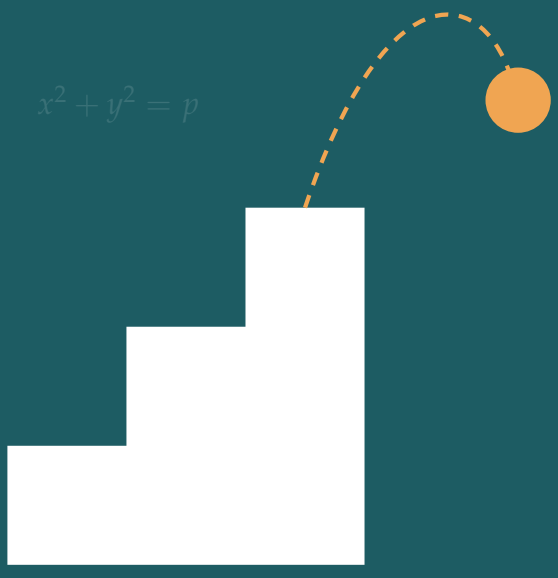
STEP 対策 · 大学の数学

Beyond STEP

第 6 章

代数と構造



KEITH McNULTY

Beyond STEP

大学数学への入り口としての
STEP 過去問

第 6 章

代数と構造

Keith McNulty

Beyond STEP：大学数学への入り口としての STEP 過去問

第 6 章：代数と構造

これは *Beyond STEP* 全 13 章のうちの第 6 章である。本書全体、各章単独の PDF、各節の印刷用ワークシート、そしてすべての STEP の問題の詳しい解答は、`beyondstep.keithmcnulty.org` で無料で閲覧・ダウンロードできる。

2026 年 11 月、オンラインにて初版発行。

本 PDF のうち著者自身の著作物（本文、解答、図、演習問題とその答えを含む）はすべて、クリエイティブ・コモンズ CC0 1.0 全世界（Creative Commons CC0 1.0 Universal）ライセンスのもとでパブリックドメインに提供されている。許可を求めることなく、いかなる目的でも複製、改変、共有してよい。詳しくは `creativecommons.org/publicdomain/zero/1.0` を参照のこと。

ここで扱う STEP の問題の著作権は Cambridge University Press & Assessment に帰属する。問題そのものは転載しておらず、各問題には公式の出典である STEP Support Programme の問題データベース、または OCR の過去問へのリンクを付している。

誤りの指摘は、`github.com/keithmcnulty/step_book_mcnulty` への issue として歓迎する。

章

6

代数と構造

代数のあらゆる巧妙な技巧の背後には構造がある。そして構造を理解することは、どれほど多くの技巧を知ることよりも価値がある。

この章の内容

6.1	1 の累乗根を根にもつ多項式	STEP III 2010
6.2	ガウスの正 17 角形	STEP II 1991
6.3	$\sqrt{2}+\sqrt{3}+\sqrt{5}$ を根にもつ多項式	STEP II 2023
6.4	四次方程式を解く	STEP III 2017
6.5	公理から考える微分	STEP II 1992
6.6	部分群の和集合	STEP II 1988
6.7	四元数群	STEP III 1993
6.8	特異行列からなる群	STEP III 1996
A	演習問題の答え	p. 59

方程式から構造へ

> 数学とは、異なるものに同じ名前を与える技術である。
>
> — アンリ・ポアンカレ（Henri Poincaré）

その歴史の大部分において、代数とは方程式を解くことであった。バビロニア人は 4000 年前に 2 次方程式（quadratic）を解き、16 世紀のイタリアの数学者たちは 3 次方程式（cubic）と 4 次方程式（quartic）を解いた。そしてその後 300 年近くにわたり、5 次方程式（quintic）はあらゆる試みを退け続けた。1820 年代から 1830 年代にかけてついに得られた解決は、代数を根本から変えた。アーベル（Niels Henrik Abel）は 5 次方程式に対する一般的な解の公式が存在しないことを証明し、ガロア（Évariste Galois）はどの方程式が解けるのかを正確に説明した。彼が調べたのは方程式そのものではなく、**その根の対称性**であった。そのために彼は新しい種類の数学的対象を発明しなければならなかった。それが群（group）である。

答えを計算することから構造を研究することへ、という転換こそが本章の主題である。現代の代数は「解は何か？」と問う代わりに、「これはどのような種類の対象であり、どのような演算が許されるのか？」と問う。その答えは、昔の技巧がなぜうまくいったのかを説明し、さらに技巧だけでは決して決着のつかなかった問題をも解決するのである。

なぜ構造が重要なのか

2000 年もの間あらゆる試みを退けてきた、古代からの三つの問題がある。定規とコンパス（ruler and compasses）を用いて、立方体の体積を 2 倍にすること、任意の角を三等分すること、正 7 角形を作図すること、である。いずれも不可能であり、19 世紀に見出されたその証明は、巧妙な作図ではなく構造についての議論である。すなわち、定規とコンパスで到達できる数の体（field）の**次数**（degree）についての議論である（Section 6.3）。同じ理論によって、正 17 角形がなぜ作図**できる**のか（Section 6.2）、そして 4 次方程式は解けるのに 5 次方程式はなぜ解けないのか（Section 6.4）も説明される。

構造はまた、分野を越えて通用する。群の公理（axiom）を満たすものには、結晶の対称性、多項式の根の置換（permutation）、3 次元空間の回転、ルービックキューブの操作、楕円曲線（elliptic curve）上の点などがある。公理から一度証明された定理は、そ

のすべてにおいて成り立つ。ポアンカレの言う「異なるものに同じ名前を与える」というこの経済性こそが、抽象代数学（abstract algebra）をこれほど強力なものにしているのである。

大学で出会うこと

1 年次には**群**（三つの公理を満たす演算をもつ集合）に出会い、たいていは**環**（ring）と**体**（加法と乗法をもつ集合）にも出会う。部分群（subgroup）の大きさは群の大きさを割り切るというラグランジュ（Lagrange）の定理を証明し、置換、対称群、行列群に出会うことになる。2 年次と 3 年次には、これらが次のものへとつながっていく。体と群を結びつけ、方程式と作図に関する古典的な問題に答える**ガロア理論**（Galois theory）、行列を通して群を研究する**表現論**（representation theory）、そして Section 1.7 の考え方が確かな基礎の上に置かれる**代数的整数論**（algebraic number theory）である。本章の最後の三つの節は群を扱う。群はもはや STEP の出題範囲には含まれていない（2019 年に削除された）が、問題はそれだけで完結しており、各節では必要な定義を与えている。

本章を貫く問い

三つの大きな問い

1. **何から何を作ることができるか？**有理数から平方根をとることで、あるいは方程式を解くことで、どのような数に到達できるのか。そして、ある数に到達**できない**ことはどのように証明するのか。
2. **方程式の解の公式はなぜうまくいくのか？** 2 次方程式、3 次方程式、4 次方程式に解の公式があることの隠れた理由は何か。そして次数が 5 になると何が変わるのか。
3. **抽象化によって何が得られるのか？**対象を、それが従う規則だけによって記述すると何が起こるのか。

本章で扱う考え方

§	主題	考え方
6.1	円分多項式（cyclotomic polynomial）	1 の冪根（root of unity）を位数で分類する
6.2	正 17 角形	ガウス（Gauss）周期：和と積から 2 次方程式が得られる
6.3	最小多項式（minimal polynomial）	根号（radical）を消去する；次数は掛け合わされる
6.4	4 次方程式を解く	対称関数（symmetric function）；分解 3 次式（resolvent cubic）
6.5	公理からの微分	規則によって決定される演算
6.6	部分群の和集合	群の公理から論じる
6.7	四元数群（quaternion group）	演算を行列で表現する
6.8	特異行列（singular matrix）からなる群	定義を文字どおりに読む

本章の読み方

これらの問題の多くは力ずくで解くことができる。すべてを展開し、係数を比較し、すべての場合を確かめればよい。必要ならまずそうしてみるとよい。そのうえで振り返り、何が力ずくの方法を成功させたのか、その背後に構造的な理由があるのかを問うてみてほしい。構造的な理由はたいていより短く、常により多くのことを明らかにしてくれる。そして力ずくの方法が通用しなくなったときに必要となるのは、まさにそれなのである。

6.1 1 の累乗根を根にもつ多項式

問題

STEP III 2010、問 3

先に進む前に、まず問題を読んでおこう。問題は STEP Support Programme の問題データベースにある：

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

導入

1 の n 乗根（nth roots of unity）、すなわち $z^n = 1$ の解は、正 n 角形の頂点に並んでいる。しかし、それらはすべて同じ性質をもつわけではない。たとえば 1 の 12 乗根のうち、1 はすでに 1 の 1 乗根であり、-1 は 1 の平方根、i は 4 乗根である。12 個のうち 4 個だけ、すなわち**原始的**（primitive）なものだけが、1 に戻るまでに 12 ステップすべてを必要とする。

1 の冪根を、必要なステップ数によって分類し、それぞれの類から多項式を作ると、**円分多項式**（cyclotomic polynomials、ギリシャ語で「円を分割する」の意）が得られる。素数が整数の基本的な構成要素であるのと同じように、円分多項式は $z^n - 1$ の基本的な構成要素である。円分多項式は、ガウス（Gauss）による正 17 角形の作図（Section 6.2）や 1 の冪根フィルター（Section 5.2）、さらには現代整数論の多くの部分の背後にある。

取りかかる前に

考えてみよう 1 の n 乗根はどれも $z^n = 1$ を満たす。しかし、1 を与える最小の正の冪は n より小さいかもしれない。四つの 1 の 4 乗根 $1, \mathrm{i}, -1, -\mathrm{i}$ のそれぞれについて、その最小の冪はいくつか？

$1^1 = 1$、$(-1)^2 = 1$ であり、$\mathrm{i}^4 = (-\mathrm{i})^4 = 1$ で、これより小さい冪では 1 にならない。したがって最小の冪はそれぞれ $1, 4, 2, 4$ である。この最小の冪をその 1 の冪根の**位数**（order）とよび、原始 n 乗根とはちょうど位数が n であるもののことである。この問

題全体を通じて鍵となる事実は、**どの 1 の冪根もただ一つの位数をもつ**ということである。

順を追って解く

段階 1　最初のいくつか

原始 4 乗根は i と $-\mathrm{i}$ であるから、$C_4(x) = (x-\mathrm{i})(x+\mathrm{i}) = x^2+1$ である。 ■

> **考えてみよう**　位数が $1, 2, 3, 5$ および 6 である 1 の冪根はそれぞれどれか？（1 の 6 乗根を図示し、位数によって分類してみよ。）

位数 1：1 のみであるから、$C_1(x) = x-1$。位数 2：-1 のみであるから、$C_2(x) = x+1$。

位数 3：1 以外の 1 の 3 乗根、すなわち $\frac{x^3-1}{x-1}$ の根である。よって $C_3(x) = x^2+x+1$。

位数 5：1 以外の 5 乗根であり、これは $\frac{x^5-1}{x-1}$ の根であるから、$C_5(x) = x^4+x^3+x^2+x+1$。

位数 6：6 乗根 $e^{k\pi\mathrm{i}/3}$, $k = 0,\dots,5$ のうち、$k = 0, 3$ のものは位数がそれぞれ $1, 2$ であり、$k = 2, 4$ のものは位数 3 である。残るのは $e^{\pm\pi\mathrm{i}/3}$ であるから、

$$C_6(x) = (x - e^{\mathrm{i}\pi/3})(x - e^{-\mathrm{i}\pi/3}) = x^2 - 2x\cos\tfrac{\pi}{3} + 1 = x^2 - x + 1. \qquad \blacksquare$$

段階 2　x^4+1 を与える n はどれか？

$x^4+1=0$ の根は $x^4 = -1$ を満たすので、$x^8 = 1$ であるが $x^4 \neq 1$ である。その位数は 8 を割り切るが 4 を割り切らないので、8 である。逆に、位数 8 の根は $x^8 = 1$, $x^4 \neq 1$ を満たすので、$x^4 = -1$ である。原始 8 乗根は 4 個あり、x^4+1 の根も 4 個あるから、$n = 8$ である。 ■

段階 3　素数の場合

p が素数ならば、1 の p 乗根の位数は p を割り切るので、1 または p である。したがって 1 以外の p 乗根はすべて原始的であり、

$$C_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1. \qquad \blacksquare$$

段階 4　円分多項式は他の二つの円分多項式の積にならない

手を止めて、やってみよう $C_q = C_r C_s$ と仮定する。C_r の根を一つとる。その位数はいくつか？この恒等式はその位数について何を教えてくれるか？そこから何が導かれるか？

C_r の根（$e^{2\pi i/r}$ は原始的であるから、少なくとも一つは存在する）はどれも $C_r C_s = C_q$ の根であるから、位数は q である。しかしその位数は r でもあり、1 の冪根の位数はただ一つであるから、$r = q$ である。すると $C_q = C_q C_s$ となり、C_q は零多項式ではないから、$C_s = 1$ である。しかし C_s は少なくとも一つの根 $e^{2\pi i/s}$ をもつので、これは不可能である。よって、このような q, r, s は存在しない。 ■

振り返り

- **位数で分類する。** どの 1 の冪根もただ一つの位数をもち、位数でまとめることで $z^n - 1$ の根は互いに交わらない類に分かれる。
- **根によって多項式を定める。** 各 C_n は、どの数がその根であるかを正確に述べることで決定された。
- **一意性から不可能性が導かれる。** 小問 (iv) で必要だったのは、一つの根が二つの異なる位数をもつことはない、というただ一つの考え方だけであった。

背後にある数学

$x^n - 1$ の因数分解

1 の n 乗根はどれも、n を割り切るある位数 d をもつ。また $d \mid n$ のとき、位数 d の 1 の d 乗根はどれも 1 の n 乗根である。したがって $x^n - 1$ の根は位数によって類に分かれ、

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

が得られる。たとえば $x^6 - 1 = C_1 C_2 C_3 C_6 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$ である。図 6.1.1 は、12 個の 1 の 12 乗根をこのように分類したものである。原始 n 乗根の個数、すなわち C_n の次数は、1 から n までの k のうち n と共通因数をもたないものの個数であり、これが**オイラーのトーシェント関数**（Euler's totient function）$\varphi(n)$ である。次数を比較すると、恒等式 $\sum_{d \mid n} \varphi(d) = n$ が得られる。

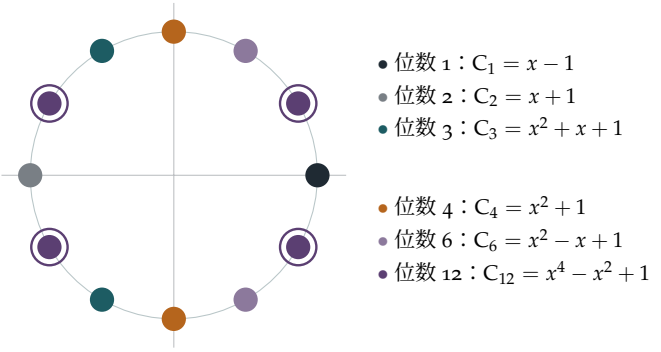


図 6.1.1　12 個の 1 の 12 乗根を位数によって色分けしたもの。4 個の原始 12 乗根（丸で囲んだもの）は C_{12} の根である。すべての類を合わせると $x^{12} - 1 = C_1C_2C_3C_4C_6C_{12}$ となり、次数は $1 + 1 + 2 + 2 + 2 + 4 = 12$ である。

整数係数と、ある意外な事実

定義からは明らかではないが、どの円分多項式も**整数**係数をもつ。（$x^n - 1$ の因数分解と数学的帰納法（induction）を用いる。C_n は $x^n - 1$ をそれ以前の円分多項式の積で割ったものであり、整数係数の多項式をモニック（monic、最高次の係数が 1）な整数係数多項式で筆算により割っても、係数は整数のままである。）長い間、知られていた例はすべて係数が $0, 1, -1$ のいずれかであった。最初の例外は C_{105} で、これは項 $-2x^7$ を含み、1883 年に Migotti によって発見された。$105 = 3 \times 5 \times 7$ は、相異なる三つの奇素因数をもつ最小の数である。実は、円分多項式の係数はいくらでも大きくなりうる。

既約性

小問 (iv) は、円分多項式が他の二つの円分多項式の積にならないことを示している。実はもっと強いことが成り立つ。C_n は、より低い次数の有理数係数多項式の積にはまったく因数分解できないのである。ガウスはこれを n が素数の場合に証明し（これは大学の最初の代数の講義で学ぶ**アイゼンシュタインの判定法**（Eisenstein's criterion）から導かれる）、クロネッカー（Kronecker）とデデキント（Dedekind）が一般の n の場合に証明した。この**既約性**（irreducibility）こそが、円分多項式を 1 の冪根に関連する多項式の中の「素数」たらしめているものであり、1 の冪根のガロア理論（Galois theory）の出発点でもある。

思考のスキル

分類してから組み立てる

問題に現れる対象を、ただ一つに定まる明確な不変量（*invariant*）によって類に分け、類ごとに構造を組み立てよ。

ここでの不変量は 1 の冪根の位数であった。各根はちょうど一つの位数をもつので類は重ならず、$x^n - 1$ はそれらの類にわたる積に分解される。同じパターン（一意的な不変量が互いに交わらない分解を与えること）は、素因数分解（prime factorisation）や有限アーベル群（finite abelian groups）の分類の根底にもある。

次の一歩

1. **因数分解を確かめる。** $(x-1)(x+1)(x^2+x+1)(x^2-x+1) = x^6 - 1$ であること、および $x^{12} - 1$ が図 6.1.1 のように因数分解されることを確かめよ。

2. **素数の 2 倍。** p が奇素数ならば $\mathrm{C}_{2p}(x) = \mathrm{C}_p(-x)$ であることを示せ。$p = 3$ の場合にこれを確かめよ。

3. **トーシェント関数。** 素数 p に対して $\varphi(p^k) = p^k - p^{k-1}$ であること、および $\mathrm{C}_{p^k}(x) = \mathrm{C}_p\left(x^{p^{k-1}}\right)$ であることを示せ。これを用いて C_9 を求めよ。

4. **少し長い問題。** やや難 $x^{15} - 1 = \mathrm{C}_1\mathrm{C}_3\mathrm{C}_5\mathrm{C}_{15}$ を用いて、$\mathrm{C}_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$ であることを示せ。

さらに学ぶために

- **Ian Stewart, *Galois Theory***（CRC Press）。学部生向けの標準的な入門書（『ガロア理論』）。円分多項式と正多角形が早い段階で登場する。
- **Harold Davenport, *The Higher Arithmetic***（Cambridge University Press）。1 の冪根とその算術を扱っている（『高等算術』）。
- **Marcus du Sautoy, *Finding Moonshine***（Fourth Estate）。対称性と群論についての一般向けの読み物で、ガロアの物語も含まれている。

6.2 ガウスの正 17 角形

問題

STEP II 1991、問 4

先に進む前に、まず問題を読んでおこう。問題は STEP Support Programme の問題データベースにある：

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

導入

1796 年 3 月 30 日、ゲッティンゲン（Göttingen）の 18 歳の学生が、生涯にわたって書き続けることになる数学日記の最初の記述を残した。彼は、正 17 角形（regular 17-sided polygon）を定規とコンパス（ruler and compasses）で作図する方法を発見したのである。古代ギリシャ人は、辺の数が 3, 4, 5, 15 の正多角形と、それらの辺の数を 2 倍にしたものの作図法を知っていたが、それから二千年の間、新たに一つでも付け加えた者はいなかった。カール・フリードリヒ・ガウス（Carl Friedrich Gauss）は後に、この発見によって文献学者ではなく数学者になる決心をしたと語っており、墓石に正 17 角形を刻むよう頼んだとも伝えられている。

この作図の核心は、本問の後半部分にある。すなわち、ある特定の四つの余弦の和が $\frac{\sqrt{17}-1}{4}$ に等しいという事実であり、これは平方根しか含まない数である。平方根から組み立てられる長さは定規とコンパスで作図でき、ガウスは同じ種類の手順をさらに三回重ねることで、$\cos\frac{2\pi}{17}$ そのものを作図することができた。

取りかかる前に

考えてみよう $\cos\frac{2\pi}{5}$ に関する前半部分が、なぜ 17 角形についての問題に登場するのだろうか。

これは準備運動であり、同じ考え方をより小さな多角形に適用している。五角形の場合、和 $\cos\phi + \cos 2\phi$ は有理数係数の二次方程式（quadratic）を満たすので、二次方程式を解くことで求められる。17 角形の場合も、四つの余弦の和 z が二次

方程式を満たすことが分かる。どちらの場合も、鍵は余弦どうしを掛け合わせ、$\cos A\cos B=\tfrac12(\cos(A+B)+\cos(A-B))$ を用いて、積を同じ角の余弦の和に戻すことである。

順を追って解く

段階 1　正五角形

考えてみよう　$y^2=(\cos\phi+\cos 2\phi)^2$ を展開し、各積を和に直したうえで、$5\phi=2\pi$ を用いて 3ϕ や 4ϕ のような角を簡約せよ。

$y^2=\cos^2\phi+2\cos\phi\cos 2\phi+\cos^2 2\phi=\tfrac12(1+\cos 2\phi)+(\cos 3\phi+\cos\phi)+\tfrac12(1+\cos 4\phi)$.

$5\phi=2\pi$ であるから、$\cos 3\phi=\cos(2\pi-2\phi)=\cos 2\phi$ かつ $\cos 4\phi=\cos\phi$ である。よって

$$y^2=1+\tfrac12(\cos\phi+\cos 2\phi)+(\cos\phi+\cos 2\phi)=1+\tfrac32 y,$$

すなわち $2y^2=3y+2$ である。 ■$2y^2-3y-2=(2y+1)(y-2)=0$ の解は $y=2$ と $y=-\tfrac12$ である。しかし $y=2$ となるには二つの余弦がともに 1 に等しくなければならず、そうはならないので、$y=-\tfrac12$ である。 ■

段階 2　1 の 17 乗根の和は 0 である

$\sum_{k=0}^{16}\cos k\theta$ は $\sum_{k=0}^{16}\omega^k$ の実部である。ここで $\omega=e^{i\theta}$ は 1 の原始 17 乗根（primitive root of unity）である。この等比級数（geometric series）の和は $\frac{\omega^{17}-1}{\omega-1}=0$ である。■

したがって $\sum_{k=1}^{16}\cos k\theta=-1$ である。$\cos(17-k)\theta=\cos k\theta$ であるから項は二つずつ組になり、

$$\sum_{k=1}^{8}\cos k\theta=-\tfrac12.$$

段階 3　余弦を二つのグループに分ける

考えてみよう　$z=\cos\theta+\cos 2\theta+\cos 4\theta+\cos 8\theta$ とし、残りの四つの余弦の和 $\cos 3\theta+\cos 5\theta+\cos 6\theta+\cos 7\theta$ を z' とする。$z+z'$ はいくらか。

段階 2 より $z+z'=-\tfrac12$ である。さらに zz' も求められれば、z と z' はある二次方程式の解となる。

> **手を止めて、やってみよう** zz' を計算せよ。これを 16 個の積 $\cos a\theta \cos b\theta$ に展開し、それぞれを二つの余弦の和に直して、$\cos\theta, \cos 2\theta, \ldots, \cos 8\theta$ のそれぞれが何回現れるかを数えよ。（角は $\cos k\theta = \cos(17-k)\theta$ と $\cos(-k\theta) = \cos k\theta$ を用いて簡約する。）

各積は $\cos a\theta \cos b\theta = \frac{1}{2}(\cos(a+b)\theta + \cos(a-b)\theta)$ となるので、zz' は 32 個の余弦の和の $\frac{1}{2}$ 倍である。$a \in \{1,2,4,8\}$、$b \in \{3,5,6,7\}$ となる 16 組を順に調べていく。たとえば $a=1, b=3$ からは $\cos 4\theta$ と $\cos 2\theta$ が得られ、$a=8, b=7$ からは $\cos 15\theta = \cos 2\theta$ と $\cos\theta$ が得られる。十六組すべてについてこれを実行すると、$\cos\theta, \ldots, \cos 8\theta$ のそれぞれがちょうど四回ずつ現れる。したがって

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

段階 4　二次方程式

よって z と z' は $t^2 + \frac{1}{2}t - 1 = 0$、すなわち $4t^2 + 2t - 4 = 0$ の解であり、その解は $t = \frac{-1 \pm \sqrt{17}}{4}$ である。どちらが z だろうか。数値的には $\cos\theta \approx 0.932$, $\cos 2\theta \approx 0.739$, $\cos 4\theta \approx 0.092$, $\cos 8\theta \approx -0.983$ であるから、$z \approx 0.78 > 0$ である。ゆえに

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

振り返り

- **積を和に直す。** 余弦の積和公式（product-to-sum formula）によって、y^2 と zz' が同じ余弦たちの和に変わり、計算がその中で閉じた。
- **和と積から二次方程式が得られる。** $z+z'$ と zz' が分かることは、z と z' を解にもつ二次方程式が分かることと同じである。
- **正しい分け方が肝心である。** 八つの余弦を $\{1,2,4,8\}$ と $\{3,5,6,7\}$ に分けたことで、zz' の中にどの添字も等しい回数だけ現れた。でたらめに分けたのではうまくいかない。

背後にある数学

ガウス周期

なぜ $\{1,2,4,8\}$ なのか。17 を法として、3 の累乗 $3^0, 3^1, 3^2, \ldots$ は 0 でないすべての剰余（residue）を巡る。

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

一つおきに $3^0, 3^2, 3^4, \ldots$ をとると 1, 9, 13, 15, 16, 8, 4, 2 が得られ、これらは 17 を法として ±1, ±2, ±4, ±8 であり、ちょうど z に現れる角である。残りの半分からは $\pm3, \pm5, \pm6, \pm7$ が得られ、これは z' に現れる角である。ガウスは、このような類にわたる ω^k の和を**周期**（*periods*）と呼んだ。$17 - 1 = 16 = 2^4$ であるから、剰余は四回半分に分けることができ、各段階で周期は、前の段階の周期を係数に含む二次方程式を満たす。四つの二次方程式、つまり四つの平方根によって、有理数から $\cos\frac{2\pi}{17}$ まで降りていくことができる。

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

どの段階も平方根しか含まず、平方根は（相似な三角形や半円を用いて）定規とコンパスで作図できるので、正 17 角形は作図可能である。

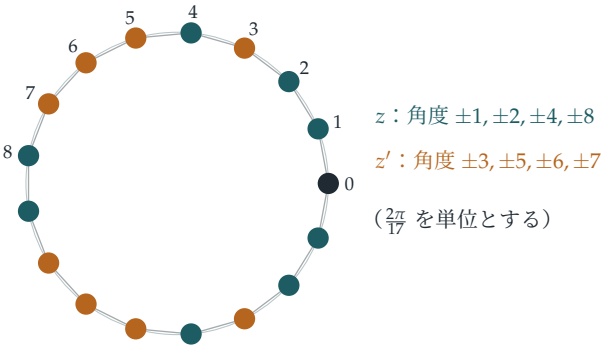


図 6.2.1　正 17 角形の頂点を、ガウスの二つの周期に分けたもの。ティール色の頂点は（$\frac{2\pi}{17}$ を単位として）角度 $\pm1, \pm2, \pm4, \pm8$ の位置にあり、それらの x 座標の和は $2z = \frac{-1+\sqrt{17}}{2}$ である。琥珀色の頂点からは $2z' = \frac{-1-\sqrt{17}}{2}$ が得られる。

どの多角形が作図できるか

ガウスが主張し、1837 年にヴァンツェル（Pierre Wantzel）が証明したところによれば、正 n 角形が定規とコンパスで作図できるのは、n が 2 の累乗と相異なる**フェルマー素数**（*Fermat primes*）、すなわち $2^{2^m}+1$ の形の素数の積との積であるとき、かつそのときに限る。知られているフェルマー素数は 3, 5, 17, 257, 65537 であり、これらは Section 1.1 のフェルマー数である。（フェルマー（Fermat）はこの形の数がすべて素数であると予想したが、オイラー（Euler）は $2^{32}+1$ が 641 で割り切れることを示した。それ以降、新たなフェルマー素数は一つも見つかっていない。）したがって正 257 角形と正 65537 角形は作図可能である。19 世紀には Johann Hermes が約十年をかけて正 65537 角形の作図法を詳細に書き上げ、その手稿はゲッティンゲンに保管されている。正 7 角形と正 11 角形は作図できない。7 と 11 はフェルマー素数ではないからである（$7-1=6$ と $11-1=10$ は 2 の累乗ではない）。正 9 角形も作図できない。$9=3^2$ ではフェルマー素数 3 が重複するからである。ヴァンツェルの証明には、Section 6.3 で扱う体の拡大次数（field degrees）の理論が用いられる。

思考のスキル

> **和と積を計算して二次方程式を見つける**
>
> ある量を求めるには、それに自然な相棒を組み合わせ、両者の和と積を計算して、得られる二次方程式を解けばよい。
>
> 腕の見せどころは、和も積も計算できるように相棒を選ぶことにある。本問では、相棒は 17 を法とする剰余の対称性から得られ、この考え方を四回繰り返すことで、ガウスは作図法にたどり着いた。

次の一歩

1. **正七角形。** STEP II 1995、問 6（`step.maths.org/questions/95-s2-q6`）に取り組んでみよう。この問題は、1 の累乗根をグループに分けるというガウスの考え方を 1 の 7 乗根に適用し、余弦の和と正弦の和の正確な値を求めるものである。正弦の和の符号を決めるところが微妙な一歩である。

2. **正五角形。** $\cos\frac{2\pi}{5}=\frac{\sqrt{5}-1}{4}$ を示し、それを用いて正五角形の定規とコンパスによる作図法を説明せよ。

3 **もう一方の周期。** $z' = \cos 3\theta + \cos 5\theta + \cos 6\theta + \cos 7\theta = \frac{-1-\sqrt{17}}{4}$ であることを数値的に確かめよ。

4 **生成元。** 17 を法とする 3 の累乗は 0 でないすべての剰余を与えるが、2 の累乗はそうではないことを示せ。2 の累乗はどの剰余を与えるか。

さらに学ぶために

- **Ian Stewart, *Galois Theory***（CRC Press）。『ガロア理論』。定規とコンパスによる作図と正 17 角形を扱う章がある。
- **Richard Courant & Herbert Robbins, *What Is Mathematics?***（Oxford University Press）。『数学とは何か』。第 3 章は、正 17 角形を含む作図についての、初等的で見事な解説である。
- **Daniel Kehlmann, *Measuring the World***（Quercus）。『世界の測量』。ガウスとフンボルト（Alexander von Humboldt）を描いた喜劇的な小説であり、息抜きに最適である。

6.3 $\sqrt{2}+\sqrt{3}+\sqrt{5}$ を根にもつ多項式

問題

STEP II 2023、問 4

先に進む前に、まず問題を読んでおこう。問題は、OCR が配布している 2023 年の STEP 過去問一式（zip ファイル）のうち、STEP II の問題用紙にある：

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

導入

$\sqrt{2}$ は整数係数の多項式 x^2-2 の根である。$\sqrt{3}$ も同様に x^2-3 の根である。では、$\sqrt{2}+\sqrt{3}$ もまた何らかの整数係数多項式の根になるだろうか。$\sqrt{2}+\sqrt{3}+\sqrt{5}$ や $\sqrt[3]{2}+\sqrt[3]{3}$ ではどうだろうか。

整数係数多項式の根となる数を**代数的**（algebraic）な数という。この問題は、実際に手を動かして根号を消去していくことで、代数的な数の和が代数的であることを示している。現れる次数 4、8、6、9 は偶然ではない。これらはそれぞれの数がどれほど「複雑」かを測るものであり、この尺度、すなわち**体の拡大次数**（degree of a field extension）こそが、古代ギリシアの立方体倍積問題と角の三等分問題に最終的な決着をつけたのである。

取りかかる前に

考えてみよう $\sqrt{2}$ を根にもつ多項式を見つけるには、$x=\sqrt{2}$ の両辺を 2 乗して平方根を取り除く。では、異なる 2 つの平方根を 1 つずつ取り除くにはどうすればよいだろうか。

一方の平方根を片側に孤立させて 2 乗すれば、それは消える。次にもう一方を孤立させて再び 2 乗する。2 乗するたびに次数は 2 倍になりうる。これがこの問題の戦略のすべてである。根号を 1 つずつ消去していくのである。

順を追って解く

段階 1　2 つの平方根

$(x-\sqrt{2})^2=3$ ならば $x^2-2\sqrt{2}\,x+2=3$ であるから、$x^2-1=2\sqrt{2}\,x$ となる。2 乗すると残りの平方根が消える。$(x^2-1)^2=8x^2$、すなわち

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

そして $x=\sqrt{2}+\sqrt{3}$ は $(x-\sqrt{2})^2=(\sqrt{3})^2=3$ を満たすので、$\mathrm{f}(\sqrt{2}+\sqrt{3})=0$ である。 $\blacksquare$

段階 2　3 つの平方根

考えてみよう　$x=\sqrt{2}+\sqrt{3}+\sqrt{5}$ とおくと、$x-\sqrt{5}=\sqrt{2}+\sqrt{3}$ は f の根である。$\mathrm{f}(x-\sqrt{5})=0$ を $P(x)+\sqrt{5}\,Q(x)=0$ の形に書け。そのあと $\sqrt{5}$ をどのように消去すればよいだろうか。

$(x-\sqrt{5})^2=x^2+5-2\sqrt{5}x$ および $(x-\sqrt{5})^4=\bigl(x^2+5-2\sqrt{5}x\bigr)^2=x^4+30x^2+25-4\sqrt{5}\,x(x^2+5)$ を用いて展開すると

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

整理すると $P(x)=x^4+20x^2-24$、$Q(x)=-4x^3-20x+20x=-4x^3$ である。よって $x^4+20x^2-24=4\sqrt{5}\,x^3$ となる。2 乗して

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

これを展開すると

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

（確認：$400-48=352$ を用いると $(x^4+20x^2-24)^2=x^8+40x^6+352x^4-960x^2+576$ であり、ここから $80x^6$ を引けば g が得られる。）

段階 3　3 次方程式の根と平方根

考えてみよう　$x=a+\sqrt{2}$ ならば、$x-\sqrt{2}$ は t^3-3t+1 の根である。代入し、$\sqrt{2}$ を含む項と含まない項に分けてから 2 乗せよ。

$(x-\sqrt{2})^3=x^3-3\sqrt{2}\,x^2+6x-2\sqrt{2}$ であるから

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

したがって $(x^3+3x+1)^2 = 2(3x^2-1)^2$ である。展開すると $x^6+6x^4+2x^3+9x^2+6x+1 = 18x^4-12x^2+2$ となるので

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

用いたのは a が t^3-3t+1 の根であるという事実だけなので、同じ議論が $b+\sqrt{2}$ と $c+\sqrt{2}$ についても成り立つ。（h の残りの 3 つの根は $a-\sqrt{2}$、$b-\sqrt{2}$、$c-\sqrt{2}$ であり、これらは 2 乗したときに入り込んだものである。）

段階 4　2 つの立方根

> **手を止めて、やってみよう**　$x = \sqrt[3]{2}+\sqrt[3]{3}$ とおく。両辺を 3 乗せよ。その結果を x とただ 1 つの立方根を用いて表せるだろうか。

$u = \sqrt[3]{2}$、$v = \sqrt[3]{3}$ として $(u+v)^3 = u^3+v^3+3uv(u+v)$ を用いると

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

もう一度 3 乗すれば最後の立方根が消える。$(x^3-5)^3 = 27\cdot 6\,x^3 = 162x^3$ である。$(x^3-5)^3 = x^9-15x^6+75x^3-125$ と展開して

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

振り返り

- **根号は 1 つずつ消去する。**根号を孤立させ、適切な累乗をとり、これを繰り返す。
- **有理部分と無理部分を分ける。**式を $P+\sqrt{5}\,Q$ の形に書き、$P^2 = 5Q^2$ を用いるのが鍵となる一手である。
- **2 乗すると余分な根が加わる。**2 乗するたびに、$a+\sqrt{2}$ に対する $a-\sqrt{2}$ のような「共役」（conjugate）な根が入り込む。最終的な多項式はそれらすべてを根にもつ。

背後にある数学

体とその次数

p、q を有理数とする数 $p+q\sqrt{2}$ 全体の集合 $\mathbb{Q}(\sqrt{2})$ は、加法、減法、乗法、（0 でない数による）除法について閉じている。すなわち、これは**体**（field）である。これは $\mathbb{Q}$ 上の 2 次元の「ベクトル空間」（vector space）であり、基底（basis）は $1, \sqrt{2}$ である。

そこで、これは $\mathbb{Q}$ 上**次数**（degree）2 をもつという。$\sqrt{3}$ を添加すると $\mathbb{Q}(\sqrt{2},\sqrt{3})$ が得られ、その基底は $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$、次数は 4 である。さらに $\sqrt{5}$ も添加すると次数は 8 になる（図 6.3.1）。**塔法則**（tower law）とは、体の塔をのぼるにつれて次数が掛け合わされるという法則である。ある数が生成する体の次数は、その数の**最小多項式**（minimal polynomial）、すなわちその数が満たす有理数係数多項式のうち次数が最小のものの次数に等しい。この問題の多項式 f と g は最小多項式であることが示せるので、$\sqrt{2}+\sqrt{3}$ の次数は 4、$\sqrt{2}+\sqrt{3}+\sqrt{5}$ の次数は 8 である。実際、ただ 1 つの数 $\sqrt{2}+\sqrt{3}+\sqrt{5}$ が次数 8 の体全体を生成するのである。

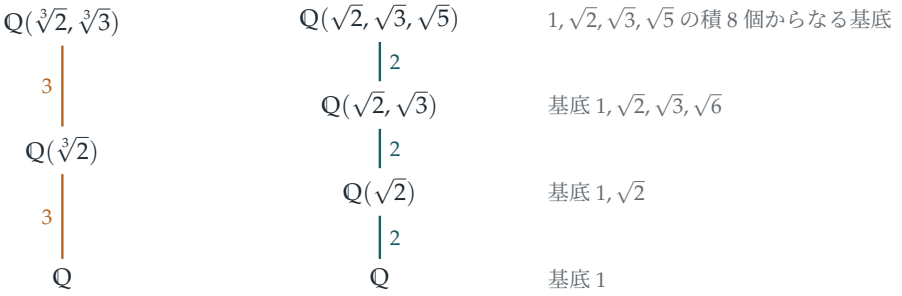


図 6.3.1　体の塔。右：平方根を 1 つ添加するごとに次数は 2 倍になり、$2\times2\times2=8$ が得られる。これは g の次数である。左：立方根を 1 つ添加するごとに次数は 3 倍になり、$3\times3=9$ が得られる。これは k の次数である。塔をのぼると次数は掛け合わされる。この**塔法則**こそが、定規とコンパスによる作図の不可能性の証明の鍵である。

立方体倍積問題

定規とコンパスによる作図（ruler-and-compass construction）で得られる長さは、有理数から出発して 1 次方程式と 2 次方程式を繰り返し解くことで得られるものに限られる。そのような各段階は次数 1 または 2 の体の拡大を与えるので、塔法則により、作図可能な長さはすべて次数が 2 の累乗である体に属し、それ自身の次数も 2 の累乗となる。ところが $\sqrt[3]{2}$ の最小多項式は x^3-2 であり、その次数は 3 である。3 は 2 の累乗ではないから $\sqrt[3]{2}$ は作図不可能であり、紀元前 430 年ごろに提起された、定規とコンパスで立方体の体積を 2 倍にするというデロスの問題は不可能である。ヴァンツェル（Pierre Wantzel）は 1837 年にこれを証明し、あわせて一般の角の三等分が不可能であることと、作図可能な正多角形の分類（Section 6.2）も示した。2000 年にわたる試みは、次数に関する議論によって終止符を打たれたのである。

代数的数は体をなす

この問題の方法は、具体例を通じて、代数的数の和が代数的であることを示している。一般には、これは線形代数を用いて証明される。α と β の次数をそれぞれ m、n とすると、数 $\alpha^i\beta^j$（$i<m$、$j<n$）全体は次元が高々 mn の空間を張るので、$mn+1$ 個の累乗 $1, \alpha+\beta, (\alpha+\beta)^2, \ldots$ は一次従属（linearly dependent）でなければならない。これにより次数が高々 mn の多項式が得られる。ここで得た次数 $4=2\times2$、$6=3\times2$、$9=3\times3$ はまさにこのパターンに当てはまる。代数的でない数を**超越的**（transcendental）な数という。e と π はその例であり（エルミート（Hermite）、1873 年、およびリンデマン（Lindemann）、1882 年）、π が超越数であるというリンデマンの定理によって、円積問題もまた不可能であることが証明された。

思考のスキル

消去し、そして測る

根号を含む式が満たす多項式を求めるには、根号を孤立させて累乗をとることで、根号を 1 つずつ取り除く。

そのうえで、次数が何を教えてくれるかを問う。最小多項式の次数はその数の不変量であり、次数を比較することは、何かが不可能であることを証明するための最も強力な方法の一つである。

次の一歩

1. **原始元（primitive element）。** $y=\sqrt{2}+\sqrt{3}$ とする。$y^3=11\sqrt{2}+9\sqrt{3}$ を示し、$\sqrt{2}=\frac{1}{2}(y^3-9y)$ を導け。したがって、すべての数 $p+q\sqrt{2}+r\sqrt{3}+s\sqrt{6}$ は y の多項式として表せる。

2. **種類の異なる根号。** $\sqrt{2}+\sqrt[3]{3}$ を根にもつ、次数 6 の整数係数多項式を求めよ。

3. **既約性（irreducibility）。** x^4-10x^2+1 は有理数の根をもたず、整数係数の 2 つの 2 次式の積として表せないことを示せ。（**ヒント：** $(x^2+ax+b)(x^2-ax+c)$ を試してみよ。）これより $\sqrt{2}+\sqrt{3}$ の次数が 4 であることを導け。

4. **角の三等分（trisection）。** $\cos3\theta=4\cos^3\theta-3\cos\theta$ を示し、$\cos20^\circ$ が $8x^3-6x-1=0$ の根であることを導け。この 3 次方程式が有理数の根をもたないと仮定して（これを確かめよ）、60° の角を定規とコンパスで三等分できない理由を説明せよ。

さらに学ぶために

- **Ian Stewart, *Galois Theory***（CRC Press）。『ガロア理論』。体の拡大、塔法則、古典的な作図問題を、大学生向けに解説している。
- **Richard Courant & Herbert Robbins, *What Is Mathematics?***（Oxford University Press）。『数学とは何か』。第 3 章では、予備知識なしでギリシアの三大問題の不可能性を証明している。
- **Robin Hartshorne, *Geometry: Euclid and Beyond***（Springer）。定規とコンパスによる作図を現代代数学の観点から扱っている。

6.4 四次方程式を解く

問題

STEP III 2017、問 3

先に進む前に、まず問題を読んでおこう。問題は STEP Support Programme の問題データベースにある：

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

導入

二次方程式（quadratic equation）の解の公式は誰もが学ぶ。三次方程式（cubic）や四次方程式（quartic）にも解の公式は存在する。それらは 16 世紀のイタリアで、秘密の勝負と先取権をめぐる激しい論争のさなかに発見された。ジェロラモ・カルダーノ（Gerolamo Cardano）は 1545 年の著書 *Ars Magna*（『アルス・マグナ』）で両方の解法を発表した。三次方程式の解法はニコロ・タルタリア（Niccolò Tartaglia）から得たもので、タルタリアはカルダーノに秘密を守ると誓わせていた。四次方程式の解法はカルダーノ自身の弟子ロドヴィコ・フェラーリ（Lodovico Ferrari）によるものである。その後およそ三百年にわたって、数学者たちは五次方程式（quintic）の解の公式を探し求めたが、ついに見つけることはできなかった。

この問題は四次方程式を解く仕掛けを示しており、しかもその仕掛けには深い意味がある。四つの根を、考えられる三通りの方法で二つずつ組にし、そこから三つの新しい量を作る。この三つの量はある三次方程式を満たし、それは解くことができる。そしてこれらの量から元の根が求まるのである。これが**なぜ**うまくいくのか、すなわち四つの根は三つの量に帰着できるのに、五つの根は同じように帰着できないのはなぜか、という問いこそが、ガロア（Galois）を群論（group theory）の創始へと導いたのである。

取りかかる前に

考えてみよう　四つの対象 $\alpha, \beta, \gamma, \delta$ を二つの組に分ける方法は何通りあるか。

三通りある。$\{\alpha\beta, \gamma\delta\}$、$\{\alpha\gamma, \beta\delta\}$、$\{\alpha\delta, \beta\gamma\}$ である（図 6.4.1）。問題に現れる三つの量 $\alpha\beta + \gamma\delta$ などは、これら三つの組分けに対応している。四つの根をどのように並べ替えても、三つの組分けが互いに入れ替わるだけである。したがって、三つの量についての対称式（symmetric expression）はどれも四つの根についての対称式であり、p, q, r, s を用いて表せる。これが、三つの量が p, q, r, s のみを含む係数をもつ三次方程式を満たす理由である。

順を追って解く

段階 1　欠けている係数

考えてみよう　三次方程式 $y^3 + Ay^2 + By + C = 0$ において、根の和を A で表すとどうなるか。また、$(\alpha\beta + \gamma\delta) + (\alpha\gamma + \beta\delta) + (\alpha\delta + \beta\gamma)$ を四次方程式の係数で表すとどうなるか。

三次方程式の根の和は $-A$ である。三つの量の和は、$\alpha, \beta, \gamma, \delta$ から二つずつ選んだ積六つすべての和であり、四次式 $x^4 + px^3 + qx^2 + rx + s$ についてこれは q に等しい。よって $A = -q$ である。

段階 2　具体的な三次方程式

$p = 0, q = 3, r = -6, s = 10$ のとき、三次方程式は

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

となる。

考えてみよう　84 の小さな約数を試してみよ。

$y = 2$ とすると $8 - 12 - 80 + 84 = 0$ となる。割り算をすると $y^3 - 3y^2 - 40y + 84 = (y - 2)(y^2 - y - 42) = (y - 2)(y - 7)(y + 6)$ である。最大の根は 7 なので、$\alpha\beta + \gamma\delta = 7$ である。 ■

段階 3　根の組

$(\alpha + \beta)(\gamma + \delta) = \alpha\gamma + \alpha\delta + \beta\gamma + \beta\delta$ であり、これは二つずつの積六つすべての和から

$\alpha\beta+\gamma\delta$ を引いたもの、すなわち $q-7=3-7=-4$ である。

また $\alpha\beta\cdot\gamma\delta=\alpha\beta\gamma\delta=s=10$ である。よって $\alpha\beta$ と $\gamma\delta$ は和が 7、積が 10 であり、$t^2-7t+10=(t-2)(t-5)$ の根である。$\alpha\beta>\gamma\delta$ とすると、$\alpha\beta=5, \gamma\delta=2$ である。■

段階 4 四次方程式を解く

> **手を止めて、やってみよう** $\alpha+\beta$ と $\gamma+\delta$ を求めよ。両者の和（p から）と積（段階 3 から）はわかっている。どちらがどちらかを決めるには r を用いよ。

$\alpha+\beta+\gamma+\delta=-p=0$ かつ $(\alpha+\beta)(\gamma+\delta)=-4$ なので、$\{\alpha+\beta,\gamma+\delta\}=\{2,-2\}$ である。係数 r からは三つずつの積四つの和が得られる：$\alpha\beta\gamma+\alpha\beta\delta+\alpha\gamma\delta+\beta\gamma\delta=-r=6$。これは $\alpha\beta(\gamma+\delta)+\gamma\delta(\alpha+\beta)=5(\gamma+\delta)+2(\alpha+\beta)$ と書ける。$\alpha+\beta=2$ ならばこれは $-10+4=-6$ となり、$\alpha+\beta=-2$ ならば $10-4=6$ となる。よって $\alpha+\beta=-2$, $\gamma+\delta=2$ である。

すると α,β は $t^2+2t+5=0$ の根であり、$-1\pm2\mathrm{i}$ となる。また γ,δ は $t^2-2t+2=0$ の根であり、$1\pm\mathrm{i}$ となる。四つの根は

$$x=-1\pm2\mathrm{i},\qquad x=1\pm\mathrm{i}.\qquad\blacksquare$$

である。検算：$(x^2+2x+5)(x^2-2x+2)=x^4+3x^2-6x+10$。

振り返り

- **対称式。**どの段階でも、解と係数の関係（relations between roots and coefficients）、すなわち根の和や積を用いた。
- **次数を下げる。**四次方程式の問題が三次方程式（**分解三次方程式**（resolvent cubic））に、さらに二つの二次方程式になった。
- **すべての情報を使う。**p と q から和と積が得られ、s によって $\alpha\beta$ と $\gamma\delta$ が分けられ、r によってどの組がどちらの和に対応するかが決まった。

背後にある数学

仕掛けがうまくいく理由：根の置換

1770 年、ジョゼフ＝ルイ・ラグランジュ（Joseph-Louis Lagrange）は、三次方程式や四次方程式の解法がなぜうまくいくのかを問い、その答えを根の**置換**（permutation）

に見いだした。四つの根を並べ替える方法は 24 通りある。そのどれによっても、三つの量 $y_1 = \alpha\beta + \gamma\delta$, $y_2 = \alpha\gamma + \beta\delta$, $y_3 = \alpha\delta + \beta\gamma$ は互いに入れ替わるだけである。四つの根の並べ替えはそれぞれ、三つの組分けの並べ替えを引き起こすのである（図 6.4.1）。したがって、これらの量は根について対称な係数をもつ次数 3 の多項式を満たす。現代の言葉でいえば、対称群（symmetric group）S_4（24 個の置換すべて）から S_3（組分けの 6 個の置換）への全射な群準同型（group homomorphism）が存在し、それこそが四次方程式を三次方程式に帰着できる理由である。

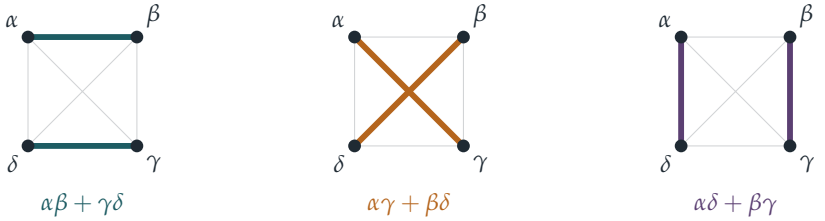


図 6.4.1　四つの根を二つの組に分ける三通りの方法と、それに対応する分解三次方程式の根。$\alpha, \beta, \gamma, \delta$ をどのように並べ替えても、これら三つの図が互いに入れ替わるだけである。そのため、三つの量は四次方程式の係数で表せる係数をもつ三次方程式を満たす。

五次方程式

五つの根の場合について、ラグランジュは根の置換のもとで少数の値しかとらない同様の量を探したが、役に立つものは見つからなかった。1799 年にパオロ・ルフィニ（Paolo Ruffini）が、そして 1824 年にニールス・ヘンリック・アーベル（Niels Henrik Abel）が（証明を完成させて）、四則演算と冪根（radicals）だけを用いた五次方程式の根の一般的な公式は存在しないことを示した。その数年後、エヴァリスト・ガロアは、どの多項式が冪根によって解けるのかを正確に説明した。それは、**根の対称性のなす群**がある特定の仕方でより単純な部分に分解できるような多項式である。対称群 S_4 はそのように分解できる（S_3 やより小さな群を経由して）が、S_5 はできない。S_5 には、それ以上分解できない大きさ 60 の「単純」（simple）な部分が含まれているからである。ガロアは 1832 年、二十歳で決闘により命を落とす前夜に、自らの理論を急いで書き上げた。この理論は今日、数学の学位課程における至宝の一つであり、通常は三年次に学ぶ。

三次方程式を解く

三次方程式そのものも同様の仕掛けで解ける。被約三次式（depressed cubic）$x^3 - 3px + q$ を二つの完全立方（perfect cube）の組み合わせとして書くと、二次方程式に帰着される。これが演習にある 2011 年の問題の方法であり、カルダーノの公式と同値である。三次方程式が三つの実数解をもつときでも、この公式は途中で複素数（complex numbers）を必要とする。この現象が、数学者たちに複素数を真剣に扱うことを迫ったのである（第 5 章の導入を参照）。

思考のスキル

> **対称性が複雑さを減らす**
>
> 根から作ったいくつかの量が、根を置換したときに互いに入れ替わるだけならば、それらの量は係数を計算できるより低い次数の多項式を満たす。
>
> これがガロア理論（Galois theory）の萌芽である。すなわち、方程式を理解するには、その根の対称性を理解せよ、ということである。

次の一歩

1. **三次方程式を確かめる。** $y_1 = \alpha\beta + \gamma\delta$ などとするとき、$y_1y_2 + y_2y_3 + y_3y_1 = pr - 4s$ であることを確かめよ。（展開して、$\sum\alpha = -p, \sum\alpha\beta\gamma = -r, \alpha\beta\gamma\delta = s$ を用いよ。）

2. **立方の和としての三次方程式。** STEP III 2011、問 3（`step.maths.org/questions/11-s3-q3`）に取り組んでみよ。この問題は、三次式を二つの立方の組み合わせとして書くことで三次方程式を解くもので、本節とはまったく異なる道筋である。答えを数値的に確かめよ。

3. **もう一つの四次方程式。** 本節の方法を用いて $x^4 - 4x^3 + 7x^2 - 6x + 2 = 0$ を解け。（分解三次方程式の根の一つは小さな整数である。）

4. **置換を数える。** $\alpha, \beta, \gamma, \delta$ の 24 個の置換のうち、組分け $\{\alpha\beta, \gamma\delta\}$ を自分自身に移すものをすべて求めよ。それが 8 個あることを示せ。（これらは S_4 の部分群（subgroup）をなす。）

さらに学ぶために

- **Mario Livio, *The Equation That Couldn't Be Solved*** (Simon & Schuster)。五次方程式と群論誕生の物語を、一般の読者向けに描いたもの。
- **Ian Stewart, *Why Beauty Is Truth: A History of Symmetry*** (Basic Books)。バビロニアの方程式からガロア、そしてその先までを扱う。
- **Ian Stewart, *Galois Theory*** (CRC Press)。学部生向けの教科書で、まさにこの内容を扱う歴史的な序章がある。

6.5 公理から考える微分

問題

STEP II 1992、問 4

先に進む前に、まず問題を読んでおこう。問題は STEP Support Programme の問題データベースにある：

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

導入

微分（differentiation）とは何か。学校では極限（limit）$\lim_{h\to 0}\frac{f(x+h)-f(x)}{h}$ によって定義され、そのあとで規則を学ぶ。和の導関数（derivative）は導関数の和であること、積の法則（product rule）などである。この問題はその順序をひっくり返す。極限のことは完全に忘れよう。ある演算について知っているのは、それが和の法則、積の法則、定数に関する規則に従い、x を 1 に写すということだけだとする。すると、少なくとも多項式（polynomial）の上では、それは微分で**なければならない**ことを、この問題は示している。

これは微積分に対する代数学者の見方である。すなわち、演算は公式によってではなく、それが従う規則によって特徴づけられる。積の法則に従う演算は**導分**（derivation）とよばれ、代数学、幾何学、物理学のいたるところに現れる。意外なことに、同じ考え方が現代の機械学習（machine learning）システムを訓練するソフトウェアの内部でも働いている。

取りかかる前に

考えてみよう 規則 (i) は積の法則である。積の法則から、定数について何がわかるだろうか。（定数を積とみなしてみよう。）

数 1 は 1×1 に等しい。1×1 に積の法則を適用すると $\Diamond 1$ がそれ自身と関係づけられ、そこからそれが 0 でなければならないことが導かれる。一般に、このような公理（axiom）を扱うときのこつは、巧みに選んだ単純な入力に公理を適用することである。

順を追って解く

段階 1　定数

> **考えてみよう**　$\mathrm{f} = \mathrm{g} = 1$ として規則 (i) を適用せよ。次に、ほかの定数に対しては規則 (iv) を用いよ。

$\Diamond 1 = \Diamond(1 \cdot 1) = 1 \cdot \Diamond 1 + 1 \cdot \Diamond 1 = 2\Diamond 1$ であるから、$\Diamond 1 = 0$ である。任意の定数（constant）λ に対して、規則 (iv) より $\Diamond \lambda = \Diamond(\lambda \cdot 1) = \lambda \Diamond 1 = 0$ である。 ■

段階 2　累乗

規則 (iii) を用いると $\Diamond x^2 = \Diamond(x \cdot x) = x\Diamond x + x\Diamond x = 2x$ である。さらに

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

> **手を止めて、やってみよう**　すべての正の整数 n について $\Diamond x^n = n x^{n-1}$ であることを、数学的帰納法（induction）によって証明せよ。

$n = 1$ の場合は規則 (iii) そのものである。$\Diamond x^n = n x^{n-1}$ ならば

$$\Diamond x^{n+1} = \Diamond(x^n \cdot x) = x\Diamond x^n + x^n \Diamond x = x \cdot n x^{n-1} + x^n = (n+1)x^n. \qquad \blacksquare$$

段階 3　すべての多項式

一般の多項式は $\mathrm{h}(x) = a_0 + a_1 x + \cdots + a_m x^m$ である。規則 (ii)（を繰り返し適用したもの）と規則 (iv) により

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

振り返り

- **公理が演算を決定する。**極限に一切触れない 4 つの規則が、多項式上の $\Diamond$ を完全に決定した。
- **生成元（generators）。**すべての多項式は、定数と x から加法と乗法を用いて組み立てられる。構成要素に対して $\Diamond$ が何をするか、そしてそれが組み立てのための演算とどう関わるかがわかれば、それはいたるところで決まる。

- **構成に沿った帰納法。** 証明は多項式の組み立て方をなぞっていた。まず乗法の繰り返しによって累乗を扱い、次に和を扱ったのである。

背後にある数学

導分

ある代数系の上の演算 D が加法的であり、積の法則 $D(fg) = fD(g) + gD(f)$ を満たすとき、それを**導分**という。この問題が示すのは、多項式の上では、定数を 0 に写す導分は $D(x)$ によって完全に決定されるということである。実際 $D(h) = h'(x)\,D(x)$ であり、自由に選べるのは多項式 $D(x)$ だけである。規則 (iii) は $D(x) = 1$ と定めている。導分は数学のさまざまな場面に現れる。幾何学では、曲面上の**ベクトル場**（vector field）を、その曲面上の関数に対する導分として定義できる（ベクトル場の方向に関数を微分するのである）。代数学では、ある構造の導分はその「無限小の対称性」を測る。物理学では、量子力学の交換子（commutator）$[A, B] = AB - BA$ が各引数について導分になっている。

極限を使わない微積分

代数的な導関数は、極限がまったく意味をもたない状況でも機能する。素数 p を法とする算術のような有限体（finite field）の上には極限は存在しないが、多項式の形式的導関数（formal derivative）は同じ規則によって定義され、それでもなお重根（repeated root）を検出できる。多項式 f が重根をもつのは、f と f' が共通因数をもつときであり、かつそのときに限る。たとえば、$p \nmid n$ のとき $x^n - 1$ が重根をもたないことはこのようにして示される。これは、Section 6.1 の円分多項式（cyclotomic polynomial）を有限体上で定義するのに必要な事実である。同じ考え方は符号理論（coding theory）や暗号理論（cryptography）でも用いられている。

自動微分

ここで現代的な応用を紹介しよう。$\varepsilon^2 = 0$ だが $\varepsilon \neq 0$ であるような数 ε を考え出し、**二重数**（dual numbers）$a + b\varepsilon$ で計算を行う。すると $(a + b\varepsilon)(c + d\varepsilon) = ac + (ad + bc)\varepsilon$ となり、ε の部分はまさに積の法則に従う。したがって、任意の多項式について

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

が成り立ち、二重数 $x + \varepsilon$ において f を評価すると、値と導関数の値が同時に、しかも正確に計算される。極限は不要であり、小さな差をとることによる丸め誤差も生じない（図 6.5.1）。これを**フォワードモード自動微分**（forward-mode automatic

differentiation）という。その親戚であるリバースモードは、数十億のパラメータをもつニューラルネットワーク（neural networks）を訓練するのに使われるアルゴリズム（**誤差逆伝播法**（backpropagation））である。このようなシステムが学習するたびに、積の法則と連鎖律（chain rule）を導分として一歩ずつ適用しているのである。

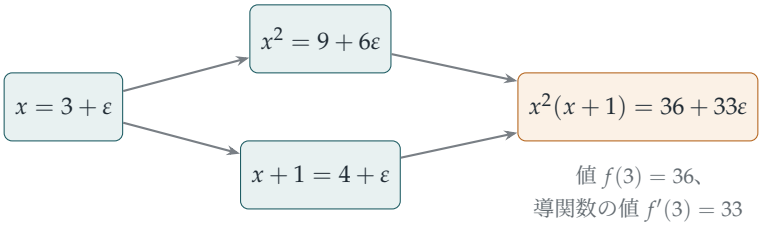


図 6.5.1　二重数（$\varepsilon^2 = 0$）を用いた、$x = 3$ における $f(x) = x^2(x+1)$ の自動微分。各段階は問題の規則に従っている。すなわち $(3+\varepsilon)^2 = 9 + 6\varepsilon$、$(9+6\varepsilon)(4+\varepsilon) = 36 + (9+24)\varepsilon$ である。ε の係数は $f'(3) = 3 \cdot 9 + 2 \cdot 3 = 33$ であり、正確に計算されている。

思考のスキル

性質によって特徴づける

演算をそれが従う規則によって記述し、その規則が演算をただ一つに決定することを示す。

これは公理的方法（axiomatic method）であり、大学の代数学の中心にある。その強みは、公理から証明したことが、それを満たすあらゆる演算に当てはまる点にある。多項式の微分であれ、曲面上の関数の微分であれ、まだ発明されていない何かであれ、である。

次の一歩

1. **別の導分。** $\Diamond$ が規則 (i)、(ii)、(iv) を満たすが、1 の代わりに $\Diamond x = x$ であるとする。$\Diamond \mathrm{h}(x) = x\,\mathrm{h}'(x)$ を示せ。$\Diamond$ は x^n をどう写すか。

2. **商の法則。** 規則 (i) が引き続き成り立つと仮定して、$\Diamond$ を有理関数（rational functions）f/g に拡張する。$\mathrm{g} \cdot \frac{\mathrm{f}}{\mathrm{g}} = \mathrm{f}$ に規則 (i) を適用して、商の法則（quotient rule）を導け。

3 **重根。** $(x-a)^2$ が多項式 f を割り切るならば、$x-a$ は f′ を割り切ることを示せ。これを用いて、x^n-1 が重根をもたないことを示せ。

4 **二重数。** 二重数を用いて、$f(x)=(x^2+1)^3$ に対する $f(2)$ と $f'(2)$ を計算し、連鎖律で検算せよ。

さらに学ぶために

- **Peter Cameron, *Introduction to Algebra***（Oxford University Press）。大学 1 年次の水準で環（rings）、多項式、体（fields）を扱い、形式的導関数も取り上げている。
- **Andreas Griewank & Andrea Walther, *Evaluating Derivatives***（SIAM）。自動微分に関する標準的な文献。上級者向け。
- **Michael Nielsen, *Neural Networks and Deep Learning***（オンラインで無料公開）。第 2 章で誤差逆伝播法がわかりやすく解説されている。

6.6 部分群の和集合

問題

STEP II 1988、問 9

先に進む前に、まず問題を読んでおこう。問題は STEP Support Programme の問題データベースにある：

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

導入

これは本書でもっとも短い問題の一つであり、同時に大学の数学らしさがもっともよく表れた問題の一つでもある。題材は対称性を記述する数学の言語である**群**（group）で、問われているのはパズルのような問いである。すなわち、群をその内部にあるより小さな二つの群で覆い尽くすことはできるだろうか。答えは「できない」であり、証明はわずか 3 行で済む。ところが、小さな群が三つあれば覆うことができる。これは意外な事実である。

群論は 2019 年まで STEP の出題範囲に含まれており、現在では大学 1 年次の定番の内容である。この問題に必要なのは以下に述べる定義だけであり、群論の研究者がどのように考えるかを初めて味わうのにうってつけである。公理（axiom）だけを用いた、短く巧妙な議論である。

取りかかる前に

群とは、演算（積の形 ab で書く）をもつ集合 G であって、次の条件を満たすものである。

- 演算は**結合的**（associative）である：$(ab)c = a(bc)$。
- すべての a に対して $ea = ae = a$ を満たす**単位元**（identity）e が存在する。
- すべての a に対して、$aa^{-1} = a^{-1}a = e$ を満たす**逆元**（inverse）a^{-1} が存在する。

例としては、加法に関する整数全体（正の数、負の数、0）、乗法に関する 0 でない実数

全体、合成に関する正方形の回転全体などがある。G の**部分群**（subgroup）とは、G の部分集合 K であって、同じ演算に関してそれ自身が群となるものである。すなわち、K は e を含み、$a, b \in K$ ならば $ab \in K$ かつ $a^{-1} \in K$ が成り立つ。

> **考えてみよう**　K が部分群で、$a \in K$ だが $b \notin K$ であるとき、ab は K に属しうるだろうか。

属しえない。もし $ab \in K$ ならば、$b = a^{-1}(ab)$ は K の二つの元の積となり、したがって K に属してしまう。このささやかな観察が証明のすべてである。

順を追って解く

段階 1　二つの部分群では覆えない

背理法（proof by contradiction）を用いる。$G = G_1 \cup G_2$ であるが、G_1 も G_2 も G 全体ではないと仮定する。

> **考えてみよう**　$G_1 \neq G$ であるから、G_1 に属さない元が存在する。その元はどこに属さなければならないか。G_2 についても同様である。次に、その二つの元を掛け合わせてみよ。

$a \notin G_1$ を満たす $a \in G$ をとる。すべての元は G_1 または G_2 に属するので、$a \in G_2$ である。また $b \notin G_2$ を満たす $b \in G$ をとると、$b \in G_1$ である。積 ab を考える。これは G_1 または G_2 に属する。

- $ab \in G_1$ の場合：$b \in G_1$ であるから、$a = (ab)b^{-1} \in G_1$ となり矛盾する。
- $ab \in G_2$ の場合：$a \in G_2$ であるから、$b = a^{-1}(ab) \in G_2$ となり矛盾する。

いずれの場合も矛盾が生じるので、$G_1 = G$ または $G_2 = G$ である。 ■

G が有限であることは一度も使っていないことに注意しよう。この結果はすべての群について成り立つ。

段階 2　三つの部分群なら覆える

> **手を止めて、やってみよう**　三つの部分群の和集合（union）となる群であって、どの部分群も群全体ではないものを見つけよ。（**ヒント**：すべての元が自分自身の逆元であるような小さな群を試してみよ。）

クラインの四元群（Klein four-group）$V = \{e, a, b, c\}$ を考える。規則は $a^2 = b^2 = c^2 = e$

および $ab = ba = c$、$bc = cb = a$、$ca = ac = b$ である。（具体的には、正方形でない長方形の四つの対称変換、すなわち何もしない変換、180° の回転、二つの軸それぞれに関する鏡映である。あるいは、ビット 0、1 の組 (x, y) 全体に 2 を法とする加法を考えたものでもよい。）その三つの部分群

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

はいずれも 2 個の元からなり、どれも群全体ではないが、合わせると V のすべての元を含む（図 6.6.1）。 ■

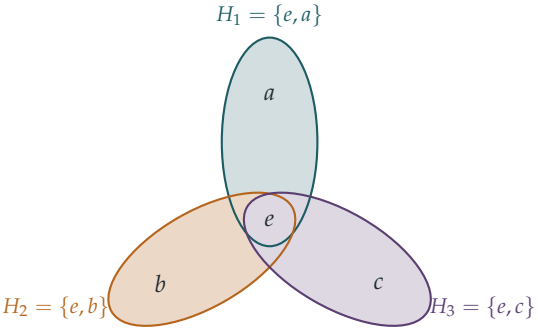


図 6.6.1　クラインの四元群 $\{e, a, b, c\}$ は、位数（order）2 の三つの部分群の和集合である。これらの部分群は単位元 e だけを共有している。問題の前半により、どの群も二つの真部分群（proper subgroup）だけの和集合にはなりえない。

振り返り

- **証拠となる元を選び、組み合わせる。**証明では、各部分群の外にある元を一つずつ選び、それらを掛け合わせた。この「それぞれから一つずつとって組み合わせる」という手法は、代数学できわめてよく使われる。
- **閉じていることの威力。**用いた部分群の性質は、積と逆元について閉じている（closed）ということだけであった。
- **必要な仮定を確かめる。**有限性は与えられていたが、使われなかった。ある仮定が不要であると気づくことも、証明を理解することの一部である。

背後にある数学

対称性の言語

群は 19 世紀に、いくつもの方向から同時に生まれた。多項式の根の置換に関するガロア（Galois）の研究（Section 6.4）、置換に関するコーシー（Cauchy）の研究、そして幾何学や結晶学における対称性の研究である。上で述べた抽象的な定義、すなわち三つの公理を満たすものはすべて群であるという定義は、19 世紀末までに確立した。その威力は一般性にある。この問題のように公理から証明された定理は、数の群、行列の群、対称変換の群、置換の群のすべてについて同時に成り立つのである。今日、群はいたるところに現れる。素粒子物理学（標準模型は対称性の群の上に築かれている）、化学（分子の対称性がスペクトルを決める）、暗号理論（楕円曲線の群、Section 1.9）、そしてルービックキューブの解法などである。

いくつの部分群が必要か

この問題からは自然な問いが生まれる。和集合が群全体となるような真部分群の個数の最小値はいくつか。この問題により、それが 2 になることはない。1926 年に Gaetano Scorza は、群が三つの真部分群の和集合となるのは、クラインの四元群を「商」（quotient）としてもつときであり、かつそのときに限ることを示した。1994 年に J. H. E. Cohn はこの一般的な問題を研究していくつかの予想を立て、1997 年に M. J. Tomkinson は、この最小値が 7 となる群は存在しないことを証明した。一方、3 から 6 までの数はすべて実際に現れる。述べるのは簡単だが驚くほど奥が深い、このような問いは群論に典型的なものである。

ベクトル空間

同様の議論により、実数上のベクトル空間（vector space）（平面や 3 次元空間など）は、有限個の真部分空間（proper subspace）の和集合には決してならないことが示される。つまり、平面は原点を通る有限個の直線の和集合にはならない。しかし有限体（finite field）上ではそれが可能である。二つの元からなる体の上の平面は、まさにクラインの四元群そのものであり、その三本の直線の和集合となっている。

思考のスキル

公理から議論する

抽象代数学では、対象について、それが満たす公理以外には何もわからないことが多い。証明はそれらの公理だけを用いなければならない。

このため、議論はここでのように短く簡潔なものにならざるをえず、そしてあらゆる場合に適用できるものとなる。慣れるには少し時間がかかるが、これは大学 1 年次の代数学の授業でもっとも特徴的な体験の一つである。

次の一歩

1. **群であることを確かめる。** クラインの四元群の乗積表を書き出し、群の公理を確かめよ。また、乗法に関する群 $\{1, i, -1, -i\}$ とは同じでないことを示せ。（ヒント：自分自身の逆元となっている元はどれか。）

2. **巡回群。** すべての元がある一つの元 g のべきであるとき、その群は**巡回群**（cyclic group）であるという。巡回群は、いくつあっても真部分群の和集合にはならないことを示せ。（ヒント：g を含む部分群はどれか。）

3. **整数全体。** $(\mathbb{Z}, +)$ が部分群 $2\mathbb{Z}$（偶数全体）と $3\mathbb{Z}$（3 の倍数全体）の和集合ではないことを直接示せ。また、何らかの二つの真部分群の和集合になることはあるか。

4. **平面内の直線。** やや難 平面 $\mathbb{R}^2$ は原点を通る有限個の直線の和集合ではないことを示せ。（ヒント：各直線は、放物線 $y = x^2$ 上の点を原点以外には高々一つしか含まない。）

さらに学ぶために

- **M. A. Armstrong, *Groups and Symmetry***（Springer）。幾何学的な例を軸に展開される、美しい図版入りの入門書（『群と対称性』）。
- **Nathan Carter, *Visual Group Theory***（Mathematical Association of America）。図を通して群を学ぶ本で、大学入学前に最適である（『目で見る群論』）。
- **Peter Neumann, Gabrielle Stoy & Edward Thompson, *Groups and Geometry***（Oxford University Press）。オックスフォード大学 1 年次の古典的な教科書（『群と幾何学』）。

6.7 四元数群

問題

STEP III 1993、問 5

先に進む前に、まず問題を読んでおこう。問題は STEP Support Programme の問題データベースにある：

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

導入

1843 年 10 月 16 日、ダブリンのロイヤル運河沿いを妻と散歩していたハミルトン（William Rowan Hamilton）は、何年も追い求めていたひらめきを得た。彼は、複素数が数の組（対）を掛け合わせるのと同じように、三つ組の数を掛け合わせようとしては失敗していた。そのとき突然、答えには 4 つの数と、順序が意味をもつ乗法、すなわち $ij \neq ji$ となる乗法が必要だと気づいたのである。彼はその規則をブルーム橋の石に刻みつけた。

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

これが**四元数**（quaternions）である。この問題では、四元数を複素数の組から構成し、その中にねじれた乗法をもつ 8 個の元からなる小さな群（group）を見いだす。今日、四元数はあらゆるコンピュータゲーム、フライトシミュレータ、宇宙船の誘導システムにおいて、3 次元の回転を記述するのに用いられている。

取りかかる前に

群の定義については Section 6.6 を参照せよ。さらに 2 つの用語を導入する。群の元 g の**位数**（order）とは、$g^n = e$ となる最小の正の整数 n のことである。また、2 つの群が**同型**（isomorphic）であるとは、演算を保つ 1 対 1 の対応がそれらの間に存在することであり、つまり両者は「ラベルが違うだけの同じ群」である。

? **考えてみよう** 組 (z_1, z_2) を「数」$z_1 + z_2\mathrm{j}$ を表すものと考えよ。ここで j は新しい記号で、$\mathrm{j}^2 = -1$ を満たし、複素数 w に対して $\mathrm{j}w = w^*\mathrm{j}$ を満たすとす

? る。これらの規則を用いて $(z_1 + z_2\mathrm{j})(w_1 + w_2\mathrm{j})$ を計算せよ。$\circ$ の式が得られるだろうか。

$(z_1 + z_2\mathrm{j})(w_1 + w_2\mathrm{j}) = z_1w_1 + z_1w_2\mathrm{j} + z_2\mathrm{j}w_1 + z_2\mathrm{j}w_2\mathrm{j} = z_1w_1 + z_1w_2\mathrm{j} + z_2w_1^*\mathrm{j} + z_2w_2^*\mathrm{j}^2$ であり、これは $(z_1w_1 - z_2w_2^*) + (z_1w_2 + z_2w_1^*)\mathrm{j}$ に等しい。その通りである。演算 $\circ$ は、姿を変えた四元数の乗法なのである。

順を追って解く

段階 1　行列による結合法則の証明

$(a \circ b) \circ c = a \circ (b \circ c)$ を直接確かめるのは長い計算になる。もっと鮮やかな方法がある。

? **考えてみよう**　(z_1, z_2) に複素行列 $M = \begin{pmatrix} z_1 & z_2 \\ -z_2^* & z_1^* \end{pmatrix}$ を対応させる。行列の積 $M(z_1, z_2)\,M(w_1, w_2)$ の第 1 行は何か。

積の第 1 行は $(z_1w_1 - z_2w_2^*,\ z_1w_2 + z_2w_1^*)$ であり、これはちょうど $(z_1, z_2) \circ (w_1, w_2)$ である。第 2 行は $(-(z_1w_2 + z_2w_1^*)^*,\ (z_1w_1 - z_2w_2^*)^*)$ であるから、積も同じ特別な形をしている。したがって $M(a \circ b) = M(a)M(b)$ である。行列の乗法は結合法則（associativity）を満たし、M は 1 対 1 である（第 1 行から z_1、z_2 を読み取れる）から、$\circ$ は結合法則を満たす。 ■

段階 2　可換ではない

$(0,1) \circ (\mathrm{i}, 0) = (0 \cdot \mathrm{i} - 1 \cdot 0,\ 0 \cdot 0 + 1 \cdot \mathrm{i}^*) = (0, -\mathrm{i})$ であるが、$(\mathrm{i}, 0) \circ (0, 1) = (0, \mathrm{i})$ である。よって $\circ$ は可換（commutative）ではない。

次の 4 つの特別な積は定義から直ちに従う。

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

段階 3　8 個の元からなる群

四元数の記法では $A = 1$、$C = \mathrm{i}$、$B = \mathrm{j}$、$D = \mathrm{ij} = \mathrm{k}$ であり、E, G, F, H はそれぞれの符号を変えたものである。S_1 のすべての元は、$u \in \{1, \mathrm{i}, -1, -\mathrm{i}\}$ として $(u, 0)$ または $(0, u)$ の形をしている。

考えてみよう 4 つの特別な積を用いて、S_1 が閉じていることを示せ。単位元は何か。

4 つの特別な積により、$(u,0)$ または $(0,u)$ の形の 2 つの元の積は再びこれらのいずれかの形になり、その第 1 成分または第 2 成分は uv、uv^* または $-uv^*$ である。$\{1,\mathrm{i},-1,-\mathrm{i}\}$ は乗法、共役（conjugation）、符号の反転について閉じている（closed）から、積は S_1 に属する。単位元（identity）は $A=(1,0)$ である。実際、$(1,0)\circ(w_1,w_2)=(w_1,w_2)$ かつ $(w_1,w_2)\circ(1,0)=(w_1,w_2)$ である。

手を止めて、やってみよう 各元の位数と逆元を求めよ。

A の位数は 1 である。$E\circ E=(-1,0)\circ(-1,0)=(1,0)$ であるから、E の位数は 2 である。$C=(\mathrm{i},0)$ については $C\circ C=(-1,0)=E$ であるから、C の位数は 4 であり、$C^{-1}=C^3=E\circ C=G$ である。$B=(0,1)$ については $B\circ B=(-1\cdot 1^*,0)=(-1,0)=E$ であるから、B の位数は 4 であり、$B^{-1}=F$ である。同様に $D\circ D=(-\mathrm{i}\cdot\mathrm{i}^*,0)=(-\mathrm{i}\cdot(-\mathrm{i}),0)=(-1,0)=E$ であるから、D の位数は 4 で、逆元は H である。そして G、F、H はそれぞれ C、B、D の逆元（inverse）であり、これらの位数も 4 である。まとめると次のようになる。

元	A	B	C	D	E	F	G	H
逆元	A	F	G	H	E	B	C	D
位数	1	4	4	4	2	4	4	4

閉じていること、結合法則（第 1 段階）、単位元、逆元がそろったので、S_1 は群である。■これを**四元数群**（quaternion group）Q_8 という。

段階 4 部分群

$\{A,B,E,F\}=\{1,\mathrm{j},-1,-\mathrm{j}\}$ は B のべきからなる。すなわち $B^1=B$、$B^2=E$、$B^3=F$、$B^4=A$ である。よってこれは閉じていて逆元を含むから、部分群（subgroup）であり、位数 4 の**巡回群**（cyclic group）である。行列 $J=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$ は $J^2=-I$、$J^3=-J$、$J^4=I$ を満たすから、これも位数 4 の巡回群を生成する。$B^k\leftrightarrow J^k$ という対応は同型写像（isomorphism）である。■（実際、J はちょうど $M(0,1)$、つまり B に対応する行列である。）

振り返り

- **行列で表現する。**直接確かめるのは骨の折れる結合法則が、行列の乗法から受け継

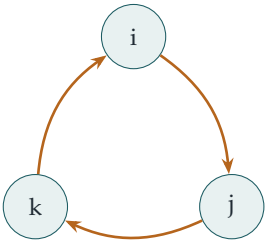
がれた。

- **式の背後にある構造を見つける。**奇妙な演算 $\circ$ は四元数の乗法であり、そのことに気づくとすべてが易しくなった。
- **位数と逆元が群を特徴づける。**位数の表を見るだけで、Q_8 が普通でない群であることがわかる。位数 2 の元が 1 個、位数 4 の元が 6 個あるのである。

背後にある数学

複素数の先へ

実数は、加法・乗法・除法ができる 1 次元の数の体系であり、複素数は 2 次元の体系である。ハミルトンの四元数は 4 次元であり、やはり除法はできるが、乗法はもはや可換ではない（図 6.7.1）。1878 年、フロベニウス（Ferdinand Frobenius）は、$\mathbb{R}$、$\mathbb{C}$、$\mathbb{H}$（ハミルトンにちなむ）の 3 つが、結合的な乗法をもつ実数上の有限次元「多元体」（division algebras）のすべてであることを証明した。結合法則を諦める代わりに、実数・複素数・四元数と同様に大きさが乗法的である、すなわち $|xy| = |x|\,|y|$ という性質を保つことにすると、もうちょうど 1 つだけ存在する。1840 年代に John Graves とケイリー（Arthur Cayley）が発見した 8 次元の**八元数**（octonions）である。1898 年、フルヴィッツ（Adolf Hurwitz）は、このような体系がこの 4 つに限ることを証明した。（大きさに関する条件を外すと、ほかにもっと奇妙な非結合的多元体が存在するが、ボット（Raoul Bott）、ミルナー（John Milnor）、ケルヴェア（Michel Kervaire）による 1958 年の深い定理によれば、有限次元の実多元体の次元は必ず 1、2、4、8 のいずれかである。）



矢印の向き：$ij = k,\ jk = i,\ ki = j$

矢印と逆向き：$ji = -k,\ kj = -i,\ ik = -j$

さらに $i^2 = j^2 = k^2 = -1$

図 6.7.1　ハミルトンの乗法規則。i、j、k のうち 2 つを矢印の向きに掛けると残りの 1 つが得られ、矢印と逆向きに掛けると残りの 1 つの符号を変えたものが得られる。8 個の元 $\pm 1, \pm i, \pm j, \pm k$ が、この問題の四元数群 Q_8 をなす。

3 次元の回転

絶対値が 1 の四元数は 3 次元空間の回転を記述する。単位ベクトルの軸 $\mathbf{u}$ のまわりの角 θ の回転は $q = \cos\frac{\theta}{2} + \sin\frac{\theta}{2}(u_1\mathrm{i} + u_2\mathrm{j} + u_3\mathrm{k})$ に対応し、ベクトル $\mathbf{v}$（$v_1\mathrm{i} + v_2\mathrm{j} + v_3\mathrm{k}$ と表す）に $\mathbf{v} \mapsto q\mathbf{v}q^{-1}$ によって作用する。回転の合成は四元数の乗法にほかならない。この方法は行列や角度を用いるよりも効率的で数値的に安定しており、さらに「ジンバルロック」（gimbal lock）を回避できる。ジンバルロックとは自由度が 1 つ失われる現象で、アポロ計画の宇宙飛行士たちは、ジャイロスコープに基づく航法装置でこれに対処しなければならなかった。半角 $\frac{\theta}{2}$ は、深い事実への手がかりでもある。360° 回転すると $q = -1$ となり、1 にはならないのである。これは物理学者が電子のふるまい（スピン（spin））の中に見ている事実である。

4 つの平方数

四元数の絶対値は、複素数の場合と同様に乗法的であり、$|pq| = |p||q|$ が成り立つ。これを成分で書き下すと、オイラー（Euler）の**四平方恒等式**（four-square identity）が得られる。すなわち、4 つの平方数の和どうしの積は、それ自身 4 つの平方数の和である。これは、すべての正の整数が 4 つの平方数の和であるというラグランジュ（Lagrange）の定理の鍵となるステップである。この定理は Section 7.8 で証明する。これは Section 1.6 の二平方の結果の 4 次元版にあたる。

思考のスキル

> **抽象的な対象を具体的に表現する**
>
> 抽象的な演算について考えにくいときは、それがなじみのある演算になるような具体的なモデル、たとえば行列を見つけよ。
>
> そうすれば結合法則のような性質は労せずして得られる。群を行列で表現して研究するというこの考え方は、**表現論**（representation theory）という大きく美しい分野へと発展していく。

次の一歩

1 **ハミルトンの規則。** 組を用いて、$C \circ B = D$ および $B \circ C = H$、すなわち $\mathrm{ij} = \mathrm{k}$ および $\mathrm{ji} = -\mathrm{k}$ を確かめよ。

2 **位数 2 の元はただ 1 つ。** $E = -1$ が Q_8 における唯一の位数 2 の元であることを示せ。このことから、Q_8 は正方形の対称性の群（位数 2 の元を 5 個もつ）と同型でないことを導け。

3 **4 つの平方数。** $\det M(z_1, z_2) = |z_1|^2 + |z_2|^2$ を示せ。$\det(M_1 M_2) = \det M_1 \det M_2$ を用いて、4 つの平方数の和どうしの積は 4 つの平方数の和であることを導け。

4 **部分群。** Q_8 の部分群をすべて求めよ。$\{A\}$ 以外のすべての部分群は E を含むこと、および Q_8 が位数 4 の 3 つの巡回部分群の和集合であることを示せ（Section 6.6 と比較せよ）。

さらに学ぶために

- **John Conway & Derek Smith, *On Quaternions and Octonions***（A. K. Peters）。四元数と八元数の幾何と算術。高度だが非常に興味深い。
- **John Baez,「The octonions」**, *Bulletin of the American Mathematical Society* 39 (2002)。オンラインでも無料で読める。すばらしい概説であり、序論は今すぐにでも読める。
- **Andrew Hanson, *Visualizing Quaternions***（Morgan Kaufmann）。回転のための四元数と、そのグラフィックスへの応用。

6.8 特異行列からなる群

問題

STEP III 1996、問 6

先に進む前に、まず問題を読んでおこう。問題は STEP Support Programme の問題データベースにある：

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

導入

行列式（determinant）が 0 である行列は逆行列（inverse）をもたない、ということは誰もが学ぶ。それならば、すべての元が逆元をもつ行列の群（group）には、正則でない行列、すなわち特異行列（singular matrix）は含まれえないはずではないか。

実は含まれうるのである。からくりは「逆」という言葉にある。群において $\mathbf{A}$ の逆元とは、$\mathbf{A}$ と演算して**その群の**単位元（identity）を与える元のことであり、群の単位元が単位行列 $\mathbf{I}$ でなければならないとはどこにも書かれていない。この問題では、すべての行列が特異であり、単位元そのものも行列式 0 の行列であるような群を構成する。これは定義を文字どおりに読むことの教訓であり、抽象的な構造と、それに初めて出会ったときのなじみ深い例との違いについての教訓でもある。

取りかかる前に

群の定義については Section 6.6 を参照せよ。

? **考えてみよう** 小問 (i) において、単位行列 $\mathbf{I}$ は $\begin{pmatrix} a & a \\ a & a \end{pmatrix}$ の形をしていない。では、S の単位元は何でありうるだろうか。

それは S のある行列 $\mathbf{E}$ であって、S のすべての $\mathbf{X}$ に対して $\mathbf{EX} = \mathbf{XE} = \mathbf{X}$ を満たすものでなければならない。これは $\mathbf{E}$ がこの特別な形の行列にどう作用するかだけに関する条件であり、すべての行列に関する条件ではない。方程式を解いて求めればよい。

順を追って解く

段階 1　演算について閉じていること

4 つの成分がすべて a である行列を $\mathbf{M}_a$ と書く。すると

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

であり、$a, b \neq 0$ のとき $2ab \neq 0$ である。よって S は演算について閉じている（closed）。■

段階 2　群の公理

> **考えてみよう**　行列の積は結合的である。単位元については $\mathbf{M}_e\mathbf{M}_a = \mathbf{M}_a$ を解け。逆元については $\mathbf{M}_a\mathbf{M}_b = \mathbf{M}_e$ を解け。

結合法則（associativity）は行列の積から受け継がれる。**単位元**：すべての a に対して $\mathbf{M}_e\mathbf{M}_a = \mathbf{M}_{2ea} = \mathbf{M}_a$ となるのは、ちょうど $e = \tfrac{1}{2}$ のときである。公式の対称性から $\mathbf{M}_a\mathbf{M}_{1/2} = \mathbf{M}_a$ も成り立つ。よって

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

が S の単位元である。**逆元**：$b = \tfrac{1}{4a}$ のとき $\mathbf{M}_a\mathbf{M}_b = \mathbf{M}_{2ab} = \mathbf{M}_{1/2}$ であり、この b は 0 でないから、$\mathbf{M}_{1/(4a)}$ が S における $\mathbf{M}_a$ の逆元である。よって S は群である。■どの元も行列式は $a^2 - a^2 = 0$ である。

段階 3　特異性は広がる

> **手を止めて、やってみよう**　$\mathbf{A} \in G$ が特異であるとし、$\mathbf{B}$ を G の任意の元とする。$\mathbf{B}$ を $\mathbf{A}$ を含む積として表し、行列式をとってみよ。

$\mathbf{A}^{-1}$ で、群 G における $\mathbf{A}$ の逆元を表す（行列としての逆行列とは限らない）。すると $\mathbf{C} = \mathbf{A}^{-1}\mathbf{B}$ は G の元であり、

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

行列式をとると $\det\mathbf{B} = \det\mathbf{A}\,\det\mathbf{C} = 0$ である。よって G のすべての元は特異である。■特に、行列の群のある 1 つの元が行列として正則（invertible）であれば、すべての元が正則である。行列の群は、すべてが正則であるか、すべてが特異であるかのどちらかである。

段階 4 3×3 の例

考えてみよう 小問 (i) を 3×3 行列に一般化できるだろうか。あるいは、3 つの座標のうち 2 つを「無視する」行列を使って、もっと簡単なものを見つけられるだろうか。

次をとる。

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

左上隅の成分が a と b である行列の積は、左上隅の成分が ab である行列なので、G は演算について閉じている。積は結合的である。単位元は左上隅の成分が 1 の行列であり、左上隅が a の行列の逆元は左上隅が $\frac{1}{a}$ の行列である。よって G は群であり、どの元も行列式は 0 である。■（別の例：9 つの成分がすべて $a\neq 0$ に等しい 3×3 行列の全体。その単位元はすべての成分が $\frac{1}{3}$ の行列である。）

振り返り

- **定義を文字どおりに読む。**群の単位元とは、**その群の中で**単位元としてはたらく元のことであり、なじみ深い単位行列である必要はない。
- **構造を方程式から求める。**S の単位元と逆元は、推測ではなく方程式を解くことで求めた。
- **行列式は乗法的である。**この 1 つの性質だけで、特異性が 1 つの元からすべての元へ広がることが示された。

背後にある数学

冪等元と隠れた可逆性

任意の行列の群の単位元 $\mathbf{E}$ は $\mathbf{E}^2=\mathbf{E}$ を満たす。すなわち**冪等**（idempotent）である。幾何学的には、冪等行列は**射影**（projection）である。つまり、すべてのベクトルをある部分空間（subspace）の上に写し、その部分空間内のベクトルは動かさない。小問 (i) では、$\mathbf{E}$ は平面を直線 $y=x$ の上に射影し、各行列 $\mathbf{M}_a$ はまずその直線上に射影してから、直線に沿って $2a$ 倍に伸縮する（図 6.8.1）。直線上では、群は可逆な伸縮として作用し、直線に垂直な方向は単に無視している。したがって S の正体は、平面内の直線上に住む、乗法に関する 0 でない実数全体の群（対応 $\mathbf{M}_a\mapsto 2a$ による）である。

これは一般に成り立つ。すなわち、どんな行列の群も、基底を取り替えれば、その単位元の像の上に作用する正則行列の群に、0 を詰めて埋め込んだものになっている。

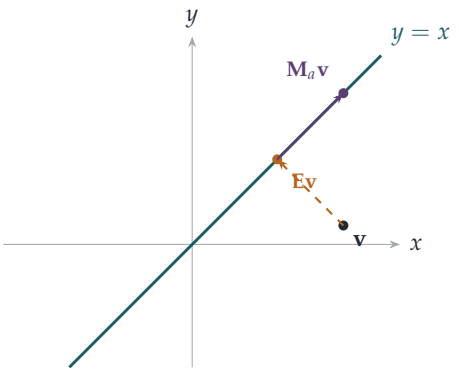


図 6.8.1　小問 (i) の行列のはたらき。単位元 $\mathbf{E}$ はすべてのベクトル $\mathbf{v}$ を直線 $y = x$ の上に射影する（琥珀色の破線）。各 $\mathbf{M}_a$ は同じ射影を行ったのち、直線に沿って $2a$ 倍に伸縮する（紫色。ここでは $2a = \frac{16}{9}$）。直線そのものの上では、群は通常の可逆な拡大・縮小として作用する。

抽象と具体

人々が最初に研究した群は具体的なものであった。置換、対称性、正則行列などである。抽象的な定義（3 つの公理を満たす演算をもつ集合）は、それらから抽出されたものである。この問題は抽象的な見方の価値を示している。S と乗法に関する 0 でない実数全体の群とは**同型**（isomorphic）であり、一方は特異行列からなり他方は数からなるにもかかわらず、装いが違うだけの同じ群なのである。見かけの異なる 2 つの構造がいつ「同じ」であるかを見抜くことは代数学の中心的なスキルの 1 つであり、同型という概念は、数学者がそれを厳密にするための手段である。

思考のスキル

なじみ深い対象についての暗黙の仮定を疑う

なじみ深い対象が抽象的な定義の中に現れたら、そのなじみ深い性質のうちどれが定義で実際に要求されているかを確かめよ。

「行列の群の単位元は $\mathbf{I}$ である」というのは当然のように聞こえるが、定義の一部ではない。そしてこの仮定を捨てることで、真に新しい例が得られた。この

ような仮定を疑うことこそ、多くの新しい数学的構造が発見されてきた方法である。

次の一歩

1 **同型写像。**写像 $\mathbf{M}_a \mapsto 2a$ が、S から 0 でない実数全体への一対一対応（one-to-one correspondence）であって、行列の積を数の積に移すことを示せ。

2 **群にならない例。**$a \neq 0$ である行列 $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ 全体の集合は積について閉じているが、群ではないことを示せ。（**ヒント：**単位元を探してみよ。左単位元はあるか。右単位元はあるか。）

3 **冪等行列。**$\mathbf{E}^2 = \mathbf{E}$ を満たす 2×2 実行列 $\mathbf{E}$ をすべて求めよ。また、それらを幾何学的に説明せよ。

4 **すべての成分が等しい行列。**すべての成分が $a \neq 0$ に等しい $n \times n$ 行列全体は積について群をなすことを示し、その単位元を求めよ。

さらに学ぶために

- **M. A. Armstrong, *Groups and Symmetry*** (Springer)。行列の群と同型を、多くの幾何学的な例とともに扱う。
- **Gilbert Strang, *Introduction to Linear Algebra*** (Wellesley-Cambridge)。射影と冪等行列がわかりやすく説明されている。
- **Joseph Gallian, *Contemporary Abstract Algebra*** (CRC Press)。風変わりな群の例を多く含む、親しみやすい入門書。

これまでに学んだこと

本章は、代数学が方程式を解くことから構造を調べることへと移り変わったことから出発し、三つの問いを立てた。何から何が作れるのか、方程式の解の公式はなぜうまくいくのか、そして抽象化によって何が得られるのか、である。本章の八つの問題が示したことを以下にまとめる。

1. 何から何が作れるか？

Section 6.3 では、冪根（radical）を一つずつ消去することで、$\sqrt{2}+\sqrt{3}$、$\sqrt{2}+\sqrt{3}+\sqrt{5}$、$\sqrt[3]{2}+\sqrt[3]{3}$ を根にもつ多項式を求めた。その次数（degree）はそれぞれ 4、8、9 であった。これらの次数は不変量（invariant）であり、その数が生成する体（field）の次数にほかならない。体の塔（tower of fields）を上るにつれて次数は掛け算で積み重なるので、平方根だけでたどり着ける数の次数は 2 の冪になる。このただ一つの事実から、立方体の倍積（doubling the cube）が不可能であること（$\sqrt[3]{2}$ の次数は 3 である）、そして 60° の角は三等分（trisection）できないことが証明される。

逆の方向として、Section 6.2 では何かが作図できる仕組みを見た。1 の 17 乗根（roots of unity）をガウス（Gauss）の周期に分けると、和 $\cos\frac{2\pi}{17}+\cos\frac{4\pi}{17}+\cos\frac{8\pi}{17}+\cos\frac{16\pi}{17}$ は $\frac{-1+\sqrt{17}}{4}$ を根にもつ二次方程式を満たした。さらに三つの二次方程式を経て $\cos\frac{2\pi}{17}$ に至り、こうして正 17 角形の作図が得られる。これら二つの節の土台にあったのが、Section 6.1 の円分多項式（cyclotomic polynomial）である。円分多項式は x^n-1 を構成する基本単位であり、1 の冪根をその位数（order）によって分類することで得られた。

2. 方程式の解の公式はなぜうまくいくのか？

Section 6.4 では四次方程式（quartic）の秘密を明らかにした。四つの根から、根の組の作り方それぞれに対応する三つの量 $\alpha\beta+\gamma\delta$、$\alpha\gamma+\beta\delta$、$\alpha\delta+\beta\gamma$ を作る。根をどのように並べ替えても、これら三つの量が入れ替わるだけなので、これらは係数のわかっている三次方程式（cubic）を満たす。その三次方程式を解き、続いて二つの二次方程式を解けば根が得られた。ラグランジュ（Lagrange）は、これがうまくいくのは四つの対象の置換（permutation）が三通りの組分けにどう作用するかによることを見抜いた。ガロア（Galois）は、五つの根に対してこれがうまくいかないのは、五つの対象の置換全体のなす群（group）が、それ以上分解できない部分を含んでいるからだと

見抜いた。解の公式とは、群の構造が落とす影なのである。

3. 抽象化によって何が得られるか？

最後の四つの節では、対象をそれが従う規則によって記述した。

- Section 6.5 では、四つの規則（加法性（additivity）、積の法則（product rule）、定数についての規則、$\Diamond x = 1$）によって、極限を一切使わずに、ある演算が微分でなければならないことが導かれた。同じ規則が、現代のソフトウェアにおける自動微分（automatic differentiation）を支えている。
- Section 6.6 では、群の公理（group axioms）から出発するわずか三行の議論によって、どんな群も二つの真部分群（proper subgroup）の和集合にはならないことが、すべての群について一度に示された。
- Section 6.7 では、複素数の組に対する奇妙な演算が、実はハミルトン（Hamilton）の四元数（quaternion）の乗法であることがわかり、それを行列で表すことで結合法則（associativity）が自動的に成り立った。
- Section 6.8 では、群の定義を文字どおりに読むことで、特異行列（singular matrix）からなる群が得られた。その単位元（identity）は単位行列ではなく、しかもその群は「本当は」0 でない実数全体のなす群が姿を変えたものであった。

いずれの場合も、抽象的な見方によって、計算だけでは見えにくくなっていたであろう事柄が説明されたのである。

4. 代数学の道具箱

手法	使った場面
ただ一つに定まる不変量による分類	1 の冪根の位数による分類（6.1）
和と積から二次方程式を作る	ガウス周期（6.2）、四次方程式（6.4）
積和公式（product-to-sum formulas）	正 17 角形（6.2）
冪根の消去	最小多項式（minimal polynomial）（6.3）
次数と塔法則（tower law）	作図の不可能性（6.3）
根の対称式（symmetric functions）	分解三次方程式（resolvent cubic）（6.4）
公理による演算の決定	導分（derivation）（6.5）
群の公理からの議論	部分群の和集合（6.6）
行列表現（matrix representation）	四元数（6.7）
同型（isomorphism）	特異行列からなる群（6.8）

この先へ

- 四元数は、Section 7.8 のラグランジュの四平方定理（four-square theorem）へとつながる。
- 独自の規則をもつ代数的対象としての行列は、第 7 章の主題である。
- ガウス整数（Gaussian integers）のように、素因数分解（factorisation）が一意に定まらないことがある数の体系の算術は、Section 1.7 のテーマであった。

大学に入る前にさらに先へ進みたい人のために

- **Mario Livio, *The Equation That Couldn't Be Solved***：五次方程式（quintic）、ガロア、そして群論の誕生を描く。
- **Nathan Carter, *Visual Group Theory***：図を通して群を学ぶ。最初に読むのに理想的な一冊。
- **M. A. Armstrong, *Groups and Symmetry***：幾何学を土台にした大学初年級の講義。
- **Ian Stewart, *Galois Theory***：物語の全貌に挑む準備ができたときに。

ガロアは決闘の末に二十歳で世を去り、数十ページの原稿を遺した。数学の世界がそれを理解するには何十年もの歳月を要した。ガロアが見抜いたのは、方程式の最も深い秘密はその係数ではなく、解のもつ対称性の中にあるということであった。異なるものに同じ名前を与え、それらが共有する構造を調べるというこの洞察は、今や数学のあらゆる分野に行き渡っている。読者はそれが多項式、多角形、四元数、行列の中で働く様子を見てきた。大学に進めば、ほとんどあらゆる場所でそれに出会うことになるだろう。

「次の一歩」の解答

これらは完全な解答ではなく、簡潔な答えとヒントである。結果と鍵となる手順を示してあるので、自分の解答を確かめるのに使ってほしい。答えを見る前に、まずそれぞれの演習問題にきちんと取り組むこと。

6.1 1 の累乗根を根にもつ多項式

1. $(x-1)(x+1) = x^2-1$ かつ $(x^2+x+1)(x^2-x+1) = x^4+x^2+1$ であり、これらの積は x^6-1 である。同様に $x^{12}-1 = (x^6-1)(x^6+1)$ であり、$x^6+1 = (x^2+1)(x^4-x^2+1) = C_4C_{12}$ である。

2. $2p$ の約数（divisor）は $1, 2, p, 2p$ であるから、$C_{2p} = \frac{x^{2p}-1}{(x-1)(x+1)C_p(x)} = \frac{x^p+1}{x+1}$ である。また、p は奇数であるから $C_p(-x) = \frac{(-x)^p-1}{-x-1} = \frac{x^p+1}{x+1}$ である。$p=3$ のとき：$C_6 = x^2-x+1 = C_3(-x)$。

3. p^k 以下の数のうち p^k と共通の因数をもつものは、p の倍数 p^{k-1} 個である。原始 p^k 乗根（primitive p^kth root）は、$x^{p^k}-1$ の根のうち $x^{p^{k-1}}-1$ の根でないものであるから、$C_{p^k} = \frac{x^{p^k}-1}{x^{p^{k-1}}-1} = C_p\left(x^{p^{k-1}}\right)$ である。よって $C_9 = x^6+x^3+1$ である。

4. $C_{15} = \frac{(x^{15}-1)(x-1)}{(x^3-1)(x^5-1)}$ である。$(x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)$ に問題文の 8 次式（octic）を掛けると $x^{15}-1$ になることを、展開して確かめよ。

6.2 ガウスの正 17 角形

1. $\eta+\eta'$ は実数でない 6 つの 7 乗根すべての和であり、-1 である。$\eta\eta'$ を展開すると、指数が $4, 6, 0, 5, 0, 1, 0, 2, 3 \pmod 7$ である 9 つの項 α^{a+b} が得られる。すなわち 1 が 3 つと、実数でない各根が 1 回ずつ現れるので、$\eta\eta' = 3-1 = 2$ である。よって η, η' は $\frac{-1\pm i\sqrt{7}}{2}$ である。η の実部から余弦の和が得られる。η の虚部は $\sin\frac{2\pi}{7} + \sin\frac{4\pi}{7} - \sin\frac{\pi}{7}$ であり、$\sin\frac{4\pi}{7} = \sin\frac{3\pi}{7} > \sin\frac{\pi}{7}$ であるから正である。したがって虚部は $+\frac{\sqrt{7}}{2}$ である。

2. $\zeta = e^{2\pi i/5}$ とすると、周期（period）$\zeta+\zeta^4 = 2\cos\frac{2\pi}{5}$ と $\zeta^2+\zeta^3$ の和は -1、積は -1 であるから、これらは $t^2+t-1=0$ の根であり、正のほうから $\cos\frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$ が得られる。作図（construction）するには：単位円の中で、直角をはさむ 2 辺が 1 と $\frac{1}{2}$ である直角三角形の斜辺は $\frac{\sqrt{5}}{2}$ である。これから $\frac{1}{2}$ を引いて半分にする

と $\cos\frac{2\pi}{5}$ が得られる。その距離の点で軸に立てた垂線は、$(1,0)$ に隣り合う頂点で円と交わる。この弦を円周に沿って順に移していけばよい。

3. どちらも小数第 5 位までで -1.28078 である。

4. 3 のべきは $3,9,10,13,5,15,11,16,14,8,7,4,12,2,6,1$ であり、16 個すべてが現れる。2 のべきは 8 回で繰り返し（$2^8 = 256 \equiv 1$）、$\{1,2,4,8,9,13,15,16\}$ を与える。これは 17 を法（modulo）とする 0 でない平方数全体である。

6.3 $\sqrt{2}+\sqrt{3}+\sqrt{5}$ を根にもつ多項式

1. $y^3 = 2\sqrt{2}+6\sqrt{3}+9\sqrt{2}+3\sqrt{3} = 11\sqrt{2}+9\sqrt{3}$ であり、$9y = 9\sqrt{2}+9\sqrt{3}$ であるから、$y^3 - 9y = 2\sqrt{2}$ である。すると $\sqrt{3} = y - \sqrt{2}$ と $\sqrt{6} = \sqrt{2}\sqrt{3}$ も y の多項式（polynomial）で表される。

2. $x - \sqrt{2} = \sqrt[3]{3}$ とおいて両辺を 3 乗すると、$x^3 + 6x - 3 = \sqrt{2}(3x^2+2)$ となる。さらに 2 乗すると $x^6 - 6x^4 - 6x^3 + 12x^2 - 36x + 1 = 0$ が得られる。

3. 有理数解の候補は ± 1 だけであり、どちらも解ではない。x^3 の項がないので、モニック（monic）な 2 次式への因数分解は $(x^2+ax+b)(x^2-ax+c)$ の形になり、$a(c-b) = 0$、$b+c-a^2 = -10$、$bc = 1$ となる。$a = 0$ ならば $b+c = -10$ かつ $bc = 1$ となるが、これは整数では不可能である。$b = c = \pm 1$ ならば $a^2 = 12$ または 8 となり、これも不可能である。よってこの 4 次式は既約（irreducible）であり、$\sqrt{2}+\sqrt{3}$ の次数（degree）は 4 である。

4. ド・モアブル（De Moivre）の定理より $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ であり、$\theta = 20^\circ$ とすると $\frac{1}{2} = 4c^3 - 3c$ となる。候補 $\pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}, \pm\frac{1}{8}$ はどれも解ではない。よって $\cos 20^\circ$ の次数は 3 であるが、作図可能な（constructible）長さの次数はすべて 2 のべきであるから、60° から 20° を作図することはできない。

6.4 四次方程式を解く

1. $y_1y_2 + y_2y_3 + y_3y_1$ は 12 個の項 $\alpha^2\beta\gamma$（1 つの根の 2 乗とほかの 2 つの根の積）の和である。また $\left(\sum\alpha\right)\left(\sum\alpha\beta\gamma\right)$ は、この 12 個の項に $4\alpha\beta\gamma\delta$ を加えたものである。よってこの和は $(-p)(-r) - 4s$ である。

2. 係数を比較すると $a+b = 1$、$a\alpha + b\beta = 0$、$a\alpha^2 + b\beta^2 = -p$ が得られ、これは $\alpha \neq \beta$ のとき解ける。2 つの条件が保証しているのはまさにこのことである。$p \neq 0$ により t の方程式は真の 2 次方程式になり（$p = 0$ ならば $-qt = 0$ に退化し、根は 0 だけになる）、$q^2 \neq 4p^3$ によりその判別式（discriminant）$q^2 - 4p^3$ は 0 でなくなる。$x^3 - 24x + 48$ では $p = 8$、$q = 48$ であり、$8t^2 - 48t + 64 = 0$ から $\alpha = 2$、$\beta = 4$ が得られる。すると $\left(\frac{x-2}{x-4}\right)^3 = -\frac{b}{a} = \frac{\alpha}{\beta} = \frac{1}{2}$ であるから

$x-2=2^{-1/3}(x-4)$ となり、これを整理すると与えられた根 $x\approx -5.6946$ が得られる。

3. 分解 3 次式（resolvent cubic）は $y^3-7y^2+16y-12=(y-3)(y-2)^2$ である。根 $y=3$ から $(x^2-2x+1)(x^2-2x+2)$ が導かれるので、根は 1（2 回）と $1\pm \mathrm{i}$ である。

4. どちらかの組の中で入れ替えるか否か（4 通り）、2 つの組どうしを入れ替えるか否か（2 通り）により、恒等置換、$(\alpha\beta)$、$(\gamma\delta)$、$(\alpha\beta)(\gamma\delta)$、$(\alpha\gamma)(\beta\delta)$、$(\alpha\delta)(\beta\gamma)$、$(\alpha\gamma\beta\delta)$、$(\alpha\delta\beta\gamma)$ が得られる。これは正方形の対称群（symmetry group）と同じ構造をもつ群である。

6.5 公理から考える微分

1. 定数は依然として 0 に写り、規則 (i) と帰納法（induction）により $\Diamond x^n = x^{n-1}\Diamond x + x\Diamond x^{n-1} = nx^n$ である。線形性（linearity）により $\Diamond \mathrm{h} = x\mathrm{h}'$ である。

2. $\Diamond \mathrm{f} = \frac{\mathrm{f}}{\mathrm{g}}\Diamond \mathrm{g} + \mathrm{g}\Diamond\frac{\mathrm{f}}{\mathrm{g}}$ であるから、$\Diamond\frac{\mathrm{f}}{\mathrm{g}} = \frac{\mathrm{g}\Diamond \mathrm{f} - \mathrm{f}\Diamond \mathrm{g}}{\mathrm{g}^2}$ である。

3. $\mathrm{f} = (x-a)^2\mathrm{g}$ ならば $\mathrm{f}' = (x-a)\big(2\mathrm{g} + (x-a)\mathrm{g}'\big)$ である。x^n-1 の重根（repeated root）は nx^{n-1} の根でもあるはずなので 0 となるが、0 は x^n-1 の根ではない。

4. $(2+\varepsilon)^2+1 = 5+4\varepsilon$ であり、$(5+4\varepsilon)^3 = 125+300\varepsilon$ である。よって $f(2)=125$、$f'(2)=300$ である。合成関数の微分法（chain rule）によっても $3(x^2+1)^2\cdot 2x = 3\cdot 25\cdot 4 = 300$ となる。

6.6 部分群の和集合

1. $V=\{e,a,b,c\}$ とすると、$a^2=b^2=c^2=e$ であり、a,b,c のうちどの 2 つの積も残りの 1 つになる。どの元も自分自身が逆元（inverse）である。$\{1,\mathrm{i},-1,-\mathrm{i}\}$ では i の逆元は $-\mathrm{i}$ であるから、この 2 つの群（group）は異なる。

2. g が真部分群（proper subgroup）H に含まれるならば、g のすべてのべきも H に含まれるので、H は群全体になってしまう。

3. 1 は偶数でも 3 の倍数でもない。より一般に、$\mathbb{Z}$ は（1 で生成される）巡回群（cyclic group）であるから、前の演習問題により、いくつの真部分群の和集合（union）にもならない。

4. 直線 $y=mx$ が $y=x^2$ と交わるのは $x=0$ と $x=m$ だけであり、直線 $x=0$ が交わるのは原点だけである。よって k 本の直線は、$t\neq 0$ である無数の点 (t,t^2) のうち高々 k 個しか含まない。

6.7 四元数群

1. $C \circ B = (\mathrm{i}, 0) \circ (0, 1) = (0, \mathrm{i}) = D$ であり、$B \circ C = (0, 1) \circ (\mathrm{i}, 0) = (0, \mathrm{i}^*) = (0, -\mathrm{i}) = H$ である。

2. A の位数（order）は 1、E の位数は 2 である。残りの 6 つはどれも 2 乗すると E になるので、位数は 4 である。正方形の対称群には位数 2 の元が 5 つ（4 つの鏡映と半回転）あるので、2 つの群は同型（isomorphic）ではない。

3. $\det M = z_1 z_1^* + z_2 z_2^* = |z_1|^2 + |z_2|^2$ であり、これは 4 つの実数の平方の和である。$M(z)M(w)$ は $z \circ w$ の行列であるから、行列式（determinant）を掛け合わせると $(a_1^2 + \cdots + a_4^2)(b_1^2 + \cdots + b_4^2)$ は $|u_1|^2 + |u_2|^2$ と表され、これもまた 4 つの平方の和である。

4. 部分群は $\{A\}$、$\{A, E\}$、$\{A, E, C, G\}$、$\{A, E, B, F\}$、$\{A, E, D, H\}$、Q_8 である。A 以外のどの元もそのべきとして E をもつので、$\{A\}$ 以外のどの部分群も E を含む。位数 4 の 3 つの部分群を合わせると、8 つの元すべてを含む。

6.8 特異行列からなる群

1. $\mathbf{M}_a \mathbf{M}_b = \mathbf{M}_{2ab}$ であり、$2(2ab) = (2a)(2b)$ である。この写像は一対一（one-to-one）であり、0 でない実数全体への全射（onto）である。

2. $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix}$ であり $ac \neq 0$ であるから、この集合は閉じている（closed）。$\begin{pmatrix} 1 & e \\ 0 & 0 \end{pmatrix}$ の形の行列はすべて左単位元（left identity）である。しかし $\mathbf{E} = \begin{pmatrix} e & f \\ 0 & 0 \end{pmatrix}$ として $\mathbf{XE} = \mathbf{X}$ となるには $e = 1$ かつ $f = b/a$ が必要であり、これは $\mathbf{X}$ に依存する。よって右単位元は存在せず、単位元も存在しないので、群ではない。

3. $\mathbf{0}$、$\mathbf{I}$、および $bc = a(1 - a)$ を満たす行列 $\begin{pmatrix} a & b \\ c & 1 - a \end{pmatrix}$（トレース 1、行列式 0）である。これらは、平面をある直線へ別の直線に沿って写す射影（projection）である。

4. 成分がすべて a である行列 $\mathbf{J}_a$ は $\mathbf{J}_a \mathbf{J}_b = \mathbf{J}_{nab}$ を満たす。単位元は $\mathbf{J}_{1/n}$ であり、$\mathbf{J}_a$ の逆元は $\mathbf{J}_{1/(n^2 a)}$ である。

Beyond STEP

STEP は、ほとんどの中高生がこれまでに受けるなかで最も難しい数学の試験である。そして最も優れた試験の一つでもある。その問題は短く、見慣れず、奥が深い。なかでも最良の問題は、姿を変えた大学数学の小さな断片なのである。

本書は、1987 年の第 1 回試験に先立つ見本問題（specimen papers）から 2025 年の試験問題までのなかから、特に興味深い STEP の問題を選び、その一つひとつを扉として用いる。どの問題も、優れた学生が途中で抱く疑問に触れながら丁寧に解き、そのうえで扉の向こうへと踏み出す。その考え方はどこから来たのか、大学では何へと発展するのか、次に何を読めばよいのか。

本書は、STEP に向けて準備を進める才能ある数学者の卵のうち、過去問演習以上のものを求める人のために書かれている。数学専攻の学部生のように考え始め、その先に何が待っているのかを知ってほしい。

- 純粋数学（pure mathematics）、力学（mechanics）、確率（probability）、統計（statistics）にわたる 13 の章
- STEP の過去問 136 題、それぞれに道筋を示した解答つき
- すべての問題の背後にある大学数学
- 解答つきの発展演習と、さらに学ぶための文献案内

全 13 章のうちの第 6 章。 本書全体、すべての章、すべての解答は、次のサイトで自由に閲覧・ダウンロード・共有できる：

beyondstep.keithmcnulty.org

本文はパブリックドメイン（public domain）に提供されている（CC0 1.0）。STEP の問題 © Cambridge University Press & Assessment.