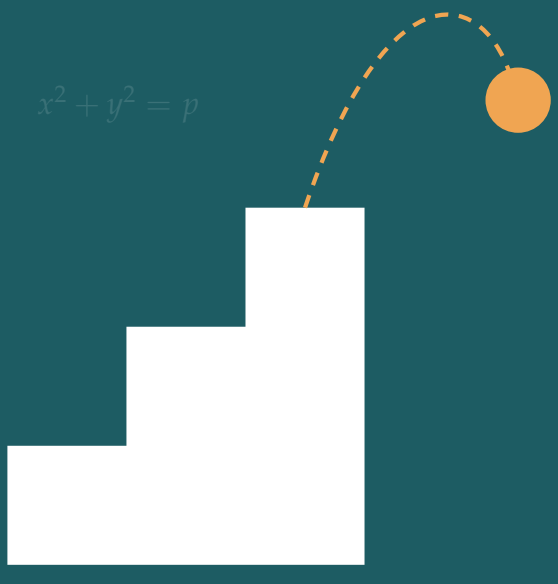
STEP 대비 · 대학 수학

Beyond STEP

제6장

대수와 구조



KEITH McNULTY

Beyond STEP

STEP 기출문제로 여는
대학 수학의 세계

제6장

대수와 구조

Keith McNulty

Beyond STEP: STEP 기출문제로 여는 대학 수학의 세계

제6장: 대수와 구조

이 PDF는 *Beyond STEP*의 전체 13개 장 가운데 제6장이다. 책 전체, 각 장의 개별 PDF, 모든 절의 인쇄용 연습지, 모든 STEP 문제의 자세한 풀이를 `beyondstep.keithmcnulty.org`에서 무료로 읽고 내려받을 수 있다.

2026년 11월 온라인 초판 발행.

이 PDF에서 지은이가 직접 만든 모든 것, 곧 본문, 풀이, 그림, 연습문제와 해답은 크리에이티브 커먼즈 CC0 1.0 Universal 라이선스에 따라 퍼블릭 도메인(public domain)으로 공개한다. 누구든 허락을 구하지 않고 어떤 목적으로든 복사하고, 고쳐 쓰고, 공유할 수 있다. 자세한 내용은 `creativecommons.org/publicdomain/zero/1.0`을 보라.

여기에서 다루는 STEP 문제의 저작권은 Cambridge University Press & Assessment에 있다. 문제는 이 책에 싣지 않았으며, 각 문제마다 공식 출처인 STEP Support Programme의 문제 데이터베이스나 OCR의 기출 시험지로 가는 링크를 달았다.

오류 제보는 `github.com/keithmcnulty/step_book_mcnulty`에 이슈로 남겨 주기 바란다.

장

6

대수와 구조

대수학의 모든 기발한 요령 뒤에는 구조가 있으며, 그 구조를 이해하는 것은 요령을 아무리 많이 아는 것보다 값지다.

이 장의 내용

6.1 근이 모두 단위근인 다항식 STEP III 2010

6.2 가우스의 정17각형 STEP II 1991

6.3 $\sqrt{2}+\sqrt{3}+\sqrt{5}$를 근으로 갖는 다항식 STEP II 2023

6.4 사차방정식 풀기 STEP III 2017

6.5 공리에서 출발하는 미분 STEP II 1992

6.6 부분군의 합집합 STEP II 1988

6.7 사원수군 STEP III 1993

6.8 특이행렬로 이루어진 군 STEP III 1996

A 연습문제 해답 59쪽

방정식에서 구조로

> 수학은 서로 다른 것에 같은 이름을 붙이는 기술이다.
>
> — 앙리 푸앵카레(Henri Poincaré)

역사의 대부분 동안 대수학(algebra)은 방정식을 푸는 일을 뜻했다. 바빌로니아인은 4000년 전에 이차방정식(quadratic equation)을 풀었고, 16세기 이탈리아 수학자들은 삼차방정식(cubic equation)과 사차방정식(quartic equation)을 풀었다. 그러고 나서 거의 300년 동안 오차방정식(quintic equation)은 모든 시도를 견뎌 냈다. 1820년대와 1830년대에 마침내 해결이 이루어졌을 때, 대수학은 완전히 바뀌었다. 닐스 헨리크 아벨(Niels Henrik Abel)은 오차방정식의 일반적인 근의 공식이 존재하지 않음을 증명했고, 에바리스트 갈루아(Évariste Galois)는 어떤 방정식을 풀 수 있는지를 정확히 설명했는데, 방정식 자체가 아니라 **근**(*root*)**의 대칭**(*symmetry*)을 연구함으로써 그렇게 했다. 이를 위해 그는 새로운 종류의 수학적 대상, 곧 군(group)을 고안해야 했다.

답을 계산하는 것에서 구조를 연구하는 것으로의 이 전환이 바로 이 장의 주제이다. 현대 대수학은 "해가 무엇인가?"라고 묻는 대신 "이것은 어떤 종류의 대상이며, 어떤 연산을 허용하는가?"라고 묻는다. 그 답은 옛 요령들이 왜 통했는지를 설명해 주고, 요령만으로는 결코 해결할 수 없었던 문제들을 매듭짓는다.

구조가 왜 중요한가

2000년 동안 모든 시도를 견뎌 낸 세 가지 고대 문제가 있다. 자와 컴퍼스(ruler and compasses)만으로 정육면체의 부피를 두 배로 늘리는 것, 임의의 각을 삼등분하는 것, 정7각형을 작도(construction)하는 것이다. 이 가운데 어느 것도 불가능하며, 19세기에 발견된 그 증명은 기발한 작도가 아니라 구조에 관한 논증이다. 곧 자와 컴퍼스로 도달할 수 있는 수들이 이루는 체(field)의 **차수**(*degree*)에 관한 논증이다(Section 6.3). 같은 이론으로 정17각형은 왜 **작도할 수 있는지**(Section 6.2), 그리고 사차방정식은 풀 수 있지만 오차방정식은 왜 풀 수 없는지(Section 6.4)도 설명된다.

구조는 또한 여러 곳으로 옮겨 간다. 결정(crystal)의 대칭, 다항식의 근들의 치환(permutation), 3차원 공간의 회전, 루빅스 큐브의 움직임, 타원곡선(elliptic curve) 위의 점들은 모두 군의 공리(axiom)를 만족한다. 공리로부터 한 번 증명한 정리는 이 모두에서 성립한다. 푸앵카레의 말처럼 "서로 다른 것에 같은 이름을 붙이는" 이 경제성이야말로 추상대수학(abstract algebra)을 그토록 강력하게 만드는 것이다.

대학에서 만나게 될 것

1학년 때는 **군**(세 가지 공리를 만족하는 연산이 주어진 집합)을 만나고, 대개 **환**(*ring*)과 **체**(덧셈과 곱셈이 주어진 집합)도 만난다. 부분군(subgroup)의 크기가 군의 크기를 나눈다는 라그랑주(Lagrange) 정리를 증명하고, 치환, 대칭군(symmetry group), 행렬군(matrix group)을 만난다. 2학년과 3학년에는 이것들이 체와 군을 연결하고 방정식과 작도에 관한 고전적인 질문에 답하는 **갈루아 이론**(*Galois theory*), 행렬을 통해 군을 연구하는 **표현론**(*representation theory*), 그리고 Section 1.7의 아이디어를 튼튼한 기반 위에 세우는 **대수적 정수론**(*algebraic number theory*)으로 이어진다. 이 장의 마지막 세 절은 군에 관한 것이다. 군은 더 이상 STEP 출제 범위(syllabus)에 포함되지 않지만(2019년에 빠졌다), 문제들은 그 자체로 완결되어 있으며 각 절에서 필요한 정의를 제시한다.

이 장을 관통하는 질문들

세 가지 큰 질문

1. **무엇으로부터 무엇을 만들 수 있는가?** 유리수(rational number)로부터 제곱근을 취하거나 방정식을 풀어서 어떤 수에 도달할 수 있으며, 어떤 수에 도달할 수 없다는 것은 어떻게 증명하는가?
2. **방정식의 근의 공식은 왜 성립하는가?** 이차, 삼차, 사차방정식에 근의 공식이 있는 숨은 이유는 무엇이며, 오차가 되면 무엇이 달라지는가?
3. **추상화로 무엇을 얻는가?** 대상을 그것이 따르는 규칙만으로 기술하면 어떤 일이 일어나는가?

이 장의 아이디어

§	주제	아이디어
6.1	원분다항식(cyclotomic polynomial)	1의 거듭제곱근(root of unity)을 위수(order)에 따라 분류한다
6.2	정17각형	가우스(Gauss) 주기: 합과 곱이 이차방정식을 준다
6.3	최소다항식(minimal polynomial)	거듭제곱근(radical)을 소거한다; 차수는 곱해진다
6.4	사차방정식 풀기	대칭함수(symmetric function); 분해삼차식(resolvent cubic)
6.5	공리로부터 출발하는 미분(differentiation)	규칙에 의해 결정되는 연산
6.6	부분군의 합집합	군의 공리로부터 논증하기
6.7	사원수군(quaternion group)	연산을 행렬로 표현하기
6.8	특이행렬(singular matrix)로 이루어진 군	정의를 문자 그대로 읽기

이 장을 읽는 방법

이 문제들 중 상당수는 힘으로 밀어붙이는 계산(brute force)으로 풀 수 있다. 모든 것을 전개하고, 계수를 비교하고, 모든 경우를 확인하는 것이다. 필요하다면 먼저 그렇게 하라. 그런 다음 돌아보며, 무엇 덕분에 그 계산이 통했는지, 그리고 그 뒤에 구조적인 이유가 있는지 물어보라. 구조적인 이유는 대개 더 짧고, 언제나 더 많은 것을 밝혀 주며, 힘으로 밀어붙이는 계산이 불가능해질 때 필요한 것이 바로 그것이다.

6.1 근이 모두 단위근인 다항식

문제

STEP III 2010, 3번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:

`step.maths.org/questions/10-s3-q3`

도입

n차 단위근(roots of unity), 즉 $z^n = 1$의 해는 정n각형의 꼭짓점에 놓인다. 그러나 이들이 모두 같은 성격인 것은 아니다. 예를 들어 12차 단위근 가운데 1은 이미 1차 단위근이고, -1은 2차 단위근이며, i는 4차 단위근이다. 열두 개 가운데 **원시**(*primitive*) 단위근인 네 개만이 열두 걸음을 모두 거쳐야 1로 돌아온다.

단위근을 필요한 걸음 수에 따라 분류하고 각 부류마다 다항식을 하나씩 만들면 **원분다항식**(*cyclotomic polynomials*)을 얻는다(그리스어로 "원을 나눈다"는 뜻이다). 소수가 자연수를 이루는 기본 구성 요소이듯이 원분다항식은 $z^n - 1$을 이루는 기본 구성 요소이며, 가우스(Gauss)의 정17각형 작도(Section 6.2), 단위근 필터(Section 5.2), 그리고 현대 정수론의 많은 부분의 바탕에 놓여 있다.

시작하기 전에

생각해 보기 모든 n차 단위근은 $z^n = 1$을 만족한다. 그러나 1이 되는 가장 작은 양의 거듭제곱 지수는 n보다 작을 수도 있다. 네 개의 4차 단위근 1, i, -1, $-\mathrm{i}$ 각각에 대하여 그 가장 작은 지수는 무엇인가?

$1^1 = 1$, $(-1)^2 = 1$이고, $\mathrm{i}^4 = (-\mathrm{i})^4 = 1$이며 이보다 작은 지수로는 성립하지 않는다. 따라서 가장 작은 지수는 각각 1, 4, 2, 4이다. 이 가장 작은 지수를 단위근의 **위수**(*order*)라 하며, 원시 n차 단위근은 바로 위수가 n인 단위근이다. 이 문제 전체의 핵심이 되는 사실은 **모든 단위근의 위수는 정확히 하나로 정해진다**는 것이다.

차근차근 풀기

1단계 처음 몇 개

원시 4차 단위근은 i와 $-\mathrm{i}$이므로 $\mathrm{C}_4(x) = (x-\mathrm{i})(x+\mathrm{i}) = x^2+1$이다. ■

> **생각해 보기** 위수가 1, 2, 3, 5, 6인 단위근은 각각 무엇인가? (6차 단위근을 그려 보고 위수에 따라 분류해 보아라.)

위수 1: 1뿐이므로 $\mathrm{C}_1(x) = x-1$이다. 위수 2: -1뿐이므로 $\mathrm{C}_2(x) = x+1$이다.

위수 3: 1이 아닌 3차 단위근, 즉 $\frac{x^3-1}{x-1}$의 근이다. 따라서 $\mathrm{C}_3(x) = x^2+x+1$이다.

위수 5: 1이 아닌 5차 단위근으로, 이들은 $\frac{x^5-1}{x-1}$의 근이다. 따라서 $\mathrm{C}_5(x) = x^4+x^3+x^2+x+1$이다.

위수 6: 6차 단위근 $e^{k\pi\mathrm{i}/3}$, $k = 0, \dots, 5$ 가운데 $k = 0, 3$인 것의 위수는 각각 1, 2이고, $k = 2, 4$인 것의 위수는 3이다. 남는 것은 $e^{\pm\pi\mathrm{i}/3}$이므로

$$\mathrm{C}_6(x) = (x-e^{\mathrm{i}\pi/3})(x-e^{-\mathrm{i}\pi/3}) = x^2 - 2x\cos\tfrac{\pi}{3} + 1 = x^2 - x + 1. \qquad ■$$

2단계 어떤 n에서 x^4+1이 나오는가?

$x^4+1=0$의 근은 $x^4 = -1$을 만족하므로 $x^8 = 1$이지만 $x^4 \neq 1$이다. 따라서 그 위수는 8의 약수이지만 4의 약수는 아니므로 8이다. 역으로 위수가 8인 근은 $x^8 = 1$, $x^4 \neq 1$을 만족하므로 $x^4 = -1$이다. 원시 8차 단위근은 네 개이고 x^4+1의 근도 네 개이므로 $n = 8$이다. ■

3단계 소수

p가 소수(prime)이면 p차 단위근의 위수는 p의 약수이므로 1 또는 p이다. 따라서 1을 제외한 모든 p차 단위근은 원시 단위근이고,

$$\mathrm{C}_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + x + 1. \qquad ■$$

4단계 어떤 원분다항식도 다른 두 원분다항식의 곱이 아니다

> **잠깐, 직접 해 보기** $\mathrm{C}_q = \mathrm{C}_r\mathrm{C}_s$라고 하자. C_r의 근 하나를 잡자. 그 위수는 무엇인가? 이 항등식은 그 위수에 대해 무엇을 말해 주는가? 그 결과 무엇이 강제되는가?

C_r의 모든 근($e^{2\pi\mathrm{i}/r}$이 원시 단위근이므로 근은 적어도 하나 있다)은 $\mathrm{C}_r\mathrm{C}_s = \mathrm{C}_q$의 근이므로 위수가 q이다. 그런데 이 근의 위수는 r이기도 하고, 단위근의 위수는 하나뿐이므로 $r = q$이

다. 그러면 $C_q = C_q C_s$이고, C_q는 영다항식이 아니므로 $C_s = 1$이다. 그러나 C_s는 적어도 하나의 근 $e^{2\pi i/s}$를 가지므로 이는 불가능하다. 따라서 그러한 q, r, s는 존재하지 않는다. ■

돌아보기

- **위수에 따라 분류하라.** 모든 단위근은 유일한 위수를 가지며, 위수에 따라 묶으면 $z^n - 1$의 근이 서로소인 부류들로 나뉜다.
- **근으로 다항식을 정의하라.** 각 C_n은 어떤 수들이 정확히 그 근인지를 밝힘으로써 결정되었다.
- **유일성에서 불가능성이 나온다.** 소문항 (iv)에는 단 하나의 아이디어만 필요했다. 하나의 근이 서로 다른 두 위수를 가질 수는 없다는 것이다.

숨은 수학

$x^n - 1$의 인수분해

모든 n차 단위근은 n의 약수인 어떤 위수 d를 가지며, d차 단위근 가운데 위수가 d인 것은 $d \mid n$일 때 모두 n차 단위근이다. 따라서 $x^n - 1$의 근은 위수에 따라 여러 부류로 나뉘고, 다음을 얻는다.

$$x^n - 1 = \prod_{d \mid n} C_d(x).$$

예를 들어 $x^6 - 1 = C_1 C_2 C_3 C_6 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$이다. 그림 6.1.1은 열두 개의 12차 단위근을 이런 방식으로 분류한 것이다. 원시 n차 단위근의 개수, 즉 C_n의 차수는 k 가운데 1과 n 사이에 있으면서 n과 공약수가 없는 것의 개수이며, 이것이 바로 **오일러 피 함수**(*Euler's totient function*) $\varphi(n)$이다. 차수를 비교하면 항등식 $\sum_{d \mid n} \varphi(d) = n$을 얻는다.

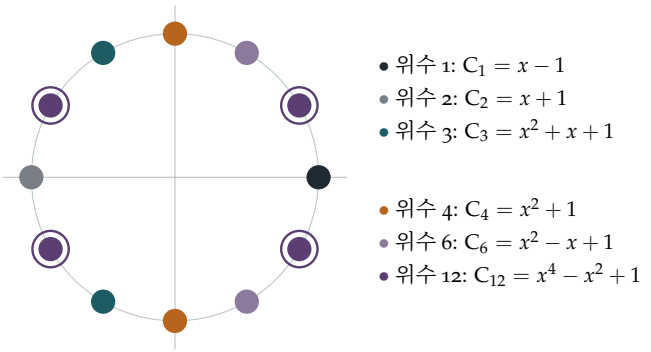


그림 6.1.1 위수에 따라 색칠한 열두 개의 12차 단위근. 네 개의 원시 12차 단위근(고리 표시)은 C_{12}의 근이다. 모든 부류를 합치면 $x^{12} - 1 = C_1C_2C_3C_4C_6C_{12}$이고, 차수는 $1 + 1 + 2 + 2 + 2 + 4 = 12$이다.

정수 계수, 그리고 뜻밖의 사실

정의만 보아서는 분명하지 않지만, 모든 원분다항식의 계수는 **정수**이다. ($x^n - 1$의 인수분해와 수학적 귀납법(induction)을 이용한다. C_n은 $x^n - 1$을 그보다 앞선 원분다항식들의 곱으로 나눈 것이고, 정수 계수 다항식을 최고차항의 계수가 1인(monic) 정수 계수 다항식으로 나누는 다항식의 나눗셈에서는 계수가 계속 정수로 남는다.) 오랫동안 알려진 모든 예는 계수가 0, 1, -1뿐이었다. 첫 번째 예외는 1883년 Migotti가 발견한 C_{105}로, 이 다항식에는 $-2x^7$이라는 항이 있다. $105 = 3 \times 5 \times 7$은 서로 다른 홀수 소인수를 세 개 가지는 가장 작은 수이다. 사실 원분다항식의 계수는 원하는 만큼 크게 만들 수 있다.

기약성

소문항 (iv)는 어떤 원분다항식도 다른 두 원분다항식의 곱이 아님을 보여 준다. 실제로는 훨씬 강한 사실이 성립한다. C_n은 유리수 계수를 가진 더 낮은 차수의 다항식들로 전혀 인수분해되지 않는다. 가우스는 소수 n에 대하여 이를 증명했고(이는 대학 첫 대수학 강의에서 배우게 될 **아이젠슈타인 판정법**(*Eisenstein's criterion*)에서 나온다), 크로네커(Kronecker)와 데데킨트(Dedekind)는 일반적인 n에 대하여 증명했다. 이 **기약성**(*irreducibility*) 덕분에 원분다항식은 단위근과 관련된 다항식 가운데 "소수"의 역할을 하며, 이는 단위근에 대한 갈루아(Galois) 이론의 출발점이 된다.

사고 기술

분류한 다음 쌓아 올리기

문제 속의 대상들을 하나의 잘 정의된 불변량(*invariant*)에 따라 부류로 나누고, 부류별로 구조를 쌓아 올려라.

여기서 불변량은 단위근의 위수였다. 각 근의 위수가 정확히 하나이므로 부류들은 겹치지 않으며, $x^n - 1$은 이 부류들에 걸친 곱으로 분해된다. 같은 패턴(유일한 불변량이 서로소인 분해를 낳는 것)이 소인수분해와 유한 아벨 군(finite abelian groups)의 분류의 바탕에도 놓여 있다.

더 도전하기

1 **인수분해 확인하기.** $(x-1)(x+1)(x^2+x+1)(x^2-x+1) = x^6-1$임을 확인하고, $x^{12}-1$이 그림 6.1.1에서처럼 인수분해됨을 확인하여라.

2 **소수의 두 배.** p가 홀수인 소수이면 $C_{2p}(x) = C_p(-x)$임을 보여라. $p = 3$일 때 이를 확인하여라.

3 **오일러 피 함수.** 소수 p에 대하여 $\varphi(p^k) = p^k - p^{k-1}$이고 $C_{p^k}(x) = C_p\left(x^{p^{k-1}}\right)$임을 보여라. 이를 이용하여 C_9를 구하여라.

4 **조금 긴 문제.** 심화 $x^{15}-1 = C_1C_3C_5C_{15}$를 이용하여 $C_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$임을 보여라.

더 읽을거리

- **Ian Stewart, *Galois Theory*** (CRC Press). 갈루아 이론에 대한 표준적인 학부 입문서이다. 원분다항식과 정다각형이 앞부분에 나온다.
- **Harold Davenport, *The Higher Arithmetic*** (Cambridge University Press). 단위근과 그 산술을 다룬다.
- **Marcus du Sautoy, *Finding Moonshine*** (Fourth Estate). 대칭과 군론을 다룬 교양서로, 갈루아의 이야기도 담겨 있다.

6.2 가우스의 정17각형

문제

STEP II 1991, 4번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:

`step.maths.org/questions/91-s2-q4`

도입

1796년 3월 30일, 괴팅겐의 열여덟 살 학생이 평생 쓰게 될 수학 일기의 첫 항목을 적었다. 그는 자와 컴퍼스(ruler and compasses)만으로 정17각형을 작도하는 방법을 발견한 것이다. 그리스인들은 변이 3개, 4개, 5개, 15개인 정다각형(regular polygon)과 그 변의 수를 두 배씩 늘린 정다각형을 작도하는 법을 알고 있었지만, 그 뒤 이천 년 동안 아무도 새로운 정다각형을 단 하나도 더하지 못했다. 카를 프리드리히 가우스(Carl Friedrich Gauss)는 훗날 이 발견 덕분에 문헌학자가 아니라 수학자가 되기로 마음먹었다고 말했고, 자신의 묘비에 정17각형을 새겨 달라고 부탁했다고 전해진다.

이 작도의 핵심은 이 문제의 후반부에 있다. 특정한 네 코사인의 합이 $\frac{\sqrt{17}-1}{4}$, 즉 제곱근만 들어 있는 수와 같다는 것이다. 제곱근으로 만들어지는 길이는 자와 컴퍼스로 작도할 수 있으며, 같은 종류의 단계를 세 번 더 거쳐 가우스는 $\cos\frac{2\pi}{17}$ 자체를 작도할 수 있었다.

시작하기 전에

생각해 보기 정17각형에 관한 문제에 왜 $\cos\frac{2\pi}{5}$에 관한 첫 부분이 나오는가?

이것은 같은 아이디어를 더 작은 다각형에 적용해 보는 준비 운동이다. 정오각형의 경우 합 $\cos\phi + \cos 2\phi$는 유리수 계수의 이차방정식(quadratic equation)을 만족하므로, 이 이차방정식을 풀어 구할 수 있다. 정17각형의 경우에도 네 코사인의 합 z가 이차방정식을 만족함이 드러날 것이다. 두 경우 모두의 요령은 코사인끼리 곱한 다음 $\cos A \cos B = \frac{1}{2}(\cos(A+B) + \cos(A-B))$를 이용하여 곱을 다시 같은 각들의 코사인의 합으로 바꾸는 것이다.

차근차근 풀기

1단계 정오각형

생각해 보기 $y^2 = (\cos\phi + \cos 2\phi)^2$을 전개하고, 각 곱을 합으로 바꾼 뒤, $5\phi = 2\pi$를 이용하여 3ϕ나 4ϕ 같은 각을 줄여 보자.

$y^2 = \cos^2\phi + 2\cos\phi\cos 2\phi + \cos^2 2\phi = \frac{1}{2}(1+\cos 2\phi) + (\cos 3\phi + \cos\phi) + \frac{1}{2}(1+\cos 4\phi)$.

$5\phi = 2\pi$이므로 $\cos 3\phi = \cos(2\pi - 2\phi) = \cos 2\phi$이고 $\cos 4\phi = \cos\phi$이다. 따라서

$$y^2 = 1 + \tfrac{1}{2}(\cos\phi + \cos 2\phi) + (\cos\phi + \cos 2\phi) = 1 + \tfrac{3}{2}y,$$

즉 $2y^2 = 3y + 2$이다. ■$2y^2 - 3y - 2 = (2y+1)(y-2) = 0$의 근은 $y = 2$와 $y = -\frac{1}{2}$이다. 그런데 $y = 2$가 되려면 두 코사인이 모두 1이어야 하는데 그렇지 않으므로 $y = -\frac{1}{2}$이다. ■

2단계 17제곱 단위근의 합은 0이다

$\sum_{k=0}^{16}\cos k\theta$는 $\sum_{k=0}^{16}\omega^k$의 실수부이다. 여기서 $\omega = e^{i\theta}$는 원시(primitive) 17제곱 단위근(root of unity)이다. 이 등비급수(geometric series)는 $\frac{\omega^{17}-1}{\omega-1} = 0$이다. ■

따라서 $\sum_{k=1}^{16}\cos k\theta = -1$이다. $\cos(17-k)\theta = \cos k\theta$이므로 항들이 짝을 이루고,

$$\sum_{k=1}^{8}\cos k\theta = -\tfrac{1}{2}.$$

3단계 코사인을 두 묶음으로 나누기

생각해 보기 $z = \cos\theta + \cos 2\theta + \cos 4\theta + \cos 8\theta$라 하고, 나머지 네 코사인의 합 $\cos 3\theta + \cos 5\theta + \cos 6\theta + \cos 7\theta$를 z'이라 하자. $z + z'$은 얼마인가?

2단계에 의해 $z + z' = -\frac{1}{2}$이다. zz'도 구할 수 있다면 z와 z'은 어떤 이차방정식의 두 근이 된다.

잠깐, 직접 해 보기 zz'을 계산하라. 이를 16개의 곱 $\cos a\theta\cos b\theta$로 전개하고, 각각을 두 코사인의 합으로 바꾼 다음, $\cos\theta, \cos 2\theta, \ldots, \cos 8\theta$가 각각 몇 번 나타나는지 세어 보라. ($\cos k\theta = \cos(17-k)\theta$와 $\cos(-k\theta) = \cos k\theta$를 이용하여 각을 줄인다.)

각 곱은 $\cos a\theta\cos b\theta = \frac{1}{2}(\cos(a+b)\theta + \cos(a-b)\theta)$가 되므로, zz'은 32개의 코사인의 합에 $\frac{1}{2}$을 곱한 것이다. $a \in \{1,2,4,8\}$, $b \in \{3,5,6,7\}$인 16개의 쌍을 차례로 살펴보자. 예

를 들어 $a=1, b=3$이면 $\cos 4\theta$와 $\cos 2\theta$가 나오고, $a=8, b=7$이면 $\cos 15\theta = \cos 2\theta$와 $\cos\theta$가 나온다. 열여섯 쌍 모두에 대해 이렇게 계산하면 $\cos\theta, \dots, \cos 8\theta$가 각각 정확히 네 번씩 나타난다. 그러므로

$$zz' = \tfrac{1}{2} \times 4 \times \sum_{k=1}^{8} \cos k\theta = 2 \times \left(-\tfrac{1}{2}\right) = -1.$$

4단계 이차방정식

따라서 z와 z'은 $t^2 + \frac{1}{2}t - 1 = 0$, 즉 $4t^2 + 2t - 4 = 0$의 두 근이고, 그 근은 $t = \frac{-1\pm\sqrt{17}}{4}$이다. 어느 쪽이 z인가? 수치로 보면 $\cos\theta \approx 0.932$, $\cos 2\theta \approx 0.739$, $\cos 4\theta \approx 0.092$, $\cos 8\theta \approx -0.983$이므로 $z \approx 0.78 > 0$이다. 그러므로

$$z = \frac{-1+\sqrt{17}}{4} = -\frac{1-\sqrt{17}}{4}. \qquad \blacksquare$$

돌아보기

- **곱을 합으로.** 코사인의 곱셈 공식은 y^2과 zz'을 같은 코사인들의 합으로 바꾸어 주었고, 그래서 계산이 닫힌 형태로 마무리되었다.
- **합과 곱이 이차방정식을 준다.** $z+z'$과 zz'을 아는 것은 z와 z'을 두 근으로 하는 이차방정식을 아는 것과 같다.
- **올바르게 나누는 것이 중요하다.** 여덟 개의 코사인을 $\{1,2,4,8\}$과 $\{3,5,6,7\}$로 나누었기 때문에 zz'에서 모든 지표가 똑같은 횟수만큼 나타났다. 아무렇게나 나누면 이렇게 되지 않는다.

숨은 수학

가우스 주기

왜 $\{1,2,4,8\}$인가? 17을 법으로 할 때, 3의 거듭제곱 $3^0, 3^1, 3^2, \dots$은 0이 아닌 모든 나머지(residue)를 거친다.

$$1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6.$$

하나 걸러 하나씩, 즉 $3^0, 3^2, 3^4, \dots$을 택하면 1, 9, 13, 15, 16, 8, 4, 2가 나오는데, 이는 17을 법으로 ±1, ±2, ±4, ±8이며, 정확히 z에 들어 있는 각들이다. 나머지 절반은 $\pm3, \pm5, \pm6, \pm7$로, z'에 들어 있는 각들이다. 가우스는 이러한 묶음에 걸친 ω^k의 합을 주기(*period*)라고 불렀다. $17-1 = 16 = 2^4$이므로 나머지들을 네 번 반으로 나눌 수 있고,

각 단계에서 주기들은 이전 단계의 주기들이 계수에 들어 있는 이차방정식을 만족한다. 이 차방정식 네 개, 즉 제곱근 네 개를 거쳐 유리수에서 $\cos\frac{2\pi}{17}$까지 내려갈 수 있다.

$$\cos\tfrac{2\pi}{17} = \tfrac{1}{16}\Big(-1+\sqrt{17}+\sqrt{34-2\sqrt{17}} \\ +2\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}\Big).$$

모든 단계에 제곱근만 들어 있고, 제곱근은 (닮은 삼각형이나 반원을 이용하여) 자와 컴퍼스로 작도할 수 있으므로, 정17각형은 작도 가능(constructible)하다.

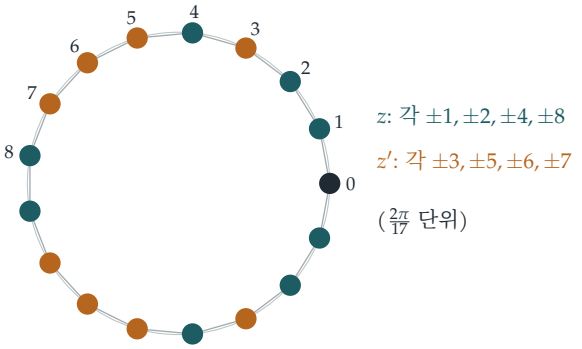


그림 6.2.1 가우스의 두 주기로 나눈 정17각형의 꼭짓점. 청록색 꼭짓점은 ($\frac{2\pi}{17}$ 단위로) 각 $\pm1, \pm2, \pm4, \pm8$에 있으며, 이들의 x좌표의 합은 $2z = \frac{-1+\sqrt{17}}{2}$이다. 호박색 꼭짓점은 $2z' = \frac{-1-\sqrt{17}}{2}$을 준다.

어떤 다각형을 작도할 수 있는가?

가우스가 주장하고 1837년 피에르 방첼(Pierre Wantzel)이 증명한 바에 따르면, 정n각형을 자와 컴퍼스로 작도할 수 있는 것은 n이 2의 거듭제곱과 서로 다른 **페르마 소수**(*Fermat prime*)들의 곱의 곱일 때, 그리고 그때뿐이다. 페르마 소수란 $2^{2^m}+1$ 꼴의 소수이다. 알려진 페르마 소수는 3, 5, 17, 257, 65537이며, 이는 Section 1.1의 페르마 수이다. (페르마(Fermat)는 이런 수가 모두 소수라고 추측했지만, 오일러(Euler)가 $2^{32}+1$이 641로 나누어떨어짐을 보였고, 그 뒤로 더 이상의 페르마 소수는 발견되지 않았다.) 따라서 정257각형과 정65537각형은 작도 가능하다. 19세기에 Johann Hermes는 약 십 년에 걸쳐 정65537각형의 작도법을 완성했고, 그의 원고는 괴팅겐에 보관되어 있다. 정7각형과 정11각형은 작도할 수 없는데, 7과 11이 페르마 소수가 아니기 때문이다($7-1=6$과 $11-1=10$은 2의 거듭제곱이 아니다). 정9각형도 작도할 수 없는데, $9=3^2$에서 페르마 소수 3이 반복되기 때문이다. 방첼의 증명은 Section 6.3에서 다루는 체의 차수(degree of a field extension) 이론을 이용한다.

사고 기술

합과 곱을 계산하여 이차방정식 찾기

어떤 양을 구하려면, 그것과 자연스럽게 짝을 이루는 상대를 찾아 둘의 합과 곱을 계산하고, 그로부터 얻은 이차방정식을 풀어라.

요령은 합과 곱을 모두 계산할 수 있도록 짝을 고르는 데 있다. 여기서는 17을 법으로 한 나머지들의 대칭성에서 짝이 나왔고, 이 아이디어를 네 번 되풀이하여 가우스는 작도법을 얻었다.

더 도전하기

1 **정칠각형.** STEP II 1995, 6번 문제 (`step.maths.org/questions/95-s2-q6`)을 풀어 보라. 단위근을 묶는 가우스의 아이디어를 7제곱 단위근에 적용하여, 코사인의 합과 사인의 합의 정확한 값을 구하는 문제이다. 사인 합의 부호를 결정하는 것이 미묘한 단계이다.

2 **정오각형.** $\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$임을 보이고, 이를 이용하여 자와 컴퍼스로 정오각형을 작도하는 방법을 설명하라.

3 **다른 주기.** $z' = \cos 3\theta + \cos 5\theta + \cos 6\theta + \cos 7\theta = \frac{-1-\sqrt{17}}{4}$임을 수치로 확인하라.

4 **생성원.** 17을 법으로 할 때 3의 거듭제곱은 0이 아닌 모든 나머지를 주지만, 2의 거듭제곱은 그렇지 않음을 보여라. 2의 거듭제곱은 어떤 나머지들을 주는가?

더 읽을거리

- **Ian Stewart, *Galois Theory*** (CRC Press). 자와 컴퍼스 작도와 정17각형을 다루는 장이 있다.
- **Richard Courant & Herbert Robbins, *What Is Mathematics?*** (Oxford University Press). 제3장은 정17각형을 포함하여 작도를 초등적으로 아름답게 설명한다.
- **Daniel Kehlmann, *Measuring the World*** (Quercus). 가우스와 알렉산더 폰 훔볼트(Alexander von Humboldt)에 관한 유쾌한 소설로, 머리를 식히기에 좋다.

6.3 $\sqrt{2}+\sqrt{3}+\sqrt{5}$를 근으로 갖는 다항식

문제

STEP II 2023, 4번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 OCR에서 내려받을 수 있는 2023년 STEP 시험지 묶음(zip 파일) 가운데 STEP II 시험지에 있다:

`www.ocr.org.uk/Images/707102-2023-past-papers.zip`

도입

$\sqrt{2}$는 정수 계수 다항식 x^2-2의 근이다. $\sqrt{3}$도 x^2-3의 근이다. 그렇다면 $\sqrt{2}+\sqrt{3}$도 어떤 정수 계수 다항식의 근일까? $\sqrt{2}+\sqrt{3}+\sqrt{5}$나 $\sqrt[3]{2}+\sqrt[3]{3}$은 어떨까?

정수 계수 다항식의 근이 되는 수를 **대수적 수**(algebraic number)라 한다. 이 문제는 직접 손으로 근호를 소거하여 대수적 수의 합이 다시 대수적 수임을 보인다. 이 과정에서 나오는 차수 4, 8, 6, 9는 우연이 아니다. 이 차수는 각 수가 얼마나 "복잡한지"를 재는 척도이며, 바로 이 척도, 곧 **체의 확대 차수**(degree of a field extension)가 고대 그리스의 문제인 정육면체의 배적 문제와 각의 삼등분 문제를 마침내 해결하였다.

시작하기 전에

생각해 보기 $\sqrt{2}$를 근으로 갖는 다항식을 찾으려면 $x=\sqrt{2}$의 양변을 제곱하여 제곱근을 없앤다. 서로 다른 두 제곱근은 어떻게 하나씩 없앨 수 있을까?

한 제곱근을 한쪽으로 분리한 뒤 제곱하면 그 제곱근이 사라진다. 그다음 다른 제곱근을 분리하여 다시 제곱한다. 제곱할 때마다 차수는 두 배가 될 수 있다. 이것이 이 문제의 전략 전부이다. 근호를 하나씩 소거하는 것이다.

차근차근 풀기

1단계 두 개의 제곱근

$(x-\sqrt{2})^2 = 3$이면 $x^2 - 2\sqrt{2}\,x + 2 = 3$이므로 $x^2 - 1 = 2\sqrt{2}\,x$이다. 양변을 제곱하면 남은 제곱근이 사라져 $(x^2-1)^2 = 8x^2$, 즉

$$x^4 - 10x^2 + 1 = 0. \qquad \blacksquare$$

이다. 또 $x = \sqrt{2}+\sqrt{3}$은 $(x-\sqrt{2})^2 = (\sqrt{3})^2 = 3$을 만족하므로 $f(\sqrt{2}+\sqrt{3}) = 0$이다. $\blacksquare$

2단계 세 개의 제곱근

? **생각해 보기** $x = \sqrt{2}+\sqrt{3}+\sqrt{5}$라 하면 $x - \sqrt{5} = \sqrt{2}+\sqrt{3}$은 f의 근이다. $f(x-\sqrt{5}) = 0$을 $P(x) + \sqrt{5}\,Q(x) = 0$ 꼴로 나타내 보자. 그다음 $\sqrt{5}$는 어떻게 소거할까?

$(x-\sqrt{5})^2 = x^2 + 5 - 2\sqrt{5}x$와 $(x-\sqrt{5})^4 = \left(x^2+5-2\sqrt{5}x\right)^2 = x^4 + 30x^2 + 25 - 4\sqrt{5}\,x(x^2+5)$를 이용하여 전개하면

$$f(x-\sqrt{5}) = \left(x^4+30x^2+25\right) - 4\sqrt{5}\,x(x^2+5) - 10\left(x^2+5\right) + 20\sqrt{5}\,x + 1.$$

이다. 정리하면 $P(x) = x^4 + 20x^2 - 24$이고 $Q(x) = -4x^3 - 20x + 20x = -4x^3$이다. 따라서 $x^4 + 20x^2 - 24 = 4\sqrt{5}\,x^3$이다. 양변을 제곱하면

$$\left(x^4+20x^2-24\right)^2 = 80x^6,$$

이고, 전개하면

$$g(x) = x^8 - 40x^6 + 352x^4 - 960x^2 + 576. \qquad \blacksquare$$

를 얻는다. (검산: $400 - 48 = 352$를 이용하면 $(x^4+20x^2-24)^2 = x^8 + 40x^6 + 352x^4 - 960x^2 + 576$이고, 여기서 $80x^6$을 빼면 g가 된다.)

3단계 삼차방정식의 근과 제곱근

? **생각해 보기** $x = a + \sqrt{2}$이면 $x - \sqrt{2}$는 $t^3 - 3t + 1$의 근이다. 이를 대입하고, $\sqrt{2}$가 있는 항과 없는 항을 나눈 뒤 제곱하라.

$(x-\sqrt{2})^3 = x^3 - 3\sqrt{2}\,x^2 + 6x - 2\sqrt{2}$이므로

$$(x-\sqrt{2})^3 - 3(x-\sqrt{2}) + 1 = \left(x^3+3x+1\right) - \sqrt{2}\left(3x^2-1\right) = 0.$$

이다. 따라서 $(x^3+3x+1)^2 = 2(3x^2-1)^2$이다. 전개하면 $x^6 + 6x^4 + 2x^3 + 9x^2 + 6x + 1 = 18x^4 - 12x^2 + 2$이므로

$$h(x) = x^6 - 12x^4 + 2x^3 + 21x^2 + 6x - 1. \qquad \blacksquare$$

이다. a가 t^3-3t+1의 근이라는 사실만 사용했으므로 같은 논증이 $b+\sqrt{2}$와 $c+\sqrt{2}$에도 그대로 적용된다. (h의 나머지 세 근은 $a-\sqrt{2}$, $b-\sqrt{2}$, $c-\sqrt{2}$이며, 이들은 제곱하는 과정에서 끼어든 것이다.)

4단계 두 개의 세제곱근

> **잠깐, 직접 해 보기** $x=\sqrt[3]{2}+\sqrt[3]{3}$이라 하자. 양변을 세제곱하라. 그 결과를 x와 세제곱근 하나만으로 나타낼 수 있는가?

$u=\sqrt[3]{2}$, $v=\sqrt[3]{3}$으로 두고 $(u+v)^3=u^3+v^3+3uv(u+v)$를 이용하면

$$x^3=2+3+3\sqrt[3]{6}\,x, \qquad \text{따라서} \qquad x^3-5=3\sqrt[3]{6}\,x.$$

이다. 다시 세제곱하면 마지막 세제곱근이 사라져 $(x^3-5)^3=27\cdot 6\,x^3=162x^3$이 된다. $(x^3-5)^3=x^9-15x^6+75x^3-125$로 전개하면

$$\mathrm{k}(x)=x^9-15x^6-87x^3-125. \qquad \blacksquare$$

이다.

돌아보기

- **근호는 하나씩 소거한다.** 근호 하나를 분리하고, 알맞은 거듭제곱을 한 다음, 이를 반복한다.
- **유리 부분과 무리 부분을 나눈다.** 식을 $P+\sqrt{5}\,Q$ 꼴로 쓰고 $P^2=5Q^2$을 이용하는 것이 핵심 단계이다.
- **제곱하면 근이 늘어난다.** 제곱할 때마다 $a+\sqrt{2}$에 대한 $a-\sqrt{2}$처럼 "켤레"(conjugate) 근이 끼어든다. 최종 다항식은 이 근들을 모두 근으로 갖는다.

숨은 수학

체와 그 차수

p, q가 유리수일 때 $p+q\sqrt{2}$ 꼴인 수 전체의 집합 $\mathbb{Q}(\sqrt{2})$는 덧셈, 뺄셈, 곱셈, (0이 아닌 수로의) 나눗셈에 대하여 닫혀 있다. 즉 이 집합은 **체**(field)이다. 이 체는 $\mathbb{Q}$ 위의 2차원 "벡터 공간"(vector space)이고 기저(basis)는 1, $\sqrt{2}$이므로, $\mathbb{Q}$ 위에서 **차수**(degree)가 2라고 한다. 여기에 $\sqrt{3}$을 첨가하면 기저가 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$이고 차수가 4인 $\mathbb{Q}(\sqrt{2},\sqrt{3})$을 얻고, $\sqrt{5}$까지 첨가하면 차수가 8이 된다(그림 6.3.1). **탑 법칙**(tower law)에 따르면 체의 탑을

따라 올라가면서 차수는 곱해진다. 어떤 수가 생성하는 체의 차수는 그 수의 **최소다항식**(minimal polynomial), 곧 그 수를 근으로 갖는 유리수 계수 다항식 가운데 차수가 가장 낮은 것의 차수와 같다. 이 문제의 다항식 f와 g가 최소다항식임을 보일 수 있으므로, $\sqrt{2}+\sqrt{3}$의 차수는 4이고 $\sqrt{2}+\sqrt{3}+\sqrt{5}$의 차수는 8이다. 실제로 수 $\sqrt{2}+\sqrt{3}+\sqrt{5}$ 하나가 차수 8인 체 전체를 생성한다.

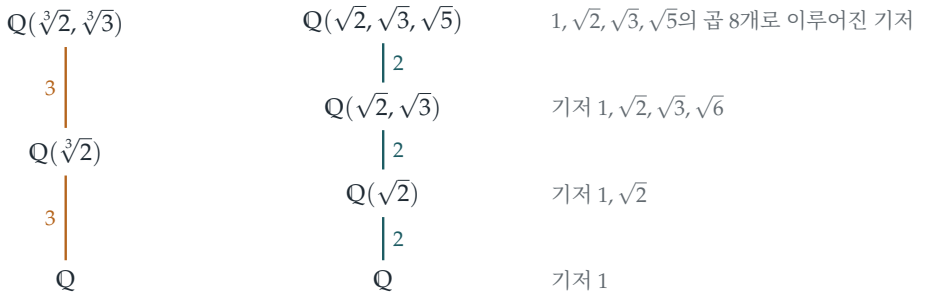


그림 6.3.1 체의 탑. 오른쪽: 제곱근을 하나 첨가할 때마다 차수가 두 배가 되어 $2\times2\times2=8$, 곧 g의 차수가 된다. 왼쪽: 세제곱근을 하나 첨가할 때마다 차수가 세 배가 되어 $3\times3=9$, 곧 k의 차수가 된다. 탑을 따라 올라가면서 차수는 곱해진다. 이 **탑 법칙**이 자와 컴퍼스 작도의 불가능성 증명의 열쇠이다.

정육면체의 배적 문제

자와 컴퍼스를 이용한 작도(ruler-and-compass construction)로 얻을 수 있는 길이는 유리수에서 출발하여 일차방정식과 이차방정식을 거듭 풀어 얻는 길이뿐이다. 이러한 각 단계는 차수가 1 또는 2인 체의 확대를 주므로, 탑 법칙에 의해 작도 가능한 길이는 모두 차수가 2의 거듭제곱인 체에 속하고, 그 길이 자체의 차수도 2의 거듭제곱이다. 그런데 $\sqrt[3]{2}$의 최소다항식은 차수가 3인 x^3-2이다. 3은 2의 거듭제곱이 아니므로 $\sqrt[3]{2}$는 작도할 수 없고, 따라서 기원전 430년 무렵에 제기된, 자와 컴퍼스로 정육면체의 부피를 두 배로 만드는 델로스 문제(Delian problem)는 불가능하다. Pierre Wantzel은 1837년에 이를 증명하였고, 아울러 일반적인 각의 삼등분이 불가능함과 작도 가능한 정다각형의 분류(Section 6.2)도 증명하였다. 이천 년에 걸친 시도가 차수에 관한 논증 하나로 끝난 것이다.

대수적 수는 체를 이룬다

이 문제의 방법은 몇 가지 예에서 대수적 수의 합이 대수적 수임을 보여 준다. 일반적인 경우는 선형대수로 증명한다. α와 β의 차수가 각각 m과 n이면, $(i<m,\ j<n$인$)$ 수 $\alpha^i\beta^j$ 전체는 차원이 최대 mn인 공간을 생성(span)하므로, $mn+1$개의 거듭제곱 $1,\alpha+\beta,(\alpha+\beta)^2,\ldots$은 일차 종속(linearly dependent)이어야 하고, 이로부터 차수가 최대 mn인 다항식을 얻는다. 우리가 얻은 차수 $4=2\times2,\ 6=3\times2,\ 9=3\times3$은 이 패턴에 정확히 들어맞는다. 대

수적 수가 아닌 수를 **초월수**(transcendental number)라 한다. e와 π가 그 예이며(에르미트(Hermite), 1873년, 린데만(Lindemann), 1882년), π가 초월수라는 린데만의 정리는 원과 넓이가 같은 정사각형의 작도 역시 불가능함을 증명하였다.

사고 기술

> **소거한 다음, 측정하라**
>
> 근호로 나타낸 식이 만족하는 다항식을 찾으려면, 근호를 분리하고 거듭제곱하여 하나씩 없앤다.
>
> 그다음 차수가 무엇을 말해 주는지 물어라. 최소다항식의 차수는 그 수의 불변량(invariant)이며, 차수를 비교하는 것은 어떤 일이 불가능함을 증명하는 가장 강력한 방법 가운데 하나이다.

더 도전하기

1 **원시원소.** $y=\sqrt{2}+\sqrt{3}$이라 하자. $y^3=11\sqrt{2}+9\sqrt{3}$임을 보이고, 이로부터 $\sqrt{2}=\frac{1}{2}(y^3-9y)$임을 이끌어 내어라. 따라서 모든 수 $p+q\sqrt{2}+r\sqrt{3}+s\sqrt{6}$은 y에 대한 다항식으로 나타낼 수 있다.

2 **섞인 근호.** $\sqrt{2}+\sqrt[3]{3}$을 근으로 갖는, 정수 계수의 6차 다항식을 구하여라.

3 **기약성(irreducibility).** x^4-10x^2+1은 유리수 근을 갖지 않으며, 정수 계수 이차식 두 개의 곱으로 나타낼 수 없음을 보여라. (**힌트:** $(x^2+ax+b)(x^2-ax+c)$ 꼴을 시도해 보라.) 이로부터 $\sqrt{2}+\sqrt{3}$의 차수가 4임을 이끌어 내어라.

4 **삼등분.** $\cos 3\theta=4\cos^3\theta-3\cos\theta$임을 보이고, 이로부터 $\cos 20^\circ$가 $8x^3-6x-1=0$의 근임을 이끌어 내어라. 이 삼차식이 유리수 근을 갖지 않는다고 할 때(이를 확인하라), 자와 컴퍼스로 60°인 각을 삼등분할 수 없는 이유를 설명하여라.

더 읽을거리

- **Ian Stewart, *Galois Theory*** (CRC Press). 갈루아 이론. 체의 확대, 탑 법칙, 고전적인 작도 문제를 학부생을 위해 다룬다.
- **Richard Courant & Herbert Robbins, *What Is Mathematics?*** (Oxford University Press). 수학이란 무엇인가. 제 3장에서 선수 지식 없이 그리스 작도 문제의 불가능성을 증명한

다.

- **Robin Hartshorne, *Geometry: Euclid and Beyond*** (Springer). 기하학: 유클리드와 그 너머. 자와 컴퍼스 작도를 현대 대수학으로 다룬다.

6.4 사차방정식 풀기

문제

STEP III 2017, 3번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:

`step.maths.org/questions/17-s3-q3`

도입

이차방정식(quadratic equation)의 근의 공식은 모든 학생이 배운다. 삼차방정식(cubic)과 사차방정식(quartic)의 근의 공식도 존재한다. 이 공식들은 16세기 이탈리아에서 비밀 대결과 우선권을 둘러싼 격렬한 논쟁 속에서 발견되었다. 지롤라모 카르다노(Gerolamo Cardano)는 1545년 저서 *Ars Magna*(**위대한 술법**)에서 두 공식을 모두 발표했는데, 삼차방정식의 공식은 (그에게 비밀 유지를 맹세하게 했던) 니콜로 타르탈리아(Niccolò Tartaglia)에게서, 사차방정식의 공식은 자신의 제자 로도비코 페라리(Lodovico Ferrari)에게서 얻은 것이었다. 그 뒤 거의 300년 동안 수학자들은 오차방정식(quintic)의 근의 공식을 찾으려 했지만 헛수고였다.

이 문제는 사차방정식을 푸는 요령을 보여 주며, 이 요령에는 깊은 의미가 담겨 있다. 네 근을 두 개씩 짝짓는 세 가지 방법에 따라 세 개의 새로운 양을 만든다. 이 세 양은 하나의 삼차방정식을 만족하고, 그 삼차방정식은 풀 수 있으며, 그 해로부터 원래의 근을 구할 수 있다. 이 방법이 **왜** 통하는지, 즉 왜 네 근은 세 개의 양으로 줄일 수 있는데 다섯 근은 같은 방식으로 줄일 수 없는지라는 물음이 갈루아(Galois)를 군론(group theory)의 창시로 이끌었다.

시작하기 전에

? **생각해 보기** 네 대상 $\alpha, \beta, \gamma, \delta$를 두 쌍으로 나누는 방법은 몇 가지인가?

세 가지이다. $\{\alpha\beta, \gamma\delta\}$, $\{\alpha\gamma, \beta\delta\}$, $\{\alpha\delta, \beta\gamma\}$이다(그림 6.4.1). 문제에 나오는 세 양 $\alpha\beta + \gamma\delta$ 등은 이 세 가지 짝짓기에 대응한다. 네 근을 어떻게 재배열하든 세 짝짓기는 자기들끼리 뒤섞일 뿐이다. 따라서 세 양에 대한 대칭식(symmetric expression)은 모두 네 근에 대한 대

칭식이 되고, p, q, r, s로 나타낼 수 있다. 바로 이 때문에 세 양은 계수가 p, q, r, s만으로 이루어진 삼차방정식을 만족한다.

차근차근 풀기

1단계 빠진 계수

생각해 보기 삼차방정식 $y^3 + Ay^2 + By + C = 0$에서 근의 합을 A로 나타내면 무엇인가? 그리고 $(\alpha\beta + \gamma\delta) + (\alpha\gamma + \beta\delta) + (\alpha\delta + \beta\gamma)$를 사차방정식의 계수로 나타내면 무엇인가?

삼차방정식의 근의 합은 $-A$이다. 세 양의 합은 $\alpha, \beta, \gamma, \delta$에서 두 개씩 곱한 여섯 개의 곱을 모두 더한 것이고, 사차식 $x^4 + px^3 + qx^2 + rx + s$에서 이 값은 q이다. 따라서 $A = -q$이다.

2단계 구체적인 삼차방정식

$p = 0, q = 3, r = -6, s = 10$이면 삼차방정식은 다음과 같다.

$$y^3 - 3y^2 + (0 - 40)y + (120 - 0 - 36) = y^3 - 3y^2 - 40y + 84 = 0.$$

생각해 보기 84의 작은 약수들을 대입해 보라.

$y = 2$를 대입하면 $8 - 12 - 80 + 84 = 0$이다. 나누어 보면 $y^3 - 3y^2 - 40y + 84 = (y - 2)(y^2 - y - 42) = (y - 2)(y - 7)(y + 6)$이다. 가장 큰 근은 7이므로 $\alpha\beta + \gamma\delta = 7$이다. ■

3단계 근의 쌍

$(\alpha + \beta)(\gamma + \delta) = \alpha\gamma + \alpha\delta + \beta\gamma + \beta\delta$이고, 이는 두 개씩 곱한 여섯 개의 곱의 합에서 $\alpha\beta + \gamma\delta$를 뺀 것, 즉 $q - 7 = 3 - 7 = -4$이다.

또 $\alpha\beta \cdot \gamma\delta = \alpha\beta\gamma\delta = s = 10$이다. 따라서 $\alpha\beta$와 $\gamma\delta$는 합이 7이고 곱이 10이므로 $t^2 - 7t + 10 = (t - 2)(t - 5)$의 두 근이다. $\alpha\beta > \gamma\delta$이므로 $\alpha\beta = 5, \gamma\delta = 2$이다. ■

4단계 사차방정식 풀기

잠깐, 직접 해 보기 $\alpha + \beta$와 $\gamma + \delta$를 구하라. 두 값의 합(p로부터)과 곱(3단계로부터)은 알고 있다. 어느 쪽이 어느 값인지 정하려면 r을 이용하라.

$\alpha + \beta + \gamma + \delta = -p = 0$이고 $(\alpha + \beta)(\gamma + \delta) = -4$이므로 $\{\alpha + \beta, \gamma + \delta\} = \{2, -2\}$이다. 계수 r은 세 개씩 곱한 네 곱의 합을 준다. 즉 $\alpha\beta\gamma + \alpha\beta\delta + \alpha\gamma\delta + \beta\gamma\delta = -r = 6$이다. 이

식은 $\alpha\beta(\gamma+\delta)+\gamma\delta(\alpha+\beta)=5(\gamma+\delta)+2(\alpha+\beta)$로 쓸 수 있다. $\alpha+\beta=2$이면 이 값은 $-10+4=-6$이고, $\alpha+\beta=-2$이면 $10-4=6$이다. 따라서 $\alpha+\beta=-2$, $\gamma+\delta=2$이다.

이제 α, β는 $t^2+2t+5=0$의 두 근이므로 $-1\pm 2\mathrm{i}$이고, γ, δ는 $t^2-2t+2=0$의 두 근이므로 $1\pm\mathrm{i}$이다. 네 근은 다음과 같다.

$$x=-1\pm 2\mathrm{i}, \qquad x=1\pm\mathrm{i}. \qquad \blacksquare$$

검산: $(x^2+2x+5)(x^2-2x+2)=x^4+3x^2-6x+10$.

돌아보기

- **대칭함수.** 모든 단계에서 근과 계수의 관계, 즉 근의 합과 곱을 이용했다.
- **차수를 낮춰라.** 사차방정식 문제가 삼차방정식(**분해 삼차방정식**(resolvent cubic))이 되었고, 다시 두 개의 이차방정식이 되었다.
- **모든 정보를 활용하라.** p와 q는 합과 곱을 주었고, s는 $\alpha\beta$와 $\gamma\delta$를 구분해 주었으며, r은 어느 쌍이 어느 합에 대응하는지 정해 주었다.

숨은 수학

이 요령이 통하는 이유: 근의 치환

1770년 조제프루이 라그랑주(Joseph-Louis Lagrange)는 삼차방정식과 사차방정식의 풀이법이 왜 통하는지 물었고, 그 답을 근의 **치환**(permutation)에서 찾았다. 네 근을 재배열하는 방법은 24가지이다. 이 모든 재배열에서 세 양 $y_1=\alpha\beta+\gamma\delta$, $y_2=\alpha\gamma+\beta\delta$, $y_3=\alpha\delta+\beta\gamma$는 자기들끼리 뒤섞일 뿐이다. 네 근의 각 재배열은 세 짝짓기의 재배열을 유도한다(그림 6.4.1). 따라서 이 세 양은 계수가 근에 대해 대칭인 3차 다항식을 만족한다. 현대적인 언어로 말하면, 대칭군(symmetric group) S_4(24개의 모든 치환)에서 S_3(짝짓기의 6가지 치환)로 가는 전사 군 준동형사상(group homomorphism)이 존재하며, 이것이 사차방정식을 삼차방정식으로 줄일 수 있는 이유이다.

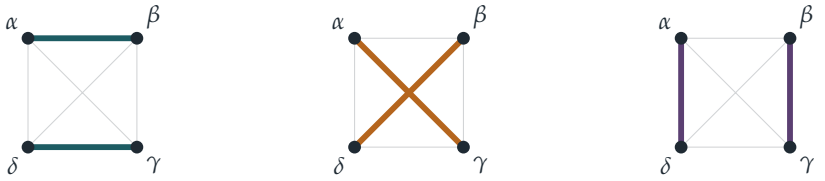


그림 6.4.1 네 근을 두 쌍으로 나누는 세 가지 방법과, 그에 대응하는 분해 삼차방정식의 근. $\alpha, \beta, \gamma, \delta$를 어떻게 재배열하든 이 세 그림은 자기들끼리 치환될 뿐이다. 이 때문에 세 양은 계수를 사차방정식의 계수로 나타낼 수 있는 삼차방정식을 만족한다.

오차방정식

라그랑주는 다섯 근에 대해서도 근의 치환에 따라 몇 가지 값만 취하는 비슷한 양을 찾으려 했지만, 쓸모 있는 것을 찾지 못했다. 1799년 파올로 루피니(Paolo Ruffini)가, 그리고 1824년 닐스 헨리크 아벨(Niels Henrik Abel)이 (증명을 완성하여) 사칙연산과 거듭제곱근(radical)만으로 오차방정식의 근을 나타내는 일반적인 공식은 존재하지 않음을 보였다. 몇 년 뒤 에바리스트 갈루아는 어떤 다항식이 거듭제곱근으로 풀리는지 정확히 설명했다. 바로 **근의 대칭군**을 특정한 방식으로 더 단순한 조각들로 분해할 수 있는 다항식이다. 대칭군 S_4는 (S_3와 더 작은 군들을 거쳐) 분해할 수 있지만, S_5는 더 이상 분해할 수 없는 크기 60의 "단순(simple)" 조각을 포함하므로 분해할 수 없다. 갈루아는 1832년 스무 살의 나이로 결투에서 목숨을 잃기 전날 밤, 서둘러 자신의 이론을 글로 남겼다. 이 이론은 오늘날 수학과 학부 과정의 백미 중 하나이며, 보통 3학년에 배운다.

삼차방정식 풀기

삼차방정식 자체도 비슷한 요령으로 풀 수 있다. 축약 삼차식(depressed cubic) $x^3 - 3px + q$를 두 완전세제곱식의 결합으로 나타내면 이차방정식으로 줄어든다. 이것이 연습문제에 있는 2011년 문제의 방법이며, 카르다노의 공식과 동치이다. 삼차방정식이 세 실근을 가질 때에도 이 공식은 계산 과정에서 복소수(complex number)를 필요로 하는데, 바로 이 현상 때문에 수학자들은 복소수를 진지하게 받아들일 수밖에 없었다(5장의 도입 참고).

사고 기술

대칭은 복잡함을 줄인다

근으로 만든 어떤 양들이 근을 치환할 때 자기들끼리만 치환된다면, 그 양들은 계수를 계산할 수 있는 더 낮은 차수의 다항식을 만족한다.

이것이 갈루아 이론(Galois theory)의 씨앗이다. 방정식을 이해하려면 그 근의 대칭을 이해하라.

더 도전하기

1 **삼차방정식 확인하기.** $y_1 = \alpha\beta + \gamma\delta$ 등일 때 $y_1y_2 + y_2y_3 + y_3y_1 = pr - 4s$임을 확인하라. (전개한 뒤 $\sum\alpha = -p$, $\sum\alpha\beta\gamma = -r$, $\alpha\beta\gamma\delta = s$를 이용하라.)

2 **세제곱의 합으로 본 삼차방정식.** STEP III 2011, 3번 문제 (`step.maths.org/questions/11-s3-q3`)을 풀어 보라. 이 문제는 삼차방정식을 두 세제곱식의 결합으로 나타내어 푸는데, 이 절의 방법과는 상당히 다른 길이다. 답을 수치적으로 확인해 보라.

3 **또 하나의 사차방정식.** 이 절의 방법으로 $x^4 - 4x^3 + 7x^2 - 6x + 2 = 0$을 풀어라. (분해삼차방정식의 한 근은 작은 정수이다.)

4 **치환 세기.** $\alpha, \beta, \gamma, \delta$의 24가지 치환 가운데 짝짓기 $\{\alpha\beta, \gamma\delta\}$를 자기 자신으로 보내는 것을 모두 찾아라. 그런 치환이 8개임을 보여라. (이들은 S_4의 부분군(subgroup)을 이룬다.)

더 읽을거리

- **Mario Livio, *The Equation That Couldn't Be Solved*** (Simon & Schuster). 오차방정식과 군론의 탄생 이야기를 일반 독자를 위해 풀어낸 책이다.
- **Ian Stewart, *Why Beauty Is Truth: A History of Symmetry*** (Basic Books). 바빌로니아의 방정식에서 갈루아와 그 너머까지 다룬다.
- **Ian Stewart, *Galois Theory*** (CRC Press). 학부 교재로, 바로 이 내용을 다루는 역사적 도입부가 있다.

6.5 공리에서 출발하는 미분

문제

STEP II 1992, 4번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:

`step.maths.org/questions/92-s2-q4`

도입

미분(differentiation)이란 무엇인가? 학교에서는 미분을 극한(limit) $\lim_{h\to 0} \frac{f(x+h)-f(x)}{h}$로 정의하고, 그다음 여러 규칙을 배운다. 합의 도함수(derivative)는 도함수의 합이라는 규칙, 곱의 미분법(product rule) 등이다. 이 문제는 이 순서를 뒤집는다. 극한은 완전히 잊어버리자. 어떤 연산에 대해 아는 것이라고는 그 연산이 합의 법칙, 곱의 법칙, 상수에 관한 법칙을 따르고 x를 1로 보낸다는 사실뿐이라고 하자. 그러면 이 문제가 보여 주듯이, 적어도 다항식(polynomial)에서는 그 연산이 **반드시** 미분이어야 한다.

이것이 미적분을 바라보는 대수학자의 관점이다. 연산은 공식이 아니라 그 연산이 따르는 규칙으로 특징지어진다. 곱의 법칙을 따르는 연산을 **도분**(derivation)이라고 하며, 도분은 대수학, 기하학, 물리학 곳곳에 등장한다. 놀랍게도 같은 아이디어가 현대의 기계 학습 시스템을 훈련시키는 소프트웨어 안에서도 작동하고 있다.

시작하기 전에

생각해 보기 규칙 (i)은 곱의 법칙이다. 곱의 법칙이 어떻게 상수에 대해 무언가를 알려 줄 수 있을까? (상수를 곱으로 생각해 보자.)

수 1은 1×1과 같다. 1×1에 곱의 법칙을 적용하면 $\Diamond 1$을 자기 자신과 연결하는 관계식이 나오고, 이 관계식 때문에 그 값은 o일 수밖에 없다. 일반적으로 이런 공리(axiom)를 다룰 때의 요령은 영리하게 고른 간단한 입력에 공리를 적용하는 것이다.

차근차근 풀기

1단계 상수

생각해 보기 $\mathrm{f} = \mathrm{g} = 1$로 놓고 규칙 (i)을 적용하라. 그다음 다른 상수에 대해서는 규칙 (iv)를 사용하라.

$\Diamond 1 = \Diamond(1 \cdot 1) = 1 \cdot \Diamond 1 + 1 \cdot \Diamond 1 = 2\Diamond 1$이므로 $\Diamond 1 = 0$이다. 임의의 상수 λ에 대해 규칙 (iv)에 의해 $\Diamond \lambda = \Diamond(\lambda \cdot 1) = \lambda \Diamond 1 = 0$이다. ■

2단계 거듭제곱

규칙 (iii)을 사용하면 $\Diamond x^2 = \Diamond(x \cdot x) = x\Diamond x + x\Diamond x = 2x$이다. 그러면

$$\Diamond x^3 = \Diamond(x^2 \cdot x) = x\Diamond x^2 + x^2\Diamond x = x \cdot 2x + x^2 = 3x^2.$$

잠깐, 직접 해 보기 모든 양의 정수 n에 대해 $\Diamond x^n = nx^{n-1}$임을 수학적 귀납법(induction)으로 증명하라.

$n = 1$인 경우는 규칙 (iii)이다. $\Diamond x^n = nx^{n-1}$이면

$$\Diamond x^{n+1} = \Diamond(x^n \cdot x) = x\Diamond x^n + x^n\Diamond x = x \cdot nx^{n-1} + x^n = (n+1)x^n. \quad ■$$

3단계 모든 다항식

일반적인 다항식은 $\mathrm{h}(x) = a_0 + a_1 x + \cdots + a_m x^m$이다. 규칙 (ii)를 (반복해서) 적용하고 규칙 (iv)를 적용하면

$$\begin{aligned}\Diamond \mathrm{h}(x) &= \Diamond a_0 + a_1\Diamond x + a_2\Diamond x^2 + \cdots + a_m\Diamond x^m \\ &= a_1 + 2a_2 x + \cdots + m a_m x^{m-1} = \mathrm{h}'(x). \quad ■\end{aligned}$$

돌아보기

- **공리가 연산을 결정한다.** 극한은 전혀 언급하지 않은 네 개의 규칙만으로 다항식 위에서 $\Diamond$가 완전히 결정되었다.
- **생성원(generators).** 모든 다항식은 상수와 x로부터 덧셈과 곱셈을 써서 만들어진다. 기본 재료에 대해 $\Diamond$가 무엇을 하는지, 그리고 만드는 연산과 어떻게 어우러지는지를 알면 모든 곳에서 그 값이 결정된다.

▶ **구성을 따라가는 귀납법.** 증명은 다항식이 만들어지는 방식을 그대로 따라갔다. 먼저 곱셈을 반복해 거듭제곱을 다루고, 그다음 합을 다루었다.

숨은 수학

도분

어떤 대수적 체계 위의 연산 D가 덧셈을 보존하고 곱의 법칙 $D(fg) = fD(g) + gD(f)$를 만족하면, 이를 **도분**이라고 한다. 이 문제는 다항식 위에서 상수를 0으로 보내는 도분이 $D(x)$에 의해 완전히 결정된다는 것을 보여 준다. 실제로 $D(h) = h'(x)\,D(x)$이므로, 남은 자유는 다항식 $D(x)$를 고르는 것뿐이다. 규칙 (iii)은 $D(x) = 1$로 정한다. 도분은 수학 전반에 나타난다. 기하학에서는 곡면 위의 **벡터장**(vector field)을 그 곡면 위의 함수들에 작용하는 도분으로 정의할 수 있다(벡터장은 함수를 그 장의 방향으로 미분한다). 대수학에서는 어떤 구조의 도분이 그 구조의 "무한소 대칭"을 측정한다. 물리학에서는 양자역학의 교환자(commutator) $[A, B] = AB - BA$가 각 변수에 대해 도분이다.

극한 없는 미적분

대수적인 도함수는 극한이 전혀 의미가 없는 상황에서도 작동한다. 소수 p를 법으로 하는 산술과 같은 유한체(finite field) 위에서는 극한이 없지만, 다항식의 형식적 도함수(formal derivative)는 같은 규칙으로 정의되며 여전히 중근(repeated root)을 찾아낸다. 다항식 f가 중근을 가질 필요충분조건은 f와 f'이 공통인수를 가지는 것이다. 예를 들어 $p \nmid n$일 때 $x^n - 1$이 중근을 갖지 않음을 이런 방법으로 보이며, 이 사실은 Section 6.1의 원분다항식(cyclotomic polynomial)을 유한체 위에서 정의하는 데 필요하다. 같은 아이디어가 부호이론(coding theory)과 암호학(cryptography)에서도 쓰인다.

자동 미분

현대적인 응용을 하나 살펴보자. $\varepsilon^2 = 0$이지만 $\varepsilon \neq 0$인 수 ε을 새로 만들어 내고, **이원수**(dual numbers) $a + b\varepsilon$으로 산술을 한다. 그러면 $(a + b\varepsilon)(c + d\varepsilon) = ac + (ad + bc)\varepsilon$이다. 즉 ε 부분은 정확히 곱의 법칙을 따른다. 따라서 임의의 다항식에 대해

$$f(x + \varepsilon) = f(x) + f'(x)\,\varepsilon,$$

이고, f에 이원수 $x + \varepsilon$을 대입하여 계산하면 함숫값과 미분계수가 동시에, 정확하게 계산된다. 극한도 필요 없고, 작은 차이에서 생기는 반올림 오차도 없다(그림 6.5.1). 이를 **전진 모드 자동 미분**(forward-mode automatic differentiation)이라고 한다. 그 사촌인 후진 모드는 수십억 개의 매개변수를 가진 신경망(neural network)을 훈련시키는 데 쓰이는 알고리즘(**역전파**(backpropagation))이다. 이런 시스템이 학습할 때마다, 시스템은 곱의 법칙

과 연쇄법칙(chain rule)을 도분으로서 한 단계씩 적용하고 있는 것이다.

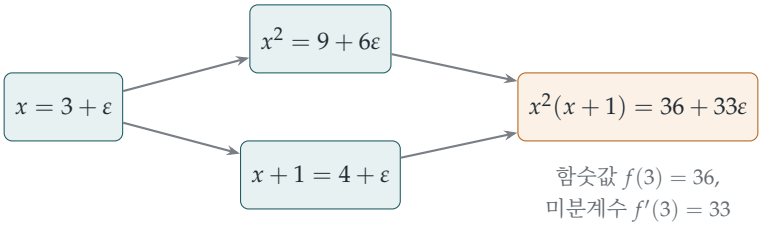


그림 6.5.1 $f(x) = x^2(x+1)$의 $x = 3$에서의 이원수($\varepsilon^2 = 0$)를 이용한 자동 미분. 각 단계는 이 문제의 규칙을 따른다. $(3+\varepsilon)^2 = 9 + 6\varepsilon$이고, $(9+6\varepsilon)(4+\varepsilon) = 36 + (9+24)\varepsilon$이다. ε의 계수는 $f'(3) = 3\cdot 9 + 2\cdot 3 = 33$이며, 정확하게 계산된다.

사고 기술

성질로 특징짓기

연산을 그것이 따르는 규칙으로 기술한 다음, 그 규칙이 연산을 유일하게 결정함을 보여라.

이것이 대학 대수학의 중심인 공리적 방법(axiomatic method)이다. 이 방법의 힘은 공리로부터 증명한 모든 것이 그 공리를 만족하는 모든 연산에 적용된다는 데 있다. 그것이 다항식의 미분이든, 곡면 위 함수의 미분이든, 아직 발명되지 않은 무언가이든 마찬가지이다.

더 도전하기

1 **다른 도분.** $\Diamond$가 규칙 (i), (ii), (iv)를 만족하되, 1 대신 $\Diamond x = x$라고 하자. $\Diamond \mathrm{h}(x) = x\,\mathrm{h}'(x)$임을 보여라. $\Diamond$는 x^n을 무엇으로 보내는가?

2 **몫의 미분법.** 규칙 (i)이 여전히 성립한다고 가정하고 $\Diamond$를 유리함수(rational function) f/g로 확장하라. $\mathrm{g}\cdot\frac{\mathrm{f}}{\mathrm{g}} = \mathrm{f}$에 규칙 (i)을 적용하여 몫의 미분법(quotient rule)을 유도하라.

3 **중근.** $(x-a)^2$이 다항식 f를 나누면 $x-a$가 f'을 나눔을 보여라. 이를 이용하여 $x^n - 1$이 중근을 갖지 않음을 보여라.

4 **이원수.** 이원수를 이용하여 $f(x) = (x^2 + 1)^3$에 대해 $f(2)$와 $f'(2)$를 계산하고, 연쇄법칙으로 검산하라.

더 읽을거리

- **Peter Cameron, *Introduction to Algebra*** (Oxford University Press). 대학 1학년 수준에서 환, 다항식, 체를 다루며 형식적 도함수도 소개한다.
- **Andreas Griewank & Andrea Walther, *Evaluating Derivatives*** (SIAM). 자동 미분에 관한 표준 참고서이다. 고급 수준.
- **Michael Nielsen, *Neural Networks and Deep Learning*** (온라인 무료 공개). 2장에서 역전파를 명쾌하게 설명한다.

6.6 부분군의 합집합

문제

STEP II 1988, 9번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:

`step.maths.org/questions/88-s2-q9`

도입

이 문제는 이 책에서 가장 짧은 문제 가운데 하나이면서, 대학 수학의 성격을 가장 잘 보여 주는 문제 가운데 하나이다. 이 문제는 대칭을 다루는 수학의 언어인 **군**(group)에 관한 것이다. 그리고 퍼즐처럼 들리는 질문을 던진다. 군 안에 들어 있는 더 작은 군 두 개로 그 군 전체를 덮을 수 있을까? 답은 "아니다"이고, 증명은 세 줄이면 된다. 그런데 더 작은 군 세 개로는 덮을 수 있다. 이는 뜻밖의 사실이다.

군론(group theory)은 2019년까지 STEP 출제 범위에 들어 있었고, 지금은 대학 1학년 과정의 기본 내용이다. 이 문제를 풀려면 아래에 제시한 정의만 알면 된다. 그리고 이 문제는 군론 학자들이 어떻게 생각하는지를 처음 맛보기에 안성맞춤이다. 공리만을 사용하는 짧고 영리한 논증이기 때문이다.

시작하기 전에

군이란 다음 조건을 만족하는 연산(곱셈처럼 ab로 쓴다)이 주어진 집합 G이다.

- 연산이 **결합법칙**(associative)을 만족한다. 즉 $(ab)c = a(bc)$이다.
- 모든 a에 대하여 $ea = ae = a$인 **항등원**(identity) e가 존재한다.
- 모든 a에 대하여 $aa^{-1} = a^{-1}a = e$인 **역원**(inverse) a^{-1}가 존재한다.

예를 들어 덧셈에 대한 정수(양수, 음수, 0) 전체, 곱셈에 대한 0이 아닌 실수 전체, 합성에 대한 정사각형의 회전 전체는 모두 군이다. **부분군**(subgroup)이란 G의 부분집합 K로서 같은 연산에 대하여 그 자체로 군이 되는 것이다. 즉 K는 e를 포함하고, $a, b \in K$이면 $ab \in K$이

고 $a^{-1} \in K$이다.

> **생각해 보기** K가 부분군이고 $a \in K$이지만 $b \notin K$일 때, ab가 K에 속할 수 있을까?

그럴 수 없다. $ab \in K$이면 $b = a^{-1}(ab)$는 K의 두 원소의 곱이므로 K에 속하게 된다. 이 작은 관찰이 증명의 전부이다.

차근차근 풀기

1단계 부분군 두 개로는 덮을 수 없다

모순을 이끌어 내기 위해, $G = G_1 \cup G_2$이지만 G_1과 G_2 모두 G 전체가 아니라고 가정하자.

> **생각해 보기** $G_1 \neq G$이므로 G_1에 속하지 않는 원소가 있다. 그 원소는 어디에 있어야 할까? G_2에 대해서도 마찬가지로 생각해 보자. 이제 두 원소를 곱해 보자.

$a \notin G_1$인 $a \in G$를 고르자. 모든 원소는 G_1이나 G_2에 속하므로 $a \in G_2$이다. 또 $b \notin G_2$인 $b \in G$를 고르면 $b \in G_1$이다. 곱 ab를 생각하자. 이 곱은 G_1이나 G_2에 속한다.

- $ab \in G_1$인 경우: $b \in G_1$이므로 $a = (ab)b^{-1} \in G_1$이다. 모순이다.
- $ab \in G_2$인 경우: $a \in G_2$이므로 $b = a^{-1}(ab) \in G_2$이다. 모순이다.

어느 경우든 모순에 이르므로 $G_1 = G$이거나 $G_2 = G$이다. ∎

G가 유한하다는 사실은 한 번도 사용하지 않았다는 점에 주목하자. 이 결과는 모든 군에서 성립한다.

2단계 부분군 세 개로는 덮을 수 있다

> **잠깐, 직접 해 보기** 세 부분군의 합집합이 되는 군을 찾아라. 단, 세 부분군 가운데 어느 것도 군 전체가 아니어야 한다. (**힌트:** 모든 원소가 자기 자신의 역원인 작은 군을 시도해 보라.)

클라인 4원군(Klein four-group) $V = \{e, a, b, c\}$를 생각하자. 연산 규칙은 $a^2 = b^2 = c^2 = e$이고 $ab = ba = c$, $bc = cb = a$, $ca = ac = b$이다. (구체적으로는 정사각형이 아닌 직사각형의 네 가지 대칭, 즉 아무것도 하지 않기, 180° 회전, 두 축 각각에 대한 대칭이동이다. 또는 비트 0, 1로 이루어진 순서쌍 (x, y) 전체에 법 2에 대한 덧셈을 준 것이라 해도 된다.) 이 군의 세 부분군

$$H_1 = \{e, a\}, \qquad H_2 = \{e, b\}, \qquad H_3 = \{e, c\}$$

은 각각 원소가 두 개이고, 어느 것도 군 전체가 아니며, 이들을 합하면 V의 모든 원소를 포

함한다(그림 6.6.1). ■

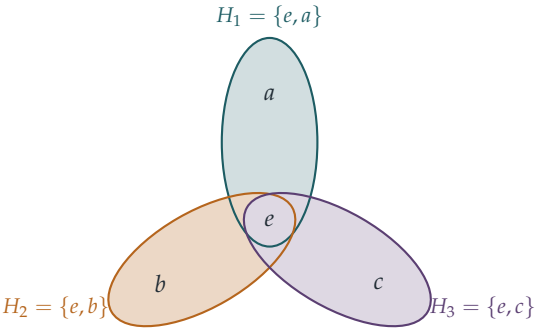


그림 6.6.1 클라인 4원군 $\{e, a, b, c\}$는 위수(order)가 2인 세 부분군의 합집합이며, 이 부분군들은 항등원 e에서만 겹친다. 문제의 첫 부분에 따르면, 어떤 군도 진 부분군(proper subgroup) 두 개만의 합집합이 될 수는 없다.

돌아보기

- **증거가 되는 원소를 골라 결합하라.** 증명에서는 각 부분군 밖에 있는 원소를 하나씩 골라 곱했다. 이렇게 "각각에서 하나씩 골라 결합하는" 방법은 대수학에서 매우 자주 쓰인다.
- **닫혀 있음은 강력하다.** 부분군의 성질 가운데 사용한 것은 곱셈과 역원에 대하여 닫혀 있다(closed)는 것뿐이었다.
- **필요한 가정을 확인하라.** 유한하다는 조건은 주어졌지만 사용하지 않았다. 어떤 가정이 불필요하다는 것을 알아차리는 것도 증명을 이해하는 일의 일부이다.

숨은 수학

대칭의 언어

군은 19세기에 여러 방향에서 동시에 생겨났다. 다항식의 근의 치환에 대한 갈루아(Galois)의 연구(Section 6.4), 치환에 관한 코시(Cauchy)의 연구, 그리고 기하학과 결정학에서의 대칭 연구가 그것이다. 세 공리를 만족하는 것이면 무엇이든 군이라고 하는 위의 추상적인 정의는 19세기 말에 자리 잡았다. 이 정의의 힘은 일반성에 있다. 이 문제의 정리처럼 공리로부터 증명한 정리는 수의 군, 행렬의 군, 대칭의 군, 치환의 군에서 동시에 성립한다. 오늘날 군은 어디에나 있다. 입자물리학(표준 모형은 대칭군 위에 세워져 있다), 화학(분자의 대칭이 스펙트럼을 결정한다), 암호학(타원곡선 군, Section 1.9), 그리고 루빅스 큐브 풀이에도 군이 쓰인다.

부분군이 몇 개 필요할까?

이 문제에서 자연스러운 질문이 떠오른다. 합집합이 군 전체가 되는 진부분군의 최소 개수는 얼마일까? 이 문제에 따르면 그 수는 결코 2가 아니다. 1926년에 Gaetano Scorza는 군이 세 진부분군의 합집합이 될 필요충분조건이 클라인 4원군을 "몫군(quotient)"으로 가지는 것임을 보였다. 1994년에 J. H. E. Cohn은 일반적인 문제를 연구하여 여러 결과를 추측하였고, 1997년에 M. J. Tomkinson은 3부터 6까지의 모든 수는 이 최소 개수로 나타나지만, 이 최소 개수가 7인 군은 존재하지 않음을 증명하였다. 이처럼 진술은 간단하지만 놀랄 만큼 미묘한 질문은 군론의 전형적인 모습이다.

벡터 공간

비슷한 논증으로, 실수 위의 벡터 공간(vector space)(평면이나 3차원 공간 같은 것)은 결코 유한 개의 진부분공간(proper subspace)의 합집합이 될 수 없음을 보일 수 있다. 즉 평면은 원점을 지나는 유한 개의 직선의 합집합이 아니다. 그러나 유한체(finite field) 위에서는 가능하다. 원소가 두 개인 체 위의 평면은 바로 클라인 4원군이며, 이는 세 직선의 합집합이다.

사고 기술

공리로부터 논증하라

추상대수학에서는 대상이 만족하는 공리 말고는 그 대상에 대해 아무것도 모를 때가 많다. 증명은 그 공리만을 사용해야 한다.

그 때문에 논증은 여기서처럼 짧고 깔끔해질 수밖에 없고, 어디에나 적용할 수 있게 된다. 익숙해지는 데 시간이 걸리며, 이는 대학 1학년 대수학 강의에서 겪는 가장 독특한 경험 가운데 하나이다.

더 도전하기

1 **군인지 확인하기.** 클라인 4원군의 곱셈표를 작성하고 군의 공리를 확인하라. 이 군이 곱셈에 대한 군 $\{1, i, -1, -i\}$와 같지 않음을 보여라. (**힌트:** 자기 자신의 역원인 원소는 어느 것인가?)

2 **순환군.** 모든 원소가 한 원소 g의 거듭제곱일 때 그 군을 **순환군**(cyclic group)이라 한다. 순환군은 진부분군을 몇 개 쓰더라도 그 합집합이 될 수 없음을 보여라. (**힌트:** g를 포함하는 부분군은 어느 것인가?)

3 **정수.** $(\mathbb{Z}, +)$가 부분군 $2\mathbb{Z}$(짝수 전체)와 $3\mathbb{Z}$(3의 배수 전체)의 합집합이 아님을 직접 보여라. 이 군은 어떤 두 진부분군의 합집합이 될 수 있는가?

4 **평면 위의 직선.** 심화평면 $\mathbb{R}^2$가 원점을 지나는 유한 개의 직선의 합집합이 아님을 보여라. (힌트: 각 직선은 원점을 제외하면 포물선 $y = x^2$ 위의 점을 많아야 하나 포함한다.)

더 읽을거리

- **M. A. Armstrong, *Groups and Symmetry*** (Springer). 『군과 대칭』. 기하학적 예를 중심으로 전개하며 그림이 아름다운 입문서이다.
- **Nathan Carter, *Visual Group Theory*** (Mathematical Association of America). 『시각적 군론』. 그림으로 군을 배우는 책으로, 대학 입학 전에 읽기에 이상적이다.
- **Peter Neumann, Gabrielle Stoy & Edward Thompson, *Groups and Geometry*** (Oxford University Press). 『군과 기하학』. 옥스퍼드 대학 1학년 과정의 고전적인 교재이다.

6.7 사원수군

문제

STEP III 1993, 5번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:

`step.maths.org/questions/93-s3-q5`

도입

1843년 10월 16일, 윌리엄 로언 해밀턴(William Rowan Hamilton)은 아내와 함께 더블린의 로열 운하를 따라 걷다가, 여러 해 동안 좇던 영감을 번뜩 얻었다. 그는 복소수(complex numbers)가 수의 쌍을 곱하듯이 수의 세 쌍을 곱하는 방법을 찾으려 했지만 번번이 실패했다. 그런데 갑자기 답이 보였다. 수가 네 개 필요하고, 곱하는 순서가 중요한 곱셈, 즉 $ij \neq ji$인 곱셈이 필요하다는 것이었다. 그는 브룸 다리(Brougham Bridge)의 돌에 다음 규칙을 새겼다.

$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{ijk} = -1.$$

이것이 바로 **사원수**(quaternions)이다. 이 문제는 복소수의 쌍으로 사원수를 만들고, 그 안에서 뒤틀린 곱셈을 가진 원소 여덟 개짜리 작은 군을 찾아낸다. 오늘날 사원수는 모든 컴퓨터 게임, 비행 시뮬레이터, 우주선 유도 장치에서 3차원 회전을 기술하는 데 쓰인다.

시작하기 전에

군의 정의는 Section 6.6를 보라. 용어 두 가지를 더 알아 두자. 군(group)의 원소 g의 **위수**(order)는 $g^n = e$를 만족하는 가장 작은 양의 정수 n이다. 그리고 두 군 사이에 연산을 보존하는 일대일 대응(one-to-one correspondence)이 있으면 두 군은 **동형**(isomorphic)이라고 한다. 즉 두 군은 "이름표만 다른 같은 군"이다.

? **생각해 보기** 쌍 (z_1, z_2)를 "수" $z_1 + z_2\mathrm{j}$를 나타내는 것으로 생각하자. 여기서 j는 $\mathrm{j}^2 = -1$이고 복소수 w에 대하여 $\mathrm{j}w = w^*\mathrm{j}$를 만족하는 새로운 기호이다. 이 규칙을 써서 $(z_1 + z_2\mathrm{j})(w_1 + w_2\mathrm{j})$를 곱해 보라. ∘의 공식이 나오는가?

$(z_1 + z_2\mathrm{j})(w_1 + w_2\mathrm{j}) = z_1w_1 + z_1w_2\mathrm{j} + z_2\mathrm{j}w_1 + z_2\mathrm{j}w_2\mathrm{j} = z_1w_1 + z_1w_2\mathrm{j} + z_2w_1^*\mathrm{j} + z_2w_2^*\mathrm{j}^2$이고, 이는 $(z_1w_1 - z_2w_2^*) + (z_1w_2 + z_2w_1^*)\mathrm{j}$이다. 그렇다. 연산 $\circ$는 변장한 사원수 곱셈이다.

차근차근 풀기

1단계 행렬을 이용한 결합법칙

$(a \circ b) \circ c = a \circ (b \circ c)$를 직접 확인하려면 계산이 길다. 더 깔끔한 방법이 있다.

> **생각해 보기** (z_1, z_2)에 복소 행렬 $M = \begin{pmatrix} z_1 & z_2 \\ -z_2^* & z_1^* \end{pmatrix}$를 대응시키자. 행렬의 곱 $M(z_1, z_2)\,M(w_1, w_2)$의 첫째 행은 무엇인가?

곱의 첫째 행은 $(z_1w_1 - z_2w_2^*,\ z_1w_2 + z_2w_1^*)$로 정확히 $(z_1, z_2) \circ (w_1, w_2)$이고, 둘째 행은 $(-(z_1w_2 + z_2w_1^*)^*,\ (z_1w_1 - z_2w_2^*)^*)$이므로 곱도 같은 특수한 꼴이다. 따라서 $M(a \circ b) = M(a)M(b)$이다. 행렬의 곱셈은 결합법칙을 만족하고, M은 일대일이므로(첫째 행에서 z_1, z_2를 읽어 낼 수 있다) $\circ$는 결합법칙(associativity)을 만족한다. ■

2단계 교환법칙이 성립하지 않음

$(0,1) \circ (\mathrm{i}, 0) = (0 \cdot \mathrm{i} - 1 \cdot 0,\ 0 \cdot 0 + 1 \cdot \mathrm{i}^*) = (0, -\mathrm{i})$이지만 $(\mathrm{i}, 0) \circ (0, 1) = (0, \mathrm{i})$이다. 따라서 $\circ$는 교환법칙(commutative law)을 만족하지 않는다.

네 가지 특수한 곱은 정의에서 바로 나온다.

$$(z,0) \circ (w,0) = (zw, 0), \qquad (z,0) \circ (0,w) = (0, zw),$$
$$(0,z) \circ (w,0) = (0, zw^*), \qquad (0,z) \circ (0,w) = (-zw^*, 0).$$

3단계 원소 여덟 개의 군

사원수 표기로 쓰면 $A = 1$, $C = \mathrm{i}$, $B = \mathrm{j}$, $D = \mathrm{ij} = \mathrm{k}$이고, E, G, F, H는 각각 이들의 음수이다. S_1의 모든 원소는 $u \in \{1, \mathrm{i}, -1, -\mathrm{i}\}$에 대하여 $(u, 0)$ 또는 $(0, u)$ 꼴이다.

> **생각해 보기** 네 가지 특수한 곱을 이용하여 S_1이 닫혀 있음을 보여라. 항등원은 무엇인가?

네 가지 특수한 곱에 의해, $(u, 0)$ 또는 $(0, u)$ 꼴인 두 원소의 곱은 다시 이 두 꼴 가운데 하나이고, 그 첫째 또는 둘째 성분은 uv, uv^* 또는 $-uv^*$이다. $\{1, \mathrm{i}, -1, -\mathrm{i}\}$는 곱셈, 켤레(conjugation), 부호 바꾸기에 대하여 닫혀 있으므로(closed), 그 곱은 S_1에 속한다. 항등원(identity)은 $A = (1, 0)$이다. $(1,0) \circ (w_1, w_2) = (w_1, w_2)$이고 $(w_1, w_2) \circ (1,0) =$

(w_1, w_2)이기 때문이다.

> **잠깐, 직접 해 보기** 각 원소의 위수와 역원을 구하라.

A의 위수는 1이다. $E \circ E = (-1,0) \circ (-1,0) = (1,0)$이므로 E의 위수는 2이다. $C = (\mathrm{i}, 0)$에 대하여 $C \circ C = (-1,0) = E$이므로 C의 위수는 4이고 $C^{-1} = C^3 = E \circ C = G$이다. $B = (0,1)$에 대하여 $B \circ B = (-1 \cdot 1^*, 0) = (-1,0) = E$이므로 B의 위수는 4이고 $B^{-1} = F$이다. 마찬가지로 $D \circ D = (-\mathrm{i} \cdot \mathrm{i}^*, 0) = (-\mathrm{i} \cdot (-\mathrm{i}), 0) = (-1,0) = E$이므로 D의 위수는 4이고 역원은 H이다. 그리고 G, F, H는 C, B, D의 역원(inverse)이며 위수는 역시 4이다. 정리하면 다음과 같다.

원소	A	B	C	D	E	F	G	H
역원	A	F	G	H	E	B	C	D
위수	1	4	4	4	2	4	4	4

닫혀 있고, 결합법칙(1단계)을 만족하며, 항등원과 역원이 있으므로 S_1은 군이다. ■이 군을 사원수군(quaternion group) Q_8이라고 한다.

4단계 부분군

$\{A, B, E, F\} = \{1, \mathrm{j}, -1, -\mathrm{j}\}$는 B의 거듭제곱으로 이루어져 있다. $B^1 = B$, $B^2 = E$, $B^3 = F$, $B^4 = A$이다. 따라서 이 집합은 닫혀 있고 역원을 포함하므로 부분군(subgroup)이며, 위수가 4인 순환군(cyclic group)이다. 행렬 $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$는 $J^2 = -I$, $J^3 = -J$, $J^4 = I$를 만족하므로 역시 위수가 4인 순환군을 생성한다. $B^k \leftrightarrow J^k$로 대응시키면 동형사상이 된다. ■(사실 J는 정확히 $M(0,1)$, 즉 B의 행렬이다.)

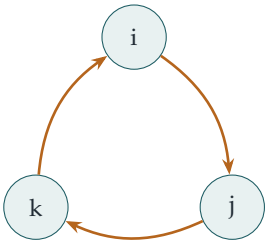
돌아보기

- **행렬로 표현하라.** 직접 확인하기 고통스러운 결합법칙을 행렬 곱셈으로부터 물려받았다.
- **공식 뒤에 숨은 구조를 찾아라.** 낯선 연산 $\circ$는 사원수 곱셈이었고, 이를 알아차리자 모든 것이 쉬워졌다.
- **위수와 역원은 군을 묘사한다.** 위수 표만 보아도 Q_8이 특이하다는 것을 알 수 있다. 위수가 2인 원소는 하나뿐이고 위수가 4인 원소는 여섯 개이다.

숨은 수학

복소수 너머

실수는 덧셈, 곱셈, 나눗셈을 할 수 있는 1차원 수 체계를 이루고, 복소수는 2차원 수 체계를 이룬다. 해밀턴의 사원수는 4차원이며 여전히 나눗셈을 할 수 있지만, 곱셈은 더 이상 교환법칙을 만족하지 않는다(그림 6.7.1). 1878년 프로베니우스(Ferdinand Frobenius)는 $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$(해밀턴의 머리글자) 이 세 가지가 실수 위의 유한 차원 "나눗셈 대수"(division algebra) 가운데 곱셈이 결합법칙을 만족하는 유일한 것임을 증명했다. 결합법칙을 포기하되, 실수, 복소수, 사원수에서처럼 크기가 곱셈적인 성질 $|xy| = |x|\,|y|$를 유지하면 정확히 하나가 더 있다. 1840년대에 John Graves와 케일리(Arthur Cayley)가 발견한 8차원의 **팔원수**(octonions)이다. 1898년 후르비츠(Adolf Hurwitz)는 이 네 가지가 그러한 체계의 전부임을 증명했다. (크기에 대한 조건을 빼면 이보다 더 기묘한 비결합 나눗셈 대수가 또 있지만, 보트(Raoul Bott), 밀너(John Milnor), 케르베르(Michel Kervaire)가 1958년에 증명한 깊은 정리에 따르면 모든 유한 차원 실수 나눗셈 대수의 차원은 1, 2, 4, 8 중 하나이다.)



화살표 방향: $\mathrm{ij} = \mathrm{k}$, $\mathrm{jk} = \mathrm{i}$, $\mathrm{ki} = \mathrm{j}$

반대 방향: $\mathrm{ji} = -\mathrm{k}$, $\mathrm{kj} = -\mathrm{i}$, $\mathrm{ik} = -\mathrm{j}$

그리고 $\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1$

그림 6.7.1 해밀턴의 곱셈 규칙. i, j, k 중 두 개를 화살표 방향으로 곱하면 나머지 하나가 되고, 화살표 반대 방향으로 곱하면 나머지 하나에 음의 부호를 붙인 것이 된다. 여덟 개의 원소 $\pm 1, \pm\mathrm{i}, \pm\mathrm{j}, \pm\mathrm{k}$는 이 문제의 사원수군 Q_8을 이룬다.

3차원의 회전

절댓값이 1인 사원수는 3차원 공간의 회전을 나타낸다. 단위 축 $\mathbf{u}$를 중심으로 각 θ만큼 회전하는 것은 $q = \cos\frac{\theta}{2} + \sin\frac{\theta}{2}(u_1\mathrm{i} + u_2\mathrm{j} + u_3\mathrm{k})$에 대응하고, 이는 벡터 $\mathbf{v}$($v_1\mathrm{i} + v_2\mathrm{j} + v_3\mathrm{k}$로 쓴다)에 $\mathbf{v} \mapsto q\mathbf{v}q^{-1}$로 작용한다. 회전을 합성하는 것은 사원수를 곱하는 것이다. 이 방법은 행렬이나 각을 쓰는 것보다 효율적이고 수치적으로 안정적이며, "짐벌 잠금"(gimbal lock)을 피할 수 있다. 짐벌 잠금은 자유도 하나를 잃는 현상으로, 아폴로 우주비행사들은 자이로스코프 기반 항법 장치를 쓰면서 이 문제를 피해 가야 했다. 반각 $\frac{\theta}{2}$는 깊은 사실에 대한 단서이기도 하다. 360°만큼 회전하면 1이 아니라 $q = -1$이 되는데, 물리학자들은 이 사실을 전자의 행동(스핀(spin))에서 관찰한다.

네 제곱수

사원수의 절댓값은 복소수의 절댓값과 마찬가지로 곱셈적이다. 즉 $|pq| = |p||q|$이다. 이를 풀어 쓰면 오일러(Euler)의 **네 제곱수 항등식**(four-square identity)을 얻는다. 네 제곱수의 합 두 개의 곱은 그 자체로 네 제곱수의 합이라는 것이다. 이는 모든 양의 정수가 네 제곱수의 합이라는 라그랑주(Lagrange)의 정리에서 핵심 단계이다. 이 정리는 Section 7.8에서 증명하며, Section 1.6의 두 제곱수 결과의 4차원 사촌이다.

사고 기술

추상적인 대상을 구체적으로 표현하라

추상적인 연산을 다루기 어렵다면, 그 연산이 익숙한 연산이 되는 행렬 같은 구체적인 모형을 찾아라.

그러면 결합법칙 같은 성질은 저절로 따라온다. 군을 행렬로 표현하여 연구한다는 이 아이디어는 **표현론**(representation theory)이라는 크고 아름다운 분야로 자라난다.

더 도전하기

1 **해밀턴의 규칙.** 쌍을 이용하여 $C \circ B = D$이고 $B \circ C = H$임을, 즉 $\mathrm{ij} = \mathrm{k}$이고 $\mathrm{ji} = -\mathrm{k}$임을 확인하라.

2 **위수가 2인 원소는 하나뿐.** Q_8에서 위수가 2인 원소는 $E = -1$뿐임을 보여라. 이로부터 Q_8이 정사각형의 대칭군(위수가 2인 원소가 다섯 개이다)과 동형이 아님을 보여라.

3 **네 제곱수.** $\det M(z_1, z_2) = |z_1|^2 + |z_2|^2$임을 보여라. $\det(M_1 M_2) = \det M_1 \det M_2$를 이용하여, 네 제곱수의 합 두 개의 곱이 네 제곱수의 합임을 보여라.

4 **부분군.** Q_8의 부분군을 모두 구하라. $\{A\}$가 아닌 모든 부분군은 E를 포함함을 보이고, Q_8이 위수가 4인 세 순환 부분군의 합집합임을 보여라(Section 6.6와 비교해 보라).

더 읽을거리

- **John Conway & Derek Smith, *On Quaternions and Octonions*** (A. K. Peters). 사원수와 팔원수의 기하학과 산술을 다룬다. 수준이 높지만 매혹적이다.
- **John Baez, "The octonions"**, *Bulletin of the American Mathematical Society* 39 (2002); 온

라인에서 무료로 볼 수도 있다. 훌륭한 개관 논문이며, 서론은 지금 읽어도 이해할 수 있다.

- **Andrew Hanson, *Visualizing Quaternions*** (Morgan Kaufmann). 회전을 위한 사원수를 그래픽스 응용과 함께 다룬다.

6.8 특이행렬로 이루어진 군

문제

STEP III 1996, 6번 문제

더 읽어 나가기 전에 문제부터 읽어 보자. 이 문제는 STEP Support Programme의 문제 데이터베이스에 있다:

`step.maths.org/questions/96-s3-q6`

도입

행렬식(determinant)이 0인 행렬은 역행렬(inverse matrix)을 갖지 않는다는 것은 모든 학생이 배운다. 그렇다면 모든 원소가 역원을 갖는 행렬의 군(group)에는 특이(singular) 행렬이 들어 있을 수 없지 않을까?

들어 있을 수 있다. 함정은 "역원(inverse)"이라는 말에 있다. 군에서 $\mathbf{A}$의 역원은 $\mathbf{A}$와 결합하여 **그 군의** 항등원(identity element)을 만드는 원소이고, 군의 항등원이 반드시 단위행렬 $\mathbf{I}$여야 한다는 조건은 어디에도 없다. 이 문제는 모든 행렬이 특이 행렬인 군을 만들며, 그 군의 항등원은 행렬식이 0인 행렬이다. 이 문제는 정의를 글자 그대로 읽는 법, 그리고 추상적인 구조와 그 구조를 처음 만났을 때의 익숙한 예가 어떻게 다른지를 가르쳐 준다.

시작하기 전에

군의 정의는 Section 6.6을 참고한다.

? **생각해 보기** 소문항 (i)에서 단위행렬 $\mathbf{I}$는 $\begin{pmatrix} a & a \\ a & a \end{pmatrix}$ 꼴이 아니다. 그렇다면 S의 항등원은 무엇일 수 있을까?

그것은 S의 모든 $\mathbf{X}$에 대하여 $\mathbf{EX} = \mathbf{XE} = \mathbf{X}$를 만족하는, S에 속한 어떤 행렬 $\mathbf{E}$여야 한다. 이는 모든 행렬이 아니라 이 특별한 꼴의 행렬에 $\mathbf{E}$가 어떻게 작용하는지에 대한 조건일 뿐이다. 방정식을 풀어서 찾아보자.

차근차근 풀기

1단계 닫힘성

네 성분이 모두 a인 행렬을 $\mathbf{M}_a$라 쓰자. 그러면

$$\mathbf{M}_a\mathbf{M}_b = \begin{pmatrix} a & a \\ a & a \end{pmatrix}\begin{pmatrix} b & b \\ b & b \end{pmatrix} = \begin{pmatrix} 2ab & 2ab \\ 2ab & 2ab \end{pmatrix} = \mathbf{M}_{2ab},$$

이고, $a, b \neq 0$이면 $2ab \neq 0$이다. 따라서 S는 닫혀 있다(closed). ■

2단계 군의 공리

> **생각해 보기** 행렬의 곱셈은 결합법칙을 만족한다. 항등원을 찾으려면 $\mathbf{M}_e\mathbf{M}_a = \mathbf{M}_a$를 풀고, 역원을 찾으려면 $\mathbf{M}_a\mathbf{M}_b = \mathbf{M}_e$를 푼다.

결합법칙(*associativity*)은 행렬의 곱셈에서 그대로 물려받는다. **항등원:** 모든 a에 대하여 $\mathbf{M}_e\mathbf{M}_a = \mathbf{M}_{2ea} = \mathbf{M}_a$가 성립할 필요충분조건은 $e = \tfrac{1}{2}$이다. 공식이 대칭이므로 $\mathbf{M}_a\mathbf{M}_{1/2} = \mathbf{M}_a$도 성립한다. 따라서

$$\mathbf{E} = \begin{pmatrix} \tfrac{1}{2} & \tfrac{1}{2} \\ \tfrac{1}{2} & \tfrac{1}{2} \end{pmatrix}$$

가 S의 항등원이다. **역원:** $b = \tfrac{1}{4a}$이면 $\mathbf{M}_a\mathbf{M}_b = \mathbf{M}_{2ab} = \mathbf{M}_{1/2}$이고 이 b는 0이 아니므로, $\mathbf{M}_{1/(4a)}$가 S에서 $\mathbf{M}_a$의 역원이다. 따라서 S는 군이다. ■모든 원소의 행렬식은 $a^2 - a^2 = 0$이다.

3단계 특이성은 퍼진다

> **잠깐, 직접 해 보기** $\mathbf{A} \in G$가 특이 행렬이라 하고, $\mathbf{B}$를 G의 임의의 원소라 하자. $\mathbf{B}$를 $\mathbf{A}$가 들어간 곱으로 나타낸 다음 행렬식을 취해 보라.

$\mathbf{A}^{-1}$를 군 G에서의 $\mathbf{A}$의 역원(반드시 역행렬일 필요는 없다)이라 하자. 그러면 $\mathbf{C} = \mathbf{A}^{-1}\mathbf{B}$는 G에 속하고

$$\mathbf{AC} = \mathbf{A}\mathbf{A}^{-1}\mathbf{B} = \mathbf{E}\mathbf{B} = \mathbf{B}.$$

이다. 행렬식을 취하면 $\det\mathbf{B} = \det\mathbf{A}\,\det\mathbf{C} = 0$이다. 따라서 G의 모든 원소는 특이 행렬이다. ■특히 행렬군의 한 원소가 행렬로서 가역이면 모든 원소가 가역이다. 즉 행렬군은 모두 가역이거나 모두 특이이다.

4단계 3×3 예

생각해 보기 소문항 (i)을 3×3 행렬로 일반화할 수 있을까? 아니면 세 좌표 중 두 개를 "무시하는" 행렬을 써서 더 간단한 예를 찾을 수 있을까?

다음을 생각하자.

$$G = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} : a \neq 0 \right\}.$$

모서리 성분이 a와 b인 두 행렬의 곱은 모서리 성분이 ab인 행렬이므로 G는 닫혀 있다. 곱셈은 결합법칙을 만족하고, 항등원은 모서리 성분이 1인 행렬이며, 모서리 성분이 a인 행렬의 역원은 모서리 성분이 $\frac{1}{a}$인 행렬이다. 따라서 G는 군이고, 모든 원소의 행렬식은 0이다. ■(또 다른 예: 아홉 성분이 모두 $a \neq 0$인 3×3 행렬들. 이때 항등원은 모든 성분이 $\frac{1}{3}$인 행렬이다.)

돌아보기

- **정의를 글자 그대로 읽는다.** 군의 항등원은 그 군 안에서 항등원 역할을 하는 원소이면 무엇이든 된다. 익숙한 단위행렬일 필요는 없다.
- **구조를 방정식으로 구한다.** S의 항등원과 역원은 추측이 아니라 방정식을 풀어서 찾았다.
- **행렬식은 곱셈적이다.** 이 성질 하나로 특이성이 한 원소에서 모든 원소로 퍼진다는 것을 보였다.

숨은 수학

멱등원과 숨은 가역성

임의의 행렬군의 항등원 $\mathbf{E}$는 $\mathbf{E}^2 = \mathbf{E}$를 만족한다. 즉 **멱등**(*idempotent*)이다. 기하적으로 멱등 행렬은 **사영**(*projection*)이다. 즉 모든 벡터를 어떤 부분공간(subspace) 위로 보내고, 그 부분공간 안의 벡터는 그대로 둔다. 소문항 (i)에서 $\mathbf{E}$는 평면을 직선 $y = x$ 위로 사영하고, 각 행렬 $\mathbf{M}_a$는 먼저 그 직선 위로 사영한 다음 직선을 따라 $2a$배로 늘인다(그림 6.8.1). 직선 위에서 이 군은 가역인 늘이기로 작용하며, 직선에 수직인 방향은 그냥 무시한다. 따라서 S는 실제로는 곱셈에 대한 0이 아닌 실수의 군($\mathbf{M}_a \mapsto 2a$를 통해)이 평면 안의 한 직선 위에 놓여 있는 것이다. 이는 일반적으로도 참이다. 모든 행렬군은 기저 변환(change of basis)을 하고 나면, 항등원의 상(image) 위에 작용하는 가역 행렬들의 군에 0을 덧붙인 것이다.

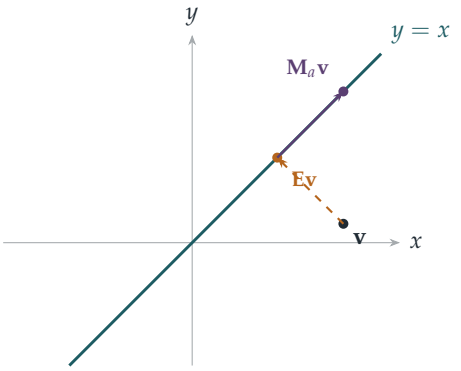


그림 6.8.1 소문항 (i)의 행렬들이 하는 일. 항등원 $\mathbf{E}$는 모든 벡터 $\mathbf{v}$를 직선 $y = x$ 위로 사영한다(호박색, 점선). 각 $\mathbf{M}_a$는 같은 사영을 한 다음 직선을 따라 $2a$배로 늘인다(자주색. 여기서는 $2a = \frac{16}{9}$). 직선 위에서 이 군은 보통의 가역인 배율 변환으로 작용한다.

추상과 구체

사람들이 처음 연구한 군은 치환(permutation), 대칭(symmetry), 가역 행렬처럼 구체적인 것이었다. 추상적인 정의(세 공리(axiom)를 만족하는 연산이 주어진 집합)는 이런 예들로부터 걸러 낸 것이다. 이 문제는 추상적인 관점의 가치를 보여 준다. 하나는 특이 행렬로, 다른 하나는 수로 이루어져 있는데도 S와 곱셈에 대한 0이 아닌 실수의 군은 동형(*isomorphic*)이다. 즉 옷만 다르게 입은 같은 군이다. 겉모습이 다른 두 구조가 언제 "같은지" 알아보는 것은 대수학의 핵심 기술 가운데 하나이며, 동형이라는 개념은 수학자들이 이를 엄밀하게 표현하는 방법이다.

사고 기술

익숙한 대상에 대한 숨은 가정을 의심하라

익숙한 대상이 추상적인 정의 속에 나타나면, 그 대상의 익숙한 성질 가운데 정의가 실제로 요구하는 것이 무엇인지 확인하라.

"행렬군의 항등원은 $\mathbf{I}$이다"라는 말은 당연하게 들리지만 정의의 일부가 아니며, 이 가정을 버리자 진정으로 새로운 예가 나왔다. 이렇게 가정을 의심하는 것이 많은 새로운 수학적 구조가 발견되는 방식이다.

더 도전하기

1 **동형사상.** 사상 $\mathbf{M}_a \mapsto 2a$가 S에서 0이 아닌 실수로의 일대일 대응(one-to-one correspondence)이며, 행렬의 곱셈을 수의 곱셈으로 바꾼다는 것을 보여라.

2 **군이 아닌 경우.** $a \neq 0$인 행렬 $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$의 집합은 곱셈에 대하여 닫혀 있지만 군이 아님을 보여라. (힌트: 항등원을 찾아보라. 좌항등원(left identity)이 있는가? 우항등원(right identity)은?)

3 **멱등 행렬.** $\mathbf{E}^2 = \mathbf{E}$인 2×2 실행렬 $\mathbf{E}$를 모두 구하라. 이들을 기하적으로 설명하라.

4 **모든 성분이 같은 행렬.** 모든 성분이 $a \neq 0$인 $n \times n$ 행렬들이 곱셈에 대하여 군을 이룸을 보이고, 그 항등원을 구하라.

더 읽을거리

- **M. A. Armstrong, *Groups and Symmetry*** (Springer). 행렬군과 동형사상을 많은 기하적 예와 함께 다룬다.
- **Gilbert Strang, *Introduction to Linear Algebra*** (Wellesley-Cambridge). 사영과 멱등 행렬을 명쾌하게 설명한다.
- **Joseph Gallian, *Contemporary Abstract Algebra*** (CRC Press). 특이한 군의 예가 많이 담긴 친절한 입문서이다.

우리가 배운 것

이 장은 방정식을 푸는 일에서 구조를 연구하는 일로 옮겨 간 대수학의 변화와 함께 세 가지 질문으로 시작하였다. 무엇으로부터 무엇을 만들 수 있는가, 방정식의 근의 공식은 왜 성립하는가, 그리고 추상화로 무엇을 얻는가. 이 장의 여덟 문제가 보여 준 것을 정리하면 다음과 같다.

1. 무엇으로부터 무엇을 만들 수 있는가?

Section 6.3에서는 거듭제곱근(radical)을 하나씩 소거하여 $\sqrt{2}+\sqrt{3}$, $\sqrt{2}+\sqrt{3}+\sqrt{5}$, $\sqrt[3]{2}+\sqrt[3]{3}$을 근으로 갖는 다항식을 구하였고, 그 차수는 각각 4, 8, 9였다. 이 차수들은 불변량(invariant), 즉 그 수가 생성하는 체(field)의 차수이다. 체의 탑(tower of fields)을 따라 올라가면 차수가 곱해지므로, 제곱근만으로 도달할 수 있는 수의 차수는 2의 거듭제곱이다. 이 사실 하나로 정육면체의 부피를 두 배로 만드는 작도가 불가능하다는 것($\sqrt[3]{2}$의 차수는 3이다)과 60°인 각을 삼등분할 수 없다는 것이 증명된다.

반대 방향으로, Section 6.2에서는 어떤 것을 실제로 **만들 수 있는** 방법을 보았다. 17제곱하여 1이 되는 1의 거듭제곱근(roots of unity)들을 가우스(Gauss)의 주기(period)로 나누면, 합 $\cos\frac{2\pi}{17}+\cos\frac{4\pi}{17}+\cos\frac{8\pi}{17}+\cos\frac{16\pi}{17}$은 $\frac{-1+\sqrt{17}}{4}$을 근으로 갖는 이차방정식을 만족한다. 이차방정식을 세 번 더 풀면 $\cos\frac{2\pi}{17}$에 이르고, 따라서 정17각형을 작도할 수 있다. 두 절의 바탕에는 Section 6.1의 원분다항식(cyclotomic polynomial)이 있었다. 원분다항식은 1의 거듭제곱근을 위수(order)에 따라 분류하여 얻는 것으로, x^n-1을 이루는 기본 구성 요소이다.

2. 방정식의 근의 공식은 왜 성립하는가?

Section 6.4에서는 사차방정식(quartic)의 비밀을 보았다. 네 근으로부터 세 양 $\alpha\beta+\gamma\delta$, $\alpha\gamma+\beta\delta$, $\alpha\delta+\beta\gamma$를 만드는데, 이는 근을 둘씩 짝짓는 방법 하나마다 하나씩 대응한다. 근을 어떻게 재배열하더라도 이 세 양은 서로 자리만 바뀔 뿐이므로, 이들은 계수를 알 수 있는 삼차방정식을 만족한다. 이 삼차방정식을 풀고 이어서 이차방정식 두 개를 풀면 근이 구해진다. 라그랑주(Lagrange)는 이 방법이 통하는 까닭이 네 대상의 치환(permutation)이 세 가지 짝짓기에 작용하는 방식에 있음을 알아차렸고, 갈루아(Galois)는 다섯 대상의 치환군(group)이 더 이상 쪼갤 수 없는 부분을 포함하기 때문에 근이 다섯 개일 때는 이 방법이 실패함을 알아냈다. 근의 공식은 군 구조의 그림자인 것이다.

3. 추상화로 무엇을 얻는가?

마지막 네 절에서는 대상을 그것이 따르는 규칙으로 기술하였다.

- Section 6.5에서는 네 가지 규칙(가법성(additivity), 곱의 법칙(product rule), 상수에 대한 규칙, $\Diamond x = 1$)만으로, 극한을 전혀 쓰지 않고도 어떤 연산이 미분일 수밖에 없음을 보였다. 같은 규칙이 현대 소프트웨어의 자동미분(automatic differentiation)을 움직인다.
- Section 6.6에서는 군의 공리로부터 세 줄짜리 논증으로, 어떤 군도 두 진부분군(proper subgroup)의 합집합이 될 수 없음을 모든 군에 대해 한꺼번에 보였다.
- Section 6.7에서는 복소수 순서쌍에 대한 낯선 연산이 알고 보니 해밀턴(Hamilton)의 사원수(quaternion) 곱셈이었고, 이를 행렬로 표현하자 결합법칙(associativity)이 저절로 성립하였다.
- Section 6.8에서는 군의 정의를 문자 그대로 읽어 특이행렬(singular matrix)들로 이루어진 군을 만들었다. 이 군의 항등원(identity)은 단위행렬이 아니며, 이 군은 "사실은" 0이 아닌 실수들의 군이 모습을 바꾼 것이다.

각각의 경우에 추상적인 관점은 계산만으로는 가려졌을 무언가를 설명해 주었다.

4. 대수학의 도구 상자

방법	사용한 곳
유일한 불변량에 따른 분류	위수에 따른 1의 거듭제곱근 분류 (6.1)
합과 곱으로 이차방정식 만들기	가우스 주기 (6.2); 사차방정식 (6.4)
곱을 합으로 바꾸는 공식	정17각형 (6.2)
거듭제곱근 소거	최소다항식(minimal polynomial) (6.3)
차수와 탑 법칙(tower law)	작도 불가능성 (6.3)
근의 대칭함수(symmetric function)	분해 삼차방정식(resolvent cubic) (6.4)
공리로 연산 결정하기	도분(derivation) (6.5)
군의 공리로부터 논증하기	부분군의 합집합 (6.6)
행렬 표현(matrix representation)	사원수 (6.7)
동형(isomorphism)	특이행렬군 (6.8)

다음으로

- 사원수는 Section 7.8의 라그랑주의 네 제곱수 정리(four-square theorem)로 이어진다.
- 고유한 규칙을 갖는 대수적 대상으로서의 행렬은 7장의 주제이다.
- 인수분해(factorisation)가 유일하지 않을 수 있는 가우스 정수(Gaussian integer)와 같

은 수 체계의 산술은 Section 1.7의 주제였다.

대학에 가기 전에 더 나아가고 싶다면

- **Mario Livio, *The Equation That Couldn't Be Solved***: 오차방정식(quintic), 갈루아, 그리고 군론의 탄생.
- **Nathan Carter, *Visual Group Theory***: 그림으로 보는 군. 처음 접하기에 이상적이다.
- **M. A. Armstrong, *Groups and Symmetry***: 기하학을 바탕으로 한 대학 첫 강좌.
- **Ian Stewart, *Galois Theory***: 전체 이야기를 받아들일 준비가 되었을 때.

갈루아는 결투 끝에 스무 살의 나이로 세상을 떠났고, 수학계가 이해하는 데 수십 년이 걸린 몇십 쪽의 원고를 남겼다. 그가 본 것은 방정식의 가장 깊은 비밀이 계수에 있는 것이 아니라 해들의 대칭성에 있다는 사실이었다. 서로 다른 것들에 같은 이름을 붙이고 그것들이 공유하는 구조를 연구한다는 이 통찰은 이제 수학 전체에 스며 있다. 여러분은 이 통찰이 다항식, 다각형, 사원수, 행렬에서 작동하는 것을 보았다. 대학에 가면 거의 모든 곳에서 이를 보게 될 것이다.

더 도전하기 해답

여기 실린 것은 완전한 풀이가 아니라 간단한 답과 힌트이다. 결과와 핵심 단계를 제시하므로 자신의 풀이를 확인하는 데 쓸 수 있다. 답을 보기 전에 각 문제를 제대로 풀어 보라.

6.1 근이 모두 단위근인 다항식

1. $(x-1)(x+1) = x^2-1$이고 $(x^2+x+1)(x^2-x+1) = x^4+x^2+1$이며, 이 둘의 곱은 x^6-1이다. 마찬가지로 $x^{12}-1 = (x^6-1)(x^6+1)$이고 $x^6+1 = (x^2+1)(x^4-x^2+1) = \mathrm{C}_4\mathrm{C}_{12}$이다.

2. $2p$의 약수(divisor)는 1, 2, p, $2p$이므로 $\mathrm{C}_{2p} = \frac{x^{2p}-1}{(x-1)(x+1)\mathrm{C}_p(x)} = \frac{x^p+1}{x+1}$이다. 또한 p가 홀수이므로 $\mathrm{C}_p(-x) = \frac{(-x)^p-1}{-x-1} = \frac{x^p+1}{x+1}$이다. $p=3$이면 $\mathrm{C}_6 = x^2-x+1 = \mathrm{C}_3(-x)$이다.

3. p^k 이하의 수 중에서 p^k와 공통인 인수를 갖는 것은 p의 배수 p^{k-1}개이다. 원시 p^k제곱근(primitive p^kth root)은 $x^{p^k}-1$의 근 중에서 $x^{p^{k-1}}-1$의 근이 아닌 것이므로 $\mathrm{C}_{p^k} = \frac{x^{p^k}-1}{x^{p^{k-1}}-1} = \mathrm{C}_p\left(x^{p^{k-1}}\right)$이다. 따라서 $\mathrm{C}_9 = x^6+x^3+1$이다.

4. $\mathrm{C}_{15} = \frac{(x^{15}-1)(x-1)}{(x^3-1)(x^5-1)}$이다. $(x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)$에 주어진 8차식(octic)을 곱하면 $x^{15}-1$이 됨을 전개하여 확인하라.

6.2 가우스의 정17각형

1. $\eta+\eta'$은 실수가 아닌 7제곱근(seventh root) 여섯 개의 합이므로 -1이다. $\eta\eta'$을 전개하면 지수가 $4,6,0,5,0,1,0,2,3 \pmod 7$인 아홉 개의 항 α^{a+b}가 나온다. 즉 1이 세 개이고 실수가 아닌 근이 각각 한 번씩 나오므로 $\eta\eta' = 3-1 = 2$이다. 따라서 η, η'은 $\frac{-1\pm\mathrm{i}\sqrt{7}}{2}$이다. η의 실수부(real part)에서 코사인의 합을 얻는다. η의 허수부(imaginary part)는 $\sin\frac{2\pi}{7}+\sin\frac{4\pi}{7}-\sin\frac{\pi}{7}$이고, $\sin\frac{4\pi}{7} = \sin\frac{3\pi}{7} > \sin\frac{\pi}{7}$이므로 양수이다. 따라서 허수부는 $+\frac{\sqrt{7}}{2}$이다.

2. $\zeta = \mathrm{e}^{2\pi\mathrm{i}/5}$라 하면, 주기(period) $\zeta+\zeta^4 = 2\cos\frac{2\pi}{5}$와 $\zeta^2+\zeta^3$의 합은 -1, 곱은 -1이므로 이 둘은 $t^2+t-1=0$의 근이고, 그중 양수인 것에서 $\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$를 얻는다. 작도하려면 다음과 같이 한다. 단위원에서 직각을 낀 두 변의 길이가 1과 $\frac{1}{2}$인 직각삼각형의 빗변(hypotenuse)은 $\frac{\sqrt{5}}{2}$이다. 여기서 $\frac{1}{2}$을 빼고 반으로 나누면 $\cos\frac{2\pi}{5}$를 얻는다. 그 거리에서 축에 수직인 직선은 $(1,0)$에 이웃한 꼭짓점에서 원과 만난다. 이

현(chord)을 원을 따라 차례로 옮겨 가면 된다.

3. 둘 다 소수점 아래 다섯째 자리까지 -1.28078이다.

4. 3의 거듭제곱은 $3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1$로, 열여섯 개가 모두 나온다. 2의 거듭제곱은 여덟 단계마다 반복되며($2^8 = 256 \equiv 1$) $\{1, 2, 4, 8, 9, 13, 15, 16\}$을 주는데, 이는 17을 법으로 하는 0이 아닌 제곱수(square modulo 17)이다.

6.3 $\sqrt{2}+\sqrt{3}+\sqrt{5}$를 근으로 갖는 다항식

1. $y^3 = 2\sqrt{2} + 6\sqrt{3} + 9\sqrt{2} + 3\sqrt{3} = 11\sqrt{2} + 9\sqrt{3}$이고 $9y = 9\sqrt{2} + 9\sqrt{3}$이므로 $y^3 - 9y = 2\sqrt{2}$이다. 그러면 $\sqrt{3} = y - \sqrt{2}$와 $\sqrt{6} = \sqrt{2}\sqrt{3}$도 y에 대한 다항식이다.

2. $x - \sqrt{2} = \sqrt[3]{3}$으로 놓고 세제곱하면 $x^3 + 6x - 3 = \sqrt{2}(3x^2 + 2)$이다. 이를 제곱하면 $x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1 = 0$을 얻는다.

3. 가능한 유리근(rational root)은 ± 1뿐인데, 어느 것도 근이 아니다. x^3항이 없으므로 최고차항의 계수가 1인(monic) 이차식 두 개로 인수분해하면 $(x^2 + ax + b)(x^2 - ax + c)$ 꼴이 되고, $a(c - b) = 0$, $b + c - a^2 = -10$, $bc = 1$이다. $a = 0$이면 $b + c = -10$, $bc = 1$인데, 이는 정수에서 불가능하다. $b = c = \pm 1$이면 $a^2 = 12$ 또는 8이 되어 역시 불가능하다. 따라서 이 사차식은 기약(irreducible)이고 $\sqrt{2} + \sqrt{3}$의 차수(degree)는 4이다.

4. 드무아브르(De Moivre)의 정리에서 $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$이고, $\theta = 20^\circ$로 두면 $\frac{1}{2} = 4c^3 - 3c$이다. 후보 $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$는 모두 근이 아니다. 따라서 $\cos 20^\circ$의 차수는 3이다. 그런데 작도 가능한(constructible) 길이는 모두 차수가 2의 거듭제곱이므로, 60°로부터 20°를 작도할 수 없다.

6.4 사차방정식 풀기

1. $y_1y_2 + y_2y_3 + y_3y_1$은 $\alpha^2\beta\gamma$ 꼴의 열두 항(한 근의 제곱에 다른 두 근을 곱한 것)의 합이다. 그리고 $\left(\sum \alpha\right)\left(\sum \alpha\beta\gamma\right)$는 이 열두 항에 $4\alpha\beta\gamma\delta$를 더한 것이다. 따라서 그 합은 $(-p)(-r) - 4s$이다.

2. 계수를 비교하면 $a + b = 1$, $a\alpha + b\beta = 0$, $a\alpha^2 + b\beta^2 = -p$를 얻는다. 이는 $\alpha \neq \beta$일 때 풀 수 있는데, 바로 두 조건이 이를 보장한다. $p \neq 0$이면 t에 대한 방정식이 진짜 이차방정식이 되고($p = 0$이면 $-qt = 0$으로 줄어들어 근이 0 하나뿐이다), $q^2 \neq 4p^3$이면 그 판별식(discriminant) $q^2 - 4p^3$이 0이 아니다. $x^3 - 24x + 48$의 경우 $p = 8$, $q = 48$이고, $8t^2 - 48t + 64 = 0$에서 $\alpha = 2$, $\beta = 4$이다. 그러면 $\left(\frac{x-2}{x-4}\right)^3 = -\frac{b}{a} = \frac{\alpha}{\beta} = \frac{1}{2}$이므로 $x - 2 = 2^{-1/3}(x - 4)$이고, 이를 정리하면 주어진 근 $x \approx -5.6946$을 얻는다.

3. 분해 삼차식(resolvent cubic)은 $y^3 - 7y^2 + 16y - 12 = (y - 3)(y - 2)^2$이다. 근 $y = 3$에서 $(x^2 - 2x + 1)(x^2 - 2x + 2)$를 얻으므로 근은 1(두 번)과 $1 \pm \mathrm{i}$이다.

4. 각 쌍 안에서 바꿀지 말지(4가지), 그리고 두 쌍끼리 바꿀지 말지(2가지)를 정한다. 즉 항등치환(identity), $(\alpha\beta)$, $(\gamma\delta)$, $(\alpha\beta)(\gamma\delta)$, $(\alpha\gamma)(\beta\delta)$, $(\alpha\delta)(\beta\gamma)$, $(\alpha\gamma\beta\delta)$, $(\alpha\delta\beta\gamma)$이다. 이는 정사각형의 대칭군(symmetry group)과 똑같은 구조이다.

6.5 공리에서 출발하는 미분

1. 상수는 여전히 0이 되고, 규칙 (i)과 귀납법(induction)에 의해 $\diamondsuit x^n = x^{n-1}\diamondsuit x + x\diamondsuit x^{n-1} = nx^n$이다. 선형성(linearity)에 의해 $\diamondsuit \mathrm{h} = x\mathrm{h}'$이다.
2. $\diamondsuit \mathrm{f} = \frac{\mathrm{f}}{\mathrm{g}}\diamondsuit \mathrm{g} + \mathrm{g}\diamondsuit\frac{\mathrm{f}}{\mathrm{g}}$이므로 $\diamondsuit\frac{\mathrm{f}}{\mathrm{g}} = \frac{\mathrm{g}\diamondsuit\mathrm{f} - \mathrm{f}\diamondsuit\mathrm{g}}{\mathrm{g}^2}$이다.
3. $\mathrm{f} = (x-a)^2\mathrm{g}$이면 $\mathrm{f}' = (x-a)\big(2\mathrm{g} + (x-a)\mathrm{g}'\big)$이다. $x^n - 1$의 중근(repeated root)은 nx^{n-1}의 근이어야 하므로 0이어야 한다. 그러나 0은 $x^n - 1$의 근이 아니다.
4. $(2+\varepsilon)^2 + 1 = 5 + 4\varepsilon$이고 $(5+4\varepsilon)^3 = 125 + 300\varepsilon$이다. 따라서 $f(2) = 125$, $f'(2) = 300$이다. 연쇄법칙(chain rule)으로 계산하면 $3(x^2+1)^2 \cdot 2x = 3 \cdot 25 \cdot 4 = 300$이다.

6.6 부분군의 합집합

1. $V = \{e, a, b, c\}$에서 $a^2 = b^2 = c^2 = e$이고, a, b, c 중 어느 두 개의 곱도 나머지 하나이다. 모든 원소가 자기 자신의 역원(inverse)이다. $\{1, \mathrm{i}, -1, -\mathrm{i}\}$에서는 i의 역원이 $-\mathrm{i}$이므로 두 군은 서로 다르다.
2. g가 진부분군(proper subgroup) H에 속한다면 g의 모든 거듭제곱도 H에 속하므로, H는 군 전체가 되어 버린다.
3. 1은 짝수도 아니고 3의 배수도 아니다. 더 일반적으로, $\mathbb{Z}$는 순환군(cyclic group)이므로(1로 생성된다) 앞의 문제에 의해 진부분군을 몇 개 모으더라도 그 합집합(union)이 될 수 없다.
4. 직선 $y = mx$는 $y = x^2$와 $x = 0$과 $x = m$에서만 만나고, 직선 $x = 0$은 원점에서만 만난다. 따라서 k개의 직선은 $t \neq 0$인 무수히 많은 점 (t, t^2) 중 많아야 k개만 포함한다.

6.7 사원수군

1. $C \circ B = (\mathrm{i}, 0) \circ (0, 1) = (0, \mathrm{i}) = D$이고, $B \circ C = (0, 1) \circ (\mathrm{i}, 0) = (0, \mathrm{i}^*) = (0, -\mathrm{i}) = H$이다.
2. A의 위수(order)는 1, E의 위수는 2이다. 나머지 여섯 원소는 각각 제곱하면 E이므로 위수가 4이다. 정사각형의 대칭군에는 위수가 2인 원소가 다섯 개(반사 네 개와 반 바퀴 회전) 있으므로 두 군은 동형(isomorphic)이 아니다.
3. 행렬식(determinant)은 $\det M = z_1 z_1^* + z_2 z_2^* = |z_1|^2 + |z_2|^2$이고, 이는 네 실수의 제곱의 합이다. $M(z)M(w)$는 $z \circ w$의 행렬이므로, 행렬식을 곱하면 $(a_1^2 + \cdots + a_4^2)(b_1^2 +$

$\cdots + b_4^2$)를 $|u_1|^2 + |u_2|^2$, 즉 다시 네 제곱수의 합으로 나타낼 수 있다.

4. 부분군은 $\{A\}$, $\{A, E\}$, $\{A, E, C, G\}$, $\{A, E, B, F\}$, $\{A, E, D, H\}$, Q_8이다. A가 아닌 모든 원소는 거듭제곱하면 E가 나오므로, $\{A\}$가 아닌 모든 부분군은 E를 포함한다. 위수가 4인 세 부분군을 합치면 여덟 원소가 모두 들어 있다.

6.8 특이행렬로 이루어진 군

1. $\mathbf{M}_a\mathbf{M}_b = \mathbf{M}_{2ab}$이고 $2(2ab) = (2a)(2b)$이다. 이 사상(map)은 일대일(one-to-one)이며 0이 아닌 실수 전체 위로의(onto) 사상이다.

2. $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix}$이고 $ac \neq 0$이므로 이 집합은 닫혀 있다(closed). 모든 $\begin{pmatrix} 1 & e \\ 0 & 0 \end{pmatrix}$는 왼쪽 항등원(left identity)이다. 그러나 $\mathbf{E} = \begin{pmatrix} e & f \\ 0 & 0 \end{pmatrix}$에 대해 $\mathbf{XE} = \mathbf{X}$가 되려면 $e = 1$, $f = b/a$여야 하고, 이는 $\mathbf{X}$에 따라 달라진다. 따라서 오른쪽 항등원이 없으므로 항등원이 없고, 군이 아니다.

3. $\mathbf{0}$, $\mathbf{I}$, 그리고 $bc = a(1-a)$인 행렬 $\begin{pmatrix} a & b \\ c & 1-a \end{pmatrix}$(대각합(trace)이 1, 행렬식이 0)이다. 이들은 평면을 한 직선 위로 다른 직선을 따라 보내는 사영(projection)이다.

4. 모든 성분이 a인 행렬 $\mathbf{J}_a$는 $\mathbf{J}_a\mathbf{J}_b = \mathbf{J}_{nab}$를 만족한다. 항등원은 $\mathbf{J}_{1/n}$이고 $\mathbf{J}_a$의 역원은 $\mathbf{J}_{1/(n^2a)}$이다.

Beyond STEP

STEP은 대부분의 학생이 학창 시절에 치르는 수학 시험 가운데 가장 어려운 시험이다. 또한 가장 훌륭한 시험 가운데 하나이기도 하다. 문제는 짧고 낯설며 깊이가 있고, 그중 가장 뛰어난 문제들은 대학 수학의 작은 조각이 모습을 감추고 있는 것이다.

이 책은 1987년 첫 시험에 앞서 나온 예시 시험지(specimen papers)부터 2025년 시험지까지 가운데 가장 흥미로운 STEP 문제들을 골라, 각 문제를 하나의 문으로 삼는다. 모든 문제는 뛰어난 학생이 풀어 가면서 던질 법한 질문들과 함께 꼼꼼하게 풀이하고, 그런 다음 책은 그 문을 지나 한 걸음 더 나아간다. 그 아이디어가 어디에서 왔는지, 대학에서는 무엇으로 발전하는지, 그리고 다음에는 무엇을 읽으면 좋은지를 살펴본다.

이 책은 STEP을 준비하면서 기출 문제 연습 이상의 것을 원하는 재능 있는 예비 수학자를 위해 쓰였다. 수학과 학부생처럼 생각하기 시작하고, 앞으로 무엇이 자신을 기다리고 있는지 알아보고 싶은 학생들을 위한 책이다.

- 순수수학(pure mathematics), 역학(mechanics), 확률(probability)과 통계(statistics)를 아우르는 13개의 장
- 이 36개의 STEP 기출 문제와 각 문제의 안내식 풀이
- 모든 문제 뒤에 숨은 대학 수학
- 답이 실린 후속 연습 문제와 더 읽을거리

전체 13개 장 가운데 제6장. 책 전체와 모든 장,
모든 풀이를 다음 주소에서 무료로 읽고, 내려받고, 공유할 수 있다.

beyondstep.keithmcnulty.org

본문은 퍼블릭 도메인(CC0 1.0)으로 공개한다. STEP 문제 © Cambridge University Press & Assessment.

