공식은 연속 관측값이나 무수히 많은 관측 사건을 다루기에는 모자라고, 이 장의 정의는 영확률 관측값의 어려움을 피하면서 예측·회귀·통계적 조건화의 공통 언어를 제공한다. 이 장은 정보를 나타내는 σ-대수, 조건부 기댓값의 정의와 거의 확실한 유일성, 분할과 밀도를 이용한 계산, 영확률 조건에서 근방 선택이 결과를 바꾸는 예, 선형성·꺼내기·탑 성질, 그리고 제곱적분 공간에서의 직교 투영과 최적 예측을 차례로 다룬다. 선행 지식: 적분가능성, σ-대수, 조건부분포. Radon–Nikodym 정리는 존재 근거로만 소개하며 그 측도론적 증명은 요구하지 않는다.

8.1 정보를 나타내는 σ-대수

변수 Y를 관측하면 $\{Y \in B\}$ 꼴의 사건이 일어났는지 판단할 수 있다. 이 사건들이 만드는 σ-대수를 $\sigma(Y)$라고 하며 Y가 생성하는 **정보 σ-대수**(*information σ-algebra*)로 해석한다. 정보가 많을수록 구별할 수 있는 사건이 많으므로 사건족이 커진다. 아무 정보도 없으면 $\{\varnothing, \Omega\}$이고, 모든 원래 정보를 알면 $\mathcal{F}$이다.

> **예제 8.1 (유한 공간의 정보)** 공정한 주사위 결과를 X라 하고 짝수 여부 $Y = \mathbf{1}_{\{X\text{가 짝수}\}}$만 관측하자. $\sigma(Y)$는 빈집합, 전체집합, 짝수 결과의 집합 $\{2,4,6\}$, 홀수 결과의 집합 $\{1,3,5\}$로 이루어진다. X 자체를 관측할 때의 사건족 $2^{\{1,\dots,6\}}$보다 작다. 이 정보만으로 만드는 실수 예측값은 모든 홀수 결과에 같은 값을 주고 모든 짝수 결과에 같은 값을 주어야 한다.

> **정의 8.2 (정보에 대한 조건부 기댓값)** X가 적분가능하고 $\mathcal{G} \subseteq \mathcal{F}$가 σ-대수라고 하자. 다음을 만족하는 적분가능한 $\mathcal{G}$-가측 변수 Z를 $\mathbb{E}[X \mid \mathcal{G}]$의 한 **버전**(*version*)이라 한다.
>
> $$\mathbb{E}[Z\mathbf{1}_A] = \mathbb{E}[X\mathbf{1}_A], \qquad A \in \mathcal{G}. \tag{8.1}$$
>
> $\mathbb{E}[X \mid Y]$는 $\mathbb{E}[X \mid \sigma(Y)]$를 뜻한다.

$\mathcal{G}$-가측이라는 조건은 주어진 정보만으로 예측값을 정할 수 있다는 뜻이다. 적분 일치 조건은 정보로 구별할 수 있는 어떤 부분집단에서도 체계적으로 평균을 더하거나 빼지 않도록 한다. $A = \Omega$를 넣으면 전체 기댓값 공식 $\mathbb{E}\big[\mathbb{E}[X \mid \mathcal{G}]\big] = \mathbb{E}X$가 즉시 나온다.

> **명제 8.3 (거의 확실한 유일성)** 같은 $X, \mathcal{G}$에 대해 두 버전 Z, W가 위 정의를 만족하면 $Z = W$가 거의 확실히 성립한다.

증명. $A = \{Z > W\} \in \mathcal{G}$이다. 정의 식 (8.1)을 서로 빼면 $\mathbb{E}[(Z-W)\mathbf{1}_A] = 0$이다. 적분하는 변수 $(Z-W)\mathbf{1}_A$는 비음수이므로 거의 확실히 0이다. 그런데 A 위에서 $Z - W > 0$이므로 $\mathbb{P}(Z > W) = 0$이다. Z와 W의 역할을 바꾸면 $\mathbb{P}(Z < W) = 0$이므로 결론을 얻는다. $\square$

존재는 Radon–Nikodym 정리로 보장된다. $A \in \mathcal{G}$에 대해 $\nu(A) = \mathbb{E}[X\mathbf{1}_A]$로 정의한 유한 부호 측도는 $\mathcal{G}$ 위에서 $\mathbb{P}$에 절대연속이며, 그 도함수가 조건부 기댓값이다. 이 문장은 존재의 이론적 근거를 설명한다. 실제 계산에서는 분할별 평균이나 조건부 밀도가 더 직접적이다.

8.2 분할과 밀도로 계산하기

가산 분할 $B_1, B_2, \dots$가 정보를 만들고 각 $\mathbb{P}(B_j) > 0$이면

$$\mathbb{E}[X \mid \mathcal{G}] = \sum_{j} \frac{\mathbb{E}[X\mathbf{1}_{B_j}]}{\mathbb{P}(B_j)}\,\mathbf{1}_{B_j} \tag{8.2}$$

이다. 같은 정보조각 안에서는 값이 일정하다. 확률 0인 조각에는 임의의 유한값을 지정해도 거의 확실한 버전이 같다. (우변이 $\mathcal{G}$-가측이고 B_j 위에서 정의 식 (8.1)의 양변이 일치함을 직접 확인할 수 있다.)

> **예제 8.4 (주사위의 홀짝 정보)** 앞 예에서 홀수 조건의 평균은 $(1+3+5)/3 = 3$이고 짝수 조건의 평균은 4이다. 따라서 $\mathbb{E}[X \mid Y] = 3 + Y$이다. 그 평균은 3.5로 원래 주사위 평균과 같다. 조건부 분산은 두 경우 모두 $8/3$이며, 조건부 평균의 분산은 $\operatorname{Var}(3+Y) = 1/4$이다. 합은 $8/3 + 1/4 = 35/12$로 원래 분산 $\operatorname{Var} X = 35/12$와 일치한다(전체 분산의 분해, 제20권 제5장).

결합밀도가 존재하면 $f_Y(y) > 0$인 곳에서

$$f_{X\mid Y}(x \mid y) = \frac{f_{X,Y}(x,y)}{f_Y(y)}, \qquad m(y) = \int_{\mathbb{R}} x\, f_{X\mid Y}(x \mid y)\,\mathrm{d}x \tag{8.3}$$

로 계산한다. 적분가능성 아래에서 $m(Y)$는 조건부 기댓값의 버전이다. 밀도는 거의 모든 점에서만 유일하므로 특정 영확률 점에서의 값까지 이 정의가 강제하는 것은 아니다. 연속성 같은 추가 조건을 가진 자연스러운 버전을 골라 쓰는 일과 정의가 모든 점에서 유일하다고 주장하는 일은 다르다.

> **예제 8.5 (공동 정규변수의 조건부 평균)** (X, Y)가 공동 정규이고 평균이 μ_X, μ_Y, 양의 분산이 σ_X^2, σ_Y^2, 상관이 $|\rho| < 1$이라고 하자. 결합밀도의 지수를 x에 관해 완전제곱하면
>
> $$X \mid Y = y \;\sim\; N\!\left(\mu_X + \rho\,\frac{\sigma_X}{\sigma_Y}(y-\mu_Y),\; \sigma_X^2(1-\rho^2)\right)$$
>
> 인 연속 버전을 얻는다. 따라서 조건부 평균은 y의 직선이다. 이 선형성은 공동 정규모형의 특수한 구조이며 일반적인 결합분포에서는 조건부 평균이 곡선일 수 있다.

8.3 영확률 조건과 근방 선택

$\mathbb{P}(Y = y) = 0$이면 $\mathbb{P}(A \cap \{Y = y\})/\mathbb{P}(Y = y)$는 $0/0$이어서 정의가 아니다. 조건부 밀도는 이 비율을 형식적으로 계산한 결과가 아니라 전체 결합분포를 적분으로 분해하는 방식이다. “좁은 근방으로 조건화하고 극한을 취한다”는 방법도 근방을 어떻게 좁히는지 지정해야 한다.

예제 8.6 (같은 영확률 집합으로 줄어드는 다른 근방) X, Y가 독립인 $\mathrm{Unif}(-1,1)$이라고 하자. $0<\varepsilon<2/3$에서

$$A_\varepsilon=\{|Y|<\varepsilon\},\qquad B_\varepsilon=\{|Y|<\varepsilon(1+X/2)\}$$

를 생각한다. ($\varepsilon<2/3$이면 $\varepsilon(1+X/2)<1$이어서 B_ε 안의 Y 구간이 $(-1,1)$에 들어간다.) 두 사건족은 $\varepsilon\downarrow 0$일 때 모두 직선 $\{Y=0\}$으로 줄어든다. 그러나 A_ε으로 조건화하면 X는 원래의 균등분포이며 평균은 0이다. B_ε으로 조건화하면 $X=x$에서 허용되는 세로 폭이 $1+x/2$에 비례하여

$$f_{X\mid B_\varepsilon}(x)=\frac{1}{2}\left(1+\frac{x}{2}\right),\quad -1<x<1,\qquad \mathbb{E}[X\mid B_\varepsilon]=\int_{-1}^{1}\frac{x}{2}\Big(1+\frac{x}{2}\Big)\,dx=\frac{1}{6}$$

이다. 두 조건부 평균은 극한에서도 다르다. 모순이 아니라 조건화하는 양의 확률 사건들이 다르기 때문이다. 이 계산으로 특정 영확률 집합에 대한 조건부 법칙을 아무 근방으로나 유일하게 정할 수 없음을 확인한다.

역사 (Borel–Kolmogorov 역설). 영확률 사건에 대한 조건화가 근방의 선택에 의존한다는 현상은 구면 위의 위도·경도 조건화 예로 잘 알려져 있으며 Borel–Kolmogorov 역설이라고 불린다. Kolmogorov의 1933년 공리화는 영확률 사건에 대한 조건화를 "조건 변수가 주어진 σ-대수에 대한 조건부 기댓값"으로 다시 정의하여 이 문제를 정리했다.

표준적인 실수값 관측변수들에 대해서는 정규 조건부분포를 선택할 수 있다. 이때도 조건변수의 분포에 대해 거의 모든 값에서만 유일하다. 조건화의 좌표나 관측 절차가 의미를 갖는 문제에서는 그 절차까지 모형의 일부로 적는다.

8.4 기본 성질과 탑 성질

다음 성질들은 필요한 적분가능성을 전제로 한다. $\mathcal{G}$-가측이고 적분가능한 변수 Z는 이미 아는 값이므로 $\mathbb{E}[Z\mid\mathcal{G}]=Z$이다. 조건부 기댓값은 선형이며 순서를 보존한다. H가 유계이고 $\mathcal{G}$-가측이면

$$\mathbb{E}[HX\mid\mathcal{G}]=H\,\mathbb{E}[X\mid\mathcal{G}] \tag{8.4}$$

이다. 유계 조건은 편리한 충분조건이다. 적절한 곱의 적분가능성 아래에서는 더 일반화되지만, 무한대끼리 상쇄하는 형식 조작을 허용하는 것은 아니다.

정리 8.7 (탑 성질) $\mathcal{H}\subseteq\mathcal{G}\subseteq\mathcal{F}$이고 X가 적분가능하면

$$\mathbb{E}\big[\mathbb{E}[X\mid\mathcal{G}]\mid\mathcal{H}\big]=\mathbb{E}[X\mid\mathcal{H}]\quad\text{거의 확실히.} \tag{8.5}$$

증명. 왼쪽은 $\mathcal{H}$-가측이다. $A\in\mathcal{H}$이면 $A\in\mathcal{G}$이므로 정의를 두 번 적용하여

$$\mathbb{E}\Big\{\mathbb{E}\big[\mathbb{E}[X\mid\mathcal{G}]\mid\mathcal{H}\big]\mathbf{1}_A\Big\}=\mathbb{E}\big\{\mathbb{E}[X\mid\mathcal{G}]\mathbf{1}_A\big\}=\mathbb{E}[X\mathbf{1}_A]$$

를 얻는다. 유일성(명제 8.3)으로 결론이 성립한다. $\square$

정보를 더 많이 이용해 평균을 낸 뒤 더 적은 정보로 다시 평균을 내면, 처음부터 적은 정보를 쓴 것과 같다. 사건족의 포함관계 없이 임의의 두 조건을 같은 방식으로 지워서는 안 된다. 반대 순서에서는 $\mathbb{E}\big[\mathbb{E}[X\mid\mathcal{H}]\mid\mathcal{G}\big]=\mathbb{E}[X\mid\mathcal{H}]$ 인데, 안쪽 변수가 이미 $\mathcal{G}$-가측이기 때문이다.

X가 $\mathcal{G}$와 독립이면 $\mathbb{E}[X\mid\mathcal{G}]=\mathbb{E}X$이다. 여기서 독립은 모든 $A\in\mathcal{G}$와 X의 사건이 독립이라는 뜻이다. 반대로 조건부 평균이 상수라는 것만으로 X와 정보 전체가 독립이라고 결론낼 수는 없다. 조건별 분산 등 다른 분포 특성이 달라질 수 있기 때문이다.

> **예제 8.8 (평균 독립과 분포 독립)** 공정한 Bernoulli 변수 Y와 독립인 공정한 부호 S에 대해 $X=(1+Y)S$라고 하자. $\mathbb{E}[X\mid Y]=0=\mathbb{E}X$지만 $|X|=1+Y$이므로 독립이 아니다. 조건부 분산은 $Y=0$에서 1, $Y=1$에서 4이다. 평균만 보존하는 조건은 분포 전체의 독립보다 약하다.

8.5 제곱적분 공간의 투영

> **정리 8.9 (직교성과 최적 예측)** $\mathbb{E}X^2<\infty$이고 $m=\mathbb{E}[X\mid\mathcal{G}]$이면 $\mathbb{E}m^2\le\mathbb{E}X^2$이다. 모든 제곱적분가능한 $\mathcal{G}$-가측 변수 Z에 대해
>
> $$\mathbb{E}[(X-m)Z]=0, \tag{8.6}$$
>
> $$\mathbb{E}[(X-Z)^2]=\mathbb{E}[(X-m)^2]+\mathbb{E}[(m-Z)^2]. \tag{8.7}$$
>
> 따라서 m은 주어진 정보로 만드는 제곱적분가능한 예측 가운데 평균제곱오차를 최소화하며, 최소화 해는 거의 확실한 의미에서 유일하다.

증명. 조건부 Jensen 부등식으로 $m^2\le\mathbb{E}[X^2\mid\mathcal{G}]$를 얻고 평균을 취하면 첫 결론이다. 유계 Z의 직교성은 꺼내기 식 (8.4)과 알려진 인자 꺼내기에서 얻는다: $\mathbb{E}[(X-m)Z]=\mathbb{E}\big[Z\,\mathbb{E}[X-m\mid\mathcal{G}]\big]=0$이다. 일반 제곱적분가능 Z는 절단 근사 $Z_n=Z\mathbf{1}_{\{|Z|\le n\}}$와 Cauchy–Schwarz로 확장한다. Z_n은 유계이고 $\mathcal{G}$-가측이므로 $\mathbb{E}[(X-m)Z_n]=0$이며

$$\big|\mathbb{E}[(X-m)Z]\big|=\big|\mathbb{E}[(X-m)(Z-Z_n)]\big|\le\sqrt{\mathbb{E}(X-m)^2}\sqrt{\mathbb{E}(Z-Z_n)^2}\to 0$$

이다. 식 (8.7)은 $X-Z=(X-m)+(m-Z)$의 제곱을 전개하고 $m-Z$가 제곱적분가능한 $\mathcal{G}$-가측 변수이므로 교차항이 식 (8.6)로 소거된 것이다. 마지막으로 식 (8.7)에서 $\mathbb{E}[(X-Z)^2]$는 $\mathbb{E}[(m-Z)^2]=0$, 곧 $Z=m$ 거의 확실일 때에만 최솟값에 이른다. $\square$

이 결과는 조건부 평균의 기하학적 해석을 제공한다. L^2의 내적 $\langle U,V\rangle=\mathbb{E}(UV)$에서 m은 X를 정보로 표현 가능한 닫힌 부분공간에 직교 투영한 값이다. “투영”은 단순히 그림상의 비유가 아니라 위 피타고라스 등식으로 확인되는 정확한 구조이다.

> **명제 8.10 (정보가 늘 때 평균제곱오차)** $\mathbb{E}X^2<\infty$이고 $\mathcal{H}\subseteq\mathcal{G}$이면
>
> $$\mathbb{E}\big[(X-\mathbb{E}[X\mid\mathcal{G}])^2\big]\le\mathbb{E}\big[(X-\mathbb{E}[X\mid\mathcal{H}])^2\big] \tag{8.8}$$
>
> 이다.

증명. $\mathbb{E}[X\mid\mathcal{H}]$는 제곱적분가능한 $\mathcal{H}$-가측 변수이므로 $\mathcal{G}$-가측이기도 하다. 정리 8.9에 의해 $\mathbb{E}[X\mid\mathcal{G}]$는 $\mathcal{G}$-가측 예측 가운데 평균제곱오차를 최소화하므로 식 (8.8)이 성립한다. $\square$

정보가 많은 쪽에서 허용하는 예측 함수 집합이 더 크므로 최솟값은 커질 수 없다. 이 명제는 참 조건부 분포를 알고 최적으로 예측한다는 수학적 결과이다. 유한 자료로 복잡한 모형을 추정할 때 실제 예측오차가 언제나 줄어든다는 뜻은 아니다. 추정오차와 과적합은 통계학에서 별도로 다룬다(제22권 제2장).

8.6 연습문제와 해설

연습문제 8.11 $U \sim \mathrm{Unif}(-1,1)$이고 $Y = U^2$이다. $\mathbb{E}[U \mid Y]$와 $\mathbb{E}[U^2 \mid Y]$를 구하라.

풀이. 부호 대칭으로 첫 값은 0이다. 엄밀하게는 임의의 보렐 집합 B에 대해 $\mathbb{E}[U \mathbf{1}_{\{U^2 \in B\}}] = 0$이므로 조건부 기댓값 정의를 만족한다. 둘째 값은 이미 알려진 Y이므로 Y이다. 조건부 평균이 0이어도 U와 U^2가 독립인 것은 아니다.

연습문제 8.12 $\mathbb{P}(B) = 1/4$이고 $\mathcal{G} = \sigma(B)$이다. $\mathbb{E}[X\mathbf{1}_B] = 1$, $\mathbb{E}[X\mathbf{1}_{B^c}] = 3/2$일 때 조건부 평균과 전체 평균을 구하라.

풀이. B에서는 $1/(1/4) = 4$, B^c에서는 $(3/2)/(3/4) = 2$이다. 곧 $\mathbb{E}[X \mid \mathcal{G}] = 4 \cdot \mathbf{1}_B + 2 \cdot \mathbf{1}_{B^c}$이다. 전체 평균은 $4(1/4) + 2(3/4) = 5/2$이다.

연습문제 8.13 공동 정규 X, Y가 평균 0, 분산 1, 상관 $1/2$를 갖는다. $\mathbb{E}[X \mid Y]$와 그 예측의 평균제곱오차를 구하라.

풀이. 조건부 평균은 $Y/2$이며 조건부 분산은 $3/4$이다. 따라서 평균제곱오차도 $3/4$이다. 정보가 없을 때 최적 상수 예측 0의 오차 1보다 작다.

연습문제 8.14 $\mathbb{E}[X \mid \mathcal{G}] = X$가 거의 확실하면 무엇을 의미하는가? 이것만으로 X가 상수인가?

풀이. X는 $\mathcal{G}$-가측인 버전을 가지므로 주어진 정보로 거의 확실히 결정할 수 있다. X가 상수라는 뜻은 아니다. 예를 들어 $\mathcal{G} = \sigma(X)$이면 임의의 적분가능한 X에 대해 성립한다.

연습문제 8.15 X가 제곱적분가능하고 $\mathcal{H} \subseteq \mathcal{G}$일 때 두 정보 수준의 최소 평균제곱오차 차이를 구하라.

풀이. 투영의 피타고라스 등식에서

$$\mathbb{E}\big[(X - \mathbb{E}[X \mid \mathcal{H}])^2\big] - \mathbb{E}\big[(X - \mathbb{E}[X \mid \mathcal{G}])^2\big] = \mathbb{E}\big[(\mathbb{E}[X \mid \mathcal{G}] - \mathbb{E}[X \mid \mathcal{H}])^2\big]$$

이다. 추가 정보가 예측 평균을 바꾸지 않을 때에만 차이가 0이다.

다음 연결. 조건부 기댓값은 정보에 대한 정의이고 조건부 밀도는 그 정의를 계산하는 한 방식이다. 다음 장에서는 분포를 변환함수로 표현하여 분포의 식별과 독립합의 극한을 준비한다(제20권 제9장).

제 9 장

변환함수, 분포의 식별, 모멘트

개요 **변환함수**는 분포를 하나의 함수로 옮겨 놓은 것으로, 확률생성함수·적률생성함수·Laplace 변환·특성함수가 이에 속한다. 앞 묶음에서 생성함수는 모멘트를 계산하고 독립합의 분포를 알아내는 도구였다. 이 장은 언제 그 도구가 정당한지, 같은 모멘트가 같은 분포를 의미하는지, 특성함수가 분포를 결정한다는 주장을 무엇이 뒷받침하는지를 정리한다. 변환의 공식보다 정의역과 유일성 조건이 중심이며, 적률생성함수가 존재하는 조건에서 모멘트를 미분으로 얻는 명제, 특성함수의 기본 구조와 표준정규의 특성함수, Gaussian 평활화에 의한 유일성 정리와 역변환, 모멘트가 같아도 분포가 다른 반례, 누적생성함수와 지수적 기울임을 차례로 다룬다. 선행 지식: 확률생성함수와 적률생성함수의 기본 계산, 복소 지수함수, 적분의 극한 교환. Fourier 역변환은 필요한 명제를 명시하여 사용한다.

9.1 세 변환의 역할 비교

확률생성함수(*probability generating function*) $G_X(z) = \mathbb{E}z^X$는 음이 아닌 정수값 분포에 적합하다. 계수에 확률질량이 직접 들어가며 $0 \le z \le 1$에서는 항상 유한하다. **적률생성함수**(*moment generating function*) $M_X(t) = \mathbb{E}e^{tX}$는 실수축의 지수적 꼬리 정보를 담지만 $t = 0$ 이외에서는 존재하지 않을 수 있다. **특성함수**(*characteristic function*) $\varphi_X(t) = \mathbb{E}e^{itX}$는 복소수값이지만 모든 실수값 분포에서 존재한다($\left|e^{itX}\right| = 1$).

비음수 변수에는 **Laplace 변환**

$$L_X(s) = \mathbb{E}e^{-sX}, \qquad s \ge 0$$

도 편리하다. $e^{-sX} \le 1$이므로 항상 존재하고, 적률생성함수가 정의되는 곳에서는 $L_X(s) = M_X(-s)$이다. 동일한 기호 s, t라도 부호와 정의역을 확인한다. 독립합에 대해 네 변환 모두 적절한 정의역에서 곱으로 분리된다.

> **예제 9.1 (지수 꼬리와 변환의 정의역)** $X \sim \mathrm{Exp}(\lambda)$이면
>
> $$M_X(t) = \frac{\lambda}{\lambda - t} \quad (t < \lambda), \qquad L_X(s) = \frac{\lambda}{\lambda + s} \quad (s \ge 0)$$
>
> 이다. $t = \lambda$에서는 적률생성함수의 적분이 발산한다. 유리함수 $\lambda/(\lambda - t)$를 $t > \lambda$에 형식적으로 대입하면 음수가 되지만 e^{tX}의 기댓값은 음수가 될 수 없다. 적분으로 정의한 변환의 유효 범위를 버리고 식만 연장한 결과이다.

9.2 모멘트를 얻는 미분의 조건

명제 9.2 (지수적 적분가능성의 효과) 어떤 $\delta > 0$에 대해 $M_X(t) < \infty$가 $|t| < \delta$에서 성립하면 모든 양의 정수 r에 대해 $\mathbb{E}\,|X|^r < \infty$이고

$$M_X^{(r)}(t) = \mathbb{E}\big[X^r e^{tX}\big] \tag{9.1}$$

가 그 열린 구간 내부에서 성립한다. 특히 $M_X^{(r)}(0) = \mathbb{E}X^r$이다.

지배함수의 구성. 고정된 내부점 t 주위에서 $t-\eta$, $t+\eta$도 구간 안에 들도록 $\eta > 0$를 고른다. 다항식은 지수함수보다 느리게 증가하므로 어떤 유한한 상수 C에 대해 $|x|^r \le C e^{\eta|x|}$이고, 따라서

$$|x|^r\, e^{tx} \le C\big\{e^{(t-\eta)x} + e^{(t+\eta)x}\big\}$$

이다($x \ge 0$에서는 $e^{\eta|x|}e^{tx} = e^{(t+\eta)x}$, $x < 0$에서는 $e^{(t-\eta)x}$). 우변은 적분가능하다. 미분 차분에도 더 작은 근방을 택해 같은 형태의 적분가능한 지배함수를 줄 수 있다. 평균값 정리로 차분몫 $[e^{(t+h)x} - e^{tx}]/h = x e^{(t+\theta h)x}$ $(0<\theta<1)$을 같은 종류의 지배함수로 누르면 된다. 지배수렴정리로 미분과 기댓값을 교환한다. $t = 0$에서도 같은 상계가 절대 모멘트를 보장한다.

특성함수는 항상 존재하지만 미분은 별도의 문제이다. $\mathbb{E}\,|X| < \infty$이면 $\big|[e^{ihX}-1]/h\big| \le |X|$를 이용하여 $\varphi_X'(0) = i\,\mathbb{E}X$를 얻는다. r차 절대 모멘트가 유한하면 반복해서 $\varphi_X^{(r)}(0) = i^r\,\mathbb{E}X^r$이다. 반대 방향의 미분가능성과 모멘트 존재 사이에는 세부 조건이 있어, 필요한 방향만 명확히 사용하는 것이 좋다.

예제 9.3 (모든 모멘트가 있어도 적률생성함수는 없을 수 있다) $Z \sim N(0,1)$, $X = e^{Z}$이면 $\mathbb{E}X^r = e^{r^2/2}$가 모든 실수 r에 대해 유한하다. 그러나 $t > 0$이면

$$M_X(t) = \frac{1}{\sqrt{2\pi}} \int_{\mathbb{R}} \exp\!\big(te^{z} - z^2/2\big)\,\mathrm{d}z = \infty$$

이다. $z \to \infty$에서 te^{z}가 $z^2/2$보다 빠르게 증가하므로 적분함수는 충분히 큰 z에서 1 이상이다. 따라서 적분은 발산한다. ($t \le 0$이면 $X > 0$이므로 $e^{tX} \le 1$이어서 $M_X(t)$는 유한하지만, 0의 양쪽 열린 근방에서는 존재하지 않는다.) 개별 모멘트의 존재와 영점 주변에서 변환이 수렴하는 것은 다른 요구이다.

9.3 특성함수의 기본 구조

실수 상수 a, b에 대해

$$\varphi_{aX+b}(t) = e^{itb}\varphi_X(at) \tag{9.2}$$

이다. 독립인 변수들의 합은 특성함수의 곱에 대응한다. 독립성이 없으면 **결합 특성함수**

$$\varphi_{X,Y}(s,t) = \mathbb{E}e^{i(sX+tY)}$$

를 사용해야 하며 합의 특성함수는 $\varphi_{X,Y}(t,t)$이다. 주변 특성함수 둘의 곱으로 바꾸는 것은 추가 가정이다.

모든 특성함수는 **양의 정부호** 조건을 만족한다. 임의의 복소수 $c_1, \dots, c_m$과 실수 $t_1, \dots, t_m$에 대해

$$\sum_{j,k=1}^{m} c_j \overline{c_k}\, \varphi_X(t_j - t_k) = \mathbb{E}\left| \sum_{j=1}^{m} c_j e^{i t_j X} \right|^2 \geq 0$$

이다. 따라서 $\varphi(0) = 1$, 연속성, 절댓값 상계 1을 갖는 임의의 함수가 자동으로 특성함수가 되는 것은 아니다. 양의 정부호성과 연속성을 이용한 역방향 특성화는 Bochner 정리로 이어지며, 여기서는 필요조건만 사용한다.

명제 9.4 (표준정규의 특성함수) $Z \sim N(0,1)$이면 $\varphi_Z(t) = e^{-t^2/2}$이다.

증명. $\mathbb{E}|Z| < \infty$이므로 미분할 수 있다. 표준정규 밀도 ϕ는 $\phi'(x) = -x\phi(x)$를 만족하므로 부분적분으로

$$\varphi_Z'(t) = i\int_{\mathbb{R}} x e^{itx}\phi(x)\,dx = -i\int_{\mathbb{R}} e^{itx}\phi'(x)\,dx = i\cdot it\int_{\mathbb{R}} e^{itx}\phi(x)\,dx = -t\,\varphi_Z(t)$$

이다. 경계항 $[e^{itx}\phi(x)]_{-\infty}^{\infty}$은 Gaussian 꼬리 때문에 0이다. 초기값 $\varphi_Z(0) = 1$인 이 미분방정식 $\varphi' = -t\varphi$의 해가 $e^{-t^2/2}$이다. $\square$

이 증명은 실수 적률생성함수에 복소수를 형식적으로 대입하지 않고 직접 계산한다. 복소 적분의 해석적 연장이 정당한 경우도 있지만, 초급 계산에서는 직접적인 지배와 부분적분이 조건을 더 잘 드러낸다. $X \sim N(\mu, \sigma^2)$이면 식 (9.2)에 의해 $\varphi_X(t) = e^{i\mu t - \sigma^2 t^2/2}$이다.

9.4 특성함수가 분포를 결정하는 이유

정리 9.5 (특성함수의 유일성) 실수값 확률변수 X, Y가 모든 $t \in \mathbb{R}$에 대해 같은 특성함수를 가지면 같은 분포를 갖는다.

Gaussian 평활화를 통한 증명 개요. 독립인 표준정규 잡음 Z를 더한 $X + \varepsilon Z$의 밀도는

$$f_{X,\varepsilon}(x) = \mathbb{E}\left[\frac{1}{\varepsilon\sqrt{2\pi}}\, e^{-(x-X)^2/(2\varepsilon^2)}\right]$$

이다. Gaussian 함수의 Fourier 표현 $\frac{1}{\varepsilon\sqrt{2\pi}} e^{-u^2/(2\varepsilon^2)} = \frac{1}{2\pi}\int e^{-itu} e^{-\varepsilon^2 t^2/2}\,dt$와 Fubini 정리를 사용하면

$$f_{X,\varepsilon}(x) = \frac{1}{2\pi}\int_{\mathbb{R}} e^{-itx}\varphi_X(t)\, e^{-\varepsilon^2 t^2/2}\,dt \tag{9.3}$$

이다. $|\varphi_X(t)| \leq 1$이고 Gaussian 인자가 적분가능하므로 순서 교환이 정당하다. 따라서 특성함수가 같으면 모든 $\varepsilon > 0$에서 평활화된 밀도가 같다. $\varepsilon Z \to 0$이 거의 확실히 성립하므로(분포만 중요하므로 Z를 X와도 Y와도 독립으로 잡는다) 임의의 유계 연속함수 g에 대해 지배수렴으로

$$\mathbb{E}g(X) = \lim_{\varepsilon\downarrow 0} \mathbb{E}g(X+\varepsilon Z) = \lim_{\varepsilon\downarrow 0} \mathbb{E}g(Y+\varepsilon Z) = \mathbb{E}g(Y)$$

이다. 유계 연속함수 적분의 일치는 분포를 결정한다. 예를 들어 반직선의 지시함수를 연속함수로 위아래에서 근사하면 공통 연속점에서 분포함수의 일치를 얻고, 우연속성으로 모든 점으로 확장한다. $\square$

이 논증은 원래 분포에 밀도가 없어도 작동한다. 정규 잡음을 더하면 매끄러운 밀도가 생기고, 변환에서 그 잡음은 적분가능한 인자를 곱하는 역할을 한다. 일반적인 Fourier 역변환 정리는 더 넓지만 유일성의 핵심은 이렇게 볼 수 있다.

명제 9.6 (적분가능한 특성함수의 역변환) $\int_{\mathbb{R}} |\varphi_X(t)|\,\mathrm{d}t < \infty$이면 X는 연속인 밀도를 가지며

$$f_X(x) = \frac{1}{2\pi}\int_{\mathbb{R}} e^{-itx}\varphi_X(t)\,\mathrm{d}t \tag{9.4}$$

이다.

이 조건은 충분조건이다. 밀도가 있다고 해서 특성함수가 반드시 절대적분가능한 것은 아니다. 예를 들어 $\mathrm{Unif}(0,1)$의 특성함수 $(e^{it}-1)/(it)$는 sinc 형태이고 절댓값의 적분이 발산한다. 그런 경우에는 다른 형태의 역변환 정리나 극한 해석을 사용해야 한다. (증명의 요지는 식 (9.3)에서 $\varepsilon \downarrow 0$으로 보내고 지배수렴을 쓰는 것이다.)

9.5 모멘트의 일치와 분포의 일치

유한 지원집합의 경우 모멘트들은 유한한 선형방정식을 통해 확률질량을 결정할 수 있다(Vandermonde 행렬의 가역성). 영점 근방에서 유한한 적률생성함수를 갖는 분포도 그 근방의 변환, 따라서 모멘트 전개를 통해 유일하게 결정된다. 그러나 모든 모멘트가 유한하다는 사실만으로 모멘트열이 분포를 항상 결정하는 것은 아니다.

예제 9.7 (같은 모든 정수차 모멘트를 갖는 서로 다른 밀도) 표준 로그정규 밀도를

$$f(x) = \frac{1}{x\sqrt{2\pi}}\,e^{-(\log x)^2/2}, \qquad x>0$$

라 하자. $|a|\le 1$에 대해

$$f_a(x) = f(x)\bigl[1 + a\sin(2\pi\log x)\bigr]$$

는 비음수이다. $Z\sim N(0,1)$로 바꾸어 $(x=e^z)$ 음이 아닌 정수 k에 대해

$$\int_0^\infty x^k f(x)\sin(2\pi\log x)\,\mathrm{d}x = \mathbb{E}\bigl[e^{kZ}\sin(2\pi Z)\bigr] = e^{k^2/2-2\pi^2}\sin(2\pi k) = 0$$

이다. 마지막 등식은 $e^{kz}\phi(z) = e^{k^2/2}\phi(z-k)$와 표준정규의 특성함수 $\mathbb{E}e^{2\pi i W} = e^{-2\pi^2}$에서 얻는다. $k=0$이 정규화를 보장하고, 모든 정수 $k\ge 0$의 모멘트는 원래 로그정규와 같다. a가 다르면 밀도가 양의 측도인 집합에서 달라지므로 실제 분포는 다르다.

이 예는 "모든 모멘트가 같으면 분포가 같다"는 명제가 조건 없이 거짓임을 보여 준다. 특성함수의 유일성과 모순되지 않는다. 여기서는 같은 모멘트열을 갖지만 특성함수 전체가 같은 것은 아니다.

역사 (로그정규 반례). 로그정규분포가 모멘트로 결정되지 않는다는 사실은 Stieltjes가 연분수와 모멘트 문제를 연구하던 1890년대에 제시한 예로 알려져 있다. 모멘트 문제의 분류에서 이런 분포를 "모멘트 비결정"이라 부르며, 지수적 꼬리를 갖는 경우(영점 근방에서 적률생성함수가 유한한 경우)는 이 병리에서 벗어난다.

9.6 누적생성함수와 지수적 기울임

$M_X(t)$가 유한한 열린 구간에서

$$K_X(t) = \log M_X(t)$$

를 **누적생성함수**(*cumulant generating function*)라 한다. 영점 근방에서

$$K_X'(0) = \mathbb{E}X, \qquad K_X''(0) = \operatorname{Var}(X)$$

이다. 독립합의 적률생성함수는 곱이므로 누적생성함수는 합이 된다. 이 성질은 중심극한정리에서 제곱항만 남는 구조와 큰편차에서 지수율을 최적화하는 구조를 연결한다(제20권 제11장, 제20권 제12장).

정의 9.8 (지수적 기울임) $M_X(t) < \infty$인 t에 대해 원래 확률측도에 가중치

$$\frac{e^{tX}}{M_X(t)}$$

를 곱한 새 확률측도를 정의할 수 있다. 이 가중치는 비음수이고 평균이 1이다. 새 측도 아래의 기댓값을 $\mathbb{E}_t$로 쓴다. 이 변형을 **지수적 기울임**(*exponential tilting*)이라 한다.

미분이 정당한 구간 내부에서는

$$K_X'(t) = \mathbb{E}_t X, \qquad K_X''(t) = \operatorname{Var}_t(X) \geq 0 \tag{9.5}$$

이다. 실제로 $K_X'(t) = M_X'(t)/M_X(t) = \mathbb{E}[Xe^{tX}]/M_X(t) = \mathbb{E}_t X$이고, $K_X'' = M_X''/M_X - (M_X'/M_X)^2 = \mathbb{E}_t X^2 - (\mathbb{E}_t X)^2$이다. 따라서 K_X는 볼록하다. 변환의 로그가 단순히 계산을 줄이는 기호가 아니라 새 가중분포의 평균과 분산을 담는다는 뜻이다.

예제 9.9 (Bernoulli 분포의 기울임) $X \sim \mathrm{Bern}(p)$, $0 < p < 1$이면 기울인 분포의 성공확률은

$$p_t = \frac{pe^t}{1 - p + pe^t}$$

이다. $t > 0$은 성공에 더 큰 가중치를 주어 $p_t > p$로 만든다. 로그 오즈는 $\log[p_t/(1-p_t)] = \log[p/(1-p)] + t$이다. 이 표현은 마지막 장의 이항 꼬리확률 최적화와 지수족 모형에 연결된다(제20권 제12장).

9.7 연습문제와 해설

연습문제 9.10 $X \sim \mathrm{Pois}(\lambda)$의 누적생성함수와 첫 두 도함수를 구하라.

풀이. $K_X(t) = \lambda(e^t - 1)$이고 $K_X'(t) = K_X''(t) = \lambda e^t$이다. $t = 0$에서 평균과 분산이 모두 λ임을 얻는다. 기울인 분포는 평균 λe^t의 Poisson 분포이다.

연습문제 9.11 X, Y가 독립이며 특성함수가 각각 $e^{-t^2/2}$, e^{-2t^2}이다. $2X - Y$의 분포를 구하라.

풀이. 두 분포는 각각 $N(0,1)$과 $N(0,4)$이다. 변환법으로 합성 특성함수는 $\varphi_{2X}(t)\varphi_{-Y}(t) = e^{-2t^2}e^{-2t^2} = e^{-4t^2}$이며 $N(0,8)$을 나타낸다.

연습문제 9.12 X가 ± 1을 같은 확률로 가지면 특성함수는 무엇인가? 음수가 되는 구간이 있어도 괜찮은가?

풀이. $\varphi_X(t) = (e^{it} + e^{-it})/2 = \cos t$이다. 특성함수는 밀도나 확률이 아니므로 음수일 수 있다. 절댓값 상계와 양의 정부호 조건을 만족한다.

연습문제 9.13 X의 적률생성함수 식이 $M_X(t) = (1-2t)^{-3}$, $t < 1/2$로 주어졌다. 분포와 평균, 분산을 식별하라.

풀이. *shape* 3, *rate* $1/2$, 곧 *scale* 2인 감마분포이다. 평균은 $3/(1/2) = 6$, 분산은 $3/(1/2)^2 = 12$이다. *rate*와 *scale*을 뒤바꾸면 틀린 모멘트를 얻게 된다. (유일성 때문에 정의역 $t < 1/2$ 안의 열린 구간에서 이 식이 주어지면 분포가 결정된다.)

연습문제 9.14 서로 다른 분포가 모든 음이 아닌 정수차 모멘트를 공유하는 앞의 로그정규 예에서, 왜 $a = 1$도 유효한 밀도를 만드는가?

풀이. $1 + \sin(2\pi \log x) \geq 0$이며 $k = 0$ 계산으로 적분이 1이다. 일부 점에서 밀도가 0이 되는 것은 문제가 아니다. 두 함수가 확률밀도가 되려면 모든 점에서 엄격히 양수일 필요가 없다.

다음 연결. 분포의 변환을 다루려면 적분의 존재와 극한 교환을 구별해야 한다. 다음 장에서는 확률변수열이 가까워진다는 여러 의미를 비교하여 극한정리에 필요한 언어를 정리한다(제20권 제10장).

제 10 장

확률변수열의 수렴과 반례

개요 확률변수열의 수렴은 수열 $x_n \to x$의 극한 개념을 확률변수에 옮긴 것이며, 결과마다 값이 다르고 분포도 가진다는 점 때문에 하나가 아니라 네 가지로 갈라진다. 이 장은 거의 확실한 수렴, 확률수렴, L^p 수렴, 분포수렴을 정의하고, 이들 사이의 함의를 증명한 다음, 각 역방향이 실패하는 반례를 하나씩 구성한다. 이어서 Borel–Cantelli 보조정리와 거의 확실하게 수렴하는 부분수열, 지배수렴과 균등적분가능성에 의한 극한과 기댓값의 교환, 연속사상 정리와 Slutsky 정리를 다룬다. 이 구분은 큰수법칙, 중심극한정리, 통계 추정의 일관성을 정확히 읽기 위한 기본 문법이다. 선행 지식: 수열과 함수의 극한, 확률의 연속성, Markov 부등식. 이 장에서 거의 확실한 수렴과 확률수렴은 같은 확률공간 위의 변수들에 대해 말한다.

수열 x_n이 x에 가까워진다는 말은 하나지만, 확률변수는 결과마다 값이 다르고 분포도 가진다. 따라서 각 결과에서 가까워지는지, 큰 오차가 날 확률이 작아지는지, 평균적인 오차가 줄어드는지, 분포의 모양만 가까워지는지를 구별해야 한다.

10.1 네 가지 수렴의 정의

정의 10.1 (확률변수열의 수렴) 같은 확률공간의 확률변수 X_n, X에 대해 다음을 정의한다.

(1) **거의 확실한 수렴**(*almost sure convergence*): $\mathbb{P}(\{\omega : X_n(\omega) \to X(\omega)\}) = 1$. $X_n \to X$ a.s.로 쓴다.

(2) **확률수렴**(*convergence in probability*): 모든 $\varepsilon > 0$에서 $\mathbb{P}(|X_n - X| > \varepsilon) \to 0$. $X_n \xrightarrow{\mathbb{P}} X$로 쓴다.

(3) **L^p 수렴**($p \geq 1$): X_n, X가 모두 L^p에 속하고, 즉 각각의 p차 절대모멘트가 유한하며, $\mathbb{E}\,|X_n - X|^p \to 0$. $X_n \xrightarrow{L^p} X$로 쓴다.

한편 **분포수렴**(*convergence in distribution*) $X_n \xrightarrow{d} X$는 F_X의 모든 연속점 x에서 $F_{X_n}(x) \to F_X(x)$라는 뜻이다. 이 정의에는 같은 확률공간이 필요하지 않다.

L^1은 평균 절대오차, L^2는 평균제곱오차를 통제한다. 확률수렴은 큰 오차가 드물게 일어난다고만 말하므로 드물게 매우 큰 값이 나오는 상황의 평균 오차까지 통제하지는 않는다. 분포수렴은 표본별 차이 $X_n - X$를 직접 비교하지 않는다는 점에서 다른 수렴들과 구별된다.

예제 10.2 (분포함수의 불연속점) 상수 $X_n = 1/n$, $X = 0$이면 거의 확실히 수렴한다. 그러나 $F_{X_n}(0) = 0$, $F_X(0) = 1$이다. 분포수렴이 실패한 것이 아니다. 0은 극한 분포의 불연속점이므로 정의가 그 점의 수렴을 요구하지 않는다. 다른 모든 점에서는 요구한 수렴이 성립한다.

10.2 수렴 사이의 함의

정리 10.3 (수렴 사이의 함의) 다음 함의가 성립한다.

$$\text{거의 확실한 수렴} \implies \text{확률수렴} \implies \text{분포수렴},$$

$$L^p \text{ 수렴} \implies \text{확률수렴}.$$

$1 \le q < p$이고 확률측도 위에서 L^p 수렴하면 L^q 수렴도 한다.

증명. 거의 확실히 $X_n \to X$이면 고정된 $\varepsilon > 0$에서 $\mathbf{1}_{\{|X_n - X| > \varepsilon\}} \to 0$이 거의 확실히 성립한다. 수렴 집합의 각 점에서 n이 크면 $|X_n - X| \le \varepsilon$이기 때문이다. 상계가 1이므로 지배수렴으로 기대값, 곧 오차 확률이 0으로 간다. L^p에서 확률수렴으로는

$$\mathbb{P}(|X_n - X| > \varepsilon) \le \frac{\mathbb{E}\,|X_n - X|^p}{\varepsilon^p}$$

를 사용한다(Markov 부등식). 또한 Jensen 또는 Hölder 부등식으로 $\mathbb{E}\,|X_n - X|^q \le (\mathbb{E}\,|X_n - X|^p)^{q/p}$이다.

확률수렴에서 분포수렴으로 가려면 $\eta > 0$에 대해

$$F_X(x - \eta) - \mathbb{P}(|X_n - X| > \eta) \le F_{X_n}(x) \le F_X(x + \eta) + \mathbb{P}(|X_n - X| > \eta)$$

를 사용한다. $\{X \le x - \eta\} \subset \{X_n \le x\} \cup \{|X_n - X| > \eta\}$이고 $\{X_n \le x\} \subset \{X \le x + \eta\} \cup \{|X_n - X| > \eta\}$이기 때문이다. 먼저 $n \to \infty$, 다음에 $\eta \downarrow 0$으로 보내면 F_X의 연속점에서 두 경계가 $F_X(x)$로 모인다. □

일반적으로 위 화살표들을 거꾸로 뒤집을 수 없다. 각각의 역이 실패하는 이유를 별도 예제로 확인해야 한다. 반례에서 모든 변수를 같은 공간에 구성하는지, 극한이 상수인지, 평균이 존재하는지를 명시한다.

10.3 역방향이 실패하는 세 반례

예제 10.4 (분포수렴만으로 확률수렴하지 않는다) Z가 ± 1을 같은 확률로 가지고 $X_n = -Z$, $X = Z$라고 하자. 모든 X_n의 분포는 X와 같으므로 분포수렴은 자명하다. 그러나 $|X_n - X| = 2$가 항상 성립하므로 X로 확률수렴하지 않는다. 같은 분포와 같은 결과별 값은 서로 다른 개념이다.

예제 10.5 (확률수렴하지만 평균 오차는 사라지지 않는다) $U \sim \mathrm{Unif}(0,1)$이고 $X_n = n\mathbf{1}_{\{U < 1/n\}}$라고 하자. 모든 $U > 0$에 대해 충분히 큰 n에서는 $X_n = 0$이므로 거의 확실히 0으로 수렴한다. 그러나

$$\mathbb{E}\,|X_n| = n \cdot \frac{1}{n} = 1$$

이어서 L^1으로 수렴하지 않는다. 더 드문 큰 값이 평균을 계속 기억한다. 따라서 거의 확실한 수렴만으로 기댓값과 극한을 교환할 수 없다.

예제 10.6 (확률수렴하지만 거의 확실히 수렴하지 않는 타자기 수열) $U \sim \mathrm{Unif}[0,1)$이다.

$n = 2^k + j$, $0 \le j < 2^k$ 로 유일하게 쓰고

$$X_n = \mathbf{1}_{\{j2^{-k} \le U < (j+1)2^{-k}\}}$$

로 정의한다. k 번째 묶음에는 길이가 2^{-k} 인 구간들을 차례로 훑는 변수 2^k 개가 있다. 각 변수의 1일 확률은 2^{-k} 이므로 $X_n \xrightarrow{\mathbb{P}} 0$ 이다. 그러나 각 $U \in [0,1)$ 는 매 묶음에서 정확히 한 번 선택된다. 따라서 $X_n(U) = 1$ 이 무한히 자주 나오고, 0도 무한히 자주 나온다. 어느 표본점에서도 수열이 수렴하지 않는다.

마지막 예는 “각 시점의 오류 확률이 작다”와 “한 경로에서 오류가 결국 없어졌다”가 다름을 보여 준다. 이 차이를 분석하는 표준 도구가 다음의 Borel–Cantelli 보조정리이다.

표 10.1 수렴 사이의 함의와 역방향의 반례

방향	역이 실패하는 이유	반례
$L^p \Rightarrow \mathbb{P}$	드문 큰 값이 평균을 유지한다	예제 10.5
a.s. $\Rightarrow \mathbb{P}$	오류 위치가 계속 이동한다	예제 10.6
$\mathbb{P} \Rightarrow d$	분포는 표본별 값을 비교하지 않는다	예제 10.4
a.s. $\Rightarrow L^p$	지배하는 적분가능 변수가 없다	예제 10.5

10.4 Borel–Cantelli 보조정리

사건열 A_n 에 대해

$$\limsup_{n} A_n = \bigcap_{m=1}^{\infty} \bigcup_{n \ge m} A_n$$

는 A_n 이 무한히 자주 일어나는 사건이다. 약자로 A_n i.o.(*infinitely often*)라고도 쓴다. 모든 m 이후에 적어도 한 번 일어난다는 뜻을 집합식이 그대로 표현한다.

정리 10.7 (Borel–Cantelli)

(1) $\sum_n \mathbb{P}(A_n) < \infty$ 이면 $\mathbb{P}(A_n \text{ i.o.}) = 0$ 이다. 독립성은 필요 없다.

(2) A_n 들이 서로 독립이고 $\sum_n \mathbb{P}(A_n) = \infty$ 이면 $\mathbb{P}(A_n \text{ i.o.}) = 1$ 이다.

증명. 첫 결론은 $\mathbb{P}\big(\bigcup_{n \ge m} A_n\big) \le \sum_{n \ge m} \mathbb{P}(A_n) \to 0$ 과 사건의 위로부터 연속성으로 얻는다. 둘째에서 고정된 $m \le N$ 에 대해 독립성과 $1 - x \le e^{-x}$ 를 사용하면

$$\mathbb{P}\Big(\bigcap_{n=m}^{N} A_n^{c}\Big) = \prod_{n=m}^{N} \big[1 - \mathbb{P}(A_n)\big] \le \exp\Big(-\sum_{n=m}^{N} \mathbb{P}(A_n)\Big) \to 0.$$

따라서 어떤 고정된 m 이후로 한 번도 안 일어날 확률은 0이다. 이 사건들을 m 에 대해 가산 합집합하면 유한 번만 일어날 확률도 0이다. $\square$

두 번째 결론에서 독립성은 무조건 삭제할 수 없다. 모든 $A_n = A$ 이고 $0 < \mathbb{P}(A) < 1$ 이면 확률합은 발산하지만 무한히 자주 일어날 확률은 $\mathbb{P}(A)$ 이다. 첫 결론에는 독립성을 추가할 필요가 없다는 점도 기억한다.

예제 10.8 (오류 확률의 합으로 경로를 통제하기) 모든 양의 정수 r에 대해 $\sum_{n} \mathbb{P}(|X_n - X| > 1/r) < \infty$이면 $X_n \to X$가 거의 확실히 성립한다. 각각의 r에서 문턱을 넘는 일이 유한 번만 일어나고, 이 확률 1 사건들을 가산 교집합하면 된다. 단순히 각 확률이 0으로 간다는 조건보다 강하다.

10.5 부분수열과 상수 극한

명제 10.9 (확률수렴에서 거의 확실히 수렴하는 부분수열) $X_n \xrightarrow{\mathbb{P}} X$이면 어떤 증가하는 부분수열 n_k에 대해 $X_{n_k} \to X$가 거의 확실히 성립한다.

증명. 확률수렴 정의로 $\mathbb{P}(|X_{n_k} - X| > 2^{-k}) < 2^{-k}$가 되도록 순서대로 n_k를 고른다. 확률합이 유한하므로 Borel–Cantelli 첫 결론에 의해 이 부등식 위반이 유한 번만 일어난다. 나머지에서는 오차가 2^{-k} 이하이므로 거의 확실히 수렴한다. □

이 결과는 원래 전체 수열이 거의 확실히 수렴한다는 뜻이 아니다. 타자기 수열에서 각 묶음의 첫 구간만 고르는 부분수열은 거의 확실히 0으로 수렴하지만 전체 수열은 그렇지 않다.

명제 10.10 (상수로의 분포수렴) 상수 c에 대해서는 $X_n \xrightarrow{d} c$와 $X_n \xrightarrow{\mathbb{P}} c$가 동치이다.

증명. 역방향은 일반적인 함의이다. 정방향에서 $c - \varepsilon, c + \varepsilon$는 상수분포의 연속점이다. 따라서 $\mathbb{P}(X_n \le c - \varepsilon) \to 0$, $\mathbb{P}(X_n > c + \varepsilon) \to 0$이다. 두 꼬리를 합치면 $\mathbb{P}(|X_n - c| > \varepsilon) \to 0$을 얻는다. □

상수 극한은 통계학에서 분산 추정량이나 정규화 인자가 일정한 값으로 가까워질 때 자주 등장한다. 분포수렴 일반의 약함과 이 특별한 동치를 혼동하지 않는다.

10.6 극한과 기댓값의 교환

정리 10.11 (지배수렴의 확률적 형태) $X_n \to X$가 거의 확실히 성립하고, 모든 n에 대해 $|X_n| \le Y$인 적분가능 변수 Y가 존재하면 X도 적분가능하며

$$\mathbb{E}\,|X_n - X| \to 0, \qquad \mathbb{E}X_n \to \mathbb{E}X.$$

증명. $|X| \le Y$가 거의 확실히 성립하므로 $|X_n - X| \le 2Y$에 지배수렴을 적용하면 된다. $|\mathbb{E}X_n - \mathbb{E}X| \le \mathbb{E}\,|X_n - X|$이므로 둘째 결론도 따른다. □

지배하는 변수는 n에 따라 커지는 상수가 아니라 모든 n에 공통으로 적용되는 적분가능한 대상이어야 한다.

정의 10.12 (균등적분가능성) 적분가능한 변수족 $\{X_n\}$이

$$\lim_{K \to \infty} \sup_{n} \mathbb{E}\big[|X_n| \, \mathbf{1}_{\{|X_n| > K\}}\big] = 0$$

을 만족하면 **균등적분가능**(*uniformly integrable*)하다고 한다.

이 조건은 큰 값 영역이 평균에 기여하는 양을 모든 n에 대해 동시에 작게 만들 수 있다는 뜻이다. 단순히 $\sup_n \mathbb{E}\,|X_n| < \infty$보다 강하다. 앞의 $n\mathbf{1}_{\{U<1/n\}}$는 평균이 항상 1이지만 균등적분가능하지 않다. 실제로 $K < n$이면 $\mathbb{E}[X_n \mathbf{1}_{\{X_n>K\}}] = 1$이므로 상한이 K와 무관하게 1이다.

정리 10.13 (확률수렴과 균등적분가능성) $X_n \xrightarrow{\mathbb{P}} X$이고 $\{X_n\}$이 균등적분가능하면 X는 적분가능하고 $X_n \xrightarrow{L^1} X$이다. 반대로 L^1 수렴하는 수열은 균등적분가능하다.

정방향은 큰 값 영역과 절단된 유계 영역을 나누어 증명한다. 큰 값 영역은 균등적분가능성으로 통제하고, 유계 영역에서는 확률수렴과 오차 문턱 분할로 기댓값을 얻는다. X의 적분가능성과 꼬리 제어는 거의 확실히 수렴하는 부분수열에 Fatou 보조정리를 적용하여 확보한다. 이 정리는 조건과 결론의 완전한 관계를 나타내지만 세부 절단 증명은 적분론의 심화 내용으로 남긴다.

역방향은 짧게 확인할 수 있다. $X_n \xrightarrow{L^1} X$이고 $M = \sup_n \mathbb{E}\,|X_n| < \infty$라 하자(수렴하는 수열은 L^1 노름이 유계이다). $\varepsilon > 0$이 주어지면 어떤 N 이후 $\mathbb{E}\,|X_n - X| < \varepsilon/2$이고, $\mathbb{P}(A) < \delta$이면 $\mathbb{E}[|X|\,\mathbf{1}_A] < \varepsilon/2$가 되는 $\delta > 0$이 있다(X의 적분가능성). Markov 부등식으로 $\mathbb{P}(|X_n| > K) \le M/K < \delta$가 되도록 K를 잡으면 $n > N$에서

$$\mathbb{E}\big[|X_n|\,\mathbf{1}_{\{|X_n|>K\}}\big] \le \mathbb{E}\,|X_n - X| + \mathbb{E}\big[|X|\,\mathbf{1}_{\{|X_n|>K\}}\big] < \varepsilon$$

이다. 남은 유한 개의 $n \le N$은 각각 적분가능하므로 K를 더 키워 처리한다.

명제 10.14 (편리한 충분조건) 어떤 $p > 1$에 대해 $\sup_n \mathbb{E}\,|X_n|^p < \infty$이면 $\{X_n\}$은 균등적분가능하다.

증명. $|X_n| > K$에서 $|X_n| \le |X_n|^p / K^{p-1}$이므로

$$\sup_n \mathbb{E}\big[|X_n|\,\mathbf{1}_{\{|X_n|>K\}}\big] \le \frac{\sup_n \mathbb{E}\,|X_n|^p}{K^{p-1}} \to 0. \qquad \square$$

10.7 연속사상 정리와 Slutsky 정리

정리 10.15 (연속사상 정리) $X_n \xrightarrow{d} X$이고 Borel 가측함수 g의 불연속점 집합에 X가 들어갈 확률이 0이면 $g(X_n) \xrightarrow{d} g(X)$이다. 확률수렴과 거의 확실한 수렴에도 같은 연속성 조건 아래 대응하는 결론이 성립한다.

정규 극한 변수에 제곱을 취하여 카이제곱 극한을 얻는 계산은 연속사상 정리의 예이다. 역수 함수는 0에서 연속이 아니므로 분모가 0에 닿을 가능성을 확인해야 한다. 모든 점에서 연속일 필요는 없고 극한 변수가 불연속점을 피하면 충분하다.

정리 10.16 (Slutsky 정리) $X_n \xrightarrow{d} X$이고 $Y_n \xrightarrow{\mathbb{P}} c$($c$는 상수)이면

$$X_n + Y_n \xrightarrow{d} X + c, \qquad X_n Y_n \xrightarrow{d} cX.$$

$c \neq 0$이면 $X_n / Y_n \xrightarrow{d} X/c$이다. 분모가 0인 예외 표본에는 임의의 값을 정해도 그 확률이 0으로 가면 극한에 영향을 주지 않는다.

정리의 핵심은 $(X_n, Y_n) \xrightarrow{d} (X, c)$라는 결합수렴이다. 상수로 집중하는 성분은 다른 성분과의 의존성을 따로 가정하지 않아도 결합 극한을 고정한다. 이어서 연속사상을 적용한다.

흔한 오류 (주변분포의 수렴과 합의 극한). 두 성분이 각각 비퇴화 분포로 수렴한다는 조건만으로 합의 극한을 정할 수는 없다. $Z \sim N(0,1)$, $X_n = Z$, $Y_n = (-1)^n Z$라 하면 두 주변분포는 항상 표준정규이다. 그러나 합은 짝수 n에서 $2Z$, 홀수 n에서 0이므로 분포가 번갈아 바뀐다.

10.8 연습문제와 해설

연습문제 10.17 $U \sim \mathrm{Unif}(0,1)$이고 $X_n = n^2 \mathbf{1}_{\{U < 1/n\}}$이다. 거의 확실한 극한과 평균을 구하라.

풀이. 모든 $U > 0$에서 결국 지시변수가 0이므로 거의 확실한 극한은 0이다. 평균은 $\mathbb{E}X_n = n^2 \cdot (1/n) = n$으로 발산한다. 확률수렴은 기대값의 유계성조차 보장하지 않는다.

연습문제 10.18 $\mathbb{P}(|X_n - X| > \varepsilon) \le C_\varepsilon / n^2$가 모든 n과 모든 $\varepsilon > 0$에서 성립한다. 거의 확실한 수렴을 증명하라.

풀이. $\varepsilon = 1/r$인 가산 문턱들에 대해 확률합이 유한하다. Borel–Cantelli 첫 결론과 가산 교집합으로 각 문턱 초과가 유한 번만 일어나므로 거의 확실히 수렴한다. C_ε가 문턱에 따라 달라도 무방하다.

연습문제 10.19 $X_n \xrightarrow{\mathbb{P}} X$, $\sup_n \mathbb{E}X_n^2 < \infty$이다. $\mathbb{E}X_n \to \mathbb{E}X$를 결론낼 수 있는가?

풀이. 가능하다. $p = 2$의 균등 모멘트 상계로 균등적분가능성을 얻고(명제 10.14), 확률수렴과 결합하여 L^1 수렴을 적용한다(정리 10.13). 같은 조건만으로 L^2 수렴까지 결론낼 수는 없다.

연습문제 10.20 직전 문제의 조건으로 L^2 수렴이 보장되지 않는 예를 구하라.

풀이. $X_n = \sqrt{n}\,\mathbf{1}_{\{U<1/n\}}$이면 거의 확실히 0으로 수렴하고 $\mathbb{E}X_n^2 = 1$이다. 평균 절대값은 $1/\sqrt{n}$으로 줄어들지만 평균제곱은 줄어들지 않는다.

연습문제 10.21 $X_n \xrightarrow{d} Z \sim N(0,1)$, $Y_n \xrightarrow{\mathbb{P}} 2$일 때 X_n^2 / Y_n의 극한 분포를 구하라.

풀이. 연속사상과 Slutsky 정리로 $Z^2/2$에 분포수렴한다. $Z^2 \sim \chi^2_1$이므로 극한은 χ^2_1의 절반이다. X_n, Y_n의 독립성은 요구되지 않는다.

수렴의 종류와 조건을 명시하면 큰수법칙의 평균 안정화와 중심극한정리의 오차 분포를 서로 혼동하지 않을 수 있다. 다음 장(제20권 제11장)은 두 역할을 분리하여 정리한다.

제 11 장

큰수법칙, 중심극한정리, 델타 방법

개요 큰수법칙은 표본평균의 오차가 0으로 가까워진다는 정리이고, 중심극한정리는 그 오차를 $\sqrt{n}$배 확대했을 때 정규분포가 남는다는 정리이며, 델타 방법은 추정량에 매끄러운 함수를 적용했을 때 오차 분포가 어떻게 바뀌는지 설명하는 방법이다. 이 장은 독립 동일분포 표본에 대해 강한 큰수법칙(진술과 유한 분산 경우의 완전한 증명), 특성함수에 의한 중심극한정리의 증명, Berry–Esseen 형태의 오차 상계, 표본분산에 의한 표준화, 일차와 이차 델타 방법을 차례로 다룬다. 세 도구는 서로 연결되지만, 하나의 결론이 나머지를 자동으로 대체하지는 않는다. 선행 지식: 수렴의 종류(제20권 제10장), 독립합의 분산과 특성함수(제20권 제9장), Taylor 전개. 평균의 안정화와 표준화한 오차의 분포를 분리하여 읽는다.

큰수법칙은 평균의 오차가 0에 가까워지는지를 말한다. 중심극한정리는 그 작은 오차를 $\sqrt{n}$배 확대했을 때 어떤 분포가 남는지를 말한다. 델타 방법은 추정량에 매끄러운 함수를 적용했을 때 오차 분포가 어떻게 바뀌는지 설명한다.

11.1 약한 법칙과 강한 법칙의 범위

독립이고 공통 평균 μ, 공통 유한 분산 σ^2인 변수의 평균은

$$\mathbb{E}\overline{X}_n = \mu, \qquad \operatorname{Var}(\overline{X}_n) = \frac{\sigma^2}{n}$$

이므로 L^2와 확률의 의미에서 μ로 수렴한다. 앞 묶음의 증명은 Chebyshev 부등식 한 번으로 끝난다. 그러나 거의 확실한 수렴은 경로 전체를 통제해야 하므로 같은 부등식을 매 n에 적용한 $1/n$ 상계만으로 Borel–Cantelli 첫 결론을 쓸 수 없다. $\sum 1/n$이 발산하기 때문이다.

정리 11.1 (독립 동일분포의 강한 큰수법칙) $X_1, X_2, \dots$가 독립 동일분포이고 $\mathbb{E}\,|X_1| < \infty$이면

$$\frac{1}{n}\sum_{j=1}^{n} X_j \longrightarrow \mathbb{E}X_1 \quad \text{거의 확실히.}$$

유한한 분산은 이 정리의 필수조건이 아니다. 다만 적분가능성만으로 증명하려면 절단법 등 추가 도구가 필요하다. 아래에서는 조건을 더 강하게 둔 유한 분산 경우를 완전히 증명한다. 이 증명을 일반 정리 전체의 증명이라고 표시하지 않는다.

11.2 최대 부등식과 유한 분산 강한 법칙

보조정리 11.2 (Kolmogorov 최대 부등식) 독립이고 평균 0이며 유한 분산인 $Y_1, \dots, Y_n$에 대해 $S_k = \sum_{j=1}^{k} Y_j$라 하자. 모든 $a > 0$에 대해

$$\mathbb{P}\Big(\max_{1 \le k \le n} |S_k| \ge a\Big) \le \frac{\operatorname{Var}(S_n)}{a^2} = \frac{\sum_{j=1}^{n} \operatorname{Var}(Y_j)}{a^2}.$$

증명. A_k를 처음으로 $|S_k| \ge a$가 되는 시점이 k라는 사건이라 하자. A_k들은 배반이며 $Y_1, \dots, Y_k$만으로 결정된다. 미래합 $S_n - S_k$는 이 정보와 독립이고 평균 0이다. 따라서

$$\mathbb{E}[S_n^2 \mathbf{1}_{A_k}] = \mathbb{E}[S_k^2 \mathbf{1}_{A_k}] + \mathbb{E}[(S_n - S_k)^2 \mathbf{1}_{A_k}] \ge a^2 \mathbb{P}(A_k).$$

교차항 $2\mathbb{E}[S_k \mathbf{1}_{A_k}(S_n - S_k)]$은 독립성과 미래합의 영평균 때문에 사라진다. 배반 사건들에 대해 합하면 $\mathbb{E}S_n^2 \ge a^2 \sum_k \mathbb{P}(A_k)$이다. 오른쪽 합이 최대값 사건의 확률이고, $\mathbb{E}S_n^2 = \operatorname{Var}(S_n)$이므로 결론을 얻는다. □

정리 11.3 (유한 분산의 강한 법칙: 증명 가능한 범위) 독립인 Y_j들이 평균 0이고 $\sup_j \operatorname{Var}(Y_j) \le C < \infty$이면

$$S_n / n \longrightarrow 0 \quad \text{거의 확실히.}$$

특히 독립 동일분포이며 평균 μ, 유한 분산인 X_j에는 $Y_j = X_j - \mu$를 적용할 수 있다.

증명. 최대 부등식에서 $n = 2^m$, $a = \varepsilon 2^m$을 선택하면

$$\mathbb{P}\Big(\max_{k \le 2^m} |S_k| \ge \varepsilon 2^m\Big) \le \frac{C}{\varepsilon^2 2^m}.$$

m에 대한 확률합이 유한하므로 모든 양의 유리수 ε에 대해 문턱 초과는 유한 번만 일어난다. 따라서 $2^{-m} \max_{k \le 2^m} |S_k| \to 0$이 거의 확실히 성립한다. $2^{m-1} < n \le 2^m$이면

$$\frac{|S_n|}{n} \le 2 \, \frac{\max_{k \le 2^m} |S_k|}{2^m} \longrightarrow 0.$$

이로써 dyadic 시점 사이까지 통제된다. □

예제 11.4 (동일분포만으로 충분하지 않다) Z가 공정한 Bernoulli 변수이고 모든 $X_j = Z$라고 하자. 각 변수의 평균은 $1/2$지만 평균 $\overline{X}_n = Z$는 $1/2$로 수렴하지 않는다. 독립성 또는 이를 대체하는 의존성 제어가 필요하다. 시행을 많이 기록했다는 사실만으로 독립적인 정보가 늘어난 것은 아니다.

11.3 중심극한정리의 정확한 표준화

정리 11.5 (독립 동일분포 중심극한정리) X_j들이 독립 동일분포이고 $\mathbb{E}X_1 = \mu$, $0 < \sigma^2 = \operatorname{Var}(X_1) < \infty$이면

$$Z_n = \frac{\sum_{j=1}^{n} X_j - n\mu}{\sigma \sqrt{n}} = \frac{\sqrt{n}(\overline{X}_n - \mu)}{\sigma} \xrightarrow{d} N(0,1). \tag{11.1}$$

합의 표준편차는 $\sigma\sqrt{n}$이고 평균의 표준편차는 $\sigma/\sqrt{n}$이다. 두 표현을 섞으면 n 또는 $\sqrt{n}$의 계수가 틀어진다. 분산 0인 경우에는 변수가 거의 확실히 상수이므로 정규화 식을 사용하지 않는다.

보조정리 11.6 (특성함수의 이차 전개) $\mathbb{E}Y = 0$, $\mathbb{E}Y^2 = 1$이면

$$\varphi_Y(t) = 1 - \frac{t^2}{2} + o(t^2) \qquad (t \to 0).$$

Taylor 나머지 $e^{iu} - 1 - iu + u^2/2$를 u^2로 나눈 함수는 $u \to 0$에서 0으로 가고 실수축에서 유계이다. $u = tY$를 대입하면 나머지를 t^2로 나눈 값이 상수배 Y^2로 지배된다. 지배수렴과 첫 두 모멘트 조건으로 전개를 얻는다. 삼차 모멘트를 가정할 필요는 없다.

중심극한정리의 특성함수 증명. $Y_j = (X_j - \mu)/\sigma$로 표준화한다. 독립성에 의해

$$\varphi_{Z_n}(t) = \left[\varphi_Y\!\left(\frac{t}{\sqrt{n}}\right)\right]^n = \left[1 - \frac{t^2}{2n} + o(n^{-1})\right]^n \longrightarrow e^{-t^2/2}.$$

마지막 수렴에는 복소수 열 $z_n \to z$에 대해 $(1 + z_n/n)^n \to e^z$라는 사실을 쓴다. 마지막 함수는 표준정규의 특성함수이며 원점에서 연속이다. Lévy 연속성 정리를 적용하면 분포수렴이 성립한다. $\square$

여기서 사용한 Lévy 연속성 정리는 특성함수들이 점별로 어떤 함수 φ로 수렴하고 그 함수가 원점에서 연속이면, φ가 어떤 확률분포의 특성함수이며 해당 분포로 약수렴한다는 정리이다. 이 심화 정리는 위 증명의 외부 입력임을 명시한다. 원점 연속성은 삭제할 수 없다. 예를 들어 $N(0, n)$의 특성함수는 $t \neq 0$에서 0으로, $t = 0$에서 1로 수렴한다. 질량이 멀리 퍼져 나가므로 실수축 위의 확률분포로 수렴하지 않는다.

역사 (큰수법칙과 중심극한정리의 계보). 이항분포에 대한 정규근사는 de Moivre(1733)가 대칭 경우에서 처음 보였고 Laplace가 일반화하였다. 일반적인 독립 합에 대한 중심극한정리는 Lyapunov(1901)와 Lindeberg(1922)가 조건을 정교하게 다듬었고, 독립 동일분포 변수의 강한 큰수법칙을 유한 평균 조건만으로 증명한 것은 Kolmogorov(1933)이다. 본문의 최대 부등식은 Kolmogorov의 이름으로 불리는 도구이다.

11.4 정규근사와 유한 표본의 한계

예제 11.7 (이항 꼬리의 근사와 정확한 합) $S \sim \mathrm{Bin}(100, 0.4)$이면 평균은 40, 분산은 24이다. 정수 구간 $35 \le S \le 45$의 정확한 확률은

$$\sum_{k=35}^{45} \binom{100}{k} (0.4)^k (0.6)^{100-k}.$$

연속성 보정을 사용하는 정규근사는

$$\Phi\!\left(\frac{45.5 - 40}{\sqrt{24}}\right) - \Phi\!\left(\frac{34.5 - 40}{\sqrt{24}}\right)$$

이다. 정수 질량을 폭 1인 구간으로 대응시키는 근사이므로 양 끝에 $1/2$를 보정했다. 정확한 합은 약 0.738573이고 위 정규근사는 약 0.738428이다. 보정 없이 $\Phi((45-40)/\sqrt{24}) - \Phi((35-40)/\sqrt{24})$를 쓰면 약 0.6926으로 크게 낮아진다. 이 보정은 중심극한정리의 가정을 대체하지 않으며 모든 이산분포에서 동일한 오차 개선을 보장하는 보편 법칙도 아니다.

정리 11.8 (Berry–Esseen 형태의 오차 상계) 중심극한정리의 조건에 더해 $\rho = \mathbb{E}\,|X_1 - \mu|^3 < \infty$ 이면 어떤 보편적인 유한 상수 C에 대해

$$\sup_{x} \left| \mathbb{P}(Z_n \le x) - \Phi(x) \right| \le \frac{C\rho}{\sigma^3 \sqrt{n}}.$$

이 정리는 삼차 절대 모멘트가 있는 경우 분포함수 근사의 속도를 제공한다. 특정 수치 상수를 채택할 때에는 사용하는 정리의 버전과 가정을 함께 확인해야 한다. 여기서는 최적 상수나 그 증명을 주장하지 않는다. n이 크다는 말만으로 충분한 근사라고 단정하지 않고 꼬리와 모멘트 비율을 살펴야 한다.

흔한 오류 (무한 분산에서의 $\sqrt{n}$ 정규화). 무한 분산 분포에서는 위 $\sqrt{n}$ 정규화가 틀릴 수 있다. 예를 들어 독립 표준 Cauchy 변수들의 평균은 모든 n에서 다시 표준 Cauchy 분포다. 특성함수 $e^{-|t|}$를 사용하면 평균의 특성함수가 $[e^{-|t|/n}]^n = e^{-|t|}$이기 때문이다. 이 예의 평균은 애초에 기댓값이 존재하지 않으며, 유한 평균의 큰수법칙과 모순되지 않는다.

11.5 분산을 추정하여 표준화하기

독립 동일분포이고 유한한 양의 분산을 가정하자. 표본분산

$$S_n^2 = \frac{1}{n-1} \sum_{j=1}^{n} (X_j - \overline{X}_n)^2, \qquad n \ge 2$$

은 σ^2로 거의 확실히 수렴한다. 실제로

$$S_n^2 = \frac{n}{n-1} \left(\frac{1}{n} \sum_{j=1}^{n} X_j^2 - \overline{X}_n^2 \right)$$

이고, $\mathbb{E}X_1^2 < \infty$이므로 X_j^2에 적분가능성 형태의 강한 큰수법칙을 적용한다. 여기서는 X_j^2의 분산, 즉 X_j의 사차 모멘트까지 요구하는 유한 분산 증명만으로 대체해서는 안 된다. 일반 강한 법칙을 사용했음을 명확히 한다. $\overline{X}_n \to \mu$ 거의 확실히와 함께 $n/(n-1) \to 1$을 쓰면 $S_n^2 \to \mathbb{E}X_1^2 - \mu^2 = \sigma^2$이다.

$S_n \xrightarrow{\mathbb{P}} \sigma > 0$과 Slutsky 정리로

$$\frac{\sqrt{n}(\overline{X}_n - \mu)}{S_n} \xrightarrow{d} N(0,1)$$

이다. 정규모집단일 때에는 유한 표본에서 정확히 t_{n-1} 분포를 따른다는 더 강한 결과가 있지만, 임의의 모집단에 대해 그 유한 표본 등식을 적용할 수 없다. 점근적 정규성, 정확한 t 분포, 정규근사라는 서로 다른 주장을 분리한다.

11.6 일차 델타 방법

정리 11.9 (일차원 델타 방법) $\sqrt{n}(T_n - \theta) \xrightarrow{d} N(0, \tau^2)$이고 g가 θ의 근방에서 정의되며 θ에서 미분가능하다고 하자. 그러면

$$\sqrt{n}[g(T_n) - g(\theta)] \xrightarrow{d} N\big(0, [g'(\theta)]^2 \tau^2\big). \tag{11.2}$$

T_n이 g의 정의역 밖에 있는 드문 사건은 임의로 정의하여 그 확률이 0으로 가게 처리할 수 있다.

증명. 먼저 가정에서 $T_n \xrightarrow{\mathbb{P}} \theta$가 따른다. $\sqrt{n}(T_n - \theta)$가 분포수렴하므로 확률적으로 유계이고, 따라서 $T_n - \theta = n^{-1/2} \cdot O_{\mathbb{P}}(1) \xrightarrow{\mathbb{P}} 0$이기 때문이다. 미분가능성으로 $g(T_n) - g(\theta) = g'(\theta)(T_n - \theta) + r(T_n)(T_n - \theta)$이며 $r(t) \to 0$ $(t \to \theta)$이다. 따라서 $r(T_n) \xrightarrow{\mathbb{P}} 0$이다. $\sqrt{n}(T_n - \theta)$는 분포수렴하므로 확률적으로 유계이고, 나머지의 곱은 확률수렴으로 0이다. Slutsky 정리로 결론을 얻는다. □

예제 11.10 (양의 평균의 로그) $\theta > 0$이고 T_n이 위 점근적 정규성을 갖는다면 $g(x) = \log x$에서

$$\sqrt{n}(\log T_n - \log \theta) \xrightarrow{d} N(0, \tau^2/\theta^2).$$

$T_n \le 0$일 확률은 일관성 때문에 0으로 가지만 유한 표본에서 존재할 수 있다. 통계량을 구현할 때에는 그 표본에서 로그를 무조건 계산하는 대신 정의역 처리 규칙을 명시해야 한다.

벡터형에서는 $\sqrt{n}(T_n - \theta) \xrightarrow{d} N_d(0, \Sigma)$이고 $g : \mathbb{R}^d \to \mathbb{R}^k$가 θ에서 미분가능하면

$$\sqrt{n}[g(T_n) - g(\theta)] \xrightarrow{d} N_k\big(0,\ Dg(\theta)\, \Sigma\, Dg(\theta)^{\top}\big).$$

예를 들어 두 평균의 비 $g(a, b) = a/b$에서는 $b \neq 0$이 필요하며 기울기는 $(1/b,\ -a/b^2)$이다. 두 평균의 공분산을 무시하면 델타 방법의 분산도 틀릴 수 있다.

11.7 도함수가 영일 때의 다른 척도

$g'(\theta) = 0$이면 일차 델타 방법의 극한은 분산 0인 상수이다. "근사가 아무 정보도 주지 않는다"는 신호일 수 있으며, 더 높은 차수의 Taylor 전개가 필요하다.

명제 11.11 (이차 델타 방법) $\sqrt{n}(T_n - \theta) \xrightarrow{d} Z$이고, g가 θ 근방에서 두 번 연속 미분가능하며 $g'(\theta) = 0$이면

$$n[g(T_n) - g(\theta)] \xrightarrow{d} \tfrac{1}{2} g''(\theta) Z^2.$$

증명. Taylor 전개 $g(T_n) - g(\theta) = \tfrac{1}{2} g''(\theta)(T_n - \theta)^2 + o((T_n - \theta)^2)$에서 나머지가 $o((T_n - \theta)^2)$이고 $n(T_n - \theta)^2$가 확률적으로 유계이므로 $n \cdot o((T_n - \theta)^2) \xrightarrow{\mathbb{P}} 0$이다. 연속사상 정리로 $n(T_n - \theta)^2 \xrightarrow{d} Z^2$이므로 Slutsky 정리에 의해 결론이 성립한다. □

특히 Z가 정규여도 Z^2는 정규가 아니다.

예제 11.12 (평균이 영인 변수의 제곱) 평균 0, 분산 $\sigma^2 > 0$인 독립 동일분포 표본의 평균에 $g(x) = x^2$를 적용하면

$$\frac{n \overline{X}_n^2}{\sigma^2} \xrightarrow{d} \chi^2_1.$$

> $\sqrt{n}$ 대신 n 척도가 필요하다. $g'(0)=0$인데도 일차 정규근사의 표준오차만 대입하면 본질적인 비정규 극한을 놓친다.

11.8 연습문제와 해설

> **연습문제 11.13** 독립 동일분포의 평균이 5, 분산이 9이다. $n=100$일 때 표본평균의 표준편차와 Chebyshev 상계 $\mathbb{P}(\left|\overline{X}_n-5\right|\ge 0.6)$를 구하라.

풀이. 표준편차는 $3/10=0.3$이고 상계는 $0.09/0.36=1/4$이다. 정규근사는 추가적인 분포 근사이며 이 상계와 같은 말이 아니다.

> **연습문제 11.14** $X_j\sim \mathrm{Exp}(2)$(비율 모수 2)가 독립 동일분포이다. $\sqrt{n}(\overline{X}_n-1/2)$의 극한 분포를 구하라.

풀이. 지수분포의 평균은 $1/2$, 분산은 $1/4$이므로 $N(0,1/4)$에 분포수렴한다. 표준정규로 만들려면 $2\sqrt{n}(\overline{X}_n-1/2)$를 사용한다.

> **연습문제 11.15** 독립 Bernoulli 표본의 성공확률이 $p\in(0,1)$이다. 표본비율 $\widehat{p}_n$의 로그 오즈에 델타 방법을 적용하라.

풀이. $g(p)=\log[p/(1-p)]$이고 $g'(p)=1/[p(1-p)]$이다. 따라서

$$\sqrt{n}\Big(\log\frac{\widehat{p}_n}{1-\widehat{p}_n}-\log\frac{p}{1-p}\Big)\xrightarrow{d}N\Big(0,\frac{1}{p(1-p)}\Big).$$

$\widehat{p}_n=0$ 또는 1인 유한 표본에서는 로그 오즈가 유한하지 않다. 그 확률은 $(1-p)^n+p^n\to 0$이므로 해당 사건에 별도 유한값을 정의한 통계량에 대해 위 점근 결론을 읽을 수 있다.

> **연습문제 11.16** $\sqrt{n}(T_n-2)\xrightarrow{d}N(0,4)$일 때 $\sqrt{n}(T_n^2-4)$의 극한 분포를 구하라.

풀이. $g(x)=x^2$, $g'(2)=4$이므로 분산은 $4^2\cdot 4=64$이며 극한은 $N(0,64)$이다. 중심이 0인 제곱 예제와 달리 여기서는 일차항이 사라지지 않는다.

> **연습문제 11.17** $\sqrt{n}\,T_n\xrightarrow{d}N(0,4)$일 때 nT_n^2의 극한 분포를 구하라.

풀이. 연속사상 정리로 $nT_n^2\xrightarrow{d}4\chi_1^2$이다. 일차 델타 방법으로 정규분포를 주장할 수 없는 경우다.

극한정리는 큰 표본의 구조를 알려 주지만 특정한 유한 표본에서 오차가 얼마인지 직접 보장하지 않을 수 있다. 다음 장(제20권 제12장)은 모멘트와 유계성 가정을 이용하여 유한 표본 꼬리확률을 통제한다.

제 12 장

확률 부등식, 집중, 큰편차의 입문

개요 확률 부등식은 확률변수에 관한 제한된 정보(모멘트, 적률생성함수, 유계성)만으로 드문 큰 오차의 확률에 상계 또는 하계를 주는 부등식이다. 이 장은 Markov 부등식에서 출발하여 Chebyshev 부등식, Cantelli 부등식, Paley–Zygmund 하계를 세우고, 적률생성함수에 Markov 부등식을 적용하는 Chernoff 방법, Hoeffding 보조정리와 부등식, 준정규 변수, Bernstein 부등식, Bernoulli 변수의 상대엔트로피 꼬리를 차례로 증명한다. 끝으로 Cramér 속도함수와 큰편차 원리의 진술을 소개하여, 유한한 n의 상계와 $n \to \infty$에서의 지수적 감소율이 어떻게 연결되는지 밝힌다. 가정이 강할수록 더 날카로운 상계를 얻지만, 가정이 성립하지 않는 자료에 그 상계를 적용하면 보장이 사라진다. 선행 지식: Markov와 Chebyshev 부등식, 적률생성함수, 볼록성, 독립성(제20권 제5장, 제20권 제9장). 이 장의 경계는 유한 표본에서 성립하는 상계이며 실제 확률과 구별한다.

평균이나 극한분포를 아는 것과 드문 큰 오차의 확률을 통제하는 것은 다른 문제이다. 확률 부등식은 제한된 가정에서 가능한 최악의 꼬리를 상계한다. 가정이 강할수록 더 날카로운 상계를 얻을 수 있지만, 유계성이나 지수적 모멘트가 없는 자료에 그 상계를 적용하면 보장이 사라진다. 이 장은 이차 모멘트에서 지수적 꼬리까지 조건을 단계적으로 비교한다.

12.1 모멘트에 근거한 기본 상계

비음수 함수 h가 문턱 사건에서 $h(X) \geq c > 0$을 만족하면 **Markov 부등식**(*Markov's inequality*)으로 그 사건의 확률을 $\mathbb{E}h(X)/c$로 제한할 수 있다. $h(x) = |x|^p$를 택하면

$$\mathbb{P}(|X| \geq t) \leq \frac{\mathbb{E}\,|X|^p}{t^p}, \qquad t > 0 \tag{12.1}$$

이다. 중심화한 제곱은 **Chebyshev 부등식**(*Chebyshev's inequality*)이고, 지수함수는 이후의 Chernoff 방법이 된다. 같은 원리에 어떤 함수를 넣는지가 필요한 가정과 꼬리 감소율을 결정한다.

명제 12.1 (Cantelli의 한쪽 부등식) $\mathbb{E}X = \mu$, $\operatorname{Var}(X) = \sigma^2 < \infty$이면 $t > 0$에서

$$\mathbb{P}(X - \mu \geq t) \leq \frac{\sigma^2}{\sigma^2 + t^2}.$$

증명. $Y = X - \mu$라 하고 $a \geq 0$을 택한다. $Y \geq t$이면 $(Y + a) \geq t + a > 0$이므로 $(Y + a)^2 \geq (t + a)^2$이다. 따라서 Markov 부등식과 $\mathbb{E}Y = 0$, $\mathbb{E}(Y + a)^2 = \sigma^2 + a^2$에 의해

$$\mathbb{P}(Y \geq t) \leq \frac{\sigma^2 + a^2}{(t + a)^2}.$$

$\sigma^2 > 0$일 때 $a = \sigma^2/t$를 대입하면 분자는 $\sigma^2(t^2 + \sigma^2)/t^2$, 분모는 $(t^2 + \sigma^2)^2/t^2$이므로 비는 $\sigma^2/(\sigma^2 + t^2)$로 원하는 값이다. $\sigma^2 = 0$이면 $Y = 0$이 거의 확실하므로 확률은 0이다. □

Chebyshev의 σ^2/t^2보다 한쪽 꼬리에 더 적합하다. 다만 두쪽 사건에 같은 값을 그대로 사용할 수는 없다. 예를 들어 평균 0, 분산 1인 변수에서 $\mathbb{P}(X \ge 2) \le 1/5$이고, 두쪽 $|X| \ge 2$에는 Chebyshev의 $1/4$가 적용된다.

명제 12.2 (Paley–Zygmund 하계) $X \ge 0$, $0 < \mathbb{E}X < \infty$, $\mathbb{E}X^2 < \infty$이면 $0 < \theta < 1$에 대해

$$\mathbb{P}(X > \theta\,\mathbb{E}X) \ge (1-\theta)^2 \frac{(\mathbb{E}X)^2}{\mathbb{E}X^2}.$$

증명. $A = \{X > \theta \mathbb{E}X\}$로 나누면 $X \mathbf{1}_{A^c} \le \theta \mathbb{E}X$이고

$$\mathbb{E}X = \mathbb{E}[X\mathbf{1}_{A^c}] + \mathbb{E}[X\mathbf{1}_A] \le \theta\,\mathbb{E}X + \mathbb{E}[X\mathbf{1}_A]$$

이다. Cauchy–Schwarz로 마지막 항은 $(\mathbb{E}X^2)^{1/2}\mathbb{P}(A)^{1/2}$ 이하이다. 따라서 $(1-\theta)\mathbb{E}X \le (\mathbb{E}X^2)^{1/2}\mathbb{P}(A)^{1/2}$이고, 양변이 비음수이므로 제곱하여 정리하면 결론을 얻는다. $\square$

이것은 상계가 아니라 양의 값이 나타날 확률의 하계이다. 평균만 크고 실제로 양수가 나올 가능성은 매우 작을 수 있으므로, 이차 모멘트와의 비율이 필요하다. 조합확률의 존재 증명과 두 번째 모멘트 방법에서 자주 사용한다.

12.2 지수적 Markov 부등식과 최적화

S의 적률생성함수가 어떤 $t > 0$에서 유한하면

$$\mathbb{P}(S \ge a) = \mathbb{P}(e^{tS} \ge e^{ta}) \le e^{-ta}\,\mathbb{E}e^{tS}$$

이다. 가능한 $t > 0$ 중 가장 작은 상계를 고르는 것이 **Chernoff 방법**(*Chernoff bound*)이다. 독립합 $S = \sum_{i} X_i$이면 로그를 취한 상계는

$$\mathbb{P}(S \ge a) \le \inf_{t>0} \exp\Big[-ta + \sum_{i} K_{X_i}(t)\Big] \tag{12.2}$$

이다. 여기서 $K_X(t) = \log \mathbb{E}e^{tX}$는 누율생성함수이고, 적률생성함수가 유한한 t만 최적화한다. 하한 꼬리에는 음의 t를 사용하거나 $-S$에 같은 방법을 적용한다.

예제 12.3 (정규 꼬리의 지수 상계) $Z \sim N(0,1)$이면 $K_Z(t) = t^2/2$이다. $a > 0$에서 $-ta + t^2/2$를 최소화하는 값은 $t = a$이므로

$$\mathbb{P}(Z \ge a) \le e^{-a^2/2}$$

이다. 실제 정규 꼬리와 동일한 것은 아니며 다항식 수준의 인자(a^{-1} 정도)를 생략한 상계이다. 그래도 a가 커질 때의 핵심 지수 감소를 반영한다.

12.3 Hoeffding 보조정리와 유계 독립합

보조정리 12.4 (Hoeffding 보조정리) $X \in [a,b]$가 거의 확실히 성립하고 $\mathbb{E}X = 0$이면 모든 실수 t에서

$$\mathbb{E}e^{tX} \le \exp\Big(\frac{t^2(b-a)^2}{8}\Big).$$

증명. $K(t) = \log \mathbb{E}e^{tX}$라 하자. X가 유계 변수이므로 모든 미분이 정당하다. 지수적으로 기울인 분포 $d\mathbb{P}_t = e^{tX}\,d\mathbb{P}/\mathbb{E}e^{tX}$ 아래에서도 지원집합은 $[a,b]$이며

$$K''(t) = \operatorname{Var}_t(X) \le \mathbb{E}_t\Big(X - \frac{a+b}{2}\Big)^2 \le \frac{(b-a)^2}{4}$$

이다. 첫 부등식은 분산이 임의의 상수 주위의 이차 모멘트 이하라는 성질이고, 둘째는 $[a,b]$ 안의 X가 구간 중점에서 $(b-a)/2$ 이내에 있다는 사실이다. $K(0)=0$, $K'(0) = \mathbb{E}X = 0$에서 이 이차 도함수 상계를 두 번 적분하면 $K(t) \le t^2(b-a)^2/8$이다. 음의 t에도 Taylor 적분 나머지 또는 반대 방향 적분으로 같은 식이 성립한다. □

정리 12.5 (Hoeffding 부등식) 독립인 $X_1, \dots, X_n$이 거의 확실히 $a_i \le X_i \le b_i$를 만족한다고 하자. $S = \sum_{i} (X_i - \mathbb{E}X_i)$이고 $u > 0$이면

$$\mathbb{P}(S \ge u) \le \exp\Big(-\frac{2u^2}{\sum_{i}(b_i - a_i)^2}\Big).$$

증명. $X_i - \mathbb{E}X_i$는 평균 0이고 길이 $b_i - a_i$의 구간에 값을 가진다. 독립성과 보조정리로 $\mathbb{E}e^{tS} \le \exp(t^2 A/8)$, $A = \sum_i (b_i-a_i)^2$이다. Chernoff 상계의 지수 $-tu + t^2A/8$을 $t = 4u/A$에서 최소화하면 $-4u^2/A + 2u^2/A = -2u^2/A$를 얻는다. $-S$의 꼬리와 합집합 상계를 사용하면 두쪽 결과가 나온다. □

분모가 0이면 $S = 0$이므로 꼬리확률은 0이다. 두쪽 꼬리는 오른쪽의 두 배로 상계할 수 있다.

예제 12.6 (유계 평균의 정확도에 필요한 표본 수) 독립인 $X_i \in [0,1]$의 평균에 대해, 동일분포를 가정하지 않아도

$$\mathbb{P}\Big(\Big|\overline{X}_n - \mathbb{E}\overline{X}_n\Big| \ge \varepsilon\Big) \le 2e^{-2n\varepsilon^2}$$

이다. 상계를 δ 이하로 만들려면

$$n \ge \frac{\log(2/\delta)}{2\varepsilon^2}$$

이면 충분하다. $\varepsilon = 0.05$, $\delta = 0.05$이면 $\log 40 / 0.005 \approx 737.78$이므로 $n \ge 738$이 한 충분조건이다. 실제 필요한 최소 표본 수라는 뜻은 아니다. 부등식이 느슨할 수 있으며 추가 분포 정보가 있으면 더 작은 표본에서도 같은 보장이 가능하다.

역사 (집중 부등식의 계보). 지수 모멘트로 합의 꼬리를 누르는 방법은 Chernoff(1952)의 이름으로 불리고, 유계 변수의 합에 대한 지수 부등식(정리 12.5)은 Hoeffding(1963)이 정리하였다. 큰편차 속도함수의 Legendre 변환 표현은 Cramér(1938)에서 비롯한다.

12.4 준정규 꼬리와 여러 좌표의 최댓값

정의 12.7 (준정규 변수) 평균 0인 변수 X가 모든 실수 t에 대해

$$\mathbb{E}e^{tX} \le e^{vt^2/2}$$

를 만족하면 분산 대리값 $v \ge 0$을 갖는 **준정규 변수**(*sub-Gaussian variable*)라고 한다. 여기서 v는 실제 분산과 같을 필요가 없지만 항상 $\operatorname{Var}(X) \le v$이다.

평균 0인 $N(0,\sigma^2)$에는 $v=\sigma^2$를 사용할 수 있다. 중심화한 $[a,b]$ 유계 변수에는 Hoeffding 보조정리로 $v=(b-a)^2/4$를 사용할 수 있다. 독립 준정규 변수들의 합에는 대리값들을 더할 수 있고, 상수배 cX에는 $c^2 v$를 사용할 수 있다.

Chernoff 최적화로

$$\mathbb{P}(|X|\ge u)\le 2e^{-u^2/(2v)}$$

이다. m개 변수 $X_1,\dots,X_m$ 각각이 같은 대리값 $v>0$을 갖는다면, 이 변수들 사이의 독립성을 요구하지 않고도

$$\mathbb{P}\Big(\max_{j\le m}|X_j|\ge u\Big)\le 2m\,e^{-u^2/(2v)}$$

이다. 따라서 확률 적어도 $1-\delta$로 최대 절댓값은 $\sqrt{2v\log(2m/\delta)}$ 이하이다. 마지막 단계는 합집합 상계이므로 좌표 사이 독립성이 필요 없지만, 각 변수의 준정규 가정은 여전히 필요하다.

흔한 오류. “분산이 유한하다”와 “준정규다”는 같은 말이 아니다. 유한 분산이 있어도 다항식 꼬리를 가진 분포는 일반적인 준정규 지수 상계를 만족하지 않는다. 자료에서 관측한 최댓값만으로 모집단 변수가 유계라고 단정할 수도 없다.

12.5 분산 정보를 함께 쓰는 Bernstein 부등식

정리 12.8 (유계 변수의 Bernstein 부등식) 독립인 평균 0 변수 X_i가 $|X_i|\le b$를 거의 확실히 만족하고 $v=\sum_i \mathbb{E}X_i^2$라 하자. $b>0$, $u>0$에서

$$\mathbb{P}\Big(\sum_i X_i\ge u\Big)\le \exp\Big[-\frac{u^2}{2(v+bu/3)}\Big].$$

증명. $0<t<3/b$에서 급수 전개와 $\mathbb{E}X_i=0$을 사용한다. $k\ge 2$이면 $\mathbb{E}|X_i|^k\le b^{k-2}\mathbb{E}X_i^2$이며 $k!\ge 2\cdot 3^{k-2}$이므로 ($k=2,3$에서 등호이고 이후에는 $k!$의 증가가 3^{k-2}보다 빠르다)

$$\mathbb{E}e^{tX_i}\le 1+\sum_{k\ge 2}\frac{t^k b^{k-2}\mathbb{E}X_i^2}{2\cdot 3^{k-2}}=1+\frac{t^2\mathbb{E}X_i^2}{2(1-tb/3)}$$

이다. 등비급수의 공비가 $tb/3<1$이다. $\log(1+x)\le x$와 독립성으로

$$\log\mathbb{E}e^{t\sum_i X_i}\le\frac{vt^2}{2(1-tb/3)}$$

이다. $v>0$일 때 $t=u/(v+bu/3)$를 Chernoff 상계에 대입한다. 이 t는 $t<3/b$를 만족하고 $1-tb/3=v/(v+bu/3)$이므로

$$-tu+\frac{vt^2}{2(1-tb/3)}=-\frac{u^2}{v+bu/3}+\frac{u^2}{2(v+bu/3)}=-\frac{u^2}{2(v+bu/3)}$$

이 되어 제시한 지수가 나온다. $v=0$이면 모든 변수가 거의 확실히 0이므로 결과는 자명하다. $\square$

작은 편차에서는 분포의 v가 지배하여 Gaussian 형태의 감소를 보인다. 큰 편차에서는 $bu/3$이 중요해진다. Hoeffding은 범위만 쓰지만 Bernstein은 실제 분산도 사용하므로 분산이 범위에 비해 작은 경우 유리할 수 있다. 어느 부등식이 더 좋은지는 수치와 문턱에 따라 비교해야 한다.

예제 12.9 (드문 성공의 평균) 독립 Bernoulli 변수 X_i의 성공확률이 p이면 중심화한 변수는 절댓값 1 이하이고 총분산은 $np(1-p)$이다. 따라서

$$\mathbb{P}(\overline{X}_n - p \ge \varepsilon) \le \exp\!\left[-\frac{n\varepsilon^2}{2\big(p(1-p) + \varepsilon/3\big)}\right].$$

작은 p에 대해서는 분산 정보를 활용하지만, p를 모르는 실제 추론에서는 알 수 없는 참값을 관측값으로 무조건 바꾸면 같은 정리가 되지 않는다. 경험적 Bernstein 경계는 이를 다루기 위한 별도 결과이다.

12.6 Bernoulli 꼬리와 상대엔트로피

$X_i \sim \mathrm{Bern}(p)$가 독립 동일분포이고 $0 < p < q < 1$이라 하자. Chernoff 경계에서

$$\mathbb{P}(\overline{X}_n \ge q) \le \inf_{t>0} \exp\!\left\{n\left[-tq + \log\!\left(1 - p + pe^{t}\right)\right]\right\}$$

이다. 미분하여 최적값을 구하면 $pe^t/(1-p+pe^t) = q$이므로

$$t_\ast = \log \frac{q(1-p)}{p(1-q)}$$

이고, $q > p$이므로 $t_\ast > 0$이다. 대입하면

$$\mathbb{P}(\overline{X}_n \ge q) \le e^{-nD(q\|p)}, \qquad D(q\|p) = q\log\frac{q}{p} + (1-q)\log\frac{1-q}{1-p} \tag{12.3}$$

이다. 이는 Bernoulli 분포들 사이의 **상대엔트로피**(*relative entropy*, Kullback–Leibler 발산)이다. 로그는 자연로그를 사용한다. $q < p$의 아래쪽 꼬리는 음의 기울임으로 같은 형태의 상계를 얻는다. $q = 1$에서는 극한 $D(1\|p) = \log(1/p)$를 사용하면 정확한 확률 p^n과 일치한다.

예제 12.10 (같은 사건에 대한 경계 비교) $S \sim \mathrm{Bin}(100, 1/2)$에서 $\mathbb{P}(S \ge 60)$을 생각하자. $\mathrm{Var}(S) = 25$이므로 Chebyshev로는 한쪽 사건을 두쪽 사건에 포함시켜 $1/4$로 상계한다. Cantelli는 $25/(25+100) = 1/5$를 준다. Hoeffding의 한쪽 상계는 e^{-2}이며, 최적 Bernoulli Chernoff 상계는

$$\exp\!\left[-100\, D(0.6\|0.5)\right]$$

이다. 실제 확률은 $2^{-100}\sum_{k=60}^{100}\binom{100}{k} \approx 0.028444$다. Hoeffding 상계는 약 0.135335, Bernoulli Chernoff 상계는 약 0.133514이다(여기서 $D(0.6\|0.5) \approx 0.020136$). 상계들은 모두 유효하지만 정확한 확률과 상당한 차이가 있을 수 있다. 계산할 수 있는 작은 이항 문제에서는 정확한 합이 검산 기준이 된다.

12.7 큰편차 원리에서 무엇을 주장하는가

집중부등식은 유한한 n의 상계를 주고, 큰편차 이론은 확률의 로그를 n으로 나눈 극한 규모를 설명한다. 독립 동일분포 X_i의 적률생성함수가 영점 근방에서 유한하면 **Cramér 이론**의 **속도함수**(*rate function*)는

$$I(x) = \sup_{t \in \mathbb{R}} \{tx - K_X(t)\}$$

이다. 여기서 $K_X(t) = +\infty$인 곳은 최적화에 기여하지 않는다. I는 볼록하고 비음수이며 보통 평균에서 0이 된다.

정확한 **큰편차 원리**(*large deviation principle*)의 한 표준 표현은 모든 열린집합 G와 닫힌집합 F에 대해

$$\liminf_{n\to\infty} \frac{1}{n}\log \mathbb{P}(\overline{X}_n \in G) \ge -\inf_{x\in G} I(x),$$
$$\limsup_{n\to\infty} \frac{1}{n}\log \mathbb{P}(\overline{X}_n \in F) \le -\inf_{x\in F} I(x)$$

가 성립한다는 것이다. 빈집합의 하한은 $+\infty$, 확률 0의 로그는 $-\infty$로 해석한다. 이 정리는 위의 영점 근방 적률생성함수 조건을 가진 실수값 독립 동일분포 표본에 대해 적용하는 심화 결과로 제시하며 여기서 일반 증명을 하지는 않는다.

모든 사건의 확률이 정확히 $e^{-nI(x)}$라는 뜻은 아니다. 열린집합과 닫힌집합의 하한이 일치하는 등 조건이 맞을 때 로그 규모가 정해진다. 앞에 붙는 다항식 인자나 유한 표본 상수는 로그를 n으로 나누면 사라질 수 있다. 중심극한정리는 평균 주위의 $n^{-1/2}$ 규모를 보고, 큰편차는 평균에서 고정된 거리만큼 벗어나는 사건의 지수적 감소를 본다.

> **예제 12.11 (정규 평균의 속도함수)** $X_i \sim N(\mu,\sigma^2)$, $\sigma>0$이면 $K(t)=\mu t+\sigma^2 t^2/2$이다. 최적 $t=(x-\mu)/\sigma^2$를 대입하여
> $$I(x)=\frac{(x-\mu)^2}{2\sigma^2}$$
> 를 얻는다. 이 값은 $t(x-\mu)-\sigma^2t^2/2=(x-\mu)^2/\sigma^2-(x-\mu)^2/(2\sigma^2)$로 직접 확인된다. $a>\mu$에서 평균의 위쪽 꼬리는 로그 규모로 $-n(a-\mu)^2/(2\sigma^2)$를 갖는다. 정규분포를 알고 있으므로 이 경우에는 정확한 꼬리 $1-\Phi(\sqrt{n}(a-\mu)/\sigma)$와 직접 비교할 수 있다.

12.8 연습문제와 해설

> **연습문제 12.12** 평균 0, 분산 4인 변수에 대해 $\mathbb{P}(X\ge 3)$의 Cantelli 상계를 구하라.

풀이. $4/(4+9)=4/13\approx 0.308$이다. Chebyshev를 통한 한쪽 상계 $4/9\approx 0.444$보다 작다. 둘 다 정확한 분포를 정하지 않는 모멘트 기반 경계다.

> **연습문제 12.13** 독립인 $[0,1]$ 변수의 평균이 그 기댓값에서 0.1 이상 벗어날 확률을 0.01 이하로 보장하려 한다. Hoeffding의 충분 표본 수를 구하라.

풀이. $n\ge \log(200)/(2\cdot 0.1^2)\approx 264.916$이므로 $n=265$면 충분하다. 정수 표본 수는 올림한다.

> **연습문제 12.14** 독립인 평균 0 준정규 변수 X_i가 각각 대리값 v_i를 갖는다. $T=\sum_i a_i X_i$의 대리값을 구하라.

풀이. 적률생성함수를 곱하면 $\mathbb{E}e^{tT}\le \exp\bigl[t^2\sum_i a_i^2 v_i/2\bigr]$이다. 따라서 $\sum_i a_i^2 v_i$를 쓸 수 있다. 계수가 음수여도 제곱으로 들어간다.

> **연습문제 12.15** $X\sim \mathrm{Bern}(p)$, $0<p<1$에 Paley–Zygmund 부등식을 적용하여 $\mathbb{P}(X>\theta p)$의 하계를 구하고 실제 확률과 비교하라.

풀이. $\mathbb{E}X=\mathbb{E}X^2=p$이므로 하계는 $(1-\theta)^2 p$이다. $0<\theta<1$이면 문턱 θp는 0과 1 사이이므로 실제 확률은 p이다. 하계는 유효하지만 일반적으로 등호는 아니다.

연습문제 12.16 Bernoulli 성공확률 $p = 1/4$일 때 표본이 모두 성공할 확률을 상대엔트로피 경계로 계산하라.

풀이. $q = 1$의 극한을 사용하면 $D(1\|1/4) = \log 4$이므로 $e^{-n\log 4} = 4^{-n}$이다. 이 경계는 해당 끝점 사건에서 정확한 확률과 일치한다.

다음 연결. 확률론의 두 묶음은 공리에서 극한과 집중까지의 기본 언어를 정리했다. 수리통계는 미지의 분포나 모수에 관해 자료에서 결론을 내리는 절차를 설계하고 그 오차를 평가한다. 확률모형의 참값이 주어진 계산과, 그 참값을 추정하여 대신 넣는 추론을 다음 권에서 구별한다.

제 21 권

확률과정

제21권은 시간에 따라 변하는 불확실한 현상을 확률과정으로 모형화하는 이론을 다룬다. 제1장은 시간지표, 유한차원 분포, 경로, 정상성의 개념을 정하고, 제2–3장은 이산시간 Markov 연쇄의 전이행렬과 정상분포, 흡수와 도달시간과 기본행렬을 다룬다. 제4장은 Poisson 과정과 지수 대기시간을, 제5장은 마팅게일과 정지 규칙을 다룬다. 제6장은 Brownian 운동, Itô 적분, 확률미분방정식으로 연속시간 확률과정의 이론을 마무리한다.

제 1 장

시간지표, 분포, 경로, 정상성

개요 확률과정은 시간지표집합 위에서 정의된 확률변수의 모임이며, 각 시각의 분포, 시각들 사이의 의존성, 하나의 표본에서 이어지는 경로를 함께 갖는 대상이다. 이 장은 확률과정의 정의와 표본경로, 유한차원 분포와 Kolmogorov 일관성, 수정과 구별불가능성의 차이, 여과와 적합성, 독립 증분과 정상 증분, 엄격 정상성과 약정상성을 차례로 정의하고 각 개념을 가르는 예제를 제시한다. 시각별 주변분포만으로는 과정이 정해지지 않으며, 같은 유한차원 분포를 가진 두 과정이 경로 수준에서는 다를 수 있다는 점이 이 장의 중심 메시지이다. 선행 지식: 확률공간, 결합분포, 조건부 기댓값, 확률수렴(제20권 제8장, 제20권 제10장). 확률과정에서는 시간별 분포와 하나의 표본에서 이어지는 경로를 구별한다.

확률변수 하나가 한 번의 불확실한 관측을 나타낸다면 확률과정은 시간이나 공간의 여러 지점에서 연결된 관측을 나타낸다. 주가, 대기열의 길이, 입자의 위치, 반복 알고리즘의 오차는 시간에 따른 변수들의 모임으로 기술할 수 있다. 각 시간의 분포만 정하는 것으로는 충분하지 않다. 시간들 사이의 의존성과 표본경로의 성질이 함께 필요하다.

1.1 확률과정의 두 관점

정의 1.1 (확률과정) 확률공간 $(\Omega, \mathcal{F}, \mathbb{P})$와 지표집합 T 위의 확률변수족 $\{X_t : t \in T\}$을 **확률과정**(*stochastic process*)이라 한다. 고정된 t에서는 $\omega \mapsto X_t(\omega)$가 확률변수이고, 고정된 ω에서는 $t \mapsto X_t(\omega)$가 **표본경로**(*sample path*)이다.

$T = \{0, 1, 2, \dots\}$이면 **이산시간** 과정, $T = [0, \infty)$이면 **연속시간** 과정이다. 상태공간도 정수, 유한집합, 실수, 벡터 등으로 달라진다. 시간의 연속성과 상태값의 연속성은 별개이다. 연속시간 Poisson 과정은 정수값을 가지며 점프하고, 이산시간 Gaussian 시계열은 실수값을 가질 수 있다.

예제 1.2 (같은 주변분포, 다른 시간 구조) $Z \sim N(0,1)$이라 하고 모든 시간에 $X_n = Z$로 두자. 다른 과정 Y_n은 독립 표준정규 변수들로 구성한다. 각 시간의 주변분포는 같지만 X_n의 경로는 상수이고 Y_n의 경로는 계속 변한다. $\operatorname{Cov}(X_m, X_n) = 1$인 반면 서로 다른 시간의 Y 공분산은 0이다. 주변분포만으로 경로와 예측을 결정할 수 없다.

과정 전체를 함수공간의 확률변수로 보려면 함수공간의 사건 체계도 지정해야 한다. 연속경로의 공간, 오른쪽 연속이고 왼쪽 극한이 있는 경로의 공간 등은 서로 다르다. 이 장에서는 필요한 경로 조건을 직접 명시하고, 함수공간 위의 측도론 전체는 후속 이론으로 남긴다.

1.2 유한차원 분포와 일관성

정의 1.3 (유한차원 분포) 유한한 시점 $t_1, \dots, t_k$에서 벡터 $(X_{t_1}, \dots, X_{t_k})$의 분포를 과정의 **유한차원 분포**(*finite-dimensional distribution*)라 한다. 모든 유한 시점 선택에 대한 이 분포족은 각 좌표를 지우면 해당 주변분포가 되고, 순서를 바꾸면 좌표를 같은 순서로 바꾼 분포가 되어야 한다. 이 두 조건을 **일관성**(*consistency*)이라 한다.

표준 Borel 상태공간에서 이런 일관성을 갖는 유한차원 분포족은 어떤 곱 확률공간 위의 과정으로 실현할 수 있다는 **Kolmogorov 확장정리**가 있다. 이것은 존재 정리이며 여기서 증명하지 않는다. 중요한 제한은 이 정리만으로 원하는 연속경로가 자동으로 보장되지는 않는다는 것이다. 경로 정칙성은 별도 모멘트 조건이나 구성으로 확보한다.

예제 1.4 (독립 증분으로 유한차원 분포 만들기) $0 = t_0 < t_1 < \cdots < t_k$에서 서로 독립인 정규 증가량 $Z_j \sim N(0, t_j - t_{j-1})$를 정하고 $X_{t_j} = \sum_{i \le j} Z_i$로 둔다. 중간 시점을 지우면 연속된 정규 증가량들이 합쳐져 같은 분포족으로 돌아간다. 독립 정규 변수의 합이 정규이고 분산이 더해지기 때문이다. 이 구조가 Brownian 운동의 유한차원 분포를 결정한다. 연속 표본경로의 존재는 마지막 장에서 별도 입력으로 명시한다.

1.3 수정과 경로 전체의 일치

정의 1.5 (수정과 구별불가능성) 같은 확률공간 위의 두 과정이 모든 고정된 t에서 $\mathbb{P}(X_t = Y_t) = 1$이면 서로 **수정**(*modification*)이라고 한다. 하나의 확률 1 사건 위에서 모든 t에 대해 동시에 같으면 **구별불가능**(*indistinguishable*)하다고 한다. 경로 전체 일치 사건의 가측성이 성립하는 설정에서 이 용어를 사용한다.

가산 지표집합에서는 확률 1 사건의 가산 교집합으로 두 개념이 같다. 비가산 시간에서는 그렇지 않을 수 있다.

예제 1.6 (고정 시간에는 보이지 않는 점프) $U \sim \mathrm{Unif}(0,1)$이고 $t \in [0,1]$에 대해 $X_t = 0$, $Y_t = \mathbf{1}_{\{U = t\}}$라 하자. 고정된 t마다 $\mathbb{P}(Y_t = 0) = \mathbb{P}(U \neq t) = 1$이므로 서로 수정이고 모든 유한차원 분포도 같다. 하지만 각 경로는 $t = U$에서 다르므로 구별불가능하지 않다. Y의 경로는 연속이 아니며, 한 점의 돌출을 갖는다.

명제 1.7 (연속 수정들의 일치) $[0, \infty)$ 위의 두 과정이 수정이고 둘 다 거의 확실히 연속경로를 가지면 구별불가능하다.

증명. 음이 아닌 유리수 q마다 $X_q = Y_q$인 사건의 확률은 1이다. 유리수들이 가산이므로 모든 유리 시점에서 같고 두 경로가 모두 연속인 공통 사건 Ω_0의 확률도 1이다. $\omega \in \Omega_0$와 임의의 실수 시점 t에 대해 유리수열 $q_m \to t$를 택하면 $X_t(\omega) = \lim_m X_{q_m}(\omega) = \lim_m Y_{q_m}(\omega) = Y_t(\omega)$이다. 따라서 그 사건 위에서 모든 시점의 값이 같다. $\square$

1.4 정보의 증가와 적합성

정의 1.8 (여과와 적합성) 시간이 증가할수록 커지는 σ-대수족 $\{\mathcal{F}_t\}$을 **여과**(*filtration*)라고 한다. $s \le t$이면 $\mathcal{F}_s \subseteq \mathcal{F}_t$이다. 각 X_t가 $\mathcal{F}_t$-가측이면 과정은 이 여과에 **적합**하다고 한다. 적응한다고도 표현한다. **자연 여과**는 $\mathcal{F}_t^X = \sigma(X_s : s \le t)$이다.

여과는 시점 t까지 무엇을 알고 있는지 나타낸다. "미래를 보지 않는다"는 조건을 수학적으로 표현할 때 사용한다. 자연 여과보다 큰 여과를 사용하면 추가 정보가 들어갈 수 있으며, 독립성이나 마팅게일 성질이 유지되는지 다시 확인해야 한다.

정의 1.9 (독립 증분과 정상 증분) 서로 겹치지 않는 시간구간의 증가량들이 독립이면 **독립 증분**을 갖는다고 한다. $X_{t+h} - X_t$의 분포가 t와 무관하고 길이 h에만 의존하면 **정상 증분**을 갖는다고 한다.

정상 증분은 과정 자체가 정상이라는 뜻이 아니다. 예를 들어 Brownian 운동의 분산은 시간에 따라 증가하므로 과정은 정상이지 않지만 증가량의 분포는 구간 길이에만 의존한다. 현재보다 앞의 전체 정보와 미래 증가량의 독립성을 말할 때에는 사용하는 여과를 포함하여 가정한다.

1.5 엄격 정상성과 약정상성

정의 1.10 (엄격 정상과정과 약정상과정) 허용되는 모든 시간 이동 h와 모든 유한 시점들에 대해

$$(X_{t_1+h}, \dots, X_{t_k+h}) \overset{d}{=} (X_{t_1}, \dots, X_{t_k})$$

이면 **엄격 정상과정**(*strictly stationary process*)이라 한다. 모든 변수가 유한 이차 모멘트를 가지고 평균이 일정하며 공분산이 시차에만 의존하면 **약정상과정**(*weakly stationary process*)이라 한다.

실수값 이산시간 약정상과정에서는

$$\mathbb{E}X_n = \mu, \qquad \operatorname{Cov}(X_n, X_{n+h}) = \gamma(h)$$

로 쓴다. $\gamma(-h) = \gamma(h)$이고 $|\gamma(h)| \le \gamma(0)$이다. 또한 임의의 계수 a_j에 대해 $\sum_{j,k} a_j a_k \gamma(j-k) \ge 0$이어야 한다. 공분산 행렬의 양의 준정부호 조건이 모든 시간 선택에 적용된다.

성질의 근거. $\operatorname{Cov}(X_n, X_{n-h}) = \operatorname{Cov}(X_{n-h}, X_n) = \gamma(h)$이므로 $\gamma(-h) = \gamma(h)$이다. Cauchy–Schwarz로 $|\operatorname{Cov}(X_n, X_{n+h})| \le \sqrt{\operatorname{Var} X_n \operatorname{Var} X_{n+h}} = \gamma(0)$이다. 유한 합 $\sum_j a_j X_j$의 분산은 $\sum_{j,k} a_j a_k \operatorname{Cov}(X_j, X_k) = \sum_{j,k} a_j a_k \gamma(j-k)$이고 분산은 음이 아니다. □

엄격 정상성과 유한 이차 모멘트가 함께 있으면 약정상이다. 역방향은 일반적으로 거짓이지만, 공동 Gaussian 과정에서는 평균과 공분산이 모든 유한차원 분포를 결정하므로 약정상성이 엄격 정상성을 준다.

예제 1.11 (약정상이지만 엄격 정상이 아니다) 서로 독립인 X_n들을 짝수 시간에는 공정한 ± 1, 홀수 시간에는 표준정규로 정한다. 모두 평균 0, 분산 1이고 서로 다른 시점의 공분산은 0이다. 따라서 약정상이지만 한 시점 이동이 주변분포를 바꾸므로 엄격 정상이 아니다. 약정상 조건이

오직 첫 두 모멘트만 살핀다는 한계를 보여 준다.

1.6 연습문제와 해설

연습문제 1.12 $X_t = tZ$, $Z \sim N(0,1)$, $t \geq 0$의 평균과 분산을 구하고 정상성을 판단하라.

풀이. 평균은 0, 공분산은 $\operatorname{Cov}(X_s, X_t) = st$이다. 분산이 t^2로 변하므로 약정상도 엄격 정상도 아니다. 증분 $(t+h)Z - tZ = hZ$의 분포는 길이에만 의존하므로 정상 증분이지만 서로 다른 구간 증가량들은 독립이 아니다.

연습문제 1.13 독립 동일분포 과정은 왜 엄격 정상인가?

풀이. 서로 다른 시점들의 결합분포는 동일한 주변분포의 곱이다. 시점을 함께 이동해도 같은 곱이 된다. 중복 시점이 있는 벡터에서도 좌표의 동일성 구조가 보존되므로 결론이 같다.

연습문제 1.14 X_t의 분포가 모든 t에서 같으면 엄격 정상인가?

풀이. 그렇지 않다. Z, W가 독립 공정 부호이고 $(X_0, X_1, X_2) = (Z, Z, W)$이면 주변분포는 같지만 (X_0, X_1)은 항상 같은 값이고 (X_1, X_2)는 독립이다. 시간 이동이 이차원 분포를 바꾼다.

연습문제 1.15 두 연속 과정이 모든 유리 시점에서 거의 확실히 같을 때 실수 시점 전체에서도 동시에 같다고 할 수 있는 이유를 설명하라.

풀이. 유리 시점에서의 확률 1 사건들을 가산 교집합하고 연속성을 적용한다(명제 1.7). 비가산 교집합만으로 결론을 얻는 것이 아니라 가산 조밀집합과 경로의 정칙성을 함께 사용한다.

다음 연결. 시간에 따른 의존성을 특별한 조건으로 단순화한 모형이 Markov 연쇄이다. 다음 장은 현재 상태가 다음 상태 예측에 충분하다는 조건을 유한 상태 행렬로 표현한다(제21권 제2장).

제 2 장

이산시간 Markov 연쇄와 정상분포

개요 이산시간 Markov 연쇄는 현재 상태가 주어지면 다음 상태의 조건부 분포가 과거 전체와 무관한 상태공간 위의 과정이며, 전이행렬과 초기분포로 유한차원 분포가 완전히 정해진다. 이 장은 Markov 성질과 전이행렬, Chapman–Kolmogorov 관계, 소통류와 주기, 정상분포의 정의와 존재, 상세평형과 가역성, 장기 방문비율을 다룬다. 정상분포를 구하는 계산(선형방정식)과 그것이 장기 거동을 설명하는 조건(기약성, 비주기성)을 구별하는 것이 요점이다. 선행 지식: 조건부 확률, 행렬곱, 유한합, 정상과정(제21권 제1장). 이 장은 별도 언급이 없으면 유한한 상태공간과 시간에 따라 변하지 않는 전이확률을 사용한다.

2.1 Markov 성질과 전이행렬

정의 2.1 (시간동질 Markov 연쇄) 상태공간 S의 과정 $X_0, X_1, \dots$가 자신의 자연 여과 $\mathcal{F}_n = \sigma(X_0, \dots, X_n)$에 대해

$$\mathbb{P}(X_{n+1} = j \mid \mathcal{F}_n) = p_{X_n j}$$

를 만족하면 **시간동질 Markov 연쇄**(*time-homogeneous Markov chain*)라 한다. **전이행렬** $P = (p_{ij})$는 $p_{ij} \ge 0$, $\sum_{j} p_{ij} = 1$을 만족한다. 초기분포를 행벡터 π_0로 나타낸다.

현재 상태를 알면 과거 전체가 다음 단계의 조건부 확률에 추가 정보를 주지 않는다는 뜻이다. 과거와 미래가 무조건 독립이라는 뜻은 아니다. 또한 시간동질성은 전이 규칙이 시간에 따라 바뀌지 않는다는 성질이며, 초기분포까지 정상이라는 뜻이 아니다. 경로의 확률은 연쇄법칙으로

$$\mathbb{P}(X_0 = i_0, \dots, X_n = i_n) = \pi_0(i_0) \prod_{k=0}^{n-1} p_{i_k i_{k+1}} \tag{2.1}$$

이다. 따라서 초기분포와 전이행렬을 모두 알아야 과정의 유한차원 분포가 정해진다. 상태 i에서 시작할 때의 확률과 기댓값은 $\mathbb{P}_i$, $\mathbb{E}_i$로 쓴다.

예제 2.2 (두 상태의 전이)

$$P = \begin{pmatrix} 0.8 & 0.2 \\ 0.3 & 0.7 \end{pmatrix}, \qquad \pi_0 = (1, 0)$$

이면 첫 단계 분포는 $(0.8, 0.2)$이다. 경로 $0 \to 1 \to 0$의 확률은 $0.2 \cdot 0.3 = 0.06$이다. 두 단계 뒤 0일 확률은 $0.8^2 + 0.2 \cdot 0.3 = 0.70$이다. 한 경로의 확률과 그 종착점에 도달하는 모든 경로의 확률을 구별한다.

2.2 여러 단계 전이와 행렬곱

정리 2.3 (Chapman–Kolmogorov 관계) n단계 전이확률은 $(P^n)_{ij}$이며, 모든 음이 아닌 정수 m, n에 대해

$$P^{m+n} = P^m P^n, \qquad \pi_n = \pi_0 P^n.$$

증명. 중간 시점 m의 상태로 사건을 분할하면

$$\mathbb{P}_i(X_{m+n} = j) = \sum_{k} \mathbb{P}_i(X_m = k)\mathbb{P}_k(X_n = j).$$

반복된 Markov 성질과 시간동질성이 두 번째 인자가 과거와 m에 의존하지 않도록 한다. 이것이 행렬곱의 성분식이다. 한 단계에서 출발하여 귀납하면 P^n 표현을 얻는다. $\square$

상태마다의 기대 보상 $f(i)$를 열벡터로 쓰면 $\mathbb{E}_i f(X_n) = (P^n f)(i)$이다. 확률분포는 왼쪽에서 행벡터로, 함수는 오른쪽에서 열벡터로 곱하는 규약을 유지하면 전치 오류를 줄일 수 있다.

2.3 소통, 닫힌 클래스, 주기

i에서 j로 어떤 유한 단계에 양의 확률로 갈 수 있으면 $i \to j$라고 한다. 서로 도달 가능하면 같은 **소통류**에 속한다. 모든 상태가 한 소통류에 있으면 **기약**(*irreducible*)이다. 밖으로 나가는 전이가 없는 상태집합을 **닫혔다**고 한다. 한 상태 i의 **주기**는

$$d(i) = \gcd\{n \ge 1 : (P^n)_{ii} > 0\}$$

로 정의하며, 반환 가능한 상태에서 사용한다. 기약 연쇄에서는 모든 상태의 주기가 같다. 주기가 1이면 **비주기적**이다. 자기고리 $p_{ii} > 0$는 그 상태의 주기가 1인 충분조건이다.

예제 2.4 (항상 번갈아 바뀌는 연쇄) $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$는 기약이지만 주기는 2이다. 0에서 시작하면 짝수 시간에 0, 홀수 시간에 1이다. 정상분포는 존재하지만 특정 초기상태의 분포는 하나의 극한으로 수렴하지 않는다.

2.4 정상분포와 정상과정

정의 2.5 (정상분포) 비음수 행벡터 π가 $\sum_i \pi_i = 1$, $\pi P = \pi$를 만족하면 **정상분포**(*stationary distribution*)라 한다. 다른 문헌에서는 불변분포라고도 한다.

π로 시작하면 모든 시점의 주변분포가 π이다. 실제로 $\pi_n = \pi P^n = \pi$이다. 또한 경로확률 공식 (2.1)에서 $\mathbb{P}(X_h = i_0, \dots, X_{h+n} = i_n) = \pi(i_0)\prod_{k} p_{i_k i_{k+1}}$이 h에 의존하지 않으므로 모든 유한차원 분포도 시간 이동에 불변이다. 따라서 정상과정이 된다. 정상분포를 구했다는 사실만으로 임의의 초기분포가 그 분포로 수렴한다고 결론낼 수는 없다.

예제 2.6 (두 상태의 평형과 접근) 앞의 $0.8, 0.2; 0.3, 0.7$ 전이행렬에서 $\pi = (u, 1-u)$로 놓으면

$u = 0.8u + 0.3(1-u)$이므로 $u = 0.6$이다. 따라서 $\pi = (0.6, 0.4)$이다. $u_n = \mathbb{P}(X_n = 0)$는

$$u_{n+1} = 0.3 + 0.5u_n, \qquad u_n = 0.6 + (u_0 - 0.6)\,0.5^n$$

이다. 이 예에서는 모든 초기분포가 정상분포로 기하급수적으로 접근한다. $u_0 = 1$이면 두 단계 확률은 0.7로 직접 계산과 일치한다.

정리 2.7 (유한 상태 연쇄의 기본 구조) 유한 상태 전이행렬에는 적어도 하나의 정상분포가 존재한다. 기약이면 정상분포는 유일하며 모든 성분이 양수이다. 기약이고 비주기적이면 모든 초기분포에 대해 $\pi_0 P^n \to \pi$이다. 기약이지만 주기적이면 점별 분포수렴은 실패할 수 있으나 시간평균 분포는 정상분포로 수렴한다.

존재는 확률단체의 콤팩트성으로 직접 볼 수 있다. $\nu_N = N^{-1}\sum_{k=0}^{N-1} \pi_0 P^k$라 하면 부분수열의 극한 π가 있고

$$\nu_N P - \nu_N = \frac{\pi_0 P^N - \pi_0}{N} \longrightarrow 0$$

이므로 $\pi P = \pi$다. 극한 π는 확률단체(닫힌 집합)에 속하므로 정상분포이다. 유일성과 비주기 수렴은 유한 Markov 연쇄의 기본 정리로 사용한다. 모든 세부 증명을 제공하는 것은 아니며, 조건이 왜 필요한지는 앞의 주기 예와 닫힌 클래스 예로 확인한다.

예제 2.8 (정상분포의 비유일성) P가 2×2 단위행렬이면 두 상태가 각각 흡수상태이다. 모든 확률벡터 $(u, 1-u)$가 정상분포이고 초기분포가 영원히 유지된다. 유한 상태라는 조건만으로 정상분포의 유일성을 얻을 수 없다.

2.5 상세평형과 가역성

명제 2.9 (상세평형) 확률벡터 π가 모든 i, j에서

$$\pi_i p_{ij} = \pi_j p_{ji}$$

를 만족하면 정상분포이다. 이를 **상세평형** 조건이라 한다.

증명. j를 고정하고 i에 대해 합하면 $\sum_i \pi_i p_{ij} = \pi_j \sum_i p_{ji} = \pi_j$이다. 마지막 합은 행 j의 합이므로 1이다. □

상세평형을 만족하는 정상 연쇄는 시간 방향을 뒤집어도 같은 경로확률을 갖는 **가역** 연쇄다. 정상성이 모든 상태에 들어오고 나가는 총량의 균형이라면 상세평형은 각 상태쌍 사이의 균형이다. 정상성보다 강한 조건이다.

예제 2.10 (가역이 아닌 정상 연쇄) 세 상태를 $0 \to 1 \to 2 \to 0$으로 확률 1로 순환하면 균등분포가 정상이다. 그러나 $\pi_0 p_{01} = 1/3$, $\pi_1 p_{10} = 0$이므로 상세평형은 실패한다. 정상분포를 구하기 위해 항상 상세평형 방정식을 풀 수 있는 것은 아니다.

2.6 장기 방문비율과 분포수렴

유한 기약 연쇄에서는 초기상태와 무관하게 각 상태 j의 방문비율이

$$\frac{1}{n}\sum_{k=0}^{n-1}\mathbf{1}_{\{X_k=j\}} \longrightarrow \pi_j \qquad \text{거의 확실히}$$

수렴한다. 이 경로별 에르고딕 결론에는 비주기성이 필요 없다. 번갈아 움직이는 두 상태 연쇄도 방문비율은 각각 $1/2$로 수렴한다. 한 시점의 분포수렴과 긴 경로의 시간평균은 다른 질문이다. 이 정리의 증명은 반환시간과 재생 구조를 사용하는 후속 이론으로 남긴다.

2.7 연습문제와 해설

연습문제 2.11 $P=\begin{pmatrix}0.9 & 0.1\\ 0.4 & 0.6\end{pmatrix}$의 정상분포를 구하라.

풀이. $0.1\pi_0=0.4\pi_1$, $\pi_0+\pi_1=1$에서 $(0.8,0.2)$이다. 두 방향 전이가 양수이고 자기고리가 있으므로 기약 비주기적이며 모든 초기분포가 이 정상분포로 수렴한다.

연습문제 2.12 초기분포 $\pi_0=(0,1)$과 앞 문제의 전이행렬에서 두 단계 뒤 분포를 구하라.

풀이. 한 단계는 $(0.4,0.6)$이며 두 단계는 $(0.4\cdot0.9+0.6\cdot0.4,\ 0.4\cdot0.1+0.6\cdot0.6)=(0.6,0.4)$이다.

연습문제 2.13 $\pi P=\pi$를 만족하는 벡터가 $(2,1)$이면 정상분포인가?

풀이. 그 자체는 합이 1이 아니므로 확률분포가 아니다. 성분이 비음수이고 합이 양수이면 정규화한 $(2/3,1/3)$이 정상분포다. 고유벡터 방정식과 확률 정규화를 모두 확인한다. 예를 들어 $P=\begin{pmatrix}1/2 & 1/2\\ 1 & 0\end{pmatrix}$에서 $(2/3,1/3)P=(1/3+1/3,\ 1/3)=(2/3,1/3)$이다.

연습문제 2.14 두 상태 번갈이 연쇄의 P^n과 초기상태 0에서의 방문비율을 설명하라.

풀이. 짝수 거듭제곱은 단위행렬, 홀수 거듭제곱은 P다. 분포는 교대로 바뀌지만 각 상태 방문 횟수의 차이는 최대 1이므로 방문비율은 $1/2$로 수렴한다.

다음 연결. 정상분포가 장기 균형을 설명한다면 도달시간은 특정 상태에 처음 닿기까지의 경로를 설명한다. 다음 장은 첫 단계 분해와 흡수 연쇄의 기본행렬로 이를 계산한다(제21권 제3장).

제 3 장

흡수, 도달시간, 기본행렬

개요 도달시간(*hitting time*)은 Markov 연쇄가 주어진 상태집합에 처음 들어가는 시각이고, 흡수(*absorption*)는 한 번 들어가면 영원히 머무는 상태에 도달하는 사건이다. 이 장은 도달시간과 첫 귀환시간을 정의하고, 첫 단계 분해로 도달확률과 평균 도달시간이 만족하는 연립일차방정식을 세운다. 유한 상태에서 평균 도달시간이 유한함을 증명하고, 흡수 연쇄의 표준 블록 형태에서 기본행렬 $N = (I - Q)^{-1}$이 방문 횟수의 기댓값이라는 사실, 평균 흡수시간 $m = N\mathbf{1}$과 흡수확률 $B = NR$을 유도한다. 이어서 도박사의 파산 문제를 풀고, 확률 1로 끝나도 평균 시간이 무한할 수 있음을 보인다. 선행 지식: Markov 성질, 연립일차방정식, 비음수 확률변수의 기댓값(제21권 제2장). 도달이 확실한지와 평균 도달시간이 유한한지는 서로 다른 문제이므로 따로 확인한다.

3.1 처음 도달하는 시간

정의 3.1 (도달시간과 첫 귀환시간) 상태공간이 S인 Markov 연쇄 $(X_n)_{n\ge 0}$와 상태집합 $A \subseteq S$에 대하여

$$\tau_A = \inf\{n \ge 0 : \ X_n \in A\} \tag{3.1}$$

를 A의 **도달시간**이라 한다. 한 번도 도달하지 않으면 $\inf \varnothing = \infty$로 둔다. 초기 상태가 이미 A에 속하면 $\tau_A = 0$이다. 상태 i로의 **첫 귀환시간**(*first return time*)은 $T_i^{+} = \inf\{n \ge 1 : \ X_n = i\}$이며, 시작 시점의 방문은 제외한다.

도달시간은 표본경로의 함수이다. 사건 $\{\tau_A \le n\}$은 $X_0, \dots, X_n$만으로 판단할 수 있어서 미래를 볼 필요가 없다. 이런 성질은 뒤에서 정지시간(*stopping time*) 개념으로 일반화된다(제21권 제5장). 도달시간의 값이 ∞일 수 있으므로 확률과 기댓값의 식을 쓸 때 이 경우를 버리지 않는다. 이후 $\mathbb{P}_i$, $\mathbb{E}_i$는 $X_0 = i$ 조건에서의 확률과 기댓값을 뜻한다.

예제 3.2 (초기 방문과 첫 귀환) 두 상태 $\{0, 1\}$의 전이행렬이

$$P = \begin{pmatrix} 0.8 & 0.2 \\ 0.3 & 0.7 \end{pmatrix}$$

이라 하자. 0에서 시작하면 $\tau_{\{0\}} = 0$이다. 반면 첫 귀환시간 T_0^{+}는 다음 단계가 0이면 1이고, 다음 단계가 1이면 그 이후 0에 돌아올 때까지 기다린 시간을 더한 값이다. 1에서 0까지의 평균 시간은 성공확률 0.3인 기하분포의 평균 $1/0.3$이므로

$$\mathbb{E}_0 T_0^{+} = 1 + 0.2 \cdot \frac{1}{0.3} = \frac{5}{3}$$

이다. 정상분포는 $\pi_0 \cdot 0.2 = \pi_1 \cdot 0.3$과 $\pi_0 + \pi_1 = 1$에서 $\pi_0 = 0.6$, $\pi_1 = 0.4$이고, $5/3 = 1/\pi_0$이다. 이는 유한 기약 연쇄의 일반적인 평균 귀환시간 공식 $\mathbb{E}_i T_i^{+} = 1/\pi_i$의 한 예이다.

3.2 첫 단계 분해

서로 겹치지 않는 목표집합 $A, B \subseteq S$에 대하여 $h_i = \mathbb{P}_i(\tau_A < \tau_B)$라 하자. A에서는 $h = 1$, B에서는 $h = 0$이며 그 밖의 상태 i에서는

$$h_i = \sum_{j} p_{ij} h_j \tag{3.2}$$

이다. 첫 단계 상태를 조건으로 나누면 원래와 같은 문제를 새로운 상태에서 다시 시작하기 때문에 성립한다. $A \cup B$에 끝내 도달하지 않을 수 있는 닫힌 클래스가 있으면, 경계값과 조화방정식 (3.2)만으로 해가 유일하지 않을 수 있다. 확률로 정의한 h는 적절한 비음수 해들 가운데 최소해로 특징지을 수 있다.

예제 3.3 (조화방정식의 해가 유일하지 않은 경우) 상태 $\{a, b, i, c\}$에서 $A = \{a\}$, $B = \{b\}$, 상태 i는 확률 $1/2$로 a로, 확률 $1/2$로 c로 가고 c는 흡수상태라 하자. 그러면 $h_a = 1$, $h_b = 0$이고 방정식은 $h_i = \tfrac{1}{2}\cdot 1 + \tfrac{1}{2} h_c$, $h_c = h_c$이다. 둘째 식은 항등식이므로 h_c가 임의의 값을 가지는 해가 모두 방정식을 만족한다. 실제 확률은 c에서 A에 도달할 수 없으므로 $h_c = 0$, $h_i = 1/2$이며 이것이 비음수 해 가운데 최소이다.

단일 목표 A의 평균 도달시간 $m_i = \mathbb{E}_i \tau_A$는 $i \in A$에서 0이고, 나머지에서는 무한대를 허용하여

$$m_i = 1 + \sum_{j \notin A} p_{ij} m_j \tag{3.3}$$

를 만족한다. 이 식도 비음수 최소해로 특징지어진다. 유한한 해를 구했다고 바로 모든 무한 상태 문제의 평균이라고 판단하지 않는다. 비음수 최소해라는 조건과 적절한 경계 또는 적분가능성 조건이 필요할 수 있다.

명제 3.4 (유한 상태에서의 유한 도달 평균) 유한 상태공간에서 모든 $i \notin A$로부터 A에 이르는 양의 확률 경로가 존재하면 τ_A는 거의 확실히 유한하고 모든 $\mathbb{E}_i \tau_A$도 유한하다.

증명. 각 상태 $i \notin A$에서 A에 이르는 양의 확률 경로를 하나씩 고른다. 상태 수가 유한하므로 경로 길이의 최댓값 $r < \infty$와 선택한 경로 확률의 최솟값 $\varepsilon > 0$이 있다. 어느 상태에서 시작해도 (이미 A에 있으면 자명하게) 다음 r단계 안에 A에 도달할 확률은 적어도 ε이다. Markov 성질을 시각 $r, 2r, \dots$에 적용하면

$$\mathbb{P}_i(\tau_A > kr) \le (1-\varepsilon)^k$$

이다. 따라서 $\mathbb{P}_i(\tau_A = \infty) \le \lim_{k} (1-\varepsilon)^k = 0$이어서 거의 확실히 도달하고,

$$\mathbb{E}_i \tau_A = \sum_{n \ge 0} \mathbb{P}_i(\tau_A > n) \le r \sum_{k \ge 0} \mathbb{P}_i(\tau_A > kr) \le r \sum_{k \ge 0} (1-\varepsilon)^k = \frac{r}{\varepsilon}$$

이다. 둘째 부등식은 $kr \le n < (k+1)r$인 r개의 n마다 $\mathbb{P}_i(\tau_A > n) \le \mathbb{P}_i(\tau_A > kr)$임을 썼다. $\square$

3.3 흡수 연쇄의 표준 블록 형태

흡수상태(*absorbing state*)는 한 번 들어가면 영원히 머무는 상태, 곧 $p_{ii} = 1$인 상태이다. 유한 상태공간에 흡수상태가 있고 모든 나머지 상태에서 흡수상태 집합에 도달할 경로가 있다고 가정

한다. 이런 연쇄를 **흡수 연쇄**(*absorbing chain*)라 한다. 상태 순서를 비흡수상태 먼저 배치하면

$$P = \begin{pmatrix} Q & R \\ 0 & I \end{pmatrix} \tag{3.4}$$

이다. Q는 비흡수상태 사이 전이이며 행합이 1 이하인 부분확률행렬이다. R은 비흡수상태에서 흡수상태로의 전이이다. 단순히 행합이 1 이하라는 사실만으로 $I-Q$가 가역인 것은 아니다. $Q=I$가 반례이다. 여기서는 유한성과 모든 상태의 흡수 도달 조건을 사용한다.

정리 3.5 (기본행렬) 위 조건에서 $Q^n \to 0$이고

$$N = \sum_{n=0}^{\infty} Q^n = (I-Q)^{-1} \tag{3.5}$$

가 존재한다. 성분 N_{ij}는 i에서 시작하여 흡수 전까지 비흡수상태 j를 방문하는 총횟수의 기댓값이다. 초기 시점 $n=0$의 방문도 포함한다. N을 **기본행렬**(*fundamental matrix*)이라 한다.

증명. $(Q^n)_{ij}$는 아직 흡수되지 않고 시간 n에 j일 확률이다. 앞 명제(명제 3.4)의 기하급수 꼬리 상계 $\mathbb{P}_i(\tau > n) \le C\rho^n (\rho<1)$로 급수가 성분별로 수렴하며 $Q^n \to 0$이다. 유한 부분합에 대해

$$(I-Q)\sum_{n=0}^{m} Q^n = I - Q^{m+1}$$

이고 반대 곱도 같으므로 $m\to\infty$의 극한에서 $(I-Q)N = N(I-Q) = I$, 곧 $I-Q$가 가역이고 역행렬이 N이다. 기대 방문횟수는 $\sum_{n\ge 0} \mathbf{1}_{\{X_n=j,\, n<\tau_A\}}$의 기댓값이다($A$는 흡수상태 집합). 비음수 항의 합과 기댓값을 교환하면 $\sum_n (Q^n)_{ij} = N_{ij}$이다. $\square$

평균 흡수시간 벡터와 흡수상태별 확률행렬은

$$m = N\mathbf{1}, \qquad B = NR \tag{3.6}$$

이다. 여기서 $m_i = \mathbb{E}_i \tau_A$, B_{ik}는 i에서 시작해 흡수상태 k에서 흡수될 확률이다. $m = N\mathbf{1}$은 흡수 전 방문 횟수를 모든 비흡수상태에 대해 더한 것이고, 첫 단계 식 (3.3)에서 $(I-Q)m = \mathbf{1}$을 얻는 것과 같다. 각 시점의 흡수 직전 상태에서 마지막 전이를 하는 경우들을 합하면 $B_{ik} = \sum_{n}\sum_{j} (Q^n)_{ij} R_{jk} = \sum_j N_{ij} R_{jk}$이다. 첫 단계 식으로도 $B = R + QB$이므로 $(I-Q)B = R$이다. 검산으로, $R\mathbf{1} = \mathbf{1} - Q\mathbf{1}$이므로 $B\mathbf{1} = N(I-Q)\mathbf{1} = \mathbf{1}$이고 B의 행합은 1이다. 곧 거의 확실히 흡수된다.

예제 3.6 (두 비흡수상태와 두 흡수상태) 상태 순서를 $1, 2, A, B$라 하고

$$P = \begin{pmatrix} 1/2 & 1/4 & 1/4 & 0 \\ 1/5 & 3/10 & 1/10 & 2/5 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

로 두자. 두 비흡수상태에서 흡수상태로 갈 수 있으며 $Q = \begin{pmatrix} 1/2 & 1/4 \\ 1/5 & 3/10 \end{pmatrix}$, $I-Q$의 행렬식은

$\frac{1}{2}\cdot\frac{7}{10}-\frac{1}{4}\cdot\frac{1}{5}=\frac{3}{10}$이므로

$$N=\begin{pmatrix}7/3 & 5/6\\ 2/3 & 5/3\end{pmatrix},\qquad m=\begin{pmatrix}19/6\\ 7/3\end{pmatrix},\qquad B=\begin{pmatrix}2/3 & 1/3\\ 1/3 & 2/3\end{pmatrix}$$

이다. 상태 1에서 시작하면 평균 약 3.16667단계 뒤 흡수되고 A로 흡수될 확률은 $2/3$이다. N의 행합은 평균 단계 수이고 B의 행합은 1이다. 서로 다른 의미의 행렬을 같은 확률행렬로 오해하지 않는다.

3.4 도박사의 파산 문제

상태 $0,1,\dots,M$에서 $0,M$은 흡수하고 내부에서 확률 p로 한 칸 증가, $q=1-p$로 한 칸 감소한다고 하자. $0<p<1$이다. h_i를 M에 먼저 도달할 확률이라 하면

$$h_0=0,\qquad h_M=1,\qquad h_i=p\,h_{i+1}+q\,h_{i-1} \tag{3.7}$$

이다. 점화식의 특성방정식은 $pr^2-r+q=0$이고 근은 1과 $r=q/p$이다. $p\neq q$에서는 $r=q/p$로 두 해가 $A+Br^i$임을 확인할 수 있고, 경계조건으로

$$h_i=\frac{1-r^i}{1-r^M} \tag{3.8}$$

이다. $p=q=1/2$에서는 재귀식이 $h_{i+1}-h_i=h_i-h_{i-1}$이므로

$$h_i=\frac{i}{M}$$

이다. 분모 $1-r^M$이 0인 대칭 경우를 별도로 처리해야 한다. 식 (3.8)에서 $r\to 1$의 극한을 취하면 $(1-r^i)/(1-r^M)\to i/M$이므로 두 경우는 연속적으로 이어진다.

대칭 경우의 평균 흡수시간은 $m_0=m_M=0$과 $m_i=1+(m_{i-1}+m_{i+1})/2$를 만족한다. $m_i=i(M-i)$를 대입하면 재귀식과 경계값을 모두 만족한다. 실제로 $1+\frac{1}{2}\big[(i-1)(M-i+1)+(i+1)(M-i-1)\big]=1+i(M-i)-1=i(M-i)$이다. 따라서

$$\mathbb{E}_i\tau_{\{0,M\}}=i(M-i). \tag{3.9}$$

유한 상태 흡수 문제에서 유일한 유한 해이므로 이 값이 평균이다.

참고 (비대칭 경우의 평균 시간). $p\neq q$이면 $m_i=\dfrac{i-M h_i}{q-p}$이다. $i/(q-p)$가 비동차식 $m_i=1+p m_{i+1}+q m_{i-1}$의 특수해이고 h_i가 동차식의 해이며 $m_0=m_M=0$이 되도록 h의 계수를 정한 것이다. 예를 들어 $p=2/3$, $M=3$, $i=1$이면 $h_1=4/7$이고 $m_1=(1-12/7)/(-1/3)=15/7$이다.

예제 3.7 공정한 보행에서 $M=10$, 시작 $i=3$이면 위쪽 경계에 먼저 도달할 확률은 0.3이고 평균 종료시간은 $3\cdot 7=21$단계이다. 종료 후 자산의 평균은 $10(0.3)=3$으로 처음 자산과 같지만, 종료시간은 일정하지 않다.

3.5 거의 확실한 도달과 무한 평균

유한 상태 조건을 빼면 확률 1로 끝나도 평균 시간이 무한할 수 있다. 정수축의 공정한 단순 무작위보행이 0에서 시작하여 1에 처음 도달하는 시간은 거의 확실히 유한하지만 기댓값은 무한하다. 뒤의 마팅게일 장에서 유계 정지시간 결과만으로 잘못 기댓값을 교환할 수 없는 반례로 사용한다(예제 5.14).

거의 확실한 도달은 유한 구간 $[-m, 1]$의 파산 확률에서 확인할 수 있다. 0에서 1을 먼저 칠 확률은 $m/(m+1)$이며 이 사건은 무한축에서도 언젠가 1을 치는 사건에 포함된다. $m \to \infty$로 보내면 도달확률이 1이다. 평균이 무한하다는 사실은 마팅게일 장의 선택정리 조건과 연결하여 별도로 증명한다.

흔한 오류 (도달 확실성과 평균의 유한성). $\mathbb{P}_i(\tau_A < \infty) = 1$이라고 해서 $\mathbb{E}_i \tau_A < \infty$는 아니다. 앞의 단순 무작위보행이 그 반례이다. 또한 식 (3.3)의 유한한 해가 존재해도 그것이 평균 도달시간이라는 보장은 없고, 평균 도달시간은 비음수 최소해이다.

3.6 연습문제와 해설

> **연습문제 3.8** 비흡수상태 하나에서 확률 $r \in [0, 1)$로 머물고 나머지 확률로 흡수된다. 기본행렬과 평균 흡수시간을 구하라.

풀이. $Q = (r)$이므로 $N = (1-r)^{-1}$이다. 초기 비흡수상태 방문을 포함한 기대 방문횟수와 흡수까지의 단계 수가 모두 $1/(1-r)$이다. $r = 1$이면 흡수되지 않으므로 가정에서 제외한다.

> **연습문제 3.9** 공정한 파산 문제에서 $M = 8$, 시작 $i = 2$의 위쪽 흡수확률과 평균 시간을 구하라.

풀이. 확률은 $2/8 = 1/4$, 평균은 $2(8-2) = 12$단계이다.

> **연습문제 3.10** $p = 2/3$, $q = 1/3$, $M = 3$, 시작 $i = 1$일 때 위쪽 흡수확률을 구하라.

풀이. $r = 1/2$이므로 $(1-1/2)/(1-1/8) = 4/7$이다. 공정한 경우의 $1/3$보다 크며 위쪽 이동확률이 더 크다는 방향과 일치한다.

> **연습문제 3.11** 흡수 기본행렬에서 N_{ii}를 초기 방문을 제외한 횟수로 바꾸려면 어떻게 하는가?

풀이. 행렬 전체에서 단위행렬을 빼면 된다. $n = 0$의 전이행렬이 I이므로 $N - I = \sum_{n \ge 1} Q^n$이다.

다음 연결. 이산시간에서는 도달까지 단계 수를 센다. 연속시간의 사건 도착에서는 대기시간 자체가 확률변수이며, 가장 기본적인 독립 도착 모형이 Poisson 과정이다(제21권 제4장).

제 4 장

Poisson 과정과 지수 대기시간

개요 Poisson 과정(*Poisson process*)은 시간축 위에 사건이 하나씩, 서로 독립적으로, 일정한 평균 속도로 도착하는 현상을 모형화한 계수과정이다. 이 장은 동질 Poisson 과정을 독립 증분과 Poisson 분포 증분으로 정의하고, 평균·분산·공분산, 첫 도착과 k 번째 도착 시간의 분포(지수분포와 감마분포), 독립 과정의 중첩과 속아내기, 도착 총개수가 주어졌을 때 도착 시각의 균등 순서통계량 표현, 시간에 따라 변하는 발생률의 확장을 다룬다. 선행 지식: Poisson·지수·감마분포, 독립 증분, 조건부 확률(제20권 제6장). 발생률(*rate*)의 시간 단위를 명시한다.

4.1 계수과정의 정의

정의 4.1 (동질 Poisson 과정) 발생률 $\lambda > 0$인 **동질 Poisson 과정** $\{N_t : t \ge 0\}$은 $N_0 = 0$이고, 증분이 서로 독립이며

$$N_{t+h} - N_t \sim \mathrm{Pois}(\lambda h), \qquad t, h \ge 0 \tag{4.1}$$

인 계수과정이다. 여기서 "증분이 서로 독립"은 서로 겹치지 않는 구간 $(t_0, t_1], (t_1, t_2], \dots$ 의 증분들이 상호 독립이라는 뜻이다. 표준적인 버전은 오른쪽 연속이고 비감소하며 크기 1의 점프를 갖는다.

짧은 구간 길이 h에 대해

$$\mathbb{P}(N_{t+h} - N_t = 1) = \lambda h + o(h), \qquad \mathbb{P}(N_{t+h} - N_t \ge 2) = o(h) \tag{4.2}$$

이고 사건이 없을 확률은 $1 - \lambda h + o(h)$이다. 이 국소 관계는 정의의 Poisson 분포에서 전개할 수 있다. 실제로 $\mathbb{P}(N_{t+h} - N_t = 1) = \lambda h e^{-\lambda h} = \lambda h - \lambda^2 h^2 + \cdots$ 이고 $\mathbb{P}(N_{t+h} - N_t \ge 2) \le (\lambda h)^2/2$이다. 역방향으로 이 성질들에서 과정을 도출하려면 독립성·동질성·적절한 정칙성까지 함께 가정해야 한다.

예제 4.2 (단위의 변경) 분당 평균 도착률이 $\lambda = 2$이면 30초 동안의 평균 사건 수는 1이고, 한 번도 도착하지 않을 확률은 e^{-1}이다. 시간 단위를 시간으로 바꾸면 발생률은 120이 된다. 숫자 2를 단위 없이 시간당 발생률로 다시 쓰면 다른 모형이다.

4.2 평균, 공분산, 정상 증분

각 t에서

$$\mathbb{E}N_t = \lambda t, \qquad \mathrm{Var}(N_t) = \lambda t \tag{4.3}$$

이다. $s \le t$이면 $N_t = N_s + (N_t - N_s)$이고 두 항이 독립이므로

$$\mathrm{Cov}(N_s, N_t) = \mathrm{Var}(N_s) = \lambda s, \qquad \mathrm{Cov}(N_s, N_t) = \lambda \min(s, t)$$

이다. 평균과 분산이 시간에 따라 변하므로 과정 자체는 정상이 아니다. 정상인 것은 같은 길이 구간의 증가량 분포이다(정상 증분). 서로 겹치는 구간의 사건 수는 일반적으로 독립이 아니다. 겹친 부분의 사건들을 공유하기 때문이다.

> **예제 4.3** $A = N_3 - N_1$, $B = N_4 - N_2$ 이면 두 길이는 모두 2 지만 구간 $(2,3]$ 이 겹친다. 겹치지 않는 세 부분 $(1,2], (2,3], (3,4]$ 로 나누면 $A = X_1 + X_2$, $B = X_2 + X_3$ 이고 $\operatorname{Cov}(A,B) = \operatorname{Var}(X_2) = \lambda$ 이다. “증분들이 독립”이라는 정의는 서로 겹치지 않는 시간 구간에 적용된다.

4.3 첫 도착과 연속 도착 사이의 시간

첫 도착시간 $T_1 = \inf\{t : N_t \geq 1\}$ 에 대해

$$\mathbb{P}(T_1 > t) = \mathbb{P}(N_t = 0) = e^{-\lambda t}$$

이므로 $T_1 \sim \operatorname{Exp}(\lambda)$ 이다. 지수분포는 무기억성 $\mathbb{P}(T_1 > s+t \mid T_1 > s) = e^{-\lambda t}$ 를 가지며, 이것이 독립 증분 성질의 다른 표현이다. 표준 Poisson 과정은 독립인 지수 대기시간 $W_1, W_2, \dots$ 를 더하여 도착시간 $T_k = W_1 + \cdots + W_k$ 로 구성할 수 있다. 이 구성에서 $T_0 = 0$ 으로 두면

$$N_t = \max\{k \geq 0 : \ T_k \leq t\} \tag{4.4}$$

이다. $\mathbb{E}W_i = 1/\lambda > 0$ 이므로 큰수법칙으로 $T_k \to \infty$ 가 거의 확실히 성립하여 유한 시간 안에 무한히 많은 도착이 몰리지 않는다.

독립 지수 대기시간 구성과 앞의 독립 Poisson 증분 정의는 동치이다. 지수분포의 무기억성과 독립성으로 각 시점 이후의 대기를 새로 시작할 수 있으며, 도착 횟수의 분포와 독립 증분을 도출한다. 이 동치의 일반적인 구성 증명 전체 대신 아래에서는 직접 계산되는 주변분포를 확인한다.

> **명제 4.4 (k 번째 도착시간)** 양의 정수 k 에 대해
>
> $$T_k \sim \operatorname{Gamma}(k, \lambda), \qquad \mathbb{E}T_k = \frac{k}{\lambda}, \qquad \operatorname{Var}(T_k) = \frac{k}{\lambda^2} \tag{4.5}$$
>
> 이다. 또한 $\{T_k \leq t\} = \{N_t \geq k\}$ 이다.

증명. 같은 발생률의 독립 지수 확률변수 k 개의 합은 형상 모수 k 인 감마분포이다. 실제로 $\operatorname{Exp}(\lambda)$ 의 적률생성함수가 $\lambda/(\lambda - u)\,(u < \lambda)$ 이므로 합의 적률생성함수는 $(\lambda/(\lambda-u))^k$ 이며 이는 $\operatorname{Gamma}(k,\lambda)$ 의 것이다. 사건의 동치는 k 번째 도착이 시간 t 까지 일어난 것과 그 시점의 사건 수가 적어도 k 라는 의미에서 따른다. 예를 들어 감마 생존함수는

$$\mathbb{P}(T_k > t) = \mathbb{P}(N_t \leq k-1) = e^{-\lambda t} \sum_{j=0}^{k-1} \frac{(\lambda t)^j}{j!}$$

로도 계산된다. □

> **예제 4.5 (세 번째 도착)** 발생률 2 인 과정에서 세 번째 도착까지 평균은 $3/2$ 시간단위이다. $T_3 > 1$ 일 확률은 $e^{-2}(1+2+2) = 5e^{-2} \approx 0.676676$ 이다. 평균 대기시간과 일정 시간 안에 사건이 충분히 쌓일 확률은 다른 요약이다.

4.4 중첩과 속아내기

명제 4.6 (독립 과정의 중첩) 독립인 발생률 λ_1, λ_2 Poisson 과정을 더하면 발생률 $\lambda_1 + \lambda_2$의 Poisson 과정이다.

증명. 각 구간의 증분은 독립 Poisson 변수 둘의 합이므로 평균 모수가 더해진다. 서로 겹치지 않는 구간의 합들은 모든 원래 증분들의 독립성으로 독립이다. 따라서 정의를 만족한다. □

각 도착에 기존 과정과 독립인 표시를 붙여 확률 p로 종류 A, 확률 $1-p$로 종류 B로 정한다고 하자(**속아내기**, *thinning*). 종류별 사건수 과정은 각각 발생률 λp, $\lambda(1-p)$의 Poisson 과정이며 서로 독립이다. 표시들이 각 도착에서 독립이고 원래 과정과도 독립이라는 조건이 필요하다. 고정된 길이 t 구간에서 종류별 개수를 K, L이라 하면 확률생성함수로

$$\begin{aligned}\mathbb{E}[z^K w^L] &= \mathbb{E}\big[(pz + (1-p)w)^{N_t}\big] \\ &= \exp\{\lambda t[p(z-1) + (1-p)(w-1)]\}\end{aligned}$$

이므로 두 Poisson 생성함수의 곱으로 분리된다. 서로 겹치지 않는 구간에서도 독립성이 유지되어 과정 수준의 결론을 얻는다. 마지막 등호는 $\mathrm{Pois}(\mu)$의 생성함수 $\mathbb{E}[x^N] = e^{\mu(x-1)}$에 $x = pz + (1-p)w$를 대입한 것이고, $x - 1 = p(z-1) + (1-p)(w-1)$이다.

예제 4.7 시간당 발생률 12의 도착에서 각 도착이 독립적으로 확률 $1/4$로 특별 표시를 받으면 특별 도착은 발생률 3이다. 30분 동안 특별 도착이 없을 확률은 $e^{-1.5} \approx 0.223130$이다. 표시가 도착 간 혼잡이나 순서에 따라 연동된다면 이 단순 속아내기 모형이 아닐 수 있다.

4.5 총개수가 주어졌을 때의 도착 위치

정리 4.8 (조건부 균등 순서통계량) $N_t = n$이 주어지면 $0 < T_1 < \cdots < T_n < t$의 결합분포는 독립 $\mathrm{Unif}(0,t)$ 표본 n개의 순서통계량 분포와 같다. $n \ge 1$, $t > 0$이다.

증명. 지수 대기시간의 결합밀도와 n번째 도착 이후 t까지 추가 도착이 없을 확률을 곱하면, 순서 영역 $0 < t_1 < \cdots < t_n < t$에서의 밀도는

$$\prod_{i=1}^{n} \lambda e^{-\lambda(t_i - t_{i-1})} \cdot e^{-\lambda(t - t_n)} = \lambda^n e^{-\lambda t}$$

이다($t_0 = 0$). 이를 $\mathbb{P}(N_t = n) = e^{-\lambda t}(\lambda t)^n / n!$로 나누면 $n!/t^n$이다. 이것은 균등 표본 순서통계량의 밀도이다. □

따라서 $0 < s < t$에서

$$N_s \mid N_t = n \sim \mathrm{Bin}(n, s/t) \tag{4.6}$$

이다. 각 도착이 독립적으로 $(0,s]$에 놓일 확률이 s/t이기 때문이다. 조건 없이 구간 증가량들은 독립이지만 전체 합을 고정하면 부분 구간 개수들은 서로 의존한다. 앞 구간에 많이 배정되면 뒤 구간에 남는 개수가 줄어든다.

예제 4.9 두 시간 동안 도착이 6번 있었다는 조건에서 첫 30분의 도착 수 평균은 $6(1/4) = 1.5$이고, 그 구간에 도착이 없을 확률은 $(3/4)^6 \approx 0.177979$이다. 조건부 계산에서는 전체 발생률이 사라지고 상대 구간 길이가 남는다.

4.6 비동질 발생률의 확장

시간에 따라 변하는 결정론적 발생률 $\lambda(t) \geq 0$가 국소적분가능하면 누적강도는 $\Lambda(t) = \int_0^t \lambda(s)\,\mathrm{d}s$이다. 독립 증분과

$$N_t - N_s \sim \mathrm{Pois}(\Lambda(t) - \Lambda(s)) \tag{4.7}$$

를 갖는 **비동질 Poisson 과정**을 정의할 수 있다. 이 과정은 보통 정상 증분을 갖지 않는다. 첫 도착의 생존함수는 $e^{-\Lambda(t)}$이며 일반적으로 지수분포가 아니다. 시간변환 $\widetilde{N}_{\Lambda(t)}$로 발생률 1의 동질 과정에서 구성할 수 있다. 여기서 $\widetilde{N}$은 발생률 1의 동질 과정이다.

4.7 연습문제와 해설

연습문제 4.10 발생률 3 과정에서 길이 2 구간의 사건수가 정확히 4일 확률을 써라.

풀이. 평균 모수는 6이므로 $e^{-6}6^4/4! = 54e^{-6}$이다. 발생률과 구간의 평균 사건수를 구별한다.

연습문제 4.11 $N_4 = 8$이 주어졌을 때 N_1의 분포를 구하라.

풀이. $\mathrm{Bin}(8, 1/4)$이다. 평균은 2이고 분산은 $8(1/4)(3/4) = 3/2$이다.

연습문제 4.12 $\lambda(t) = 2t$인 비동질 과정의 첫 도착시간 생존함수와 N_2의 평균을 구하라.

풀이. $\Lambda(t) = t^2$이므로 생존함수는 e^{-t^2}이고 평균 사건수는 $\Lambda(2) = 4$이다. 대기시간이 발생률 상수의 지수분포는 아니다.

연습문제 4.13 $N_t - \lambda t$의 평균과 분산은 무엇인가?

풀이. 평균은 0, 분산은 λt이다. 평균이 항상 0이라는 사실만으로 마팅게일이라고 결론낼 수는 없지만, 독립 증분을 사용하면 다음 장의 조건부 평균 성질을 확인할 수 있다.

다음 연결. Poisson 계수에서 평균 추세를 빼면 현재 정보로 본 미래의 조건부 평균이 현재 값과 같다. 이 공정성 구조가 마팅게일의 정의이며, 정지 규칙을 분석할 때 가정이 특히 중요해진다(제21권 제5장).

제 5 장

마팅게일과 정지 규칙

개요 마팅게일(*martingale*)은 정보가 늘어날 때 미래 값의 조건부 평균이 현재 값과 일치하는 확률과정이고, 정지시간(*stopping time*)은 현재까지의 정보만으로 멈출지 판단하는 무작위 시각이다. 이 장은 여과와 마팅게일의 정의, 관측에 따른 조건부 평균, 예측가능한 가중합(마팅게일 변환), 정지시간과 멈춘 마팅게일, 선택정리와 그 가정의 필요성, 최대 부등식을 다룬다. 이를 이용하여 도박사의 파산 문제를 다시 풀고 Poisson 마팅게일을 소개한다. 선행 지식: 조건부기대, 여과, 적분가능성, 지배수렴정리와 균등적분가능성. 이산시간 정리에서는 시간지표를 $n = 0, 1, 2, \dots$로 둔다.

5.1 현재 정보로 보는 미래의 평균

마팅게일은 값이 항상 같거나 매 경로가 평탄하다는 뜻이 아니다. 정보가 늘어날 때 미래 값의 조건부 평균이 현재 값과 일치한다는 뜻이다. 따라서 과정뿐 아니라 어떤 여과를 쓰는지도 정의의 일부이다. **여과**(*filtration*) $(\mathcal{F}_n)$은 $\mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \cdots$인 σ-대수의 증가열이고, M_n이 $\mathcal{F}_n$-가측이면 (M_n)이 $(\mathcal{F}_n)$에 **적응**(*adapted*)되었다고 한다.

정의 5.1 (마팅게일) 여과 $(\mathcal{F}_n)$에 대하여 실수값 과정 (M_n)이 **마팅게일**이려면 다음 세 조건을 만족해야 한다.

$$M_n \text{은 } \mathcal{F}_n\text{-가측}, \qquad \mathbb{E}\,|M_n| < \infty, \qquad \mathbb{E}[M_{n+1} \mid \mathcal{F}_n] = M_n \quad \text{a.s.} \tag{5.1}$$

마지막 등호를 $\geq$로 바꾼 것을 **부분마팅게일**(*submartingale*)이라 하고, $\leq$로 바꾼 것을 **초마팅게일**(*supermartingale*)이라 한다. 이 용어의 "부분"은 부분수열이라는 뜻이 아니다.

조건부 평균은 거의 확실하게만 정해지므로 정의의 등식도 거의 확실하게 해석한다. 이산시간의 모든 n에 대한 영집합을 합쳐도 영집합이어서, 필요한 등식들을 하나의 확률 1 사건에서 동시에 만족하도록 다룰 수 있다.

역사. 마팅게일이라는 말은 본래 도박의 배가 전략을 가리키는 용어였고, 확률론의 개념으로는 Lévy와 Ville의 선행 연구를 거쳐 Doob이 1940년대와 1950년대에 부분마팅게일과 정지시간 정리를 포함하는 체계로 정리하였다.

명제 5.2 마팅게일에 대하여 $m \leq n$이면

$$\mathbb{E}[M_n \mid \mathcal{F}_m] = M_m, \qquad \mathbb{E}M_n = \mathbb{E}M_0 \tag{5.2}$$

이다.

증명. $n = m + 1$은 정의이다. $n = m + 2$일 때 탑 성질과 $\mathcal{F}_m \subseteq \mathcal{F}_{m+1}$을 사용하면

$$\mathbb{E}[M_{m+2} \mid \mathcal{F}_m] = \mathbb{E}\{\mathbb{E}[M_{m+2} \mid \mathcal{F}_{m+1}] \mid \mathcal{F}_m\} = \mathbb{E}[M_{m+1} \mid \mathcal{F}_m] = M_m$$

이다. 이를 반복하면 첫 식을 얻고, 양변에 기댓값을 취하면 $m=0$에서 두 번째 식을 얻는다. $\square$

예제 5.3 (독립 증분의 합) ξ_k가 독립이고 $\mathbb{E}|\xi_k|<\infty$, $\mathbb{E}\xi_k=0$이라고 하자. $S_0=0$, $S_n=\sum_{k=1}^{n}\xi_k$와 $\mathcal{F}_n=\sigma(\xi_1,\dots,\xi_n)$에 대하여

$$\mathbb{E}[S_{n+1}\mid\mathcal{F}_n]=S_n+\mathbb{E}[\xi_{n+1}\mid\mathcal{F}_n]=S_n$$

이므로 S_n은 마팅게일이다. 독립성 대신 적응 증분이 $\mathbb{E}[\xi_{n+1}\mid\mathcal{F}_n]=0$을 만족한다고 가정해도 같은 결론이다.

예제 5.4 (제곱의 보정) 위의 독립 증분이 추가로 $\mathbb{E}\xi_k^2=1$을 만족하면 S_n^2-n도 마팅게일이다. 조건부로 전개하면

$$\mathbb{E}[S_{n+1}^2\mid\mathcal{F}_n]=S_n^2+2S_n\mathbb{E}[\xi_{n+1}\mid\mathcal{F}_n]+\mathbb{E}[\xi_{n+1}^2\mid\mathcal{F}_n]=S_n^2+1$$

이다. 제곱 과정 자체는 부분마팅게일이고, 누적 분산을 빼면 마팅게일이 된다. 증분 분산이 결정론적인 v_k이면 보정항은 n 대신 $\sum_{k=1}^{n}v_k$이다.

예제 5.5 (평균 일정만으로 부족함) $\mathbb{P}(Z=1)=\mathbb{P}(Z=-1)=1/2$이고 $M_0=0$, $M_1=Z$, $M_2=-Z$로 두자. 세 시점의 기댓값은 모두 0이다. 그러나 자연여과에서 $\mathbb{E}[M_2\mid\mathcal{F}_1]=-Z\neq Z=M_1$이므로 마팅게일이 아니다. 첫 결과를 본 뒤에는 다음 값이 그 반대라는 것을 정확히 안다.

명제 5.6 (관측에 따른 조건부 평균) Y가 적분가능하고 $(\mathcal{F}_n)$이 여과이면 $M_n=\mathbb{E}[Y\mid\mathcal{F}_n]$은 마팅게일이다.

증명. 조건부기대의 정의에 의해 적응성 및 $\mathbb{E}|M_n|\le\mathbb{E}|Y|<\infty$가 성립한다. 탑 성질로

$$\mathbb{E}[M_{n+1}\mid\mathcal{F}_n]=\mathbb{E}\{\mathbb{E}[Y\mid\mathcal{F}_{n+1}]\mid\mathcal{F}_n\}=\mathbb{E}[Y\mid\mathcal{F}_n]=M_n$$

이다. $\square$

이는 최종 관심량 Y에 대한 예측을 관측에 따라 갱신하는 과정이다. 새 정보가 실제로 들어오면 예측값은 변하지만, 현재 정보를 기준으로 다음 예측값이 어느 방향으로 바뀔지는 평균적으로 알 수 없다.

5.2 예측가능한 가중합

시간 k의 증분을 관측하기 전에 정하는 가중치를 H_k라 하자. 이산시간에서 "예측가능"은 H_k가 $\mathcal{F}_{k-1}$-가측이라는 뜻이다. H_k가 실제 미래를 정확히 예측한다는 의미가 아니다.

명제 5.7 (마팅게일 변환) (M_n)이 마팅게일이고 각 H_k가 유계이며 $\mathcal{F}_{k-1}$-가측이면

$$G_0=0,\qquad G_n=\sum_{k=1}^{n}H_k(M_k-M_{k-1}) \tag{5.3}$$

는 마팅게일이다. 각 k의 유계상수는 서로 달라도 된다.

증명. 유계성으로 각 곱이 적분가능하고 G_n은 $\mathcal{F}_n$-가측이다. 조건부기대에서 알려진 H_{n+1}을 밖으로 꺼내면

$$\mathbb{E}[G_{n+1} - G_n \mid \mathcal{F}_n] = H_{n+1}\,\mathbb{E}[M_{n+1} - M_n \mid \mathcal{F}_n] = 0. \qquad \square$$

더 일반적으로는 필요한 곱의 적분가능성과 조건부기대 연산의 정당성을 직접 확인하여 유계 가정을 완화할 수 있다. 여기서는 유계 가중치가 가장 간단한 충분조건이다. 매 시점의 기댓값 보존은 정지시간까지 무한히 기다린 뒤에도 기댓값이 보존된다는 결론과 구분해야 한다.

예제 5.8 공정한 ± 1 증분에 대하여 짝수 단계에서만 $H_k = 2$, 홀수 단계에서는 $H_k = 0$으로 두면 $\mathbb{E}G_n = 0$이고

$$\operatorname{Var}(G_n) = 4\lfloor n/2 \rfloor$$

이다. $G_n = \sum_{k \le n,\ k\ \text{짝수}} 2\xi_k$이고 짝수 $k \le n$이 $\lfloor n/2 \rfloor$개이기 때문이다. 평균을 바꾸지 않는 전략도 변동의 크기는 크게 바꿀 수 있다. 서로 다른 시점의 독립 증분 때문에 교차 공분산이 0이다.

5.3 정지시간과 멈춘 과정

정의 5.9 (정지시간) $\tau : \Omega \to \{0, 1, 2, \dots\} \cup \{\infty\}$가 모든 n에 대하여 $\{\tau \le n\} \in \mathcal{F}_n$을 만족하면 **정지시간**이라 한다. 현재까지의 정보로 이미 멈추었는지를 결정할 수 있어야 한다.

상태가 처음 어떤 집합에 들어간 시점은 정지시간이다. 이산시간 적응과정 X_n과 가측집합 A에 대해

$$\{\inf\{k \ge 0 : X_k \in A\} \le n\} = \bigcup_{k=0}^{n} \{X_k \in A\} \in \mathcal{F}_n$$

이기 때문이다. 반면 "앞으로 영원히 다시 방문하지 않게 되는 마지막 방문 시점"은 일반적으로 미래 정보를 요구한다.

예제 5.10 (마지막 앞면은 정지시간이 아님) 독립적인 공정 동전을 두 번 던지고, 마지막 앞면의 위치를 τ라 하되 앞면이 없으면 $\tau = 0$으로 두자. 첫 던짐 이후 $\{\tau \le 1\}$이 성립하는지는 두 번째가 뒷면인지에 달려 있다. 이 사건은 첫 결과만으로 결정할 수 없으므로 자연여과에 대한 정지시간이 아니다.

명제 5.11 (멈춘 마팅게일) τ가 정지시간이면 $M_{n \wedge \tau}$는 마팅게일이다.

증명. 고정된 n에서 $M_{n\wedge\tau}$는 $M_0, \dots, M_n$ 중 하나이므로 적분가능하고 $\mathcal{F}_n$-가측이다. 증분을 쓰면

$$M_{(n+1)\wedge\tau} - M_{n\wedge\tau} = \mathbf{1}_{\{\tau > n\}}(M_{n+1} - M_n)$$

이다. 정지시간 조건에 의해 앞의 지시함수는 $\mathcal{F}_n$-가측이다. 조건부기대를 취하면 오른쪽은 0이다. $\square$

이 정리는 모든 고정된 n에서 유효하다. M_τ를 정의하려면 보통 $\tau < \infty$가 거의 확실하게 성립해야 하며, $n \to \infty$로 기댓값까지 넘기는 문제는 별도이다.

5.4 선택정리: 어떤 가정이 필요한가

정리 5.12 (유계 정지시간) (M_n)이 마팅게일이고 정지시간 τ가 어떤 결정론적 정수 N에 대해 $\tau \le N$을 거의 확실하게 만족하면

$$\mathbb{E}M_\tau = \mathbb{E}M_0 \tag{5.4}$$

이다.

증명. 앞 명제에 의해 $\mathbb{E}M_{N\wedge\tau} = \mathbb{E}M_0$이고, $\tau \le N$이므로 $M_{N\wedge\tau} = M_\tau$이다. 직접적으로도

$$M_\tau = M_0 + \sum_{k=1}^{N} \mathbf{1}_{\{\tau \ge k\}} (M_k - M_{k-1})$$

를 쓰면 된다. 각 지시함수는 $\{\tau \ge k\} = \{\tau \le k-1\}^c \in \mathcal{F}_{k-1}$-가측이므로 합의 각 항의 기댓값이 0이다. $\square$

정리 5.13 (유계가 아닌 정지시간의 충분조건) $\tau < \infty$가 거의 확실하게 성립하는 정지시간이고 (M_n)이 마팅게일이라고 하자. 다음 조건들 중 어느 하나가 성립하면 M_τ는 적분가능하며 $\mathbb{E}M_\tau = \mathbb{E}M_0$이다.

(1) $\{M_{n\wedge\tau} : n \ge 0\}$가 균등적분가능하다.

(2) 모든 n에 대해 $|M_{n\wedge\tau}| \le Z$인 적분가능한 확률변수 Z가 있다.

(3) $\mathbb{E}\tau < \infty$이고, 어떤 상수 $C < \infty$에 대해 모든 $n \ge 1$에서 $|M_n - M_{n-1}| \le C$가 거의 확실하게 성립한다.

증명. τ가 유한한 경로에서 $M_{n\wedge\tau}$는 결국 M_τ와 같아지므로 거의 확실하게 수렴한다. 첫 조건이면 균등적분가능성과 확률수렴으로 L^1 수렴을 얻는다. 두 번째 조건이면 지배수렴정리가 적용된다. 세 번째 조건이면

$$|M_{n\wedge\tau}| \le |M_0| + C(n\wedge\tau) \le |M_0| + C\tau$$

이고 오른쪽의 기댓값이 유한하므로 두 번째 조건으로 돌아간다. 세 경우 모두 $\mathbb{E}M_{n\wedge\tau} = \mathbb{E}M_0$에 극한을 취한다. $\square$

이들은 사용하기 쉬운 충분조건이며 필요충분조건 목록은 아니다. 특히 "거의 확실하게 유한한 정지시간"과 "기대 정지시간이 유한함"은 서로 다르다. 세 번째 항에서 기대 정지시간만 확인하고 증분의 유계성을 생략해서도 안 된다.

예제 5.14 (거의 확실한 도달과 무한 평균 대기) S_n을 $S_0 = 0$인 대칭 단순보행, $\tau = \inf\{n : S_n = 1\}$이라 하자. 앞 장의 유한 구간 흡수확률 극한으로 $\mathbb{P}(\tau < \infty) = 1$을 알았다(제21권 제3장). 따라서 $S_\tau = 1$이지만 모든 n에 대해 $\mathbb{E}S_{\tau\wedge n} = 0$이다. 기댓값과 극한이 교환되지 않는다. 이제 $\mathbb{E}\tau < \infty$라고 가정하면 보행 증분의 절댓값은 1이므로 방금 증명한 세 번째 충분조건으로 $\mathbb{E}S_\tau = \mathbb{E}S_0 = 0$을 얻는다. 이는 $S_\tau = 1$과 모순이다. 따라서 $\mathbb{E}\tau = \infty$이고, 멈춘 변수족은 균등적분가능하지 않다. 도달이 거의 확실하다는 사실만으로 선택정리를 적용할 수 없음을 보여준다.

예제 5.15 (기대 정지시간이 유한해도 부족함) 공정 동전에서 첫 앞면이 나오는 시점을 T라 하고, k번째 시행 직전까지 모두 뒷면이면 크기 2^{k-1}인 대칭 보상을 받는 시행을 한다고 하자.

앞면이면 그 금액을 얻고 뒷면이면 잃으며, 첫 앞면 이후에는 더하지 않는다. 누적 보상 G_n은 예측가능한 유계 가중합의 마팅게일이다(가중치 $H_k = 2^{k-1}\mathbf{1}_{\{T \ge k\}}$). 각 시점 k의 가중치가 유계라는 말은 전체 k에 공통인 상수로 유계라는 말과 다르다. T는 성공확률 $1/2$의 기하분포이므로 $\mathbb{E}T = 2$이고 거의 확실하게 유한하다. 첫 성공 때의 누적 보상은

$$2^{T-1} - \sum_{k=1}^{T-1} 2^{k-1} = 1$$

이다. 그러나 시점 n에서

$$G_n = \begin{cases} 1, & T \le n, \\ -(2^n - 1), & T > n \end{cases}$$

이므로

$$\mathbb{E}G_n = (1 - 2^{-n}) - 2^{-n}(2^n - 1) = 0$$

이다. 극한의 평균은 1인데 모든 유한 단계의 평균은 0이다. 증분의 크기가 균일하게 제한되지 않고, 드물지만 큰 음의 값이 기댓값을 보존한다. 유한 평균 정지시간만으로 무한 전략의 기댓값 교환을 정당화할 수 없다.

흔한 오류. 정지 규칙을 자료를 보고 정한 뒤 고정 시점 공식의 기댓값을 그대로 쓰는 것은 별도 정당화가 필요한 단계이다. 선택정리는 정지시간 조건뿐 아니라 적분가능성과 극한 교환 조건을 함께 확인할 때 사용한다.

5.5 흡수확률과 평균시간을 마팅게일로 다시 구하기

$0, \dots, M$에서 대칭 단순보행이 경계 $0, M$에 처음 도달하는 시간을 τ라 하고 $S_0 = i$로 두자. 앞 장에서 τ가 거의 확실하게 유한하고 평균도 유한함을 증명했다. 멈춘 위치는 $0 \le S_{n\wedge\tau} \le M$으로 지배되므로

$$i = \mathbb{E}S_\tau = M\,\mathbb{P}(S_\tau = M) \tag{5.5}$$

이다. 따라서 상단 흡수확률은 i/M이다. 이는 선형 차분방정식 풀이와 일치한다. 평균시간은 마팅게일 $S_n^2 - n$에 유계 정지시간 $\tau \wedge n$을 먼저 적용하여

$$\mathbb{E}S_{\tau\wedge n}^2 - \mathbb{E}(\tau \wedge n) = i^2$$

를 얻는다. 제곱 위치는 M^2로 지배되고 시간은 단조 증가하므로, 지배수렴과 단조수렴을 각각 적용하면

$$\mathbb{E}\tau = \mathbb{E}S_\tau^2 - i^2 = M^2\frac{i}{M} - i^2 = i(M - i) \tag{5.6}$$

이다. 처음부터 유계가 아닌 τ를 임의로 대입하는 대신 유계 정지시간에서 출발하면 정당화가 분명해진다.

예제 5.16 (비대칭 보행의 지수 마팅게일) 확률 p로 $+1$, $q = 1 - p$로 -1 증분을 갖는 보행 S_n과 $r = q/p \ne 1$에 대해 r^{S_n}은 마팅게일이다. $\mathbb{E}[r^{\xi}] = pr + q/r = q + p = 1$이기 때문이다. $[0, M]$

에서 멈추면 $r^{S_{n\wedge\tau}}$는 유계이므로 선택정리로 $r^i = \mathbb{E}\, r^{S_\tau} = 1 - h + h r^M$이고, $h = \mathbb{P}(S_\tau = M)$는

$$h = \frac{r^i - 1}{r^M - 1} = \frac{1 - r^i}{1 - r^M}$$

이다. 앞 장의 파산 확률 공식과 일치한다.

5.6 최댓값을 제어하는 부등식

정리 5.17 (이산시간 Doob 최대 부등식) $X_0, \dots, X_N$이 음이 아닌 부분마팅게일이고 $\lambda > 0$이면

$$\lambda\, \mathbb{P}\Big(\max_{0\le k\le N} X_k \ge \lambda\Big) \le \mathbb{E}\big[X_N \mathbf{1}_{\{\max_{k\le N} X_k \ge \lambda\}}\big] \le \mathbb{E} X_N \tag{5.7}$$

이다.

증명. $A_k = \{X_0 < \lambda, \dots, X_{k-1} < \lambda, X_k \ge \lambda\}$로 두자. $A_k \in \mathcal{F}_k$이고 서로소이며 그 합집합은 최댓값이 λ 이상인 사건이다. 부분마팅게일 성질을 반복하면 $\mathbb{E}[X_N \mid \mathcal{F}_k] \ge X_k$이다. 따라서

$$\mathbb{E}[X_N \mathbf{1}_{A_k}] = \mathbb{E}\big[\mathbf{1}_{A_k} \mathbb{E}[X_N \mid \mathcal{F}_k]\big] \ge \mathbb{E}[X_k \mathbf{1}_{A_k}] \ge \lambda\, \mathbb{P}(A_k)$$

이다. k에 대해 더하면 첫 부등식을 얻고, 음이 아닌 X_N으로 두 번째 부등식을 얻는다. □

마팅게일 M_k에 대해 조건부 Jensen 부등식으로 $|M_k|$는 부분마팅게일이다. 제곱적분가능하면 $|M_k|^2$도 그러하므로

$$\mathbb{P}\Big(\max_{k\le N} |M_k| \ge a\Big) \le \frac{\mathbb{E} M_N^2}{a^2}, \qquad a > 0 \tag{5.8}$$

이다. 이는 각 시점의 확률을 더하는 단순 합집합 상계보다 좋은 제어를 줄 수 있다. 더 강한 L^2 형태 $\mathbb{E}\max_{k\le N}|M_k|^2 \le 4\mathbb{E}|M_N|^2$도 성립하지만, 그것은 마지막 표시식을 단순 적분하는 것만으로 나오지는 않는다.

예제 5.18 공정한 ± 1 보행에서 $\mathbb{E} S_N^2 = N$이므로 $\mathbb{P}(\max_{k\le N}|S_k| \ge a) \le N/a^2$이다. $N = 100$, $a = 20$이면 상계는 $1/4$이다. 상계가 1보다 크면 확률의 자명한 상계 1과 최소를 취한다.

5.7 Poisson 마팅게일

연속시간에서도 각 t에서 적분가능하고 적응하며 $s \le t$에 대해 $\mathbb{E}[M_t \mid \mathcal{F}_s] = M_s$이면 마팅게일이라 한다. 발생률 λ Poisson 과정의 자연여과에 대하여

$$\mathbb{E}[N_t - N_s \mid \mathcal{F}_s] = \lambda (t - s)$$

이므로 $M_t = N_t - \lambda t$는 마팅게일이다. 또한 보정된 독립 증분의 조건부 이차모멘트는 $\lambda(t-s)$이어서 $M_t^2 - \lambda t$ 역시 마팅게일이다. 연속시간의 임의 정지시간에 대한 정리는 경로와 여과의 정칙성을 추가로 다루므로, 이산시간 증명을 말없이 그대로 적용하지 않는다.

5.8 연습문제와 해설

연습문제 5.19 독립 증분 ξ_k가 평균 μ, 분산 $\sigma^2 < \infty$를 가질 때 $S_n = \sum_{k=1}^{n} \xi_k$에서 두 개의 마팅게일을 구성하라.

풀이. $M_n = S_n - n\mu$와 $M_n^2 - n\sigma^2$이다. 첫 과정의 증분은 조건부 평균 0이고 조건부 분산 σ^2이다. 원래 $S_n^2 - n\sigma^2$는 $\mu \neq 0$일 때 일반적으로 마팅게일이 아니다.

연습문제 5.20 $Y \in L^1$이고 $M_n = \mathbb{E}[Y \mid \mathcal{F}_n]$라고 하자. $\mathcal{F}_n$이 실제로 커져도 M_n이 항상 같을 수 있는가?

풀이. 가능하다. 예를 들어 모든 $\mathcal{F}_n$이 Y와 독립인 정보만 포함하면 $M_n = \mathbb{E}Y$이다. 여과의 증가는 대상 Y에 대한 정보를 반드시 증가시키지는 않는다.

연습문제 5.21 대칭 단순보행을 0에서 시작하여 -2 또는 3에 도달하면 멈춘다. 위쪽 경계에 닿을 확률과 평균 정지시간을 구하라.

풀이. 위치에 2를 더하면 구간 $[0, 5]$의 출발점 2가 된다. 따라서 확률은 $2/5$, 평균은 $2(5-2) = 6$이다. $\mathbb{E}S_\tau = 3p - 2(1-p) = 0$으로도 $p = 2/5$를 얻는다.

연습문제 5.22 앞의 두 배 가중치 예제에서 $\mathbb{E}T < \infty$인데 선택정리가 실패하는 이유를 충분조건과 연결하라.

풀이. 증분은 k번째에 최대 2^{k-1}이므로 모든 시점에 공통인 유계상수 C가 없다. 멈춘 변수족도 균등적분가능하지 않다. 실제로 $2^n - 1 > K$일 때 큰 음의 값이 주는 절대기대값은 $(2^n - 1)2^{-n}$으로 $n \to \infty$에서 1에 접근하므로, 꼬리의 기댓값을 균일하게 작게 만들 수 없다.

연습문제 5.23 N_t가 발생률 2 Poisson 과정일 때 $M_t = N_t - 2t$라 하자. $t \geq s$에서 $\mathbb{E}[M_t^2 \mid \mathcal{F}_s]$를 구하라.

풀이. $M_t = M_s + (N_t - N_s) - 2(t-s)$이고 뒤의 보정된 증분은 과거와 독립이며 평균 0, 분산 $2(t-s)$이다. 따라서 $\mathbb{E}[M_t^2 \mid \mathcal{F}_s] = M_s^2 + 2(t-s)$이다. 특히 $M_t^2 - 2t$가 마팅게일이다.

다음 연결. Brownian 운동도 독립적인 평균 0 증분을 가지며, 제곱에서 시간을 빼면 마팅게일이 된다. 다만 경로의 변동이 너무 커서 적분을 통상적인 Riemann–Stieltjes 적분과 다르게 구성해야 한다(제21권 제6장).

제 6 장

Brownian 운동, Itô 적분, 확률미분방정식

개요 표준 Brownian 운동(*standard Brownian motion*)은 독립이고 정상인 정규 증분과 연속 경로를 가지며 0에서 출발하는 실수값 과정이고, Itô 적분은 이 과정을 적분자로 하여 예측가능한 피적분과정을 적분하는 연산이다. 이 장은 Brownian 운동의 정의와 평균·공분산, 스케일 변환, 이차변동과 무한 총변동을 증명하고, 단순 예측가능 과정에 대한 Itô 적분과 Itô 등거리를 세운 뒤, $\int_0^T B_s \, \mathrm{d}B_s = (B_T^2 - T)/2$를 직접 계산하고 Itô 공식, 확률미분방정식(SDE)의 강한 해, 기하 Brownian 운동, Ornstein–Uhlenbeck 과정, Euler–Maruyama 근사의 한계를 다룬다. 요점은 경로(한 표본 위의 함수)와 분포(법칙)를 구별하는 것, 그리고 이차변동 때문에 고전 미적분의 연쇄 법칙에 $\frac{1}{2} f_{xx} \, \mathrm{d}t$ 항이 더해진다는 것이다. 선행 지식: 정규분포와 정규벡터, L^2 수렴, 조건부 기댓값, 마팅게일(제21권 제5장), 일변수 미적분. 적분의 전체 측도론적 구성보다 정의와 계산에 필요한 가정을 우선한다.

6.1 표준 Brownian 운동의 정의

정의 6.1 (표준 Brownian 운동) 실수값 과정 $(B_t)_{t \ge 0}$이 **표준 Brownian 운동**(*standard Brownian motion*)이면 다음을 만족한다.

(1) $B_0 = 0$이 거의 확실하게 성립한다.

(2) 서로 겹치지 않는 시간구간의 증분은 독립이다.

(3) $0 \le s < t$이면 $B_t - B_s \sim N(0, t - s)$이다.

(4) 확률 1로 경로 $t \mapsto B_t$가 연속이다.

W_t라는 기호도 널리 쓰인다. 여기서 '표준'이라는 말은 단위 시간당 증분 분산이 1임을 뜻한다. $X_t = \mu t + \sigma B_t$의 증분 평균은 $\mu(t-s)$, 분산은 $\sigma^2 (t-s)$이다. 특히 표준편차는 시간 길이에 비례하지 않고 그 제곱근에 비례한다.

Brownian 운동의 존재는 정합적인 Gauss 유한차원분포를 구성하고 연속인 수정(*modification*)을 얻는 정리로 보일 수 있다. 예를 들어 증분의 4차 모멘트

$$\mathbb{E}\,|B_t - B_s|^4 = 3\,|t-s|^2 \tag{6.1}$$

는 Kolmogorov 연속성 정리를 적용하는 데 필요한 추정이다(지수가 $4 = \alpha$, $2 = 1 + \beta$이므로 $\beta = 1 > 0$). 이 장에서는 존재 및 연속성 정리의 전체 증명은 범위 밖으로 두고, 위의 네 성질을 갖는 과정이 존재한다는 정리를 사용한다. 정규분포인 각 주변분포만 지정한다고 경로 연속성이 따라오는 것은 아니다.

역사 (Brownian 운동의 기원). 꽃가루 입자의 불규칙한 운동은 1827년 Robert Brown이 관찰하였고, 같은 현상의 확률적 모형은 Bachelier(1900, 주가)와 Einstein(1905, 확산)이 각자 독립적으로

제시하였다. 수학적으로 엄밀한 존재 증명은 Wiener(1923)에 의하며, 그 때문에 W_t와 'Wiener 과정' 이라는 이름이 쓰인다. Itô는 1940년대 중반에 Brownian 운동에 대한 확률적분을 정의하였다.

이후의 확률적분에서는 완비이고 우연속인 여과 $(\mathcal{F}_t)$를 쓰며, B_t가 적응하고 $B_t - B_s$가 $\mathcal{F}_s$와 독립인 Brownian 운동이라고 가정한다. 완비성은 확률 0 사건의 부분집합을 포함하는 조건이고, 우연속성은 $\mathcal{F}_t = \bigcap_{u>t} \mathcal{F}_u$이다. 자연여과를 통상적인 방식으로 보완하면 이런 설정을 얻는다. 여과에 미래의 B_T를 미리 추가하면 독립 증분의 조건부 형태가 깨질 수 있다.

명제 6.2 (평균과 공분산) 표준 Brownian 운동은 중심 Gauss 과정이며

$$\mathbb{E}B_t = 0, \qquad \operatorname{Cov}(B_s, B_t) = \min(s,t) \tag{6.2}$$

이다.

증명. $t_1 < \cdots < t_n$에서 $(B_{t_1}, \dots, B_{t_n})$는 독립 정규 증분들의 선형변환이므로 공동정규벡터이다. $s \le t$에서 $B_t = B_s + (B_t - B_s)$이고 두 항은 독립이므로 $\operatorname{Cov}(B_s, B_t) = \operatorname{Var}(B_s) = s$이다. □

Brownian 운동은 정상 증분을 가지지만 정상 과정은 아니다. 실제로 $\operatorname{Var}(B_t) = t$가 시간에 따라 증가한다. 연속이라는 사실도 값이 매끄럽게 미분가능하다는 뜻은 아니다.

예제 6.3 (조건부 정규분포) $s < t$에서 현재까지의 정보가 주어지면

$$B_t \mid \mathcal{F}_s \sim N(B_s, t-s)$$

라는 조건부 분포 표현을 쓸 수 있다. 정확한 의미는 가측함수 g가 적절히 적분가능할 때 조건부기대가 평균 B_s, 분산 $t-s$인 정규밀도로 적분한 값이라는 것이다. 따라서

$$\mathbb{E}[B_t \mid \mathcal{F}_s] = B_s, \qquad \mathbb{E}[B_t^2 \mid \mathcal{F}_s] = B_s^2 + t - s$$

이다. 둘째 식은 $B_t = B_s + (B_t - B_s)$를 제곱하고, 교차항 $2B_s\,\mathbb{E}[B_t - B_s \mid \mathcal{F}_s] = 0$과 $\mathbb{E}[(B_t-B_s)^2 \mid \mathcal{F}_s] = t-s$를 쓰면 얻는다. B_t와 $B_t^2 - t$는 각각 마팅게일이다. 후자는 $\mathbb{E}[B_t^2 - t \mid \mathcal{F}_s] = B_s^2 + t - s - t = B_s^2 - s$로 확인된다.

6.2 스케일과 경로를 구분하기

$c > 0$에 대하여 $\widetilde{B}_t = c^{-1/2} B_{ct}$도 표준 Brownian 운동이다. 연속성은 그대로이고, 서로 겹치지 않는 구간의 독립성이 보존되며, 증분의 분산이 $c^{-1} \cdot c(t-s) = t-s$이기 때문이다. 이것은 확률법칙이 같다는 명제이지 같은 경로에서 $B_{ct} = \sqrt{c}\,B_t$라는 항등식이 아니다.

예제 6.4 고정된 $t > 0$에서 B_{4t}와 $2B_t$는 둘 다 $N(0, 4t)$이다. 하지만 같은 Brownian 경로 위에서는

$$\operatorname{Var}(B_{4t} - 2B_t) = 4t + 4t - 4\operatorname{Cov}(B_{4t}, B_t) = 4t > 0.$$

따라서 일반적으로 두 확률변수는 거의 확실하게 같지 않다. ($\operatorname{Cov}(B_{4t}, B_t) = \min(4t, t) = t$이다.)

독립 정규 증분을 이용하면 유한 격자에서 Brownian 값을 정확한 결합분포로 생성할 수 있다. 하지만 이 값들을 선분으로 연결한 경로는 격자 사이에서 실제 Brownian 경로와 같지 않다. 유한 시뮬레이션 그림은 경로의 무한 변동을 직접 보여주는 증명이 될 수 없다.

6.3 이차변동과 고전적 미분의 한계

고정된 $T>0$를 n등분하고 $\Delta_i B = B_{iT/n} - B_{(i-1)T/n}$라 하자. 이차 증분합

$$Q_n = \sum_{i=1}^{n} (\Delta_i B)^2$$

은 Brownian 운동의 변동 구조를 드러낸다.

명제 6.5 (균등분할의 이차변동)

$$\mathbb{E}Q_n = T, \qquad \operatorname{Var}(Q_n) = \frac{2T^2}{n}, \qquad Q_n \longrightarrow T \quad \text{in } L^2 \tag{6.3}$$

이다. 또한 이진 분할 $n=2^m$을 따라서는 $Q_{2^m} \to T$가 거의 확실하게 성립한다.

증명. 각 증분은 독립인 $N(0, T/n)$이다. $Z\sim N(0,v)$이면 $\mathbb{E}Z^2 = v$, $\mathbb{E}Z^4 = 3v^2$이므로 $\operatorname{Var}(Z^2) = 2v^2$이다. 독립성으로 기댓값과 분산을 더하면 $\mathbb{E}Q_n = n\cdot T/n = T$, $\operatorname{Var}(Q_n) = n\cdot 2(T/n)^2 = 2T^2/n$이다. 이진 분할에서는 Chebyshev 부등식으로

$$\sum_{m=1}^{\infty} \mathbb{P}(|Q_{2^m} - T| > \varepsilon) \le \frac{2T^2}{\varepsilon^2} \sum_{m=1}^{\infty} 2^{-m} < \infty$$

이다. Borel–Cantelli 보조정리와 $\varepsilon = 1, 1/2, 1/3, \dots$에 대한 가산 교집합으로 거의 확실한 수렴을 얻는다. □

연속함수 $x:[0,T]\to\mathbb{R}$의 **총변동**(*total variation*)은 모든 분할 $0=t_0<\cdots<t_n=T$에 대한 $\sum_i |x(t_i)-x(t_{i-1})|$의 상한이다. **이차변동**(*quadratic variation*)은 분할을 세밀하게 할 때 $\sum_i |x(t_i)-x(t_{i-1})|^2$의 극한이며, 명제 6.5는 Brownian 경로의 이차변동이 $[B]_T = T$임을 말한다.

따름정리 6.6 (무한 총변동) Brownian 경로는 고정된 구간 $[0,T]$, $T>0$에서 거의 확실하게 유한한 총변동을 갖지 않는다.

증명. 연속함수 x가 총변동 $V<\infty$를 가진다면 균등분할에서

$$\sum_{i} |\Delta_i x|^2 \le \max_i |\Delta_i x| \sum_i |\Delta_i x| \le V \max_i |\Delta_i x| \longrightarrow 0$$

이다. 마지막 수렴은 $[0,T]$ 위의 연속함수가 균등연속이기 때문이다. Brownian 경로의 이진 분할 이차합은 거의 확실하게 $T>0$으로 수렴하므로 유한 총변동일 수 없다. □

이 결과는 Brownian 운동을 모든 연속 피적분함수에 대해 고전적인 유한변동 적분(Riemann–Stieltjes 적분)의 적분자로 사용할 수 없다는 점을 설명한다. ‘어디에서도 미분가능하지 않다’ 는 더 강한 사실도 성립하지만, 방금 증명한 무한 총변동만으로 그 사실까지 증명한 것은 아니다. 이 장에서는 그 더 강한 경로 정리의 증명을 생략한다.

주의 ($(\mathrm{d}B_t)^2 = \mathrm{d}t$의 의미). 형식적인 기호 $(\mathrm{d}B_t)^2 = \mathrm{d}t$는 이차변동을 기억하는 계산 규칙이다. 무한소를 실제 실수처럼 제곱한 등식이나 모든 가능한 분할에 대한 경로별 명제가 아니다. 다음의 적분 정의와 Itô 공식이 이 표기의 정확한 의미를 제공한다.

6.4 단순 예측가능 과정의 Itô 적분

결정론적 분할 $0 = t_0 < \cdots < t_n = T$에 대해

$$H_s = \sum_{i=0}^{n-1} H_i \mathbf{1}_{(t_i, t_{i+1}]}(s), \qquad H_i \text{는 } \mathcal{F}_{t_i}\text{-가측}$$

라고 하자. 구간의 시작에서 결정한 값을 그 구간에 사용한다. 제곱적분 조건

$$\mathbb{E}\int_0^T H_s^2 \, \mathrm{d}s = \sum_{i=0}^{n-1} \mathbb{E}H_i^2 \, (t_{i+1} - t_i) < \infty$$

아래에서 **Itô 적분**(*Itô integral*)의 정의는

$$\int_0^T H_s \, \mathrm{d}B_s := \sum_{i=0}^{n-1} H_i \, (B_{t_{i+1}} - B_{t_i}) \tag{6.4}$$

이다. 적분값은 확률변수이며 일반적으로 각 경로에서 고전 적분의 극한으로 먼저 정의하지 않는다. 구간 시작점의 값을 쓰는 이 규칙(왼쪽 끝점 규칙)이 Itô 적분의 본질이며, 중점이나 오른쪽 끝점을 쓰면 다른 적분이 된다.

정리 6.7 (Itô 등거리) 위의 단순 예측가능 과정에 대해

$$\mathbb{E}\int_0^T H_s \, \mathrm{d}B_s = 0, \qquad \mathbb{E}\left(\int_0^T H_s \, \mathrm{d}B_s\right)^2 = \mathbb{E}\int_0^T H_s^2 \, \mathrm{d}s \tag{6.5}$$

이다.

증명. $\Delta_i B = B_{t_{i+1}} - B_{t_i}$는 $\mathcal{F}_{t_i}$와 독립이고 평균 0이다. 따라서 $\mathbb{E}[H_i \Delta_i B] = \mathbb{E}H_i \, \mathbb{E}\Delta_i B = 0$이며, 각 항의 평균은 0이다. 또한

$$\mathbb{E}[H_i^2 (\Delta_i B)^2] = \mathbb{E}H_i^2 \, (t_{i+1} - t_i)$$

이다. $i < j$이면 $H_i \Delta_i B H_j$는 $\mathcal{F}_{t_j}$-가측이다. 마지막 증분 $\Delta_j B$의 조건부 평균이 0이므로 교차항

$$\mathbb{E}[H_i \Delta_i B H_j \Delta_j B] = \mathbb{E}\big[H_i \Delta_i B H_j \, \mathbb{E}[\Delta_j B \mid \mathcal{F}_{t_j}]\big] = 0$$

이다. 필요한 곱의 적분가능성은 각 항의 L^2 성질과 Cauchy–Schwarz 부등식으로 확보된다. 제곱을 전개하고 대각항을 더하면 결과를 얻는다. □

이 등식은 적분의 불안정성을 막는 정확한 노름 보존이다. 단순 과정 $H^{(m)}$이 어떤 H에 대해

$$\mathbb{E}\int_0^T \left| H_s^{(m)} - H_s \right|^2 \mathrm{d}s \longrightarrow 0$$

으로 수렴하면 적분도 L^2 Cauchy 수열이 된다. 그 극한을 $\int_0^T H_s \, \mathrm{d}B_s$로 정의한다. 예측가능하고 위의 제곱적분 조건을 만족하는 과정은 이런 단순 과정들로 근사할 수 있다는 밀도 정리를 사용한

다. 밀도 정리와 연속인 적분 과정의 구성 전체는 여기서 증명하지 않지만, 어떤 공간에서 극한을 취하는지는 분명하다.

이렇게 정의한 적분은 평균 0이고 등거리 관계를 만족한다. 시간 t까지의 적분은 연속인 제곱적분가능 마팅게일 버전을 갖는다. $\int_0^T H_s^2\,\mathrm{d}s < \infty$가 거의 확실하게만 성립하는 더 일반적인 경우에는 국소화를 이용한 국소 마팅게일 적분을 정의할 수 있으나, 기대값 0이 자동으로 따라오지는 않는다.

예제 6.8 (미래를 미리 사용하면 달라짐) $H_s = B_T$를 $0 < s \le T$에서 그대로 쓰려는 것은 일반적으로 예측가능하지 않다. 한 구간의 왼쪽 값이라는 규칙을 무시하고 $B_T(B_T - B_0) = B_T^2$를 만들면 기댓값이 T이다. 이것은 위에서 정의한 Itô 적분이 아니며, 제곱적분가능 Itô 적분의 평균 0 성질과 모순되지 않는다.

예제 6.9 (결정론적 피적분함수) $h \in L^2([0,T])$가 결정론적이면

$$\int_0^T h(s)\,\mathrm{d}B_s \sim N\!\left(0, \int_0^T h(s)^2\,\mathrm{d}s\right).$$

단순함수에서는 독립 정규 증분의 선형결합이다. 일반적인 h는 L^2 근사와 특성함수의 극한으로 확인한다. 분산이 0이면 상수 0인 퇴화 정규분포로 해석한다. 피적분함수가 확률적이면 이 정규분포 결론은 일반적으로 성립하지 않는다.

6.5 기본 적분과 Itô 보정항

명제 6.10 ($\int B\,\mathrm{d}B$)

$$\int_0^T B_s\,\mathrm{d}B_s = \frac{B_T^2 - T}{2}. \tag{6.6}$$

증명. 균등분할의 왼쪽 끝점 근사 $H_s^{(n)} = B_{(i-1)T/n}$를 $((i-1)T/n,\, iT/n]$에서 사용한다. 그러면

$$\mathbb{E}\int_0^T \left|B_s - H_s^{(n)}\right|^2 \mathrm{d}s = \sum_{i=1}^{n} \int_{(i-1)T/n}^{iT/n} \left(s - (i-1)T/n\right)\mathrm{d}s = \frac{T^2}{2n} \longrightarrow 0$$

이다. 한편 항등식 $(x+y)^2 - x^2 = 2xy + y^2$를 합하면

$$\sum_{i=1}^{n} B_{(i-1)T/n}\Delta_i B = \frac{1}{2}\left(B_T^2 - \sum_{i=1}^{n}(\Delta_i B)^2\right)$$

이다. 왼쪽은 Itô 등거리로 확률적분에 L^2 수렴하고, 오른쪽의 이차합은 T에 L^2 수렴한다. □

고전적 미분법의 $\int x\,\mathrm{d}x = x^2/2$에 비해 $-T/2$가 추가된다. 중점 방식으로 정의하는 Stratonovich 적분은 다른 보정 규칙을 갖는다. 따라서 두 적분의 기호나 공식을 가정 없이 섞어 쓰면 안 된다. 이 장의 모든 확률적분은 별도 표기가 없는 한 Itô 적분이다.

예제 6.11 $I_T = \int_0^T B_s\,\mathrm{d}B_s$의 평균은 0이고

$$\operatorname{Var}(I_T) = \int_0^T \mathbb{E}B_s^2\,\mathrm{d}s = \int_0^T s\,\mathrm{d}s = \frac{T^2}{2}.$$

또한 $I_T \geq -T/2$이므로 비퇴화 정규분포일 수 없다. 확률적 피적분함수에 대해 "Brownian 적분이니 항상 정규분포"라고 결론낼 수 없다는 구체적인 반례이다.

6.6 Itô 공식

정리 6.12 (일차원 Brownian 운동의 Itô 공식) $f(t,x)$가 시간에 대해 한 번, 공간에 대해 두 번 연속미분가능한 함수, 즉 $C^{1,2}$ 함수이면

$$f(t,B_t) - f(0,B_0) = \int_0^t \partial_s f(s,B_s)\,\mathrm{d}s + \int_0^t \partial_x f(s,B_s)\,\mathrm{d}B_s + \frac{1}{2}\int_0^t \partial_{xx} f(s,B_s)\,\mathrm{d}s \tag{6.7}$$

이다.

일반적인 $C^{1,2}$ 함수에서 확률적분은 필요에 따라 국소화하여 해석한다. 그 적분의 기대값을 0으로 놓으려면, 예를 들어 $\mathbb{E}\int_0^t |\partial_x f(s,B_s)|^2\,\mathrm{d}s < \infty$ 같은 충분조건을 확인해야 한다.

증명의 핵심 구조. 분할의 각 구간에서 시간에 대해 일차, 공간에 대해 이차 Taylor 전개를 한다. 공간 일차항은 왼쪽 끝점 Itô 합이고, 공간 이차항은 $\frac{1}{2}f_{xx}(\Delta B)^2$이다. 이차변동 때문에 이 항이 사라지지 않고 시간 적분으로 남는다. 시간과 공간의 혼합 나머지 및 고차항의 제어에는 국소화와 확률적 수렴 추정이 필요하다. 이 설명은 공식의 유도 구조이며 일반 $C^{1,2}$ 경우의 완전한 증명을 대신하지 않는다. 앞 절의 $f(x)=x^2$ 사례는 실제 L^2 극한으로 직접 증명했다.

예제 6.13 (지수 마팅게일) 상수 $\theta \in \mathbb{R}$에 대해

$$Z_t = \exp\!\left(\theta B_t - \frac{\theta^2 t}{2}\right)$$

로 두면 Itô 공식에서 시간항과 이차미분항이 상쇄되어 $\mathrm{d}Z_t = \theta Z_t\,\mathrm{d}B_t$이다. ($f(t,x)=e^{\theta x-\theta^2 t/2}$에서 $f_t=-\frac{\theta^2}{2}f$, $f_x=\theta f$, $f_{xx}=\theta^2 f$이므로 $f_t+\frac{1}{2}f_{xx}=0$이다.) 국소 마팅게일이라는 결론만으로 멈추지 않고, 독립 증분과 정규 적률생성함수로

$$\mathbb{E}[Z_t \mid \mathcal{F}_s] = Z_s\,\mathbb{E}\exp\!\left(\theta(B_t-B_s) - \frac{\theta^2(t-s)}{2}\right) = Z_s$$

을 직접 확인할 수 있다. 따라서 Z_t는 실제 마팅게일이고 $\mathbb{E}Z_t = 1$이다.

예제 6.14 (시간을 뺀 제곱) $f(t,x)=x^2-t$이면 $f_t=-1$, $f_x=2x$, $f_{xx}=2$이므로

$$\mathrm{d}(B_t^2 - t) = 2B_t\,\mathrm{d}B_t$$

이다. 제곱적분 조건 $\mathbb{E}\int_0^T (2B_s)^2\,\mathrm{d}s = 2T^2 < \infty$가 성립하므로 오른쪽은 평균 0인 마팅게일 적분이다.

예제 6.15 (네제곱과 4차 모멘트) $f(x)=x^4$이면 $f'=4x^3$, $f''=12x^2$이므로 $\mathrm{d}(B_t^4) = 4B_t^3\,\mathrm{d}B_t + 6B_t^2\,\mathrm{d}t$이다. $\mathbb{E}\int_0^t B_s^6\,\mathrm{d}s < \infty$이므로 확률적분의 평균은 0이고

$$\mathbb{E}B_t^4 = 6\int_0^t \mathbb{E}B_s^2\,\mathrm{d}s = 6\int_0^t s\,\mathrm{d}s = 3t^2$$

이다. 이는 식 (6.1)의 정규 모멘트와 일치한다.

6.7 확률미분방정식의 의미와 해의 조건

기호

$$\mathrm{d}X_t = b(t, X_t)\ \mathrm{d}t + \sigma(t, X_t)\ \mathrm{d}B_t, \qquad X_0 = \xi \tag{6.8}$$

는 다음 적분방정식을 줄여 쓴 것이다.

$$X_t = \xi + \int_0^t b(s, X_s)\ \mathrm{d}s + \int_0^t \sigma(s, X_s)\ \mathrm{d}B_s.$$

"Brownian 경로를 미분한 함수"를 오른쪽에 대입하는 통상 미분방정식으로 이해하지 않는다. 첫 적분은 시간에 대한 Lebesgue 적분이고 둘째가 Itô 적분이다.

이러한 **Itô 과정**(*Itô process*)에 대해 $f \in C^{1,2}$이면 공식은

$$\mathrm{d}f(t, X_t) = \left(\partial_t f + b(t, X_t)\,\partial_x f + \frac{1}{2}\sigma(t, X_t)^2\,\partial_{xx} f\right)\mathrm{d}t + \sigma(t, X_t)\,\partial_x f\ \mathrm{d}B_t \tag{6.9}$$

로 확장된다. 모든 도함수는 (t, X_t)에서 평가한다. 이는 적분형 등식의 약기이며, 원래 과정의 적분이 정의되고 필요한 국소 적분가능성이 성립하는 범위에서 사용한다. 함수가 열린 구간에서만 정의되면 그 구간을 벗어나기 전까지 국소화한다. 특히 로그함수는 양의 해에 대해 사용한다. 기대값을 취해 확률적분을 없애려면 앞 절처럼 참 마팅게일이 되는 적분가능성 조건을 따로 확인한다.

정리 6.16 (전역 Lipschitz 조건 아래 강한 해) 각 유한한 T에 대하여 $b, \sigma : [0,T] \times \mathbb{R} \to \mathbb{R}$가 가측이고, 어떤 유한 상수 L_T, K_T가 모든 $t \in [0,T]$, $x, y \in \mathbb{R}$에 대해

$$|b(t,x) - b(t,y)| + |\sigma(t,x) - \sigma(t,y)| \le L_T\,|x - y|,$$

$$|b(t,x)|^2 + |\sigma(t,x)|^2 \le K_T(1 + |x|^2)$$

을 만족한다고 하자. ξ는 $\mathcal{F}_0$-가측이고 $\mathbb{E}\,|\xi|^2 < \infty$라고 하자. 주어진 여과에 대한 Brownian 운동을 사용하면 적분방정식은 연속인 적응 강한 해를 가지며,

$$\mathbb{E}\sup_{0 \le t \le T} |X_t|^2 < \infty$$

이다. 같은 Brownian 운동과 같은 초기값을 쓰는 연속 적응 해들은 거의 확실하게 모든 시점에서 일치한다.

강한 해란 주어진 확률공간과 Brownian 운동 위에서 해를 구성한다는 의미이다. 강하다는 말이 큰 크기나 높은 정밀도를 뜻하지 않는다. 이 정리에서 $\mathcal{F}_0$의 초기정보와 미래 Brownian 증분의 독립성은 앞서 정한 Brownian 여과 가정에 포함되어 있다.

증명에 쓰이는 도구. Picard 반복으로 이전 근사를 계수에 대입한다. 시간 적분은 Cauchy–Schwarz, 확률적분은 Itô 등거리와 최대 부등식으로 제어한다. Lipschitz 추정과 Grönwall 부등식으로 수렴 및 경로별 유일성을 얻는다. 반복과 연속 버전의 전체 구성은 이 입문 장의 범위 밖이다. 아래의 두 선형 예제는 해를 직접 쓰고 Itô 공식으로 대입 검산할 수 있다.

전역 Lipschitz 조건은 편리한 충분조건이다. 이를 만족하지 않는 계수라고 곧바로 해가 없다고 결론낼 수 없다. 반대로 국소 Lipschitz만 확인했다면 유한 시간 폭발 가능성과 경계에서의 정의를 별도로 살펴야 한다.

예제 6.17 (선형 증가 조건이 깨질 때) $\sigma = 0$, $b(x) = x^2$, $x_0 = 1$이면 방정식은 상미분방정식 $x' = x^2$이고 해는 $x(t) = 1/(1-t)$이다. 이 해는 $t = 1$에서 폭발한다. b는 국소 Lipschitz이지만 전역 Lipschitz도 선형 증가도 아니므로 정리 6.16의 해가 $[0, T]$ 전체에서 존재한다고 말할 수 없다.

6.8 기하 Brownian 운동

상수 $\mu, \sigma \in \mathbb{R}$, $x_0 > 0$에 대하여

$$\mathrm{d}X_t = \mu X_t \,\mathrm{d}t + \sigma X_t \,\mathrm{d}B_t, \qquad X_0 = x_0 \tag{6.10}$$

의 해는

$$X_t = x_0 \exp\left[\left(\mu - \frac{\sigma^2}{2}\right)t + \sigma B_t\right] \tag{6.11}$$

이다. 지수함수에 Itô 공식을 적용하면 공간 이차미분항 $\sigma^2 X_t/2$가 시간지수의 $-\sigma^2/2$와 상쇄된다. 실제로 $f(t,x) = x_0 \exp[(\mu - \sigma^2/2)t + \sigma x]$에서 $f_t = (\mu - \sigma^2/2) f$, $f_x = \sigma f$, $f_{xx} = \sigma^2 f$이므로

$$\mathrm{d}X_t = \left[\left(\mu - \tfrac{\sigma^2}{2}\right) + \tfrac{\sigma^2}{2}\right] X_t \,\mathrm{d}t + \sigma X_t \,\mathrm{d}B_t = \mu X_t \,\mathrm{d}t + \sigma X_t \,\mathrm{d}B_t$$

이다. 계수는 전역 Lipschitz이므로 대입하여 찾은 해가 유일하다.

$$\mathbb{E}X_t = x_0 e^{\mu t}, \qquad \operatorname{Var}(X_t) = x_0^2 e^{2\mu t}\left(e^{\sigma^2 t} - 1\right). \tag{6.12}$$

이는 정규 적률생성함수 $\mathbb{E}e^{\lambda B_t} = e^{\lambda^2 t/2}$로 계산한다. $\lambda = \sigma$일 때 $\mathbb{E}X_t = x_0 e^{(\mu - \sigma^2/2)t} e^{\sigma^2 t/2} = x_0 e^{\mu t}$이고, $\lambda = 2\sigma$일 때 $\mathbb{E}X_t^2 = x_0^2 e^{(2\mu - \sigma^2)t} e^{2\sigma^2 t} = x_0^2 e^{2\mu t + \sigma^2 t}$이므로 평균의 제곱을 빼면 분산을 얻는다. 로그값의 평균 변화율은 $\mu - \sigma^2/2$이고 원래 값의 평균 성장률 매개변수는 μ이다. 서로 다른 양을 구분해야 한다. 로그값이 정규분포라는 이유로 원래 X_t도 정규분포라고 해석해서는 안 된다 (X_t는 로그정규분포를 따른다).

예제 6.18 $\mu = 0$, $\sigma = 1$, $x_0 = 1$이면 $\mathbb{E}X_t = 1$이지만 $\mathbb{E}\log X_t = -t/2$이다. $t = 1$에서 중앙값은 $e^{-1/2} \approx 0.606531$이고 분산은 $e - 1 \approx 1.718282$이다. 기대값이 일정하다는 것이 전형적인 경로값이나 중앙값이 일정하다는 뜻은 아니다.

6.9 Ornstein–Uhlenbeck 과정

$\kappa > 0$, $m, \sigma \in \mathbb{R}$에 대해

$$\mathrm{d}X_t = -\kappa(X_t - m)\,\mathrm{d}t + \sigma \,\mathrm{d}B_t \tag{6.13}$$

를 생각하자. 결정론적 적분인자 $e^{\kappa t}$를 사용하면, $f(t,x) = e^{\kappa t}(x - m)$에 식 (6.9)를 적용하여 $f_t = \kappa f$, $f_x = e^{\kappa t}$, $f_{xx} = 0$이므로

$$\mathrm{d}\big(e^{\kappa t}(X_t - m)\big) = \kappa e^{\kappa t}(X_t - m)\,\mathrm{d}t + e^{\kappa t}\big(-\kappa(X_t - m)\,\mathrm{d}t + \sigma\,\mathrm{d}B_t\big) = \sigma e^{\kappa t}\,\mathrm{d}B_t$$

이고 양변을 적분하면

$$X_t = m + (X_0 - m)e^{-\kappa t} + \sigma \int_0^t e^{-\kappa(t-s)}\,\mathrm{d}B_s \tag{6.14}$$

를 얻는다. 확률적분의 지수핵은 고정된 최종 시점 t에 대해 결정론적이다. $X_0 = x$가 상수일 때 분포는 정규이며

$$\mathbb{E}X_t = m + (x-m)e^{-\kappa t}, \qquad \operatorname{Var}(X_t) = \frac{\sigma^2}{2\kappa}\bigl(1 - e^{-2\kappa t}\bigr). \tag{6.15}$$

분산은 Itô 등거리로 $\sigma^2 \int_0^t e^{-2\kappa(t-s)}\,\mathrm{d}s$를 계산한 것이다.

초기값을 미래 Brownian 운동과 독립인 $N(m, \sigma^2/(2\kappa))$로 선택하면 모든 시점에서 같은 정규분포를 갖는다. 더 나아가 공동정규성과

$$\operatorname{Cov}(X_s, X_t) = \frac{\sigma^2}{2\kappa} e^{-\kappa|t-s|} \tag{6.16}$$

로 엄격 정상성을 얻는다. ($s \le t$에서 $X_t - m = e^{-\kappa(t-s)}(X_s - m) + \sigma\int_s^t e^{-\kappa(t-u)}\,\mathrm{d}B_u$이고 둘째 항이 $\mathcal{F}_s$와 독립이므로 $\operatorname{Cov}(X_s, X_t) = e^{-\kappa(t-s)}\operatorname{Var}(X_s)$이다.) 초기값을 상수로 둔 과정은 분산이 위처럼 변하므로 처음부터 정상인 과정은 아니다. 장시간 분포의 수렴과 모든 시점에서의 정상성은 서로 다른 말이다.

> **예제 6.19** $\kappa = 2$, $\sigma = 3$이면 정상분산은 $9/4$이다. 고정 초기값에서 t의 분산은 $(9/4)(1 - e^{-4t})$이며, 초기 평균과 장기 평균의 차이는 e^{-2t} 비율로 감소한다. 평균 회복 속도와 분산 회복의 지수에 각각 $2, 4$가 나타나는 이유는 분산 계산에서 핵을 제곱하기 때문이다.

6.10 격자 계산과 실제 해의 차이

등간격 $\Delta > 0$에서 **Euler–Maruyama 근사**(*Euler–Maruyama scheme*)는

$$X_{k+1}^{(\Delta)} = X_k^{(\Delta)} + b\bigl(k\Delta, X_k^{(\Delta)}\bigr)\Delta + \sigma\bigl(k\Delta, X_k^{(\Delta)}\bigr)\sqrt{\Delta}\,Z_{k+1} \tag{6.17}$$

로 쓴다. Z_k는 독립 표준정규이며 이전 근사값들과 독립인 새 잡음을 사용한다. $\sqrt{\Delta}Z_{k+1}$의 분산이 Δ인 것이 Brownian 증분의 스케일이다.

Brownian 값 자체는 이 격자에서 정확한 결합분포를 생성하지만, 비상수 계수 SDE의 Euler 근사는 일반적으로 정확한 해가 아니다. 수렴을 주장하려면 계수의 공간·시간 정칙성, 모멘트, 사용하는 오차 노름을 명시해야 한다. 여기서는 포괄적인 수렴률을 가정 없이 제시하지 않는다.

> **예제 6.20 (양수성이 보존되지 않는 근사)** $\mathrm{d}X_t = X_t\,\mathrm{d}B_t$, $X_0 = 1$에서 정확한 해는 $\exp(B_t - t/2) > 0$이다. 한 단계 $\Delta = 1$ Euler 근사는 $1 + Z_1$이므로 $Z_1 < -1$이면 음수가 된다. 예를 들어 표본값 $Z_1 = -2$에 대응하는 근사값은 -1이고, 같은 증분을 사용한 정확한 시점 1 값은 $e^{-5/2} > 0$이다. 하나의 격자 근사가 해의 구조를 보존하는지도 따로 검토해야 한다.

6.11 연습문제와 해설

> **연습문제 6.21** $\int_0^T s\,\mathrm{d}B_s$의 분포를 구하라.

풀이. 피적분함수가 결정론적이고 제곱적분가능하므로 평균 0, 분산 $\int_0^T s^2\,\mathrm{d}s = T^3/3$인 정규분포이다. $\int_0^T s\,\mathrm{d}s = T^2/2$를 분산으로 쓰면 적분의 등거리에서 제곱을 빠뜨린 것이다.

연습문제 6.22 $\int_0^T B_s \, dB_s$가 평균 0이면서 정규분포가 아닌 이유를 식으로 설명하라.

풀이. $(B_T^2 - T)/2$와 같고 평균은 0이다. $T > 0$이면 분산 $T^2/2 > 0$인데 하한 $-T/2$를 갖는다. 비퇴화 정규분포는 모든 실수 구간에 양의 확률을 주므로 이 분포와 다르다.

연습문제 6.23 $s < t$에서 $\mathbb{E}[(B_t - B_s)^4 \mid \mathcal{F}_s]$를 구하라.

풀이. 증분은 $\mathcal{F}_s$와 독립인 $N(0, t-s)$이다. 표준정규의 4차 모멘트가 3이므로 답은 $3(t-s)^2$이다. 이는 조건부기대가 확률변수 대신 상수가 되는 독립성의 사용 사례이다.

연습문제 6.24 기하 Brownian 운동에서 $d(\log X_t)$를 계산하라.

풀이. $X_t > 0$이고 $f'(x) = 1/x$, $f''(x) = -1/x^2$이다. 일반 Itô 과정에 대한 공식으로

$$d(\log X_t) = \left(\mu - \frac{\sigma^2}{2}\right) dt + \sigma \, dB_t$$

를 얻는다. 또는 이미 검산한 명시적 해에 로그를 취해 같은 식을 얻을 수 있다. 보정항을 빼먹으면 원래 SDE에 다시 대입했을 때 drift가 일치하지 않는다.

연습문제 6.25 OU 과정의 고정 초기값 분산식을 $\kappa \downarrow 0$으로 보낼 때 무엇을 얻는가? m은 고정한다.

풀이. $(1 - e^{-2\kappa t})/(2\kappa) \to t$이므로 분산은 $\sigma^2 t$에 접근한다. 평균은 $m + (x-m)e^{-\kappa t} \to x$이다. drift가 사라지는 극한에서 $x + \sigma B_t$의 평균과 분산을 회복한다. 정상분산 $\sigma^2/(2\kappa)$의 극한과 고정 초기값의 유한시간 분산 극한은 서로 다른 문제이다.

연습문제 6.26 균등 n분할 이차합 Q_n의 표준편차와 평균 대비 상대 표준편차를 구하라.

풀이. 표준편차는 $\sqrt{2}\,T/\sqrt{n}$, 평균 $T > 0$에 대한 상대 표준편차는 $\sqrt{2/n}$이다. $n = 200$이면 상대 표준편차는 0.1이다. 이 유한 분할의 변동이 0이 아니므로 시뮬레이션 한 번에서 이차합이 정확히 T가 되어야 한다고 기대하면 안 된다.

참고 (다음 연결). 이 권의 출발점은 경로와 분포의 구분이며, 마지막 계산에서도 그 구분이 유지된다. 더 깊은 이론에서는 생성자, 강한 Markov 성질, 연속시간 Markov 연쇄, 재생과정, 마팅게일 수렴, Girsanov 정리, 확산과 편미분방정식의 연결을 다룬다. 이 첫 원고는 그 일반 이론의 완성을 주장하지 않고, 정의와 가정 및 직접 검산 가능한 기본 사례를 확립한다.

제 22 권

수리통계·추론

제22권은 관측자료로부터 모집단의 성질을 추론하는 수리통계의 기초를 확률론 위에서 세운다. 제1장은 통계적 모형, 표본, 추정대상을 정하고, 제2–3장은 점추정의 편향과 평균제곱오차, 우도함수와 최대우도추정과 충분성을 다룬다. 제4–5장은 신뢰구간과 예측구간, 가설검정과 검정력과 다중검정으로 추론의 불확실성을 정량화하는 빈도주의의 방법을 다룬다. 제6장은 사전분포를 Bayes 공식으로 사후분포로 갱신하는 베이지안 추론의 기본을 다룬다.

제 1 장

통계적 모형, 표본, 추정대상

개요 통계적 모형(*statistical model*)은 관측자료 X가 따를 수 있는 확률분포들의 집합이고, 추정대상(*estimand*)은 그 모형 안에서 알고 싶은 분포의 특성이다. 이 장은 통계모형과 모수공간, 표본과 모집단, 독립 동일분포 가정, 식별가능성, 통계량·추정량·추정값의 구별, 경험분포와 플러그인 원리, 추론 절차의 평가 기준을 정의하고 그 한계를 예제로 보인다. 확률론에서는 분포가 주어졌을 때 확률과 기댓값을 계산하지만, 통계학에서는 자료에서 미지의 분포 특성을 알아내야 하므로 표본추출 과정, 모형, 추정대상, 오차 기준을 함께 지정해야 한다. 선행 지식: 확률분포, 기댓값과 분산, 조건부 확률(제20권 제4장, 제20권 제5장, 제20권 제3장). 확률론에서 분포가 주어졌을 때 계산하던 문제를 자료에서 미지의 분포 특성을 알아내는 문제로 전환한다.

통계학은 관측 자료가 알려 주는 것과 알려 주지 않는 것을 구별한다. 확률론에서는 성공확률 p가 주어졌을 때 n번 중 k번 성공할 확률을 구한다. 통계학에서는 실제 성공 횟수를 보고 p를 추정하고, 그 추정의 오차를 평가한다. 하나의 관측값으로 미지의 참값이 자동으로 정해지지 않기 때문에 표본추출 과정, 모형, 추정대상, 손실이나 오차 기준을 함께 지정해야 한다.

1.1 확률모형의 집합으로서의 통계모형

정의 1.1 (통계모형) 관측자료 X의 가능한 분포들의 집합

$$\mathcal{P} = \{P_\theta : \theta \in \Theta\} \tag{1.1}$$

을 **통계모형**(*statistical model*)이라 한다. Θ는 **모수공간**(*parameter space*)이고 θ는 **모수**(*parameter*)이다. 유한 차원의 θ로 표현하는 모형을 **모수모형**(*parametric model*)이라고 한다. **추정대상**은 $g(\theta)$ 또는 분포의 함수 $T(P)$처럼 명시한다.

예를 들어 독립 Bernoulli 표본에서는 $\theta = p \in [0,1]$이고 관측자료는 $X = (X_1, \dots, X_n)$이다. 이때 결합분포는 $P_p(X = x) = p^{\sum x_i}(1-p)^{n - \sum x_i}$이다. 정규모형에서는 $\theta = (\mu, \sigma^2)$이고 $\mu \in \mathbb{R}$, $\sigma^2 > 0$이다. 평균을 추정할 때 관심모수는 μ이며 분산은 **방해모수**(*nuisance parameter*)일 수 있다. 방해모수는 중요하지 않은 변수가 아니라 현재의 목표와 직접 일치하지 않는 미지수라는 뜻이다.

"자료가 정규분포를 따른다"는 가정은 실제 측정이 연속값인지, 이상값이 있는지, 관측이 독립인지와 별개로 확인해야 한다. 주변분포만 정규이고 관측들이 강하게 의존하면 독립 정규표본의 표준오차를 사용할 수 없다. 또한 모형 밖의 실제 자료에 대해 모형 안에서 증명된 보장을 자동으로 주장하지 않는다.

예제 1.2 (같은 숫자를 만드는 다른 모형) 100개 제품에서 불량 8개를 관측했다고 하자. 각 제품이 독립이고 공통 불량확률 p를 가지면 성공 개수는 $\mathrm{Bin}(100, p)$로 모델링할 수 있다. 이미

정해진 N개 로트에서 비복원 추출했다면 미지의 불량 총개수 K를 갖는 초기하모형이 더 직접적이다. 관측 숫자는 같아도 변동의 원인과 추정대상이 다르다. 전자의 추정대상은 p, 후자는 K 또는 불량률 K/N이며, 후자에서 불량 개수의 분산은 $np(1-p)\,\frac{N-n}{N-1}$ 꼴로 이항분산보다 작다 ($p = K/N$).

1.2 표본추출과 독립 동일분포 가정

정의 1.3 (독립 동일분포 표본) $X_1, \dots, X_n$이 독립이고 모두 같은 분포 P를 따르면 **독립 동일분포 표본**(*i.i.d. sample*)이라고 한다. 약자로 i.i.d.를 사용한다. 이는 개별 관측의 분포뿐 아니라 관측들 사이의 결합분포까지 지정하는 가정이다.

독립 동일분포는 계산에 편리하지만 모든 "무작위 표본"이 그 의미로 독립인 것은 아니다. 유한 모집단의 단순무작위 비복원 표본은 관측들이 의존한다. 시간에 따라 측정한 센서값에는 자기상관이 있을 수 있다. 한 사람을 여러 번 측정하면 사람 사이와 사람 안의 변동을 구분해야 한다. 관측 수가 많다는 사실만으로 독립적인 정보가 같은 비율로 늘어나지 않는다.

모집단(*population*)은 결론을 적용하려는 대상들의 집합 또는 자료생성 분포이다. **표본**(*sample*)은 그중 실제 관측한 부분이다. 표본이 많더라도 모집단과 체계적으로 다른 방식으로 선택되면 표본오차가 작아지는 것과 선택편향이 줄어드는 것은 별개의 문제이다.

예제 1.4 (집단 비중을 무시한 평균) 모집단의 20%가 집단 A, 80%가 집단 B이며 어떤 성공률이 각각 0.9, 0.5라고 하자. 모집단 성공률은

$$0.2(0.9) + 0.8(0.5) = 0.58.$$

두 집단에서 같은 수를 모집한 자료의 단순 평균은 큰 표본에서 0.7에 가까워진다. $(0.9+0.5)/2 = 0.7$이기 때문이다. 추정하려는 대상이 모집단 평균이라면 알려진 모집단 비중을 사용한 가중이 필요하다. 모집단 비중을 모르면 자료만으로 해결되지 않는 정보 부족이 남을 수 있다.

실험에서 처치를 무작위 배정하는 일과 사람들을 모집단에서 무작위 추출하는 일도 다르다. 전자는 집단 간 인과 비교의 내부 타당성을 돕고, 후자는 모집단으로의 일반화와 관련된다. 자원자를 모집한 뒤 처치를 무작위 배정한 실험은 두 질문에 서로 다른 답을 줄 수 있다.

1.3 추정대상과 식별가능성

평균, 중앙값, 분산, 상관계수, 상위 분위수, 특정 사건의 확률은 각각 다른 추정대상이다. 무엇을 알고 싶은지 정하지 않은 채 "자료의 대표값"을 계산하면 의사결정 목적과 어긋날 수 있다. 이상값에 민감한 평균과 중앙값은 같은 질문에 대한 교환 가능한 답이 아니다.

정의 1.5 (식별가능성) 모수모형이 $P_{\theta_1} = P_{\theta_2}$이면 반드시 $\theta_1 = \theta_2$를 만족할 때 **식별가능**(*identifiable*)하다고 한다. 모수 전체가 식별되지 않아도 추정대상 $g(\theta)$가 같은 분포들 사이에서 같은 값을 가지면 그 추정대상은 식별가능할 수 있다.

예제 1.6 (부호를 식별하지 못하는 모형) $X_i \sim \mathrm{Bern}(\theta^2)$, $\theta \in [-1, 1]$인 독립표본을 생각하자. θ와 $-\theta$는 정확히 같은 자료분포를 만든다. 표본을 무한히 늘려도 부호를 구별할 수 없다. 그러나

θ^2과 $|\theta|$는 식별가능하다. 모수공간을 $[0,1]$로 제한하면 θ 자체도 식별된다. 이는 계산법을 바꾼 결과가 아니라 모형의 가정을 바꾼 결과다.

식별 문제와 추정 정밀도의 문제는 다르다. 식별가능한 모수도 표본이 작으면 추정이 부정확할 수 있다. 식별되지 않는 모수는 계산 능력이나 표본 크기만 늘려 해결할 수 없다. 원인과 결과를 자료에서 추정할 때에는 교란, 선택, 측정오차에 관한 추가 가정이 식별의 핵심이 된다.

1.4 통계량, 추정량, 관측값

정의 1.7 (통계량, 추정량, 추정값) **통계량**(*statistic*)은 자료의 가측함수 $T(X_1,\dots,X_n)$이며, 계산식에 미지의 모수를 넣지 않는다. **추정량**(*estimator*)은 특정 추정대상을 추정하기 위해 사용하는 통계량이다. 실제 자료 x를 넣은 숫자 $T(x)$는 **추정값**(*estimate*)이다.

$\overline{X}_n = n^{-1}\sum_{i} X_i$는 관측 전에는 확률변수이고 관측 후에는 하나의 숫자다. 표본평균의 **표본분포**(*sampling distribution*)는 반복적으로 표본을 뽑을 때 그 숫자가 어떻게 변하는지 나타낸다. 이것은 모집단에서 개별 관측 하나의 분포와 다르다. 예를 들어 독립 $N(\mu,\sigma^2)$ 표본에서는

$$X_i \sim N(\mu,\sigma^2), \qquad \overline{X}_n \sim N(\mu,\sigma^2/n).$$

독립 동일분포이고 분산이 유한하면 일반 분포에서도 $\mathbb{E}\overline{X}_n=\mu$, $\operatorname{Var}(\overline{X}_n)=n^{-2}\sum_i \operatorname{Var}(X_i)=\sigma^2/n$이며, 정규성은 정확한 정규분포를 말하는 데에만 필요하다. 데이터의 표준편차와 평균의 표준오차는 같은 양이 아니다.

예제 1.8 (Bernoulli 표본의 세 수준) 자료가 $x=(1,0,1,1,0)$이면 성공 개수의 관측값은 $s=3$이고 표본비율은 0.6이다. 관측 전의 $S=\sum_i X_i$는 $\mathrm{Bin}(5,p)$를 따르는 통계량이다. 그 기댓값 $5p$와 표본비율의 표준편차 $\sqrt{p(1-p)/5}$는 미지의 p에 의존하는 이론적 특성이다. p 대신 0.6을 넣은 값은 또 하나의 추정량으로 구성한 표준오차 추정값이다. 여기서는 $\sqrt{0.6\cdot 0.4/5}=\sqrt{0.048}\approx 0.219$이다.

1.5 경험분포와 플러그인 원리

정의 1.9 (경험분포함수) 실수 자료 $X_1,\dots,X_n$의 **경험분포함수**(*empirical distribution function*)는

$$F_n(x)=\frac{1}{n}\sum_{i=1}^{n}\mathbf{1}_{\{X_i\le x\}} \tag{1.2}$$

이다. 각 관측점에 질량 $1/n$을 둔 경험분포를 P_n이라고 한다.

중복된 관측점에서는 질량들이 더해진다. 경험분포는 연속 모집단에서 얻은 표본이어도 이산분포이다. 모집단 분포 P의 함수 $T(P)$에 P_n을 대신 넣는 것이 **플러그인 원리**(*plug-in principle*)다. 평균에는 표본평균이, 이차 중심모멘트에는 분모 n인 표본분산이 나온다. 분모 $n-1$인 불편표본분산은 플러그인 값에 $n/(n-1)$을 곱하여 편향을 보정한 것이다.

예제 1.10 자료 $1,2,2,5$의 경험분포는 1에 $1/4$, 2에 $1/2$, 5에 $1/4$의 질량을 준다. 따라서

$F_n(2)=3/4$, 플러그인 평균은 2.5이다. 경험분포의 분산은

$$\frac{(1-2.5)^2+2(2-2.5)^2+(5-2.5)^2}{4}=2.25.$$

분모 $n-1$의 표본분산은 3이다$(2.25\cdot 4/3=3)$. 두 수는 서로 다른 정의와 목적을 가진다.

독립 동일분포 아래에서 고정된 x에 대한 $F_n(x)$는 평균이 $F(x)$인 Bernoulli 평균이므로 큰수법칙으로 수렴한다(제20권 제11장). 분산은 $F(x)(1-F(x))/n$이다. 모든 x에 대한 균등수렴은 **Glivenko–Cantelli 정리**라는 더 강한 명제이며, 고정점 수렴만으로 즉시 대신할 수 없다.

1.6 추론 절차와 평가 기준

점추정은 하나의 값을, 구간추정은 불확실성을 반영한 값들의 범위를, 검정은 미리 정한 오류 기준 아래 귀무가설에 반하는 증거를 평가한다. 예측은 새 관측값의 분포를 다루며 모수의 불확실성뿐 아니라 새 관측 자체의 변동을 포함한다. 같은 자료에서도 목표가 다르면 필요한 분산이 달라진다.

빈도주의적 평가는 각 고정된 참모수 아래에서 절차를 반복 적용할 때의 성능을 본다. 베이지안 분석은 모수에 사전분포를 두고 관측 후 사후분포로 불확실성을 표현한다. 두 접근을 비교할 때는 서로 다른 확률의 대상을 섞지 않는다. 예를 들어 신뢰구간의 포함확률과 사후 신용구간의 확률은 같은 해석을 자동으로 갖지 않는다.

흔한 오류 (모형·계산·추론을 섞음). 모형의 가정, 자료에서 계산한 사실, 그 가정 아래 도출한 추론을 따로 적는다. 관측자료가 하나의 모형과 잘 맞는다는 이유로 그 모형이 유일하게 참이라고 입증된 것은 아니다. 검정에서 기각되지 않았다는 말도 모형이 증명되었다는 뜻이 아니다.

1.7 연습문제와 해설

연습문제 1.11 독립 $N(\mu,4)$ 표본 25개에서 평균을 추정한다. 개별 관측의 표준편차와 표본평균의 표준편차를 구별하라.

풀이. 각각 2와 $2/\sqrt{25}=0.4$이다. 자료가 흩어진 정도와 추정량이 반복표본에서 흩어진 정도의 차이이다.

연습문제 1.12 $X\sim N(\theta_1+\theta_2,1)$에서 $(\theta_1,\theta_2)\in\mathbb{R}^2$이다. 두 모수는 식별되는가? 어떤 선형함수는 식별되는가?

풀이. 합이 같은 모수쌍은 같은 분포를 만들므로 전체 쌍은 식별되지 않는다. 합 $\theta_1+\theta_2$와 그 상수배는 식별된다. 차이는 자료분포가 구별하지 못한다.

연습문제 1.13 자료 $0,0,1,3,3$의 $F_n(0)$, $F_n(2)$, 플러그인 평균을 구하라.

풀이. 각각 $2/5$, $3/5$, $7/5$이다. 경험분포는 관측값 사이에서 일정하고 관측점에서 우연속인 계단함수다.

연습문제 1.14 독립표본을 가정한 평균의 표준오차를 하루마다 측정한 강한 자기상관 자료에 그대로 적용할 때의 문제를 설명하라.

풀이. 평균의 분산에는 $2\sum_{i<j}\operatorname{Cov}(X_i,X_j)/n^2$가 포함된다. 이를 0으로 두는 독립 공식은 양의 자기상관에서 불확실성을 과소평가할 수 있다. 모집단 분산만 추정한다고 이 문제가 해결되지 않는다.

참고 (다음 연결). 추정대상과 자료생성 모형이 정해져야 추정량의 성능을 비교할 수 있다. 다음 장은 편향, 분산, 평균제곱오차, 일관성을 각각 정의하고 서로 다른 역할을 설명한다.

제 2 장

점추정, 편향, 평균제곱오차

개요 점추정(*point estimation*)은 미지의 추정대상 $g(\theta)$에 하나의 값을 대응시키는 추정량 T를 고르는 일이며, 편향은 T의 평균이 참값에서 벗어나는 정도, 평균제곱오차는 제곱손실의 평균 위험이다. 이 장은 편향과 평균제곱오차를 정의하고 편향–분산 분해를 증명하며, 표본평균과 표본분산의 불편성, 일관성과 불편성의 독립성, 정칙 모형에서의 Fisher 정보량과 Cramér–Rao 하계, 그리고 하계가 적용되지 않는 균등분포의 끝점 추정을 다룬다. 요점은 좋은 추정량을 하나의 수식으로 보편적으로 정할 수 없고, 불편성·분산·일관성·위험이 서로 연결되지만 동치가 아니라는 것이다. 선행 지식: 기댓값과 분산, 조건부 기댓값, 큰수법칙(제20권 제5장, 제20권 제8장, 제20권 제11장). 성능은 고정된 참모수 θ 아래에서 평가하며 기댓값에 필요하면 첨자 θ를 붙인다.

좋은 추정량을 하나의 수식으로 보편적으로 정할 수는 없다. 평균적으로 참값을 맞추는지, 반복표본에서 얼마나 흔들리는지, 큰 표본에서 참값으로 수렴하는지, 특정 손실에서 위험이 작은지를 구별해야 한다. 이 기준들은 서로 연결되지만 동치가 아니다.

2.1 편향과 위험의 분해

정의 2.1 (편향과 평균제곱오차) 추정대상 $g(\theta)$의 추정량 T에 대해

$$b_\theta(T) = \mathbb{E}_\theta T - g(\theta) \tag{2.1}$$

를 **편향**(*bias*)이라 한다. 모든 $\theta \in \Theta$에서 편향이 0이면 **불편추정량**(*unbiased estimator*)이다. 제곱손실의 위험, 즉 **평균제곱오차**(*mean squared error*)는

$$\mathrm{MSE}_\theta(T) = \mathbb{E}_\theta\left[(T - g(\theta))^2\right] \tag{2.2}$$

이다.

명제 2.2 (편향–분산 분해) T가 유한한 이차 모멘트를 가지면

$$\mathrm{MSE}_\theta(T) = \mathrm{Var}_\theta(T) + b_\theta(T)^2. \tag{2.3}$$

증명. $T - g(\theta) = (T - \mathbb{E}_\theta T) + b_\theta(T)$를 제곱한다. 교차항 $2b_\theta(T)(T - \mathbb{E}_\theta T)$의 기댓값은 $b_\theta(T)$가 상수이므로 0이고, 나머지 두 항이 분산과 편향 제곱이다. □

불편성은 반복표본 평균에 관한 말이지 이번 관측값이 참값과 같다는 뜻이 아니다. 편향이 조금 있는 추정량도 분산을 충분히 줄이면 평균제곱오차가 더 작을 수 있다. 반대로 불편하지만 변동이 매우 큰 추정량은 실용적이지 않을 수 있다.

예제 2.3 (정규 평균의 축소) $\overline{X}_n \sim N(\theta, \sigma^2/n)$이고 σ^2를 안다고 하자. $T_c = c\overline{X}_n$ $(0 \le c \le 1)$이면

$$b_\theta(T_c) = (c-1)\theta, \qquad \mathrm{MSE}_\theta(T_c) = \frac{c^2\sigma^2}{n} + (1-c)^2\theta^2. \tag{2.4}$$

θ가 0 근처일 때 축소가 유리할 수 있지만, 큰 $|\theta|$에서는 편향이 커진다. 참값을 모른 채 모든 θ에서 같은 $c<1$이 항상 더 좋다고 말할 수는 없다. 정확히는 $\mathrm{MSE}_\theta(T_c) < \sigma^2/n = \mathrm{MSE}_\theta(\overline{X}_n)$일 필요충분조건이 $\theta^2 < \frac{1+c}{1-c}\cdot\frac{\sigma^2}{n}$이다$(c<1)$. 또한 θ를 알 때의 최적 $c = \theta^2/(\theta^2+\sigma^2/n)$는 미지의 θ에 의존하므로 추정량으로 쓸 수 없다.

2.2 표본평균과 표본분산

독립 동일분포이며 평균 μ, 유한 분산 σ^2인 표본에서 $\overline{X}_n$은 불편이고 분산은 σ^2/n이다. 정규성은 이 두 성질에 필요하지 않다. 정규성은 표본평균의 정확한 정규분포처럼 더 강한 결론에 사용된다.

정리 2.4 (불편 표본분산) $n \ge 2$이고 독립 동일분포 표본의 분산이 유한하면

$$S^2 = \frac{1}{n-1}\sum_{i=1}^{n}(X_i - \overline{X}_n)^2 \tag{2.5}$$

는 σ^2의 불편추정량이다.

증명. 다음 제곱합 분해를 사용한다.

$$\sum_{i}(X_i-\overline{X}_n)^2 = \sum_{i}(X_i-\mu)^2 - n(\overline{X}_n-\mu)^2.$$

(우변은 $\sum_i[(X_i-\mu)-(\overline{X}_n-\mu)]^2$을 전개하고 $\sum_i(X_i-\mu)=n(\overline{X}_n-\mu)$를 쓰면 얻는다.) 기댓값을 취하면 $n\sigma^2 - n(\sigma^2/n) = (n-1)\sigma^2$이다. □

분모 $n-1$은 자유도라는 말로 기억할 수 있지만, 위 기댓값 계산이 정확한 근거다. 표본평균을 같은 자료로 추정하면서 중심으로부터의 제곱거리가 평균적으로 감소한 양을 보정한다. 모집단 평균 μ를 실제로 안다면 $n^{-1}\sum_i(X_i-\mu)^2$ 자체가 불편하다.

불편한 분산추정량의 제곱근 S가 표준편차의 불편추정량인 것은 아니다. 제곱근은 오목하므로 Jensen 부등식에 의해 $\mathbb{E}S \le \sqrt{\mathbb{E}S^2} = \sigma$이다. 비퇴화한 경우에는 보통 엄격한 부등식이다. 비선형 함수는 불편성을 자동으로 보존하지 않는다.

예제 2.5 (유한 표본의 편향 계산) $n=10$일 때 분모 n인 분산추정량 $V_n = n^{-1}\sum_i(X_i-\overline{X}_n)^2$의 평균은 $\frac{n-1}{n}\sigma^2 = 0.9\sigma^2$이다. 상대 편향은 -0.1이다. 큰 표본에서 편향이 작아진다는 것과 유한 표본에서 불편하다는 것은 구별한다. 평균제곱오차 기준으로는 정규모형에서 분모 $n+1$의 추정량이 S^2와 V_n보다 작은 위험을 가지지만, 이는 이 장의 범위 밖이다.

2.3 일관성과 불편성의 차이

정의 2.6 (일관성) 모든 고정된 θ에서 $T_n \xrightarrow{\mathbb{P}} g(\theta)$이면 T_n은 **일관추정량**(*consistent estimator*)이다. 거의 확실하게 수렴하면 **강한 일관성**을 갖는다고 한다.

$\mathrm{MSE}_\theta(T_n) \to 0$이면 Markov 부등식으로 일관성이 따른다. 실제로 $\mathbb{P}(|T_n - g(\theta)| > \varepsilon) = \mathbb{P}\big((T_n - g(\theta))^2 > \varepsilon^2\big) \le \mathrm{MSE}_\theta(T_n)/\varepsilon^2 \to 0$이다. 따라서 편향이 0으로 가고 분산도 0으로 가는 것은 한 충분조건이다. 불편성만으로 분산이 줄어드는 것은 아니다.

> **예제 2.7 (불편하지만 일관되지 않는 추정량)** 독립 $N(\theta, 1)$ 표본에서 $T_n = X_1$만 사용하면 모든 n에서 불편하다. 하지만 분산은 항상 1이고, $\mathbb{P}_\theta(|T_n - \theta| > 1) = \mathbb{P}(|Z| > 1) \approx 0.3173$도 고정된 양수이다. 자료를 추가해도 추정량이 그 자료를 사용하지 않으므로 일관되지 않는다.

> **예제 2.8 (편향이 있지만 일관적인 추정량)** 같은 정규모형에서 $T_n = \frac{n}{n+1}\overline{X}_n$이면 편향은 $-\theta/(n+1)$이고 분산은 $n/(n+1)^2$이다. 두 항이 각각 0으로 가므로 평균제곱오차 $(n+\theta^2)/(n+1)^2$도 0으로 간다. 유한 표본에서는 편향이 있지만 일관적이다.

반대로 확률수렴만으로 기댓값 수렴이 보장되지 않으므로 일관성이 점근적 불편성을 자동으로 뜻하지도 않는다. 확률론에서 본 드물고 큰 값의 반례가 추정량에도 같은 주의를 요구한다(제20권 제10장).

2.4 정보량과 Cramér–Rao 하계

이 절의 모형은 공통 지원집합 위의 밀도 또는 질량함수 $f_\theta(x)$를 가지며, 미분과 적분을 교환할 수 있을 만큼 정칙적이라고 가정한다. 모수는 열린 구간의 실수이고 밀도는 필요한 곳에서 양수라고 하자. 경계 모수, 모수에 따라 변하는 지원집합, 비미분가능한 우도에서는 결과를 별도로 점검해야 한다.

> **정의 2.9 (점수함수와 Fisher 정보량)** 자료 전체의 **점수함수**(*score function*)와 **Fisher 정보량**(*Fisher information*)은
>
> $$U_\theta(X) = \frac{\partial}{\partial \theta} \log f_\theta(X), \qquad I(\theta) = \mathbb{E}_\theta\big[U_\theta(X)^2\big] \tag{2.6}$$
>
> 이다. 정칙성 아래에서 $\mathbb{E}_\theta U_\theta = 0$이다. 독립 동일분포 표본에서는 개별 정보량 $I_1(\theta)$에 대해 $I_n(\theta) = n I_1(\theta)$이다.

$I_n = nI_1$은 독립 표본의 점수가 개별 점수의 합이고, 독립이며 평균 0인 항들의 합의 분산은 분산의 합이기 때문이다.

> **정리 2.10 (불편추정량의 Cramér–Rao 하계)** 정칙성, $0 < I(\theta) < \infty$, 필요한 유한 모멘트와 미분 교환을 가정한다. T가 미분가능한 $g(\theta)$의 불편추정량이면
>
> $$\mathrm{Var}_\theta(T) \ge \frac{[g'(\theta)]^2}{I(\theta)}. \tag{2.7}$$

증명. 정규화 $\int f_\theta(x)\,\mathrm{d}x = 1$을 미분하면 점수의 평균이 0이다. 불편성 $\int T(x) f_\theta(x)\,\mathrm{d}x = g(\theta)$를 미분하면

$$g'(\theta) = \mathbb{E}_\theta[T U_\theta] = \mathrm{Cov}_\theta(T, U_\theta).$$

Cauchy–Schwarz 부등식으로 $[g'(\theta)]^2 \le \mathrm{Var}_\theta(T) I(\theta)$이다. $\square$

등호는 Cauchy–Schwarz의 등호 조건, 곧 $T - g(\theta)$가 U_θ의 상수배일 때에만 성립한다. 이 하계는 해당 정칙 모형의 불편추정량들에 대한 결과다. 모든 편향추정량의 평균제곱오차에 같은 식이 자동으로 적용되는 것은 아니다. 등호가 실제로 달성되는지도 모형과 추정대상에 달려 있다.

예제 2.11 (Bernoulli 성공확률) $0 < p < 1$인 독립 Bernoulli 표본에서

$$U_p = \frac{S - np}{p(1-p)}, \qquad I_n(p) = \frac{n}{p(1-p)}.$$

$\log f_p(x) = S\log p + (n-S)\log(1-p)$를 p로 미분하면 $S/p - (n-S)/(1-p) = (S-np)/(p(1-p))$이고, $\mathrm{Var}(S) = np(1-p)$이므로 $I_n(p) = np(1-p)/(p(1-p))^2 = n/(p(1-p))$이다. 따라서 p의 불편추정량 분산은 $p(1-p)/n$ 이상이다. 표본비율 S/n의 분산이 정확히 이 값이므로 하계를 달성한다($S/n = p + \frac{p(1-p)}{n} U_p$로 등호 조건과 일치). 경계 $p = 0, 1$에는 위 점수식의 분모가 0이므로 같은 정칙 계산을 그대로 쓰지 않는다.

2.5 비정칙 모형에서의 경고

예제 2.12 (균등분포의 끝점) 독립 $X_i \sim \mathrm{Unif}(0, \theta)$, $\theta > 0$라 하자. 최댓값 M의 분포함수는 $\mathbb{P}_\theta(M \le m) = (m/\theta)^n$ $(0 < m < \theta)$이다. 따라서

$$\mathbb{E}_\theta M = \frac{n\theta}{n+1}, \qquad \mathrm{Var}_\theta(M) = \frac{n\theta^2}{(n+1)^2(n+2)}.$$

$T = (n+1)M/n$은 불편이고

$$\mathrm{Var}_\theta(T) = \frac{\theta^2}{n(n+2)}.$$

(밀도 $n m^{n-1}/\theta^n$으로 $\mathbb{E}M^2 = n\theta^2/(n+2)$를 계산하면 $\mathrm{Var}(M) = n\theta^2/(n+2) - n^2\theta^2/(n+1)^2$이다.) 우도는 $\theta^{-n}\mathbf{1}_{\{M \le \theta\}}$이므로 지원집합이 모수에 따라 바뀐다. 지시함수를 무시하고 로그우도만 미분하면 점수 평균이 0이라는 성질부터 실패한다. 실제로 $\partial_\theta(-n\log\theta) = -n/\theta \neq 0$이다. 정칙 Cramér–Rao 하계를 기계적으로 적용해서는 안 된다.

최댓값은 표본이 모두 끝점 아래에 있다는 정보를 모으므로 평균과 다른 속도로 끝점을 추정한다. 위 T의 분산은 $\theta^2/(n(n+2)) = O(n^{-2})$이고, 같은 모형에서 모평균 $\theta/2$를 이용한 $2\overline{X}_n$의 분산 $\theta^2/(3n)$은 $O(n^{-1})$이다. $n = 4$이면 $\theta^2/24$와 $\theta^2/12$로 이미 두 배 차이가 난다. 일반적으로 "모든 추정량의 오차는 항상 $n^{-1/2}$"라는 주장은 참이 아니다. 모형의 경계와 정보 구조에 따라 다른 척도가 나타난다.

2.6 연습문제와 해설

연습문제 2.13 T의 편향이 2, 분산이 3이면 평균제곱오차는 얼마인가? 편향이 1, 분산이 6인 다른 추정량과 비교하라.

풀이. 두 평균제곱오차는 모두 7이다($3 + 2^2 = 6 + 1^2$). 하나는 편향이 작지만 분산이 크다. 평균제곱오차 외에 다른 손실을 쓰면 비교가 달라질 수 있다.

연습문제 2.14 독립표본의 평균 μ를 추정하는 $T = 2\overline{X}_n$의 편향과 평균제곱오차를 구하라. 모집단 분산은 $\sigma^2 < \infty$이다.

풀이. 편향은 μ, 분산은 $4\sigma^2/n$, 평균제곱오차는 $\mu^2 + 4\sigma^2/n$이다. $\mu \neq 0$이면 일관적이지 않다 $(T \to 2\mu \neq \mu)$.

연습문제 2.15 $X_i \sim N(\mu, \sigma^2)$이며 σ^2를 안다. 평균 μ의 개별 Fisher 정보량과 불편추정량 분산의 하계를 구하라.

풀이. 개별 점수는 $(X_i - \mu)/\sigma^2$, 정보량은 $1/\sigma^2$다. 표본 전체 정보량은 n/σ^2이며 하계는 σ^2/n이다. 표본평균이 달성한다.

연습문제 2.16 $\mathrm{Unif}(0, \theta)$ 표본 $n = 4$에서 최댓값이 0.8이었다. 끝점의 보정된 불편추정값을 구하라.

풀이. $(5/4)(0.8) = 1$이다. 이 숫자가 참끝점과 반드시 같다는 뜻은 아니며, 반복표본에서 평균이 참끝점이 되도록 보정한 추정량의 관측값이다.

참고 (다음 연결). 추정량의 성능 기준을 정했다면 자료가 모수에 관해 담고 있는 정보를 어떻게 추출할지 살펴볼 차례다. 다음 장은 우도, 최대우도추정, 충분성, 조건화에 의한 개선을 연결한다.

제 3 장

우도, 최대우도추정, 충분성

개요 우도함수(*likelihood function*)는 관측값을 고정하고 모수를 변수로 보아 모형의 확률밀도 또는 확률질량함수를 다시 읽은 함수이다. 이 장은 우도함수와 로그우도를 정의하고, 최대우도추정량(*maximum likelihood estimator*)의 존재와 경계 문제, 정규모형과 재매개화에서의 성질을 다룬다. 이어서 충분통계량(*sufficient statistic*)을 정의하고 인수분해 정리를 보이며, 충분통계량으로 조건화하여 추정량을 개선하는 Rao–Blackwell 정리와 완비성(*completeness*)에 근거한 Lehmann–Scheffé 정리를 소개한다. 선행 지식: 결합분포, 미분에 의한 최적화, 조건부 기댓값. 로그우도를 쓸 때에는 지원집합과 모수공간을 유지한다.

우도는 자료를 고정하고 가능한 모수값들이 그 자료를 얼마나 잘 설명하는지 비교한다. 확률모형과 같은 식을 쓰지만 변수가 무엇인지가 바뀐다. 최대우도추정은 그 비교값을 가장 크게 만드는 모수를 선택하며, 충분통계량은 모수에 관한 정보를 잃지 않고 자료를 요약하는 방법을 제시한다.

3.1 우도는 모수에 대한 확률밀도가 아니다

정의 3.1 (우도함수) 관측값 x에 대해 $L(\theta; x) = f_\theta(x)$를 **우도함수**(*likelihood function*)라 한다. 여기서 f_θ는 모수가 θ일 때의 밀도 또는 질량함수이다. 자료에만 의존하는 양의 인자를 곱해도 모수값 사이의 **우도비**와 최대점은 같다. **로그우도**는 $\ell(\theta; x) = \log L(\theta; x)$이다.

θ에 대해 적분한 값이 1일 필요는 없다. 연속자료에서 밀도값을 사용한다고 해서 정확한 관측점이 발생할 확률을 계산하는 것도 아니다. 베이지안 사후분포를 만들려면 별도의 사전분포와 정규화가 필요하다(제22권 제6장). 독립 표본에서는 $L(\theta; x) = \prod_{i=1}^{n} f_\theta(x_i)$이므로 로그우도는 합 $\ell(\theta; x) = \sum_{i=1}^{n} \log f_\theta(x_i)$가 되어 미분과 최적화가 쉬워진다. 로그는 증가함수이므로 L과 ℓ의 최대점은 같다.

예제 3.2 (성공 개수와 전체 배열) 독립 Bernoulli 표본 $x_1, \dots, x_n$에서 $s = \sum_i x_i$이면 전체 배열의 우도는 $p^s(1-p)^{n-s}$이다. 성공 개수만 관측했다면 우도는 $\binom{n}{s} p^s (1-p)^{n-s}$이다. 두 우도는 p에 의존하지 않는 인자만 다르므로 같은 최대점과 같은 우도비를 갖는다. 서로 다른 실험에서 자료의 확률을 계산한 값 자체가 같은 것은 아니다.

3.2 최대우도추정량의 존재와 경계

정의 3.3 (최대우도추정값) 모수공간 Θ에서 $L(\theta; x)$를 최대화하는 값이 존재하면 **최대우도추정값**이라 한다. 자료의 함수로 선택한 최대점을 **최대우도추정량**, 약자로 **MLE**라고 한다. 최대점이 여러 개일 수 있고, 상한만 존재하여 최대점이 없을 수도 있다.

Bernoulli 모수공간이 $[0,1]$이면 MLE는 $\widehat{p} = s/n$이다. $0 < s < n$에서는

$$\ell'(p) = \frac{s}{p} - \frac{n-s}{1-p} = 0$$

을 풀고 이차 도함수 $\ell''(p) = -s/p^2 - (n-s)/(1-p)^2$가 음수임을 확인하면 된다. $s = 0$ 또는 $s = n$에서는 내부 방정식 대신 경계를 확인해야 한다. 실제로 $s = 0$이면 $L(p) = (1-p)^n$이 $p = 0$에서, $s = n$이면 $L(p) = p^n$이 $p = 1$에서 최대이다. 모수공간을 $(0,1)$로 정했다면 두 경계 자료에서 유한한 최대점은 없고 경계로 갈 때 상한에 접근한다. 같은 미분 방정식이라도 모수공간을 빼먹으면 결론이 틀리다.

예제 3.4 (Poisson 평균의 MLE) 독립 $\mathrm{Pois}(\lambda)$ 표본에서 $S = \sum_i x_i$라 하면

$$\ell(\lambda) = -n\lambda + S\log\lambda - \sum_i \log(x_i!).$$

$S > 0$이면 $\ell'(\lambda) = -n + S/\lambda = 0$에서 MLE는 S/n이다. $S = 0$이면 $\ell(\lambda) = -n\lambda$이므로 $\lambda \geq 0$을 허용할 때 MLE는 0이고, $\lambda > 0$만 허용할 때는 최대점이 없다. 이 추정량은 모형 안에서 불편하지만($\mathbb{E}\,\overline{X}_n = \lambda$) MLE가 항상 불편하다는 일반 원리가 있는 것은 아니다.

예제 3.5 (미분으로 찾을 수 없는 최대점: 균등분포) 독립 $U(0,\theta)$ 표본에서 밀도를 $f_\theta(x) = \theta^{-1}\mathbf{1}_{\{0 \leq x \leq \theta\}}$로 잡으면

$$L(\theta; x) = \theta^{-n}\,\mathbf{1}_{\{\theta \geq \max_i x_i\}}\mathbf{1}_{\{\min_i x_i \geq 0\}}.$$

$\theta \geq \max_i x_i$에서 L은 θ에 대해 감소하므로 MLE는 표본 최댓값 $X_{(n)}$이다. 우도는 이 점에서 불연속이어서 $\ell'(\theta) = 0$을 풀어서는 최대점을 찾을 수 없다. $\mathbb{E}X_{(n)} = n\theta/(n+1)$이므로 이 MLE는 아래쪽으로 편향되어 있고, $(n+1)X_{(n)}/n$이 불편추정량이다.

3.3 정규모형의 최대우도추정

독립 $N(\mu, \sigma^2)$ 표본의 로그우도는 상수를 제외하면

$$\ell(\mu, \sigma^2) = -\frac{n}{2}\log\sigma^2 - \frac{1}{2\sigma^2}\sum_i (x_i - \mu)^2.$$

고정된 분산에서 제곱합을 최소화하는 평균은 $\bar{x}$다. 이를 넣고 $v = \sigma^2 > 0$에 대해 최대화하면 $\partial_v \ell = -n/(2v) + \sum_i (x_i - \bar{x})^2/(2v^2) = 0$에서

$$\widehat{\mu} = \bar{x}, \qquad \widehat{\sigma}^2_{\mathrm{ML}} = \frac{1}{n}\sum_i (x_i - \bar{x})^2. \tag{3.1}$$

이 식은 제곱합이 양수일 때의 내부 최대점이다. 모든 관측이 정확히 같으면 분산을 0으로 보낼 때 우도가 무한히 커지므로 $\sigma^2 > 0$ 모형 안에 유한한 최대점이 없다. 연속 정규표본 $n \geq 2$에서는 그 자료 사건의 확률이 0이지만, 반올림된 실제 자료나 $n = 1$에서는 계산 규칙을 따로 확인해야 한다.

MLE 분산은 분모가 n이며 불편추정량의 분모 $n-1$과 다르다. 둘은 서로 다른 최적화 기준에서 나온다. 정규모형에서는 $Q = \sum_i (X_i - \overline{X}_n)^2/\sigma^2 \sim \chi^2_{n-1}$이고 $\mathbb{E}Q = n-1$, $\mathrm{Var}\,Q = 2(n-1)$이므로

$\widehat{\sigma}^2_{\mathrm{ML}} = \sigma^2 Q/n$의 편향은 $-\sigma^2/n$, 분산은 $2(n-1)\sigma^4/n^2$이다. 따라서

$$\mathrm{MSE}(\widehat{\sigma}^2_{\mathrm{ML}}) = \frac{2(n-1)}{n^2}\sigma^4 + \frac{\sigma^4}{n^2} = \frac{2n-1}{n^2}\sigma^4, \qquad \mathrm{MSE}(S^2) = \frac{2}{n-1}\sigma^4. \tag{3.2}$$

$(2n-1)(n-1) = 2n^2 - 3n + 1 < 2n^2$이므로 $(2n-1)/n^2 < 2/(n-1)$이다. MLE는 편향이 있지만 이 비교에서는 더 작은 평균제곱오차를 갖는다. 이는 해당 정규모형의 결과이며 모든 분포에서 같은 식이 성립하는 것은 아니다.

3.4 재매개화와 국소해

MLE가 존재하고 관심모수를 $\psi = g(\theta)$로 바꾸면, 각 ψ에 대해 원래 우도를 해당 원상에서 최대화한 **profile 우도** $L^*(\psi) = \sup_{\theta:\, g(\theta)=\psi} L(\theta)$를 사용한다.

> **명제 3.6 (MLE의 함수 불변성)** $\widehat{\theta}$가 $L(\theta; x)$의 최대점이면 $g(\widehat{\theta})$는 profile 우도 L^*의 최대점이다. 이 의미에서 $g(\widehat{\theta})$를 $\psi = g(\theta)$의 MLE라 한다.

증명. 임의의 ψ에 대해 $L^*(\psi) \le \sup_\theta L(\theta) = L(\widehat{\theta})$이다. 한편 $\widehat{\theta}$는 $g(\theta) = g(\widehat{\theta})$인 θ 가운데 하나이므로 $L^*(g(\widehat{\theta})) \ge L(\widehat{\theta})$이다. 따라서 $L^*(g(\widehat{\theta})) = L(\widehat{\theta}) = \sup_\psi L^*(\psi)$이다. □

예를 들어 지수분포 rate λ의 MLE가 $1/\overline{X}$이면 평균 $1/\lambda$의 MLE는 $\overline{X}$이다. 다만 이 불변성은 최대점에 대한 성질이며 불편성이나 평균제곱오차와는 무관하다(예제 3.7).

최적화 도구가 반환한 정지점은 MLE와 동의어가 아니다. 로그우도가 오목하면 내부 정지점이 전역 최대라는 보장이 있지만, 혼합모형처럼 여러 국소 최대가 있는 모형에서는 다른 시작값, 경계, 발산 가능성을 확인해야 한다. 수치적으로 매우 큰 우도를 찾았다는 사실만으로 유일한 최대점을 증명한 것은 아니다.

> **예제 3.7 (지수 rate의 편향)** 독립 $\mathrm{Exp}(\lambda)$ 표본(밀도 $\lambda e^{-\lambda x}$)에서 $S = \sum_i X_i \sim \mathrm{Gamma}(n, \lambda)$이며 shape는 n, rate는 λ이다. MLE는 n/S이다. $n > 1$이면 감마의 역모멘트로
>
> $$\mathbb{E}\!\left(\frac{n}{S}\right) = \frac{n}{n-1}\lambda.$$
>
> 따라서 위쪽 편향이 있으며 $(n-1)/S$가 불편추정량이다. $n = 1$에서는 $1/X_1$의 평균이 발산하므로 같은 편향식을 유한한 값으로 쓸 수 없다.

3.5 충분통계량과 인수분해

> **정의 3.8 (충분통계량)** 통계량 $T(X)$가 주어졌을 때 원래 자료 X의 조건부분포가 모수 θ에 의존하지 않으면 T를 **충분통계량**(*sufficient statistic*)이라 한다. 정규 조건부분포의 존재 등 통상적인 가측성 조건 아래에서 해석한다.

충분성은 어떤 특정 추정량이 좋아 보인다는 뜻이 아니라 모형 전체에 대해 성립하는 정보 요약의 성질이다. 표본평균은 정규 평균의 충분통계량이 될 수 있지만 모든 분포모형에서 충분한 것은 아니다.

정리 3.9 (인수분해 정리) 공통 기준측도에 대해 밀도 또는 질량함수 f_θ를 갖는 지배된 모형에서, 통상적인 가측성 조건 아래 T가 충분한 것은

$$f_\theta(x) = g_\theta(T(x))\, h(x) \tag{3.3}$$

로 비음수 함수들을 사용해 인수분해할 수 있는 것과 동치이다. h는 모수에 의존하지 않는다.

증명. 이산형 자료에 대해 증명한다. 연속형의 일반 증명은 조건부분포와 기준측도 처리가 필요하므로 정리로 사용한다. ($\Rightarrow$) T가 충분하고 $t = T(x)$이면 $f_\theta(x) = \mathbb{P}_\theta(T = t)\,\mathbb{P}(X = x \mid T = t)$이다. 앞 인자는 $g_\theta(t)$, 뒤 인자는 모수와 무관한 $h(x)$이다. ($\Leftarrow$) 식 (3.3)가 성립하면 $\mathbb{P}_\theta(T = t) = g_\theta(t)\sum_{x' : T(x')=t} h(x')$이다. $\mathbb{P}_\theta(T = t) > 0$인 t와 $T(x) = t$인 x에 대해

$$\mathbb{P}_\theta(X = x \mid T = t) = \frac{g_\theta(t)h(x)}{g_\theta(t)\sum_{x' : T(x')=t} h(x')} = \frac{h(x)}{\sum_{x' : T(x')=t} h(x')}$$

이고 이 값은 θ에 의존하지 않는다. □

이산형에서는 $T = t$인 자료들의 조건부 확률을 계산하면 모수 인자 $g_\theta(t)$가 분자와 분모에서 약분되는 방향이 즉시 확인된다. 모수에 따른 지원집합 정보도 반드시 g_θ 안에 보존해야 한다.

예제 3.10 (세 가지 충분통계량) Bernoulli와 Poisson 독립표본에서는 합 $S = \sum_i X_i$가 충분하다. Bernoulli에서는 $f_p(x) = p^S(1-p)^{n-S}\cdot 1$로, Poisson에서는 $f_\lambda(x) = e^{-n\lambda}\lambda^S \cdot \prod_i (x_i!)^{-1}$로 인수분해된다. 정규모형에서 분산을 알고 평균만 미지이면 $\sum_i X_i$가 충분하다. 평균과 분산이 모두 미지이면

$$T(X) = \left(\sum_i X_i,\ \sum_i X_i^2\right)$$

가 충분하다. $\sum_i (x_i - \mu)^2 = \sum_i x_i^2 - 2\mu\sum_i x_i + n\mu^2$이기 때문이다. 균등 끝점 모형 $U(0,\theta)$에서는 $f_\theta(x) = \theta^{-n}\mathbf{1}_{\{0 < \min_i x_i\}}\mathbf{1}_{\{\max_i x_i < \theta\}}$이므로 최댓값이 충분하다. 경계점의 밀도값 규약은 연속분포를 바꾸지 않는다.

충분통계량의 일대일 변환도 충분하다. 예를 들어 고정된 n에서 합과 평균은 같은 정보를 갖는다. 그러나 모든 충분통계량이 차원을 최대로 줄였다는 뜻은 아니다. 원래 자료 전체도 자명하게 충분하다. 최소충분성과 완비성은 서로 다른 추가 성질이다.

3.6 조건화에 의한 추정 개선

정리 3.11 (Rao–Blackwell 정리: 제곱손실 형태) T가 충분하고 U가 추정대상 $g(\theta)$에 대해 제곱적분가능한($\mathbb{E}_\theta U^2 < \infty$) 추정량이라고 하자. 조건부분포의 모수 독립성을 이용하여 $V(T) = \mathbb{E}_\theta[U \mid T]$를 미지 모수 없이 계산할 수 있다고 하자. 그러면 V는 통계량이며

$$\mathbb{E}_\theta V = \mathbb{E}_\theta U, \qquad \mathrm{MSE}_\theta(V) \le \mathrm{MSE}_\theta(U)$$

이다. 여기서 $\mathrm{MSE}_\theta(W) = \mathbb{E}_\theta[(W - g(\theta))^2]$이다.

증명. 전체 기댓값 공식으로 평균이 같다. 또한 V는 T의 함수이고 $\mathbb{E}_\theta[U - V \mid T] = 0$이므로 교차항 $\mathbb{E}_\theta[(U-V)(V-g(\theta))] = \mathbb{E}_\theta\big[(V-g(\theta))\,\mathbb{E}_\theta[U-V\mid T]\big] = 0$이다(Jensen 부등식으로

$\mathbb{E}_\theta V^2 \le \mathbb{E}_\theta U^2 < \infty$이므로 모든 항이 유한하다). 조건부 평균의 직교 분해에서 상수 $g(\theta)$를 사용하면

$$\mathbb{E}_\theta[(U - g(\theta))^2] = \mathbb{E}_\theta[(U - V)^2] + \mathbb{E}_\theta[(V - g(\theta))^2].$$

첫 항이 비음수이므로 결과를 얻는다. $\square$

수학적으로 임의의 정보에 조건화해도 분산은 평균적으로 줄지만, 결과가 미지 모수에 의존하면 계산 가능한 추정량이 아닐 수 있다. 충분성은 이 문제에서 조건화 결과를 통계량으로 사용할 수 있게 하는 역할을 한다.

예제 3.12 (한 관측을 평균으로 개선하기) Bernoulli 표본에서 $U = X_1$은 p의 불편추정량이다. 충분통계량 S로 조건화하면 성공 위치들이 대칭이므로 $\mathbb{E}[X_1 \mid S] = S/n$이다. 분산은 $p(1-p)$에서 $p(1-p)/n$으로 줄어든다. 조건화가 버리는 것은 모수에 관한 정보가 아니라 성공 위치의 불필요한 무작위성이다.

정의 3.13 (완비성) 통계량 T의 분포족이, 모든 모수에서 $\mathbb{E}_\theta|h(T)| < \infty$이고 $\mathbb{E}_\theta h(T) = 0$이면 모든 모수에서 $h(T) = 0$이 거의 확실하다는 성질을 가질 때 **완비**(*complete*)하다고 한다.

완비충분통계량의 함수인 불편추정량은 유일한 최소분산 불편추정량이라는 Lehmann–Scheffé 정리가 있다(추정대상에 불편추정량이 존재하고 분산이 유한한 경우). 여기서 최소분산은 모든 불편추정량과 비교하며 각 모수값에서의 분산을 뜻한다. 편향추정량까지 포함한 모든 절차에 대해 항상 최적이라는 주장은 아니다.

예제 3.14 (이항 합의 완비성) $S \sim \mathrm{Bin}(n, p)$, $0 < p < 1$이고 $\mathbb{E}_p h(S) = 0$이라 하자. $(1-p)^n$으로 나누고 $z = p/(1-p) > 0$으로 놓으면

$$\sum_{s=0}^{n} h(s)\binom{n}{s} z^s = 0$$

가 모든 $z > 0$에서 성립한다. 다항식이 구간 전체에서 영이므로 모든 계수가 0이고 $h(s) = 0$이다($\binom{n}{s} \neq 0$). 따라서 합은 완비하며 표본비율의 최소분산 불편성도 이 경로로 확인할 수 있다.

역사 (우도의 기원). 최대우도추정과 충분성의 개념은 R. A. Fisher가 1920년대 초의 논문들에서 체계화하였다. Rao–Blackwell 정리는 C. R. Rao(1945)와 D. Blackwell(1947)의 결과이고, 완비성에 근거한 최적성은 Lehmann–Scheffé(1950)에서 나왔다.

3.7 연습문제와 해설

연습문제 3.15 Bernoulli 표본 $n = 8$에서 성공이 6번 나왔다. $p \in [0, 1]$의 MLE와 $p = 3/4$ 대 $p = 1/2$의 우도비를 구하라.

풀이. MLE는 $3/4$이다. 우도비는 $(3/4)^6(1/4)^2/(1/2)^8 = 729/256 \approx 2.84766$이다. 이 숫자는 두 가설의 사후확률 비가 아니며 사전 오즈가 없으면 후자를 결정할 수 없다.

연습문제 3.16 정규 자료 $1, 2, 3$에서 평균과 분산의 MLE, 분산의 불편추정값을 구하라.

풀이. 평균은 2, 제곱합은 2이므로 분산 MLE는 $2/3$, 불편추정값은 1이다.

연습문제 3.17 독립 지수표본 $n = 5$, 합 $S = 10$에서 rate의 MLE와 불편 보정 추정값을 구하라.

풀이. 각각 $5/10 = 0.5$, $4/10 = 0.4$이다. rate의 역수인 평균의 MLE는 $S/n = 2$다(이는 평균의 불편추정량이다). 그러나 그 역수 $1/2 = 0.5$는 rate의 불편추정값 0.4와 다르므로, 비선형 변환이 불편성을 보존하지 않음을 확인할 수 있다.

연습문제 3.18 충분통계량 T를 일대일 함수 $h(T)$로 바꾸면 충분성이 유지되는 이유를 설명하라.

풀이. 역함수로 T를 복원할 수 있으므로 두 통계량이 만드는 정보가 같다. 인수분해식에서도 $g_\theta(T)$를 $g_\theta(h^{-1}(h(T)))$로 바꾸면 된다. 필요한 가측성을 함께 가정한다.

참고 (다음 연결). 점추정의 하나의 숫자만으로는 표본 변동을 보여 주기 어렵다. 다음 장은 반복 표본 포함확률을 갖는 신뢰구간과 새로운 관측값에 대한 예측구간을 구별하여 구성한다(제22권 제4장).

제 4 장

신뢰구간과 예측구간

개요 신뢰구간(*confidence interval*)은 자료로부터 계산하는 구간 절차로서, 반복표본에서 참값을 포함하는 빈도가 정해진 수준 이상이 되도록 설계한 것이다. 이 장은 포함확률을 정의하고, 피벗(*pivot*)으로 정규 평균의 구간을 만들며, t 구간과 분산의 카이제곱 구간, 이항비율의 Wald·Wilson·Clopper–Pearson 구간, 점근구간과 변환, 새 관측에 대한 예측구간(*prediction interval*)을 차례로 다룬다. 선행 지식: 정규, 카이제곱, t 분포의 분위수, 중심극한정리와 Slutsky 정리. 정확한 유한표본 결론과 점근 결론을 구별한다.

신뢰구간은 자료로부터 계산하는 구간 절차이다. 관측 후 하나의 구간이 나오지만, 그 절차의 신뢰수준은 반복표본에서 참값을 포함하는 빈도로 정의된다. 분포 가정이 정확할 때의 유한 표본 구간과 큰 표본의 근사 구간은 서로 다른 보장을 갖는다.

4.1 포함확률의 정의

정의 4.1 (신뢰구간 절차) 관심모수 $g(\theta)$에 대해 자료로 계산한 구간 $C(X) = [L(X), U(X)]$가 모든 $\theta \in \Theta$에서

$$\mathbb{P}_\theta\big(g(\theta) \in C(X)\big) \geq 1 - \alpha \tag{4.1}$$

를 만족하면 신뢰수준 적어도 $1-\alpha$의 **신뢰구간**(*confidence interval*) 절차이다. 식 (4.1)의 좌변을 **포함확률**(*coverage probability*)이라 한다. 정확히 등호가 성립하는 경우도 있고, 이산모형에서는 보수적인 포함확률이 흔하다.

빈도주의 설정에서 참모수는 고정되어 있고 구간이 자료에 따라 변한다.

흔한 오류 (신뢰구간의 해석). 관측된 구간 $[l, u]$에 대해 모수가 95%의 사후확률로 들어 있다는 해석은 별도의 사전모형 없이 따라오지 않는다(제22권 제6장). “구간 안의 모든 값이 같은 정도로 그럴듯하다”는 뜻도 아니다.

같은 포함확률을 갖는 절차 중 구간 길이를 줄이고 싶은 목표가 있을 수 있다. 하지만 모든 모수에서 무조건 가장 짧은 구간 하나가 존재하는 것은 아니다. 대칭성, 불변성, 한쪽 또는 두쪽 오류 배분 등의 기준이 구간 형태에 영향을 준다.

4.2 피벗으로 정규 평균 구간 만들기

정의 4.2 (피벗) 자료와 모수의 함수 $Q(X, \theta)$의 분포가 미지 모수에 의존하지 않으면 이를 **피벗**이라고 한다. 피벗의 확률 부등식을 모수에 대해 풀면 신뢰구간을 만들 수 있다.

독립 $N(\mu,\sigma^2)$ 표본에서 $\sigma>0$을 알고 있으면

$$Z=\frac{\overline{X}_n-\mu}{\sigma/\sqrt{n}}\sim N(0,1).$$

$z_q=\Phi^{-1}(q)$라 쓰면

$$\mathbb{P}_\mu\left(-z_{1-\alpha/2}\le Z\le z_{1-\alpha/2}\right)=1-\alpha.$$

부등식 $-z_{1-\alpha/2}\le(\overline{X}_n-\mu)/(\sigma/\sqrt{n})\le z_{1-\alpha/2}$를 μ에 대해 풀면 $\overline{X}_n-z_{1-\alpha/2}\sigma/\sqrt{n}\le\mu\le\overline{X}_n+z_{1-\alpha/2}\sigma/\sqrt{n}$이므로, 정확한 구간은

$$\overline{X}_n\ \pm\ z_{1-\alpha/2}\frac{\sigma}{\sqrt{n}}. \tag{4.2}$$

알려진 분산과 정규성이라는 가정이 구간의 정확성을 만든다. 같은 공식이 임의의 모집단에서 자동으로 정확한 것은 아니다.

> **예제 4.3 (알려진 분산의 평균 구간)** $\sigma=2$, $n=100$, $\bar{x}=10$이면 95% 구간의 반길이는 $1.959964\,(2/10)\approx 0.391993$이다. 구간은 약 $[9.60801,10.39199]$이다. 같은 신뢰수준에서 표본수를 네 배로 늘리면 반길이는 절반이 된다. 표본 수를 두 배로 늘리면 절반이 되는 것이 아니다.

4.3 분산을 모를 때의 정확한 t 구간

> **정리 4.4 (정규표본의 독립 분해)** 독립 $N(\mu,\sigma^2)$ 표본 $n\ge 2$에 대해
>
> $$Z=\frac{\sqrt{n}(\overline{X}_n-\mu)}{\sigma}\sim N(0,1),\qquad V=\frac{(n-1)S^2}{\sigma^2}\sim\chi^2_{n-1}$$
>
> 이고 Z, V는 독립이다. 따라서
>
> $$T=\frac{\sqrt{n}(\overline{X}_n-\mu)}{S}\sim t_{n-1}.$$

증명. $Y_i=(X_i-\mu)/\sigma$로 놓으면 $Y=(Y_1,\dots,Y_n)^{\top}$는 독립 표준정규 성분을 가진다. 첫 행이 $(n^{-1/2},\dots,n^{-1/2})$인 직교행렬 A를 잡아 $W=AY$로 변환한다. 표준정규 벡터의 밀도 $(2\pi)^{-n/2}e^{-\|y\|^2/2}$는 직교변환에 대해 불변이므로 $W_1,\dots,W_n$도 독립 표준정규이다. 첫 좌표는 $W_1=n^{-1/2}\sum_i Y_i=\sqrt{n}\,\overline{Y}=Z$이다. 직교변환은 제곱길이를 보존하므로 $\sum_{j}W_j^2=\sum_i Y_i^2$이고, 항등식 $\sum_i Y_i^2=\sum_i(Y_i-\overline{Y})^2+n\overline{Y}^2$에서

$$\sum_{j=2}^{n}W_j^2=\sum_{i}(Y_i-\overline{Y})^2=\frac{(n-1)S^2}{\sigma^2}=V$$

이다. 따라서 V는 $n-1$개 독립 표준정규의 제곱합이어서 χ^2_{n-1} 분포이고, W_1과 $(W_2,\dots,W_n)$이 독립이므로 Z와 V도 독립이다. $T=Z/\sqrt{V/(n-1)}$이므로 비율의 t 분포는 정의에 따른다. $\square$

$t_{\nu,q}$를 t_ν 분포의 q 분위수라 하면 $\mathbb{P}(-t_{n-1,1-\alpha/2}\le T\le t_{n-1,1-\alpha/2})=1-\alpha$이고, 이를 μ에 대해 풀면 정확한 평균 구간은

$$\overline{X}_n\ \pm\ t_{n-1,1-\alpha/2}\frac{S}{\sqrt{n}}. \tag{4.3}$$

S와 분모 $\sqrt{n}$을 구분하고 자유도는 $n-1$을 사용한다. 정규모집단에서 정확한 결과이며, 비정규 자료에서는 큰 표본 근사로 사용할 수 있는지 별도로 검토한다.

예제 4.5 정규표본에서 $n=16$, $\bar{x}=10$, $s=2$라고 하자. $t_{15,0.975}\approx 2.131450$이므로 95% 구간은

$$10 \pm 2.131450\,\frac{2}{4} \approx [8.93428,\ 11.06573].$$

알려진 분산의 정규 분위수보다 큰 값을 사용하는 이유는 분산을 같은 표본에서 추정한 추가 불확실성이 비율의 t 분포에 반영되기 때문이다. $n=16$에서 $t_{15,0.975}=2.131450$은 $z_{0.975}=1.959964$보다 약 8.7% 크다.

4.4 정규 분산의 신뢰구간

$\chi^2_{\nu,q}$를 카이제곱분포의 q 분위수라 쓰면

$$\mathbb{P}\left(\chi^2_{n-1,\alpha/2} \le \frac{(n-1)S^2}{\sigma^2} \le \chi^2_{n-1,1-\alpha/2}\right) = 1-\alpha.$$

양수인 분산에 대해 역수를 취하면서 부등호 방향을 바꿔

$$\left[\frac{(n-1)S^2}{\chi^2_{n-1,1-\alpha/2}},\ \frac{(n-1)S^2}{\chi^2_{n-1,\alpha/2}}\right] \tag{4.4}$$

를 얻는다. 큰 분위수가 아래끝의 분모에, 작은 분위수가 위끝의 분모에 들어간다. 표준편차 구간은 양 끝의 제곱근을 취하면 된다.

예제 4.6 (정규 분산 구간의 수치) $n=16$, $s^2=4$이면 $(n-1)s^2=60$이다. $\chi^2_{15,0.025}\approx 6.26214$, $\chi^2_{15,0.975}\approx 27.48839$이므로 95% 분산 구간은 $[60/27.48839,\ 60/6.26214]\approx[2.1827,\ 9.5814]$이고 표준편차 구간은 약 $[1.4774,\ 3.0954]$이다. 점추정값 $s^2=4$는 구간 중앙이 아니라 아래쪽에 치우쳐 있다.

이 구간의 정확성은 정규분포에 민감하다. 평균 구간이 중심극한정리로 어느 정도 안정되는 상황에서도 분산 통계량의 정확한 카이제곱 법칙은 일반 모집단에 성립하지 않는다. 비정규 분산 추론은 사차 모멘트, 재표본 방법, 강건한 척도 등 별도 조건과 도구를 요구한다.

4.5 이항비율: Wald와 Wilson의 차이

독립 Bernoulli 표본의 비율 $\hat{p}=S/n$은 고정된 $0<p<1$에서

$$\frac{\sqrt{n}(\hat{p}-p)}{\sqrt{p(1-p)}} \xrightarrow{d} N(0,1)$$

이다. 분모의 p를 $\hat{p}$로 바꾸는 **Wald 구간**은

$$\hat{p} \pm z\sqrt{\frac{\hat{p}(1-\hat{p})}{n}}, \qquad z=z_{1-\alpha/2} \tag{4.5}$$

이다. 이는 정확한 이항 구간이 아니다. 작은 표본이나 $0,1$에 가까운 비율에서 포함확률이 나쁠 수 있고, 가능한 모수 범위를 벗어나거나 모든 성공·실패에서 길이가 0이 된다.

분모에 가설상의 p를 유지한 부등식

$$\frac{n(\hat{p}-p)^2}{p(1-p)} \le z^2$$

을 p에 대해 풀면 **Wilson 점수 구간**이 된다. 전개하면 $(n+z^2)p^2 - (2n\widehat{p}+z^2)p + n\widehat{p}^2 \le 0$이고, 이차식의 판별식은 $z^2\bigl(4n\widehat{p}(1-\widehat{p})+z^2\bigr)$이므로 두 근은

$$\frac{\widehat{p} + z^2/(2n)}{1+z^2/n} \;\pm\; \frac{z}{1+z^2/n}\sqrt{\frac{\widehat{p}(1-\widehat{p})}{n} + \frac{z^2}{4n^2}}. \tag{4.6}$$

이 구간은 $[0,1]$ 안에 있고 경계에서 퇴화하지 않지만, 정확한 유한 표본 포함확률을 모든 p에서 보장하는 구간과는 구분한다. 점수검정의 정규근사를 뒤집어서 만든 근사 구간이다.

> **예제 4.7 (성공 한 번의 구간)** $n=50$, $S=1$이면 $\widehat{p}=0.02$이다. 95% Wald 구간은 약 $[-0.01881,\ 0.05881]$로 음수까지 내려간다. Wilson 구간은 약 $[0.00354,\ 0.10495]$이며 비대칭이다. 다음 절의 Clopper–Pearson 구간은 약 $[0.00051,\ 0.10647]$로 더 넓다. 자료가 경계 근처의 성공확률에 대해 갖는 불확실성을 대칭인 플러그인 정규식이 제대로 반영하지 못한 사례다. 두 구간의 수치 차이는 같은 이름의 "오차범위"로 가려서는 안 된다.

4.6 이항검정을 뒤집은 정확 구간

> **정의 4.8 (Clopper–Pearson 구간)** $S=s$를 관측했을 때 두쪽 꼬리에 $\alpha/2$씩 배정한 **정확 이항 구간**의 아래끝 L, 위끝 U는 다음과 같다. $s=0$이면 $L=0$, $s=n$이면 $U=1$로 두고, 나머지는
>
> $$\mathbb{P}_{p=L}(S \ge s) = \alpha/2, \qquad \mathbb{P}_{p=U}(S \le s) = \alpha/2$$
>
> 를 푸는 값이다.

베타분포 분위수로 쓰면

$$L = B^{-1}_{s,\,n-s+1}(\alpha/2) \quad (s>0), \tag{4.7}$$

$$U = B^{-1}_{s+1,\,n-s}(1-\alpha/2) \quad (s<n). \tag{4.8}$$

여기서 $B^{-1}_{a,b}$는 $\mathrm{Beta}(a,b)$의 분위수함수이다. 이산성 때문에 포함확률은 보통 정확히 $1-\alpha$가 아니라 그 이상이며, 이 의미에서 보수적이다. "정확"은 정규근사 없이 이항분포 자체로 오류를 통제한다는 의미이지 구간이 항상 최단이라는 뜻은 아니다.

> **명제 4.9 (Clopper–Pearson 구간의 포함확률)** 모든 $p \in [0,1]$에서 $\mathbb{P}_p(L(S) \le p \le U(S)) \ge 1-\alpha$이다.

증명. p를 고정하고 $G(s) = \mathbb{P}_p(S \ge s)$라 하자. G는 s에 대해 증가하지 않는다. $p < L(s)$는, $q \mapsto \mathbb{P}_q(S \ge s)$가 증가함수이므로 $G(s) < \alpha/2$와 동치이다($s>0$). $A = \{s : G(s) \le \alpha/2\}$는 G의 단조성에 의해 어떤 s_0에 대해 $\{s \ge s_0\}$ 꼴이고, $G(s_0) \le \alpha/2$이므로 $\mathbb{P}_p(S \in A) = G(s_0) \le \alpha/2$이다. 따라서 $\mathbb{P}_p(p < L(S)) \le \mathbb{P}_p(S \in A) \le \alpha/2$이다. 같은 방식으로 아래 꼬리 $\mathbb{P}_p(S \le s)$를 쓰면(이때 $q \mapsto \mathbb{P}_q(S \le s)$는 감소함수이다) $\mathbb{P}_p(p > U(S)) \le \alpha/2$이다. 두 사건의 합집합 상계로 $\mathbb{P}_p(p \notin [L(S), U(S)]) \le \alpha$이다. $\square$

> **예제 4.10 (관측된 성공이 없을 때)** n번 모두 실패했으면 두쪽 구간의 위끝은 $(1-U)^n = \alpha/2$에서
>
> $$U = 1 - (\alpha/2)^{1/n}$$

이다. $n = 20$, $\alpha = 0.05$이면 위끝은 약 0.16843이다. 성공을 한 번도 관측하지 않았다고 성공확률이 반드시 0은 아니다. 한쪽 95% 상한이면 꼬리 예산을 α로 바꾸어 $1 - 0.05^{1/20} \approx 0.13911$을 얻는다.

4.7 점근구간의 조건과 변환

$\sqrt{n}(T_n - \theta) \xrightarrow{d} N(0, v(\theta))$이고 일관된 양의 분산 추정량 $\widehat{v}_n$이 있으면 Slutsky 정리에 근거한 점근구간은

$$T_n \pm z_{1-\alpha/2}\sqrt{\widehat{v}_n / n}$$

이다. 각 고정된 참모수에서 포함확률이 $1-\alpha$로 접근한다는 점근적 주장과 모든 유한 n, 모든 모수에서의 하한 보장은 다르다. 특히 경계 가까이에서 모수가 n에 따라 움직이는 문제는 별도 균등 근사가 필요할 수 있다.

양수 모수에는 로그 변환 뒤 구간을 만든 후 지수함수로 되돌리는 방법이 유용하다. 단조증가 변환 g에 대해 $g(\theta)$의 유효한 구간 $[A, B]$를 얻었다면 $[g^{-1}(A), g^{-1}(B)]$는 같은 사건을 표현하므로 포함확률이 유지된다($g(\theta) \in [A,B] \iff \theta \in [g^{-1}(A), g^{-1}(B)]$). 단조감소 변환이면 끝점 순서를 바꾼다. 변환 뒤의 근사 구간을 원래 척도로 돌리는 것은 정확 구간을 새로 만들어 주는 마법이 아니며, 출발 구간의 정확도 수준을 그대로 따른다.

4.8 모수 구간과 새 관측 예측구간

독립 정규표본과 독립인 새 관측 X_{n+1}을 생각하자. 평균 μ의 구간은 모집단 중심의 불확실성을 다룬다. 새 관측의 예측구간은 그 관측 자체의 분산까지 포함해야 한다. 분산을 모르면

$$\frac{X_{n+1} - \overline{X}_n}{S\sqrt{1 + 1/n}} \sim t_{n-1}.$$

분자는 평균 0, 분산 $\sigma^2(1 + 1/n)$의 정규변수이고 S와 독립이므로 정의에 따라 성립한다. 예측구간은

$$\overline{X}_n \pm t_{n-1,1-\alpha/2}\, S\sqrt{1 + 1/n}. \tag{4.9}$$

평균 구간의 $S/\sqrt{n}$보다 크다. $n \to \infty$여도 새 관측의 자체 변동은 없어지지 않으므로 예측구간 길이는 일반적으로 0으로 줄어들지 않는다.

4.9 연습문제와 해설

연습문제 4.11 알려진 표준편차 $\sigma = 3$인 정규표본에서 95% 평균 구간의 반길이를 0.5 이하로 만들려면 최소 몇 개면 충분한가?

풀이. $n \geq (1.959964 \cdot 3/0.5)^2 \approx 138.293$이므로 139개가 충분하다. 알려진 분산과 정규모형 아래의 계산이다.

연습문제 4.12 정규 분산 구간의 아래끝에 작은 카이제곱 분위수를 넣으면 어떤 문제가 생기는가?

풀이. 분모가 작을수록 몫은 커지므로 끝점 순서가 뒤집힌다. 피벗의 부등식을 양의 분산에 대해 풀면서 역수의 부등호 방향을 바꿔야 한다.

연습문제 4.13 n번 모두 성공한 이항표본의 두쪽 Clopper–Pearson 구간을 구하라.

풀이. 위끝은 1이고 아래끝은 $L^{n} = \alpha/2$에서 $(\alpha/2)^{1/n}$이다. 모두 실패한 예제와 성공·실패를 바꾸면 대칭적으로 얻어진다.

연습문제 4.14 표본 수가 매우 커질 때 정규모형의 평균 구간과 새 관측 예측구간의 반길이가 각각 어떻게 변하는지 설명하라.

풀이. 평균 구간의 반길이는 $n^{-1/2}$ 규모로 0에 접근한다. 예측구간의 반길이는 대략 $z_{1-\alpha/2}\sigma$에 접근하여 새 관측의 변동을 남긴다.

참고 (다음 연결). 신뢰구간은 특정 값을 기각하는 검정들을 뒤집어서 만들 수 있다. 다음 장은 검정의 오류, 검정력, p값, 다중검정을 각각 정의하여 그 연결을 설명한다(제22권 제5장).

제 5 장

가설검정, 검정력, 다중검정

개요 가설검정(*hypothesis testing*)은 귀무가설이 참일 때 특정 종류의 오류를 통제하도록 설계한 의사결정 절차이다. 이 장은 검정함수, 제1종·제2종 오류, 검정력 함수를 정의하고, 단순가설의 최강력 검정에 관한 Neyman–Pearson 보조정리를 증명하며, 정규 평균 검정의 검정력과 표본 크기, p 값, 우도비 검정과 Wilks 정리의 진술, 신뢰구간과의 대응을 다룬다. 끝으로 다중검정에서 가족별 오류율(FWER)과 거짓 발견 비율(FDR)을 구별하고 Bonferroni, Holm, Benjamini–Hochberg 절차를 소개한다. 선행 지식: 조건부 확률과 합집합 상계, 우도, 정규분포와 이항분포. 귀무가설의 확률과 귀무가설 아래 자료의 확률을 구별한다.

가설검정은 귀무가설이 참일 때 특정 종류의 오류를 통제하도록 설계한 의사결정 절차이다. 작은 p 값은 귀무가설 아래에서 드문 자료를 관측했다는 증거이며, 효과의 크기나 실제 중요성을 단독으로 나타내지 않는다. 기각하지 못한 결과도 효과가 없음을 자동으로 입증하지 않는다. 오류확률, 검정력, 추정값을 함께 해석해야 한다.

5.1 귀무가설, 오류, 검정력

정의 5.1 (검정과 검정력 함수) 모수공간의 두 부분집합 Θ_0, Θ_1에 대해 $H_0 : \theta \in \Theta_0$, $H_1 : \theta \in \Theta_1$을 검정한다. **검정함수** $\varphi(X) \in [0,1]$는 자료에서 귀무가설을 기각할 확률이다. 보통 비무작위 검정에서는 값이 0 또는 1이다. **검정력 함수**는

$$\pi(\theta) = \mathbb{E}_\theta \varphi(X)$$

이다. $\sup_{\theta \in \Theta_0} \pi(\theta) \le \alpha$이면 **유의수준** α의 검정이라 한다.

귀무가설이 참인데 기각하는 것이 **제1종 오류**다. 대립가설의 특정 참값에서 기각하지 않는 확률 $1 - \pi(\theta)$는 **제2종 오류** 확률이다. 대립가설이 여러 모수값을 포함하면 검정력은 하나의 숫자가 아니라 함수다. 작은 효과에서의 검정력과 큰 효과에서의 검정력은 다르다.

검정의 **크기**(*size*)는 귀무가설 집합에서 실제 제1종 오류 확률의 상한 $\sup_{\theta \in \Theta_0} \pi(\theta)$이고, 유의수준은 그 상한을 제한하는 설계값이다. 이산자료에서 실제 크기가 목표 α보다 작을 수 있다. 경계에서 확률적으로 일부만 기각하는 무작위 검정을 허용하면 정확히 맞추는 경우도 있지만, 실제 해석과 재현성을 위해 그 규칙을 명시해야 한다.

5.2 Neyman–Pearson 보조정리

정리 5.2 (단순가설 사이의 최강력 검정) 공통 기준측도에 대한 밀도 f_0, f_1의 두 단순가설을 비교한다. 어떤 $k \ge 0$에 대해 $f_1(x) > k f_0(x)$이면 기각하고, $f_1(x) < k f_0(x)$이면 기각하지 않으며, 등호 영역에서는 필요에 따라 무작위화하여 크기 α를 맞춘 검정 φ_*가 있다고 하자. 그러면 모든 크기 α 이하 검정 가운데 f_1 아래 검정력이 가장 크다.

증명. 임의의 경쟁 검정 φ에 대해 점별로 $[\varphi_*(x)-\varphi(x)][f_1(x)-k f_0(x)] \ge 0$이다. 실제로 $f_1 > k f_0$인 점에서는 $\varphi_* = 1 \ge \varphi$이고, $f_1 < k f_0$인 점에서는 $\varphi_* = 0 \le \varphi$이며, $f_1 = k f_0$인 점에서는 곱이 0이다. 적분하면

$$\mathbb{E}_1\varphi_* - \mathbb{E}_1\varphi \;\ge\; k\big(\mathbb{E}_0\varphi_* - \mathbb{E}_0\varphi\big) \;\ge\; 0.$$

마지막 부등식은 $\mathbb{E}_0\varphi_* = \alpha$와 경쟁 검정의 크기 제한 $\mathbb{E}_0\varphi \le \alpha$, 그리고 $k \ge 0$을 사용한다. $\square$

우도비가 큰 자료부터 기각영역에 넣는 원리가 나온다. 하지만 단순 대 단순가설의 정리를 복합가설에 아무 조건 없이 확장하여 하나의 균일최강력 검정이 항상 있다고 주장할 수는 없다. 대립가설의 서로 다른 방향들이 다른 기각영역을 요구할 수 있다.

5.3 정규 평균 검정과 검정력 계산

독립 $N(\mu, \sigma^2)$ 표본에서 σ를 알고, $H_0: \mu \le \mu_0$ 대 $H_1: \mu > \mu_0$를 검정하자. 유의수준 α의 기각규칙은

$$\overline{X}_n > \mu_0 + z_{1-\alpha}\frac{\sigma}{\sqrt{n}} \tag{5.1}$$

이다. 기각확률은 μ에 대해 증가하므로 귀무가설에서 가장 큰 오류는 경계 $\mu = \mu_0$에서 생기며 정확히 α이다. 참값 μ_1에서 $\overline{X}_n$은 $N(\mu_1, \sigma^2/n)$이므로 검정력은

$$\pi(\mu_1) = 1 - \Phi\!\left(z_{1-\alpha} - \frac{\sqrt{n}(\mu_1-\mu_0)}{\sigma}\right). \tag{5.2}$$

참고 (균일최강력성). $\mu_1 > \mu_0$를 고정하고 단순가설 $\mu = \mu_0$ 대 $\mu = \mu_1$에 Neyman–Pearson 보조정리를 적용하면, 우도비는 $\overline{X}_n$의 증가함수이므로 최강력 기각영역은 $\overline{X}_n > c$ 꼴이고 c는 μ_1에 의존하지 않는다. 따라서 식 (5.1)의 검정은 모든 $\mu_1 > \mu_0$에 대해 최강력이며, 크기가 복합귀무가설 전체에서 α 이하이므로 균일최강력 검정이다.

예제 5.3 (목표 효과에서의 표본 수) 표준편차 $\sigma = 2$, 의미 있는 차이 $\Delta = \mu_1 - \mu_0 = 0.5$, 한쪽 유의수준 0.05, 목표 검정력 0.8이라 하자. 식 (5.2)에서 $\pi(\mu_1) \ge 0.8$은 $\sqrt{n}\Delta/\sigma - z_{1-\alpha} \ge z_{0.8}$와 같으므로

$$n \ge \left\lceil \frac{\sigma(z_{0.95} + z_{0.8})}{\Delta} \right\rceil^2.$$

$z_{0.95} \approx 1.644854$, $z_{0.8} \approx 0.841621$이므로 약 98.9이고 정수로 99개가 충분하다. $n = 99$에서 실제 검정력은 약 0.8003이다. 이는 분산이 알려진 정규모형의 계산이다. 분산 추정, 탈락, 군집표본 등을 포함하면 같은 숫자를 그대로 쓰지 않는다.

두쪽 $H_0:\mu=\mu_0$ 대 $H_1:\mu\neq\mu_0$에서는 $|\sqrt{n}(\overline{X}_n-\mu_0)/\sigma|>z_{1-\alpha/2}$를 사용한다. 자료를 본 뒤 방향을 골라 한쪽 임계값을 적용하면 원래 설계한 오류 확률이 달라질 수 있다. 관심 있는 방향과 절차를 분석의 일부로 먼저 정해야 한다.

5.4 p값의 정의와 해석

정의 5.4 (유효한 p값) 귀무가설 아래에서 모든 $u\in[0,1]$와 모든 $\theta\in\Theta_0$에 대해

$$\mathbb{P}_\theta\big(p(X)\le u\big)\le u$$

를 만족하는 자료 함수 $p(X)$를 **유효한 p값**이라 한다. 관측값이 작을수록 귀무가설에 덜 부합하는 증거로 해석한다. 단순 연속모형의 적절한 꼬리변환에서는 균등분포가 되고, 이산모형에서는 일반적으로 보수적이다.

정규 한쪽 검정에서 관측된 z가 클수록 대립가설 방향의 증거라면 $p=1-\Phi(z)$이다. 두쪽 대칭 검정에서는 $p=2[1-\Phi(|z|)]$이다. $p\le\alpha$이면 해당 수준의 검정이 기각한다.

흔한 오류 (p값의 해석). p값은 귀무가설이 참일 사후확률도, 같은 결과가 재현될 확률도 아니다.

예제 5.5 (정규 통계량 $z=2$) 한쪽 p값은 약 0.02275, 두쪽 p값은 약 0.04550이다. 같은 관측 통계량이라도 가설과 기각방향이 다르면 질문이 달라진다. p값만 제시하기보다 추정된 차이, 표준오차, 구간, 표본 크기를 함께 보여 주어야 효과의 크기를 판단할 수 있다.

예제 5.6 (정확한 이항검정) 10번 중 성공 9번을 관측하고 $H_0:p=1/2$ 대 $p>1/2$를 검정하면

$$p_{\text{one}}=\mathbb{P}_{1/2}(S\ge 9)=\frac{\binom{10}{9}+\binom{10}{10}}{2^{10}}=\frac{11}{1024}\approx 0.0107422.$$

대칭인 두쪽 검정에서 $S\le 1$ 또는 $S\ge 9$를 같은 극단성으로 보면 $22/1024\approx 0.0214844$이다. 비대칭인 이산모형에서는 “두쪽”의 극단성 정의가 하나로 자동 결정되지 않는다. 사용하는 꼬리 규칙이나 우도비 순서를 명시한다.

5.5 우도비 검정과 점근 카이제곱

정의 5.7 (우도비 통계량) 복합 귀무가설 $\Theta_0\subseteq\Theta$에서, 분모의 상한이 0보다 크고 유한한 관측에 대한 **우도비**는

$$\Lambda(X)=\frac{\sup_{\theta\in\Theta_0}L(\theta;X)}{\sup_{\theta\in\Theta}L(\theta;X)}\in[0,1]$$

이며 작은 값에서 기각한다. 통계량 $-2\log\Lambda$는 클수록 귀무가설에 반하는 증거다.

예제 5.8 (알려진 분산의 정규 평균) $H_0:\mu=\mu_0$이면 제곱합 분해 $\sum_i(x_i-\mu_0)^2=\sum_i(x_i-\bar{x})^2+n(\bar{x}-\mu_0)^2$로부터

$$-2\log\Lambda=\frac{n(\overline{X}_n-\mu_0)^2}{\sigma^2}.$$

귀무가설 아래에서 정확히 χ^2_1 분포이다. 이 경우에는 점근근사가 아니라 정규 평균의 정확한 분포에서 결론이 나온다.

일반적인 정칙 모수모형에서는 Wilks 정리에 의해 귀무가설 아래의 우도비 통계량이 자유도 $d - d_0$인 카이제곱분포로 수렴한다. 여기서 d와 d_0는 전체와 귀무모형의 국소 차원이며, 식별가능성, 매끄러움, 내부의 참모수, 비특이한 정보량 등 정칙 조건이 필요하다. 분산성분이 0인 경계, 식별되지 않는 혼합모형, 표본 크기와 함께 커지는 차원 등에서는 그 결론이 바뀔 수 있다. 이 장에서는 정직한 고정 차원 결과만 진술한다.

신뢰구간과 검정은 대응한다. 각 θ_0를 수준 α 검정으로 판단하고 기각되지 않는 값들을 모으면 $1-\alpha$ 신뢰집합이 된다. 실제 참값이 그 집합에서 제외되는 사건은 참 귀무가설을 기각하는 사건이므로 포함확률 보장이 따른다. “기각되지 않는 값”은 참이라고 입증된 값이 아니라 해당 절차로 배제하지 못한 값이다.

5.6 여러 검정을 할 때의 오류

m개 귀무가설 중 참인 것의 개수를 m_0라 하자. 잘못 기각한 개수를 V, 전체 기각 개수를 R이라 한다. 적어도 하나의 거짓 기각이 날 확률

$$\mathrm{FWER} = \mathbb{P}(V \geq 1)$$

을 **가족별 오류율**(*family-wise error rate*)이라 하고, 거짓 발견 비율의 기대값

$$\mathrm{FDR} = \mathbb{E}\left[\frac{V}{\max(R, 1)}\right]$$

을 **거짓 발견율**(*false discovery rate*)이라 한다. 둘은 서로 다른 기준이다. FDR을 통제한다고 모든 자료에서 거짓 발견 비율이 그 수준 이하라는 뜻은 아니다. FWER은 하나라도 잘못 기각하는 사건을 통제하므로 더 엄격한 기준이다($V/\max(R,1) \leq \mathbf{1}_{\{V \geq 1\}}$이므로 FDR $\leq$ FWER).

명제 5.9 (Bonferroni 방법) 각 개별 p값이 자신의 귀무가설 아래에서 유효하면, $p_j \leq \alpha/m$일 때만 기각하는 절차의 FWER은 α 이하이다. 검정들 사이 독립성은 필요 없다.

증명. 참 귀무가설 집합을 I_0라 하면 합집합 상계로

$$\mathbb{P}(V \geq 1) \leq \sum_{j \in I_0} \mathbb{P}(p_j \leq \alpha/m) \leq m_0 \alpha / m \leq \alpha. \qquad \square$$

명제 5.10 (Holm 방법) p값을 $p_{(1)} \leq \cdots \leq p_{(m)}$로 정렬하고, 작은 것부터 $p_{(j)} \leq \alpha/(m-j+1)$인지 확인하며 처음 실패하면 멈추어 그 앞의 가설들만 기각한다. 개별 p값이 유효하면 임의의 의존성에서 FWER은 α 이하이다.

증명. 정렬된 순서에서 처음 나오는 참 귀무가설의 순위를 j라 하자. 그 앞의 $j-1$개는 모두 거짓 귀무가설이므로 $j - 1 \leq m - m_0$, 곧 $m - j + 1 \geq m_0$이다. Holm이 참 귀무가설을 하나라도 기각하면 $p_{(j)}$를 기각한 것이므로 $p_{(j)} \leq \alpha/(m-j+1) \leq \alpha/m_0$이다. 따라서 $\{V \geq 1\} \subseteq \{\min_{i \in I_0} p_i \leq \alpha/m_0\}$이고 합집합 상계로

$$\mathbb{P}(V \geq 1) \leq \sum_{i \in I_0} \mathbb{P}(p_i \leq \alpha/m_0) \leq m_0 \cdot \frac{\alpha}{m_0} = \alpha. \qquad \square$$

같은 개별 유효성 아래 임의의 의존성에도 FWER을 통제하며 Bonferroni보다 덜 보수적일 수 있다.

예제 5.11 (Holm의 단계별 판단) $m=4$, 정렬된 p값이 $0.003, 0.012, 0.018, 0.20$, $\alpha=0.05$라고 하자. 문턱은 차례로 0.0125, 약 0.01667, 0.025, 0.05이다. 앞의 세 개는 통과하고 마지막은 실패하므로 세 가설을 기각한다. Bonferroni의 동일 문턱 0.0125에서는 두 개만 기각된다.

5.7 FDR과 Benjamini–Hochberg 절차

Benjamini–Hochberg 절차는 정렬된 p값에 대해

$$k=\max\{j : p_{(j)} \le jq/m\} \tag{5.3}$$

를 찾고 처음 k개를 기각한다. 해당하는 j가 없으면 아무것도 기각하지 않는다. 중간 단계가 실패했다고 즉시 멈추는 Holm과 달리, 조건을 만족하는 가장 큰 인덱스를 찾는 단계상향 절차다.

모든 p값이 서로 독립이고 참 귀무가설의 p값이 유효하면 FDR은 $qm_0/m \le q$이다. 특정한 양의 의존성 조건에서도 확장되지만, 아무 의존성에서나 같은 q 보장이 성립하는 것은 아니다. 임의의 의존성에 대한 한 보수적 보정은 문턱 $jq/(mH_m)$을 쓰는 것이며 $H_m=\sum_{j=1}^{m} 1/j$이다. 이 심화 보장들의 증명은 다중검정의 후속 장에서 다룬다.

예제 5.12 (단계상향 규칙) $m=5$, $q=0.05$, 정렬된 p값이 $0.004, 0.018, 0.029, 0.041, 0.20$이면 문턱은 $0.01, 0.02, 0.03, 0.04, 0.05$이다. 가장 큰 통과 인덱스는 3이므로 처음 세 개를 기각한다. 이 자료에서 참 귀무가설들이 무엇인지 모르면 실제 거짓 발견 개수 V를 관측된 p값만으로 직접 알 수는 없다.

반복해서 중간 결과를 확인하고 $p<0.05$가 처음 나타날 때 보고하는 절차도 여러 번의 기회를 사용한다. 고정 표본용 p값의 단일 시점 보장이 자동으로 반복 관찰 전체를 통제하지 않는다. 예를 들어 서로 독립인 참 귀무 검정 20개를 각 0.05 수준으로 하면 적어도 하나 기각할 확률은 $1-0.95^{20}\approx 0.64151$이다. 실제 순차 검정은 서로 의존할 수 있어 이 숫자를 그대로 쓰지는 않지만, 분석 기회의 수를 절차의 일부로 다루어야 한다는 원리는 같다.

역사 (다중검정 절차). Bonferroni 보정은 Bonferroni 부등식에 기반하고, Holm의 단계하강 절차는 S. Holm(1979)이, FDR과 단계상향 절차는 Y. Benjamini와 Y. Hochberg(1995)가 제안했다. 단순가설의 최강력 검정은 J. Neyman과 E. S. Pearson(1933)의 결과이다.

5.8 연습문제와 해설

연습문제 5.13 한 검정의 유의수준이 0.05이고 특정 대립값에서 검정력이 0.8이다. 그 대립값에서 제2종 오류 확률을 구하라.

풀이. 0.2이다. 유의수준 0.05와 더해 1이 되는 값이 아니며, 서로 다른 참모수 아래에서 평가한 오류들이다.

연습문제 5.14 참 귀무가설 아래 p값이 균등분포일 때 $p \le 0.01$로 기각하는 절차의 제1종 오류 확률은 얼마인가?

풀이. 정확히 0.01이다. 보수적인 이산 p값이면 0.01 이하일 수 있다. p값 정의의 초균등 성질이 핵심이다.

연습문제 5.15 $m = 10$개 검정의 FWER을 0.05 이하로 통제하는 Bonferroni 개별 문턱을 구하라. 독립성은 필요한가?

풀이. 문턱은 0.005이다. 개별 p값의 유효성이 있으면 합집합 상계로 증명되므로 독립성은 필요 없다.

연습문제 5.16 $R = 0$인 자료에서 거짓 발견 비율 $V/\max(R, 1)$은 얼마인가? FDR에서 이 규약을 사용하는 이유는 무엇인가?

풀이. 아무 기각도 없으면 $V = 0$이므로 비율은 0이다. $0/0$을 피하고 거짓 발견이 없다는 자연스러운 값을 부여한다.

연습문제 5.17 평균의 두쪽 95% 신뢰구간에 μ_0가 포함되지 않는다. 대응하는 같은 모형과 같은 절차의 수준 0.05 검정은 어떤 결정을 하는가?

풀이. $H_0 : \mu = \mu_0$를 기각한다. 이 대응은 같은 검정을 뒤집어 만든 구간일 때의 결론이다. 서로 다른 근사식이나 다른 오류 배분을 섞으면 정확히 대응하지 않을 수 있다.

참고 (다음 연결). 빈도주의 검정은 참모수별 반복표본 오류를 평가한다. 다음 장은 모수에 확률분포를 부여하고 자료를 관측한 뒤 그 분포를 갱신하는 베이지안 추론을 소개한다(제22권 제6장).

제 6 장

베이지안 추론의 기본

개요 베이지안 추론(*Bayesian inference*)은 미지 모수에 관한 불확실성을 사전분포로 표현하고, 자료를 관측한 뒤 Bayes 공식으로 사후분포로 갱신하는 추론 방식이다. 이 장은 사전분포·우도·사후분포를 정의하고, 베타–이항 모형과 정규 평균 모형에서 사후분포를 직접 계산하며, 손실함수에 따른 Bayes 결정(사후평균·사후중앙값), 신용구간, 사후예측분포, Bayes 인자, 부적절 사전분포를 차례로 다룬다. 모든 결과는 사전분포와 우도 두 요소에 함께 의존하므로, 어느 결론이든 두 요소를 명시해야 재현할 수 있다. 선행 지식: Bayes 공식, 베타·감마·정규분포, 조건부 기대값. 사전분포와 우도는 서로 다른 입력이며 갱신 후에도 모형 가정을 점검해야 한다.

베이지안 추론은 미지 모수에 관한 불확실성을 사전분포로 표현하고, 자료를 관측한 뒤 사후분포로 갱신한다. 여기서 모수에 확률을 부여한다는 것은 측정 전에 모수가 물리적으로 매번 새로 추첨된다는 가정만을 뜻하지는 않는다. 추론의 대상에 대한 불확실성을 확률모형으로 기술하는 방식이다. 결과는 사전분포와 우도 모두에 의존하므로 두 요소를 명시해야 재현할 수 있다.

6.1 사전분포, 우도, 사후분포

정의 6.1 (사전밀도, 주변 자료밀도, 사후밀도) 모수의 **사전밀도**(*prior density*) $\pi(\theta)$와 자료의 조건부 밀도 $f(x \mid \theta)$가 주어졌다고 하자. x를 고정하고 θ의 함수로 본 $f(x \mid \theta)$를 **우도**(*likelihood*)라고 한다. **주변 자료밀도**

$$m(x) = \int f(x \mid \theta)\, \pi(\theta)\, \mathrm{d}\theta \tag{6.1}$$

가 유한하고 양수이면 **사후밀도**(*posterior density*)는

$$\pi(\theta \mid x) = \frac{f(x \mid \theta)\, \pi(\theta)}{m(x)} \tag{6.2}$$

이다. 이산 모수에서는 적분을 합으로 바꾼다.

식 (6.2)은 결합밀도 $f(x \mid \theta)\pi(\theta)$를 x의 주변밀도로 나눈 조건부 밀도이므로 Bayes 공식의 밀도 형태이다. 자료 x가 고정되면 $m(x)$는 모수에 의존하지 않는 정규화 상수이다. 그래서 계산 중에는 "사후분포는 우도 곱하기 사전에 비례한다", 곧 $\pi(\theta \mid x) \propto f(x \mid \theta)\pi(\theta)$라고 쓸 수 있다. 그러나 최종 확률이나 예측을 계산할 때에는 정규화가 존재하는지, 곧 $0 < m(x) < \infty$인지 확인해야 한다. 우도만으로 사후분포를 정의하는 것이 아니다.

독립성은 여전히 조건부 구조로 읽는다. 보통 자료들은 모수 θ가 주어지면 독립이다. 모수를 적분한 주변분포에서는 같은 미지 모수를 공유하기 때문에 서로 의존할 수 있다. 이 의존성은 사후예측에서도 나타난다(6.6절).

6.2 베타–이항 갱신

독립 Bernoulli 표본에서 성공합 $S = s$, 표본 수 n이고 사전분포가 $p \sim \mathrm{Beta}(a, b)$ $(a, b > 0)$라고 하자. 성공확률이 p인 표본 $x_1, \dots, x_n$의 우도는 $p^{s}(1-p)^{n-s}$이다. 우도와 사전을 곱하면

$$p^{s}(1-p)^{n-s}\, p^{a-1}(1-p)^{b-1} = p^{a+s-1}(1-p)^{b+n-s-1} \tag{6.3}$$

이다. 이것은 $\mathrm{Beta}(a+s,\ b+n-s)$ 밀도의 핵(상수배를 뺀 부분)이므로

$$p \mid x \sim \mathrm{Beta}(a+s,\ b+n-s). \tag{6.4}$$

정규화 상수까지 따지면 수열 x의 주변 확률은 베타함수 $B(\cdot,\cdot)$로 $m(x) = B(a+s, b+n-s)/B(a,b)$이다. 이처럼 사후분포가 사전과 같은 분포족에 남는 경우를 **켤레성**(*conjugacy*)이라 한다. 계산을 단순하게 하지만 해당 사전이 과학적으로 적절한지는 별도 문제이다.

사후평균은

$$\mathbb{E}[p \mid x] = \frac{a+s}{a+b+n} = \frac{a+b}{a+b+n}\cdot\frac{a}{a+b} + \frac{n}{a+b+n}\cdot\frac{s}{n} \tag{6.5}$$

이다. $n > 0$일 때 사전평균 $a/(a+b)$와 표본비율 s/n의 가중평균이며 가중치는 $a+b$와 n에 비례한다. 이 모형 안에서는 $a+b$가 사전 정보의 크기를 비교하는 한 척도로 작동하지만, 모든 사전분포에서 하나의 보편적 "가상 표본 수"가 정의되는 것은 아니다.

> **예제 6.2 (성공 일곱 번의 갱신)** 균등 사전 $\mathrm{Beta}(1,1)$에서 10번 중 성공 7번을 관측하면 사후는 $\mathrm{Beta}(8,4)$이다. 사후평균은 $2/3$이고, 두 모양 모수가 1보다 크므로 사후최빈값은
>
> $$\frac{8-1}{8+4-2} = 0.7$$
>
> 이다. 사후분산은 $8\cdot 4/(12^2\cdot 13) = 2/117 \approx 0.017094$이다. 표본비율, 사후평균, 사후최빈값은 서로 다른 요약이며 우연히 같아야 할 이유가 없다.
>
> 사전이 $\mathrm{Beta}(20,20)$이라면 같은 자료의 사후는 $\mathrm{Beta}(27,23)$이고 사후평균은 $27/50 = 0.54$이다. 사전이 더 강하게 $1/2$ 근처에 집중되어 있어서 자료가 끌어당기는 정도가 작다. 사전 선택이 결과에 영향을 준다는 사실을 감추지 말고, 해석 가능한 다른 사전들에서 주요 결론이 얼마나 변하는지 비교한다.

6.3 정규 평균의 켤레 갱신

독립 $X_i \mid \mu \sim \mathrm{N}(\mu, \sigma^2)$이고 알려진 $\sigma^2 > 0$를 사용한다. 사전은 $\mu \sim \mathrm{N}(m_0, \tau_0^2)$, $\tau_0^2 > 0$이다. 지수의 제곱항을 완전제곱하면

$$\mu \mid x \sim \mathrm{N}(m_n, \tau_n^2), \qquad \frac{1}{\tau_n^2} = \frac{1}{\tau_0^2} + \frac{n}{\sigma^2}, \qquad m_n = \tau_n^2\left(\frac{m_0}{\tau_0^2} + \frac{n\bar{x}}{\sigma^2}\right) \tag{6.6}$$

을 얻는다.

유도 (완전제곱). 항등식 $\sum_i (x_i-\mu)^2 = \sum_i (x_i-\bar{x})^2 + n(\bar{x}-\mu)^2$에서 μ에 의존하는 부분은 $n(\mu-\bar{x})^2$ 뿐이므로

$$\pi(\mu \mid x) \propto \exp\!\left[-\frac{(\mu-m_0)^2}{2\tau_0^2} - \frac{n(\mu-\bar{x})^2}{2\sigma^2}\right].$$

지수의 μ에 관한 이차식을 정리하면

$$-\frac{1}{2}\left[\left(\frac{1}{\tau_0^2}+\frac{n}{\sigma^2}\right)\mu^2-2\mu\left(\frac{m_0}{\tau_0^2}+\frac{n\bar{x}}{\sigma^2}\right)\right]+(\mu\text{에 무관한 항})=-\frac{(\mu-m_n)^2}{2\tau_n^2}+(\mu\text{에 무관한 항})$$

이다. μ에 무관한 항은 정규화 상수에 흡수되므로 식 (6.6)을 얻는다.

역분산을 **정밀도**(*precision*)라고 부르면 사후정밀도는 사전정밀도와 자료정밀도 n/σ^2의 합이다. 사후평균은 두 중심 m_0, $\bar{x}$의 정밀도 가중평균이다. 분산을 알고 있다는 가정이 중요하며, 분산도 미지이면 공동 사전과 다른 갱신식이 필요하다.

예제 6.3 $m_0=0$, $\tau_0^2=9$, $\sigma^2=4$, $n=4$, $\bar{x}=3$이면

$$\tau_n^2=\frac{1}{1/9+1}=0.9,\qquad m_n=0.9\,(3)=2.7$$

이다. 여기서 $n\bar{x}/\sigma^2=4\cdot 3/4=3$이고 $m_0/\tau_0^2=0$이다. 사후평균은 표본평균 3에서 사전중심 0 쪽으로 조금 이동한다. 사후 표준편차는 $\sqrt{0.9}\approx 0.948683$이다. 사전분산을 매우 크게 하면 사후평균은 $\bar{x}$에, 사후분산은 σ^2/n에 접근한다.

6.4 손실함수와 Bayes 추정량

정의 6.4 (Bayes 결정) 결정값 d와 모수 θ에 대한 손실 $L(d,\theta)$를 정하면, 주어진 자료에서 **사후기대손실**

$$\rho(d\mid x)=\int L(d,\theta)\,\pi(\theta\mid x)\,\mathrm{d}\theta$$

를 최소화하는 결정을 **Bayes 결정**이라고 한다.

명제 6.5 (제곱손실과 절대손실) 사후 이차 모멘트가 유한하면 제곱손실 $L(d,\theta)=(d-\theta)^2$의 최적 결정은 사후평균이다. 사후 절대 모멘트가 유한하면 절대손실 $|d-\theta|$의 최소화 해는 사후중앙값이다.

증명. 제곱손실은

$$\mathbb{E}[(d-\theta)^2\mid x]=\operatorname{Var}(\theta\mid x)+\big(d-\mathbb{E}[\theta\mid x]\big)^2$$

로 분해된다. 오른쪽 둘째 항은 $d=\mathbb{E}[\theta\mid x]$에서만 0이므로 최소해는 사후평균이고 최소 위험은 사후분산이다.

절대손실의 경우 d를 조금 증가시켰을 때 왼쪽 질량은 손실을 늘리고 오른쪽 질량은 줄인다. 최소조건은 사후질량이 양쪽에 각각 적어도 절반씩 있도록 하는 것이며, 원자질량까지 포함하면 $\mathbb{P}(\theta\le d\mid x)\ge 1/2$, $\mathbb{P}(\theta\ge d\mid x)\ge 1/2$가 된다. 이를 정확히 확인하면 다음과 같다. $d<d'$이면

$$|\theta-d'|-|\theta-d|=\begin{cases} d'-d, & \theta\le d,\\ d+d'-2\theta\in\big(-(d'-d),\,d'-d\big), & d<\theta<d',\\ -(d'-d), & \theta\ge d'\end{cases}$$

이므로 $\theta > d$일 때 이 차는 $-(d' - d)$ 이상이고, $\theta < d'$일 때 $d' - d$ 이하이다. 사후기대를 취하면

$$\rho(d' \mid x) - \rho(d \mid x) \geq (d' - d)\big[2\mathbb{P}(\theta \leq d \mid x) - 1\big],$$
$$\rho(d' \mid x) - \rho(d \mid x) \leq (d' - d)\big[2\mathbb{P}(\theta < d' \mid x) - 1\big].$$

d가 중앙값이면 $\mathbb{P}(\theta \leq d \mid x) \geq 1/2$이므로 첫 부등식에서 모든 $d' > d$에 대해 $\rho(d') \geq \rho(d)$이다. $d' < d$인 경우도 대칭으로 $\mathbb{P}(\theta \geq d \mid x) \geq 1/2$에서 같은 결론을 얻는다. 따라서 중앙값은 최소해이다. 역으로 $\mathbb{P}(\theta \leq d \mid x) < 1/2$이면 $d' \downarrow d$일 때 $\mathbb{P}(\theta < d' \mid x) \downarrow \mathbb{P}(\theta \leq d \mid x) < 1/2$이므로 둘째 부등식에 의해 d보다 위험이 작은 d'이 있다. $\mathbb{P}(\theta \geq d \mid x) < 1/2$인 경우도 대칭이다. 따라서 최소해는 모두 사후중앙값이다. $\square$

최대사후밀도점(*maximum a posteriori*, MAP)은 흔히 쓰이는 다른 요약이다. 하지만 연속 모수에 대해 단순한 "정확히 맞히면 손실 0, 아니면 1"을 쓰면 한 점의 사후확률이 모두 0이어서 모든 결정의 위험이 같다. MAP의 정당화에는 작은 근방 손실의 극한 등 추가 해석이 필요하다. 또한 밀도는 좌표변환의 야코비안을 받으므로 MAP는 일반적으로 비선형 재매개화에 불변하지 않다. MLE의 변환 성질과 혼동하지 않는다.

6.5 신용구간과 신뢰구간의 구별

사후확률이 $1 - \alpha$인 모수 집합을 **신용집합**(*credible set*)이라고 하며, 구간이면 **신용구간**이라고 한다. 연속 사후분포의 분위수 $q_{\alpha/2}, q_{1-\alpha/2}$를 사용하면 같은 꼬리 확률의 신용구간을 얻는다. 자료가 주어진 조건에서 모수에 사후확률을 부여하는 것이므로 빈도주의 신뢰구간과 확률의 대상이 다르다.

정규 사후분포에서는 대칭 구간

$$m_n \pm z_{1-\alpha/2}\,\tau_n$$

이 같은 꼬리 신용구간이다. 앞의 수치 예에서는 95% 구간이 약 $[0.84061, 4.55939]$이다. 이 구간 절차가 모든 고정된 μ에서 정확히 95%의 빈도주의 포함확률을 갖는다는 결론은 별도 검증 없이 따라오지 않는다. 사전모형까지 포함한 공동분포 아래의 평균적인 포함확률과 각 참모수에서의 포함확률은 다르다.

참고 (고정 모수에서의 포함확률). 예제 6.3의 설정($m_0 = 0$, $\tau_0^2 = 9$, $\sigma^2 = 4$, $n = 4$)에서 참모수가 μ로 고정되면 $\bar{x} \sim \mathrm{N}(\mu, 1)$이고

$$m_n - \mu = \frac{\tau_n^2}{\tau_0^2}(m_0 - \mu) + \frac{\tau_n^2 n}{\sigma^2}(\bar{x} - \mu) = -0.1\,\mu + 0.9\,Z, \qquad Z \sim \mathrm{N}(0,1)$$

이다. 구간의 반길이는 $1.959964 \cdot 0.948683 \approx 1.8594$이므로 포함확률은 $\mathbb{P}(|-0.1\mu + 0.9Z| \leq 1.8594)$이다. 수치로 계산하면 $\mu = 0$에서 약 0.961, $\mu = 3$에서 약 0.950, $\mu = 5$에서 약 0.930, $\mu = 10$에서 약 0.829이다. 사전중심에서 멀어질수록 사후평균의 편향 때문에 포함확률이 공칭 수준 95%보다 낮아진다.

최고사후밀도(*highest posterior density*) 집합은 사후밀도가 일정 문턱 이상인 점들을 모아 지정된 질량을 만드는 방식이다. 단봉 분포에서는 구간이 될 수 있지만 다봉 분포에서는 여러 조각일

수 있다. 같은 꼬리 구간과 항상 같지 않으며, 밀도 기반이므로 재매개화에 대한 성질도 분위수 구간과 다르다.

6.6 사후예측분포

정의 6.6 (사후예측분포) 새 관측 $\widetilde{X}$가 모수가 주어지면 기존 자료와 조건부 독립이라고 하자. **사후예측분포**(*posterior predictive distribution*)는

$$p(\tilde{x} \mid x) = \int f(\tilde{x} \mid \theta)\, \pi(\theta \mid x)\, \mathrm{d}\theta$$

이다.

모수를 하나의 추정값으로 고정해 대입하는 것과 달리, 사후예측은 모수의 남은 불확실성을 적분한다. 전체 분산 공식으로

$$\operatorname{Var}(\widetilde{X} \mid x) = \mathbb{E}\big[\operatorname{Var}(\widetilde{X} \mid \theta, x) \mid x\big] + \operatorname{Var}\big(\mathbb{E}[\widetilde{X} \mid \theta, x] \mid x\big) \tag{6.7}$$

을 얻는다. 첫 항은 모수를 알아도 남는 관측 변동이고 둘째는 모수 불확실성의 기여이다.

정규 평균 예에서는 $\widetilde{X} = \mu + \varepsilon$, $\varepsilon \sim \mathrm{N}(0, \sigma^2)$이 $\mu \mid x$와 독립이므로 두 정규분포의 합으로서

$$\widetilde{X} \mid x \sim \mathrm{N}\!\left(m_n,\ \sigma^2 + \tau_n^2\right)$$

이다. 수치 예의 예측분산은 $4 + 0.9 = 4.9$이다. 평균 모수의 사후분산 0.9보다 크며, 새 관측을 예측하는 구간과 평균에 대한 신용구간을 구별해야 한다.

베타–이항 모형에서 사후가 $\mathrm{Beta}(A, B)$이면 다음 한 번의 성공확률은 $A/(A+B)$이다. 다음 m번의 성공 개수 K는

$$\mathbb{P}(K = k \mid x) = \binom{m}{k} \frac{B(A + k,\ B + m - k)}{B(A, B)}, \qquad k = 0, \dots, m \tag{6.8}$$

인 베타이항 예측분포를 따른다. 여기서 $B(\cdot,\cdot)$는 베타함수이며 모수 B와 문맥으로 구별한다. 평균과 분산은

$$\mathbb{E}[K \mid x] = \frac{mA}{A+B}, \qquad \operatorname{Var}(K \mid x) = \frac{mAB(A+B+m)}{(A+B)^2(A+B+1)} \tag{6.9}$$

이다.

유도 (베타이항 예측분포). $K \mid p \sim \mathrm{Binomial}(m, p)$이므로 $\mathbb{P}(K=k \mid x) = \binom{m}{k}\mathbb{E}[p^k(1-p)^{m-k} \mid x]$이고, 베타 적분 $\int_0^1 p^{A+k-1}(1-p)^{B+m-k-1}\,\mathrm{d}p = B(A+k, B+m-k)$을 $B(A,B)$로 나누면 식 (6.8)이다. 평균은 $\mathbb{E}[mp \mid x] = mA/(A+B)$이다. 분산은 식 (6.7)에서 $\mathbb{E}[mp(1-p) \mid x] + \operatorname{Var}(mp \mid x)$이고, $\mathbb{E}[p(1-p) \mid x] = AB/\big((A+B)(A+B+1)\big)$, $\operatorname{Var}(p \mid x) = AB/\big((A+B)^2(A+B+1)\big)$이므로

$$\frac{mAB}{(A+B)(A+B+1)}\left(1 + \frac{m}{A+B}\right) = \frac{mAB(A+B+m)}{(A+B)^2(A+B+1)}$$

이다.

예제 6.7 (미래 시행의 주변 의존성) 사후가 $\mathrm{Beta}(8,4)$일 때 다음 두 번이 모두 성공할 확률은

$$\mathbb{E}[p^2 \mid x] = \frac{8\cdot 9}{12\cdot 13} = \frac{6}{13} \approx 0.461538$$

이다. 사후평균을 고정해 두 독립 시행에 대입한 값 $(2/3)^2 = 4/9$와 다르다. 두 미래 시행은 p가 주어졌을 때 독립이지만, p를 적분한 사후예측에서는 같은 미지의 성공확률을 공유하므로 양의 공분산 $\mathrm{Var}(p \mid x) = 2/117$을 갖는다. 실제로 $6/13 - 4/9 = (54-52)/117 = 2/117$이다.

6.7 Bayes 인자와 점가설

두 모형 H_0, H_1이 각각 모수에 대한 적절한 사전분포를 가지면 주변 자료밀도 $m_0(x), m_1(x)$를 계산할 수 있다. **Bayes 인자**(*Bayes factor*)와 사후 오즈의 관계는

$$B_{01}(x) = \frac{m_0(x)}{m_1(x)}, \qquad \frac{\mathbb{P}(H_0 \mid x)}{\mathbb{P}(H_1 \mid x)} = B_{01}(x)\,\frac{\mathbb{P}(H_0)}{\mathbb{P}(H_1)} \tag{6.10}$$

이다. 이 관계는 두 모형을 별도의 가설로 두고 사전확률을 부여했을 때의 Bayes 공식이다. 연속 사전만 가진 한 모형에서는 특정 점 $\theta = \theta_0$의 사전질량이 0이면 통상적인 밀도 갱신 후에도 그 점의 사후질량은 0이다. 점가설에 양의 확률을 주려면 점질량 또는 별도 모형 지시변수를 포함해야 한다.

예제 6.8 (이항검정의 p값과 다른 질문) $n = 10$, $S = 9$에서 $H_0 : p = 1/2$와 $H_1 : p \sim \mathrm{Beta}(1,1)$을 비교하자. 성공 개수의 주변확률은

$$m_0(9) = \binom{10}{9}\frac{1}{2^{10}} = \frac{10}{1024}, \qquad m_1(9) = \binom{10}{9}\int_0^1 p^9(1-p)\,\mathrm{d}p = \frac{10}{110} = \frac{1}{11}$$

이다. 따라서 $B_{01} = 110/1024 \approx 0.107422$이다. 두 가설의 사전확률이 같으면 H_0의 사후확률은 $110/(1024+110) \approx 0.097002$이다. 앞 장(제22권 제5장)의 한쪽 p값 $\mathbb{P}(S \ge 9 \mid p = 1/2) = 11/1024$와 다른 값이며, 서로 다른 확률적 질문에 답하기 때문이다. 대립 사전분포나 모형 사전오즈를 바꾸면 사후확률도 바뀐다.

6.8 부적절 사전과 사후 정규화

적분이 1인 확률분포가 아니라 상수배까지 정한 함수만을 사전처럼 사용하는 경우가 있다. 예를 들어 정규 평균에 대한 평평한 $\pi(\mu) \propto 1$은 실수축에서 적분이 무한하므로 적절한 확률분포가 아니다(**부적절 사전**, *improper prior*). 알려진 양의 분산과 $n \ge 1$의 정규자료에서는 우도와 곱한 사후가 정규화되어 $\mathrm{N}(\bar{x}, \sigma^2/n)$이 된다. 이는 식 (6.6)에서 $\tau_0^2 \to \infty$로 보낸 극한과 같다.

이처럼 부적절 사전으로도 적절한 사후를 얻을 수 있지만 항상 그런 것은 아니다. 사후 적분의 유한성을 따로 확인해야 한다. 또한 사전에 임의의 곱셈 상수가 남아 있으면 주변 자료밀도와 Bayes 인자가 그 상수에 영향을 받으므로, 일반적인 모형 비교에 같은 방식으로 그대로 사용할 수 없다. 모수의 점추정에 괜찮았던 사전이 모형 비교에도 자동으로 적합한 것은 아니다.

사전민감도 분석(*prior sensitivity analysis*)은 해석 가능한 여러 사전에서 핵심 추정값, 구간, 예측이 얼마나 달라지는지 확인하는 작업이다. **사후예측 점검**(*posterior predictive check*)은 모형

에서 새 자료를 생성했을 때 실제 자료의 중요한 특징을 재현하는지 비교한다. 이 점검이 모형을 참이라고 증명하지는 않지만, 우도와 사전의 조합이 놓치는 구조를 찾는 데 유용하다.

6.9 연습문제와 해설

연습문제 6.9 $p \sim \mathrm{Beta}(2,3)$이고 8번 중 성공 5번을 관측했다. 사후분포와 사후평균을 구하라.

풀이. 사후는 $\mathrm{Beta}(7,6)$이며 평균은 $7/13$이다. 사전의 두 모수에는 성공과 실패 수를 각각 더한다.

연습문제 6.10 위 사후에서 다음 두 번이 모두 실패할 확률을 구하라.

풀이. $\mathbb{E}[(1-p)^2 \mid x] = 6\cdot 7/(13\cdot 14) = 3/13$이다. 사후평균의 실패확률 $6/13$을 제곱한 값 $36/169$와 다르다$(3/13 = 39/169)$.

연습문제 6.11 정규 평균의 사전이 $\mathrm{N}(0,1)$, 알려진 관측분산이 4, 표본 수가 4, 표본평균이 2이다. 사후평균과 분산을 구하라.

풀이. 사후정밀도는 $1+4/4 = 2$이므로 분산은 $1/2$이다. 평균은 $(1/2)(0+4\cdot 2/4) = 1$이다. 사전과 자료의 정밀도가 같으므로 두 중심의 중간값이다.

연습문제 6.12 두 모형의 Bayes 인자가 $B_{01} = 3$이고 사전확률이 $\mathbb{P}(H_0) = 1/4$, $\mathbb{P}(H_1) = 3/4$이면 사후확률은 얼마인가?

풀이. 사전 오즈는 $1/3$이고 사후 오즈는 $3\cdot(1/3) = 1$이므로 두 사후확률은 각각 $1/2$이다. Bayes 인자 자체를 사후확률로 읽으면 안 된다.

연습문제 6.13 정규 평균의 사후분산이 0.5이고 새 관측의 조건부 분산이 4이면 사후예측분포의 분산을 구하라.

풀이. 두 기여를 더한 4.5이다. 모수 불확실성이 줄어들어도 관측 자체의 분산 4는 남는다.

참고 (다음 연결). 이 여섯 장은 통계모형에서 점추정·구간·검정·베이지안 갱신으로 이어지는 기본 틀이다. 이후 수리통계에서는 지수족과 결정이론, 점근적 효율성, 회귀·일반화선형모형, 비모수·강건 추론, 재표본과 모형 진단을 각각의 가정과 한계까지 확장한다.

제 28 권

현대 연구 지도·증명 보조기

제28권은 현재의 수학 연구를 읽는 데 무엇을 더 배워야 하는지를 보이는 지도이다. 제1장은 어떤 대상이 정의되었고 어떤 질문이 세워졌으며 어떤 도구를 쓸 수 있는지를 구별하여 연구 문장을 읽는 방법을 정리한다. 제2–5장은 소수의 분포와 덧셈의 구조, Langlands 프로그램, 기하와 위상, 편미분방정식·동역학·확률에서 해가 존재한다는 말의 여러 의미를 선택된 사례로 소개한다. 제6장은 증명 보조기와 mathlib, 인공지능을 다루며 증명된 문장이 의도한 문장인지를 묻는 관점을 제시한다. 이 권은 앞 권들의 입문서를 대체하지 않으며, 소개한 주제는 선택된 사례이다.

제 1 장

현재의 수학을 읽는 법

개요 현재의 수학을 읽는다는 것은 어떤 대상이 정의되었는지, 그 대상에 관해 어떤 질문이 세워졌는지, 사용할 수 있는 도구와 아직 사용할 수 없는 도구가 무엇인지를 구별하는 일이다. 이 장은 정리의 문장을 가정·범위·결론으로 해부하고, 양화사의 순서와 상수의 의존성, 증거·증명·검증의 구별, 불변량의 역할, 논문을 읽는 순서, 두 매개변수의 극한 순서, 정규화의 한계를 작은 예로 점검한다. 선행 지식: 명제와 양화사, 함수, 집합, 수열의 극한. 이 장의 논리적 구분은 뒤의 모든 연구 사례에 적용한다.

수학의 최전선은 알려진 공식의 맨 끝에 붙는 목록이 아니다. 어떤 대상을 정확히 정의하고, 그 대상에 관한 질문을 세우고, 사용할 수 있는 도구와 아직 사용할 수 없는 도구를 구별하는 과정이다. 새로운 정리를 읽을 때 어려운 용어를 모두 이해해야 시작할 수 있는 것은 아니다. 먼저 무엇이 주어지고 무엇을 보장하는지, 어디까지가 증명되었는지, 어떤 예에서 주장에 손으로 접근할 수 있는지를 확인하면 된다.

이 권의 연구 상태 기준일은 2026년 9월 24일이다. 날짜는 장식이 아니라 수학적 설명의 일부다. 오래된 정리의 진위는 발표 날짜가 바뀐다고 달라지지 않지만, 새 원고의 검토 상태와 코드의 버전은 바뀔 수 있다. 이 권은 기본 계산과 작은 정리는 직접 증명하고, 대규모 연구 결과는 원문의 정확한 범위를 소개한다. 수백 쪽의 논증을 몇 문단의 비유로 대체하여 완전한 증명을 제시했다고 말하지 않는다.

1.1 정리의 문장을 먼저 해부하기

가장 간단한 형태의 정리는 다음과 같다.

$$\forall x \in X, \qquad H(x) \implies C(x). \tag{1.1}$$

여기서 X는 대상의 범위, H는 가정, C는 결론이다. 세 부분 중 하나라도 바뀌면 다른 정리가 된다. 실수 전체에서의 주장과 양의 실수에서의 주장, 모든 함수와 연속함수에 대한 주장은 구분해야 한다. 논문 제목에 등장하지 않는 가정이 정리 본문에는 들어 있을 수 있다.

예제 1.1 (최댓값의 존재) 닫힌 유계구간 $[a,b]$ 위의 연속함수는 최댓값을 갖는다. 구간을 (a,b)로 바꾸면 $f(x)=x$가 반례가 된다. 연속성을 제거하면 $[0,1]$에서

$$f(x)=\begin{cases} x, & 0 \le x < 1, \\ 0, & x = 1 \end{cases}$$

가 최댓값을 갖지 않는다. 상한 1은 $x \to 1^-$에서 접근할 뿐 어떤 점에서도 도달하지 않기 때문이다. 유계성이 없으면 $f(x)=x$를 $\mathbb{R}$ 위에서 생각할 수 있다. 각각의 반례는 가정 하나의 역할을 분리해서 보여 준다.

가정을 모두 외우는 것보다 가정이 증명의 어느 지점에 쓰이는지 표시하는 편이 낫다. 위 정리의 순차적 증명에서는 상한에 접근하는 점들을 선택하고, 콤팩트성으로 수렴 부분수열을 얻고, 연속성으로 함수값의 극한을 옮긴다. 존재해야 하는 것은 점 하나지만, 그 점을 찾는 논증에는 공간 전체의 성질이 사용된다.

명제 1.2 비어 있지 않은 콤팩트 거리공간 X와 연속함수 $f : X \to \mathbb{R}$에 대하여 f는 최댓값을 갖는다.

증명. 먼저 f가 위로 유계가 아니라고 가정하자. 각 자연수 n에 대하여 $f(x_n) > n$인 x_n을 고를 수 있다. 콤팩트성으로 부분수열 x_{n_k}가 $x \in X$에 수렴한다. 연속성에 의해 $f(x_{n_k}) \to f(x)$여야 하므로 모순이다($f(x_{n_k}) > n_k \to \infty$). 이제 $M = \sup f(X)$라 놓고 $f(y_n) > M - 1/n$인 점을 고른다. 다시 수렴 부분수열 $y_{n_k} \to y$를 택하면 $f(y) = M$이다. □

참고 (증명에서 쓰인 가정). 증명에서 콤팩트성은 거리공간에서 점렬 콤팩트성의 형태로 두 번 쓰였고, 연속성은 극한을 함수값으로 옮기는 데 쓰였으며, 비공집합이라는 가정은 x_n과 y_n을 고르는 데 쓰였다. 예제 1.1의 정리는 $[a,b]$가 콤팩트(Heine–Borel 정리)이므로 이 명제의 특수한 경우이다.

이 증명은 이후 함수공간에서도 반복된다. 다만 유한차원에서는 익숙한 콤팩트성이 무한차원에서는 실패하기 때문에 약수렴, 에너지 유계성, 적절한 콤팩트성 정리로 바꾸어야 한다. 연구의 큰 부분은 바로 이러한 "증명에 필요한 한 단계"를 새로운 상황에서 회복하는 일이다.

참고 (무한차원에서 최댓값이 사라지는 예). ℓ^2의 닫힌 단위공 $\{x : \sum_k x_k^2 \le 1\}$ 위의 함수 $f(x) = \sum_{k \ge 1} (1 - 1/k) x_k^2$는 연속이고, $x \neq 0$이면 $f(x) < \sum_k x_k^2 \le 1$이다. 그러나 단위벡터 e_k에서 $f(e_k) = 1 - 1/k \to 1$이므로 상한은 1이고 최댓값은 존재하지 않는다. 닫힌 단위공이 노름 위상에서 콤팩트하지 않기 때문이다. e_k는 수렴하는 부분수열을 갖지 않는다.

1.2 양화사의 순서와 균일성

다음 두 문장은 다르다.

$$\forall x\, \exists C_x :\ |f_n(x)| \le C_x \quad (\forall n), \qquad \exists C\, \forall x, n :\ |f_n(x)| \le C.$$

왼쪽에서는 점마다 다른 상수를 쓸 수 있다. 오른쪽에서는 모든 점과 모든 n에 같은 상수를 사용한다. 연구 논문의 $O(1)$이나 $\lesssim$ 기호를 읽을 때는 상수가 어떤 매개변수에 의존하는지 반드시 확인해야 한다.

예제 1.3 (점별수렴과 균등수렴) 함수열 f_n이 f로 **점별수렴**(*pointwise convergence*)한다는 것은 각 x에서 $f_n(x) \to f(x)$라는 뜻이고, **균등수렴**(*uniform convergence*)한다는 것은 $\sup_x |f_n(x) - f(x)| \to 0$이라는 뜻이다. $[0,1)$에서 $f_n(x) = x^n$은 각 고정된 x에 대해 0으로 수렴한다. 그러나

$$\sup_{0 \le x < 1} |f_n(x)| = 1$$

이므로 균등수렴하지 않는다. 임의의 $\varepsilon > 0$에 대하여 각 x마다 충분히 큰 n이 존재한다는 사실은, 모든 x에 공통인 하나의 충분히 큰 n이 존재한다는 사실을 주지 않는다.

수론에서 "충분히 큰 x"라는 말도 같은 주의를 요구한다. 예컨대 임의의 고정된 $\varepsilon > 0$에 대한 추정과 $\varepsilon = 1/\log x$를 대입한 추정은 자동으로 같지 않다. 전자의 숨은 상수가 ε에 따라 빠르게 커질 수 있기 때문이다. $x^{\theta + o(1)}$이라는 표현은 보통 지수의 오차가 0으로 간다는 뜻이지만, 그 오차가 다른 매개변수에 대해 균일한지는 별도 정보이다.

정의 1.4 (점근 기호) $g(x) > 0$일 때 $x \to \infty$에서 $f(x) = O(g(x))$는 어떤 $C > 0$과 x_0가 존재하여 $x \geq x_0$에서 $|f(x)| \leq C g(x)$임을 뜻한다. $f(x) = o(g(x))$는 $f(x)/g(x) \to 0$임을 뜻한다. 상수의 의존성을 강조할 때 O_{ε}처럼 아래첨자를 붙인다.

경계값은 특히 조심해야 한다. 모든 $p > 1$에서 성립하는 정리가 $p = 1$에서도 성립한다고 할 수 없다. 유한한 모든 차원에서 성립하되 상수가 차원에 의존하는 정리가 무한차원에서 같은 형태로 이어진다고 할 수도 없다. "끝점" 문제는 익숙한 증명이 정확히 어디서 무너지는지를 묻는 연구 문제인 경우가 많다.

1.3 증거, 증명, 검증의 서로 다른 역할

수학에서는 예를 많이 계산하는 것이 매우 유용하지만, 보편명제를 증명하려면 그 계산이 모든 경우를 덮는 이유가 있어야 한다. 단순한 패턴 탐색과 유한한 전체 경우의 인증은 다르다. 전자는 추측의 근거이고, 후자는 경우의 완전성과 계산의 정확성이 확보되면 증명의 일부가 된다.

예제 1.5 (많은 초깃값이 충분하지 않은 이유) 다항식 $n^2 + n + 41$은 $n = 0, 1, 2$에서 소수를 준다. 더 많은 작은 값을 확인하면 강한 패턴이 보이지만, $n = 40$에서는

$$40^2 + 40 + 41 = 1681 = 41^2$$

이다. 유한한 표는 모든 자연수에 관한 명제의 증명이 될 수 없다. 반대로 "$0 \leq n \leq 39$의 각 값이 소수인가"는 유한한 문제이며, 소수판정의 정확성을 보장하는 계산으로 완결할 수 있다. 실제로 $n = 0, \dots, 39$ 모두에서 이 값은 소수이다. $n = 41$에서도 $41^2 + 41 + 41 = 41 \cdot 43$으로 합성수이다. 이 다항식은 Euler가 지적한 것으로 알려져 있다.

다음 네 가지 상태를 구분하면 연구 결과를 읽기가 수월하다.

(1) **추측**(*conjecture*): 정확한 문장은 있으나 일반적인 증명 또는 반례가 아직 제시되지 않은 상태.

(2) **공개된 증명 원고**: 저자가 완전한 논증을 주장하며 자료를 공개한 상태. 공개와 동료심사 완료는 다른 사건이다.

(3) **검토된 수학적 결과**: 전문가의 검토와 출판 이력이 있는 상태. 오탈자나 후속 수정 가능성은 여전히 존재한다.

(4) **형식 증명**(*formal proof*): 지정된 형식 체계 안에서 정확한 명제가 커널에 의해 검증되는 증명 항으로 표현된 상태. 어떤 공리를 사용했는지도 함께 읽어야 한다.

이 구분은 일렬로 늘어선 등급표가 아니다. 형식화된 명제가 원래 의도한 문제와 다를 수 있고, 훌륭한 비형식 증명이 형식화되지 않았다는 이유만으로 불완전해지는 것도 아니다. 수치 계산, 인간의 설명, 형식 검증은 각기 다른 질문에 답한다. 정확한 계산 결과를 얻었는지, 왜 참인지 이해했는지, 모든 논리적 의존성을 검사했는지를 따로 물어야 한다.

1.4 작은 모형에서 추상적 구조까지

큰 이론을 배우는 한 가지 방법은 정의가 실제로 무엇을 구별하는지 작은 예로 시험하는 것이다. 선형대수에서 두 행렬이 닮았다는 말은 행렬의 각 성분이 같다는 뜻이 아니다. 같은 선형변환을 서로 다른 기저로 표현했다는 뜻이다.

$$B = P^{-1}AP.$$

따라서 대각합, 행렬식, 고유다항식처럼 기저와 무관한 양을 찾게 된다. 이를 **불변량**(*invariant*)이라고 한다. 불변량은 다르면 대상을 구별하지만, 같다고 항상 대상을 완전히 분류하지는 않는다.

> **예제 1.6 (불변량의 한계)**
> $$A = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$
> 는 모두 대각합과 행렬식이 0이고 고유다항식도 t^2이다. 그러나 A의 계수는 0, B의 계수는 1이므로 닮지 않았다. $P^{-1}AP = 0 \neq B$가 모든 가역행렬 P에서 성립하기 때문이다. 새로운 불변량이 필요한 이유가 이 작은 예에 이미 나타난다.

현대 기하에서 호몰로지, 기본군, 특성류, 스펙트럼, 유도 범주 등을 사용하는 동기도 비슷하다. 문제는 단순히 많은 숫자를 만드는 일이 아니다. 어떤 변형 아래에서 보존되어야 하는 정보인지 먼저 정하고, 그 정보를 계산 가능하게 만드는 일이다. “분류”라는 말은 동형으로 분류하는지, 위상동형으로 분류하는지, 호모토피 동치로 분류하는지에 따라 매우 다른 문제가 된다.

1.5 논문을 읽는 네 번의 통과

첫 번째 통과에서는 초록과 주정리만 읽고 대상, 가정, 결론을 한 문장으로 다시 쓴다. 두 번째에서는 익숙한 특수 경우와 극단적인 경우를 계산한다. 세 번째에서는 증명을 여러 보조정리로 나누고 새 아이디어가 들어간 위치를 찾는다. 네 번째에서는 자신의 목적에 필요한 부분의 세부 논증을 추적한다. 처음부터 모든 줄을 동일한 속도로 읽으려 하면 어떤 단계가 핵심인지 놓치기 쉽다.

논문에서 “표준적이다”라고 생략된 부분을 만났다면, 무엇을 표준으로 사용하는지 기록한다. 예컨대 극한과 적분의 교환에는 지배수렴정리, 단조수렴정리, 균등적분가능성 등 서로 다른 근거가 필요하다. 약수렴하는 두 수열의 곱이 약수렴한다는 결론은 일반적으로 성립하지 않는다. 보조정리를 이름으로 기억하는 데서 그치지 말고 가정과 적용 대상을 함께 적어야 한다.

> **예제 1.7 (극한과 적분 교환의 실패)** $(0,1)$ 위에서 $f_n(x) = n\mathbf{1}_{(0,1/n)}(x)$라 하자. 모든 $x > 0$에 대해 $f_n(x) \to 0$이지만
> $$\int_0^1 f_n(x)\,\mathrm{d}x = 1$$
> 이다. 질량이 좁은 구간에 집중한다. $n > 1/x$이면 $x \notin (0,1/n)$이므로 $f_n(x) = 0$이 되어 점별극한은 0이다. 이후 PDE의 집중 현상, 확률의 균등적분가능성, 측도의 약수렴을 배울 때 이 예를 기준점으로 삼을 수 있다.

연구를 읽는 데 필요한 선수 지식도 한 줄의 긴 목록보다 의존 관계로 정리하는 편이 낫다. Langlands를 읽으려면 대수적 수론과 표현론이 만나야 하고, 기하적 버전에서는 층과 범주의 언

어가 추가된다. 확률 PDE에는 측도론적 확률, 함수해석, PDE의 정칙성 추정이 만난다. 한 분야를 완전히 끝내고 다른 분야로 넘어가야 하는 것이 아니라, 현재 읽는 주장을 이해할 만큼의 연결을 점진적으로 만든다.

1.6 매개변수의 극한을 바꾸면 무엇이 달라지는가

연구의 추정식에는 흔히 두 개 이상의 큰 매개변수가 있다. 예를 들어 표본 크기 n과 차원 d, 작은 공간 해상도 ε과 긴 관측시간 T가 동시에 등장한다. 하나를 고정하고 다른 것을 보내는 극한과 함께 보내는 극한은 다를 수 있다. 계산의 결과뿐 아니라 어느 순서로 극한을 취했는지 기록해야 한다.

예제 1.8 (두 극한의 순서) $a_{m,n} = m/(m+n)$이라 하자. m을 고정하고 $n \to \infty$로 보내면 0이므로

$$\lim_{m\to\infty} \lim_{n\to\infty} a_{m,n} = 0.$$

반대로 n을 고정하고 $m \to \infty$로 보내면 1이므로 순서를 바꾼 극한은 1이다. $m = n$의 대각선에서는 항상 $1/2$이다. 세 결과가 서로 다른 것은 모순이 아니라 서로 다른 질문에 답했기 때문이다.

균일한 추정은 이런 차이를 줄이는 핵심 도구다. $|f_n(x) - f(x)| \le \varepsilon_n$이 모든 x에서 성립하고 $\varepsilon_n \to 0$이면 x가 n에 따라 움직여도 오차는 ε_n 이하이다. 반면 각 고정된 x에서만 오차가 0으로 가면 $x = x_n$을 선택했을 때 실패할 수 있다. 앞에서 본 x^n의 예에서 $x_n = 1 - 1/n$을 택하면 $x_n^n \to e^{-1}$이다.

예제 1.9 (같아 보이는 오차 기호) $f_n(x) = x/n$은 각 고정된 x에 대해 $O(1/n)$이다. 하지만 x가 $\mathbb{R}$ 전체를 움직일 때 같은 상수를 사용할 수 없다. $x = n$을 넣으면 $f_n(n) = 1$이다. 따라서 논문에서 $O_x(1/n)$을 읽고 움직이는 x에 대입하려면 추가 검토가 필요하다.

"일반성을 잃지 않고"라는 문장도 대칭이나 정규화가 실제로 존재해야 사용할 수 있다. 삼각형의 한 꼭짓점을 원점으로 옮기는 것은 평행이동으로 정당화할 수 있다. 그러나 서로 다른 길이의 두 변을 마음대로 모두 1로 만드는 것은 일반적인 등거리 변환으로 할 수 없다. 정규화가 문제의 방정식, 경계조건, 관심량을 어떻게 바꾸는지 계산해야 한다.

명제 1.10 (정규화가 유지하는 비율) $a, b > 0$이고 공통 배율 $\lambda > 0$를 곱하면 a/b는 변하지 않는다. 따라서 하나의 길이를 1로 정규화할 수는 있지만 두 길이의 비율을 독립적으로 바꿀 수는 없다.

증명. $(\lambda a)/(\lambda b) = a/b$이다. $\lambda a = \lambda b = 1$이라면 $a = b$여야 한다. 일반적인 두 길이에 대해 두 조건을 동시에 강제할 수 없다. □

이 단순한 사실은 PDE의 스케일링, 통계의 표준화, 대수기하의 좌표 변경에서도 반복된다. 변환 뒤에 어떤 양이 남고 어떤 양이 바뀌는지 추적하면, 계산을 편하게 만드는 선택과 문제 자체를 바꾸는 선택을 구분할 수 있다. 추상적인 연구 문장을 읽을 때도 이러한 작은 정규화 계산이 좋은 검사 도구다.

1.7 연습과 해설

> **연습문제 1.11** “모든 $x \in \mathbb{R}$에 대해 어떤 자연수 n이 존재하여 $x < n$”과 양화사의 순서를 바꾼 문장을 쓰고, 각각의 진위를 설명하라.

풀이. 첫 문장 $\forall x \in \mathbb{R}\, \exists n \in \mathbb{N} :\ x < n$은 실수의 Archimedes 성질이다. 바꾼 문장 $\exists n \in \mathbb{N}\, \forall x \in \mathbb{R} :\ x < n$은 어떤 자연수 n이 모든 실수보다 크다는 뜻이다. 그 n에 대해 $x = n + 1$을 택하면 반례가 된다. 핵심은 자연수의 크기가 x를 보고 정해지는가이다.

> **연습문제 1.12** $f_n(x) = \mathbf{1}_{[n, n+1]}(x)$를 $\mathbb{R}$ 위에서 생각하라. 점별수렴과 적분을 비교하고 앞의 집중 예와 차이를 설명하라.

풀이. 고정된 x는 충분히 큰 n에 대해 해당 구간 밖에 있으므로 $f_n(x) \to 0$이다. 그러나 적분은 항상 1이다. 앞의 예에서는 질량이 한 점 근처에 집중했고 여기서는 무한대로 이동한다. 두 현상 모두 점별수렴만으로 적분을 제어할 수 없음을 보인다.

> **연습문제 1.13** 정리 $H \Rightarrow C$의 증명에 대해 H의 일부가 없어도 참일지 조사하려 한다. 어떻게 순서를 정하면 좋을까?

풀이. 먼저 기존 증명에서 그 가정이 사용되는 줄을 찾는다. 이어 가정을 지운 작은 예를 계산하고, 성공적인 예와 실패하는 예를 모두 수집한다. 가정이 증명 기법에만 필요한지, 명제 자체에 필수인지 구별한다. 증명의 한 방식이 실패했다는 사실은 명제의 거짓을 뜻하지 않는다.

참고 (읽기 자료). 형식화의 기본 학습 경로로는 *Mathematics in Lean*을 참고한다. 최근 거대 문제의 평가 상태를 읽는 사례로 Clay의 2026년 9월 11일 공지를 뒤의 PDE 장에서 구체적으로 다룬다. 이러한 링크는 이 본문의 모든 증명을 자동 인증했다는 뜻이 아니다.

제 2 장

소수의 분포와 덧셈의 구조

개요 소수의 분포는 양의 정수 가운데 소수가 어디에, 얼마나 자주 놓이는가를 묻는 문제이고, 덧셈의 구조는 유한집합 A에 덧셈을 적용한 합집합 $A+A$의 크기가 A 자체와 얼마나 다른가를 묻는 문제이다. 이 장은 소수가 무한히 많다는 사실과 소수 간격에 관한 서로 다른 진술을 구별하고, Euler 곱과 로그미분을 통해 곱셈 정보가 해석적 함수로 옮겨지는 경로를 보이며, 진동하는 합의 상쇄, 유한군의 Fourier 변환, 가법 에너지, 부분합 공식을 손으로 계산할 수 있는 수준에서 증명한다. 끝으로 가법 조합론과 Dirichlet 다항식에 관한 최근의 두 결과를 정확한 범위와 함께 소개한다. 선행 지식: 정수의 나눗셈, 복소수, 유한합, Cauchy–Schwarz 부등식. 제타함수 부분에는 복소해석의 기본 개념이 도움이 된다.

소수는 곱셈에 관한 기본 블록이다. 그런데 소수가 얼마나 자주 나타나는지 조사하려면 덧셈 구간, 진동하는 합, 복소함수, 확률적 모형을 함께 사용한다. 한편 가법 조합론(*additive combinatorics*)은 유한집합에 덧셈을 반복했을 때 집합이 얼마나 커지는지 묻는다. 두 분야의 공통 질문은 겉으로 불규칙해 보이는 대상에서 어떤 구조를 추출할 수 있는가이다.

2.1 소수의 무한성과 소수의 간격은 다른 문제다

정리 2.1 (소수의 무한성) 소수는 무한히 많다.

증명. 소수가 $p_1, \dots, p_r$ 뿐이라고 가정한다. 정수 $N = p_1 \cdots p_r + 1 > 1$은 어떤 소수 q로 나누어진다. 그러나 N을 각 p_i로 나눈 나머지는 1이므로 q는 목록에 없다. 모순이다. □

이 증명은 주어진 유한 목록 밖에 소수가 있음을 보장한다. 그러나 그 소수가 원래 소수들과 얼마나 가까운지는 알려 주지 않는다. N 자체가 소수일 필요도 없다. 예를 들어 $2\cdot3\cdot5\cdot7\cdot11\cdot13+1 = 30031 = 59\cdot509$이다. 존재를 증명하는 방법과 정밀한 분포를 추정하는 방법이 다를 수 있다는 첫 예이다.

반대로 연속된 합성수의 길이를 얼마든지 길게 만들 수 있다. $m \ge 2$일 때

$$m!+2,\ m!+3,\ \dots,\ m!+m$$

의 각 항은 각각 $2, 3, \dots, m$으로 나누어지고 모두 해당 약수보다 크므로 합성수이다. 따라서 소수 간격에는 임의로 큰 값이 나타난다. 이것은 소수 사이의 작은 간격이 무한히 나타날 수 있다는 주장과 모순되지 않는다. 수열의 상극한과 하극한은 서로 다른 정보를 담는다.

정의 2.2 (연속 소수의 간격) 증가하는 소수열을 p_n이라 할 때 $g_n = p_{n+1} - p_n$을 **연속 소수의 간격**(*gap between consecutive primes*)이라고 한다. $\liminf g_n \le H$라는 것은 임의의 $\varepsilon > 0$에 대해 $g_n < H + \varepsilon$인 n이 무한히 많다는 뜻이다. g_n이 정수값이고 H가 정수이면 이는 $g_n \le H$인 n이 무한히 많다는 것과 같다.

평균 간격, 최악의 간격, 무한히 자주 나타나는 작은 간격을 섞지 말아야 한다. $\pi(x)$처럼 x 이하 소수의 수를 세는 함수는 전체적인 밀도를 다루지만, $\pi(x+h)-\pi(x)$는 짧은 창 안의 분포를 다룬다. 창 길이 h를 줄일수록 전체 평균에서 보이지 않던 요동이 중요해진다.

역사 (작은 간격의 유한성). $\liminf g_n < \infty$, 곧 어떤 유한한 H에 대해 간격이 H 이하인 소수쌍이 무한히 많다는 사실은 Zhang이 2013년에 처음 증명하였다. 이어서 Maynard와 Tao가 독립적으로 다른 방법을 제시하였고, Polymath8b 프로젝트가 이를 개량하여 $H = 246$을 얻었다. 한편 간격 2가 무한히 많다는 쌍둥이 소수 추측은 아직 열려 있다.

2.2 Euler 곱: 덧셈으로 센 것을 곱셈으로 분해하기

실수 $s > 1$에서는

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} (1 - p^{-s})^{-1} \tag{2.1}$$

이다. 오른쪽은 모든 소수에 대한 곱이다. 이 식의 출발점은 복잡한 해석학이 아니라 유일소인수분해이다.

명제 2.3 (유한 Euler 곱) 유한한 소수 집합 S와 $s > 1$에 대해

$$\prod_{p \in S} (1 - p^{-s})^{-1} = \sum_{\substack{n \ge 1 \\ n\text{의 소인수가 모두 } S\text{에 속함}}} n^{-s}.$$

증명. 각 인수에 등비급수 $1 + p^{-s} + p^{-2s} + \cdots$를 대입한다. 유한 개의 절대수렴 급수를 곱하면, 각 항은 $\prod_{p \in S} p^{-k_p s}$ 꼴이다. 유일소인수분해에 의해 이러한 선택은 S의 소수만을 인수로 갖는 양의 정수와 일대일 대응한다. 여기서 모든 $k_p = 0$인 선택은 $n = 1$에 대응한다. □

S를 점차 늘리면 양의 항의 단조수렴으로 실수 $s > 1$의 Euler 곱을 얻는다. 복소수 s의 경우에는 $\operatorname{Re} s > 1$에서 절대수렴을 사용한다. 이 범위를 넘어가려면 해석적 연속이 필요하며, 수렴하지 않는 곱을 형식적으로 전개하는 것만으로 정당화할 수 없다.

소수에 관한 정보를 얻기 위해 로그미분을 취하면

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}, \qquad \operatorname{Re} s > 1, \tag{2.2}$$

가 나타난다. 여기서 Λ는 **von Mangoldt 함수**이며, 소수 p와 $k \ge 1$에 대해 $\Lambda(p^k) = \log p$이고 소수 거듭제곱이 아닌 정수에서는 $\Lambda(n) = 0$이다. 따라서 제타함수의 영점과 특이점에 관한 해석적 정보가 소수 가중합의 오차항에 영향을 주는 통로가 생긴다. 이 통로의 엄밀한 전개에는 적분 표현과 경로 이동, 영점 근처의 제어가 필요하다.

2.3 진동은 상쇄를 만든다

복소수 $z \neq 1$에 대하여

$$1 + z + \cdots + z^{N-1} = \frac{1 - z^N}{1 - z}. \tag{2.3}$$

$z = e^{i\theta}$이고 θ가 2π의 배수가 아니면 각 항의 절댓값은 1이지만 합은 N보다 훨씬 작을 수 있다. 삼각부등식은 N이라는 상계만 주므로 진동의 상쇄를 보지 못한다. 식 (2.3)은 더 강한 평가를 준다. $|1 - z^N| \le 2$이고 $|1 - e^{i\theta}| = 2\,|\sin(\theta/2)|$이므로

$$\left|\sum_{j=0}^{N-1} e^{ij\theta}\right| \le \frac{1}{|\sin(\theta/2)|}$$

이다. 우변은 N에 의존하지 않는다.

> **예제 2.4** $z = -1$이고 N이 짝수이면 합은 0이다. $N \ge 2$일 때 $z = e^{2\pi i/N}$이면 $z \ne 1$이고 $z^N = 1$이므로 합은 0이다. 반면 $z = 1$이면 합은 N이다. 위상들이 정렬되는가, 흩어지는가가 크기를 결정한다.

Dirichlet 다항식(*Dirichlet polynomial*)은 다음과 같은 유한합이다.

$$D(t) = \sum_{N < n \le 2N} a_n n^{-it} = \sum_{N < n \le 2N} a_n e^{-it\log n}.$$

t가 변하면 각 항의 위상이 서로 다른 속도로 회전한다. **큰 값 추정**(*large values estimate*)은 이 합이 매우 커지는 t가 얼마나 많을 수 있는지를 제한한다. 모든 t에서 작은 값을 보장하는 것과 큰 값을 갖는 t의 집합이 작음을 보장하는 것은 다른 주장이다. 후자는 예외를 허용하되 예외의 양을 정량화한다.

간단한 확률적 비유로, 비음수 확률변수 Y는

$$\mathbb{P}(Y \ge a) \le \frac{\mathbb{E}Y}{a} \qquad (a > 0) \tag{2.4}$$

를 만족한다. 이는 $a\mathbf{1}_{\{Y \ge a\}} \le Y$를 적분하면 얻는 **Markov 부등식**이다. 수론에서는 시간 평균이나 고차 적률을 이용하여 큰 값의 빈도를 제어한다. 더 좋은 고차 상관관계를 이해하면 단순한 평균보다 강한 추정이 가능해진다.

2.4 유한군의 Fourier 변환을 손으로 계산하기

$G = \mathbb{Z}/m\mathbb{Z}$에서 함수 $f : G \to \mathbb{C}$의 정규화된 **Fourier 계수**(*Fourier coefficient*)를

$$\widehat{f}(r) = \frac{1}{m}\sum_{x=0}^{m-1} f(x) e^{-2\pi i r x/m} \tag{2.5}$$

로 정의한다. 지수함수의 직교성은 정수 k에 대하여

$$\sum_{x=0}^{m-1} e^{2\pi i k x/m} = \begin{cases} m, & m \mid k, \\ 0, & m \nmid k \end{cases} \tag{2.6}$$

이다. 두 번째 경우에는 $z = e^{2\pi i k/m} \ne 1$이고 $z^m = 1$이므로 앞 절의 등비급수 공식 (2.3)에서 합이 0이다.

명제 2.5 (유한 Fourier 역변환과 Parseval 등식) 식 (2.5)의 정규화에서

$$f(x)=\sum_{r=0}^{m-1}\widehat{f}(r)e^{2\pi i r x/m},\qquad \sum_{r}\left|\widehat{f}(r)\right|^{2}=\frac{1}{m}\sum_{x}|f(x)|^{2}.$$

증명. 첫 식의 오른쪽에 $\widehat{f}(r)$의 정의를 넣고 유한합의 순서를 바꾸면

$$\frac{1}{m}\sum_{y}f(y)\sum_{r}e^{2\pi i r(x-y)/m}=f(x)$$

이다. 안쪽 합은 식 (2.6)에 의해 $x=y$일 때 m이고 그 밖에는 0이기 때문이다. 두 번째 식도 두 Fourier 계수를 전개하고 r에 대한 직교성을 쓰면 교차항 중 $x=y$인 것만 남는다. 곧 $\sum_r\left|\widehat{f}(r)\right|^2=\frac{1}{m^2}\sum_{x,y}f(x)\overline{f(y)}\sum_r e^{-2\pi i r(x-y)/m}=\frac{1}{m}\sum_x|f(x)|^2$이다. $\square$

이 계산에는 극한이 없으므로 수렴 문제를 걱정하지 않아도 된다. 그 대신 정규화 계수 m을 일관되게 유지해야 한다. Fourier 변환은 합성곱을 점별 곱으로 바꾸고, 덧셈 관계의 개수를 주파수 쪽의 크기로 바꾼다. 무작위에 가까운 집합은 비자명한 주파수 성분이 작고, 구조적인 집합은 특정 주파수에 큰 성분을 보일 수 있다. 다만 어떤 의미의 무작위성이 필요한지는 세고 싶은 패턴에 따라 달라진다.

2.5 작은 합집합과 가법 에너지

유한한 아벨군 또는 정수에서 $A+B=\{a+b:a\in A,\,b\in B\}$라 하자. 연속된 정수 집합 $A=\{0,1,\dots,n-1\}$는

$$|A|=n,\qquad |A+A|=2n-1$$

을 만족한다. 가능한 순서쌍은 n^2개이지만 합은 $2n-1$개뿐이다. 많은 서로 다른 순서쌍이 같은 합을 만든다는 뜻이다. 정수의 유한집합에서는 $2n-1$이 최소이다.

명제 2.6 (정수 부분집합의 합집합의 하계) 정수의 비어 있지 않은 유한집합 A에 대하여 $|A+A|\ge 2|A|-1$이다.

증명. $A=\{a_1<a_2<\cdots<a_n\}$이라 하면

$$a_1+a_1<a_1+a_2<a_2+a_2<a_2+a_3<\cdots<a_{n-1}+a_n<a_n+a_n$$

이고, 이는 $A+A$의 서로 다른 원소 $2n-1$개이다. $\square$

정의 2.7 (가법 에너지) 유한집합 A의 **가법 에너지**(*additive energy*)는

$$E(A)=\bigl|\{(a,b,c,d)\in A^4:a+b=c+d\}\bigr|$$

이다. $r(s)=\bigl|\{(a,b)\in A^2:a+b=s\}\bigr|$라 쓰면 $E(A)=\sum_s r(s)^2$이다.

명제 2.8 (에너지의 하계) 비어 있지 않은 유한집합 A에 대하여

$$E(A)\ge\frac{|A|^4}{|A+A|}.$$

증명. $\sum_{s} r(s) = |A|^2$이고, $r(s)$의 지지는 $A + A$이다. Cauchy–Schwarz 부등식을 적용하면

$$|A|^4 = \Big(\sum_{s \in A+A} r(s) \Big)^2 \le |A+A| \sum_{s} r(s)^2$$

이다. □

따라서 $|A+A| \le K\,|A|$이면 $E(A) \ge |A|^3 / K$이다. 상계는 항상 $E(A) \le |A|^3$이다. 모든 s에서 $r(s) \le |A|$이므로 $\sum_s r(s)^2 \le |A| \sum_s r(s) = |A|^3$이기 때문이다. 작은 합집합은 많은 가법 관계를 강제한다. 그 관계가 어느 정도 규칙적인 구조를 강제하는지가 역문제이다. “작은 합집합”이라는 전역적 수치 조건에서 부분군, 등차수열, 더 높은 차원의 진행과 같은 구체적 모형을 추출하려는 것이다.

> **예제 2.9 (부분군과 잉여류)** 유한 아벨군의 부분군 H는 $H + H = H$이다. 잉여류 $A = a + H$도 $A + A = 2a + H$이므로 $|A+A| = |A|$이다. 이는 작은 doubling 상수 $K = 1$의 기본 모형이다. 정수군에는 $\{0\}$ 외에 유한 부분군이 없으므로, 정수 집합의 구조를 말할 때는 등차수열 같은 다른 모형이 필요하다.

2.6 현재의 두 성과를 정확히 읽기

Gowers, Green, Manners, Tao는 특성 2에서 다항 Freiman–Ruzsa 추측(Marton 추측)을 증명했고(*Ann. of Math.* 2025), 후속 논문에서 유계 torsion 아벨군 전체로 확장했다(*Ann. Fac. Sci. Toulouse* 2026). 유계 torsion m이란 모든 g에 대해 $mg = 0$인 상황이다. 2024년 5월 20일 개정 원고의 진술은 $|A+A| \le K\,|A|$인 집합을 크기 $|H| \le |A|$의 부분군 H의 $(2K)^{O(m^3)}$개 평행이동으로 덮을 수 있다는 형태이다. m에 대한 의존성을 버리고 정수군에 그대로 옮길 수는 없다.

Guth와 Maynard의 Dirichlet 다항식 큰 값 추정은 영점 밀도와 짧은 구간의 소수 분포에 새로운 경계를 준다. 이 논문은 2026년 *Annals of Mathematics* 203권 2호에 출판되었다. 초록에 나타나는 대표적 지수는 $30/13$과 $17/30$이다. 이러한 수치는 복잡한 추정의 정밀도를 표현하지만, 그 자체가 Riemann 가설을 증명하는 것은 아니다. σ의 범위와 $o(1)$의 의미까지 사용할 때에는 원정리를 확인해야 한다. 원논문과 출판 정보를 함께 기록해 두면 판본을 추적하기 쉽다.

최근 성과를 공부할 때 목표를 두 층으로 정할 수 있다. 첫 층은 결과의 문장을 정확히 이해하는 것이다. 둘째 층은 증명의 새로운 도구를 기존의 작은 계산과 연결하는 것이다. 유한 Fourier 직교성을 직접 증명했다고 최신 가법 조합론을 모두 이해한 것은 아니지만, 정규화와 상쇄의 원리를 모른 채 정리 이름만 외우는 것보다 훨씬 단단한 출발점이 된다.

2.7 부분합 공식: 거친 계수와 매끄러운 가중치를 분리하기

산술함수의 계수 a_n은 불규칙할 수 있지만 누적합 $A(x) = \sum_{n \le x} a_n$에는 비교적 좋은 정보가 있을 수 있다. 이를 매끄러운 가중합으로 옮기는 도구가 **부분합 공식**(*summation by parts*)이다. 적분의 부분적분과 비슷하지만 한쪽 데이터가 이산적이다.

명제 2.10 (유한 부분합 공식) $A_k = \sum_{j=1}^{k} a_j$라 하면

$$\sum_{k=1}^{N} a_k b_k = A_N b_N + \sum_{k=1}^{N-1} A_k (b_k - b_{k+1}). \tag{2.7}$$

증명. $a_k = A_k - A_{k-1}$, $A_0 = 0$을 대입한다. 두 합의 인덱스를 한 칸 옮기면 중간 항들이 묶이고, 끝점 $A_N b_N$만 따로 남는다. 실제로 $N = 2$에서는 $a_1 b_1 + a_2 b_2 = (a_1 + a_2) b_2 + a_1 (b_1 - b_2)$로 바로 확인할 수 있다. $\square$

이 식은 a_k 자체보다 A_k를 잘 알 때 유리하다. 예를 들어 $a_k = (-1)^{k-1}$이면 모든 A_k의 절댓값이 1 이하이다. $b_k = 1/k$는 감소하고 0으로 간다. 이 경우 꼬리합을 같은 방식으로 정리하면 상쇄 덕분에 수렴함을 보일 수 있다. 각 항의 절댓값을 먼저 더하면 발산하는 조화급수가 나타나므로 핵심 정보를 놓친다.

예제 2.11 (부분합 유계성과 Dirichlet 판정) A_k가 균일하게 유계이고 b_k가 비음수로 감소하여 0으로 가면 $\sum a_k b_k$가 수렴한다.

설명. $|A_k| \le M$이라 하자. m부터 시작하는 부분합 $A_k^{(m)} = \sum_{j=m}^{k} a_j = A_k - A_{m-1}$도 $2M$으로 유계이다. 식 (2.7)을 m부터 N까지의 합에 적용하고 $b_k - b_{k+1} \ge 0$임을 쓰면

$$\left| \sum_{k=m}^{N} a_k b_k \right| \le 2M b_N + 2M (b_m - b_N) = 2M b_m$$

이다. 꼬리의 크기가 상수배의 b_m 이하이고 $b_m \to 0$이므로 Cauchy 조건을 만족한다. $\square$

수론에서 a_n을 소수와 관련된 함수로, b_n을 $\log n$ 또는 n^{-s}처럼 매끄러운 가중치로 선택하면 다양한 합 사이를 옮길 수 있다. 원래 계수의 추정이 조금 바뀌었을 때 최종 오차가 얼마나 달라지는지도 이 공식을 통해 계산한다. 최신 정리의 복잡한 지수가 의미를 갖는 이유는 그 지수가 여러 변환을 거친 최종 오차를 결정하기 때문이다.

예제 2.12 (단순한 누적합으로 검산) $a_k = 1$, $b_k = k$이면 왼쪽은 $1 + 2 + \cdots + N$이다. 오른쪽은

$$N^2 + \sum_{k=1}^{N-1} k\big(k - (k+1)\big) = N^2 - \frac{N(N-1)}{2} = \frac{N(N+1)}{2}$$

이다.

복잡한 정리를 적용하기 전에 이렇게 모든 양을 손으로 아는 예에서 부호와 끝점을 확인하면 오류를 줄일 수 있다.

조합론의 에너지 추정과 부분합 공식은 표면적으로 다르지만 공통 전략을 갖는다. 원래 데이터의 세부를 모두 추적하지 않고, 문제에 필요한 누적 정보나 상관 정보를 만든다. 다만 정보 축약 과정에서 무엇을 잃는지 알아야 한다. 같은 누적합 상계를 가진 두 수열이 모든 패턴을 같은 정도로 포함하는 것은 아니다.

2.8 연습과 해설

연습문제 2.13 $A=\{0,1,2\}$에 대해 $r(s)$와 $E(A)$를 구하고 에너지 하계와 비교하라.

풀이. $s=0,1,2,3,4$에서 $r(s)=1,2,3,2,1$이므로 $E(A)=1+4+9+4+1=19$이다. 일반 하계는 $3^4/5=81/5=16.2$이고, 상계는 $|A|^3=27$이므로 $16.2\le 19\le 27$이다. 하계가 등호가 되려면 Cauchy–Schwarz의 등호 조건에 따라 $r(s)$가 지지 위에서 일정해야 하므로 이 예에서는 등호가 아니다.

연습문제 2.14 $G=\mathbb{Z}/4\mathbb{Z}$에서 $f=\mathbf{1}_{\{0,2\}}$의 Fourier 계수를 구하라.

풀이. $\widehat{f}(r)=\frac{1}{4}(1+e^{-\pi i r})$이므로 짝수 r에서는 $1/2$, 홀수 r에서는 0이다. 집합의 주기적 구조가 특정 주파수에만 남는다. Parseval의 양변은 각각 $1/4+1/4=1/2$과 $2/4=1/2$이다.

연습문제 2.15 “소수 간격의 상극한은 무한대”와 “소수 간격의 하극한은 유한하다”가 논리적으로 양립함을 간단한 수열로 설명하라.

풀이. $a_{2n}=2$, $a_{2n-1}=n$이면 하극한은 2이고 상극한은 무한대이다. 이것은 실제 소수에 관한 증명은 아니지만 두 명제가 모순이 아님을 보이는 논리적 모형이다. 실제 소수에 대한 각 주장은 별도의 수론적 논증을 요구한다.

제 3 장

Langlands: 수론 · 표현 · 기하를 잇는 대응

개요 Langlands 프로그램은 서로 다른 수학적 언어로 표현되는 대칭 사이에 체계적인 대응이 있다는 관점이다. 산술 쪽에서는 수체와 함수체의 Galois 대칭이 나타나고, 해석 쪽에서는 군의 표현과 automorphic form이 나타난다. 기하적 버전에서는 곡선 위의 국소계와 다발의 모듈라이 공간, 그리고 그 위의 범주가 등장한다. 이 장은 이 세 문장의 단어들을 체의 자기동형, 합동식, p-진 절댓값, 유한군의 문자, 모듈러 형식과 Hecke 작용, 원 위의 국소계, 타원곡선의 점 세기라는 구체적인 예와 하나씩 연결한다. 선행 지식: 군과 군 준동형, 체 확대, 선형대수, 복소함수. 뒤쪽 기하적 설명에서는 기본군과 벡터다발의 직관을 사용한다.

3.1 다항식의 근을 바꾸는 대칭

$\mathbb{Q}(\sqrt{2})$의 원소는 $a+b\sqrt{2}$ 꼴이다. $\mathbb{Q}$를 고정하는 체 자기동형은 $\sqrt{2}$를 $\sqrt{2}$ 또는 $-\sqrt{2}$로 보내야 한다. $\sqrt{2}$는 $\mathbb{Q}$ 위에서 x^2-2의 근이고 자기동형은 이 방정식을 보존하기 때문이다. 따라서

$$\sigma(a+b\sqrt{2}) = a - b\sqrt{2}, \qquad \sigma^2 = \mathrm{id}$$

인 대칭이 존재한다. 이 대칭은 근을 제멋대로 바꾸는 것이 아니라 덧셈과 곱셈을 보존한다.

> **예제 3.1 (체 확대를 행렬로 보기)** $\mathbb{Q}(\sqrt{2})$를 기저 $(1, \sqrt{2})$를 가진 2차원 $\mathbb{Q}$-벡터공간으로 보면 σ는
>
> $$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
>
> 로 표현된다. $\sigma(1)=1$, $\sigma(\sqrt{2})=-\sqrt{2}$이기 때문이다. 복잡한 대칭을 행렬로 표현하여 선형대수로 연구한다는 표현론의 생각이 여기서 나타난다.

일반적으로 군 G의 **표현**(*representation*)은 군 준동형 $\rho : G \to \mathrm{GL}(V)$이다. 군의 곱이 선형변환의 합성과 호환되어야 한다. 표현의 차원, 계수체, 연속성 조건을 지정하지 않으면 문제 자체가 불분명하다. 산술에서 사용하는 Galois 표현에는 위상적인 연속성과 분기 조건이 중요한 역할을 한다.

3.2 국소 정보와 전역 정보

정수 방정식의 해를 찾기 전에 여러 소수 p로 나눈 합동식을 조사할 수 있다. 정수해가 존재하면 모든 법 p에 대한 합동해가 존재해야 한다. 따라서 국소 조건은 전역 존재의 필요조건이 될 수 있다. 그러나 모든 국소 조건이 충분조건인지는 별도의 문제이다.

> **예제 3.2 (합동식으로 얻는 장애물)** 정수 x, y에 대해 $x^2+y^2=3$은 불가능하다. 제곱수는 법 4에서 0 또는 1이므로 두 제곱의 합은 $0, 1, 2$ 중 하나이고 3이 될 수 없기 때문이다. 실수해가

존재한다는 사실은 정수해의 존재와 다르다.

p-진수는 단순히 법 p의 나머지 하나가 아니라 $p, p^2, p^3, \dots$의 정보를 서로 호환되게 모은다. 유리수 $x \neq 0$를 $x = p^k u/v$로 쓰되 u, v가 p로 나누어지지 않으면 **p-진 절댓값**(p-adic absolute value)을 $|x|_p = p^{-k}$로 정의하고 $|0|_p = 0$으로 둔다. p의 큰 거듭제곱으로 나누어지는 수는 p-진 거리로 0에 가깝다.

예제 3.3 (2-진 거리에서의 수렴) $1 + 2 + 4 + \cdots + 2^n = 2^{n+1} - 1$이므로 2-진수에서는 부분합이 -1로 수렴한다. 실제로 부분합과 -1의 차이는 2^{n+1}이고 2-진 절댓값은 $2^{-(n+1)}$이다. 실수에서 발산한다는 것과 모순되지 않는다. 서로 다른 거리를 사용했기 때문이다.

Langlands의 "국소"는 흔히 $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}_p$와 그 유한 확대 같은 국소체를 대상으로 한다. "전역"은 수체 또는 유한체 위 곡선의 함수체를 대상으로 한다. 국소적 대응을 안다고 전역적 대응이 자동으로 따라오는 것은 아니다. 전역 객체의 여러 국소 성분 사이에는 호환성과 추가적인 구조가 필요하다.

3.3 문자: 1차원 표현의 작은 실험실

아벨군 G의 복소 **문자**(*character*)란 준동형 $\chi : G \to \mathbb{C}^\times$이다. 유한군의 문자는 단위원 위에 값을 갖는다. $\chi(g)^{|G|} = \chi(g^{|G|}) = 1$이므로 $|\chi(g)| = 1$이기 때문이다. $G = \mathbb{Z}/m\mathbb{Z}$에서는

$$\chi_r(x) = e^{2\pi i r x/m} \qquad (r = 0, 1, \dots, m-1)$$

이 기본 문자이다. 앞 장의 Fourier 변환은 바로 이 문자들을 기저로 함수를 분해하는 것이었다(제28권 제2장).

명제 3.4 (비자명 문자의 합) 유한군 G의 비자명한 1차원 문자 χ에 대해 $\sum_{g \in G} \chi(g) = 0$이다.

증명. $\chi(h) \neq 1$인 h를 고른다. 곱셈 $g \mapsto hg$는 G의 순열이므로

$$\sum_{g} \chi(g) = \sum_{g} \chi(hg) = \chi(h) \sum_{g} \chi(g).$$

따라서 $(1 - \chi(h)) \sum_g \chi(g) = 0$이고 결론을 얻는다. □

이 작은 직교성은 여러 수론적 계수 문제에서 주어진 나머지류를 골라내는 장치가 된다. **Dirichlet 문자**는 $(\mathbb{Z}/q\mathbb{Z})^\times$의 문자를 정수 전체로 주기적으로 확장하되 q와 서로소가 아닌 곳에서는 0으로 정한 것이다. 그 L함수는 $\operatorname{Re} s > 1$에서

$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^s} = \prod_{p} \bigl(1 - \chi(p) p^{-s}\bigr)^{-1}$$

로 표현된다. 여기서도 문자라는 대칭 정보가 해석적 함수로 옮겨진다.

이 설명은 Langlands 프로그램의 완전한 1차원 정식을 대신하지 않는다. 정확한 1차원 산술 대응은 류체론(*class field theory*)의 언어를 요구한다. 다만 "대칭을 문자로 읽고, 문자를 함수로 읽는다"는 방향을 구체적인 유한군 계산에서 먼저 볼 수 있다.

3.4 모듈러 형식과 Hecke의 고윳값이라는 생각

상반평면 $\mathfrak{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$에는 정수 행렬의 분수선형 작용

$$z \longmapsto \frac{az+b}{cz+d}, \qquad ad - bc = 1$$

이 있다. **모듈러 형식**(*modular form*)은 이 작용 아래에서 정해진 변환법칙을 만족하고, 무한대의 cusp에서 적절한 정칙성을 갖는 함수이다. 예를 들어 무게 k의 변환법칙은

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^{k} f(z) \tag{3.1}$$

형태이다. 실제 정의에서는 사용하는 부분군, 승수, 성장 조건을 지정한다. 전체 군 $\mathrm{SL}_2(\mathbb{Z})$에 대해서는 $-I$를 대입하면 $f = (-1)^k f$이므로 홀수 무게에서는 $f = 0$이다.

주기성 때문에 $q = e^{2\pi i z}$를 써서 $f(z) = \sum_{n} a_n q^n$처럼 전개할 수 있다. Fourier 계수 a_n에 수론적 정보가 담기는 경우가 많다. **Hecke 작용**은 이러한 함수공간에 작용하는 서로 호환되는 연산자들의 계열이다. 공통 고유벡터를 찾으면 여러 연산자의 고윳값을 하나의 일관된 수론적 데이터로 읽을 수 있다.

> **예제 3.5** (동시 고유벡터의 유한차원 모형)
>
> $$T_1 = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \qquad T_2 = \begin{pmatrix} 5 & 0 \\ 0 & 7 \end{pmatrix}$$
>
> 는 교환하고 같은 기저의 벡터를 고유벡터로 갖는다. 첫 기저벡터에는 고윳값의 쌍 $(2, 5)$, 둘째에는 $(3, 7)$이 붙는다. 이 모형은 Hecke 이론의 일부 직관을 주지만, 무한차원 함수공간에서 스펙트럼을 구성하는 어려움까지 설명하지는 않는다.

> **예제 3.6** (**Ramanujan의** Δ) $\Delta(z) = q\prod_{n\ge 1}(1-q^n)^{24} = \sum_{n\ge 1}\tau(n)q^n$은 전체 군 $\mathrm{SL}_2(\mathbb{Z})$에 대한 무게 12의 모듈러 형식이며 Hecke 연산자의 공통 고유함수이다. 전개를 직접 계산하면 $\tau(1), \dots, \tau(7) = 1, -24, 252, -1472, 4830, -6048, -16744$이다. 고유함수이므로 τ는 서로소인 인수에 대해 곱셈적이고, 예를 들어 $\tau(2)\tau(3) = (-24)(252) = -6048 = \tau(6)$이다. Hecke 고윳값이 Fourier 계수와 일치한다는 점이 계수에 담긴 곱셈 구조의 원천이다.

흔한 오류. 교환하는 행렬이라고 무조건 공통 고유벡터 기저가 있는 것은 아니다. 복소수 위에서 각 행렬의 대각화 가능성과 같은 조건이 중요하다. 예를 들어 $N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$와 단위행렬 I는 교환하지만 N의 고유벡터는 e_1의 배수뿐이므로 $\mathbb{C}^2$의 공통 고유벡터 기저가 없다. 교환하는 대각화 가능 행렬들은 동시에 대각화된다. 무한차원에서는 작용소의 정의역과 스펙트럼의 성질이 더해진다.

산술 Langlands의 중요한 방향은 Galois 표현에서 나타나는 국소 데이터와 automorphic 쪽의 Hecke 고윳값을 대응시키는 것이다. 모든 수체, 모든 군, 모든 표현에 대해 같은 수준의 완결된 정리가 주어진 것은 아니다. 어떤 군의 어떤 차원인지, 국소인지 전역인지, 어떤 정칙성이나 분기 조건인지가 결과의 범위를 결정한다.

3.5 원 위의 국소계와 모노드로미

곡선 위에서 벡터공간을 연속적으로 붙인 다발을 생각하자. 작은 영역 안에서는 같은 벡터공간처럼 보이지만, 닫힌 경로를 한 바퀴 돌면 초기 벡터가 선형변환을 거쳐 돌아올 수 있다. 이 변환을 **모노드로미**(*monodromy*)라고 부른다. **국소계**(*local system*)는 이러한 경로를 따른 운반이 경로의 호모토피 종류에만 의존하도록 하는 구조이다.

> **예제 3.7 (원 위의 계수 1 국소계)** 원 S^1의 기본군은 $\mathbb{Z}$이다. 복소수 $\lambda \neq 0$를 고르면
>
> $$\rho : \mathbb{Z} \to \mathbb{C}^{\times}, \qquad n \mapsto \lambda^{n}$$
>
> 이라는 표현이 생긴다. 한 바퀴 돌 때 λ를 곱하는 1차원 국소계에 해당한다. $\lambda = 1$이면 자명한 모노드로미이고, $\lambda \neq 1$이면 한 바퀴 운반 후 일반적인 벡터가 달라진다.

계수 r에서는 한 행렬 $M \in \mathrm{GL}_r(\mathbb{C})$가 모노드로미를 정한다. 섬유의 기저를 바꾸면 M은 켤레행렬로 바뀌므로, 국소계의 동형류를 세는 문제에는 행렬의 켤레류가 자연스럽게 등장한다. 이것이 대칭과 기하 사이의 구체적인 연결이다.

기하 Langlands에서는 고정된 곡선 위의 G-다발들을 모은 공간과, 쌍대군에 관한 국소계 공간을 연결한다. G-다발들의 공간에는 자기동형을 가진 대상들이 있으므로 단순한 점집합만으로 충분하지 않을 수 있다. 모듈라이 스택과 범주의 언어가 필요한 이유이다. **쌍대군**(*Langlands dual group*)은 단순히 행렬의 전치나 역행렬을 취한 군을 뜻하지 않는다. 근과 여근(*coroot*)의 데이터를 교환하는 구성이다. 예를 들어 GL_n의 쌍대군은 $\mathrm{GL}_n(\mathbb{C})$이고, SL_n의 쌍대군은 $\mathrm{PGL}_n(\mathbb{C})$이며, Sp_{2n}의 쌍대군은 $\mathrm{SO}_{2n+1}(\mathbb{C})$이다.

3.6 왜 대응이 범주의 동치로 커지는가

집합 사이의 일대일 대응은 대상의 종류만 대응시킨다. **범주**(*category*)는 대상 사이의 사상까지 기억한다. 예를 들어 벡터공간의 차원 목록만으로는 선형사상들의 핵과 상을 이야기할 수 없다. 기하에서 층을 다루면 제한 사상, 정확열, 코호몰로지 같은 관계가 함께 나타난다. 이 관계를 보존하는 대응을 원하면 범주 수준의 진술이 자연스럽다.

기하 Langlands의 현대 정식은 automorphic 쪽의 특정 층 또는 D-가군 범주와 spectral 쪽의 적절한 유도 범주 사이의 동치를 다룬다. 이를 단순히 “다발 공간의 함수와 국소계의 일대일 대응”이라고 쓰면 핵심 조건을 잃는다. 계수, 유도 구조, 지지 조건, 정규화는 실제 정리의 일부이다. 여기서는 잘못된 축약 공식을 제시하는 대신, 두 쪽이 각각 어떤 정보를 기억하는지를 이해하는 데 집중한다.

2026년 9월 24일 기준. Gaitsgory와 Raskin을 중심으로 한 9인 공동 연구의 기하 Langlands 증명 시리즈(5부작)는 표수 0(de Rham · Betti) 설정에서 전역·비분기 categorical geometric Langlands의 증명을 제시한다. 마지막 단계인 V부는 중복도 하나 정리를 다루며, 2026년 1월 16일의 arXiv v3가 확인된다. 이 성과를 산술 Langlands 프로그램 전체의 해결로 바꿔 표현해서는 안 된다. 원문은 I부: 함자의 구성, V부: 중복도 하나, 그리고 저자의 시리즈 안내에서 확인할 수 있다.

이를 읽기 위한 학습 경로로는 여러 갈래가 있다. 산술 쪽은 Galois 이론에서 국소체, 표현론, 모듈러 형식으로 나아간다. 기하 쪽은 대수곡선, 층, D-가군, 유도 범주로 나아간다. 두 경로가

같은 제목 아래 만난다고 해서 선수 지식까지 같아지는 것은 아니다. 본문에서 결과의 범위를 이해하는 단계와 실제 증명을 따라가는 단계를 구분하는 것이 장기 학습에 도움이 된다.

3.7 타원곡선의 유한체 점을 직접 세기

산술의 대칭이 함수의 계수와 연결된다는 말을 좀 더 구체적으로 보기 위해 작은 유한체에서 곡선의 점을 세어 보자. 소수 p에 대해

$$E:\quad y^2 = x^3 + x + 1$$

의 $\mathbb{F}_p$-값 점을 생각한다. 이 예에서는 $p = 5$를 사용한다. 곡선을 사영화하면 무한원점 하나가 추가되며, 이 점도 함께 세어야 한다.

$\mathbb{F}_5$의 제곱은 $0, 1, 4$이고, 0이 아닌 제곱에는 두 개의 제곱근이 있다. $x = 0, 1, 2, 3, 4$를 대입하면 오른쪽 값은 각각 $1, 3, 1, 1, 4$이다. 따라서 가능한 y의 수는 $2, 0, 2, 2, 2$이고,

$$\#E(\mathbb{F}_5) = 2 + 0 + 2 + 2 + 2 + 1 = 9.$$

마지막 1은 무한원점이다. 이 계산에는 부동소수점 근사가 필요하지 않다. 모든 연산은 법 5의 유한 연산이다.

비교 기준 $p + 1$에서 얼마나 벗어나는지를

$$a_p = p + 1 - \#E(\mathbb{F}_p) \tag{3.2}$$

로 정의하면 $a_5 = -3$이다. 타원곡선의 수론에서는 좋은 소수에 대한 이러한 수들이 중요한 국소 데이터를 이룬다. 좋은 소수 p에서 a_p는 E의 ℓ-진 Tate 가군에 대한 Frobenius의 대각합이어서 Galois 표현과 직접 연결된다. Hasse의 정리에 의해 $|a_p| \le 2\sqrt{p}$이며, $p = 5$에서 $|-3| \le 2\sqrt{5} \approx 4.47$이다. 곡선의 모양을 실수 평면에 그린 그림만으로는 이 수를 얻을 수 없다. 서로 다른 체에서 같은 다항식을 해석한 결과가 다르기 때문이다.

> **예제 3.8 (빠진 가정을 점검하기)** 짧은 Weierstrass 형태 $y^2 = x^3 + Ax + B$가 특성 $2, 3$이 아닌 체 위에서 비특이이려면 $4A^3 + 27B^2 \neq 0$이어야 한다. 여기서는 $A = B = 1$이므로 법 5에서 $31 \equiv 1 \neq 0$이다. 따라서 이 예는 비특이 타원곡선이다. 임의의 삼차방정식을 모두 타원곡선이라고 부르면 특이한 경우를 놓친다.

이 국소 데이터들을 모아 곡선의 L함수를 구성하는 방향으로 나아갈 수 있다. 좋은 소수에서 나타나는 이차 다항식은 $1 - a_p T + pT^2$ 형태이다. 이 식과 모듈러 형식의 계수를 대응시키는 정리는 깊은 수론을 담는다.

역사 (모듈러성 정리). $\mathbb{Q}$ 위의 타원곡선의 a_p가 무게 2인 모듈러 형식의 Fourier 계수와 일치한다는 모듈러성 정리는 Wiles와 Taylor–Wiles(1995, 준안정 곡선의 경우)에서 출발하여 Breuil, Conrad, Diamond, Taylor(2001)에 의해 $\mathbb{Q}$ 위의 모든 타원곡선으로 확장되었다.

지금의 손계산은 그 정리를 증명하지 않지만, 대응이 구체적으로 어떤 숫자를 비교하는지 보여 준다.

연습문제 3.9 같은 곡선에 대해 $\mathbb{F}_7$-값 점을 세고 a_7을 계산하라.

풀이. 법 7의 제곱은 $0,1,2,4$이다. $x=0,1,\dots,6$에서 오른쪽 값은 $1,3,4,3,6,5,6$이다. y는 첫째와 셋째 경우에서 각각 두 개이고 다른 경우에는 없다. 무한원점을 더하면 $\#E(\mathbb{F}_7)=5$이므로 $a_7=8-5=3$이다. 같은 곡선이지만 소수에 따라 데이터가 달라진다. Hasse 경계 $|a_7|\le 2\sqrt{7}\approx 5.29$도 만족한다.

이제 작은 연구 읽기 과제를 만들 수 있다. 특정 소수들에서 a_p를 계산하고, 제시된 모듈러 형식의 계수와 비교하고, 그 일치가 어떤 정리의 예인지를 추적한다. 유한한 일치를 확인한 것과 모든 좋은 소수에서의 대응을 증명한 것은 구분한다. 계산은 추측을 이해하고 오류를 찾는 입구이며, 일반적인 대응의 증명은 추가적인 구조를 요구한다.

3.8 연습과 해설

연습문제 3.10 $G=\mathbb{Z}/3\mathbb{Z}$의 복소 1차원 문자를 모두 쓰고 비자명한 문자합이 0임을 확인하라.

풀이. G는 원소 1로 생성되고 $3\cdot 1=0$이므로 $\chi(1)^3=1$이다. 따라서 $\chi(1)$은 $1,\omega,\omega^2$ 중 하나이며 $\omega=e^{2\pi i/3}$이다. 곧 $\chi_r(x)=\omega^{rx}$ $(r=0,1,2)$이다. 비자명한 경우의 합은 $1+\omega+\omega^2=0$이다. 생성원의 상을 정하되 군의 관계식을 보존해야 한다는 점을 확인할 수 있다.

연습문제 3.11 원 위 국소계의 모노드로미가 M일 때, 두 바퀴와 역방향 한 바퀴 운반의 행렬은 무엇인가?

풀이. 각각 M^2와 M^{-1}이다. 경로의 이어붙임이 선형변환의 합성으로 가고, 역경로가 역변환으로 간다는 조건을 사용한다. 출발점의 기저를 P로 바꾸면 모든 모노드로미는 동시에 $P^{-1}MP$ 형태로 바뀐다.

연습문제 3.12 산술적 대응과 기하적 대응을 읽을 때 반드시 기록할 항목 네 가지를 제시하라.

풀이. 대상이 되는 체 또는 곡선, 군과 쌍대군, 국소·전역 및 분기 조건, 대응이 대상의 집합인지 표현인지 범주인지를 기록한다. 여기에 계수와 버전 날짜를 추가하면 서로 다른 정리의 범위를 혼동할 위험을 크게 줄일 수 있다.

제 4 장

기하와 위상: 공간에서 어떤 정보를 남길 것인가

개요 기하와 위상은 공간을 연구할 때 어떤 구조를 보존하고 어떤 구조를 버릴 것인지를 먼저 정하고, 그 선택에 맞는 불변량을 구성하는 분야이다. 이 장은 호모토피 동치, 사슬복합체와 호몰로지, 미분형식과 de Rham 이론의 동기, 이중수 환으로 본 접선, Hausdorff 차원과 Kakeya 문제, 고차 범주와 호모토피 유형론, Euler 특성과 Gauss–Bonnet 정리를 작은 계산으로 점검한다. 최근 결과(Kakeya 추측의 3차원 증명, 망원경 추측의 반례)는 원논문의 정확한 진술 범위만 소개하고 증명을 재현하지 않는다. 선행 지식: 미적분, 선형대수, 연속함수, 군. 대수기하의 예에는 다항식과 몫환을 사용한다.

공간을 연구하는 방법은 하나가 아니다. 거리를 보존하고 싶은지, 각도를 보존하고 싶은지, 찢거나 붙이지 않는 연속적 변형만을 허용하고 싶은지에 따라 질문이 바뀐다. 현대 기하와 위상은 이러한 서로 다른 수준을 연결한다. 대수적 방정식으로 주어진 공간을 위상적으로 조사하고, 미분방정식의 흐름으로 기하 구조를 바꾸며, 공간의 구멍을 대수적 불변량으로 표현한다.

4.1 분류 문제는 동치관계에서 시작한다

원의 둘레가 다르면 두 원은 등거리일 수 없지만 위상동형일 수 있다. 타원과 원도 위상적으로는 같다. 반면 원과 선분은 같지 않다. 원에서 한 점을 제거하면 연결이 유지되지만 선분의 내부점을 제거하면 두 부분으로 나뉜다. 이 차이는 그림의 모양보다 엄밀하게 공간을 구별한다. 무엇을 “같다”고 부를지는 허용하는 변형의 종류가 정하며, 위상동형보다 넓은 동치관계가 호모토피 동치이다.

정의 4.1 (호모토피와 호모토피 동치) 연속함수 $f, g : X \to Y$ 사이의 **호모토피**(*homotopy*)는 연속함수 $H : X \times [0,1] \to Y$로서 $H(x,0) = f(x)$, $H(x,1) = g(x)$를 만족하는 것이다. f와 g 사이에 호모토피가 있으면 $f \simeq g$로 쓴다. X, Y 사이에 합성이 각각 항등사상과 호모토픽한 사상들, 곧 연속함수 $f : X \to Y$, $g : Y \to X$로서 $g \circ f \simeq \mathrm{id}_X$, $f \circ g \simeq \mathrm{id}_Y$인 것이 있으면 두 공간은 **호모토피 동치**(*homotopy equivalent*)라고 한다. 한 점과 호모토피 동치인 공간을 **수축가능**(*contractible*)하다고 한다.

예제 4.2 $\mathbb{R}^n$은 한 점으로 수축된다. $H(x,t) = (1-t)x$가 항등사상($t = 0$)과 상수사상 $x \mapsto 0$($t = 1$)을 연결한다. 그러나 $\mathbb{R}^n \setminus \{0\}$은 같은 방식으로 수축할 수 없다. 중간에 원점을 지나면 공간 밖으로 나가기 때문이다. 대신

$$H(x,t) = \left(1 - t + \frac{t}{\|x\|}\right) x \tag{4.1}$$

는 $\mathbb{R}^n \setminus \{0\}$을 단위구면 S^{n-1}로 변형 수축시킨다. 실제로 $0 \le t \le 1$에서 계수 $1 - t + t/\|x\|$는 $1 - t \ge 0$과 $t/\|x\| \ge 0$의 합이며 두 항이 동시에 0일 수 없으므로 양수이다. 따라서 $H(x,t) \neq 0$

> 이고 H는 $\mathbb{R}^n \setminus \{0\}$에서 값을 가지는 연속함수이다. 또한 $H(x,0) = x$, $H(x,1) = x/\|x\| \in S^{n-1}$이며, $\|x\| = 1$이면 계수가 모든 t에서 1이므로 구면 위의 점은 움직이지 않는다.

한 점과 $\mathbb{R}^n$은 위상동형이 아니지만 호모토피 동치이고, $\mathbb{R}^n \setminus \{0\}$과 S^{n-1}도 마찬가지이다. 호모토피 동치는 위상동형보다 약한 동치관계이다. 호모토피 동치인 공간은 아래의 호몰로지를 포함한 호모토피 불변량을 모두 공유한다.

정의에서 허용한 범위를 유지하는 것이 중요하다. 종이에 그린 고리를 손으로 눌러 한 점으로 만들 수 있어 보이더라도, 고리가 놓인 공간의 구멍을 통과하지 않아야 한다. 추상적 조건이 시각적 직관의 빈틈을 보완한다.

4.2 경계의 경계가 0인 이유

방향을 정한 선분의 경계를 끝점에서 시작점을 뺀 것으로 정의한다.

$$\partial [v_0 v_1] = [v_1] - [v_0].$$

삼각형의 경계는 방향을 일관되게 정하여

$$\partial [v_0 v_1 v_2] = [v_1 v_2] - [v_0 v_2] + [v_0 v_1]$$

로 쓴다. 한 번 더 경계를 취하면 각 꼭짓점이 부호를 달리하여 두 번 나타나 상쇄된다.

$$\partial^2 [v_0 v_1 v_2] = ([v_2] - [v_1]) - ([v_2] - [v_0]) + ([v_1] - [v_0]) = 0. \tag{4.2}$$

일반적으로 k차 단체의 경계는 i번째 꼭짓점을 뺀 면에 부호 $(-1)^i$를 붙인 합이다.

$$\partial [v_0 \cdots v_k] = \sum_{i=0}^{k} (-1)^i [v_0 \cdots \widehat{v_i} \cdots v_k]. \tag{4.3}$$

여기서 $\widehat{v_i}$는 v_i를 뺀다는 뜻이다.

명제 4.3 (경계의 경계) 식 (4.3)로 정의한 경계 사상은 $\partial \circ \partial = 0$을 만족한다.

증명. k차 단체에서 두 꼭짓점 $v_i, v_j (i < j)$를 모두 뺀 $(k-2)$차 면이 ∂^2의 항으로 몇 번, 어떤 부호로 나타나는지 센다. 먼저 v_j를 빼고 다음에 v_i를 빼면, v_i의 위치는 바뀌지 않으므로 부호는 $(-1)^j (-1)^i$이다. 먼저 v_i를 빼고 다음에 v_j를 빼면, v_j는 앞으로 한 칸 당겨져 $(j-1)$번째가 되므로 부호는 $(-1)^i (-1)^{j-1}$이다. 두 부호는 서로 반대이므로 합이 0이다. 모든 $(k-2)$차 면이 이렇게 짝지어 상쇄된다. □

이 항등식은 호몰로지의 중심이다. k차 사슬의 군을 C_k, 경계 사상을 $\partial_k : C_k \to C_{k-1}$이라 하면

$$H_k = \ker \partial_k / \operatorname{im} \partial_{k+1} \tag{4.4}$$

로 정의한다. 이것을 k차 **호몰로지**(*homology*)라고 한다. 경계가 없는 사슬 중 실제로 더 높은 차원 사슬의 경계인 것들을 같은 것으로 취급한다. $\partial^2 = 0$이 있으므로 $\operatorname{im} \partial_{k+1} \subseteq \ker \partial_k$, 곧 분모가 분자의 부분군이 된다.

예제 4.4 (삼각형의 테두리와 채워진 삼각형) 테두리만 있는 복합체에서는 세 변을 잇는 한 바퀴의 1차 사슬이 경계가 없고, 그 안을 채우는 2차 사슬은 없다. 따라서 비자명한 H_1 이 남는다. 삼각형 내부를 2차 단체로 추가하면 그 한 바퀴는 바로 삼각형의 경계가 되어 사라진다. 같은 테두리가 있어도 “채움”이 허용되는지에 따라 불변량이 달라진다.

명제 4.5 (유한차원 사슬복합체의 호몰로지 차원) 유한차원 벡터공간의 사슬복합체에서

$$\dim H_k = \dim C_k - \operatorname{rank} \partial_k - \operatorname{rank} \partial_{k+1}. \tag{4.5}$$

증명. 계수–차원 정리(제7권 제4장)에 의해 $\dim \ker \partial_k = \dim C_k - \operatorname{rank} \partial_k$ 이다. $\operatorname{im} \partial_{k+1} \subseteq \ker \partial_k$ 이므로 몫공간의 차원은 $\dim \ker \partial_k - \dim \operatorname{im} \partial_{k+1}$ 이고, $\dim \operatorname{im} \partial_{k+1} = \operatorname{rank} \partial_{k+1}$ 이다. $\square$

이 계산은 실제 컴퓨터의 호몰로지 계산으로 이어진다. 단, 정수 계수에서는 벡터공간 차원만으로 비틀림 정보를 알 수 없다. 예컨대 $\mathbb{Z}/2\mathbb{Z}$와 영군은 유리수로 계수를 바꾸면 둘 다 사라질 수 있다. 사영평면의 정수 계수 1차 호몰로지가 $\mathbb{Z}/2\mathbb{Z}$이지만 유리수 계수에서는 0인 것이 대표적인 예이다. 어떤 계수로 계산했는지를 기록해야 한다.

4.3 미분형식과 전역적인 장애물

평면에서 f의 미분 $df = f_x\,dx + f_y\,dy$는 **정확한**(*exact*) 1차 미분형식이다. 적절한 매끄러움(f가 C^2급)이 있으면 $d(df) = 0$이므로 모든 정확한 형식은 **닫혀**(*closed*) 있다. 역방향, 곧 닫힌 형식이 정확한가는 공간 전체의 위상에 따라 달라진다.

예제 4.6 (구멍을 감지하는 적분) $\mathbb{R}^2 \setminus \{0\}$에서

$$\omega = \frac{-y\,dx + x\,dy}{x^2 + y^2}$$

를 생각한다. 직접 편미분하면 $d\omega = 0$이다. 실제로

$$d\omega = \left[\frac{\partial x}{\partial}\left(\frac{x}{x^2+y^2}\right) - \frac{\partial y}{\partial}\left(\frac{-y}{x^2+y^2}\right)\right] dx \wedge dy = \left[\frac{y^2 - x^2}{(x^2+y^2)^2} - \frac{y^2 - x^2}{(x^2+y^2)^2}\right] dx \wedge dy = 0$$

이다. 그러나 단위원 $\gamma(t) = (\cos t, \sin t)$, $0 \le t \le 2\pi$에 대해

$$\int_\gamma \omega = \int_0^{2\pi} 1\,dt = 2\pi.$$

만약 전역적으로 $\omega = df$라면 닫힌 곡선 적분은 0이어야 하므로 모순이다. 따라서 닫혔지만 정확하지 않다.

국소적으로는 각도함수 θ를 택하여 $\omega = d\theta$라고 쓸 수 있다. 예컨대 $x > 0$인 반평면에서 $\theta = \arctan(y/x)$이면 $d\theta = (x\,dy - y\,dx)/(x^2+y^2)$이다. 하지만 원점을 한 바퀴 도는 동안 각도가 2π 바뀌므로 전역 단일값 함수로 붙일 수 없다. “국소에서는 풀리지만 전역에서는 장애물이 있다”는 현상은 층과 코호몰로지의 동기이기도 하다. 이 예에서 ω의 류는 $\mathbb{R}^2 \setminus \{0\}$의 1차 de Rham 코호몰로지를 생성하며, 이 군은 1차원이다.

Stokes 정리 $\int_M d\eta = \int_{\partial M} \eta$는 미분과 경계의 관계를 표현한다. 여기서 M은 방향이 주어진 콤팩트 다양체이고 η는 $(\dim M - 1)$차 매끄러운 형식이다(제9권 제8장). 앞 절의 사슬에서 $\partial^2 = 0$

이 나타난 것처럼 여기서는 $d^2 = 0$이 나타난다. de Rham 이론은 매끄러운 다양체의 닫힌 형식과 정확한 형식의 차이를 위상적 코호몰로지와 연결한다. 두 언어가 같은 정보를 서로 다른 계산 방식으로 드러내는 것이다.

흔한 오류 (닫혔다와 정확하다). "닫힌 형식은 정확하다"는 진술은 일반적으로 거짓이다. 수축 가능한 열린 집합, 예컨대 $\mathbb{R}^n$이나 볼 위에서는 성립하지만(Poincaré 보조정리), 예제 4.6의 $\mathbb{R}^2 \setminus \{0\}$에서는 성립하지 않는다. 국소적으로 원시함수가 존재한다는 사실에서 전역적 원시함수의 존재를 추론해서는 안 된다.

4.4 점집합만으로는 보이지 않는 기하

대수기하는 다항식 방정식의 해집합을 연구하지만, 현대적 관점에서는 해집합의 점들만 남기지 않는다. 함수들의 환을 함께 보존한다. 예를 들어 체 k 위에서 방정식 $x = 0$과 $x^2 = 0$의 k-값 점은 둘 다 원점 하나다. 그러나 좌표환

$$k[x]/(x), \qquad k[x]/(x^2)$$

은 다르다. 두 번째 환에는 0이 아니지만 제곱이 0인 원소 x가 남는다.

> **정의 4.7 (쌍대수 환)** $\varepsilon^2 = 0$인 형식적 원소 ε을 사용한 환 $k[\varepsilon]/(\varepsilon^2)$를 **쌍대수 환**(*ring of dual numbers*)이라고 한다. 모든 원소는 $a + b\varepsilon (a, b \in k)$ 꼴이며
>
> $$(a + b\varepsilon)(c + d\varepsilon) = ac + (ad + bc)\varepsilon.$$

> **명제 4.8 (쌍대수에서의 미분)** k 계수 다항식 f에 대해 쌍대수 환에서
>
> $$f(a + b\varepsilon) = f(a) + b f'(a)\varepsilon. \tag{4.6}$$

증명. 단항식에 대해 $(a + b\varepsilon)^n = a^n + n a^{n-1} b\varepsilon$이다. 이항전개에서 두 개 이상의 ε을 포함하는 항은 모두 0이므로 그렇다. 계수를 곱해 유한합을 취하면 된다. □

따라서 미분은 극한 없이도 일차의 무한소 정보를 기록하는 방식으로 나타난다. 여러 변수에서는 $f(a + \varepsilon v) = f(a) + \varepsilon \nabla f(a) \cdot v$가 되어, 방정식 $f = 0$을 만족하는 접방향의 조건이 나온다. 특이점에서는 이 선형 조건이 실제 곡선의 모양을 과하게 단순화할 수 있다. 예컨대 $y^2 = x^3$의 원점에서는 모든 일차 편미분이 0이지만 곡선은 평면 전체가 아니다. 구체적으로 $f = y^2 - x^3$에 $(x, y) = (\varepsilon v_1, \varepsilon v_2)$를 대입하면 $\varepsilon^2 v_2^2 - \varepsilon^3 v_1^3 = 0$이 모든 (v_1, v_2)에 대해 성립하므로, 원점의 접공간은 평면 전체인 2차원이 된다. 매끄러운 곡선 $y = x^2$에서는 같은 대입이 $\varepsilon v_2 = 0$, 곧 $v_2 = 0$을 요구하여 접공간이 1차원이다.

스킴은 이러한 대수적 정보를 국소화하여 붙이는 언어를 제공한다. 모듈라이는 공간 하나보다 공간들의 가족을 연구하며, 유도기하는 교차와 변형의 고차 정보를 보존하려는 방향으로 나아간다. 이 장에서는 그 이론을 완결하려 하지 않고, 단순한 점집합만 남겼을 때 잃어버리는 정보가 이미 초등적인 다항식 예에 나타남을 확인한다.

4.5 크기와 차원을 구분하기: Kakeya 문제

평면의 선분은 길이가 양수지만 면적은 0이다. 더 일반적으로 측도가 0인 집합도 복잡한 기하적 구조를 가질 수 있다. 따라서 집합의 크기를 말할 때 어떤 측도나 차원을 사용하는지 지정해야 한다.

지름이 작은 집합들로 E를 덮고, 지름의 s제곱을 더하는 비용을 생각한다. 덮개는 가산 개의 집합으로 이루어진다.

$$\mathcal{H}^s_\delta(E) = \inf\left\{ \sum_{j} (\operatorname{diam} U_j)^s \,:\, E \subseteq \bigcup_j U_j,\ \operatorname{diam} U_j \le \delta \right\}. \tag{4.7}$$

$\delta \downarrow 0$의 극한 $\mathcal{H}^s(E) = \lim_{\delta \downarrow 0} \mathcal{H}^s_\delta(E)$가 s차원 **Hausdorff 측도**(*Hausdorff measure*)이다. 이 측도가 ∞에서 0으로 바뀌는 임계 지수

$$\dim_{\mathrm{H}} E = \inf\{ s \ge 0 : \mathcal{H}^s(E) = 0 \}$$

가 **Hausdorff 차원**이다. 이 정의는 덮개의 크기들이 서로 달라도 허용한다. 반면 **Minkowski 차원**(상자 차원)은 같은 해상도의 상자 수 또는 작은 이웃의 부피를 이용한다. 두 차원이 항상 같지는 않다.

> **예제 4.9 (Cantor 집합의 차원에 대한 첫 추정)** 삼진 Cantor 집합은 k 단계에서 길이 3^{-k}의 구간 2^k개로 덮인다. 이 덮개의 s차 비용은
>
> $$2^k 3^{-ks} = (2 \cdot 3^{-s})^k$$
>
> 이다. $s > \log 2 / \log 3$이면 $2 \cdot 3^{-s} < 1$이므로 $k \to \infty$에서 비용이 0으로 간다. 임의의 $\delta > 0$에 대해 $3^{-k} \le \delta$인 k는 얼마든지 크게 택할 수 있으므로 $\mathcal{H}^s_\delta = 0$이고 $\mathcal{H}^s = 0$이다. 따라서 Hausdorff 차원은 $\log 2/\log 3$ 이하이다. 반대 방향의 하계는 적절한 질량분포 추정을 추가로 요구한다. 덮개 하나를 찾은 것만으로 차원의 등호를 모두 증명한 것은 아니다.

> **예제 4.10 (두 차원이 다른 집합)** $E = \mathbb{Q} \cap [0,1]$은 가산집합이므로 Hausdorff 차원이 0이다. 번호를 붙인 점 q_j를 지름 $\epsilon 2^{-j}$의 구간으로 덮으면 $s > 0$에서 비용은 $\epsilon^s \sum_j 2^{-js}$이고, 이 값은 $\epsilon \to 0$일 때 0으로 간다. 반면 E의 닫힘은 $[0,1]$이고 상자 차원은 닫힘에서 같으므로 Minkowski 차원은 1이다.

Kakeya 집합(*Kakeya set*)은 모든 방향의 단위 선분을 포함하는 (콤팩트) 집합이다. 서로 다른 방향의 긴 선분을 모두 넣으면서 작은 크기를 유지할 수 있는지 묻는다. 선분들이 겹치면 부피를 절약하지만, 너무 많은 방향이 동시에 지나가면 겹침에는 제약이 생긴다. 평면에서는 Besicovitch가 측도가 0인 Kakeya 집합을 구성했으므로 "면적"만으로는 작아질 수 있다. 그러나 평면의 Kakeya 집합의 Hausdorff 차원은 2임이 Davies(1971)에 의해 알려져 있다. $n \ge 3$에서 Kakeya 집합의 Hausdorff 차원이 n이라는 것이 Kakeya 추측이다. 이 방향과 겹침의 긴장이 조화해석의 제한 문제, 파동의 집중 현상과 연결된다.

확인된 최근 결과. Wang과 Zahl의 2025년 2월 24일 원논문은 $\mathbb{R}^3$의 Kakeya 집합의 Hausdorff 차원과 Minkowski 차원이 모두 3임을 증명한다고 명시한다. 이는 모든 차원의 Kakeya 문제나

모든 관련 maximal 추정이 해결되었다는 말과 다르다. 이 권은 해당 긴 증명을 재현하지 않는다. 작은 튜브의 겹침을 어떻게 제어하는지 읽기 위한 출발점으로 *Volume estimates for unions of convex sets, and the Kakeya set conjecture in three dimensions*를 제시한다.

4.6 고차 구조: 같은 것이라는 증거도 보존하기

범주는 대상과 사상을 기억한다. 위상적 상황에서는 사상 사이에도 호모토피가 있고, 호모토피 사이에도 더 높은 호모토피가 있다. 이 정보를 버리지 않으려는 언어가 **고차 범주**(*higher category*)와 호모토피 일관성이다. 사상의 합성이 문자 그대로 같은지보다, 비교하는 변형이 존재하고 그 변형들이 서로 호환되는지가 중요해진다.

예를 들어 경로 세 개를 이어붙일 때 $(\alpha * \beta) * \gamma$와 $\alpha * (\beta * \gamma)$는 시간 배분이 다를 수 있다. 앞의 경우 α, β, γ를 구간 $[0, \tfrac{1}{4}]$, $[\tfrac{1}{4}, \tfrac{1}{2}]$, $[\tfrac{1}{2}, 1]$에서, 뒤의 경우 $[0, \tfrac{1}{2}]$, $[\tfrac{1}{2}, \tfrac{3}{4}]$, $[\tfrac{3}{4}, 1]$에서 지난다. 적절한 재매개화로 연결되지만, 많은 경로와 여러 합성 순서를 다루면 연결들이 서로 호환되어야 한다. “동치까지 같다”는 표현은 아무 차이나 무시한다는 뜻이 아니라, 차이를 연결하는 고차 데이터를 관리한다는 뜻이다.

호모토피 유형론(*homotopy type theory*, HoTT)에서는 타입을 공간처럼, 같은 타입의 두 항 사이의 등호를 경로처럼 해석한다. 등호에 대한 등호가 더 높은 경로에 해당한다. **일가성 공리**(*univalence axiom*)는 적절한 우주에서 타입들의 동치와 등호를 연결한다. 이 관점을 ZFC의 모든 문장을 단순히 이름만 바꿔 옮기는 작업으로 이해해서는 안 된다. 또 Lean의 기본 논리와 HoTT의 일가성 공리를 동일하게 취급해서는 안 된다. HoTT Book은 이 관점을 체계적으로 소개하는 공개 자료이다.

안정 호모토피의 최근 중요한 반례로 Burklund, Hahn, Levy, Schlank의 2023년 논문은 각 소수에서 높이 2 이상인 telescopic localization과 chromatic localization의 차이를 보인다. 이는 Ravenel의 telescope 추측에 관한 결과이다. 이 추측은 높이 0과 1에서는 이미 성립이 알려져 있었다. 초급 호몰로지 계산을 부정하는 것이 아니라, 스펙트럼과 고급 K이론에서 예상했던 정보 보존이 어디까지 가능한지 바꾸는 결과이다. 원문은 *K-theoretic counterexamples to Ravenel's telescope conjecture*이다.

4.7 Euler 특성과 곡률: 서로 다른 계산이 같은 수를 줄 때

닫힌 곡면을 유한하게 삼각분할했을 때 꼭짓점 수 V, 변 수 E, 면 수 F로

$$\chi = V - E + F \tag{4.8}$$

를 정의하고 **Euler 특성**(*Euler characteristic*)이라고 한다. 삼각형을 더 잘게 나누면 각각의 수는 변하지만 그 조합은 유지된다. 예를 들어 한 삼각형 내부에 점 하나를 넣고 세 꼭짓점과 연결하면 V는 1, E는 3, F는 2만큼 증가하므로 변화량은 $1 - 3 + 2 = 0$이다.

> **예제 4.11** 사면체의 표면은 $V = 4$, $E = 6$, $F = 4$이므로 $\chi = 2$다. 정육면체의 표면은 $V = 8$, $E = 12$, $F = 6$으로 역시 2다. 이때 면이 사각형이므로 엄밀한 삼각분할이 아니라 다각형 분할이며, 식 (4.8)은 이 경우에도 성립한다. 각 사각형에 대각선을 하나씩 그어 삼각분할로 바꾸면

$V=8$, $E=12+6=18$, $F=12$이고 $8-18+12=2$로 같은 값이 나온다. 두 경우 모두 구면과 위상동형이며 다른 분할이 같은 불변량을 준다. 이 예 두 개만으로 모든 분할에서 불변이라는 정리를 증명한 것은 아니지만, 국소적 세분 연산의 검산이 된다.

연결된 유한 그래프에서는 독립적인 순환의 수가 $E-V+1$이다. 먼저 모든 꼭짓점을 연결하는 나무를 고르면 그 나무의 변은 $V-1$개다. 남은 변 하나를 추가할 때마다 순환이 하나씩 생긴다. 이 설명을 선형대수로 표현하면 경계행렬의 핵 차원이 $E-(V-1)$이라는 계산이다. 조합적 그림과 호몰로지의 계산이 맞아떨어진다.

명제 4.12 (Euler 특성의 호몰로지 표현) 유한차원 벡터공간으로 이루어진 유한 사슬복합체에 대해

$$\sum_{k} (-1)^k \dim C_k = \sum_{k} (-1)^k \dim H_k. \tag{4.9}$$

증명. 앞의 차원 공식 (4.5)에서 $\dim H_k = \dim C_k - r_k - r_{k+1}$이라 쓰되 $r_k = \operatorname{rank} \partial_k$로 둔다. 교대합을 취하면

$$\sum_{k} (-1)^k \dim H_k = \sum_{k} (-1)^k \dim C_k - \sum_{k} (-1)^k r_k - \sum_{k} (-1)^k r_{k+1}$$

이고 마지막 합은 $\sum_k (-1)^k r_{k+1} = -\sum_k (-1)^{k+1} r_{k+1} = -\sum_k (-1)^k r_k$이다. 따라서 r_k가 이웃한 두 차수에서 반대 부호로 나타나 모두 상쇄된다. 끝점 밖의 경계 사상은 0이다. 곧 $r_0 = 0$이고 가장 높은 차수를 넘어서는 r도 0이다. $\square$

이 식은 공간을 이루는 조각의 수와 공간의 구멍 정보가 같은 교대합을 갖는 이유를 보여 준다. 단체복합체에서 $\dim C_k$는 k차 단체의 수이므로 좌변이 식 (4.8)의 χ이고, 우변은 호몰로지만으로 χ를 계산하는 공식이다. 이 때문에 χ는 분할의 선택에 의존하지 않는 위상적 불변량이다. 미분기하에서는 곡률을 적분하여 같은 위상적 수를 얻는 Gauss–Bonnet 정리가 등장한다.

정리 4.13 (Gauss–Bonnet) 닫힌 방향성 리만 곡면 M에 대해

$$\int_M K \, dA = 2\pi \chi(M). \tag{4.10}$$

여기서 K는 Gaussian 곡률이다.

경계가 있으면 경계의 측지곡률과 모서리 항 등이 추가되므로 같은 식을 그대로 쓰면 안 된다. 이 정리의 증명에는 접속과 각도의 변화 또는 삼각분할을 통한 체계적인 논증이 필요하며 이 장에서는 다루지 않는다. 여기서는 구면의 직접 계산으로 정리의 정규화와 부호를 확인한다. 단위구면의 $K=1$과 면적 4π를 넣으면 왼쪽은 4π, 오른쪽은 $2\pi \cdot 2 = 4\pi$가 된다. 국소적인 곡률을 모아 전역적 위상을 얻는다는 점이 놀랍다.

예제 4.14 (평평한 토러스) 직사각형의 마주 보는 변을 평행하게 붙이면 국소적으로 Euclid 평면과 같은 평평한 토러스를 얻는다. 이 리만 계량에서 $K=0$이고 토러스의 Euler 특성도 0이다. 3차원 공간에 흔히 그리는 도넛 표면의 유도계량은 곳에 따라 양·음의 곡률을 가진다. 바깥쪽에서는 $K>0$, 안쪽에서는 $K<0$이며 두 영역의 총곡률이 각각 $+4\pi$, -4π이어서 합은 여전히 0이다. 위상적 대상과 선택한 계량을 구분해야 한다.

흔한 오류 (Euler 특성은 곡면을 분류하지 않는다). Euler 특성이 같다고 위상동형은 아니다. 토러스와 Klein 병은 모두 $\chi = 0$이지만 방향성이 다르므로 위상동형이 아니다. χ는 위상동형(더 나아가 호모토피 동치)에 대한 불변량이지, 완전한 분류 불변량이 아니다.

현대 기하의 많은 질문은 이런 대응을 더 높은 차원과 더 복잡한 불변량으로 확장한다. 어떤 미분 작용소의 해공간 차이를 위상적 데이터로 계산하는 지표정리, 특성류를 통한 다발의 분류, 기하 흐름을 통해 표준 형태 찾기 등이 그 방향이다. 첫 학습에서는 Euler 특성과 닫힌 형식의 예를 충분히 계산하면 고급 개념이 어떤 정보를 일반화하는지 보인다.

4.8 연습과 해설

연습문제 4.15 꼭짓점 세 개, 변 세 개, 내부 면 한 개로 이루어진 채워진 삼각형의 $\dim H_0, \dim H_1, \dim H_2$를 체 계수로 계산하라.

풀이. $\dim C_0 = 3$, $\dim C_1 = 3$, $\dim C_2 = 1$이다. 기저를 $[v_0v_1], [v_1v_2], [v_0v_2]$로 잡으면 ∂_1은 각각 $v_1 - v_0$, $v_2 - v_1$, $v_2 - v_0$로 보낸다. 연결된 세 꼭짓점을 잇는 경계행렬의 계수는 2이다. 면의 경계는 $[v_1v_2] - [v_0v_2] + [v_0v_1] \neq 0$인 한 바퀴이므로 $\operatorname{rank}\partial_2 = 1$이다. $\partial_0 = 0$, $\partial_3 = 0$이다. 따라서 식 (4.5)에서

$$\dim H_0 = 3 - 0 - 2 = 1, \qquad \dim H_1 = 3 - 2 - 1 = 0, \qquad \dim H_2 = 1 - 1 - 0 = 0$$

이다. 면을 제거하면 $\operatorname{rank}\partial_2 = 0$이 되어 $\dim H_1 = 3-2-0 = 1$로 바뀐다. 검산으로 $\chi = 3-3+1 = 1 = 1-0+0$이다.

연습문제 4.16 쌍대수 환에서 $a + b\varepsilon$이 가역일 필요충분조건을 구하라. k는 체라고 가정한다.

풀이. $a \neq 0$이면 $(a+b\varepsilon)(c+d\varepsilon) = ac + (ad+bc)\varepsilon = 1$에서 $c = a^{-1}$, $ad + bc = 0$이므로 $d = -ba^{-2}$이다. 곧 역원은 $a^{-1} - ba^{-2}\varepsilon$이다. $a = 0$이면 어떤 원소를 곱해도 상수항이 0이므로 1이 될 수 없다. 따라서 필요충분조건은 $a \neq 0$이다. 점 a의 값과 무한소 방향의 정보가 서로 다른 역할을 한다.

연습문제 4.17 $\omega = d\theta$라는 국소 표현이 있는데도 원점 없는 평면에서 전역적인 원시함수가 없는 이유를 설명하라.

풀이. 작은 단순한 영역마다 각도의 가지를 고를 수 있지만, 원점을 감싸는 닫힌 경로를 따라 돌아오면 각도가 2π 변한다. 전역 단일값 함수의 미분은 닫힌 경로 적분이 0이므로 2π라는 적분값이 전역 존재를 막는다. 국소 해의 존재와 전역적 붙임의 가능성은 다른 질문이다.

제 5 장

PDE · 동역학 · 확률: 해가 존재한다는 말의 여러 의미

개요 방정식의 해가 존재한다는 진술은 어떤 초기 자료에서, 어떤 함수공간에서, 어떤 시간 구간에 대해, 어떤 의미의 해가 있다는 뜻인지를 밝혀야 비로소 정해지는 진술이다. 이 장은 상미분방정식의 유한시간 폭발, 열방정식의 에너지 감소, 약수렴과 비선형 항, 비압축성 Navier–Stokes 방정식의 에너지 구조와 스케일링, 미시적 입자에서 거시적 방정식으로의 축약, Brown 운동의 이차변동과 Itô 보정항, 확률 PDE의 재규격화, 이진 전개 사상의 민감성과 불변측도, Gronwall 부등식과 유일성을 작은 계산으로 구별한다. 최근 발표(2026년 9월 24일 기준)는 원 발표의 범위만 소개하고 증명을 재현하지 않는다. 선행 지식: 미분방정식, 다변수 미분적분, 적분, 기초 확률. 에너지 추정에는 부분적분을, 확률미분에는 조건부기댓값의 직관을 사용한다.

미분방정식을 쓰는 것과 그 방정식의 해를 이해하는 것은 다르다. 초기값이 주어졌을 때 해가 존재하는가, 유일한가, 작은 초기 오차에 안정적인가, 모든 시간에 매끄럽게 존재하는가는 서로 다른 질문이다. 수치 그림이 매끄럽다는 사실만으로 연속체 방정식의 전역 정칙성이 따라오지 않는다. 반대로 고전적인 의미의 매끄러운 해가 깨진 뒤에도 약한 의미의 해가 존재할 수 있다.

5.1 폭발을 정확히 볼 수 있는 상미분방정식

예제 5.1 $y' = y^2$, $y(0) = a > 0$의 해는

$$y(t) = \frac{a}{1 - at}, \qquad 0 \le t < \frac{1}{a} \tag{5.1}$$

이다. 변수분리로 $\int y^{-2}\,dy = \int dt$에서 $-1/y = t - 1/a$를 얻어 구할 수 있고, 미분하여 식을 확인할 수 있다. $y' = a^2/(1-at)^2 = y^2$이다. $t \uparrow 1/a$일 때 $y(t) \to \infty$이다. 초기값이 작으면 폭발 시간이 늦어지지만 유한하다는 사실은 바뀌지 않는다.

이 예는 어떤 양이 비선형적으로 자신을 증폭하면 유한시간에 커질 수 있음을 보인다. 그러나 이것만으로 유체방정식의 폭발을 주장할 수는 없다. PDE에서는 확산, 공간적 이동, 보존량, 비국소 압력 등이 함께 작용한다. ODE의 한 항만 보고 전체 PDE를 판단하는 것은 정당하지 않다.

반대로 $y' = -y^2$, $y(0) = a > 0$이면 $y(t) = a/(1+at)$이고 모든 $t \ge 0$에 대해 존재하며 감소한다. 부호 하나가 장기 거동을 바꾼다. 어떤 식이 큰 값을 만드는지뿐 아니라 어떤 항이 이를 억제하는지 비교해야 한다.

5.2 열방정식과 에너지 감소

열방정식 $u_t = \nu \Delta u$를 생각한다. $\nu > 0$이며 u가 충분히 매끄럽고 빠르게 감소하거나 주기적이라고 가정한다. 양변에 u를 곱하고 적분하면

$$\frac{1}{2}\frac{\mathrm{d}}{\mathrm{d}t}\int |u|^2 \, dx = \nu \int u \Delta u \, dx = -\nu \int |\nabla u|^2 \, dx. \tag{5.2}$$

둘째 등호는 부분적분이며, 따라서 경계항이 0이라는 가정이 필요하다. 식 (5.2)에 의해 L^2 에너지가 증가하지 않는다. 다른 경계조건에서는 경계로 드나드는 에너지를 포함해야 한다.

이 감소는 유일성도 준다. 같은 초기값을 갖는 두 해의 차 w도 열방정식을 만족하고 $w(\cdot,0)=0$이므로, 식 (5.2)에서 $\frac{\mathrm{d}}{\mathrm{d}t}\int |w|^2 \le 0$이다. 따라서 $\int |w|^2 \equiv 0$이고 두 해는 같다.

> **예제 5.2 (한 Fourier 모드의 소멸)** 원 $\mathbb{R}/2\pi\mathbb{Z}$ 위에서 초기값 $u(x,0)=\sin(kx)$(k는 정수)를 주면
>
> $$u(x,t) = e^{-\nu k^2 t}\sin(kx)$$
>
> 가 해다. 실제로 $u_t = -\nu k^2 u$이고 $\nu u_{xx} = -\nu k^2 u$이다. 큰 k일수록 빠르게 감소하므로 짧은 파장의 요동이 빨리 사라진다. 확산의 평활화 효과를 가장 간단하게 볼 수 있다.

에너지 부등식은 해의 정확한 공식을 몰라도 쓸 수 있다. 비선형 문제에서는 근사해들의 에너지를 균일하게 제어하고, 약수렴하는 부분수열을 찾아 극한을 취하는 방식이 중요하다. **약수렴**(*weak convergence*)은 $u_n \rightharpoonup u$로 쓰며, 모든 시험함수 $\varphi \in L^2$에 대해 $\int u_n \varphi \, dx \to \int u \varphi \, dx$라는 뜻이다(제13권 제3장). 하지만 약수렴만으로 비선형 항의 극한을 통과할 수 있는 것은 아니다. $u_n \rightharpoonup u$라는 정보에서 $u_n^2 \rightharpoonup u^2$를 자동으로 얻을 수 없기 때문이다.

> **예제 5.3 (진동이 남기는 결함)** $(0,2\pi)$에서 $u_n(x)=\sin(nx)$는 적절한 의미에서 약하게 0으로 수렴한다. 모든 $\varphi \in L^2(0,2\pi)$에 대해 $\int_0^{2\pi}\varphi(x)\sin(nx)\,dx \to 0$이기 때문이다(Riemann–Lebesgue 보조정리). 하지만
>
> $$u_n(x)^2 = \frac{1}{2} - \frac{1}{2}\cos(2nx)$$
>
> 는 약하게 $1/2$로 수렴한다. $\cos(2nx)$도 같은 이유로 약하게 0으로 간다. 극한의 제곱 $0^2=0$과 제곱의 극한 $1/2$이 다르다. 또한 $\|u_n\|_{L^2}^2 = \int_0^{2\pi}\sin^2(nx)\,dx = \pi$는 n에 무관하므로 수렴은 강수렴이 아니다. 작은 규모의 진동이 선형 관측에서는 사라져도 비선형 관측에는 남는다. 강한 수렴이나 추가 콤팩트성이 필요한 이유이다.

5.3 비압축성 Navier–Stokes의 구조

밀도를 1로 정규화한 비압축성 Navier–Stokes 방정식은

$$\partial_t u + (u\cdot\nabla)u + \nabla p = \nu\Delta u + f, \qquad \nabla\cdot u = 0 \tag{5.3}$$

이다. u는 속도, p는 압력, f는 외력이다. 비압축성 조건은 압력과 속도 사이에 비국소적인 제약을 만든다. 식 (5.3)의 발산을 취하면 $\nabla\cdot u=0$이므로

$$\Delta p = -\partial_i\partial_j(u_i u_j) + \nabla\cdot f$$

를 얻는다. 압력은 임의로 따로 선택하는 입력 함수가 아니라 속도장 전체에서 결정되는 양이다.

매끄럽고 경계항이 사라지는 해에 대해 에너지 계산을 하면

$$\frac{1}{2}\frac{\mathrm{d}}{\mathrm{d}t}\|u\|_2^2 + \nu\|\nabla u\|_2^2 = \int f\cdot u\,dx. \tag{5.4}$$

비선형 수송항은

$$\int u\cdot(u\cdot\nabla)u\,dx = \int u\cdot\nabla\left(\frac{|u|^2}{2}\right)dx = 0$$

으로 사라진다. 첫째 등호는 $u_i u_j \partial_j u_i = u_j\partial_j(|u|^2/2)$이고, 마지막 등호는 부분적분으로 $-\int(\nabla\cdot u)\,|u|^2/2\,dx$를 얻은 뒤 $\nabla\cdot u=0$과 경계조건을 함께 사용한 것이다. 압력항 $\int u\cdot\nabla p\,dx = -\int(\nabla\cdot u)p\,dx$도 같은 조건으로 적분에서 사라진다.

유한한 에너지는 중요한 정보지만 속도가 모든 점에서 유계임을 직접 뜻하지 않는다. $\mathbb{R}^3$에서 고정된 매끄러운 함수 ϕ에 대해 $v_\lambda(x)=\lambda^{3/2}\phi(\lambda x)$라 놓으면

$$\|v_\lambda\|_2 = \|\phi\|_2, \qquad \|v_\lambda\|_\infty = \lambda^{3/2}\|\phi\|_\infty. \tag{5.5}$$

치환 $y=\lambda x$로 $\int |v_\lambda|^2\,dx = \lambda^3\lambda^{-3}\int|\phi|^2\,dy$이므로 L^2 노름이 일정하다. 에너지는 일정하지만 작은 영역에 집중하는 최대 크기는 커진다. 이는 방정식의 실제 해를 구성한 것이 아니라 에너지 노름만으로 점별 크기를 제어할 수 없음을 보여 주는 함수족이다.

5.4 스케일링과 임계성

무외력 Navier–Stokes의 형식적 스케일링은

$$u_\lambda(x,t)=\lambda u(\lambda x,\lambda^2 t), \qquad p_\lambda(x,t)=\lambda^2 p(\lambda x,\lambda^2 t) \tag{5.6}$$

이다. (u,p)가 $f=0$인 식 (5.3)의 해이면 (u_λ,p_λ)도 해이다. 이 치환을 미분항과 비선형 항에 대입하면 모두 λ^3배가 되어 방정식의 형태가 유지된다. $\partial_t u_\lambda = \lambda^3(\partial_t u)$, $(u_\lambda\cdot\nabla)u_\lambda = \lambda^3(u\cdot\nabla)u$, $\nabla p_\lambda = \lambda^3\nabla p$, $\nu\Delta u_\lambda = \lambda^3\nu\Delta u$이기 때문이다. d차원 공간에서

$$\|u_\lambda(\cdot,t)\|_{L^q} = \lambda^{1-d/q}\,\|u(\cdot,\lambda^2 t)\|_{L^q}. \tag{5.7}$$

따라서 $q=d$이면 이 노름이 스케일링에 불변이다. 이 경우 시간에 대해서도 $\|u_\lambda(\cdot,t)\|_{L^d} = \|u(\cdot,\lambda^2 t)\|_{L^d}$이므로 $\sup_t\|u(\cdot,t)\|_{L^d}$가 스케일링에 불변이다. 이러한 노름을 **임계 노름**(*critical norm*)이라고 한다.

스케일링은 어떤 추정이 문제의 자연스러운 크기를 반영하는지 알려 주지만 증명을 대신하지 않는다. 임계 노름이 유계라는 조건으로 해를 이어갈 수 있는 정리가 있다면, 그 정리에는 시간 적분 지수와 함수공간의 조건이 정확히 들어간다. “임계”라는 이름만으로 충분조건을 추론해서는 안 된다.

주의 (2026년 9월 24일 기준의 최근 발표). 2026년 9월 8일 공개된 OpenAI 원고와 Lean 자료는 매끄러운 외력이 있는 3차원 비압축성 Navier–Stokes에서 유한시간 폭발을 구성하여 Clay 문제의 C/D 경우를 주장한다. Clay 문제의 공식 설명은 네 경우로 나뉜다. A와 B는 외력이 없을 때 $\mathbb{R}^3$과 주기 영역에서 매끄러운 해가 전역에서 존재하는가이고, C와 D는 같은 두 영역에서 외력을

허용한 폭발(전역 매끄러운 해의 부재)이다. 9월 11일 Clay는 해법 발표를 언급하면서 평가 과정은 시간을 두고 진행된다고 밝혔다. 여기서는 이 발표를 무외력 경우의 해결이나 상의 최종 승인으로 표현하지 않는다. 이번 교재 제작에서 그 대규모 Lean 증명을 독립 재빌드한 것도 아니다. 정확한 범위는 원 발표, 공개 형식화, Clay 공지를 함께 읽어야 한다.

5.5 미시적 입자에서 거시적 방정식으로

거시적 유체방정식은 분자 하나하나를 추적하지 않는다. 많은 입자계의 정보를 분포함수로 바꾸고, 다시 밀도·운동량·온도 같은 적은 수의 변수로 줄인다. 이러한 축약이 정당하려면 어느 극한에서 어떤 오차가 사라지는지 증명해야 한다.

Boltzmann 방정식의 분포함수 $F(t,x,v)$는 위치와 속도를 함께 변수로 사용한다. 밀도와 평균 속도는 형식적으로

$$\rho(t,x)=\int F(t,x,v)\,dv, \qquad \rho u(t,x)=\int vF(t,x,v)\,dv \tag{5.8}$$

로 얻는다. 방정식에 1, v, $|v|^2$ 등을 곱해 속도에 대해 적분하면 질량·운동량·에너지의 균형이 나타난다. 이 세 함수가 충돌 연산자의 충돌 불변량이어서 충돌항이 사라지기 때문이다. 하지만 낮은 차수의 모멘트 방정식에는 더 높은 차수의 모멘트가 들어가므로 이 계산만으로 닫힌 유체방정식이 완성되는 것은 아니다. 이를 **모멘트 닫힘 문제**(*moment closure problem*)라고 한다.

> **예제 5.4 (모멘트로 분포를 완전히 알 수는 없다)** 확률변수 X가 ± 1을 같은 확률로 갖는 경우와, 평균 0·분산 1인 표준정규분포는 처음 두 모멘트가 같다. 사실 세 번째 모멘트도 둘 다 0이다. 그러나 전자는 $\mathbb{E}X^4=1$, 후자는 $\mathbb{E}X^4=3$이다. 평균과 분산만 같다고 전체 분포나 모든 고차 상관이 같은 것은 아니다.

Deng, Hani, Ma의 2025년 논문은 hard sphere 입자계에서 Boltzmann의 운동론을 거쳐 특정 유체방정식을 유도하는 프로그램의 성과를 제시한다. 제목에 Hilbert 제6문제가 등장하지만, 이를 물리학 전체의 공리화가 끝났다는 뜻으로 읽어서는 안 된다. 영역, 스케일링, 극한의 순서, 얻어지는 방정식의 종류를 원문에서 확인해야 한다. 출처는 *Hilbert's sixth problem: derivation of fluid equations via Boltzmann's kinetic theory*이다.

5.6 불규칙한 경로와 Itô 보정항

Brown 운동(*Brownian motion*) B_t는 $B_0=0$이며 독립인 Gaussian 증분을 갖고 $B_t-B_s (s<t)$의 분산이 $t-s$인 연속 확률과정이다. 경로가 연속이라는 사실은 보통의 미분이 가능하다는 뜻이 아니다. 작은 시간 간격의 증분 크기는 대략 시간 간격의 제곱근 규모이므로 이차항이 누적된다.

$[0,T]$를 n개로 균등하게 나누고 $\Delta B_k=B_{(k+1)T/n}-B_{kT/n}$라 쓴다. 그러면

$$Q_n=\sum_{k=0}^{n-1}(\Delta B_k)^2, \qquad \mathbb{E}Q_n=T. \tag{5.9}$$

각 ΔB_k는 평균 0, 분산 T/n이므로 $\mathbb{E}(\Delta B_k)^2=T/n$이고 n개를 더하면 T이다. 중심 Gaussian 변수 Z는 $\mathbb{E}Z^4=3(\mathbb{E}Z^2)^2$를 만족하므로 $\mathrm{Var}((\Delta B_k)^2)=3(T/n)^2-(T/n)^2=2(T/n)^2$이고, 증분이 서로

독립이므로 분산이 더해져

$$\operatorname{Var}(Q_n) = n \cdot 2\left(\frac{T}{n}\right)^2 = \frac{2T^2}{n} \to 0. \tag{5.10}$$

따라서 $Q_n \to T$가 L^2에서 성립한다. 경로의 이차변동이 T라는 핵심 현상을 간단한 계산으로 볼 수 있다.

항등식

$$B_{t_{k+1}}^2 - B_{t_k}^2 = 2B_{t_k}\Delta B_k + (\Delta B_k)^2$$

을 합하고 극한을 취하면

$$B_T^2 = 2\int_0^T B_t\, dB_t + T \tag{5.11}$$

를 얻는다. 합하면 좌변은 $B_T^2 - B_0^2 = B_T^2$으로 이어지고, 우변의 $\sum_k (\Delta B_k)^2$이 $Q_n \to T$이다. 마지막 T가 보통의 미분법에 없는 보정항이다. 정확한 적분의 구성에는 적응성, 제곱적분가능성, 확률적 수렴의 지정이 필요하다(제21권 제6장).

> **예제 5.5 (기하 Brown 운동)** $dX_t = \mu X_t\, dt + \sigma X_t\, dB_t$, $X_0 > 0$의 해는
>
> $$X_t = X_0 \exp\left(\left(\mu - \tfrac{1}{2}\sigma^2\right)t + \sigma B_t\right) \tag{5.12}$$
>
> 이다. 지수함수에 Itô 공식을 적용하면 $\frac{1}{2}\sigma^2$항이 다시 더해져 드리프트가 μ가 된다. $-\sigma^2/2$를 빼지 않으면 원래 방정식과 다른 드리프트 $\mu + \sigma^2/2$를 얻는다. 검산으로 $\mathbb{E}e^{\sigma B_t} = e^{\sigma^2 t/2}$이므로 식 (5.12)의 기댓값은 $X_0 e^{\mu t}$이며, 이는 $m' = \mu m$의 해와 일치한다.

5.7 확률 PDE와 정의되지 않은 곱

분포는 매끄러운 시험함수에 작용하는 선형적인 일반화 함수다. Dirac 델타는 함수값을 꺼내는 작용 $\delta(\varphi) = \varphi(0)$으로 정의된다. 분포끼리의 곱은 일반적으로 정의되지 않는다. 따라서 잡음으로 구동되는 비선형 PDE를 기호 그대로 적는 것만으로 해의 의미가 정해지는 것은 아니다.

예를 들어 아주 거친 장 X의 제곱을 생각하려면 먼저 X_ε로 매끄럽게 근사할 수 있다. 하지만 X_ε^2의 평균이 $\varepsilon \downarrow 0$에서 발산하면 단순한 극한은 없다. 중심화된 양

$$X_\varepsilon^2 - \mathbb{E}[X_\varepsilon^2]$$

를 생각하는 것이 **재규격화**(*renormalization*)의 가장 작은 모형이다. 이것만으로 모든 문제의 극한이 존재하는 것은 아니며, 어떤 보정항을 빼야 하고 어떤 공간에서 수렴하는지를 증명해야 한다.

> **예제 5.6 (1차원 백색잡음의 제곱)** ξ를 1차원 백색잡음, ρ를 매끄러운 콤팩트 지지의 함수라 하고 $\rho_\varepsilon(x) = \varepsilon^{-1}\rho(x/\varepsilon)$, $\xi_\varepsilon = \rho_\varepsilon * \xi$로 둔다. 그러면 $\mathbb{E}[\xi_\varepsilon(x)^2] = \int \rho_\varepsilon(y)^2\, dy = \varepsilon^{-1}\int \rho(y)^2\, dy$이므로 $\varepsilon \downarrow 0$에서 $+\infty$로 발산한다. 따라서 ξ^2는 ξ_ε^2의 극한으로 정의될 수 없고, 상수 $\varepsilon^{-1}\int\rho^2$를 뺀 $\xi_\varepsilon^2 - \varepsilon^{-1}\int\rho^2$가 극한의 후보가 된다.

정칙성 구조와 거친 경로 이론은 불규칙한 대상의 국소 전개에 필요한 추가 정보를 체계적으로 관리한다(Hairer의 정칙성 구조는 2014년에 발표되었다). 고전 Taylor 다항식을 외우는 것에서 나아가, 어떤 잡음 기반의 기호가 필요하고 그 기호들을 실제 분포로 어떻게 해석하는지 정한다. Chandra, Hairer, Peev의 2025년 비가환 정칙성 구조 논문은 이러한 이론을 특정 위상대수 값 과정

으로 확장한다. 모든 SPDE의 해법을 제시한 것은 아니다. 원논문과 저자의 확률해석 강의 안내를 연결해 읽을 수 있다.

5.8 동역학의 민감성과 확률적 설명

원 $\mathbb{R}/\mathbb{Z}$ 위의 사상 $T(x) = 2x \pmod 1$을 생각한다. 이진 전개에서는 첫 자리를 버리는 이동처럼 작용한다. 두 점의 초기 간격이 작으면 접히기 전까지 매번 두 배로 벌어진다. 원 위의 거리가 $1/4$ 미만인 동안은 거리가 정확히 두 배가 된다. 그러나 전체 공간의 크기는 유한하므로 계속 직선적으로 멀어지는 것이 아니라 접힘과 퍼짐이 반복된다.

이 예는 결정론적 규칙이 장기 예측을 어렵게 만들 수 있음을 보여 준다. 규칙이 없어서 무작위처럼 보이는 것과, 규칙은 명확하지만 초기조건의 유한한 정확도로 장기 거동을 예측하기 어려운 것은 다르다. 불변측도와 에르고딕 이론은 개별 궤도의 위치 대신 장기 시간평균과 분포를 연구한다.

예제 5.7 T는 원 위의 균등측도를 보존한다. 적분가능한 f에 대해 구간을 반으로 나누고 치환하면

$$\int_0^1 f(Tx)\,dx = \frac{1}{2}\int_0^1 f(y)\,dy + \frac{1}{2}\int_0^1 f(y)\,dy = \int_0^1 f(y)\,dy.$$

실제로 $[0,\tfrac12]$에서는 $y = 2x$, $[\tfrac12,1]$에서는 $y = 2x-1$로 치환하며 각각 $dx = \tfrac12 dy$이다. 측도 보존을 확인한 것만으로 모든 개별 궤도가 같은 시간평균을 갖는다고 결론 내릴 수는 없다. 에르고딕성과 거의 모든 점이라는 조건을 별도로 다루어야 한다. 예컨대 고정점 $x=0$의 궤도의 시간평균은 $f(0)$이고 이것은 일반적으로 $\int_0^1 f$와 다르다. T는 Lebesgue 측도에 대해 에르고딕이므로 Birkhoff 에르고딕 정리에 의해 거의 모든 점의 시간평균이 $\int_0^1 f$와 같다.

5.9 Gronwall 부등식으로 안정성과 유일성을 얻기

PDE와 SDE에서는 해를 정확히 구하지 못해도 두 해의 차이를 제어할 수 있다. 다음 부등식은 그 출발점이다. “오차의 성장률이 현재 오차에 비례한다”는 정보를 지수함수의 상계로 바꾼다.

명제 5.8 (적분형 Gronwall 부등식) $u:[0,T]\to[0,\infty)$가 연속이고 $a,b\ge 0$에 대해

$$u(t) \le a + b\int_0^t u(s)\,ds \tag{5.13}$$

를 만족하면 $u(t)\le a e^{bt}$이다.

증명. $v(t) = a + b\int_0^t u(s)\,ds$라 놓으면 u가 연속이므로 v는 C^1이고 가정에 의해 $u\le v$이다. $b\ge 0$이므로 $v' = bu \le bv$이다. 따라서

$$\frac{\mathrm{d}}{\mathrm{d}t}\left(e^{-bt}v(t)\right) = e^{-bt}(v' - bv) \le 0.$$

$v(0)=a$이므로 $v(t)\le a e^{bt}$이고 $u\le v$를 사용하면 된다. $a=0$인 경우에도 같은 계산이 적용된다. □

예제 5.9 (Lipschitz 조건과 유일성) $y' = F(y)$의 두 해 y, z가 같은 초기값에서 출발하고, 관심 범위에서 $|F(y) - F(z)| \le L\,|y - z|$라 하면 적분형으로 쓸 때

$$|y(t) - z(t)| \le L \int_0^t |y(s) - z(s)|\, ds.$$

Gronwall 부등식에서 $a = 0$을 사용하면 차이는 항상 0이다. 따라서 그 시간 구간에서 해가 유일하다.

초기값이 다르면 $a = |y(0) - z(0)|$가 들어가서 $|y(t) - z(t)| \le a e^{Lt}$를 얻는다. 이는 유한한 시간 동안 초기 오차가 얼마나 증폭될 수 있는지를 정량화한다. 장시간에는 e^{Lt}가 커질 수 있으므로 "연속적으로 의존한다"는 말과 "언제까지나 쉽게 예측할 수 있다"는 말은 다르다.

조건을 없애면 유일성이 실패할 수 있다. 예를 들어 $y' = 2\sqrt{|y|}$, $y(0) = 0$에서는 $y(t) = 0$ 외에도 임의의 $c \ge 0$에 대해

$$y_c(t) = \begin{cases} 0, & 0 \le t \le c, \\ (t - c)^2, & t \ge c \end{cases}$$

가 해다. $t = c$에서 양쪽 미분은 모두 0이므로 식을 만족한다. 오른쪽 함수가 0 근처에서 Lipschitz가 아니라는 점이 앞의 유일성 증명과 연결된다. 실제로 $z = 0$과 비교하면 $|F(y) - F(0)| = 2\sqrt{y}$이고, $y \downarrow 0$에서 $2\sqrt{y} \le Ly$는 성립할 수 없다.

이 예를 PDE에 기계적으로 옮길 수는 없지만, 해의 유일성을 논할 때 함수공간과 정칙성 조건을 적어야 하는 이유를 보여 준다. 같은 방정식에서도 매끄러운 해 범주에서는 유일성이 성립하고 훨씬 약한 해 범주에서는 다른 현상이 나타날 수 있다. "비유일성"이라는 단어만 읽기보다 어떤 해의 범주를 대상으로 하는지 확인해야 한다.

5.10 연습과 해설

연습문제 5.10 $\|v_\lambda\|_q$를 $v_\lambda(x) = \lambda^a \phi(\lambda x)$에 대해 d차원에서 계산하라.

풀이. $q < \infty$에서 치환 $y = \lambda x$를 쓰면 $\|v_\lambda\|_q^q = \lambda^{aq - d}\,\|\phi\|_q^q$이므로 $\|v_\lambda\|_q = \lambda^{a - d/q}\,\|\phi\|_q$이다. 노름이 불변인 지수는 $a = d/q$이다. $q = \infty$에서는 λ^a 배이다.

연습문제 5.11 $X_t = X_0 + \sigma B_t$에 대해 $\mathbb{E}X_t$와 $\mathrm{Var}(X_t)$를 구하라. X_0는 상수다.

풀이. 평균은 X_0, 분산은 $\sigma^2 t$이다. $\mathbb{E}B_t = 0$, $\mathrm{Var}(B_t) = t$이기 때문이다. 평균이 일정하다고 개별 경로가 일정하다는 뜻이 아니다. 확률적 모형에서 평균 방정식만 풀면 변동의 정보를 놓칠 수 있다.

연습문제 5.12 무외력·주기 경계조건의 매끄러운 Navier–Stokes 해에서 에너지 감소를 얻는 데 비압축성 조건이 쓰이는 위치를 설명하라.

풀이. 수송항을 $\int u \cdot \nabla(|u|^2/2)\,dx$로 바꾼 뒤 부분적분하면 $-\int (\nabla \cdot u)\,|u|^2/2\,dx$가 되고, 압력항도 $-\int p\,\nabla \cdot u\,dx$가 된다. 두 항이 0이 된다. 주기성은 경계항을 없애고 점성항은 음의 기울기 제곱 $-\nu \int |\nabla u|^2\,dx$로 남는다. 이 계산이 모든 미분의 정칙성까지 보장하지는 않는다.

제 6 장

증명 보조기 · mathlib · AI: 무엇을 검증했는가

개요 **증명 보조기**(*proof assistant*)는 정확한 형식 명제와 그 명제의 증명 항(proof term)을 받아, 정해진 규칙에 맞는지를 기계적으로 검사하는 프로그램이다. 이 장은 명제와 증명을 타입과 항으로 읽는 관점, 정의적 같음과 명제적 같음의 구분, 전술, 공리 의존성, 수치 인증서, 라이브러리 mathlib의 구조를 차례로 설명하고, “증명된 문장이 의도한 문장인가”, “무엇이 가정으로 남았는가”라는 검증 보고의 기본 질문을 정리한다. 뒤쪽에서는 이분법을 존재 증명 · 알고리즘 · 오차 추정으로 동시에 읽는 예를 통해 검증과 탐색의 역할 분담을 보이고, AI가 증명을 제안하는 경우에도 같은 구분이 필요함을 논한다. 선행 지식: 명제논리, 함수, 귀납법, 기본 대수. 이 장의 작은 Lean 예제는 구조를 설명하는 학습용 소스이며, 독자가 도구 버전을 고정하고 실행 기록을 남기며 사용할 수 있다.

증명 보조기는 자연어로 쓰인 설명을 그대로 믿어 주는 프로그램이 아니다. 정확한 형식 명제와 그 명제의 증명 항을 받아, 정해진 규칙에 맞는지를 검사한다. AI는 이 증명을 찾거나 작성하는 작업을 도울 수 있지만, 발견을 제안하는 역할과 검증하는 역할은 구분해야 한다. 그 구분은 AI가 만든 증명뿐 아니라 사람이 만든 대규모 형식화에도 필요하다.

6.1 명제를 타입으로, 증명을 항으로

함수 $f : A \to B$는 A의 항을 받아 B의 항을 돌려준다. 명제 $P \Rightarrow Q$의 증명도 P의 증명을 받으면 Q의 증명을 만드는 방법으로 이해할 수 있다. 이 대응을 이용하면 논리와 함수의 구조가 맞물린다. 명제를 타입으로, 증명을 그 타입의 항으로 읽는 이 관점을 Curry–Howard 대응이라 부른다.

> **예제 6.1 (함의의 연쇄)** $P \Rightarrow Q$와 $Q \Rightarrow R$가 주어지면 $P \Rightarrow R$를 증명할 수 있다. p가 P의 증명이라고 할 때 첫 함의를 적용하여 q를 만들고, 두 번째 함의를 적용하여 r을 만든다. 함수로는 합성이다.
>
> $$P \xrightarrow{f} Q \xrightarrow{g} R, \qquad p \longmapsto g(f(p)).$$

논리곱의 증명은 두 증명을 함께 담는 구조로 생각할 수 있다. $P \wedge Q$에서 P를 꺼내거나 Q를 꺼낼 수 있으며, 둘을 다시 조립하면 $Q \wedge P$를 얻는다. 존재명제의 증명은 대상을 하나 주고 그 대상이 조건을 만족한다는 증명을 주는 방식으로 이해할 수 있다. 이러한 설명은 단순한 비유에 그치지 않고 의존형 이론(*dependent type theory*)의 실제 구성과 연결된다.

```
theorem v28_imp_trans (P Q R : Prop)
    (f : P -> Q) (g : Q -> R) : P -> R :=
  fun p => g (f p)

theorem v28_and_swap (P Q : Prop)
```

```
    (h : And P Q) : And Q P :=
  And.intro h.right h.left
```

여기서 `Prop`은 명제의 종류를 나타내고, `fun p => ...`는 `p`를 받아 뒤의 식을 돌려주는 함수다. 두 예는 전술을 쓰지 않고 증명 항을 직접 적었다. 첫 정리의 본문 `fun p => g (f p)`는 예제 6.1의 합성 $p \mapsto g(f(p))$와 같고, 둘째 정리의 `And.intro h.right h.left`는 쌍의 두 성분을 맞바꿔 다시 조립하는 식이다. 논리적 구조가 작을 때는 이렇게 쓰는 것이 인간에게도 투명할 수 있다.

6.2 정의로 같은 것과 정리로 같은 것

수학자는 $n + 0 = n$을 당연하게 쓰지만, 증명 보조기에서는 자연수 덧셈이 어떻게 정의되었는지가 중요하다. 재귀 정의의 어느 인수에 대해 계산하는지에 따라 한쪽 식은 정의를 펼치는 것만으로 같아지고, 다른쪽 식은 귀납법이 필요할 수 있다. Lean의 자연수 덧셈은 둘째 인수에 대한 재귀로 정의되어, $n + 0 = n$과 $n + \mathrm{succ}(m) = \mathrm{succ}(n + m)$이 정의에서 곧바로 나온다. 따라서 $n + 0$은 정의를 펼치면 n이 되지만, $0 + n$은 n이 구체적인 수가 아니면 펼칠 수 없다.

```
theorem v28_add_zero (n : Nat) : n + 0 = n := by
  rfl


theorem v28_zero_add (n : Nat) : 0 + n = n := by
  induction n with
  | zero => rfl
  | succ n ih => exact congrArg Nat.succ ih
```

이 예에서 `rfl`은 계산과 정의를 통해 양쪽이 같음을 확인하는 방식이다. 두 번째 증명은 $n = 0$을 확인하고, $0 + n = n$이라는 귀납가정에 후속자 함수를 적용한다. 작은 귀납 증명을 형식화하면 사람이 당연하게 생략하던 재귀 구조가 드러난다.

정의적 같음(*definitional equality*)과 **명제적 같음**(*propositional equality*)을 구분하는 것은 현대 기초론에서도 중요하다. 같은 식으로 계산되는가와, 같다는 정리를 가지고 있는가는 다른 층이다. 두 구조가 동형이라는 증명과 두 구조를 같은 타입으로 취급하는 규칙도 구분해야 한다. HoTT(호모토피 타입 이론)의 일가성(*univalence*)에 관한 논의가 이러한 문제를 다른 방식으로 조직하지만, 그 공리를 모든 증명 보조기가 기본으로 채택하는 것은 아니다.

6.3 전술은 증명을 만드는 도구다

전술(*tactic*)은 증명 상태를 변형하는 프로그램이다. 목표를 더 작은 목표로 나누고, 가정을 적용하고, 이미 알려진 정리를 찾아 합성한다. 전술이 성공했다는 표시는 최종적으로 검사할 수 있는 증명 항을 만들었다는 의미여야 한다. 전술의 이름을 많이 아는 것과 수학적 명제를 정확히 세우는 것은 별개다.

```
theorem v28_pair (P Q : Prop)
    (hp : P) (hq : Q) : And P Q := by
  constructor
  . exact hp
  . exact hq
```

처음 목표는 두 증명을 묶는 것이다. `constructor`가 목표를 P와 Q의 두 부분으로 나누고, 각각 이미 주어진 가정을 사용한다. 이 작은 예는 큰 자동화에서도 유지되는 원리다. 자동화가 수천 단계를 처리하더라도 최종 명제와 사용된 가정이 변해서는 안 된다.

자동화가 실패하면 이유를 분류해야 한다. 정리가 거짓일 수도 있고, 참이지만 도구가 찾지 못했을 수도 있고, 자연수와 정수의 형 변환이 누락되었을 수도 있다. 함수의 정의역이나 부등식의 엄격성 차이처럼 작은 형식 차이가 원인인 경우도 많다. 실패 메시지는 수학적 반례와 같지 않다.

6.4 빈 가정과 달라진 문제를 찾아내기

형식 검증에서 가장 중요한 첫 질문은 “증명된 문장이 의도한 문장인가”이다. 다음 두 명제는 다르다.

$$\forall x \in \mathbb{R},\ x^2 > 0, \qquad\qquad \forall x \in \mathbb{R},\ x \neq 0 \implies x^2 > 0.$$

첫 문장은 $x = 0$에서 거짓이고 둘째는 참이다. 둘째를 증명하고 첫째를 해결했다고 말하면 문제를 바꾼 것이다.

> **예제 6.2 (공허하게 참인 명제)** 모순된 가정 $x > 1$과 $x < 0$을 동시에 놓으면 어떤 결론도 논리적으로 따라온다. 따라서 대규모 형식화에서 가정이 일관된 상황을 실제로 허용하는지 작은 모형을 확인하는 일이 유용하다. 모든 증명에서 가정의 무모순성을 내부적으로 증명해야 한다는 뜻은 아니지만, 의도와 달리 가정이 강해진 실수를 찾아내야 한다.

분모, 극한, 최댓값의 형식화에서는 특별한 주의가 필요하다. 일부 체 라이브러리에서는 나눗셈을 모든 입력에 대해 정의하기 위해 $0^{-1} = 0$과 같은 관례를 사용한다. 이 관례 아래에서 $0/0 = 0$이므로 $x/x = 1$은 $x = 0$에서 오히려 거짓이다. 따라서 이는 $x/x = 1$을 아무 가정 없이 증명할 수 있다는 뜻이 아니다. $x \neq 0$을 넣은 정리를 사용해야 한다. 계산기가 입력을 받아들였다는 사실과 수학적으로 의도한 조건이 충족되었다는 사실은 다르다.

> **예제 6.3 (유한 실험이 무한 정리를 대신하는 형식화)** “모든 $n \le 10^6$에서 성립한다”를 정확하게 증명한 코드는 가치가 있다. 그러나 목표가 “모든 자연수 n에서 성립한다”였다면 빠진 범위가 있다. 코드가 완벽히 검증되었어도 이 간극은 사라지지 않는다. 명제의 양화 범위는 출력 결과보다 먼저 읽어야 한다.

6.5 공리와 의존성을 추적하기

어떤 결론을 증명할 때 이미 알려진 정리를 사용할 수 있다. 그 정리가 다시 다른 정리에 의존한다면 전체 의존성 그래프를 따라가야 한다. 작은 **커널**(*kernel*)이 최종 증명 항을 검사하더라도, 허용된 공리를 무엇으로 설정했는지가 결과의 의미를 결정한다.

Lean에서는 정리 이름에 대한 다음 명령으로 공리 의존성을 조사할 수 있다.

```
#print axioms v28_imp_trans
#print axioms v28_zero_add
```

앞 절의 두 정리는 전술 `rfl`과 귀납법만 쓰므로, 정상적인 환경에서는 어느 공리에도 의존하지 않는다는 취지의 출력이 나온다. 출력의 정확한 문구는 도구 버전에 따라 다를 수 있으므로, 실행 기록을 남길 때 버전과 함께 적는다.

고전 논리, 선택, 명제 외연성, 몫의 원리와 같은 기초적 선택은 라이브러리의 기반을 이룰 수 있다. 이를 연구 문제의 결론을 그대로 가정하는 것과 혼동해서는 안 된다. 반대로 미증명 사실을 별도 공리로 넣었다면 결과는 그 사실을 가정한 **조건부 정리**이다. `sorry`와 같은 미완성 자리표시자를 남긴 상태를 완성된 검증과 같은 의미로 보고해서는 안 된다.

> **예제 6.4 (조건부 논증도 정확히 표시하면 유용하다)** 명제 H로부터 어려운 결론 C를 도출하는 모든 단계를 형식화했다고 하자. 이 작업은 $H \Rightarrow C$라는 정리를 준다. H의 독립된 증명을 연결하면 C가 따라온다. 아직 연결하지 않았다면 무엇이 남았는지 명확해진다. 조건부 형식화의 가치는 이 경계를 드러내는 데 있다.

2026년 9월 24일 확인한 PrimeGaps186 저장소는 세 가지 명시적인 입력 공리에 조건부인 Lean 전개와 수치 인증서를 제공한다고 설명한다. 따라서 이를 목표 명제 $\liminf_n (p_{n+1} - p_n) \le 186$의 무조건적 완전한 Lean 증명이라고 소개하면 잘못이다. 그 사례에서 배울 핵심은 발표 제목보다 최종 명제, 입력 공리, 수치 계산의 역할을 먼저 읽는 습관이다. 이 저장소의 내용은 해당 시점의 설명에 근거한 것이며, 이 교재가 직접 재빌드하여 확인한 것이 아니다.

6.6 수치 인증서가 증명이 되는 방식

수치 계산에는 적어도 세 층이 있다. 부동소수점 근사값을 출력하는 계산, 오차를 엄밀하게 감싼 구간 계산, 그리고 유한한 정수·유리수 **인증서**(*certificate*)를 검사하는 계산이다. 첫째 결과가 작게 보인다고 수학적으로 0이라고 결론 내릴 수 없다. 둘째와 셋째는 문제에 맞게 구성하면 엄밀한 증명의 일부가 될 수 있다.

> **예제 6.5 (제곱근을 구간으로 인증하기)** $1.4142^2 < 2 < 1.4143^2$를 정수 계산으로 확인하면
>
> $$1.4142 < \sqrt{2} < 1.4143$$
>
> 을 얻는다. 소수점 출력을 믿는 대신 양변에 10^8을 곱해 정수 비교로 바꿀 수 있다. 실제로 $1.4142^2 \cdot 10^8 = 199\,996\,164 < 200\,000\,000 < 200\,024\,449 = 1.4143^2 \cdot 10^8$이다. $t \mapsto t^2$이 $[0, \infty)$에서 순증가하므로 이 부등식에서 위의 구간 포함이 따라온다. 구간의 양 끝점이 정확한 유리수라는 사실이 중요하다.

근의 존재를 인증할 때에도 근삿값 하나만으로는 부족하다. 연속함수 f가 구간 양 끝에서 부호를 바꾸면 중간값정리로 적어도 하나의 근을 보장할 수 있다. 도함수가 그 구간에서 양수임을 엄밀히 보이면 근의 유일성도 얻는다. 근삿값을 찾는 단계와 존재·유일성을 인증하는 단계가 분리된다.

명제 6.6 미분가능한 $f:[a,b]\to\mathbb{R}$가 $f(a)<0<f(b)$이고 모든 $x\in(a,b)$에서 $f'(x)>0$이면 (a,b)에 정확히 하나의 근이 있다.

증명. 미분가능한 함수는 연속이므로 중간값정리로 근이 하나 이상 존재하고, $f(a),f(b)\neq 0$이므로 근은 (a,b) 안에 있다. 서로 다른 두 근 $c<d$가 있다면 f는 $[c,d]$에서 연속이고 (c,d)에서 미분가능하며 $f(c)=f(d)$이므로 Rolle 정리에 의해 $(c,d)\subset(a,b)$에서 도함수가 0인 점이 있어야 한다. 이는 가정과 모순이다. □

대형 계산 증명에서는 이 같은 작은 논증을 훨씬 많은 구간과 부등식에 적용한다. 유한한 인증서를 재검사하는 프로그램과 인증서를 생성하는 탐색 프로그램을 나누면, 복잡한 탐색의 모든 세부를 신뢰하지 않고도 결과를 확인할 수 있는 경우가 있다. 다만 인증서의 수학적 의미를 연결하는 정리가 필요하다.

6.7 mathlib는 정리 목록이 아니라 연결된 언어다

mathlib에는 수론, 대수, 위상, 해석 등 여러 분야의 정의와 정리가 연결되어 있다. 같은 구조를 서로 다른 이름으로 다시 정의하면 이미 존재하는 정리를 적용하기 어려워질 수 있다. 예컨대 군을 직접 새 구조로 만들기보다 표준 군 구조를 사용하면 준동형, 부분군, 몫군에 대한 결과를 함께 사용할 수 있다.

라이브러리의 추상화는 한 정리를 여러 구체적 상황에 적용하게 해 준다. 실수에서의 부등식처럼 보이는 결과가 더 일반적인 순서체에서 증명되어 있으면 유리수 등에도 재사용할 수 있다. 반대로 필요 이상으로 추상화하면 초심자가 형과 가정을 읽기 어려워질 수 있다. 학습에서는 구체적 예와 추상적 정리를 번갈아 확인하는 것이 좋다.

버전 관리도 수학적 재현성의 일부다. 같은 파일 이름이라도 라이브러리의 정의와 정리 이름이 바뀔 수 있다. 실행한 프로젝트의 commit, `lean-toolchain`, 의존성 목록, 검증 명령과 로그를 함께 남겨야 한다. 단순히 “최신 mathlib에서 된다”고 적으면 시간이 지난 뒤 무엇을 실행했는지 재현하기 어렵다.

공개 자료. mathlib4 저장소와 Apache 2.0 라이선스, Mathematics in Lean, Lean 공식 문서를 함께 참고할 수 있다. 코드의 라이선스를 별도 교재의 모든 문장과 그림에 자동 적용해서는 안 된다. 실제 인용과 개작은 해당 자료의 권리 표시를 따른다.

6.8 거대 형식화의 최근 사례와 남는 질문

2026년 9월 4일 Anthropic은 Fermat의 마지막 정리에 대한 대규모 Lean 형식화를 발표하고 코드를 공개했다. 새로움은 이미 증명된 정리를 컴퓨터가 검사할 수 있는 구조로 옮기는 데 있다. 이것을 Fermat의 문제에 대한 새로운 초등적 증명이라고 소개해서는 안 된다. 이 교재는 해당 프로젝트를 로컬에서 독립 재빌드했다고 주장하지 않으며, 공개 발표와 자료의 존재를 기준으로 연구 지도를 제공한다. 독자는 공식 발표와 공개 저장소를 직접 확인할 수 있다.

대규모 형식화가 공개되면 다음 질문들이 남는다. 최상위 정리는 원래 문장과 정확히 같은가. 사용한 공리는 무엇인가. 의존성에 미완성 부분이 없는가. 설명문과 코드의 대응이 읽기 쉬운가.

재검사가 가능한 시간과 자원 안에 실행되는가. 검증된 중간 결과를 다른 연구자가 재사용할 수 있는가. 정답 여부만이 아니라 이해 가능성과 유지보수성이 새로운 연구 대상이 된다.

AI가 보조정리를 제안하거나 전술을 찾아주는 것은 유용할 수 있다. 하지만 자연어 설명에서 변수의 범위를 슬쩍 바꾸거나, 필요한 가정을 누락하거나, 비슷한 정리의 이름을 잘못 가져오는 오류는 여전히 검토해야 한다. AI의 확신에 찬 문장은 인증서가 아니다. 정확한 명제, 실제 증명 자료, 독립적인 확인 경로를 남기는 것이 핵심이다.

6.9 작은 형식화 프로젝트를 완성하는 순서

처음부터 유명한 난제를 목표로 삼기보다, 인간이 완전히 이해하는 작은 정리를 고른다. 자연수 합 공식, 유한집합의 이중계수, 간단한 수열 부등식 등이 좋다. 먼저 종이에 증명을 쓰고, 각 줄에 필요한 정의와 보조정리를 표시한다. 이어 형식 명제의 입력과 출력이 종이의 문장과 같은지 비교한다.

다음에는 가장 작은 예부터 실행한다. 일반 정리를 여러 보조정리로 나누면 실패가 발생한 위치를 찾기 쉽다. 마지막에는 컴파일 성공뿐 아니라 미완성 표시와 추가 공리, 최상위 정리의 가정 목록을 확인한다. 프로젝트 설명에는 무엇을 실행했고 무엇을 아직 실행하지 않았는지를 분리해서 적는다.

> **예제 6.7 (홀수 제곱의 홀수성)** 정수 $n = 2k + 1$이면
>
> $$n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$
>
> 이므로 n^2도 홀수다. 형식화할 때에는 홀수의 정의가 어떤 형태인지 먼저 확인하고, 존재 증인 $2k^2 + 2k$를 제공하며, 남은 다항식 항등식을 검증한다. 짧은 증명이지만 존재명제, 대입, 대수 계산을 모두 포함한다.

자연어와 코드를 병행하는 이유는 서로 다른 오류를 잡기 때문이다. 자연어는 논증의 목적과 핵심 아이디어를 드러내고, 코드는 누락된 조건과 정의의 불일치를 드러낸다. 어느 한쪽만 길게 늘리는 대신 두 표현 사이의 대응을 명확히 하면 작은 프로젝트도 신뢰할 수 있는 학습 결과가 된다.

6.10 이분법을 증명과 알고리즘으로 동시에 읽기

연속함수 f가 $f(a) < 0 < f(b)$를 만족할 때 **이분법**(*bisection method*)은 구간의 중점을 검사하여 부호가 바뀌는 절반을 반복해서 택한다. 각 단계에서 중요한 것은 단순히 중점을 계산했다는 사실이 아니라, 해를 포함하는 구간이라는 **불변조건**(*invariant*)을 유지했다는 사실이다.

n번째 구간을 $[a_n, b_n]$이라 하자$(a_0 = a,\ b_0 = b)$. 중점 $m_n = (a_n + b_n)/2$에서 $f(m_n) = 0$이면 끝난다. 그렇지 않으면 $f(m_n)$의 부호에 따라 $[a_n, m_n]$ 또는 $[m_n, b_n]$를 택한다. 정확한 부호 판정이 가능하다는 조건 아래,

$$f(a_n) < 0 < f(b_n), \qquad b_n - a_n = 2^{-n}(b - a) \tag{6.1}$$

이 유지된다.

구간들은 중첩되고 길이는 0으로 간다. 실수의 완비성에 의해 공통점 r이 하나 존재한다. a_n은 증가하고 b_n은 감소하며 둘 다 r로 수렴하므로, 연속성과 식 (6.1)에서 $f(r) = \lim f(a_n) \le 0$이고 $f(r) = \lim f(b_n) \ge 0$이다. 따라서 $f(r) = 0$이다. $r \in [a_n, b_n]$이므로 중점을 근삿값으로 쓰면 오차는 구간 길이의 절반 이하이다.

$$|m_n - r| \le 2^{-n-1}(b - a). \tag{6.2}$$

따라서 원하는 오차 ε를 얻기 위한 반복 횟수를 미리 정할 수 있다. 존재 정리, 알고리즘, 오차 추정이 한 논증 안에서 연결된다.

> **예제 6.8 (이분법의 한 단계씩 따라가기)** $f(x) = x^2 - 2$를 $[a, b] = [1.4, 1.5]$에서 생각한다 ($f(1.4) = -0.04 < 0 < 0.25 = f(1.5)$). $m_0 = 1.45$에서 $f(m_0) = 0.1025 > 0$이므로 $[a_1, b_1] = [1.4, 1.45]$이다. $m_1 = 1.425$에서 $f(m_1) = 0.030625 > 0$이므로 $[a_2, b_2] = [1.4, 1.425]$이다. $m_2 = 1.4125$에서 $f(m_2) = -0.00484375 < 0$이므로 $[a_3, b_3] = [1.4125, 1.425]$이고 길이는 $0.0125 = 2^{-3} \cdot 0.1$이다. 허용 오차 $\varepsilon = 10^{-6}$를 보장하려면 식 (6.2)에서 $2^{-n-1} \cdot 0.1 \le 10^{-6}$, 곧 $2^{n+1} \ge 10^5$이어야 하고, $2^{16} = 65\,536 < 10^5 < 131\,072 = 2^{17}$이므로 $n = 16$이 필요한 최소의 단계 수이다.

흔한 오류. 부동소수점 계산에서 $f(m_n)$가 0에 매우 가까우면 부호를 잘못 판정할 수 있다. 엄밀한 이분법 인증에는 정확한 산술이나 오차를 포함한 구간 판정이 필요하다. 실제 프로그램이 어떤 판정 방법을 쓰는지 확인해야 한다.

형식화 관점에서는 명세, 불변조건, 종료 또는 수렴 논증을 분리할 수 있다. 유한 단계의 프로그램은 지정한 길이 이하의 구간을 돌려주는 것이 명세가 될 수 있다. 그 구간에 실제 근이 있다는 사실은 중간값정리와 유지된 부호 조건에서 따라온다. 무한한 반복 자체를 컴퓨터가 끝낼 필요는 없다. 임의의 허용 오차에 대해 유한한 인증서를 만들 수 있음을 보이면 된다.

> **예제 6.9 (검사 프로그램의 역할)** 생성 프로그램이 유리수 끝점 a, b를 찾아 주고, 별도의 검사 프로그램이 $f(a) < 0 < f(b)$와 $b - a \le \varepsilon$를 확인한다고 하자. f가 유리수 계수 다항식이면 끝점에서의 값은 정확한 유리수로 계산할 수 있다. 연속성은 다항식에 대한 일반 정리에서 얻는다. 생성 프로그램이 어떤 탐색을 했는지 모두 신뢰하지 않아도 이 인증서를 검토할 수 있다.

이 구조는 AI 보조 연구에도 유용하다. AI는 후보 구간이나 보조정리, 조합적 객체를 빠르게 제안할 수 있다. 검증 단계는 그 후보가 정확한 명세를 만족하는지 독립적으로 확인한다. 다만 모든 수학 문제가 이분법처럼 짧은 인증서를 갖는 것은 아니다. 인증서의 존재와 검사 비용 역시 문제의 구조에 따라 달라진다.

6.11 연습과 해설

> **연습문제 6.10** $P \wedge Q \Rightarrow P$와 $P \Rightarrow P \vee Q$의 증명 구조를 함수와 생성자의 언어로 설명하라.

풀이. 첫째는 주어진 쌍에서 첫 성분을 꺼내는 연산이다. 둘째는 P의 증명을 받아 논리합의 왼쪽 경우를 선택하는 연산이다. Q가 참인지 판단할 필요가 없다. 어떤 논리 규칙이 계산적으로 무엇을 하는지 확인할 수 있다.

연습문제 6.11 $x/x = 1$을 모든 실수에 대해 주장한 파일이 검증되었다고 들었다. 가장 먼저 무엇을 확인해야 하는가?

풀이. 정리의 실제 형식 문장을 확인한다. $x \neq 0$이 가정으로 들어갔는지, 정의역이 0을 제외하는 타입인지, 나눗셈이 표준 체의 나눗셈인지, 결론을 강제하는 추가 공리가 있는지 살펴본다. 표준 체의 나눗셈에서는 $0/0 = 0$이므로 가정 없는 명제 $\forall x,\ x/x = 1$은 증명될 수 없고, 그렇게 보고되었다면 형식 문장이 요약과 다르다는 신호이다. 사람이 전한 요약만으로 형식 명제를 추측하지 않는다.

연습문제 6.12 정리 $H \Rightarrow C$를 형식화한 경우에 "C를 완전히 형식화했다"는 보고를 어떻게 고치면 정확한가?

풀이. "가정 H로부터 C를 도출하는 부분을 형식 검증했으며, H의 증명 연결은 별도 단계로 남아 있다"고 쓴다. H가 외부 원논문의 정리라면 그 정확한 판본과 문장을 제시한다. H가 이미 라이브러리에서 증명된 경우에는 해당 의존성을 연결하고 최상위 공리 목록을 다시 확인한다.

연습문제 6.13 $f(x) = x^2 - 2$의 양의 근이 $(1.4, 1.5)$에 정확히 하나 있음을 인증하라.

풀이. $f(1.4) = -0.04 < 0$, $f(1.5) = 0.25 > 0$이고 구간에서 $f'(x) = 2x > 0$이다. 존재는 중간값정리, 유일성은 엄격한 증가성 또는 Rolle 정리로 얻는다(명제 6.6). 계산된 소수들은 유한소수이므로 정확한 유리수 비교로 바꾸어 검증할 수 있다.

연습문제 6.14 자신이 만든 작은 증명 프로젝트를 다른 사람에게 전달할 때 필요한 재현 정보와 수학적 설명을 구분해 적어 보라.

풀이. 재현 정보에는 소스, 도구 버전, 의존성 commit, 실행 명령, 성공 로그가 들어간다. 수학적 설명에는 정확한 정리, 가정의 의미, 사용한 보조정리, 증명의 핵심 아이디어, 형식화하지 않은 부분이 들어간다. 두 목록이 모두 있어야 실행과 이해를 함께 이어갈 수 있다.

부록

개정 기록

부록 A

개정 내역

개요 이 판(백과사전식 개정판 · 3차 집필본 0.3.0 (2026-11-13))은 직전 판의 원고를 처음부터 다시 조판하면서 내용을 검토한 개정판이다. 집필 단계에서 원본의 오류를 고치고 빠진 내용을 보충했으며, 독립 검토 단계에서 모든 수식과 유도를 다시 계산해 대조했다. 아래에 작업 단위별 집계와, 원본에서 바로잡은 오류의 목록을 싣는다. 보충한 내용의 전체 목록은 원고 저장소의 `CHANGELOG.md`에 있다.

A.1 집계

구분	건수
원본 오류 수정	27
내용 보충	761
독립 검토에서 바로잡은 사항	67

작업 단위	오류 수정	보충	검토 수정
제1권 제1–2장	4	19	9
제1권 제3–5장	0	5	2
제1권 제6–7장	0	13	0
제1권 제8–9장	0	10	2
제1권 제10–11장	0	13	1
제2권 제1–3장	0	6	0
제2권 제4–6장	0	9	0
제2권 제7–9장	0	10	0
제3권 제1–2장	0	5	0
제3권 제3–4장	0	11	0
제3권 제5장	5	10	0
제4권 제1장	0	5	0
제4권 제2장	0	7	0
제4권 제3장	0	4	2
제4권 제4장	0	7	0
제4권 제5장	0	5	0

작업 단위	오류 수정	보충	검토 수정
제4권 제6장	0	5	0
제4권 제7장	0	5	0
제4권 제8장	0	9	0
제4권 제9장	0	7	0
제4권 제10장	0	6	0
제4권 제11장	0	4	1
제4권 제12장	0	11	0
제5권 제1–2장	0	13	1
제5권 제3장	0	3	1
제5권 제4장	0	3	0
제5권 제5장	0	5	1
제5권 제6장	0	5	1
제7권 제1장	0	5	0
제7권 제2장	0	6	0
제7권 제3장	0	5	1
제7권 제4장	0	4	0
제7권 제5장	0	4	2
제7권 제6장	0	4	0
제7권 제7장	0	4	1
제7권 제8장	0	3	0
제8권 제1장	0	6	0
제8권 제2장	0	5	0
제8권 제3장	0	11	1
제8권 제4장	0	13	0
제8권 제5장	0	8	1
제8권 제6장	0	8	0
제9권 제1–2장	0	5	1
제9권 제3–4장	0	6	0
제9권 제5–6장	0	8	0
제9권 제7–8장	0	9	0
제10권 제1–2장	0	7	0
제10권 제3–5장	0	4	0
제10권 제6–8장	1	22	4
제11권 제1–3장	5	20	12

작업 단위	오류 수정	보충	검토 수정
제11권 제4–6장	1	4	0
제11권 제7–8장	0	5	0
제12권 제1–3장	0	11	1
제12권 제4–6장	0	7	0
제12권 제7–8장	0	13	4
제13권 제1–3장	0	18	3
제13권 제4–6장	3	7	2
제13권 제7–8장	0	6	1
제14권 제1–3장	0	23	0
제14권 제4–6장	0	22	5
제14권 제7–8장	0	14	1
제15권 제1–3장	0	21	1
제15권 제4–6장	0	10	2
제15권 제7–8장	0	7	0
제19권 제1–3장	0	11	0
제19권 제4–5장	0	7	2
제19권 제6장	0	4	0
제20권 제1장	0	3	0
제20권 제2장	0	8	0
제20권 제3장	0	6	0
제20권 제4장	0	4	0
제20권 제5장	0	3	1
제20권 제6장	0	6	0
제20권 제7–8장	0	13	0
제20권 제9장	0	7	0
제20권 제10장	0	6	0
제20권 제11장	0	9	0
제20권 제12장	0	8	0
제21권 제1–2장	0	8	0
제21권 제3–4장	0	12	0
제21권 제5장	0	7	0
제21권 제6장	0	8	0
제22권 제1–2장	1	8	0
제22권 제3–4장	2	13	0

작업 단위	오류 수정	보충	검토 수정
제22권 제5장	0	5	0
제22권 제6장	0	8	0
제28권 제1장	0	6	0
제28권 제2장	1	7	0
제28권 제3장	0	8	0
제28권 제4장	1	8	0
제28권 제5장	0	11	0
제28권 제6장	3	7	0

A.2 원본에서 바로잡은 오류

제1권 제1–2장

- **원본 45쪽 연습문제 1.9 풀이** 역원의 유일성 증명 $b = b(ac) = (ba)c = c$에 빠진 단계 $(ba)c = (ab)c = 1 \cdot c$를 넣고, 사용한 법칙에 교환법칙을 추가함 (원본은 결합법칙과 항등원만 썼다고 했으나 $ba = ab = 1$로 바꾸는 데 교환법칙이 필요함)
- **원본 45쪽 예제 1.6** 크기 검사를 '약 2500 근처'에 더해 하한·상한 $2400 < 48 \cdot 51 < 2550$으로 구체화하고, 24480과 2248이 각각 어느 검사에 걸리는지 밝힘 (2248은 마지막 자리가 8이고 2500에서 10% 정도만 벗어나므로 원본에 적힌 두 검사만으로는 걸러진다고 단정할 수 없음)
- **원본 45쪽 예제 1.7** '분모끼리 더한 12/30'을 '분자는 분자끼리, 분모는 분모끼리 더한 12/30'으로 고침 (12/30은 분자 7+5와 분모 12+18을 각각 더한 결과이며 분모만 더한 것이 아님)
- **원본 48쪽 예제 2.6** '나머지들은 198>54>36>18>0'을 '제수와 나머지의 열'로 고침 (198은 나머지가 아니라 첫 단계의 제수임)

제3권 제5장

- **원본 124쪽 5.2절, 정의 5.3 다음 문단** 초점 조건 '$a > c \geq 0$'을 타원에서는 $a > c > 0$, 원까지 포함할 때 $a > c \geq 0$으로 나누어 적음 (정의 5.3은 '서로 다른 두 초점'을 요구하므로 $c = 0$을 타원의 조건에 그대로 넣으면 정의와 어긋남)
- **원본 126쪽 예제 5.8** '이 점의 기울기는 2/3'을 '원점과 이 점을 잇는 직선의 기울기는 2/3'으로 고침 (기울기는 점이 아니라 직선의 양이며, 방향각의 탄젠트와 비교하는 대상은 원점에서 그 점으로 가는 직선임)
- **원본 126쪽 5.6절 첫 문단** '원점이 아닌 점에서 $r = \sqrt{x^2 + y^2}$'을, $r = \sqrt{x^2 + y^2}$은 모든 점에서 성립하고 원점이 아닌 점에서 방향각이 2π의 정수배를 제외하고 유일하다는 진술로 나눔 (반지름 공식은 원점에서도 성립하며, 원점을 제외해야 하는 것은 방향각의 유일성뿐임)
- **원본 126쪽 예제 5.10** r을 곱해 얻은 식에서 '따라서 원이다'로 넘어가던 부분에 역방향 확인(원 위의 원점 아닌 점에서 $\cos\theta > 0$이고 $r = 2a\cos\theta$가 복원됨, 원점은 $\theta = \pi/2$에서 얻어짐)을 넣음 (r을 곱하는 변형은 동치가 아니어서 한 방향의 포함 관계만 주며, 자취가 원 전체라는 결론에는 역방향이 필요함)

- **원본 125쪽 그림 5.1 설명** '주황 점'을 '검은 점'으로 바꾸고 세 곡선의 방정식($x^2 = 4y$, $x^2/9+y^2/4 = 1$, $4x^2/9 - y^2 = 1$)을 설명에 명시함 (개정판 그림은 흑백 선 그림이므로 색 이름이 맞지 않고, 원본 설명에는 어떤 곡선을 그렸는지가 없었음)

제10권 제6–8장

- **원본 379쪽, 제8장 명제 8.5(Jordan 분해)의 증명** 증명이 "$F = V_a^x(F) - (V_a^x(F) - F(x))$"라는, 괄호를 풀면 $F = F$가 되어버리는 자명한 항등식만 적혀 있어 두 항이 실제로 증가함수라는 사실을 보이지 않았다. $V(x) = V_a^x(F)$라 두고 $x < y$에서 $V(y) - V(x) \geq |F(y) - F(x)| \geq F(y) - F(x)$를 이용해 $V(x)$와 $V(x) - F(x)$가 둘 다 증가함수임을 직접 보이는 증명으로 고쳤다. (원본의 식은 모든 F에 대해 항상 성립하는 항등식이어서, 유계변동 함수가 두 증가함수의 차로 쓰인다는 명제의 증명이 되지 못한다.)

제11권 제1–3장

- **원본 384쪽 예제 1.4** g(z)=|z|^2이 z=0에서만 Cauchy–Riemann 방정식을 만족한다는 결론의 근거에 u_y=2y, v_x=0을 보태어 두 방정식 2x=0, 2y=0을 모두 제시함 (원본은 u_x=2x, v_y=0만 적었는데 이것만으로는 x=0밖에 나오지 않아 추론이 불완전함)
- **원본 387쪽 2.3절** 'Log는 음의 실수축 $(-\infty,0]$에서 불연속'을 '음의 실수축의 모든 점에서 불연속이고 분지절단은 반직선 $(-\infty,0]$'으로 고침 (Log는 0에서 정의되지 않으므로 0에서의 불연속을 말할 수 없음)
- **원본 387쪽 2.4절 둘째 항목** 'z^{1/2}는 두 값 ±를 갖는다'를 '두 값 ±e^{(1/2)Log z}'로 완성함 (원본 식이 ± 뒤에서 끊겨 있음)
- **원본 388쪽 정리 2.5 다음 문단** 실변수 C^∞ 함수에 일치의 원리가 없다는 예를 'x>0에서 e^{-1/x^2}, x≤0에서 0' 인 함수로 명시함 (원본이 든 e^{-1/x^2} 자체는 영점이 한 점뿐이라 '집적점을 갖는 집합에서 0이지만 항등적으로 0은 아님'이라는 반례가 되지 못함)
- **원본 391쪽 예제 3.7** '제5–7장의 유수 정리와 편각 원리'를 '제6장의 유수 정리와 제7장의 편각 원리'로 고침 (권 구성표에서 제5장은 Laurent 급수이고 유수 정리는 제6장, 편각 원리는 제7장임)

제11권 제4–6장

- **원본 394쪽 연습문제 4.11 풀이** $\oint_{|z|=3} \sin z/(z^2(z-\pi))\,dz$ 풀이에서 'π 근처의 기여는 $2\pi i \sin\pi/\pi^2 = 0$이다'라는 문장이 $z = \pi$가 적분 경로 $|z| = 3$ 내부에 있는 것처럼 읽혔던 것을, $3 < \pi$이므로 $z = \pi$는 사실 경로 바깥에 있으며 $\sin\pi = 0$으로 그 점이 애초에 제거가능 특이점(정칙점)이어서 경로 안팎과 무관하게 기여가 0이라는 설명으로 바꿈

제13권 제4–6장

- **원본 444쪽 명제 4.3 (자기수반 작용소의 성질)** (iii) $\sigma(T) \subseteq \mathbb{R}$과 $\|T\| = \sup_{\|x\|=1} |\langle Tx, x\rangle|$의 증명을 새로 작성함 (원문은 (i), (ii)만 '유한차원과 같은 계산'이라며 한 줄로 넘기고 (iii)의 증명은 아예 제시하지 않았다)
- **원본 445쪽 예제 4.5 (Hilbert–Schmidt 적분 작용소)** 자기수반 조건을 실수 대칭 $k(x,y) = k(y,x)$에서 복소 Hilbert 공간에 맞는 켤레대칭 $k(x,y) = \overline{k(y,x)}$로 바로잡음 (같은 쪽에서 정의한 수반 작용소 $\langle Tx, y\rangle = \langle x, T^*y\rangle$와 들어맞으려면 켤레가 필요하다. 복소 계수가 섞인 핵에서는 원문의 조건이 자기수반성을 보장하지 못한다)
- **원본 451쪽 정의 6.1 (정칙 Sturm–Liouville 문제)** '$p > 0$, p', q, $w > 0$이 연속'이라는 표기가 q에도 양수 조건을 거는 것으로 읽힐 수 있어, q는 부호 조건 없는 연속 실함수이고 w만 양수라고 명확히 구분함 (정칙 Sturm–Liouville 이론은 q의 부호를 요구하지 않는다(뒤에서 언급하는 Legendre 방정식도 $q \equiv 0$이다). $q > 0$을 요구하면 정리의 적용 범위가 부당하게 좁아진다)

제22권 제1–2장

- **원본 639쪽 1.5절** 불편 표본분산을 플러그인 값에 ‘‘편향 보정을 더한 것”이라고 한 서술을 $n/(n-1)$을 곱하여 보정한 것으로 바로잡음 (불편 표본분산은 플러그인 분산에 $n/(n-1)$을 곱한 값이며 보정은 덧셈이 아니라 곱셈이다(예제 1.10에서 $2.25 \cdot 4/3 = 3$))

제22권 제3–4장

- **원본 647쪽 정리 3.9 (Rao–Blackwell)** 평균제곱오차가 어느 추정대상에 대한 것인지 밝히지 않았으므로 추정대상 $g(\theta)$를 정리 진술에 명시하고 $\mathrm{MSE}_\theta(W) = \mathbb{E}_\theta[(W - g(\theta))^2]$로 정의함 (증명에는 상수 $g(\theta)$가 등장하지만 진술에는 정의가 없어 MSE의 기준이 불명확했음)
- **원본 647쪽 정리 3.9 증명 및 648쪽 Lehmann–Scheffé 진술** 교차항이 사라지는 이유(조건부 기댓값 $\mathbb{E}[U - V \mid T] = 0$)와 유한 분산 조건을 명시함 (원본의 직교 분해는 V의 제곱적분가능성과 교차항 소거를 가정 없이 사용함)

제28권 제2장

- **원본 671쪽 예제 2.4** z=e^{2\pi i/N}일 때 합이 0이라는 진술에 N 이상 2라는 가정을 보충함 (N=1이면 z=1이고 합이 1이므로 원래 진술이 성립하지 않음)

제28권 제4장

- **원본 685쪽 예제 4.9** 정육면체 표면(면이 사각형)에 대해 삼각분할로 정의한 Euler 특성을 그대로 적용한 서술을 바로잡고, 다각형 분할에서도 성립함을 밝히며 각 면에 대각선을 그어 삼각분할한 경우 V=8, E=18, F=12로 8-18+12=2임을 검산으로 추가 (Euler 특성을 삼각분할로 정의했는데 정육면체의 분할은 삼각분할이 아니므로 정의의 범위를 벗어난 적용이었음)

제28권 제6장

- **원본 695쪽 6.4절 ($0^{-1} = 0$ 관례 문단)** ‘‘$x/x = 1$을 아무 가정 없이 증명할 수 있다는 뜻이 아니다” 라는 진술에 이유를 보강하여, 이 관례에서는 $0/0 = 0$이므로 $x = 0$에서 $x/x = 1$이 오히려 거짓임을 명시함 (원문은 결론만 있고 가정 없는 명제가 증명 불가능한 이유가 빠져 있어 부정확하게 읽힘)
- **원본 697쪽 6.10절 (공통점 r에서 $f(r) = 0$)** ‘‘연속성으로 $f(r) = 0$”에 빠진 단계를 채워 $f(r) = \lim f(a_n) \le 0$, $f(r) = \lim f(b_n) \ge 0$으로 보임 (부호 조건은 유한 단계에서 엄격 부등식이고 극한에서는 비엄격 부등식이므로 두 방향 부등식을 모두 쓰지 않으면 $f(r) = 0$이 따라오지 않음)
- **원본 696쪽 명제 6.6의 증명** 근이 열린구간 (a, b) 안에 있음($f(a), f(b) \neq 0$)과 Rolle 정리의 적용 조건(닫힌구간 $[c, d]$에서 연속, 열린구간에서 미분가능)을 명시함 (명제는 (a, b)에 정확히 하나의 근이 있다고 주장하므로 중간값정리로 얻은 근이 끝점이 아님을 보여야 함)

찾아보기

기호

(스칼라) 선적분 385
(Lebesgue) 영집합 379
(Riemann) 적분가능 379
ℓ^p 505
σ-대수 406, 636
σ-유한 418
C^1 함수 368
C^k 함수 371
d-정규 630
F 분포 668, 675
k 색칠 196
L^p 수렴 698
m위 극 459
n제곱근 61
p-진 절댓값 803
p 진 정수환 603
p 진 지수 602
t 분포 668

A

Abel 공식 480

B

Banach 공간 505
Bayes 결정 783
Bayes 인자 786
Benjamini–Hochberg 절차 779
Bernoulli 방정식 475
Bernoulli 변수 668
Bernoulli 분포 668
Bessel 부등식 304, 510
BIBO 안정 490
Bode 선도 490
Borel σ-대수 406
Borel 집합 653
Bromwich 적분 489
Brown 운동 819

C

Cantor 집합 400
Cantor 함수 429
Carathéodory 확장정리 408
Carleson 정리 511
Carmichael 수 578
Cauchy 분포 675
Cauchy 수열 351
Cauchy 점열 363
Cauchy 주값 347
Céa 보조정리 535
Chebyshev 부등식 710
Chernoff 방법 711
Cramer 공식 82
Cramér 이론 714

D

de Rham 코호몰로지 395
Dedekind 정역 599
Devaney의 정의 501
Dirac 델타 489
Dirac 측도 407
Dirichlet 다항식 797
Dirichlet 문자 803
Dirichlet 원리 535
Dirichlet 정리 511
Dirichlet 합성곱 585
Dirichlet 핵 514
Duhamel 공식 485

E

Euclid 정역 557
Euler 곱 587
Euler 공식 442
Euler 트레일 623
Euler 특성 813
Euler 함수 576
Euler 회로 623
Euler–Maruyama 근사 750

F

Faber 정리 514
Feigenbaum 상수 500
Fisher 정보량 760
Floquet 이론 485
Fourier 계수 797
Fourier 변환 531
Fréchet 미분 368

G

Galois 군 571
Galois 확대 571
Gauss 소거 252
Gibbs 현상 511, 528
Glivenko–Cantelli 정리 756
Gram–Schmidt 과정 511

H

Hall 조건 630
Hausdorff 차원 812
Hausdorff 측도 812
Heaviside 함수 533
Hecke 작용 804
Hermite 다항식 511
Hermitian 308
Hessian 행렬 371
Hilbert 공간 509
Householder 반사 310

I

Itô 과정 748
Itô 적분 745

J

Jacobi 기호 582
Jacobi 행렬 367
Jordan 블록 298, 485, 564
Jordan 표준형 298, 564

K

Kakeya 집합 812
Kolmogorov 확장정리 719

L

Laplace 방정식 522
Laplace 변환 488, 692
Lax 동치정리 515
Lebesgue 가측 407
Lebesgue 상수 514
Lebesgue 외측도 407
Lebesgue 점 427
Lebesgue 측도 408
Lebesgue–Stieltjes 측도 430
Legendre 기호 579
Legendre 다항식 511
Lerch 정리 489
Lipschitz 477
Lyapunov 지수 500

M

Maclaurin 다항식 355
Markov 부등식 710, 797
Minkowski 상수 600
Minkowski 차원 812
MLE 763
Möbius 변환 468
Möbius 함수 584
Moore–Penrose 의사역행렬 311

N

n제곱근 44
Neumann 급수 507

Newton 방법 331
Noether 성질 558

P

Pell 방정식 591
Picard 반복 478
Plancherel 정리 531
Poisson 분포 668, 670
Poisson 핵 470, 531
Poisson binomial 분포 668
profile 우도 765

R

Radon–Nikodym 도함수 431
Rankine–Hugoniot 조건 523
rate 672
Rayleigh 밀도 684
Riccati 방정식 475
Riemann 구면 434
Riemann zeta 함수 587
Riesz 보조정리 507
Routh–Hurwitz 판정법 486
Runge 현상 514

S

SAT 192
scale 672
Simpson 역설 651
Smith 표준형 563
Sobolev 공간 533
Student의 t 분포 675
Sturm–Liouville 이론 526
Sylow p-부분군 551

T

Taylor 다항식 355
Tseitin 변환 145

V

Vandermonde 항등식 645
Vieta 공식 86
von Mangoldt 함수 584, 796

W

Wald 구간 771
Weierstrass 함수 514
Wilson 점수 구간 772
Wirtinger 미분 437
Wronski 행렬식 480

ㄱ

가군 561, 562
가능도 649
가능도비 649
가법 에너지 798
가분 511
가산 235, 636
가산 가법성 407
가산 무한 235
가산가법성 637
가역 279, 724
가정 규칙 161
가족별 오류율 778
가측 410
가측 직사각형 417
가측공간 406
가측성 653
가해군 572
가환군 538
가환환 553
간선 621
갈퀴 분기 497
갈퀴 분기(아임계) 497
감김수 452
감마분포 668, 672
감마함수 672
감소수열 39
감쇠 진동수 481
값 630
강제적 534
강한 귀납법 170

강한 일관성 759
강한 Huygens 원리 524
거듭제곱 43
거듭제곱근으로 풀린다 572
거듭제곱급수 354
거리 31, 362
거의 모든 곳 408
거의 확실 639
거의 확실한 수렴 698
거짓 발견율 778
건전성 242
검산 6
검정력 함수 775
검정함수 775
검토된 수학적 결과 791
격자 188
결합 특성함수 693
결합법칙 5
결합분포 681
결합분포함수 681
결합질량 681
경계 363
경계값 문제 473
경로독립 386
경로연결 365
경우분석 150
경험분포함수 755
계 473
계산 가능하게 열거되는 공리계 244
계수 83, 274, 563
계수법 641
고립특이점 459
고유값 293
고유공간 293
고유벡터 293
고유변수 164
고유진동수 481
고전적 귀류 규칙 163
고정점 375, 499
고차 범주 813
곡선 447
곡선의 길이 447
곱 σ-대수 417
곱셈적 584
곱셈적 함수 576
곱의 법칙 609, 641
공개된 증명 원고 791
공리꼴 218
공배수 13
공분산 659, 661
공분산 행렬 682
공약수 10
공역 103
공진 주파수 481
공집합 218
공허한 참 139
관성 599
관성모멘트 382
교대 경로 629
교대군 542
교대성 286
교란순열 644
교차비 468
교환법칙 5
구문적으로 완전 242
구별불가능 719
구조 156
구조적 귀납 143, 171
국소계 805
국소극값점 327
국소최대점 327
국소최소점 327
군 538
군속도 532
궤도 492, 549, 615
귀납 가정 168
귀납적 정의 143
귀납적 집합 220

귀류법 149
균등분포 668
균등수렴 402, 790
균등연속 365
균등적분가능 701
균등적분가능성 416
그래디언트 368
그래프 104, 180, 196
극대 매칭 629
극대 아이디얼 554
극대원소 187
극소원소 187
극좌표 131
극한 315
극한(수열) 39
극한주기 495
극형식 60
근접 성질(상한) 36
근판정 353
급수 352
기댓값 659
기본 행 연산 251
기본인자 형태 563
기본해 530, 591
기본행렬 485, 728
기수 235
기약 77, 723
기약 행 사다리꼴 252
기약분수 23
기약원 557
기저 265, 266, 562
기하분포 668, 669
기하적 중복도 296
긴반지름 126
깊이 200
꼬임 원소 562
꼭짓점 196, 621
꼭짓점 (이차곡선) 125

ㄴ

나눈다(약수 관계) 10
나머지 9
나무 622
나선 485
내부 363
내적 107, 302, 509
넓이 380
노름 302, 362, 505, 591, 597
논리곱 137, 142
논리곱 정규형 145
논리식 142, 155
논리적 귀결 144, 158
논리적으로 동치 143
논리합 137, 142
논리합 정규형 145
누적분포함수 653, 654
누적생성함수 696

ㄷ

다변량 정규벡터 682
다중집합 611
다항계수 643
다항식 73
단면 417
단사 104, 180, 273
단사(함수의 성질) 103
단순 경로 622
단순 닫힌 곡선 447
단순 무향 그래프 621
단순군 547
단순연결 387
단순함수 410
단원 553, 597
단위 16
단위 전파 194
단위원 111, 225
단위절 194
단조수렴 정리 40
단조수열 39

닫혀 810
닫혀 있음 538
닫혔다 723
닫힌 곡선 447
닫힌 형식 395
닫힌집합 363
닮음 119, 282
당김 394
대각관계 175
대각선 논증 184
대각합 283, 533, 597
대각화 293
대각화 가능 295
대수적 567
대수적 정수 596
대수적 중복도 296
대우 149
대칭 262, 527
대칭성 520
대칭적 176
대칭차 636
대칭행렬 308
도 110
도달시간 726
도입 규칙 162
도함수 321
독립 243, 649, 657
독립 동일분포 표본 754
독립 증분 720
동등연속 404
동반행렬 564
동질 Poisson 과정 731
동차계 254
동차방정식 480
동차형 475
동치 137
동치관계 176
동치류 176, 225, 423
동형사상 275, 544
동형정리 544
두 배 각 공식 114
등각동형 468
등각사상 468
등각성 436
등거리변환 119
등경사선 473
디오판토스 방정식 13

ㄹ

라디안 110
로그 46, 443
로그우도 763
로그정규변수 674
류 방정식 551
리만적분 334
리만적분가능 335
리만합 334
리터럴 145

ㅁ

마팅게일 735
망 크기 334
망원경 합 66
매개곡선 385
매개변수 70
매개변수 변화법 481
매장 226
매칭 629
멱 123
멱급수 440
멱등함수 207
멱영 279
면 626
면적분 387
명제 137
명제 변수 142
명제논리 142
명제적 같음 824
모노드로미 805

모듈러 형식 804
모멘트 닫힘 문제 819
모수 753
모수공간 753
모수모형 753
모집단 754
모형 158
모형론 157
몫 9
몫군 544
몫집합 178
무게중심 109
무리방정식 88
무리수 34
무제한 내포 원리 214
무한 경로 200
무한원점 434
묶인 변수 64
문자 803
문장 156
미분가능 321, 367
미분계수 321
미분방정식 473
미분형식 393
미정계수법 481
밑 변환 공식 47
밑(거듭제곱) 43
밑(기수법) 3
밑(로그) 46

ㅂ

반각 공식 115
반대 리터럴 192
반대칭 262
반대칭적 176
반례 152
반사슬 188
반사적 176
반평가 144
발산 389
발산(수열) 39
방해모수 753
방향미분 367
방향장 473
배수 10
배음 527
백분율 25
버전 687
범주 805
법 54
베주 계수 12
베타분포 668, 673
베타함수 673
벡터 107
벡터공간 258
변 196
변곡점 330
변분방정식 479
변수 70
변수분리법 526
변수분리형 474
변환함수 692
별과 막대 643
별모양 387
별모양 영역 451
보존장 386
보편성 500
보행 622
복소 거듭제곱 444
복소 선적분 447
복소미분가능 434
복소미분계수 434
복소수 2, 58
복원추출 642
복잡도 142
볼록 330
볼록함수 373
부동소수점 52
부분 정확성 172

부분 평가 194
부분 피벗팅 255
부분공간 260
부분군 539
부분마팅게일 735
부분몫 589
부분수열 351
부분순서 186
부분순서 집합 186
부분집합 213
부분합 공식 799
부적절 사전 786
부정 142
부정형 317
부피 380
부호 542
부호표 91
분기 495, 599, 600
분기점 497
분리 공리꼴 214
분리 정리 513
분리가능 571
분리선 493
분모 23
분배법칙 5
분산 659, 661
분산관계 532
분수 23
분수체 553
분위수 656
분위수함수 653
분자 23
분지 443
분지절단 443
분포 533, 653
분포수렴 698
분할 176, 334
분해 599
분해체 568
불변량 792
불변식 172
불변인자 형태 563
불변조건 828
불안정 473
불편추정량 758
비가산 235
비동질 Poisson 과정 734
비동차계 254
비례 25
비복원추출 642
비분산 532
비선형 473
비아르키메데스적 602
비율 25
비주기적 723
빈 절 145

ㅅ

사건 635
사슬 188
사인 111, 442
사전민감도 분석 786
사전밀도 781
사전확률 649
사후기대손실 783
사후밀도 781
사후예측 점검 786
사후예측분포 785
사후확률 649
산술함수 584
삼각부등식 118
상 180, 271, 273
상계 35, 95, 187
상관계수 661
상대엔트로피 714
상대오차 50
상미분방정식 473
상세평형 724
상수 70

상용로그 47
상한 35, 187
상한 공리 36
상합 379
상호독립 650
색칠수 626
생성공간 261
생성하는 부분군 540
서로 배반 636
서로소 13, 542
서수 238
선도성분 252
선속 388
선택공리 242
선형 473
선형독립 265
선형범함수 275
선형사상 271
선형종속 265
선형함수 275
선형화 행렬 492
섬유 179, 180, 609
세분 334
셈측도 407
소 아이디얼 554
소수 16
소원 557
소통류 723
속도함수 714
속박 156
속아내기 733
수 2
수렴 346, 350, 363
수렴(수열) 39
수렴반지름 354, 440
수렴분수 590
수렴원판 440
수반 518
수반행렬 289
수열 38
수정 719
수직 107
수체 596
수축 가능 808
순서 30
순서동형 188
순서매장 188
순서보존 188
순서쌍 215
순서체 227
순수 리터럴 194
순열 610, 641
순환 542, 622
순환 그래프 626
순환 부분군 540
순환군 540
순환마디 26
순환소수 26
순환형 542
숫자 2
숲 622
스콜렘 역설 246
스펙트럼 517
스펙트럼반지름 517
시간동질 Markov 연쇄 722
시컨트 113
시퀀트 164
시험함수 533
식별가능 754
신뢰구간 769
신용구간 784
신용집합 784
신장 나무 623
실수 2
실수부 58
십진법 3
쌍곡 평형점 492
쌍곡선 127

쌍곡선함수 130, 442
쌍곡형 522
쌍대공간 506
쌍대군 805
쌍대수 환 811
쌍별독립 650
쌍조건문 142
쐐기곱 393

ㅇ

아래로 유계 35
아래합 334
아르키메데스 성질 38
아이디얼 553, 554
아핀 부분공간 262
아핀 사상 271
안장-마디 분기 497
안장점 485
안정 473, 486
안정 극한주기 495
안정 다양체 485
안정성 53
안정자 549
안정자군 615
알파 이름변경 156
약미분 533
약분 23
약수 10
약수렴 817
약정상과정 720
약해 523, 533, 534
양의 정부호 309, 694
양화사 136
엄격 정상과정 720
에라토스테네스의 체 20
엔트로피 조건 523
여과 720, 735
여인수 288
역 149
역관계 175
역방향 용량 631
역삼각함수 116
역상 180
역수 227
역원 5, 55
역함수 104, 182
연결 성분 622
연결사 142
연립방정식 82
연분수 589
연산 순서 6
연속 318, 365
연속 균등분포 671
연속 소수의 간격 795
연속 스펙트럼 517
연속시간 718
연속체 가설 239
연쇄법칙 648
열린 공 363
열린 식 136
열린집합 363
열방정식 522
열벡터 251
영공간 83
영역 434
영원소 225
영인자 226, 553
영집합 408
영차원 274
영향 영역 524
오른쪽 역 182, 280
오즈 649
완비 364, 767
완비격자 188
완비성 36, 227, 510
완비성 공리 36
완전 곱셈적 584
완전 곱셈적 함수 576
완전 그래프 621

완전 이분 그래프 627
완전 형식 395
완전방정식 475
완전수 586
완전순열 614
완전집합 400
외미분 394
외연성 213
왼쪽 역 182, 280
용량 630
우극한 316
우도 781
우도비 763, 777
우도함수 763
원분다항식 559
원상 105
원소 관계 213
원시근 560, 576
원시다항식 559
원시함수 338, 448
원자식 155
원주각 122
위로 유계 35
위상선 474
위상속도 532
위수 538, 540, 576
위치적 기수법 3
위합 334
유계 35, 505, 534
유계변동 428
유계수렴정리 414
유계역정리 514
유니터리 309
유도부분그래프 196
유리 지수 45
유리 표준형 564
유리방정식 88
유리수 2, 23, 227
유리식 79
유리형 함수 460
유수 461, 600
유의수준 775
유일성 139
유일인수분해정역 558
유클리드 노름 362
유클리드 알고리즘 11
유한 235
유한 계수 작용소 519
유한 균등모형 641
유한 전파 속도 524
유한 충족가능 199
유한 확대 566
유한생성 562
유한소수 25
유한요소법 535
유한차원 분포 719
유효숫자 50
유효한 p값 777
음이항분포 668, 669
의미론적 귀결 161
의미론적 완전성 242
의존 영역 524
이계 편미분 371
이계도함수 325
이계도함수 판정 330
이데알류군 599, 600
이력현상 498
이분 그래프 625
이분법 319, 828
이산로그 577
이산시간 718
이산형 654
이상 끌개 501
이상 중적분 382
이상적분 342, 346
이심률 132
이완 진동 496
이중 계수 611

이진 나무 200
이진법 3
이차 무리수 591
이차변동 744
이차비잉여 579
이차잉여 579
이항계수 610
이항관계 175
이항분포 668
이항정리 611
인접행렬 622
인증서 826
일가성 공리 813
일관성 719
일관적 242
일관추정량 759
일차 언어 155
일차방정식 81, 250
임계 노름 818
임계점 372
임펄스 응답 490
입체사영 434
잉여 스펙트럼 517
잎 622

ㅈ

자기수반 308, 518
자기수반성 520
자명한 부분공간 260
자연 여과 720
자연로그 47
자연수 2
자연스러운 정의역 70
자연연역 161
자유가군 562
자유변수 156, 254
자율계 492
자율방정식 473
작도가능수 567
작용 549, 614
작용소 노름 506
잔여 네트워크 631
잘 정립된 522
잘 정의되어 151
재규격화 820
재매개화 385
적률생성함수 668, 675, 692
적분가능 412, 659
적분인자 474
적응 735
적절한 꼭짓점 색칠 626
적합 720
전건 긍정 162
전단사 104, 180
전달함수 490
전변동 428
전사 104, 180, 273
전순서 186
전술 824
전역최대점 327
전역최소점 327
전이행렬 722
전체 정확성 172
전칭 136
전해석함수 434
절 145
절단 229, 631
절대수렴 347
절대연속 427, 430, 431, 655
절대오차 50
절댓값 31, 59
점 107
점 스펙트럼 517
점근선 127
점근안정 486
점별수렴 402, 790
점수함수 760
점유 벡터 643
접선 121, 321

접평면 369
정규 모드 486
정규부분군 545
정규부분군(역사적 용례) 539
정규분포 668, 673
정규직교기저 304, 511
정규직교집합 304
정규화 528
정렬 정리 242
정렬순서 188
정밀도 783
정방향 용량 631
정보 σ-대수 687
정상 증분 720
정상분포 723
정상상태 527
정수 2, 225
정수 기저 597
정역 226, 553
정의역 103, 156
정의적 같음 824
정의적 CNF 변환 193
정적분 334
정지시간 737
정칙 385
정칙 매개곡면 387
정칙 특이점 482
정칙 함수 434
정칙 Sturm–Liouville 문제 527
정칙값 376
정칙성 408
정칙성 이론 535
정칙점 482
정확 이항구간 772
정확한 810
제1종 오류 775
제2종 오류 775
제거 가능한 불연속점 316
제거 규칙 162
제거가능 특이점 459
제곱근 44
제한된 양화사 218
조건 53
조건문 137, 142
조건부 기댓값 687
조건부 독립 650
조건부 정리 826
조건부 확률 647
조건수 53
조건수렴 347
조밀(조밀성) 38
조밀하다 227
조합 610, 642
조화함수 391, 437, 530
존재 136
종료 척도 172
좌극한 316
좌잉여류 541
좌표 266
좌표계 107
주값 44, 116
주기 111, 723
주기 k인 점 499
주기 창 500
주기배가 분기 500
주로그 443
주변 자료밀도 781
주변질량 681
주분지 444
주아이디얼 554
주아이디얼정역 557
주요부 458
주파수 응답 490
주편각 60, 443
준동형사상 544
준선 125
준순서 186
준정규 변수 712

중근 85
중복도 86
중복조합 610, 643
중심 (이차곡선) 126
중심각 122
중심화군 549
증가수열 39
증대 경로 629
증명 보조기 823
증명 판단 161
증인 138
지수 43
지수 법칙 43
지수 차수 488
지수분포 668, 672
지수생성함수 619
지수적 기울임 696
지수함수 45, 442
지시함수 380
지원집합 681
지표 541
지표방정식 482
직관주의 논리 163
직교여공간 305
직교집합 304
직교투영 306
직교행렬 309
직접곱군 547
직합 262
진부분공간 260
진성 특이점 459
진수 46
진술 136
진클래스 215
질량 382
질량중심 382
집적점 315
집합 상계 638
짝함수 105
짧은반지름 126

ㅊ

차수 73, 566, 621
차원 265, 268
첫 귀환시간 726
체 553
초기값 문제 473
초기값 정리 490
초기하분포 644, 668, 670
초른 보조정리 242
초마팅게일 735
초월임계 분기 497
초월적 567
초점 125
초평면 275
총변동 744
최대 매칭 629
최대공약수 10
최대우도추정값 763
최대우도추정량 763
최대원소 187
최대하계 35
최댓값 35, 95
최선 근사 591
최소공배수 13
최소다항식 567
최소상계 35, 187
최소원소 187
최소제곱 307
최소제곱법 510
최솟값 35
최종값 정리 490
추이적 176, 238
추정값 755
추정대상 753
추정량 755
추측 791
축 (포물선) 125
축약 QR 분해 305

축약사상 원리 507
축척인자 391
충격파 523
충분조건 137
충분통계량 765
충족가능하다 143
충족불가능하다 143
측도 407
측도공간 407
치역 103
치환 220

ㅋ

카이제곱분포 668, 674
칸토어 짝짓기 함수 236
커널 825
켤레 59
켤레류 549
켤레성 782
켤레전치 283
켤레조화함수 437
켤레지수 423
코사인 111, 442
코시 수열 40
코시컨트 113
코탄젠트 113
콤팩트 364
콤팩트 작용소 519
콤팩트성 199
크기 775
큰 값 추정 797
큰편차 원리 715
클래스 215

ㅌ

타당하다 143
타원 126
타원형 522
타원형 정칙성 535
탄젠트 113
통계량 755
통계모형 753
퇴화 이차곡선 129
트레일 622
특성곡선 522, 523
특성다항식 294
특성방정식 480
특성함수 668, 677, 692
특이 Sturm–Liouville 문제 528
특이값 310

ㅍ

파국적 상쇄 52
파동방정식 522
판별식 85, 597
판별식 (이차곡선) 129
퍼센트포인트 25
페르마 유사소수 56
편각 60
편각 원리 465
편미분 367
편미분방정식 473, 522
편향 758
평가 143
평균값 성질 454
평균벡터 682
평균제곱오차 758
평면 그래프 626
평형점 492
평형해 473
평활화 효과 526
폐포 363
포물선 125
포물형 522
포섭 192
포함확률 769
포화 629
포획 158
포획 없는 치환 158
표본 754

표본경로 718
표본공간 635
표본분포 755
표수 555
표준 몫사상 178
표준 Brownian 운동 742
표준분해 18
표준정규분포 673
표준편차 661
표현 802
플러그인 원리 755
피벗 252, 769
피벗 변수 254
피보나치 수열 171
피타고라스 항등식 111
필요조건 137

ㅎ

하강계승 642
하계 35, 187
하한 35, 187
하합 379
할당 156
함수 103
함수해석학 505
합동 54, 119
합성 175
합성곱 489
합성수 16
합성열 547
합성함수 105
합의 법칙 609
항 155
항등식 71
항등원 5
항등행렬 279
항진 절 192
해 250
해결 결과 194
해결 규칙 145, 194
해석적 358
해석적 함수 445
해집합 517
핵 271, 273
행 사다리꼴 252
행렬 251
행렬식 285
행렬표현 277
향할 수 있는 곡면 387
허수부 58
형식 증명 791
형식적 멱급수 618
호모토피 808
호모토피 동치 808
호모토피 유형론 813
호모토픽 451
호몰로지 809
호의 길이 385
호환 542
혼돈적 501
홀함수 105
확대 566
확대행렬 251
확률공간 635
확률과정 718
확률밀도함수 653, 655
확률벡터 681
확률변수 653
확률생성함수 668, 675, 692
확률수렴 698
확률질량함수 653, 654
확률측도 407, 635
확장된 복소평면 434
확장된 실수 398
환 553
환(다음 장) 552
회전 389
후건 긍정의 오류 137
후속자 219, 223, 238

후진대입 252
흐름 630
흡수 연쇄 728
흡수상태 727