代数学序論 I,II

高山　幸秀

諸注意：

- 代数学序論 I, II（２回生配当)、および、環・体論 I, II(３回生配当) の内容はだいたい以下のものと思ってよい。
  - 代数学序論 I: 代数方程式論（体論・ガロア理論入門)、群論入門、
  - 代数学序論 II: 群論
  - 環・体論 I: 環論入門（多項式の理論を含む）
  - 環・体論 II: 体論・ガロア理論（ガロア理論では群論の理解が前提となる）

  このように「代数学序論 I, II」と「環・体論 I, II」は密接に関連している。
- 本文で使われる記号上の注意は以下の通り。
  - $\mathbb{N} = \{1, 2, 3, \ldots\}$ (自然数全体の集合) と約束する。
  - $\mathbb{Z}_{\geq 0} = \{0, 1, 2, \ldots\}$ (非負整数全体の集合）と約束する。
  - ２つの数 a, b の最大公約数を (a, b) と表す。
- 定理や命題の証明で「環・体論 I, II で習え」等と書いてある部分は、とりあえず事実だけ認めて、その結果を積極的に使えばよいものである。勿論、３回生に進んだときにきちんとした証明を勉強することが望ましい。
- 勉強の仕方としては、要するに
  - 代数学特有の抽象的な議論のスタイルを身に着ける (新しい思考スタイルは、ある程度頭の痛い思いをしないと身につかないものである)。
  - 抽象理論の背景にある具体例を理解する (さまざまな具体例を統一的に理解するために抽象理論があること忘れてはならない)。

  が出来れば良いのだが、そのための方法論として、例えば以下のような方法が考えられる。
  (1) まず、本文に書かれている例を完全に理解する。必要に応じて、本文中の定義や定理などを参照する。
  (2) 次に演習問題を解いてみる。必要に応じて、本文中の定義や定理などを参照する。（やや難）等の表示がしてあるものを除き、演習問題は全て基本的で、本テキストで学ぶ際にぜひやって欲しい計算や考察を示している。
  (3) さらに、定義、定理・命題・補題の主張内容を理解し、理論全体の流れを掴む。
  (4) それから、各定理・命題の証明を理解する。特に本格的に代数学を学びたい人は、できれば証明を何度も読み返して徹底的に理解し、テキストを見ずに人前説明できるぐらいにすることが望ましい。このことによって、代数学で必要な議論や思考のスタイルが身につくからである。

Date: ２００９年１月７日版、２０１０年月６月９日改訂.

はじめに

0.1. **代数学略史.** 代数学は代数方程式論とともに発展してきた。その歴史を概観すると、以下のようになる。

(1) 紀元前３世紀頃：バビロニア人が２次方程式の解法の一部を発見
(おそらくチグリス・ユーフラテス川氾濫後の土地測量の必要性から？)
(2) 紀元９世紀頃: アラビア人が２次方程式の解法を完成
(しかし複素数解の概念はなかったと思われる)
(3) 1515 年： S. del Ferro が３次方程式の解法（の一部）を発見するも、公表せず。
(4) 1545 年： G. Cardano が（N. Tartaglia を介して？）S. del Ferro のアイディアを聞き知り、独自に３次方程式の解法を発見。複素数の概念を導入。その後、弟子の L. Ferrari が４次方程式の解法を発見。
(5) 1746 年：J. d'Alembert **「代数学の基本定理」**を発見
(6) 1771 年：J. L. Lagrange が Cardano, Ferrari の解法の不備を修正し、３次・４次方程式の解法を完成させる。ここで、方程式の解の置換という**群論的考察**のアイディアを導入。
(7) 1772 年：J. L. Lagrange, 代数学の基本定理の別証明
(8) 1796 年：C. F. Gauß, 群論的考察 にもとづき $X^p - 1 = 0$ ($p > 2$, 素数) 型の方程式の解法を研究。
(9) 1799 年：C. F. Gauß, 代数学の基本定理の別証明
(10) 1820 年：N. H. Abel, 群論的考察 に基づいて５次以上の代数方程式が一般には非可解であることを発見。
(11) 1830-32 年：E. Galois が Lagrange の 群論的考察 の方法を徹底的に掘り下げ、所謂**「Galois 理論」**を完成。しかし当時の数学者には理解されず。彼の研究の良き理解者であったであろう Lagrange も既に 1813 年に亡くなっていた。
(12) 1846 年頃：J. Liouville がガロア理論の意義を認め、内容を整理したものを公表。その後の約５０年は、ガロア理論のより深い理解と発展のために、E. Steinitz, R. Dedekind, L. Kronecker, E. Artin, D. Hilbert など、多くの数学者が精力的に取り組む。

0.2. **代数学の発展.**

- ２次方程式の解法の発見から３・４次方程式の解法発見まで約７００年を要し、それから５次以上の方程式の非可解性とその理由の本質的解明（ガロア理論）の誕生までに約３００年を要している。これは、それらの間に本質的な違いがあることを意味する。
  - 最初の７００年：２次方程式の計算のように、式変形の計算だけで３・４次方程式を解こうとして、なかなかうまく行かなかった。
  - 次の３００年：３・４次方程式の解法を得るのに何故７００年もかかったのか？その本質的原因が分かるための時間がかかった。
- 代数学の過去１０００年の経験から人類が得た思想は、「群という抽象的な構造を通して、単なる式変形のテクニックの集積だけでは見えない本質が見えてくる」ということだと考えられる。この思想は現代数学の主要な分野、例えば、
  - 微分方程式のガロア理論とも呼ばれるＬｉｅ群論

  - 関数族に対する作用素の構造を調べる作用素環論
  - 図形の連続変形で保存される性質を、群論を通して調べる代数的位相幾何学
  - その領域を定義域に持つ関数全体の群論的性質を通して幾何学や解析学を研究する代数幾何学、複素多様体論、代数解析学

  などに息づいている。また、群の構造を詳しく調べる方法論などを研究する分野として
  - ホモロジー代数学
  - 表現論

  といった、代数学の一分野も発展している。
- また、ガロア理論は代数的整数論として、また、代数方程式論は１変数の１つの代数方程式の理論から、多変数の連立方程式の理論、すなわち代数幾何学や数論幾何学として、現代でも活発に研究されている。

1. 代数方程式と拡大体

1.1. **代数方程式.**

1.1.1. 代数学の基本定理. 代数学の基本定理は、「任意の代数方程式の解は、複素数体の中で全て見つかる」ことを主張する。

定理 1 (代数学の基本定理)**.** $n(\geq 1)$ 次の代数方程式

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1}x + a_n = 0, \qquad (a_1, \ldots, a_n \in \mathbb{C})$$

は複素数体 $\mathbb{C}$ の中で重複度をこめて n 個の解をもつ。従って、適当な複素数 $\alpha_1, \ldots, \alpha_n$ (重複を許す) が存在して

$$f(x) = \prod_{i=1}^{n}(x - \alpha_i)$$

と一次式の積に分解する。

Proof. 複素解析を使った方法（３回生「複素解析」)、ガロア理論（３回生「環・体論 II」）を使った方法、その他いくつかの証明が知られている。 □

代数学の基本定理は「解は複素数の範囲で見つかるはず」と主張しているけれど、「その解をどうやって見つければ良いか？」という問題に対しては、何も答えていない。方程式を実際とのように解くかは、全く別の問題である。この問題を考えるには、まず「代数方程式を解く」ということはどういうことか？をきちんと考え直さなければならない。

1.1.2. 「代数的に解く」ということ. よく知られている１次方程式

$$f(x) = ax + b = 0 \quad (a, b \in \mathbb{C}, ; a \neq 0)$$

の解の公式 $x = -\dfrac{b}{a}$ や、２次方程式

$$f(x) = ax^2 + bx + c = 0, \quad (a, b \in \mathbb{C},\ a \neq 0)$$

の解の公式

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

は、方程式の係数に四則演算、あるいは、冪根（今の場合は平方根）演算を使って解を書き表しているのである。

定義 2 (代数的に解く)**.** 代数方程式の解を、その係数に四則演算と冪根演算を施して解を書き表すことを「(代数方程式を）**代数的に解く**」または「(代数方程式を）**冪根で解く**」と言う。

また、「解の公式」とは、係数の値に依存しない解の表示方法を示したものである。実際、上に示した一次方程式や二次方程式の解の公式は、係数の a, b, c がどんな値であるかに関わらず、必ずこの形で解が書き表せる、ということを表したものである点に注意しよう。

代数方程式の解法については、以下のことがわかっている。

- ３次、４次方程式の解の公式は存在する。

- ５次以上の代数方程式には解の公式が 存在しない ことが証明されている。
- ５次以上の代数方程式の中には、冪根で解けるものと解けないものが存在する。

代数方程式が代数的に解けたり、解けなかったり、解の公式が作れたり作れなかったりするのは何故か？その本質的理由は N. H. Abel と E. Galois による理論（ガロア理論と呼ばれる）によって明らかにされる。そこで重要な役割を果たすのが、「群論 (group theory)」と「体論 (field theory)」である。

体論は３回生「環・体論 I, II」で詳しく論じられるので、代数学序論 I, II では群論に重点をおいて考察してゆく。

1.2. **体論からの準備.** とくに３次以上の代数方程式を研究する際、次のような考え方が重要である：代数学の基本定理 (定理 1) によれば、代数方程式の解は複素数 $\mathbb{C}$ の中に必ず見つかるが、解を捜す「数の範囲」を $\mathbb{C}$ よりももっと限定した方が考えやすい。そこで、最初はせいぜい有理数と係数に現れる数 が関係する「数の範囲」で考え、それで足りなければ「数の範囲」を少しずつ「拡大」してゆくのである。

この「数の範囲」や「拡大」の意味を正確に述べよう。

1.2.1. 拡大体. 正確で形式的な体の定義については３回生「環・体論 I」で学ぶが、ここでは次のように考えておけば良いだろう。

定義 3 (体)**.** 四則演算が自由にできる、すなわち四則演算した結果に得られる値が全て含まれているような集合を「**体** (「たい」と読む)(field)」と呼ぶ。２つの体 K, L が、$K \subset L$ なる関係にあるとき、「L は K の**拡大体** (extension field)」「K は L の部分体」または「拡大体 L/K」と言う。

例 4 (有理数体)**.** 有理整数環 $\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, \cdots\}$ は加法、減法、乗法の結果は全て $\mathbb{Z}$ に含まれているが、除法の結果は

$$\frac{4}{2} = 2 \in \mathbb{Z} \qquad \text{しかし} \qquad \frac{3}{2} = 1.5 \notin \mathbb{Z}$$

と、必ずしも $\mathbb{Z}$ に含まれているとは限らないので、体ではない。しかし、有理数体 $\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z}, n \neq 0, (m, n) = 1\}$ は体である。実数体 $\mathbb{R}$, 複素数体 $\mathbb{C}$ もやはり体である。

例 5 (拡大体)**.** 典型例は、たとえば

$$\mathbb{Q} \ \subset \ \mathbb{R} \ \subset \ \mathbb{C}$$

である。複素数体 $\mathbb{C}$ は、実数体 $\mathbb{R}$ に純虚数 $i = \sqrt{-1}$ を「付け加えた」ものだから、

$$\mathbb{C} = \mathbb{R}(\sqrt{-1})$$

と書き表される。一方、有理数体 $\mathbb{Q}$ と実数体 $\mathbb{R}$ のギャップは大きい：

$$\mathbb{R} - \mathbb{Q} \ni \pi(\text{円周率}),\ e\ (\text{自然対数底}),\ \sqrt{2},\ \sqrt{3},\ \sqrt{5}, \ldots,$$

と $\mathbb{Q}$ に沢山のもの（それは無限個である！）を「付け加え」ないと $\mathbb{R}$ にならない。そこで、$\mathbb{Q}$ に高々有限個の新しい要素、例えば、$\sqrt{2}$ と π, を付け加えた中間的な体（これを「**中間体**」とよぶ）

$$\mathbb{Q} \ \subset \ \mathbb{Q}(\sqrt{2}, \pi) \ \subset \ \mathbb{R}$$

を考えた方が、代数的な議論はやりやすいのである。

例 5 で使った「体に新しい要素を『付け加える』」という言葉の意味を正確に述べよう。$a \in L - K$ に対し、「K **上** a **で生成された（単純）拡大体** $K(a)$」を次のように定義する：

$$\begin{aligned} K(a) &= K \text{ と } a \text{ を含む } L \text{ の部分体のうち最小のもの} \\ &= \left\{ \frac{f(a)}{g(a)} : f(x), g(x) \in K[x], g(a) \neq 0 \right\} \end{aligned}$$

ここで、$K[x]$ は K 係数の 1 変数 x の多項式全体の集合を表し、これを「**多項式環** (polynomial ring)」と呼ぶ。すなわち、

$$K[x] = \left\{ c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 \mid \begin{array}{l} n \in \mathbb{Z}_{\geq 0}, \\ c_i \in K \ (i = 0, 1, \ldots, n) \end{array} \right\}$$

例 6 (単純拡大)**.** $K = \mathbb{Q} \subset L = \mathbb{R}$ とし、$a = \pi$ (円周率) $\in \mathbb{R}$ とすると、

$$\begin{aligned} & K(a) \\ &= \mathbb{Q}(\pi) \\ &= \left\{ \frac{a_0 + a_1\pi + \cdots + a_n\pi^n}{b_0 + b_1\pi + \cdots + b_m\pi^m} : a_i, b_j \in \mathbb{Q}, b_0 + b_1\pi + \cdots + b_m\pi^m \neq 0, n, m \geq 0 \right\} \end{aligned}$$

これは、後で述べる超越拡大体の典型例である。

例 7 (単純拡大)**.** $K = \mathbb{R} \subset L = \mathbb{C}$ とし、$a = \sqrt{-1} \in \mathbb{C}$ とすると、

$$\begin{aligned} & \mathbb{R}(\sqrt{-1}) \\ &= \left\{ \frac{a_0 + a_1\sqrt{-1} + \cdots + a_n(\sqrt{-1})^n}{b_0 + b_1\sqrt{-1} + \cdots + b_m(\sqrt{-1})^m} : a_i, b_j \in \mathbb{R}, b_0 + b_1\sqrt{-1} + \cdots + b_m(\sqrt{-1})^m \neq 0 \right\} \\ & \quad \text{ここで } \sqrt{-1}^2 = -1 \text{ を使えば} \\ &= \left\{ \frac{a_0 + a_1\sqrt{-1}}{b_0 + b_1\sqrt{-1}} : a_0, a_1, b_0, b_1 \in \mathbb{R}, (b_0, b_1) \neq (0, 0) \right\} \\ &= \left\{ a_0 + a_1\sqrt{-1} : a_0, a_1 \in \mathbb{R} \right\} = \mathbb{C} \end{aligned}$$

これは、後で述べる代数拡大体の典型例である。すなわち、拡大体を作るときに付け加えた $\sqrt{-1}$ が、代数方程式 $X^2 + 1 = 0$ の根になっている。

K に複数の要素 $a_1, \ldots, a_n$ を付け加えた拡大も、同様に考えることができて

$$K(a_1, a_2, \ldots, a_n)$$

と書くことにする。これは次の形で書ける。

命題 8. $K(a_1, a_2, \ldots, a_n)$ は、次の形で書き表せる。

$$\begin{aligned} & K(a_1, a_2, \ldots, a_n) \\ &= \left\{ \frac{f(a_1, a_2, \ldots, a_n)}{g(a_1, a_2, \ldots, a_n)} \mid \begin{array}{l} f(x_1, x_2, \ldots, x_n), g(x_1, x_2, \ldots, x_n) \in K[x_1, x_2, \ldots, x_n], \\ g(a_1, a_2, \ldots, a_n) \neq 0 \end{array} \right\} \end{aligned}$$

ここで $K[x_1, x_2, \ldots, x_n]$ は、K 係数の変数 $x_1, \ldots, x_n$ についての多項式全体の集合（「n 変数多項式環」とよばれる）である。

1.2.2. 1 の原始 n 乗根. 代数方程式

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1) = 0$$

は重根を持たないことが知られている。従って、解集合 U_n $(\subset \mathbb{C})$ は自明な解 $x = 1$ を含む n 個の要素を持つ。U_n の要素 $\zeta(\neq 1)$ の中には、

$$\{\zeta, \zeta^2, \zeta^3, \ldots, \zeta^{n-1}, \zeta^n (= 1)\} = U_n$$

となるものが（一般には複数）含まれていることも知られている。この ζ は一般に

$$\zeta = \cos\left(\frac{2k\pi}{n}\right) + i \cdot \sin\left(\frac{2k\pi}{n}\right), \quad 0 < k < n,\ (k, n) = 1$$

の形で書き表せる (Euler の公式により $\zeta^n = 1$ となることに注意)。このような ζ のことを「1 **の原始** n **乗根** (primitive n-th root of unity)」と呼ぶ。
（詳細は「環・体論 I,II」）

例 9 (1 の原始 2 乗根)**.** $x^2 - 1 = (x-1)(x+1) = 0$ の解集合は $U_2 = \{1, -1\}$. 原始 2 乗根は

$$\zeta = \cos(\pi) + i \cdot \sin(\pi) = -1.$$

実際、$U_2 = \{-1, (-1)^2 = 1\}$ となっている。

例 10 (1 の原始 3 乗根)**.** $x^3 - 1 = (x-1)(x^2 + x + 1) = 0$ の解集合は

$$U_3 = \left\{1, \frac{-1 - \sqrt{-3}}{2}, \frac{-1 + \sqrt{-3}}{2}, \right\}$$

で、原始 3 乗根は

$$\zeta = \cos\left(\frac{2\pi}{3}\right) + i \cdot \sin\left(\frac{2\pi}{3}\right) = \frac{-1 + \sqrt{-3}}{2}$$

または

$$\zeta' = \cos\left(\frac{4\pi}{3}\right) + i \cdot \sin\left(\frac{4\pi}{3}\right) = \frac{-1 - \sqrt{-3}}{2}.$$

実際、

$$U_3 = \{\zeta, \zeta^2 (= \zeta'^2), \zeta^3 (= 1)\} = \{\zeta', \zeta'^2 (= \zeta), \zeta'^3 (= 1))\}.$$

となっている。

例 11 (1 の原始 4 乗根)**.** $x^4 - 1 = (x-1)(x^3 + x^2 + x + 1) = 0$ の解集合は $U_4 = \{1, -1, i, -i\}$ であり、原始 4 乗根は、

$$\zeta = \cos\left(\frac{\pi}{2}\right) + i \cdot \sin\left(\frac{\pi}{2}\right) = i$$

または

$$\zeta' = \cos\left(\frac{3\pi}{2}\right) + i \cdot \sin\left(\frac{3\pi}{2}\right) = -i.$$

実際、

$$\begin{aligned} U_4 &= \{i,\ i^2 (= -1),\ i^3 (-i),\ i^4 (= 1)\} \\ &= \{-i,\ (-i)^2 = i,\ (-i)^3 = -1,\ (-i)^4 (= 1)\}. \end{aligned}$$

となっている。

1.2.3. 代数方程式の基礎体と分解体. さて、代数方程式

$$x^n + a_1 x^{n-1} + \cdots a_{n-1}x + a_n = 0 \qquad (a_1, \ldots, a_{n-1}, a_n \in \mathbb{C})$$

に対して、「解を捜す数の範囲のもっとも小さいもの」という意味の「**基礎体** (base field)」を

$$K = \mathbb{Q}(a_1,\ \ldots,\ a_n)$$

とおく。K は有理数に方程式の係数を加えたものだが、代数方程式を「代数的に解く」際には、係数や係数の整数倍、有理数倍を加減乗除し、場合によってはその冪根をとったりするので、この範囲は最低限必要と思われる。その意味でこれを基礎体として採用するのは、自然なことだと考えらえるのである。

また、上の代数方程式の根を $x_1, x_2, \ldots, x_n \in \mathbb{C}$（今は重根かどうかといった微妙な問題にはあえて目をつぶる）とすれば、拡大体

$$L = K(x_1, x_2, \ldots, x_n)$$

の中には当然 $x_1, \ldots, x_n$ は含まれている。この L のことを代数方程式の「**分解体** (splitting field)」と呼ぶ。分解体と基礎体がかけ離れている場合、一般にその方程式を解くのは厄介である。

例 12 (二次方程式). $f(x) = x^2 + ax + b$ に対し

$$K = \mathbb{Q}(a,b) = \left\{ \frac{f(a,b)}{g(a,b)} : f(x,y), g(x,y) \in \mathbb{Q}[x,y], g(a,b) \neq 0 \right\}$$

となる (命題 8 参照)。また、二次方程式の分解体は

$$\begin{aligned} L &= K\left(\frac{-a+\sqrt{a^2-4b}}{2}, \frac{-a-\sqrt{a^2-4b}}{2}\right) \\ &\quad \text{しかし } a \in K \text{ だから、本質的に新しい要素は } \sqrt{a^2-4b} \\ &\quad \text{だけだから、体論の簡単な議論により} \\ &= K(\sqrt{a^2-4b})(= \mathbb{Q}(a,b,\sqrt{a^2-4b})) \\ &\quad \text{ここで } (\sqrt{a^2-4b})^2 = a^2-4b \in K \text{ であることを使えば} \\ &\quad \text{命題 } 8 \text{ により} \\ &= \left\{ \frac{\alpha+\beta\sqrt{a^2-4b}}{\gamma+\delta\sqrt{a^2-4b}} : \alpha,\beta,\gamma,\delta \in K = \mathbb{Q}(a,b) \right\} \\ &= \left\{ \alpha+\beta\sqrt{a^2-4b} : \alpha,\beta \in K = \mathbb{Q}(a,b) \right\} \end{aligned}$$

従って、$\sqrt{a^2-4b} \in K$ ならば $K = L$ となるが、さもなければ $K \neq L$ となり、方程式を解くのはすこし複雑になる。例えば、$a, b \in \mathbb{Q}$ とすれば $K = \mathbb{Q}$ で、$\sqrt{a^2-4b} \in K = \mathbb{Q}$ ならば、方程式は有理数解を持つ。つまり、有理数の範囲だけで解を捜せば良い。さもなければ、実数解や複素数解など、より広い数の範囲で解を捜さなければならない。つまり、拡大体を考える必要が生じるのである。

上の例 12 でみたように、二次方程式ではせいぜい

$$K \subset L = K(\sqrt{a^2-4b})$$

といった簡単な拡大体を考えれば良いが、３次・４次の方程式になると、基礎体 K と分解体 L の間にいくつかの中間体を考えていかねばならならず、議論はより複雑なものになる。

1.2.4. 冪根による拡大. 代数方程式 $X^n - c = 0,\ c \neq 0 \in K,$ の根は一般には（重根を含めて) n 個存在するが、そのうちの一つを適当に選んで $\sqrt[n]{c}$ と表す。このとき、1 の原始 n 乗根を ζ とすれば、$X^n - c = 0$ の解全体は

$$\zeta\sqrt[n]{c},\ \zeta^2\sqrt[n]{c}, \ldots, \zeta^{n-1}\sqrt[n]{c},\ \zeta^n\sqrt[n]{c}(=\sqrt[n]{c})$$

である。

例 13. 方程式 $X^3 - 2 = 0$ を考える。その解集合は $\zeta = \frac{-1+\sqrt{-3}}{2}$ として

$$\{\sqrt[3]{2},\ \zeta\sqrt[3]{2},\ \zeta^2\sqrt[3]{2}\}.$$

ここでは、$\sqrt[3]{2},\ \zeta\sqrt[3]{2},\ \zeta^2\sqrt[3]{2}$ のどれか一つを改めて $\sqrt[3]{2}$ と呼び直す。

この例だと、$\zeta\sqrt[3]{2}$ や $\zeta^2\sqrt[3]{2}$ までも $\sqrt[3]{2}$ と呼んでも良いことになり、いささか不合理なような印象をもつかもしれない。しかし、このような記法の必要性は、以下のようなより一般の例をみればわかる。

例 14. 方程式 $X^3 + 8i = 0$ を考える。その解集合は $\zeta = \frac{-1+\sqrt{-3}}{2}$ として

$$\{2i,\ 2i\zeta = -i + \sqrt{3},\ 2i\zeta^2 = -i - \sqrt{3}\}.$$

ここで、$\sqrt[3]{-8i}$ は上の３つのもののうちのいずれか。

代数方程式を解くとき、解を基礎体 K の要素の冪根で表さなければならないことがある。従って、K にその冪根を付け加えたより広い数の範囲で解を捜すのである。高次の方程式を解く場合は、同様の操作を何度も繰り返す必要が生じる。例えば、４次方程式を解く時には、ある種の３次方程式を解かねばならず、その後である種の２次方程式も解かねばならない。従って、基礎体に何らかの３乗根を付け加えた数の範囲を考え、さらにそれに何らかの２乗根を付け加えた数の範囲を考える。このような操作のことを「冪根による拡大」と呼ぶ。すなわち、

定義 15 (冪根による拡大)**.** 有限次拡大 L/K が「**冪根による拡大** (extension by radicals)」であるとは、適当な拡大体列

$$K = E_0 \subset E_1 \subset \cdots \subset E_m = L$$

があって、各 E_{i+1} は E_i に方程式 $X^{n_i} - a_i = 0\ (a_i \in E_i)$ の根のひとつ $\sqrt[n_i]{a_i}$ を付け加えたものになっている、すなわち $E_{i+1} = E_i(\sqrt[n_i]{a_i})$ となっている場合をいう。

注意 16. 代数方程式 $X^n - c = 0,\ (0 \neq)c \in \mathbb{C}$ を考える。基礎体は $K = \mathbb{Q}(c)$. ζ を 1 の原始 n 乗根（つまり $X^n - 1 = 0$ の根) とすると、この方程式の分解体は

$$L = K(\zeta\sqrt[n]{c},\ \zeta^2\sqrt[n]{c}, \ldots, \zeta^{n-1}\sqrt[n]{c},\ \zeta^n\sqrt[n]{c})$$

だから、

$$K \subset K(\sqrt[n]{c}) \subset L \subseteq K(\sqrt[n]{c}, \zeta)$$

ここで、$K(\sqrt[n]{c}, \zeta)$ は K の冪根による拡大である。

注意 17. 2 次方程式の解の公式は、冪根による拡大体

$$K = \mathbb{Q}(a, b) \subseteq K(\sqrt{a^2 - 4b}) = L$$

というふうに旨く作れば、L の中に解をみつけることができることを意味している。(ここで 1 の原始 *2* 乗根は -1 だから、注意 *16* にて $L = K(\sqrt[p]{c}, \zeta)$ となることに注意。)

1.2.5. 代数拡大. 今後おもに考えるのは、以下に定義される (有限次) 代数拡大である。

定義 18 (代数拡大)**.** 拡大体 $K(a_1, \ldots, a_n)/K$ において、適当な $f_1(x), \ldots, f_n(x) \in K[x]$ によって

$$f_1(a_1) = \cdots = f_n(a_n) = 0$$

となっているとき、$K(a_1, \ldots, a_n)$ を K の「**代数拡大体** (algebraic extension)」と呼ぶ。代数的でない拡大体を「**超越拡大体** (transcendental extension)」と呼ぶ。

例 19 (代数拡大と超越拡大の例)**.** 円周率 π は、有理数係数の代数方程式の解にならないこと (「超越性」とよぶ) が知られている。従って、拡大体 $\mathbb{Q}(\pi)/\mathbb{Q}$ は超越拡大である (cf. 例 6)。正確には超越的な数だけで拡大体を作っているので「純超越拡大」と呼ぶ。また、$\sqrt{2}$ は 2 次方程式 $x^2 - 2 = 0$ の解だから、$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ は代数拡大。しかし、$\mathbb{Q}(\pi, \sqrt{2})/\mathbb{Q}$ は超越的な元 π も使っているから代数拡大ではなく、超越拡大である。

代数拡大体 L/K の非常に重要な性質は、L が K-線形空間になっていることである。

例 20. 拡大体 $\mathbb{C}/\mathbb{R}$ は $\mathbb{C} = \mathbb{R}(\sqrt{-1})$ で、$i = \sqrt{-1}$ は $x^2 + 1 = 0$ の根だから、代数拡大体。また、$\mathbb{C}$ の要素は

$$\alpha \cdot 1 + \beta \cdot \sqrt{-1}, \qquad (\alpha, \beta \in \mathbb{R})$$

と一意的に表せるから (cf. 例 7)、$\{1, \sqrt{-1}\}$ を基底とする $\mathbb{R}$-線形空間で、$\dim_{\mathbb{R}} \mathbb{C} = 2$ である。

何故このようなことが起こるかを考えてみよう。$\sqrt{-1}$ が $x^2 + 1 = 0$ の根で $x^2 + 1$ が $\mathbb{Q}$ 係数の多項式で、$\mathbb{Q}$ 係数の 1 次式には因数分解できないことから、ユークリッドの互除法定理により、任意の一次式 $a + bx$ $(a, b \in \mathbb{Q})$ に対して

$$f(x) \cdot (a + bx) + g(x) \cdot (x^2 + 1) = 1$$

となるような多項式 $f(x), g(x)$ が必ず存在する。この式に $x = \sqrt{-1}$ を代入すると $f(\sqrt{-1}) \cdot (a + b\sqrt{-1}) = 1$, すなわち、

$$\frac{1}{a + b\sqrt{-1}} = f(\sqrt{-1})$$

を得る。ここで $f(x)$ がどんな多項式であっても、$f(\sqrt{-1}) = c + d\sqrt{-1}$ $(c, d \in \mathbb{Q})$ の形になることに注意すると、

$$\frac{p + q\sqrt{-1}}{a + b\sqrt{-1}} = (p + q\sqrt{-1})(c + d\sqrt{-1})$$

となり、これを整理すると、結局 $r + s\sqrt{-1}$ $(r, s \in \mathbb{Q})$ の形の式になる。

上の例を一般化したものが、以下の命題である。

命題 21. $f(x) \in K[x]$ を既約多項式、すなわち、$f(x) = g(x)h(x)$ となるような 1 次以上の多項式 $g(x), h(x) \in K[x]$ は存在しないものとする。この時、c を $f(c) = 0$ となるような数によって代数拡大 $K(c)$ を考えれば、$K(c)$ は K-線形空間であり、

$$\dim_K K(c) = \deg f(x).$$

となる。$N = \dim_K K(c)$ のとき、「$K(c)$ は K の N 次拡大」であるという。

ここで、多項式 $f(x) \in K[x]$ が「**可約** *(reducible)*」であるとは、$K[x]$ の中で因数分解されること、すなわち、

$$f(x) = h(x)k(x) \quad h(x), k(x) \in K[x], \deg h(x), \deg k(x) \geq 1$$

となることを言い、既約でない場合を「**既約** *(irreducible)*」と言う。また、整数の場合と同様に、次の定理が成り立つ。

定理 22 (Euclid の互除法)**.** 体 K 上の一変数多項式 $f(x), g(x) \in K[x]$ に対して、

$$P(x)f(x) + Q(x)g(x) = (f(x), g(x))$$

となるような $P(x), Q(x) \in K[x]$ が存在する。

Proof. 3 回生「環・体論 I, II」で学べ。1 変数多項式のユークリッドの互除法定理は、整数の場合のユークリッド互除法定理と本質的に同じである（Appendix A 参照)。 □

命題 21 の証明. 定義により

$$\begin{aligned} & K(c) \\ = & \left\{ \frac{a_0 + a_1 c + \cdots + a_n c^n}{b_0 + b_1 c + \cdots + b_m c^m} : a_i, b_j \in K,\ b_0 + b_1 c + \cdots + b_m c^m \neq 0,\ n, m \geq 0 \right\} \\ & f(c) = 0 \text{ であることを使えば、} N = \deg f(x) \text{ として} \\ = & \left\{ \frac{a_0 + a_1 c + \cdots + a_{N-1} c^{N-1}}{b_0 + b_1 c + \cdots + b_{N-1} c^{N-1}} : a_i, b_j \in K,\ b_0 + b_1 c + \cdots + b_{N-1} c^{N-1} \neq 0 \right\} \end{aligned}$$

さて、$f(x)$ が既約で、$g(x) := b_0 + b_1 x + \cdots + b_{N-1} x^{N-1}$ は $\deg g(x) < \deg f(x)$ であることから、$(f(x), g(x)) = 1$ とわかる (証明：もしそうでなければ $f(x) = h(x)k(x)$, $h(x) = (f(x), g(x))$ $1 \leq \deg h(x) < \deg f(x)$, $h(x), k(x) \in k[x]$ と因数分解されることになり、$f(x)$ の既約性に反する)。従って、Euclid の互除法により、

$$G(x)f(x) + H(x)g(x) = 1$$

となるような $G(x), H(x) \in K[x]$ が存在する。そこで $x = c$ を代入すると

$$H(c)g(c) = 1 \quad \text{すなわち} \quad \frac{1}{g(c)} = H(c)$$

となる。よって、

$$K(c) = \left\{ a_0 + a_1 c + \cdots + a_{N-1} c^{N-1} : a_i \in K \right\}$$

となり、$K(c)$ の任意の要素は一意的に

$$a_0 + a_1 c + \cdots + a_{N-1} c^{N-1} \quad (a_i \in K)$$

と表されるから、

$$K(c) = \langle 1, c, c^2, \ldots, c^{N-1} \rangle_K$$

となり、$\dim_K K(c) = N$ を得る。 □

一般の拡大体 $K(a_1, \ldots, a_t)/K$ も命題 21 を繰り返し適用すれば、K-線形空間であることがわかる (具体例については例えば、例 36 をみよ)。

1.3. 代数方程式のガロア群.

1.3.1. 体の自己同型群. 代数拡大体 L/K が与えられたとする。L は K-線形空間である。このとき、L の K-自己同型（写像）σ とは、正則な K-線形写像（つまり逆行列の存在する正方行列で表せる線形写像)

$$\sigma : L \longrightarrow L$$

で、さらに、「積を積に写す」ものである。具体的には、次の 3 条件をみたす：

(1) $\sigma(\alpha \cdot x + \beta \cdot y) = \alpha \cdot \sigma(x) + \beta \cdot \sigma(y)$, $\alpha, \beta \in K$, $x, y \in L$ (K-線形性)
(2) $\sigma(xy^{-1}) = \sigma(x)\sigma(y)^{-1}$, $x, y \in L$), すなわち、積は積に、積についての逆元は積についての逆元に写像する。
(3) σ は全単射。

このような自己同型全体の集合を $\mathrm{Aut}_K(L)$ と書くことにする。
この集合は「群」と呼ばれる特殊な構造をもつ。

定義 23 (群)**.** 集合 G に演算 "$\cdot$" が定義されていて、次の条件を満たすとき、G は「**群** (group)」であるという：

1) 演算で閉じていること: 任意の $g, h \in G$ に対し、$g \cdot h \in G$.
2) 単位元の存在: 特別な元 $1_G \in G$ が存在して、任意の $g \in G$ に対し

$$g \cdot 1_G = 1_G \cdot g = g.$$

この 1_G のことを G の「**単位元** (identity)」と呼ぶ。
3) 逆元の存在: 任意の $g \in G$ に対して、ある元 $\rho_g \in G$ が存在して、

$$g \cdot \rho_g = \rho_g \cdot g = 1_G$$

このとき、$g^{-1} := \rho_g$ を g の「**逆元** (inverse)」とよぶ。
4) 結合法則: 任意の $g, h, k \in G$ に対して、

$$(g \cdot h) \cdot k = g \cdot (h \cdot k)$$

が成り立つ。

群の演算記号や単位元を明示するために、単に G とは書かずに、$(G, \cdot)$ や $(G, \cdot, 1_G)$ という風に書くこともある。また、

(1) G の要素の個数 $\sharp G$ を、群の「**位数** (order)」とよぶ。

(2) $\sharp G = \infty$ なら「**無限群** (infinite group)」、$\sharp G < \infty$ なら「**有限群** (finite group)」と呼ぶ。
(3) 演算の交換法則：「任意の $g, h \in G$ に対して、$gh = hg$」が成り立つ場合、「**アーベル群 (Abel 群)**(abelian group)」と呼ぶ。

命題 24. 群 G の単位元 1_G は一意的である。

Proof. 単位元が 2 つ ($e_1, e_2 \in G$) あったとする。まず e_1 は単位元だから、

$$e_1 e_2 = e_2 e_1 = e_2.$$

また、e_2 も単位元だから

$$e_2 e_1 = e_1 e_2 = e_1$$

この 2 つの式から $e_1 = e_2$ を得る。 □

命題 25. 群 G の任意の要素 $x \in G$ に対して、その逆元 x^{-1} は一意的である。

Proof. 逆元が 2 つあったとする：$x^{-1} = y_1, y_2 \in G$. y_1 は x の逆元だから、

$$1_G = xy_1.$$

また、y_2 も x の逆元だから、上式に左から y_2 を掛けると

$$y_2 = y_2 e = y_2(xy_1) = (y_2 x)y_1 = ey_1 = y_1$$

すなわち $y_1 = y_2$ を得る。 □

演習問題 1. 次のもののうち、どれが群になるか？

(1) $(\{1, -1\}, \times, 1)$, $\times$ は通常の整数の掛け算
(2) $(\mathbb{R}, \times, 1)$
(3) $(\mathbb{R}, +, 0)$
(4) $(\mathbb{Z}, \times, 1)$
(5) $(\mathbb{Q}, \times, 1)$
(6) $(\mathbb{Q}, +, 0)$
(7) $(\mathbb{Z}, +, 0)$
(8) $(\mathbb{N} \cup \{0\}, +, 0)$
(9) $(\mathbb{Q}[x], +, 0)$, 但し、$\mathbb{Q}[x]$ は有理数係数の変数 x についての多項式全体の集合。
(10) $(\mathbb{Q}[x, y], \times, 1)$, 但し、$\mathbb{Q}[x, y]$ は有理数係数の変数 x, y についての多項式全体の集合。
(11) $(GL(2, \mathbb{R}), \times, E_2)$, ただし E_2 は 2 次の単位行列で $\times$ は行列の積、また、

$$GL(2, \mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R},\ ad \neq bc \right\}.$$

とする。
(12) $(GL(2, \mathbb{R}), +, O_2)$, ただし O_2 は 2 次の零行列で $+$ は行列の和
(13) $(\{1, \zeta, \zeta^2\}, \times, 1)$, ただし, $\zeta = \frac{-1+\sqrt{-3}}{2}$.

命題 26. $\mathrm{Aut}_K(L)$ は、合成写像を演算と考えれば群になっている。

Proof. 実際、自己同型写像の合成はやはり自己同型写像になり、単位元は恒等写像、逆元は逆写像（全単射だからかならず逆写像がつくれる）。また、合成写像の性質より、結合法則も明らかに成り立つ。 □

注意 27 (群論の起源)**.** 群構造は数学のさまざまなところで見出され、「面白い数学にはからなず群が関係している」と考える数学者も居る。群論の起源はおそらく *J. L. Lagrange* が、古くから知られていた３次・４次方程式の解法の仕組みを詳しく調べ、解の対象性を発見したことにあると思われる。*Lagrange* のアイディアは、*C. F. Gauß, N. H. Abel, E. Galois* らによって深められ、そこから群論が生まれたようである。つまり群論の起源は代数方程式論にあり、$\mathrm{Aut}_K(L)$ や次に述べるガロア群 $\mathrm{Gal}\,(L/K)$ はもっとも由緒正しい群の具体例だと言える。しかしながら、その後群論は代数方程式論からは独立した一般理論として発展し、代数方程式以外のさまざまな分野（微分方程式、関数解析、幾何学、トポロジーなど）ところに応用されて現在にいたっている。

1.3.2. ガロア群. 代数方程式

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0, \quad (a_1, \ldots, a_n \in \mathbb{C})$$

の解を $x_1, \ldots, x_n \in \mathbb{C}$ とするとき、基礎体

$$K = \mathbb{Q}(a_1, \ldots, a_n)$$

と分解体

$$L = K(x_1, \ldots, x_n)$$

に対して、

$$\mathrm{Gal}\,(L/K) := \mathrm{Aut}_K(L)$$

と定義し、これを方程式 $f(x) = 0$ のガロア群と呼ぶ。また、(適当な条件をみたす) 中間体 $K \subset H \subset L$ に対して、$\mathrm{Gal}\,(L/H)$ や $\mathrm{Gal}\,(H/K)$ を考える。

代数方程式を深く理解するためには、ガロア群 $\mathrm{Gal}\,(L/K), \mathrm{Gal}\,(L/H), \mathrm{Gal}\,(H/K)$ を調べることが重要であり、方程式のガロア群の構造を調べることにより、

(1) ３、４次方程式の解の公式の意味
(2) （５次以上の）代数方程式が、冪根で解けるかどうかの判定
(3) ５次以上の代数方程式の「解の公式」が存在しない本質的な理由

といったことが初めて明らかになるのである。

2. 2次方程式再論

拡大体やガロア群の理論が真に威力を発揮するのは3次以上の代数方程式であるが、ここでは前節で述べた考え方— つまり、「一番小さい基礎体から始めて、少しずつ大きな拡大体を考えながら、最終的に方程式の分解体にたどりつくというやり方で代数方程式の解を搜す」というアイディア— に馴れるために、まず2次方程式の例を考えてみる。

2.1. **2次方程式の解法と分解体.** 2次方程式の解法は、その分解体の構成方法を示している。例 12 の内容と重複するが、もう一度詳しくみてみよう。以下で使われている

- 方程式を変形して、より簡単な形の標準形を考えること。
- 判別式を考えて、その平方根による拡大体を考えること。

の2つの考え方は、3次や4次の方程式でも使われる。

2.1.1. 2次方程式の標準形. 2次方程式は

$$f(x) = x^2 + ax + b = \left(x + \frac{a}{2}\right)^2 - \frac{a^2 - 4b}{4} = 0$$

と変形することにより、

$$g(X) := X^2 - c = 0, \quad (\text{ただし、} c = \frac{a^2 - 4b}{4})$$

を解きさえすれば、あとは、$x = X - \dfrac{a}{2}$ によって解を得る（$g(X) = 0$ を2次方程式の「標準形」と呼んでもよい)。ここで

$$\Delta = a^2 - 4b$$

は、元の方程式の「判別式」であることに注意。また、2次方程式 $f(x) = 0$ の基礎体は $K = \mathbb{Q}(a, b)$ で、明らかに $\Delta \in K$ だが、$\sqrt{\Delta} \in K$ かどうかは一般にはわからない。

2.1.2. 拡大体 $K(\sqrt{\Delta})$. まずは、基礎体に判別式の平方根を付け加えた代数拡大

$$K \subseteq K(\sqrt{\Delta})$$

を考える。

(1) $\sqrt{\Delta} \in K$ の場合: $g(X) \in K[X]$ は可約である。すなわち、$K[X]$ の中で

$$g(X) = X^2 - \frac{\Delta}{4} = (X - \frac{\sqrt{\Delta}}{2})(X + \frac{\sqrt{\Delta}}{2})$$

と因数分解され、1次方程式の問題に帰着される。

(2) $\sqrt{\Delta} \notin K$ の場合: 冪根による2次拡大体

$$K \subset K(\sqrt{\Delta})$$

を考えると、$X = \pm\frac{\sqrt{\Delta}}{2} \in L - K$ が $g(X) = 0$ の解になることがわかり、結局

$$x = \pm\frac{\sqrt{\Delta}}{2} - \frac{a}{2} = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$$

なる解を得る。また、$\sqrt{\Delta} \neq 0$ ゆえ（理由：もし $\sqrt{\Delta} = 0$ ならば $0 \in K$ より、仮定に反する）、方程式は相異なる 2 つの解を持つ。

いずれにせよ、$L = K(\sqrt{\Delta})$ が 2 次方程式の分解体であることがわかる。

2.2. **2 次方程式のガロア群.** 2 次方程式

$$f(x) = x^2 + ax + b = 0 \quad (a, b \in \mathbb{C})$$

に対し、基礎体を $K = \mathbb{Q}(a, b)$ とおく。方程式の解を x_1, x_2 としたとき、$f(x)$ の分解体 $L = K(x_1, x_2)$ を考え、ガロア群 $\mathrm{Gal}\,(L/K)$ を計算しよう。

以下では、特に 2.2.2 で見るように

- $\mathrm{Gal}\,(L/K)$ は、2 次方程式の解の「置換」になっている

というところが重要で、このことは 3 次以上の代数方程式を考える場合にも効いてくる。

2.2.1. $\sqrt{\Delta} \in K$ の場合. このとき、$L = K$ だから、定義により

$$\mathrm{Gal}\,(L/K) = \mathrm{Gal}\,(K/K) = \{1_K \mid 1_K : K \to K \text{ 恒等写像}\}$$

となる。これは単位元だけからなる群 (これを「**自明な群** (trivial group)」とよぶ) である。

2.2.2. $\sqrt{\Delta} \in K$ でない場合. このとき、

$$L = K\left(\frac{-a + \sqrt{\Delta}}{2},\ \frac{-a + \sqrt{\Delta}}{2}\right) = K(\sqrt{\Delta}) \neq K$$

である。

演習問題 2. このことを示せ。(ヒント：2 次方程式の 2 つの解 x_1, x_2 を使って Δ を、逆に Δ を使って x_1, x_2 を書き表せることを示せばよい。)

従って、任意の $\sigma \in \mathrm{Gal}\,(L/K)$ は $\sigma(\sqrt{\Delta})$ の値を与えることによって決まる。では、この値は何でもよいのだろうか？そうではない。$f(x) = 0$ の（相異なる）解を x_1, x_2 としたとき、

$$0 = f(x_1) = x_1^2 + ax_1 + b, \quad 0 = f(x_2) = x_2^2 + ax_2 + b$$

だから、これに σ を作用させると

$$\begin{aligned} 0 &= \sigma(0) \\ &= \sigma(f(x_1)) = \sigma(x_1^2 + ax_1 + b) \\ &= \sigma(x_1^2) + \sigma(ax_1) + \sigma(b) = \sigma(x_1^2) + a\sigma(x_1) + b \\ &\qquad K\text{-線形性による} \\ &= \sigma(x_1)^2 + a\sigma(x_1) + b \\ &\qquad \sigma \text{ は積を積に移すから} \end{aligned}$$

同様に

$$0 = \sigma(f(x_2)) = \sigma(x_2)^2 + a\sigma(x_2) + b$$

となる。つまり、$\sigma(x_1), \sigma(x_2)$ は、やはり同じ 2 次方程式の解でなければならない。よって

$$\sigma(x_1) = \frac{-a + \sigma(\sqrt{\Delta})}{2} \in \{x_1, x_2\}$$

同様に

$$\sigma(x_2) = \frac{-a - \sigma(\sqrt{\Delta})}{2} \in \{x_1, x_2\}$$

でなければならない。すなわち、

$$\sigma(\sqrt{\Delta}) = \sqrt{\Delta} \quad \text{または} \quad -\sqrt{\Delta}$$

しかありえない。前者の場合は恒等射 1 にほかならない。後者を改めて σ と置くと、$\sigma^2 = 1$ となる (但し、σ^2 は合成写像 $\sigma \circ \sigma$ のことである)。そこで、

$$\mathrm{Gal}\,(L/K) = \langle \sigma \mid \sigma^2 = 1 \rangle$$

と書ける。右辺は「$\sigma^2 = 1$ なる関係式を満たす要素 σ で**生成された**群」と読む。「生成された」とは「その要素を使って、ありとあらゆる演算を行って出てくる答を全部含む集合を作る」という意味である。今の場合、σ という要素 1 つだけでは、それ自身を何乗かする演算ぐらいしかできない。ところが 2 乗したらもう恒等射になってしまう。だから結局

$$\langle \sigma \mid \sigma^2 = 1 \rangle = \{1, e\}$$

となるわけである。このような群を**２次の巡回群**と呼ぶ。また、２つのもの（今の場合は２つの解 x_1 と x_2) を並べ替える操作の集まりになっていることから、**２次の対称群** $\mathfrak{S}_2$ と呼ばれることもある。

3. 3 次方程式論

2 次方程式の場合、分解体は基本的には基礎体 K に判別式 Δ の平方根を付け加えた $L = K(\sqrt{\Delta})$ であり、ガロア群 $\mathrm{Gal}\,(L/K)$ は自明か、あるいは、2 次の巡回群であった。

3 次方程式の場合もやはり判別式 Δ が定義されるが、$K(\sqrt{\Delta})$ は一般に分解体 L よりも小さく、$K(\sqrt{\Delta})$ を更に拡大体しないとと L にならない。ではどのように拡大すれば分解体 L にたどりつけるのか？そこに 2 次方程式の場合とは違った、3 次方程式の代数的解法の複雑さが現れるのである。

3.1. 3 次方程式の標準形.

3 次方程式 $f(x) = 0$ は

$$\begin{aligned} f(x) &= x^3 + ax^2 + bx + c \qquad (a, b, c \in \mathbb{C}) \\ &= \left(x + \frac{a}{3}\right)^3 + p\left(x + \frac{a}{3}\right) + q \end{aligned}$$

ただし $p = b - \frac{a^2}{3}$, $q = c - \frac{ab}{3} + \frac{2a^3}{27}$, のように変形するとにより、$x + \frac{a}{3}$ を改めて x と置き直して

$$f(x) = x^3 + px + q \quad (p, q \in \mathbb{C})$$

の形のものを考える。基礎体は $K = \mathbb{Q}(p, q)$ とする。

また、$f(x) \in K[x]$ は既約と仮定する。なぜならば、もし $f(x)$ が可約だとすると、$f(x) = (x - s)(x^2 + tx + u)$ または $f(x) = (x - s)(x - t)(x - u)$, $s, t, u \in K$, と因数分解され、1 次方程式や 2 次方程式の問題に帰着されてしまうからである。さらに、

命題 28. $f(x) \in K[x]$ が既約とする。このとき、$f(x) = 0$ の解を x_1, x_2, x_3 とすれば、$x_1, x_2, x_3 \notin K$.

Proof. 背理法で証明する。もし $x_1 \in K$ ならば $f(x) = (x - x_1)g(x)$, $g(x) \in K[x]$ は適当な 2 次式, と因数分解されるから、$f(x)$ の既約性の仮定に反する。x_2, x_3 についても同様。 □

さらに、

命題 29. $f(x) \in K[x]$ が既約とする。このとき x_1, x_2, x_3 は互いに異なる。すなわち、方程式 $f(x) = 0$ は重解をもたない。

Proof. 背理法で証明する。もし重解 α をもつなら、それは $d(x) := (f(x), f'(x)) = 0$ の解である。すなわち、$f(\alpha) = f'(\alpha) = 0$. ここで $\deg f(x) > \deg f'(x)$ だから、割り算を行って

$$f(x) = q(x)f'(x) + r(x), \quad \exists q(x), \exists r(x) \in K[x], \deg r(x) < \deg f'(x)$$

とできて、さらに $x = \alpha$ とすることにより、$r(\alpha) = 0$ とできる。ここで $\deg r(x) < \deg f'(x) = 2$ だから、$r(x) = c(x - \alpha)$, $c \in K - \{0\}$, なる形か、あるいは $r(x) = 0$ でなければならない。前者なら $\alpha \in K$ となり $f(x) = (x - \alpha)g(x)$, $g(x) \in K[x]$ は適当な 2 次式、と因数分解されてしまい、既約性に反する。また、$r(x) = 0$ も $f(x) = q(x)f'(x)$ で $\deg q(x) = 1$ だから、やはり $f(x)$ の既約性に反する。 □

演習問題 3. 命題 29 の証明で使った以下の事実を証明せよ：$f(x) \in K[x]$ を任意の多項式（3 次とは限らない）とする。代数方程式 $f(x) = 0$ が重解を持つならば、$f(x)$

と $f'(x)$ は1次以上の共通因子を持つ。(ヒント：代数学の基本定理により $\mathbb{C}[x]$ の中で1次因子に因数分解してから、x について微分してみよ。)

3次方程式 $f(x)=0$ を解くということは、解 x_1,x_2,x_3 を具体的に求めることだが、解 x_1,x_2,x_3 が分かれば $f(x)=0$ の分解体 $K(x_1,x_2,x_3)$ も分かる。逆に、分解体 $K(x_1,x_2,x_3)$ が分かる時には、解 x_1,x_2,x_3 も分かっているはずである。すなわち

「方程式を解くこと」＝「方程式の分解体を求めること」

と考えることができる。では、分解体はどうやって求めれば良いのか？その指針を与えるのが (ガロア) 群である。

3.2. **3次方程式のガロア群.** 分解体 $L=K(x_1,x_2,x_3)$ が詳しく分からない段階でも、ガロア群 $\mathrm{Gal}\,(L/K)$ がどんなものであるか、おおよそのところは分かる。このことを手掛かりにして分解体を捜すことができる。まずは、ガロア群の様子を見てみよう。

ガロア群の任意の要素 $\sigma\in\mathrm{Gal}\,(L/K)$ は、$\sigma(x_1),\sigma(x_2),\sigma(x_3)\in L$ の値を与えることにより決まるが、この値は自由に取れるわけではない。実際、

$$0=f(x_i)=x_i^3+px_i+q\in L\qquad(i=1,2,3)$$

に σ を作用させると、σ が K-線形写像で、かつ、積を積に移すことから、

$$0=\sigma(f(x_i))=\sigma(x_i)^3+p\sigma(x_i)+q.$$

従って

$$\sigma(x_i)\in\{x_1,x_2,x_3\}\qquad(i=1,2,3),$$

でなければならない。これは、x_i の添字 i のところに注目すれば、「σ は $1,2,3$ という数字の並べ換えを誘導する」と考えることができる。

このことをもう少し正確に述べよう。

定義 30 (対称群 $\mathfrak{S}_n$)**.** n 次の「**対称群** (symmetric group)」$\mathfrak{S}_n$ とは、次のようなものである。

$$\mathfrak{S}_n=\left\{\begin{pmatrix}1&2&\cdots&n\\ i_1&i_2&\cdots&i_n\end{pmatrix}:\{i_1,i_2,\ldots,i_n\}=\{1,2,\ldots,n\}\right\}$$

(すなわち、$i_1\,i_2\,\ldots\,i_n$ は $1\,2\,\ldots\,n$ を並べ換えたもの)
また、任意の元

$$\sigma=\begin{pmatrix}1&\cdots&n\\ i_1&\cdots&i_n\end{pmatrix}\in\mathfrak{S}_n$$

を $\sigma(k)=i_k,\ k=1,\ldots,n,$ なる写像

$$\sigma:\{1,\ldots,n\}\longrightarrow\{1,\ldots,n\}$$

と考えれば、写像の合成 $\sigma\circ\tau$ により積 $\sigma\tau$ を定義でき、$\mathfrak{S}_n$ は群になる。また、その位数は $\sharp(\mathfrak{S}_n)=n!$ となる。

注意 31. n 次対称群 $\mathfrak{S}_n$ は、1回生前期の線形代数で行列式を定義する時に出てきたことを思い出そう。

そこで、$n=3$ の場合を考えて、

$$\mathrm{Gal}\,(L/K)\ni\sigma \text{ s.t. } \begin{cases}\sigma(x_1)=x_{i_1},\\ \sigma(x_2)=x_{i_2},\\ \sigma(x_3)=x_{i_3}\end{cases} \longmapsto \begin{pmatrix}1&2&3\\ i_1&i_2&i_3\end{pmatrix}\in\mathfrak{S}_3$$

なる対応によって、3次方程式のガロア群は3次の対称群の一部だと考える：

$$\mathrm{Gal}\,(L/K)\subset\mathfrak{S}_3$$

しかも $\mathrm{Gal}\,(L/K)$ 自身も $\mathfrak{S}_3$ で定義されている積演算と同じ演算で群になっている。このことを、「$\mathrm{Gal}\,(L/K)$ は $\mathfrak{S}_3$ の部分群である」と言う。

定義 32 (部分群)**.** 群 $(G,*,1_G)$ の部分集合 $H\subset G$ が「**部分群** (subgroup)」であるとは、H 自身が G の群としての積演算"$*$"と単位元"1_G"を使って群になっているときをいう。具体的には、次の3条件を満たす場合をいう：

(1) $1_H=1_G$
(2) $x,y\in H$ ならば $x*y\in H$
(3) $x\in H$ ならば $x^{-1}\in H$ (x^{-1} は $x\in G$ の G の元としての逆元)

また、自明な部分群 $\{1_G\}, G$ 以外の部分群のことを「**真の部分群** (proper subgroup)」と呼ぶ。自明な部分群は、単に1と略記することもある。

以下は部分群であることの簡単な判定法を与えている。

命題 33. 群 $(G,\cdot,1_G$ の部分集合 $H\subset G$ に対して、以下は同値である：
(i) H は部分群である。
(ii) 任意の $x,y\in H$ に対して、$x\cdot y^{-1}\in H$

Proof. (i) $\Rightarrow$ (ii): $x,y\in H$ に対して、定義 32 の条件 3. より $y^{-1}\in H$, よってさらに条件 2. より $x\cdot y^{-1}\in H$ を得る。

(ii) $\Rightarrow$ (i): 任意の元 $x\in H$ に対して、(ii) より $x\cdot x^{-1}=1_G\in H$. すなわち定義 32 の条件 1 が得られた。そこで、$1_G,x\in H$ に (ii) を適用すると、$1_G\cdot x^{-1}=x^{-1}\in H$. すなわち、定義 32 の条件 3 が得られた。最後に、$x,y\in H$ に対して条件 3 より $y^{-1}\in H$ だから、$x,y^{-1}\in H$ に (ii) を適用して、$x\cdot(y^{-1})^{-1}=x\cdot y\in H$. すなわち、定義 32 の条件 2 が得られた。 □

ガロア群が置換群の部分群であることは分かったが、それが分解体の構成にどのように関係するのだろうか？その答えは、次節の「ガロアの基本定理」によって与えられる。

3.3. **ガロアの基本定理.** 基礎体 K と分解体 L との中間体の集合

$$\mathcal{F}=\{E\mid K\subset E\subset L \text{ 中間体}\}$$

および、ガロア群の部分群の集合

$$\mathcal{G}=\{G\mid G\subset \mathrm{Gal}\,(L/K) \text{ 部分群}\}$$

を考え、これらの間の対応

$$\begin{array}{rccc}\Psi: & \mathcal{F} & \longrightarrow & \mathcal{G}\\ & E & \longmapsto & \mathrm{Gal}\,(L/E)\end{array}$$

および

$$\begin{array}{rccl} \Phi: & \mathcal{G} & \longrightarrow & \mathcal{F} \\ & G & \longmapsto & L^G = \{x \in L \mid \sigma(x) = x \quad \forall \sigma \in H\} \end{array}$$

を考える。$\mathrm{Gal}\,(L/E)$ が $\mathrm{Gal}\,(L/K)$ の部分群になる理由は、$K(\subset E)$ だけを固定する (つまり $x \in K$ に対して $\sigma(x) = x$ となるということ) 自己同型よりも、さらに E の要素までも固定するという余分の条件が付け加わった自己同型の方が少ないからである。

これらの対応は次のようにパラフレーズできる。

- 中間体 E に対して、E の元を全て固定するような L の自己同型を対応させる（Ψ 対応)。
- 部分群 $G \subset \mathrm{Gal}\,(L/K)$ に対して、それが固定する L の要素ばかりを集めた中間体を対応させる (Φ 対応)。

定理 34. 上の仮定のもとで、

(i) [**ガロアの基本定理**] $\Psi \circ \Phi = \mathrm{id}_{\mathcal{G}}$, $\Phi \circ \Psi = \mathrm{id}_{\mathcal{F}}$. すなわち、$\Phi$, Ψ は全単射。

(ii) 任意の $E \in \mathcal{F}$ に対し、$[L : E] = \sharp\mathrm{Gal}\,(L/E)$.

Proof. 3 回生「環・体論 II」で習え。 □

定理 34 は、拡大体の列

$$K \subset E_1 \subset E_2 \subset \cdots \subset L$$

と、ガロア群の部分群の列

$$\mathrm{Gal}\,(L/K) \supset \mathrm{Gal}\,(L/E_1) \supset \mathrm{Gal}\,(L/E_2) \supset \cdots \supset \mathrm{Gal}\,(L/L) = 1$$

が（包含関係を逆にして）１：１に対応していること、さらには、ガロア群の位数が拡大体の線形空間としての次数を表すことを意味する。

また、次の命題は拡大体の線形空間として次数を計算する際に有用である。

命題 35. 中間体 $K \subset H \subset L$ に対して、$[L : K] = [L : H][H : K]$.

Proof. 3 回生「環・体論 II」で習え。 □

例 36 (命題 35 の例)**.** 拡大体

$$\mathbb{Q} \ \subset \ \mathbb{Q}(\sqrt{2}) \ \subset \ \mathbb{Q}(\sqrt{2}, i) \qquad (i = \sqrt{-1})$$

に対し、命題 21、および、その後のコメントの考え方を使って線形空間としての構造を調べよう。まず、$\sqrt{2}$ は既約式 $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ による方程式 $f(x) = 0$ の解だから、命題 21 により、1 と $\sqrt{2}$ を基底とする $\mathbb{Q}$-線形空間

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q} \cdot 1 \oplus \mathbb{Q} \cdot \sqrt{2}$$

であり、$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. また、$\mathbb{Q}(\sqrt{2}, i)$ は $\mathbb{Q}(\sqrt{2})$ に $i = \sqrt{-1}$ を付け加えた拡大体だが、i は既約式 $g(x) = x^2 + 1 \in \mathbb{Q}(\sqrt{2})[x]$ による方程式 $g(x) = 0$ の解だから、命題 21 により 1 と i を基底とする $\mathbb{Q}(\sqrt{2})$-線形空間

$$\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2}) \cdot 1 \oplus \mathbb{Q}(\sqrt{2}) \cdot i$$

となり、$[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 2$ をえる。よって、命題 35 によれば、

$$[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$$

では、$\mathbb{Q}(\sqrt{2},i)$ の $\mathbb{Q}$-基底はなにか？それは、上の計算から

$$\begin{aligned}\mathbb{Q}(\sqrt{2},i) &= \mathbb{Q}(\sqrt{2})\cdot 1 \oplus \mathbb{Q}(\sqrt{2})\cdot i \\ &= (\mathbb{Q}\cdot 1 \oplus \mathbb{Q}\cdot\sqrt{2})\cdot 1 \oplus (\mathbb{Q}\cdot 1 \oplus \mathbb{Q}\cdot\sqrt{2})\cdot i \\ &= \mathbb{Q}\cdot 1 \oplus \mathbb{Q}\cdot\sqrt{2} \oplus \mathbb{Q}\cdot i \oplus \mathbb{Q}\cdot i\sqrt{2}\end{aligned}$$

となるから、$\{1,\ \sqrt{2},\ i,\ i\sqrt{2}\}$ が基底となっている。

3.4. **del Ferro-Tartaglia-Cardano-Lagrange の公式.** 任意の 3 次方程式は代数的に解くことができ、解の公式は以下の通りである。

定理 37 (Cardano)**.** [1] *3*次方程式 $f(x)=x^3+px+q=0$ の解を x_1,x_2,x_3 とすると、

$$x_1=u+v,\quad x_2=\zeta^2u+\zeta v,\quad x_3=\zeta u+\zeta^2 v$$

ただし、ζ は 1 の原始 3 乗根で、

$$u=\sqrt[3]{-\frac{q}{2}+\sqrt{\left(\frac{p}{3}\right)^3+\left(\frac{q}{2}\right)^2}},\quad v=\sqrt[3]{-\frac{q}{2}-\sqrt{\left(\frac{p}{3}\right)^3+\left(\frac{q}{2}\right)^2}}$$

であり、この 3 乗根は $uv=-\frac{p}{3}$ を満たすものを選ぶものとする。

この定理は、

$$K\subseteq K(\sqrt{\tilde{\Delta}})\subseteq K(\sqrt{\tilde{\Delta}},u,v)=L\quad \text{ただし、}\quad \tilde{\Delta}=\left(\frac{p}{3}\right)^3+\left(\frac{q}{2}\right)^2$$

という風に、中間体 $K(\sqrt{\tilde{\Delta}})$ を介した 2 段階に分けて分解体を構成すれば良いことを表している。ここで $\tilde{\Delta}$ は本質的に（3 次方程式の）判別式と同じものである。分解体を求めるとき、まず判別式の平方根による拡大体を考え、それでもまだ分解体が得られなければ、ガロア群の情報をうまく使ってさらなる拡大体を考えるのだが、ここでは判別式の平方根による拡大体にさらに u,v という 2 つの元を付け加えて分解体を構成しているのである。では、u,v はどうやってして見つけたのだろうか？以下で詳しく見ていこう。

3.4.1. 判別式 *discriminant* の平方根による拡大体 $K(\sqrt{\Delta})$. 一般に代数方程式

$$f(x)=(x-x_1)(x-x_2)\cdots(x-x_n)=0\quad (x_1,x_2,\ldots,x_n\in\mathbb{C})$$

に対して、

$$\Delta:=\delta^2,\quad \delta:=\prod_{i<j}(x_i-x_j) \tag{1}$$

を判別式 (dicriminant) と呼ぶ。

例 38. 2 次方程式 $f(x)=x^2+ax+b=(x-x_1)(x-x_2)$ の場合、

$$\Delta=(x_1-x_2)^2=(x_1+x_2)^2-4x_1x_2=a^2-4b$$

となり、お馴染みの「判別式」が得られる。

[1] この公式は、del Ferro, Tartaglia, Cardano, Lagrange らの努力によって最終的にこの形に纏められたと考えられるので、「Cardano の公式」と呼ぶよりも、むしろこの節の表題にあるように del Ferro-Tartaglia-Cardano-Langrange の公式とする方が、現代の数学者社会でのクレジットのつけ方に合っているのではないかと思われる。

ここでは３次方程式なので、

$$\delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

を考える。２次方程式の場合と同様、判別式 Δ は方程式の係数を使って書き表すことができる。

命題 39. $\Delta = -4p^3 - 27q^2 \ (\in K)$.

解と係数の関係 $x_1 + x_2 + x_3 = 0$, $x_1x_2 + x_2x_3 + x_3x_1 = p$, $x_1x_2x_3 = -q$ を使って直接計算で

$$\Delta = \delta^2 = (x_1^2x_2 + x_2^2x_3 + x_3^2x_1 - x_1x_2^2 - x_2x_3^2 - x_3x_1^2)^2 = -4p^3 - 27q^2$$

を導くのは、かなり骨が折れる。別の方法で計算しよう。

命題 39 の証明. $f(x) = (x - x_1)(x - x_2)(x - x_3) = x^3 + px + q$ より

$$f'(x) = (x - x_2)(x - x_3) + (x - x_1)(x - x_3) + (x - x_1)(x - x_2) = 3x^2 + p.$$

いま $x - x_i$ と $f'(x)$ の**終結式** *(resultant)* $\mathrm{Res}(x - x_i, f'(x))$ なるものを考える。それは次のような式である。

$$\mathrm{Res}(x - x_i, f'(x)) = \det \begin{bmatrix} 1 & -x_1 & 0 \\ 0 & 1 & -x_1 \\ 3 & 0 & p \end{bmatrix}$$

を考える。ここに現れる行列の最初の２行は $x - x_i$ の係数を右にひとつずつずらして並べたもので、$\deg f'(x) = 2$ に合わせて２行分とっている。３行目は $f'(x)$ の係数を並べたもので、$\deg(x - x_i) = 1$ であることに合わせて１行だけ書いている。これを計算すると、

$$\mathrm{Res}(x - x_i, f'(x)) = 3x_i^2 + p = f'(x_i)$$

となる。また、上で計算した $f'(x)$ の式を使えば

$$\begin{aligned} & f'(x_1) \cdot f'(x_2) \cdot f'(x_3) \\ = \ & (x_1 - x_2)(x_1 - x_3) \cdot (x_2 - x_1)(x_2 - x_3) \cdot (x_3 - x_1)(x_3 - x_2) \\ = \ & -\Delta \end{aligned}$$

を得る。ここで２次方程式 $f'(x) = 0$ の解を y_1, y_2 とすれば、$f'(x) = (x - y_1)(x - y_2)$ と因数分解されるから

$$f'(x_1) \cdot f'(x_2) \cdot f'(x_3) = \prod_{\substack{1 \le i \le 3 \\ 1 \le j \le 2}} (x_i - y_j)$$

そこで、次のことを示せばよい。

$$(-\Delta =) \prod_{\substack{1 \le i \le 3 \\ 1 \le j \le 2}} (x_i - y_j) = \det \begin{bmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 3 & 0 & p & 0 & 0 \\ 0 & 3 & 0 & p & 0 \\ 0 & 0 & 3 & 0 & p \end{bmatrix} (= 4p^3 + 27q^2)$$

ここで、上の行列式の部分は $f(x) = (x - x_1)(x - x_2)(x - x_3)$ と $f'(x)$ の終結式 $\mathrm{Res}(f(x), f'(x))$ で、上の行列の１行目と２行目までは、$f(x)$ の係数を１つずつず

らして $\deg' f(x) = 2$ 個並べたもの、３～５行目は $f'(x)$ の係数を１つずつずらして $\deg f(x) = 3$ 個並べたものになっている。つまり我々は

$$\begin{aligned} & \mathrm{Res}(x - x_1, f'(x)) \cdot \mathrm{Res}(x - x_2, f'(x)) \cdot \mathrm{Res}(x - x_3, f'(x)) \\ = \quad & -\mathrm{Res}((x - x_1)(x - x_2)(x - x_3), f'(x)) \end{aligned}$$

であることを言おうとしているわけである。

このことはより一般の次のような状況で示した方がわかりやすい。すなわち、

$$f(x) = x^3 + a_1 x^2 + a_2 x + a_3 = (x - x_1)(x - x_2)(x - x_3)$$

と

$$g(x) = x^2 + b_1 y^2 + b_2 = (x - y_1)(y - y_2)$$

という２つの多項式を考える。このとき

$$\mathrm{Res}(f(x), g(x)) = \det \begin{bmatrix} 1 & a_1 & a_2 & a_3 & 0 \\ 0 & 1 & a_1 & a_2 & a_3 \\ 1 & b_1 & b_2 & 0 & 0 \\ 0 & 1 & b_1 & b_2 & 0 \\ 0 & 0 & 1 & b_1 & b_2 \end{bmatrix}$$

は a_1, a_2, a_3, b_1, b_2 のついての多項式であり、解と係数の関係により、結局 x_1, x_2, x_3, y_1, y_2 についての多項式になる。もし、ある i, j について $x_i = y_j$, すなわち、$f(\alpha) = g(\alpha) = 0$ となる $x = \alpha (= x_i = y_j)$ が存在すれば、

$$\begin{bmatrix} 1 & a_1 & a_2 & a_3 & 0 \\ 0 & 1 & a_1 & a_2 & a_3 \\ 1 & b_1 & b_2 & 0 & 0 \\ 0 & 1 & b_1 & b_2 & 0 \\ 0 & 0 & 1 & b_1 & b_2 \end{bmatrix} \begin{bmatrix} \alpha^4 \\ \alpha^3 \\ \alpha^2 \\ \alpha \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \cdot f(\alpha) \\ f(\alpha) \\ \alpha^2 \cdot g(\alpha) \\ \alpha \cdot g(\alpha) \\ g(\alpha) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

従って、連立一次方程式方程式の理論より、$\mathrm{Res}(f(x), g(x)) = 0$ でなければならない。このことは、$1 \leq i \leq 3, 1 \leq j \leq 2$ の範囲で i, j を取り替えて $x_i - y_j = 0$ としてみても同じである。従って、(因数定理により)$\mathrm{Res}(f(x), g(x))$ が

$$R = \prod_{\substack{1 \leq i \leq 3 \\ 1 \leq j \leq 2}} (x_i - y_j)$$

で割り切れる。R は x_1, x_2, x_3, y_1, y_2 に関する 6 次の斉次式[2]。一方、$\mathrm{Res}(f(x), g(x))$ の次数は a_1, a_2, a_3 がそれぞれ x_1, x_2, x_3 に関する $1, 2, 3$ 次式で、b_1, b_2 がそれぞれ y_1, y_2 に関する $1, 2$ 次式であることから、行列式を計算してみればやはり x_1, x_2, x_3, y_1, y_2 に関する 6 次斉次式だとわかる。従って、

$$\mathrm{Res}(f(x), g(x)) = c \cdot R \quad (c \in \mathbb{C})$$

となるが、$y_1^3 y_2^3$ 項の係数を比較すれば、$c = 1$ とわかる。 □

[2]同じ次数の単項式ばかりからなる多項式のことを**斉次式** *(homogeneous polynomial)* と呼ぶ。

演習問題 4 (やや難)**.** 一般に n 次多項式 $f(x)=\prod_{i=1}^{n}(x-x_i)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n\in\mathbb{C}[x]$ と、その導関数 $f'(x)=b_0x^{n-1}+\cdots+b_{n-2}x+b_{n-1}$ に対して、

$$\Delta=(-1)^{\frac{n(n-1)}{2}}\cdot\det\begin{bmatrix}
1 & a_1 & a_2 & \cdots & a_n & & \\
 & 1 & a_1 & \cdots & a_{n-1} & a_n & \\
 & & & \cdots & \cdots & \cdots & \\
 & & & 1 & a_1 & \cdots & a_n \\
b_0 & b_1 & \cdots & \cdots & b_{n-1} & & \\
 & b_0 & b_1 & \cdots & \cdots & b_{n-1} & \\
 & & & \cdots & \cdots & \cdots & \\
 & & & b_0 & b_1 & \cdots & b_{n-1}
\end{bmatrix}$$

となっていることを示せ。ただし、上の行列は $2n-1$ 次の正方行列で、の $1\sim(n-1)$ 列目は $f(x)$ の係数を 1 つずつ右にずらしながら並べたもの、$n\sim(2n-1)$ 列目は $f'(x)$ の係数を 1 つずつ右にずらしながら並べたもの。文字も点も書かれていない部分は、全て 0 が入っているものとする。(ヒント：線形代数の教科書で「終結式」の項を調べてみよ。命題 39 の証明は、線形代数の教科書に書かれていることを特殊な場合にあてはめたものなので、教科書を読む際に参考にすると良いであろう。)

命題 40. $\sqrt{\Delta}=\pm\delta\in L$

Proof. L は分解体だから $x_1,x_2,x_3\in L$. ところが δ は x_1,x_2,x_3 の式だから、L に含まれる。 □

そこで、判別式の平方根による拡大体

$$K\subset K(\delta)=K(\sqrt{\Delta})$$

を考えることにする。

$$[K(\delta):K]=1\text{ または }2$$

であることに注意 ($\delta\in K$ のとき、$[K(\delta):K]=1$)。

3.4.2. $K(\sqrt{\Delta})$ と L とのギャップは何か？. さて、定理 34 と命題 35 によれば、

$$6=3!=\sharp\mathfrak{S}_3\geq\sharp\mathrm{Gal}\,(L/K)=[L:K]=[L:K(\sqrt{\Delta})][K(\sqrt{\Delta}):K]$$

ここで、$[K(\sqrt{\Delta}):K]\leq 2$ だったから、一般的解法を考える場合は $[K(\sqrt{\Delta}):K]=2$ の場合を考えて、上の式より $[L:K(\sqrt{\Delta})]\leq 3$ を得る。ここで $[L:K(\sqrt{\Delta})]<3$ となるのは $[L:K(\sqrt{\Delta})]=1$, つまり $L=K(\sqrt{\Delta})$ の場合に限られることがわかる（詳細は略[3])。従って、やはり一般的解法を考える場合は、

$$[L:K(\sqrt{\Delta})]=3$$

の場合を考えておけばよい。従って、再び定理 34 により

$$\sharp\mathrm{Gal}\,(L/K(\sqrt{\Delta}))=[L:K(\sqrt{\Delta})]=3$$

となる。つまり、ガロアの基本定理を使えば代数拡大 $L/K(\sqrt{\Delta})$ は位数 3 のガロア群に対応する拡大だとわかるから、そういうものを見つけることが次の目標となる。つまり、

- そもそも、位数 3 の群とはどんなものか？

[3]定理 34 と Lagrange の公式 (系 50) によるが

• そういう群をガロア群として持つ拡大体はどうやって構成すればよいのか？

それを以下で見ていこう。

3.4.3. 巡回群.

定義 41 (巡回群)**.** 群 G とその部分集合 $S = \{g_1, g_2, \ldots, g_k\} \subset G$ が与えられたとする。このとき、「S **で生成された** G **の部分群** (subgroup generated by S)

$$\langle S \rangle = \langle g_1, g_2, \ldots, g_k \rangle$$

とは、S を含む最小の部分群のことをいう。ここで「最小」とは、集合の包含関係について最小ということ、すなわち、$S \subset N \subset \langle S \rangle$ なる部分群 N があれば、必ず $N = \langle S \rangle$ となるという意味である。特に、$\langle g \rangle$, *i.e.,* $k = 1$, の場合を、「**巡回（部分）群** (cyclic (sub-)group)」と呼ぶ。

定義 42 (要素の位数)**.** 群 G の元 $x \in G$ に対して、$x^N = 1_G$ なる自然数 N が存在するとき（存在するとは限らない)、そのような N のうちの最小のもの n を x の「**位数** (order)」と呼ぶ。(群の位数 $\sharp G$ と混同しないこと！)

$\langle g_1, g_2, \ldots, g_k \rangle$ がどんなものかを具体的に書き下すのは、一般には難しい。しかし、$k = 1$ の場合だけは以下のように簡単である。

命題 43. 巡回（部分）群 $H = \langle g \rangle \subset G$ は、

$$H = \{\ldots, g^{-3}, g^{-2}, g^{-1}, 1_G, g, g^2, g^3, \ldots\}$$

の形をしている。有限群の場合は、$n = \mid H \mid < \infty$ とおけば、

$$H = \{1_G, g, g^2, g^3, \ldots, g^{n-1}\}$$

の形をしている。

Proof. 定義により、$\langle g \rangle$ は単位元 1_G と g を使ったありとあらゆる演算の結果を全て含む集合を考えればよい。1_G 同士はいくら演算をしても 1_G 以外の結果は出てこないし、1_G と g で演算をしても、やはり g しか出てこない。残るは g 同士の演算で、これより $g, g^2, g^3, \ldots$ が出てくる。また、逆元も必要だから、$g^{-1}, g^{-2}, g^{-3}, \ldots$ も出てくる。

g の位数が有限なら、どこかで $g^n = 1_G$, $n > 1$, となるから、それ以上はそれまでの演算の繰り返しになるだけで、新しい演算結果は出てこない。また、このとき、$g \cdot g^{n-1} = 1_G$ となるから、$g^{-1} = g^{n-1}$. つまり逆元も g^m, $m \geq 1$, の形で表される。従って、$G = \{1_G, g, g^2, g^3, \ldots, g^n\}$ のような形になる。 □

系 44. 群 G に対して、元 $x \in G$ の位数が n の時、巡回部分群 $\langle x \rangle$ の (群としての) 位数は n である。

Proof. 位数の定義より明らか。 □

演習問題 5. 有限群 G の位数を n とし、$a \in G$ を単位元以外の元とする。この時、a の位数が合成数ならば、適当な $\ell \in \mathbb{N}$ によって $b := a^\ell$ をとれば b の位数を素数とすることができる。このことを示せ。(ヒント：例えば a の位数が pq (p, q は相異なる素数) の時、a^p の位数は q であり、a^q の位数は p である。では、a の位数 n を素因数

分解して $n = p_1^{a_1} \cdots p_k^{a_k}$, $p_1, \ldots, p_k$ は相異なる素数、とした場合、$b := a^\ell$ の位数を p_1 とするには ℓ をどうとればよいか？)

部分群 $H \subset G$ と要素 $g \in G$ に対して、

$$gH = \{gh \ : \ h \in H\}, \quad Hg = \{hg \ : \ h \in H\}$$

と定義する。

補題 45. 部分群 $H \subset G$ に対して、以下は同値である：
(i) $g \in H$
(ii) $gH = H$.

Proof. $(i) \Rightarrow (ii)$: $g \in H$ だから、$gH \subset H$ は明らか。さらに、$g^{-1} \in H$ だから $gH = \{gh \ : \ h \in H\} \supset \{g(g^{-1}h) \ : \ h \in H\} = H$. $(ii) \Rightarrow (i)$: $1_G \in H$ だから、$g = g \cdot 1_G \in gH = H$. □

有限群の部分群の位数を数えるためは、次の結果が有用である。

命題 46. (有限とは限らない) 群 G とその部分群 $H \subset G$ に対して、
(i) $g \in G$ に対して $\sharp gH = \sharp H$.
(ii) $G = \bigcup_{g \in G} gH$ で、これは *disjoint union* , すなわち、相異なる $g, g' \in G$ に対して $gH = g'H$ か、または、$gH \cap g'H = \emptyset$ のいずれかが成り立つ。

Proof. (i) は

$$g^{-1} : gH \longrightarrow H, \quad gh \longmapsto g^{-1}gh = h$$

によって gH と H の間に全単射 (それを g^{-1} と名付けた) がつくれることから、明らか。

(ii) を言うためには、次の 2 つのことを言えばよい。
(a) 任意の $h \in H$ に対し、$h \in \bigcup_{g \in G} gH$
(b) 任意の $g, (\neq) g' \in G$ に対して、$gH = g'H$ であるか $gH \cap g'H = \emptyset$ のいずれか

(a) については、H が部分群ゆえ $1_G \in H$ であることから、$h = h \cdot 1_G \in hH \subset \bigcup_{g \in G} gH$ を得る。(b) については、もし $gH \cap g'H \neq \emptyset$ ならば $gH = g'H$ となることを言えばよい。そこで、$gH \cap g'H \ni c$ が存在したとする。すると $c = gh_1 = g'h_2$ となる $h_1, h_2 \in H$ が存在する。よって、$g' = g(h_1 h_2^{-1}) \in gH$ 従って、$g'H \subset gH$. 同様にして $gH \subset g'H$ もいえるから、結局 $gH = g'H$ となる。 □

定義 47 (剰余類)**.** 命題 *46* で示した、分解 $G = \bigcup_{g \in G} gH$ のことを右分解と呼び、各 gH のことを「**右剰余類**」(right residue class) と呼ぶ。右剰余類 gH に現れる $g \in G$ のことを「**代表元**」(representative) と呼ぶ。全く同様に、「**左剰余類**」(left residue class) による左分解 $G = \bigcup_{g \in G} Hg$ を考えることができる。

命題 46 の証明でもみたように、代表元は一意的ではない。以下のことは、剰余類を考える上で非常に基本的で重要な結果である。

系 48. 群 G とその部分群 $N \subset G$ により、剰余分解 $G = \bigcup_{g\in G} gH$ を考えたとき、各剰余類 gH の代表元 g は一意的には決まらない。このとき、以下は同値である。

(i) g, g' は同じ剰余類の異なる代表元である：$gH = g'H$.

(ii) $g'g^{-1} \in H$, *i.e.*, $g' \in gH$ (すなわち、「g と g' は H の元の分だけ食い違う」)

Proof. 命題 46 の証明より明らか。 □

命題 46 より $\sharp gH = \sharp H$ $(g \in G)$ だが、全く同様にして $\sharp Hg = \sharp H$ であることもわかる。ことから、特に G が有限群の場合は、以下の概念が重要である。

定義 49 (部分群の指数)**.** 有限群 G とその部分群 $H \subset G$ に対して、右（左）剰余類の個数を $(G : H)$ と書き、これを H の G における「**指数** (index)」と呼ぶ。

以下に示す Lagrange の公式は、有限群の理論では最も基本的な公式のひとつで、有限群の構造を詳しく調べる際によく使われる。

系 50 (Lagrange の公式)**.** 有限群 G とその部分群 $H \subset G$ に対して、

$$\sharp G = \sharp H \times (G : H).$$

Proof. 命題 46 により、適当な $g_1, \ldots, g_n \in G$ によって

$$\begin{aligned} \sharp G &= \sharp\{\bigcup_{i=1}^{n} g_i H\} \quad \text{(disjoint union)} \\ &= \sum_{i=1}^{n} \sharp g_i H = \sum_{i=1}^{n} \sharp H = n \times \sharp H \end{aligned}$$

ところが、$n = (G : H)$ にほかならないから、上記の公式を得る。 □

一般に位数だけ与えられただけでは有限群の構造は決まらない。しかし、素数位数の場合には、以下が成り立つ。これは Lagrange の公式の使い方の典型例の一つでもある。

命題 51. 位数が素数 p の有限群 G は巡回群である。

Proof. $x \in G - \{1_G\}$ を任意にとり、$x, x^2, x^3, \ldots$ と冪を考える。G は有限群だから、十分大きな $n \geq 1$ に対して、x^n はそれ以前のある冪 x^m $(m < n)$ に等しくなければならない：$x^n = x^m$. 両辺に x^{-m} を掛ければ、$x^{n-m} = 1_G$ を得る。すなわち、$x^k = 1_G$ となる $k > 1$ が存在する。そのような k のうちで最小のものをとっておく。すなわち、

$$\langle x \rangle = \{x, x^2, x^3, \ldots, x^{k-1}, 1_G = x^k\} \subset G$$

もし $\langle x \rangle \neq G$ ならば、$k < p$. よって Lagrange の公式 (系 50) より $k \mid p$ でなければならず、p が素数で $k > 1$ であることに矛盾。よって $G = \langle x \rangle$, すなわち G は巡回群である。 □

3.4.4. 巡回拡大. ガロアの基本定理 (定理 34) は、「(代数) 拡大の様子は群によって記述される」と主張していた。巡回拡大とは、巡回群によって記述される代数拡大のことである。すなわち、

定義 52 (巡回拡大)**.** 拡大体 L/K が「**巡回拡大** (cyclic extension)」とは、Gal (L/K) が巡回群になる場合をいう。

3 次方程式の問題の戻ると、今の場合 $L/K(\sqrt{\Delta})$ のガロア群は位数 3 の群になるとわかっているのだから、命題 51 により、それは 3 次巡回拡大になるわけである。

巡回拡大体は冪根による拡大によって作ることができる。すなわち、

定理 53 ([1]4.8.3)**.** $\mathbb{Q}$ と 1 の原始 d 乗根 ζ を含む体 K の d 巡回拡大 L/K は、$x^d - c = 0$, $c \in K$, なる形の方程式の根 $x = a$ によって $L = K(a)$ となる。

Proof. 3 回生「環・体論 II」で習え。 □

我々は基礎体を $K = \mathbb{Q}(p, q)$ (p, q は 3 次方程式の標準形の係数) として、2 次拡大 $K(\sqrt{\Delta})/K$ を考え、さらに分解体 L は $K(\sqrt{\Delta})$ の 3 次巡回拡大であろうと考えた。しかるに定理 53 によれば、3 次巡回拡大を構成するには 1 の原始 3 乗根 ζ が必要とわかった。そこで、基礎体 K に最初から ζ を付け加えておくことにする: $K = \mathbb{Q}(p, q, \zeta)$. こうしておいても、今までの議論にほとんど本質的な変更は必要はなく、やはり $K(\sqrt{\Delta})/K$ は 2 次巡回拡大であり、$L/K(\sqrt{\Delta})$ は 3 次巡回拡大であることに注意する。以後、基礎体は $K = \mathbb{Q}(p, q, \zeta)$ であるとして議論を続けよう。

さて、定理 53 によれば、1 の原始 3 乗根 ζ と、適当な $c \in K(\Delta)$ による方程式 $x^3 - c = 0$ の根 $x = a$ を使って $L = K(\Delta, a)$ とすれば良さそうである。あとは、c や a を決定すればよい。$a \in L$ については、次の定理が知られている。

定理 54 (ヒルベルトの定理９０)**.** 定理 *53* における $a \in L$ は、適当な $(0 \neq) x \in L$ と Gal (L/K) の生成元 σ によって

$$a = x + \zeta\sigma(x) + \zeta^2\sigma^2(x) + \cdots + \zeta^{d-1}\sigma^{d-1}(x)$$

の形で書ける。

Proof. 3 回生「環・体論 II」で習え。 □

定理 53 と定理 54 によれば、Gal $(K(\Delta, a)/K) = \langle\sigma\rangle$, $\sigma^3 = 1$ に対して

$$a = x + \zeta\sigma(x) + \zeta^2\sigma^2(x) \tag{2}$$

なる適当な元 $x \in K(\Delta, a)$ が存在する。ここで

$$\zeta = \frac{-1 + \sqrt{-3}}{2}, \quad \zeta^2 = \frac{-1 - \sqrt{-3}}{2}$$

とする。そしてあとは、x を求めればよいわけである。

しかし残念ながら、ヒルベルトの定理９０は、この x をどのように求めれば良いかについては、何も主張していない。そこでもうすこし工夫が必要になってくる。

3.4.5. 3次巡回拡大 $L/K(\sqrt{\Delta})$ の構成. ヒルベルトの定理９０（定理 54）から得られた式 (2) の $x \in L$ として、仮に３次方程式の解 x_1, x_2, x_3（のひとつ）をとってみることにしよう。つまり、$\langle\sigma\rangle = \mathrm{Gal}\,(L/K(\sqrt{\Delta}))$, $\sigma^3 = 1$, として、$x = x_1$ としてみる。このとき必要ならば x_1, x_2, x_3 の添字をつけかえて

$$x = x_1, \quad \sigma(x) = \sigma(x_1) = x_2, \quad \sigma^2(x) = \sigma(x_2) = x_3$$

と考えてもよい。このときの a を D_ζ と書き表そう:

$$D_\zeta = x_1 + \zeta x_2 + \zeta^2 x_3 \tag{3}$$

これが果たして我々が捜している a s.t. $L = K(\Delta, a) = K(x_1, x_2, x_3)$ かどうかは、まだ分からないが、もし

$$D_\zeta^3 \in K(\sqrt{\Delta}) \tag{4}$$

が成り立てば、定理 53 により、兎に角 $K(D_\zeta, \sqrt{\Delta})/K(\sqrt{\Delta})$ が３次巡回拡大になってくれて、$K(D_\zeta, \sqrt{\Delta}) = L$ であるという期待が持てる。また、3.1 節で考えた３次方程式の標準形を考えているのだから、解と係数の関係より、

$$D_1 = x_1 + x_2 + x_3 = 0 \tag{5}$$

とおく。

(4) の証明. 実際、D_ζ が $K(\sqrt{\Delta})$ の適当な要素の３乗根になっていること、すなわち $(D_\zeta)^3 \in K(\sqrt{\Delta})$ となって、$(D_\zeta)^3$ は $\delta = \sqrt{\Delta}$ の式で書き表せることを確かめよう。まず、

$$\delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 - x_1^2 x_3 - x_2^2 x_1 - x_3^2 x_2.$$

だから、

$$\begin{aligned}
(D_\zeta)^3 &= (x_1 + \zeta x_2 + \zeta^2 x_3)^3 \\
&= x_1^3 + x_2^3 + x_3^3 + 6x_1x_2x_3 \\
&\quad + 3\zeta(x_1^2x_2 + x_2^2x_3 + x_3^2x_1) + 3\zeta^2(x_1^2x_3 + x_2^2x_1 + x_3^2x_2) \\
&= x_1^3 + x_2^3 + x_3^3 + 6x_1x_2x_3 - \frac{3}{2}\sum_{i\neq j} x_i^2 x_j + \frac{3\sqrt{-3}}{2}\cdot\delta \\
&= (x_1 + x_2 + x_3)^3 - \frac{9}{2}(x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) \\
&\quad + \frac{27}{2}x_1x_2x_3 + \frac{3\sqrt{-3}}{2}\cdot\delta \\
&= -\frac{27}{2}q + \frac{3\sqrt{-3}}{2}\cdot\delta \qquad (\text{解と係数の関係、とくに } D_1 = 0)
\end{aligned}$$

これは確かに

$$K(\sqrt{\Delta}) = K(\delta) = \mathbb{Q}(p, q, \zeta) = \mathbb{Q}(p, q, \frac{-1 + \sqrt{-3}}{2}) = \mathbb{Q}(p, q, \sqrt{-3})$$

の要素である。 □

ここで後の議論での必要上、上の計算をもう少し進めると、(5) および命題 39 により、

$$(D_\zeta)^3 = -\frac{27}{2}q + \frac{3\sqrt{3(4p^3+27q^2)}}{2} = 27\left(-\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}\right)$$

となる。

次に (x_1, x_2, x_3) を (x_1, x_3, x_2) と入れ替えて、

$$D_{\zeta^2} = x_1 + \zeta^2 x_2 + \zeta x_3 \tag{6}$$

を考える。これは 1 の原始 3 乗根を ζ から ζ^2 に入れ替えてみたわけである。すると上と同様の計算により

$$(D_{\zeta^2})^3 = 27\left(-\frac{q}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}\right) \in K(\sqrt{\Delta})$$

となり、定理 53 により 3 次巡回拡大 $K(\sqrt{\Delta}, D_{\zeta^2})/K(\sqrt{\Delta})$ が得られる。

さて、以上により 2 つの 3 次巡回拡大

- $K(\sqrt{\Delta}, D_\zeta)/K(\sqrt{\Delta})$
- $K(\sqrt{\Delta}, D_{\zeta^2})/K(\sqrt{\Delta})$

が得られたわけだが、これらは実は同じものである。そのことを示すには、次のように議論すればよい：

Step 1: $D_\zeta,\ D_{\zeta^2}$ の 2 つを付け加えた拡大体 $K(\sqrt{\Delta}, D_\zeta, D_{\zeta^2})/K(\sqrt{\Delta})$ を考える。

$$K(\sqrt{\Delta}, D_\zeta),\ K(\sqrt{\Delta}, D_{\zeta^2}) \subseteq K(\sqrt{\Delta}, D_\zeta, D_{\zeta^2})$$

もし上の 2 つの拡大体が別のものならば、ここで得られた拡大体は 3 次よりも大きいはずである。

Step 2: しかるに

$$L = K(x_1, x_2, x_3) = K(\sqrt{\Delta}, D_\zeta, D_{\zeta^2})$$

であることが示せる。

Step 3: 従って、

$$K(\sqrt{\Delta}, D_\zeta),\ K(\sqrt{\Delta}, D_{\zeta^2}) \subseteq L$$

となり、これらは全て $K(\sqrt{\Delta})$ の 3 次巡回拡大だから、実は全て等しいとわかる。

そこで **Step 2** だけ示せばよい。

$$L = K(x_1, x_2, x_3) \supseteq K(\sqrt{\Delta}, D_\zeta, D_{\zeta^2})$$

は、$\Delta,\ D_\zeta,\ D_{\zeta^2}$ の定義と $\zeta \in K$ であることから明らか。逆の包含関係は、簡単のため

$$u = \frac{D_\zeta}{3} = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}},\quad v = \frac{D_\zeta}{3} = \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}}$$

とおいて (3)(5)(6) を連立方程式として解けば、

$$\begin{aligned} x_1 &= \frac{D_\zeta + D_{\zeta^2}}{3} = u + v \in K(\sqrt{\Delta}, D_\zeta, D_{\zeta^2}) \\ x_2 &= \frac{\zeta^2 D_\zeta + \zeta \cdot D_{\zeta^2}}{3} = \zeta^2 \cdot u + \zeta \cdot v \in K(\sqrt{\Delta}, D_\zeta, D_{\zeta^2}) \\ x_3 &= \frac{\zeta \cdot D_\zeta + \zeta^2 \cdot D_{\zeta^2}}{3} = \zeta \cdot u + \zeta^2 \cdot v \in K(\sqrt{\Delta}, D_\zeta, D_{\zeta^2}) \end{aligned}$$

を得ることからわかる。

以上により、分解体、そして同時に解 x_1, x_2, x_3 が得られた。

最後に、D_ζ, D_{ζ^2} を求めるには 3 乗根をとらなければならないが、3 乗根は 2 つあるので、どちらを選ぶべきかという問題が生じる。$1 + \zeta + \zeta^2 = 0$ に注意して

$$\begin{aligned} D_\zeta \cdot D_{\zeta^2} &= (x_1 + \zeta x_2 + \zeta^2 x_3)(x_1 + \zeta^2 x_2 + \zeta x_3) \\ &= x_1^2 + x_2^2 + x_3^2 + (\zeta + \zeta^2)(x_1 x_2 + x_2 x_3 + x_1 x_3) \\ &= x_1^2 + x_2^2 + x_3^2 - (x_1 x_2 + x_2 x_3 + x_1 x_3) \\ &= (x_1 + x_2 + x_3)^2 - 3(x_1 x_2 + x_2 x_3 + x_1 x_3) = -3p \end{aligned}$$

従って、$uv = -\frac{p}{3}$ とすればよい。

4. 3次対称群 $\mathfrak{S}_3$ とその構造

ここでは3次方程式の理論で活躍した3次対称群 $\mathfrak{S}_3$ を詳しく調べながら、群論の一般理論のいくつかを学ぶ。

3次対称群を具体的に書き下すと、以下のようになる

$$\mathfrak{S}_3 = \left\{ \begin{array}{l} 1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \\ \sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \ \tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \ \tau\sigma\tau = \sigma\tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \end{array} \right\}$$

また、位数は $|\mathfrak{S}_3| = 3! = 6$ である。

注意 55. ここで積の順序に注意する。例えば、

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

は、合成写像 $\sigma \circ \tau$ のことであって、$\tau \circ \sigma$ ではない。

演習問題 6. 数字の列 1 2 3 をまず τ で並べ変えて、さらに σ で並べ替えると、$\sigma\tau$ で並べ替えたのと同じ結果になることを確かめよ。同様の計算を、$\tau\sigma$, $\tau\sigma\tau$, $\sigma\tau\sigma$ でやってみよ。それ以外にも、$\tau\sigma\tau\sigma\tau$ や、$\sigma\tau\sigma\tau\sigma$, $\tau\tau$, $\sigma\sigma$ など、σ と τ を使った色々な積を計算してみて、いずれも上に示した $\mathfrak{S}_3$ のどれかになることを確かめよ。

4.1. **$\mathfrak{S}_3$ の部分群を決定する.** $\mathfrak{S}_3$ の部分集合は合計 $2^6 = 64$ 個あるが、部分群はそれよりも少ない。実際、Lagrange の公式 (系 50) から、部分群 $N \subset \mathfrak{S}_3$ の位数は $\mathfrak{S}_3$ の位数 $(= 6)$ の約数だから、$\sharp N = 1, 2, 3$ の3種類しかない。各位数について調べていくと、真部分群は以下の5つしかない。

- 位数1の部分群：$\langle 1 \rangle = \{1\}$ (単位元のみの部分群)
- 位数2の部分群 (1)：$\langle \sigma \rangle = \{1, \sigma\}$. $\sigma^2 = 1$ であることに注意。
- 位数2の部分群 (2)：$\langle \tau \rangle = \{1, \tau\}$. $\tau^2 = 1$ であることに注意。
- 位数2の部分群 (3)：$\langle \tau\sigma\tau \rangle = \langle \sigma\tau\sigma \rangle = \{1, \tau\sigma\tau = \sigma\tau\sigma\}$. $(\tau\sigma\tau)^2 = (\sigma\tau\sigma)^2 = 1$ であることに注意。
- 位数3の部分群：$\langle \sigma\tau \rangle = \{1, \sigma\tau, (\sigma\tau)^2 = \tau\sigma\}$. これは3次交代群とよび、$\mathfrak{A}_3$ と書く。

演習問題 7. $\mathfrak{S}_3$ の部分群が上のものに限られることを確かめよ。(上記以外の部分集合 $H \subset \mathfrak{S}_3$ をとり、H の要素同士の全ての演算を考えてみよ。H が部分群だとすれば、それらの演算結果もやはり H に含まれていなければならないことから、結局 H は上のいずれかに一致しなければならないことがわかる。)

4.2. **正規部分群.** 部分群の中でも「正規部分群」と呼ばれるものは、特別な性質を持っていて、それを使って新しい群（剰余群とよぶ）を作ることができる。剰余群は代数学のあらゆるところで極めて重要な役割を果たす。

部分群 $N \subset G$ に対して、次のことに注意しよう：

- 一般に $gN = Ng$ とはならない
- $g \notin N$ の時、一般に gN も Ng も部分群にはならない

但し、$g \in N$ の時は $gN = Ng = N$ となるので、部分群になる (補題 45 参照)。

例 56 ($gN \neq Ng$ となる例)**.** $N = \langle \sigma \rangle = \{1, \sigma\} \subset \mathfrak{S}_3 = G$ を考える。

- $g = \tau \in G$ の場合：

$$gN = \{\tau, \tau\sigma\} \neq \{\tau, \sigma\tau\} = Ng$$

で、両者とも部分群ではない。
- $g = \sigma\tau \in G$ の場合：

$$gN = \{\sigma\tau, \sigma\tau\sigma\} \neq \{\sigma\tau, \sigma\sigma\tau\} = \{\sigma\tau, \tau\} = Ng$$

で、両者とも部分群ではない。
- $g = \tau\sigma \in G$ の場合：

$$gN = \{\tau\sigma, \tau\sigma\sigma\} = \{\tau\sigma, \tau\} \neq \{\tau\sigma, \sigma\tau\sigma\} = Ng$$

で、両者とも部分群ではない。
- $g = \tau\sigma\tau = \sigma\tau\sigma \in G$ の場合：

$$gN = \{\tau\sigma\tau, \sigma\tau\sigma\sigma\} = \{\tau\sigma\tau, \sigma\tau\} \neq \{\tau\sigma\tau, \tau\sigma\} = \{\tau\sigma\tau, \sigma\sigma\tau\sigma\}Ng$$

で、両者とも部分群ではない。

ここで、部分集合 (部分群でなくてもよい)$H, K \subset G$ に対し、

$$HK = \{hk \ : \ h \in H \ k \in K\}$$

と書くことにする。群の結合法則から、部分集合 $H, L, K \subset G$ に対し

$$(HK)L = H(KL)$$

などが成り立つ。

定義 57 (正規部分群)**.** 部分群 $N \subset G$ が「**正規部分群** (normal subgroup)」とは、任意の $g \in G$ に対し $gNg^{-1} = N$, *i.e.,* $gN = Ng$ が成り立つ場合をいい、$N \triangleleft H$ または $G \triangleright N$ とかく。

例 58 ($\mathfrak{S}_3$ の非正規部分群)**.** 例 56, および同様の考察により、$\langle\sigma\rangle$, $\langle\tau\rangle$, $\langle\sigma\tau\sigma = \tau\sigma\tau\rangle$ はいずれも正規部分群でないことがわかる。

演習問題 8. 例 58 の事実を確かめよ。

例 59 ($\mathfrak{S}_3$ の正規部分群)**.** $\{1, \sigma\tau, (\sigma\tau)^2 = \tau\sigma\} = \mathfrak{A}_3 \triangleleft \mathfrak{S}_3$ である。このことを示すには、$g \in \mathfrak{S}_3 - \mathfrak{A}_3 = \{\sigma, \tau, \tau\sigma\tau = \sigma\tau\sigma\}$ に対して $g\mathfrak{A}_3g^{-1} = \mathfrak{A}_3$ であることを確かめれば良い。さらに、$\mathfrak{A}_3 = \langle\sigma\tau\rangle$ だから、

$$g\sigma\tau g^{-1} \in \mathfrak{A}_3$$

であることさえ言えれば十分である。実際、このとき、

$$g\tau\sigma g^{-1} = g(\sigma\tau)^2g^{-1} = g(\sigma\tau)(\sigma\tau)g^{-1} = (g\sigma\tau g^{-1})(g\sigma\tau g^{-1}) \in \mathfrak{A}_3$$

が従うからである。

- $g = \sigma \in G$ の場合： $g^{-1} = \sigma$ に注意して、

$$g\sigma\tau g^{-1} = \sigma\sigma\tau\sigma = \tau\sigma \in \mathfrak{A}_3.$$

- $g = \tau \in G$ の場合：$g^{-1} = \tau$ に注意して、

$$g\sigma\tau g^{-1} = \tau\sigma\tau\tau = \tau\sigma \in \mathfrak{A}_3.$$

- $g = \tau\sigma\tau(= \sigma\tau\sigma) \in G$ の場合：$g^{-1} = \tau\sigma\tau(= \sigma\tau\sigma)$ に注意して、

$$g\sigma\tau g^{-1} = \sigma\tau\sigma(\sigma\tau)\tau\sigma\tau = \sigma\tau\sigma\tau = \tau\sigma\tau\tau = \tau\sigma \in \mathfrak{A}_3.$$

また、$\{1\} \subset \mathfrak{S}_3$ は自明な正規部分群 (すなわち $\{1\} \triangleleft \mathfrak{S}_3$). さらに、$\{1\} \triangleleft \mathfrak{A}_3$ とも考えることができる。

正規部分群の著しい性質は、剰余群がつくれることである。

命題 60. $N \triangleleft G$ とする。このとき命題 *46* により、剰余類への分解

$$G = \bigcup_{g\in G} gN = \bigcup_{g\in G} Ng \quad (disjointunion)$$

が得られるが、さらに、剰余類の集合

$$G/N := \{gN, g'N, g''N, \ldots\} = \{Ng, Ng', Ng'', \ldots\}$$

は、次の演算によって群になっている：

$$(gN)\cdot(g'N) = gg'N.$$

Proof. まず注意しなければならないことは、G/N の「演算」が本当に演算として「正しく」定義されているかどうかである (このことを、「**演算が well-defined である**」という)。つまり、系 48 でみたように、剰余類の書き表し方は一通りではない。だから、上の「演算」は剰余類の書き表し方に依存せずに演算結果が只一つに決まるように定義されていなければならない。すなわち、

$$gN = hN,\ g'N = h'N \quad \Rightarrow \quad (gN)\cdot(g'N) = (hN)\cdot(h'N)$$

が成り立ってないといけない。このことをまず示そう。$gN = hN,\ g'N = h'N$ ならば、系 48 より

$$g = hn_1, \quad g' = h'n_2 \qquad (n_1, n_2 \in N)$$

と書き表せる。そこで

$$\begin{aligned}
(gN)\cdot(g'N) &= gg'N \quad (G/N \text{における演算の定義}) \\
&= g(g'N) = g(Ng') \quad (N \triangleleft G \text{だから}) \\
&= hn_1(Nh'n_2) = hNh'n_2 \quad \text{補題 } 45 \\
&= hh'Nn_2 \quad (N \triangleleft G \text{だから}) \\
&= hh'N \quad \text{補題 } 45 \\
&= (hN)\cdot(h'N) \quad (G/N \text{における演算の定義}).
\end{aligned}$$

これで、演算が well-defined であることが示せた。

この演算における単位元は $1_G N = N$ であり、gN の逆元が $g^{-1}N$ であることは明らか。結合法則も、G の結合法則より従う。 □

注意 61. 補題 *45* より $NN = N$ であることに注意すれば、$N \triangleleft G$ に対して G の演算だけを使って

$$(gN)(g'N) = g(Ng')N = gg'NN = ggN$$

とわかる。つまり、命題 *60* で定義した剰余群における演算は、元の群 G における演算を流用しているのである。

定義 62 (剰余群)**.** 命題 60(iii) でつくられた群 G/N を、(G の正規部分群 N による)「**剰余群** (residue class group)」と呼ぶ。

正規鎖の概念によって、代数方程式の理論と深く関連する「可解群」の概念を定義することができる。

定義 63 (正規鎖)**.** 部分群 $N_0 \subset N_1 \subset \cdots N_k \subset N_{k+1} = G$ に対して、

$$N_i \triangleleft N_{i+1} \quad (i = 0, 1, \ldots, k)$$

が成り立っているとき、「**正規鎖** (normal chain)」と呼ぶ。この時、剰余群の系列

$$N_{i+1}/N_i \quad (i = 0, 1, \ldots, k)$$

がつくれることに注意する。

例 64 ($\mathfrak{S}_3$ の正規鎖)**.** 例 *59* により、

$$\{1\} \triangleleft \mathfrak{A}_3 \triangleleft \mathfrak{S}_3$$

なる正規鎖が存在する。この時、

$$\mathfrak{A}_3/\{1\} = \mathfrak{A}_3$$

は 3 次の巡回群。また、$\mathfrak{S}_3/\mathfrak{A}_3$ の要素は、

$$\mathfrak{A}_3, \sigma\mathfrak{A}_3, \tau\mathfrak{A}_3, \sigma\tau\mathfrak{A}_3, \tau\sigma\mathfrak{A}_3, \tau\sigma\tau\mathfrak{A}_3$$

の 6 つが考えられるが系 *48* に従って 2 つが等しくなる条件をチェックすると、

- $\tau^{-1}\sigma = \tau\sigma \in \mathfrak{A}_3$ ゆえ、$\sigma\mathfrak{A}_3 = \tau\mathfrak{A}_3$.
- $(\tau\sigma\tau)^{-1}\sigma = \tau\sigma\tau\sigma = \sigma\tau\sigma\sigma = \sigma\tau \in \mathfrak{A}_3$ ゆえ、$\sigma\mathfrak{A}_3 = \tau\sigma\tau\mathfrak{A}_3$.
- $(\tau\sigma)^{-1}\sigma\tau = \sigma\tau\sigma\tau = \tau\sigma\tau\tau = \tau\sigma \in \mathfrak{A}_3$ ゆえ、$\sigma\tau\mathfrak{A}_3 = \tau\sigma\mathfrak{A}_3$.
- $\tau\sigma \in \mathfrak{A}_3$ ゆえ、ゆえ、$\tau\sigma\mathfrak{A}_3 = \mathfrak{A}_3$.
- $(\tau\sigma\tau)^{-1}\sigma\tau = \tau\sigma\tau\sigma\tau = \sigma\tau\sigma\sigma\tau = \sigma\tau\tau = \sigma \notin \mathfrak{A}_3$ ゆえ、$\sigma\tau\mathfrak{A}_3 \neq \tau\sigma\tau\mathfrak{A}_3$.

よって、

$$\sigma\mathfrak{A}_3 = \tau\mathfrak{A}_3 = \tau\sigma\tau\mathfrak{A}_3 (= \sigma\tau\sigma\mathfrak{A}_3) \neq \sigma\tau\mathfrak{A}_3 = \tau\sigma\mathfrak{A}_3 = \mathfrak{A}_3$$

従って、

$$\mathfrak{S}_3/\mathfrak{A}_3 = \{\mathfrak{A}_3, \sigma\mathfrak{A}_3\}$$

であり、これは 2 次の巡回群である。

定義 65 (可解群)**.** 群 G が「**可解群** (solvable group)」であるとは、正規鎖 $\{1\} = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft N_k \triangleleft N_{k+1} = G$ で、剰余群 N_{i+i}/N_i, $i = 0, 1, \ldots, k$, が全て巡回群になるものが存在する場合をいう。

注意 66. 可解群の本来の定義は、N_{i+1}/N_i が全て アーベル群 になることであるが、G が有限群の場合は上の定義と一致する (命題 111, 5.4.7 [1]).

命題 67. $\mathfrak{S}_2$ は可解群である。

演習問題 9. 上の命題 67 を証明せよ。

命題 68. $\mathfrak{S}_3$ は可解群である。

Proof. 例 64 により正規列

$$\{1\} \subset \mathfrak{A}_3 \subset \mathfrak{S}_3$$

が存在し、しかもその剰余群 $\mathfrak{A}_3/\{1\} = \mathfrak{A}_3$, $\mathfrak{S}_3/\mathfrak{A}_2$ は位数 3, および, 2 の有限群だから、命題 51 によりいずれも巡回群。 □

$\mathfrak{S}_3$ が可解群であることは、3 次方程式の解の公式が存在する本質的理由である（詳細は定理 118 参照）。

5. 4次方程式論

ここでは3次方程式で使った考え方を、4次方程式に適用してみる。すなわち、次のような方針で考えてゆこう。

- 4次方程式をできるだけ扱いやすい「標準形」に変形しておく。
- 4次方程式の解を x_1, x_2, x_3, x_4 とし、基礎体 K から出発して分解体 $L = K(x_1, x_2, x_3, x_4)$ を構成する（このことはすなわち4次方程式を解くことと同じ意味である）。
- まずは、判別式の平方根による2次拡大 $K(\sqrt{\Delta})$ を考え、それを足場にして拡大 $L/K(\sqrt{\Delta})$ を考える。
- 拡大 $L/K(\sqrt{\Delta})$ がどんなものでなければならないかは、ガロア群は4次対称群の部分群である $(\mathrm{Gal}\,(L/K) \subset \mathfrak{S}_4)$ ことから見通しを立てる。

5.1. **標準形.** 4次方程式 $F(X) = X^4 + aX^3 + bX^2 + cX + d = 0$ は、

$$\begin{aligned} F(X) &= (X + \frac{a}{4})^4 + (b - \frac{3a^2}{8})(X + \frac{a}{4})^2 + (c - \frac{ab}{2} + \frac{a^3}{8})(X + \frac{a}{4}) \\ &\quad + \frac{5a^4}{256} - \frac{a^4}{32} + \frac{a^2 b}{16} - \frac{ac}{4} + d \end{aligned}$$

と変形できるから、$x = X + \frac{a}{4}$ とおいて

$$f(x) = 0 \qquad f(x) = x^4 + px^2 + qx + r \in K[x]$$

と考える。ここで基礎体はとりあえず $K = \mathbb{Q}(p, q, r)$ とするが、3次方程式の議論で3次巡回拡大を作るときに行ったように、後で必要に応じて1の原始4乗根か3乗根 ζ を付け加えたものに取り替える必要が出てくる可能性も考慮しておく。また、方程式の解を x_1, x_2, x_3, x_4 とし、分解体を $L = K(x_1, x_2, x_3, x_4)$ とする。

以下の目標は、次の定理を証明することである。

定理 69 (Ferrari)**.** 4次方程式 $x^4 + px^2 + qx + r = 0,\ p, q, r \in K,$ の解は

$$\begin{aligned} x_1 &= \frac{1}{2}(\sqrt{-z_1} + \sqrt{-z_2} + \sqrt{-z_3}) \\ x_2 &= \frac{1}{2}(\sqrt{-z_1} - \sqrt{-z_2} - \sqrt{-z_3}) \\ x_3 &= \frac{1}{2}(-\sqrt{-z_1} + \sqrt{-z_2} - \sqrt{-z_3}) \\ x_4 &= \frac{1}{2}(-\sqrt{-z_1} - \sqrt{-z_2} + \sqrt{-z_3}) \end{aligned}$$

ただし、z_1, z_2, z_3 は、3次方程式

$$z^3 - 2pz^2 + (p^2 - 4r)z + q^2 = 0$$

の解で、

$$\sqrt{-z_1} \cdot \sqrt{-z_2} \cdot \sqrt{-z_3} = -q$$

となるように平方根を選ぶものとする。

5.2. **判別式の平方根による２次拡大.** まず、解と係数の関係より

$$x_1 + x_2 + x_3 + x_4 = 0. \tag{7}$$

判別式 $\Delta = \delta^2$, $\delta = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$ は命題 39 や演習 4 と同様の方法で計算することができ、詳細は省略するが

$$\Delta = 144pq^2r - 128p^2r^2 - 4p^3q^2 + 16p^4r - 27q^4 + 256r^3 \in K$$

となることが知られている。これを使って拡大

$$K \subset K(\sqrt{\Delta}) \subset L$$

を作ることができる。$\delta \in K$ の時は $[K(\sqrt{\Delta}) : K] = 1$ となり、$\delta \notin K$ の時は $[K(\sqrt{\Delta}) : K] = 2$ となる。

5.3. $K(\sqrt{\Delta})$ **と分解** L **のギャップ.** 3.2 節と同様に考えて、ガロア群 $\mathrm{Gal}\,(L/K)$ は 4 次対称群 $\mathfrak{S}_4$ の部分群だから、定理 34 と命題 35 によれば、

$$24 = 4! = \sharp\mathfrak{S}_4 \geq \sharp\mathrm{Gal}\,(L/K) = [L : K] = [L : K(\sqrt{\Delta})][K(\sqrt{\Delta}) : K]$$

ここで、$[K(\sqrt{\Delta}) : K] \leq 2$ だったから、一般的解法を考える場合は $[K(\sqrt{\Delta}) : K] = 2$ の場合を考えて、上の式より

$$[L : K(\sqrt{\Delta})] \leq 12$$

を得る。従って、再び定理 34 により

$$\sharp\mathrm{Gal}\,(L/K(\sqrt{\Delta})) = [L : K(\sqrt{\Delta})] \leq 12$$

となる。つまり、ガロアの基本定理を使えば代数拡大 $L/K(\sqrt{\Delta})$ は (高々) 位数 12 のガロア群に対応する拡大だとわかるから、そういうものを見つけることが次の目標となる。

３次方程式の場合は、$L/K(\sqrt{\Delta})$ が巡回拡大であろうと予想がついたが、４次方程式の場合は「位数 12（以下）のガロア群に対応する拡大体」というだけでは、詳しい状況はわからない。そこで我々は、「まず判別式の平方根による２次拡大 $K(\sqrt{\Delta})/K$ をつくり、それを足場にして、分解体 $L(\supset K(\sqrt{\Delta}))$ を考える」という方針を、とりあえず捨てることにしよう。

5.3.1. ある３次方程式の分解体 $K(z_1, z_2, z_3)$. そこで天下り的に

$$z_1 = (x_1 + x_2)(x_3 + x_4) \in L$$

とおく。z_1 に $\mathfrak{S}_4$ を

$$\sigma(x_i) = x_{\sigma(i)}, \qquad 1 \leq i \leq 4,\ \sigma \in \mathfrak{S}_4$$

によって作用させることにより

$$\begin{aligned} z_1 &= (x_1 + x_2)(x_3 + x_4) \in L \\ z_2 &= (x_1 + x_3)(x_2 + x_4) \in L \\ z_3 &= (x_1 + x_4)(x_2 + x_3) \in L \end{aligned}$$

が得られる。$\mathfrak{S}_4$ の z_1 への作用で新たに得られるものは、この z_1, z_2, z_3 が全てである。

演習問題 10. $z_2 = \sigma(z_1)$ となるような $\sigma \in \mathfrak{S}_4$ は以下の通りであることを確かめよ。

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}.$$

また、$z_1 = \sigma(z_1)$,$z_3 = \sigma(z_1)$ となる $\sigma \in \mathfrak{S}_4$ をそれぞれ全て求めよ。(ヒント：いずれも 8 個存在する)

補題 70. z_1, z_2, z_3 は 3 次方程式

$$x^3 - (z_1 + z_2 + z_3)x^2 + (z_1z_2 + z_2z_3 + z_3z_1)x - z_1z_2z_3 = 0 \tag{8}$$

の解で $b_1 := z_1 + z_2 + z_3,\ b_2 := z_1z_2 + z_2z_3 + z_3z_1,\ b_3 := z_1z_2z_3 \in K$ である。

Proof. 前半は解と係数の関係から明らか。後半は、b_1, b_2, b_3 のいずれも $\mathfrak{S}_4$ の作用で不変である。ここで $\mathrm{Gal}\ (L/K) \subset \mathfrak{S}_4$ であることを思い出すと、これらの式は $\mathrm{Gal}\ (L/K)$ の全ての元の作用で不変である。従ってガロアの基本定理 (定理 34) より $b_1, b_2, b_3 \in K$. □

そこで拡大体

$$K \subseteq K(z_1, z_2, z_3) \subseteq L$$

を考えると、$M := K(z_1, z_2, z_3)$ は 3 次方程式 (8) の分解体だから、$\sharp\mathrm{Gal}\ (M/K) = [M : K] \leq \sharp\mathfrak{S}_3 = 6$ である。従って、定理 34 と命題 35 により

$$\sharp\mathrm{Gal}\ (L/M) = [L : M] = [L : K]/[M : K] \leq \sharp\mathfrak{S}_4/6 = 4$$

となり、あとは M の（高々）4 次拡大を考えればよいことになる。

つまり、判別式の平方根による拡大体 $K(\sqrt{\Delta})$ を足場にして分解体 L を構成しようとすれば、ガロア群の位数が１２の拡大体を考えなければならなかったが、M を足場にして考えれば、位数が 4 の拡大体を考えればよい。これなら何とかなりそうである。

5.3.2. $K(z_1, z_2, z_3)$ から L への道のり. (7) を使うと、

$$\begin{aligned} x_1 + x_2 &= \sqrt{-z_1} \\ x_3 + x_4 &= -\sqrt{-z_1} \\ x_1 + x_3 &= \sqrt{-z_2} \\ x_1 + x_4 &= \sqrt{-z_3} \\ x_2 + x_3 &= -\sqrt{-z_3} \end{aligned}$$

とわかるので、結局

$$\begin{aligned} x_1 &= \frac{1}{2}(\sqrt{-z_1}+\sqrt{-z_2}+\sqrt{-z_3}) \\ x_2 &= \frac{1}{2}(\sqrt{-z_1}-\sqrt{-z_2}-\sqrt{-z_3}) \\ x_3 &= \frac{1}{2}(-\sqrt{-z_1}+\sqrt{-z_2}-\sqrt{-z_3}) \\ x_4 &= \frac{1}{2}(-\sqrt{-z_1}-\sqrt{-z_2}+\sqrt{-z_3}) \end{aligned}$$

と書ける。だから、(8) の３次方程式を解けば、所期の４次方程式の解が求まるのである。上の式から、$L = K(x_1, x_2, x_3, x_4) = M(\sqrt{-z_1}, \sqrt{-z_2}, \sqrt{-z_3})$ とわかるが、

$$\begin{aligned} &(x_1+x_2)(x_1+x_3)(x_1+x_4) \\ &= x_1^2(x_1+x_2+x_3+x_4) + \sum_{i<j<k} x_i x_j x_k = \sum_{i<j<k} x_i x_j x_k = -q \end{aligned}$$

だから、

$$\sqrt{-z_1}\cdot\sqrt{-z_2}\cdot\sqrt{-z_3} = -q$$

を満たしていなければならない。従って、

$$\sqrt{-z_3} = -\frac{q}{\sqrt{-z_1}\sqrt{-z_2}} \in M(\sqrt{-z_1}, \sqrt{-z_2})$$

となり、結局

$$K \subset M = K(z_1, z_2, z_3) \subset L = M(\sqrt{-z_1}, \sqrt{-z_2})$$

なる拡大を考えればよい。M の高々４次の拡大体として得られる L とは、具体的には M の $\sqrt{-z_1}, \sqrt{-z_2}$ を付け加えることによって作れることが分かった。

5.3.3. 対称式と基本対称式. 前節にて、x_1, x_2, x_3, x_3 の式に対する４次対称群 $\mathfrak{S}_4$ の作用を考えたが、この考え方は代数学では頻繁に使われるので、一般的な形で述べておこう。

n 変数の任意の多項式 $f(x_1, \ldots, x_n)$ に対して、n 次対称群 $\mathfrak{S}_n$ の作用を次のように定義する：$\sigma \in \mathfrak{S}_n$ に対して、

$$\sigma f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

このとき、$\sigma f(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$ ならば f は「**対称式** *(symmmetric polynomial)*」であるという。

定理 71. 任意の対称式は、基本対称式

$$s_k = \sum_{1\le i_1<\cdots<i_k\le} x_{i_1}\cdots x_{i_k} \quad (k = 1, \ldots, n)$$

の多項式として表せる。すなわち、(変数 $y_1, \ldots, y_n$ に関する) 適当な多項式 $G(y_1, \ldots, y_n)$ が存在して

$$f(x_1, \ldots, x_n) = G(s_1, \ldots, x_n)$$

とかける。

Proof. 環・体論 I で習え。 □

例 72 (対称式)**.** *3* 変数 x, y, z の多項式として、$f(x,y,z) = x^2 + y^2 + z^2$ は対称式だが、これは基本対称式の式として

$$f(x,y,z) = s_1^2 - 2s_2, \quad s_1 = x + y + z,\ s_2 = xy + yz + xz$$

とかける。すなわち、$G(y_1, y_2) = y_1^2 - 2y_2$ とすればよい。

5.3.4. 3 次方程式 (8) の決定. 最後に 3 次方程式 (8) の具体的な形を決定しよう。それには b_1, b_2, b_3 の値がわかればよい。

$$\begin{aligned}
b_1 &= z_1 + z_2 + z_3 = 2\sum_{i<j} x_i x_j \\
b_2 &= z_1 z_2 + z_2 z_3 + z_1 z_3 = \sum_{i<j} x_i x_j + 3\sum_{j<j} x_i^2 x_j x_k + 6x_1 x_2 x_3 x_4 \\
b_3 &= z_1 z_2 z_2 = \sum_{i,j,k} x_i^3 x_j^2 x_k + 2\sum_{i<j<k} x_i^3 x_j x_k x_\ell + 2\sum_{i<j<k} x_i^2 x_j^2 x_k^2 + 4\sum_{i<j,\ k<\ell} x_i^2 x_j^2 x_k x_\ell
\end{aligned}$$

となる。

演習問題 11. この計算を確かめよ。

これらは $\mathfrak{S}_4$ の作用で不変だから、以下の定理 71 により、基本対称式

$$\begin{aligned}
\sigma_1 &= x_1 + x_2 + x_3 + x_4 = 0 \\
\sigma_2 &= \sum_{i<j} x_i x_j = p \\
\sigma_3 &= \sum_{i<j<k} x_i x_j x_k = -q \\
\sigma_4 &= x_1 x_2 x_3 x_4 = r
\end{aligned}$$

を使って書き表すことができる。

実際にそれを計算すると

$$\begin{aligned}
b_1 &= 2\sigma_2 = 2p \\
b_2 &= \sigma_2^2 + \sigma_1\sigma_3 - 4\sigma_4 = p^2 - 4r \\
b_3 &= \sigma_1\sigma_2\sigma_3 - \sigma_1^2\sigma_4 - \sigma_3^2 = -q^2
\end{aligned}$$

となる。

演習問題 12. この計算を確かめよ。

よって方程式 (8) は

$$z^3 - 2pz^2 + (p^2 - 4r)z + q^2 = 0$$

となる。

6. 4次対称群 $\mathfrak{S}_4$ とその構造

ここでは、4次方程式論で活躍した4次対称群 $\mathfrak{S}_4$ を詳しく調べることにより、3次対称群 $\mathfrak{S}_3$ のときよりもさらに詳しい群論の理論を学ぶ。

6.1. **対称群の元の表記法.** $\mathfrak{S}_4$ は位数が 24 とかなり多いので、$\mathfrak{S}_3$ の時のような表記よりも簡略なものが求められる。そこでいくつかの簡略表記法を導入しよう。

定義 73 (互換)**.** $\sigma \in \mathfrak{S}_n$ が、$i, j \in \{1, \ldots, n\}$ の2つの数字だけを入れ替える時、すなわち

$$\sigma(i) = j, \qquad \sigma(j) = i, \qquad \sigma(k) = k \quad (k \neq i, j)$$

となっているとき、「**互換** (transposition)」と呼び、$\sigma = (ij)$ と略記する。

例 74. 4節の冒頭に示した3次対称群 $\mathfrak{S}_3$ において、$\sigma = (12)$, $\tau = (13)$, $\tau\sigma\tau = \sigma\tau\sigma = (23)$ は互換である。

定義 75 (巡回置換)**.** $\sigma \in \mathfrak{S}_n$ が、ある部分集合 $\{i_1, i_2, \ldots, i_k\} \subset \{1, \ldots, n\}$ *($i_1 < i_2 < \cdots < i_k$ であるとは限らない)* の要素を「順繰り」に置き換えるとき、すなわち、

$$\begin{aligned} \sigma(i_j) &= i_{j+1} \quad (1 \leq j < k), \\ \sigma(i_k) &= i_1, \\ \sigma(j) &= j \quad (j \in \{1, 2, \ldots, n\} - \{i_1, i_2, \ldots, \imath_k\}) \end{aligned}$$

なるとき、σ を「**(長さ k の) 巡回置換** (cyclic permutation, k-cycle)」と呼び、$\sigma = (i_1\ i_2\ \ldots,\ i_k)$ と略記する。互換は長さ2の巡回置換であることに注意。

例 76. 4節の冒頭に示した3次対称群 $\mathfrak{S}_3$ において、$\sigma\tau = (132)(= (213) = (321))$ と $\tau\sigma = (123)(= (231) = (312))$ は長さ3の巡回置換である。

命題 77. 任意の巡回置換は互換の積に書ける。

Proof. 実際、

$$\sigma = (i_1\ i_2\ \ldots,\ i_{k-1}\ i_k) = (i_1\ i_k)(i_1\ i_{k-1}) \cdots (i_1\ i_2)$$

とすればよい。 □

例 78. 長さ3の巡回置換 $\sigma = (142) \in \mathfrak{S}_4$ は、

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

の略記であり、互換の積

$$\sigma = (12)(14)$$

と書ける。実際、

$$(12)(14) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

となる。

注意 79. 互換の積として書き表す方法は、ただ一つとは限らず、一般には何通りもある。命題 77 は一つの方法示したにすぎない。例えば

$$(12)(23)(34) = (12)(24)(24)(23)(34) = (14)(13)(12).$$

命題 80. 任意の元 $\sigma \in \mathfrak{S}_n$ は巡回置換の (disjoint な) 積として書ける。すなわち、

$$\sigma = (i_1 i_2, \ldots, i_k)(j_1 j_2 \ldots, j_t) \cdots (\cdots)$$

で $\{i_1, i_2, \ldots, i_k\}$, $\{j_1, j_2, \ldots, j_t\}$, *etc.* は互いに交わりが空な集合。従って命題 77 により、対称群の任意の元は互換の積として書き表すことができる。

Proof. $\sigma \in \mathfrak{S}_n$ を任意にとり、$1 \in \{1, 2, \ldots, n\}$ に繰り返し作用させる:$\sigma(1), \sigma^2(1), \sigma^3(1), \ldots$. これらは全て $\{1, 2, \ldots, n\}$ の要素だから、いつかは $\sigma^p(1) = 1$ となる自然数 p が現れる。そこで、この数列を $i_1, i_2, i_3, \ldots, i_{p-1}$ とおくと、巡回置換 $(i_1 i_2 i_3 \ldots i_{p-1})$ が作れる。もし $p - 1 < n$ ならば $\{1, \ldots, n\} - \{i_1, i_2, i_3, \ldots, i_{p^1}\}$ から適当な数 j を一つとって、今度は $\sigma(j), \sigma^2(j), \sigma^3(j), \ldots$ なる数列を作って同様の考察をする。これを繰り返せば命題の主張を得る。 □

例 81. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix} \in \mathfrak{S}_5$ を考えよう。

$$\sigma(1) = 4, \quad \sigma^2(1) = \sigma(4) = 3, \quad \sigma^3(1) = \sigma(3) = 1$$

だから、まず巡回置換 (143) が現れた。次に $2 \in \{1, 2, 3, 4, 5\} - \{1, 4, 3\}$ を考えると、

$$\sigma(2) = 5, \quad \sigma^2(2) = \sigma(5) = 2$$

だから、巡回置換 (25) が現れた。これで $\{1, 2, 3, 5\}$ の数字は全て尽くされた。よって

$$\sigma = (143)(25) = (25)(143) = (25)(13)(14)$$

となる。

例 82 (4 次対称群 $\mathfrak{S}_4$)**.** 4 次対称群の *24* 個の要素は以下の通り：

単位元 $\cdots$	1,
互換 $\cdots$	$(12), (13), (14), (23), (24), (34)$,
disjoint な互換 2 つの積 $\cdots$	$(12)(34), (13)(24), (14)(23)$,
長さ 3 の巡回置換 $\cdots$	$(123), (124), (132), (134), (142), (143), (234), (243)$,
長さ 4 の巡回置換 $\cdots$	$(1234), (1243), (1324), (1342), (1423), (1432)$

演習問題 13. 例 82 の各要素を $\begin{pmatrix} 1 & 2 & 3 & 4 \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix}$ 型の表記や、互換の積で書き表してみよ。

6.2. **群の準同型写像と同型写像.** 数学の中で写像は、2 つの集合を比較するために使われる。例えば、集合の間に全単射写像が作れれば、2 つの集合の濃度が等しいこと、すなわち、集合としての大きさの比較ができる。数学では、単なる集合ではなく、集合にさらに何らかの「構造」を付け加えたものを考える。例えば、要素同士の和やスカラー積の構造（線形構造）を与えれば線形空間になる。2 つの線形空間を比較するために、線形写像を考えた。あるいは、集合の要素の間に「遠い・近い」を表す距離の概念を考え、それを一般化した構造（位相構造）を考えたとき、2

つの位相空間を比較する写像のことを連続写像と呼んだ。今われわれは、集合に１個の演算の構造を付け加えた群を考えている。２つの群の構造を比較するための写像が以下で定義する準同型写像である。

定義 83 ((準) 同型写像)**.** ２つの群 $(G,\cdot)$, $(H,*)$ の間の写像 $f:G\to H$ が「**準同型写像** (homomorphism)」であるとは、群構造が保存されること、すなわち

$$f(x\cdot y)=f(x)*f(y)\quad (x,y\in G)$$

が成り立つ場合をいう。また、準同型写像 f が全単射の場合、f は「**同型写像** (isomorphism)」であるといい、この時、G と H は「**同 型** (isomorphic)」であるといい、$G\cong H$ と書く。

命題 84. 群 $(G,\cdot,1_G)$ と $(H,*,1_H)$ の間準同型 $f:G\longrightarrow H$ に対し、
(i) $f(1_G)=1_H$,
(ii) 任意の $x\in G$ に対し $f(x^{-1})=f(x)^{-1}$.

Proof. (i) の証明： $f(1_G)=f(1_G\cdot 1_G)=f(1_G)*f(1_G)$. 従って、

$$\begin{aligned}1_H &= f(1_G)*f(1_G)^{-1}=(f(1_G)*f(1_G))*f(1_G)^{-1}\\ &= f(1_G)*(f(1_G)*f(1_G)^{-1})\quad (\text{結合律})\\ &= f(1_G)*1_H\\ &= f(1_G)\end{aligned}$$

(ii) の証明：任意の $x\in G$ に対して、(i) を使って

$$1_H=f(1_G)=f(x\cdot x^{-1})=f(x)*f(x^{-1})$$

だから、両辺に左から $f(x)^{-1}$ を作用させれば

$$\begin{aligned}f(x)^{-1} &= f(x)^{-1}*1_H=f(x)^{-1}*(f(x)*f(x^{-1}))\\ &= (f(x)^{-1}*f(x))*f(x^{-1})\quad (\text{結合律})\\ &= 1_H*f(x^{-1})=f(x^{-1}).\end{aligned}$$

□

また次の性質は極めて基本的で、良く使われる。

命題 85. 群の準同型写像 $f:G\longrightarrow H$ と部分群 $K\subset H$ に対して、
(i) K の f による逆像 $f^{-1}(K)=\{x\in G\mid f(x)\in K\}$ は G の部分群である。
(ii) f の像 $f(G)=\{f(x)\mid x\in G\}$ は H の部分群である。

Proof. (i): $f^{-1}(K)$ が部分群であることを示すには命題 33 より「$x,y\in f^{-1}(K)$ ならば $x\cdot y^{-1}\in f^{-1}(K)$」となることを示せばよい。実際、$y\in f^{-1}(K)$ ならば $f(y)\in K$ だが、K が部分群ゆえ $f(y)^{-1}\in K$. 命題 84 より $f(y^{-1})=f(y)^{-1}\in K$. よって $y^{-1}\in f^{-1}(K)$. さらに $x\in f^{-1}(K)$ なら $f(x)\in K$ だから、$f(x\cdot y^{-1})=f(x)\cdot f(y^{-1})\in K$. よって $x\cdot y^{-1}\in f^{-1}(K)$ を得る。

(ii) は (i) と同様に「$f(x), f(y) \in f(G)$, $x, y \in G$, ならば $f(x) \cdot f(y)^{-1} \in f(G)$」を確かめればよい。実際、$f(y)$, $y \in G$, に対して命題 84 より $f(y)^{-1} = f(y^{-1}) \in f(G)$ だから、$f(x) \cdot f(y)^{-1} = f(x) \cdot f(y^{-1}) = f(x \cdot y^{-1}) \in f(G)$. □

6.3. **４次対称群の部分群.** $\sharp\mathfrak{S}_4 = 24$ だから、Lagrange の公式 (系 50) より、部分群 H の位数は 24 の約数である $1, 2, 3, 4, 6, 8, 12, 24$ のいずれかである。位数 1 は $H = \{1\}$, 位数 24 は $H = \mathfrak{S}_4$ だから、あとは $2, 3, 4, 6, 8, 12$ の場合を考えれば良い。

6.3.1. 位数 *2* の部分群. (disjoint な) 互換で生成される巡回群である。すなわち、

$$\langle(12)\rangle, \langle(13)\rangle, \langle(14)\rangle, \langle(23)\rangle, \langle(24)\rangle, \langle(34)\rangle, \langle(12)(34)\rangle, \langle(13)(24)\rangle, \langle(14)(23)\rangle$$

の９個ある。

6.3.2. 位数 *3* の部分群. 長さ 3 の巡回置換で生成される巡回群である。すなわち、

$$\langle(123)\rangle, \langle(124)\rangle, \langle(132)\rangle, \langle(134)\rangle, \langle(142)\rangle, \langle(143)\rangle, \langle(234)\rangle, \langle(243)\rangle$$

の８個あるかのように見えるが、実際は

$$(234)^2 = (243), \quad (134)^2 = (143), \quad (124)^2 = (142), \quad (123)^2 = (132)$$

となっている。

演習問題 14. このことを確かめよ。

従って

$$\begin{aligned} D_1 &= \langle(234)\rangle = \{1, (234), (243)\}, \\ D_2 &= \langle(134)\rangle = \{1, (134), (143)\}, \\ D_3 &= \langle(124)\rangle = \{1, (124), (142)\}, \\ D_4 &= \langle(123)\rangle = \{1, (123), (132)\} \end{aligned}$$

の４個。

6.3.3. 位数 *4* の部分群. まず、長さ４の巡回置換で生成される巡回群が考えらえる。

$$\begin{aligned} (1234)^2 &= (13)(24), \quad (1234)^3 = (1432), \quad (1234)^4 = 1 \\ (1342)^2 &= (14)(23), \quad (1342)^3 = (1243), \quad (1342)^4 = 1 \\ (1423)^2 &= (12)(34), \quad (1423)^3 = (1324), \quad (1423)^4 = 1 \end{aligned}$$

となっている。

演習問題 15. このことを確かめよ。

従って

$$\begin{aligned} Z_1 &= \langle(1234)\rangle = \{1, (1234), (13)(24), (1432)\} \\ Z_2 &= \langle(1342)\rangle = \{1, (1342), (14)(23), (1243)\} \\ Z_3 &= \langle(1423)\rangle = \{1, (1423), (12)(34), (1324)\} \end{aligned}$$

演習問題 16. $Z_1 = \langle(1432)\rangle$, $Z_2 = \langle(1243)\rangle$, $Z_3 = \langle(1324)\rangle$ であることを確かめよ。また、Z_1, Z_2, Z_3 の部分群を全て求めよ。(ヒント：Z_i, $i = 1, 2, 3,$ の位数は 4 だから、Lagrange の公式 (系 50) より部分群の位数は $1, 2, 4$ のいずれか。位数 2 の部分群は位数 2 の要素からなる巡回部分群になるはず。)

それ以外の部分群として、位数 2 の元 a, b を適当に持ってきて、

$$\langle a, b\rangle = \{1, a, b, ab(= ba)\}$$

の形の部分群が作れる。すなわち、

$$\begin{aligned}
\mathfrak{B}_4 &= \{1, (12)(34), (13)(24), (14)(23)\} \\
V_1 &= \{1, (12), (34), (12)(34)\} \\
V_2 &= \{1, (13), (24), (13)(24)\} \\
V_3 &= \{1, (14), (23), (14)(23)\}
\end{aligned}$$

定義 86 (Klein の 4 元群)**.** 上の $\mathfrak{B}_4$ を「**Klein の 4 元群** (Klein's four group)」と呼ぶ。

以上により、合計 7 個の部分群が存在する。

6.3.4. 位数 *6* の部分群. $i = 1, 2, 3, 4$ に対して

$$C_i = \{\sigma \in \mathfrak{S}_4 \mid \sigma(i) = i\}$$

は $\mathfrak{S}_3$ と同型になるから、位数はちょうど 6 になる。

演習問題 17. このことを確かめよ。(ヒント：例えば、写像 $\varphi : C_1 \to \mathfrak{S}_3$ を、C_1 の各要素 $\sigma \in C_1$ に対して $\tilde{\sigma} = \begin{pmatrix} 1 & 2 & 3 \\ \sigma(2) & \sigma(3) & \sigma(4) \end{pmatrix} \in \mathfrak{S}_3$ を対応させるものと定義すれば、これが同型写像になっている。)

具体的に C_i を計算すると

$$\begin{aligned}
C_1 &= \{1, (23), (24), (34), (234), (243)\} \\
C_2 &= \{1, (13), (14), (34), (134), (143)\} \\
C_3 &= \{1, (12), (14), (24), (124), (142)\} \\
C_4 &= \{1, (12), (13), (23), (123), (132)\}
\end{aligned}$$

演習問題 18. 上の C_i, $i = 1, 2, 3, 4$ はいずれも位数 2 と 3 の元 a, b を適当にとって

$$\langle a, b\rangle = \{1, a, b, b^2, ab, ab^2\}$$

(但し、ba, b^2a, bab etc. は上に現れるいずれかの要素と等しくなる) の形をしていることを確かめよ。(ヒント：どの要素が a でどれが b にあてはまるか、考えてみよ。)

演習問題 19. C_4 は *4* 章の最初に示した $\mathfrak{S}_3$ と全く同じものである。どの要素が $\mathfrak{S}_3$ の $\sigma, \tau, \sigma\tau, \tau\sigma, \tau\sigma\tau$ に相当するかを調べよ。

よって、合計 4 個。他には長さ 6 の巡回置換で生成された巡回部分群が考えられるが、そのようなものは存在しない。

演習問題 20. なぜ $\mathfrak{S}_4$ の元に長さ 6 の巡回置換が存在しないのか？理由を考えよ。(ヒント：巡回置換の定義と $\mathfrak{S}_4$ の定義を見比べる。)

6.3.5. 位数 *8* の部分群. 考えられるパターンとしては、以下のものがある。

C2a: $\langle a, b \mid a^4 = b^2 = 1, ab = ba \rangle$ （アーベル群）
C2b: $\langle a, b \mid a^4 = b^2 = 1, ab = ba^3 \rangle$
C4a: $\langle a, b \mid a^4 = b^4 = 1, a^2 = b^2, ab = ba \rangle$ (アーベル群)
C4b: $\langle a, b \mid a^4 = b^4 = 1, a^2 = b^2, ac = ba^3 \rangle$
K2a: $\langle a, b, c \mid a^2 = b^2 = c^2 = 1, a, b, c \text{ は可換} \rangle$ （アーベル群）
K2b: $\langle a, b, c \mid a^2 = b^2 = c^2 = 1, ab = ba, ac = cb \rangle$
K4a: $\langle a, b, c \mid a^2 = b^2 = c^4 = 1, c^2 = a, a, b, c \text{ は可換} \rangle$ （アーベル群）

しかし $\mathfrak{S}_4$ の部分群として存在するのは、**K2b** 型だけである。ここで **K2b** 型の群の中に Klein の 4 元群 $\mathfrak{B}_4$

$$\mathfrak{B}_4 = \langle a, b \mid a^2 = b^2 = 1,\ ab = ba \rangle = \{1, a, b, ab\}$$

が含まれていることに注意しよう。すなわち $\mathfrak{B}_4$ に新しい元 c を付け加えて位数 8 の部分群が構成されるのである。具体的には、

$$\begin{aligned}
P_1 &= \mathfrak{B}_4 \cup (12)\mathfrak{B}_4 = \mathfrak{B}_4 \cup (34)\mathfrak{B}_4 \\
&= \left\{ \begin{array}{l} 1, (12)(34), (13)(24), (14)(23), \\ (12), (34), (12)(13)(24)(= (1324)), (12)(14)(23)(= (1423)) \end{array} \right\} \\
P_2 &= \mathfrak{B}_4 \cup (13)\mathfrak{B}_4 = \mathfrak{B}_4 \cup (24)\mathfrak{B}_4 \\
&= \left\{ \begin{array}{l} 1, (12)(34), (13)(24), (14)(23), \\ (13), (13)(12)(34)(= (1234)), (24), (13)(14)(23)(= (1432)) \end{array} \right\} \\
P_3 &= \mathfrak{B}_4 \cup (14)\mathfrak{B}_4 = \mathfrak{B}_4 \cup (23)\mathfrak{B}_4 \\
&= \left\{ \begin{array}{l} 1, (12)(34), (13)(24), (14)(23), \\ (14), (14)(12)(34)(= (1243)), (14)(13)(24)(= (1342)), (23) \end{array} \right\}
\end{aligned}$$

の 3 個が存在する。

演習問題 21. P_i, $(i = 1, 2, 3)$ が実際に **K2b** 型になっていることを確かめよ。(ヒント：例えば、$P_1 = \mathfrak{B}_4 \cup (12)\mathfrak{B}_4$ 場合は $a = (13)(24)$, $b = (14)(23)$, $c = (12)$ とおけば、$ab = ba = (12)(34)$, $ac = cb = (1423)$, $bc = ca = (1324)$, $abc = cab = (34)$ となる。$P_1 = \mathfrak{B}_4 \cup (34)\mathfrak{B}_4$ の場合は a, b はそのままで $c = (34)$ と変えてみると **K2b** 型にあてはまるかどうか、ac, cb, bc, ca, abc, cab を実際計算して確かめよ。P_2, P_3 型では a, b のあてはめを変えなければならないが、どうすればよいだろうか？)

6.3.6. 位数 *12* の部分群. 位数 12 の部分群を H とする。各要素 $x \in H$ は巡回部分群を作るから、その位数は Lagrange の公式 (系 50) より、12 の約数である $2, 3, 4, 6, 12$ のいずれかである。$\mathfrak{S}_4$ には位数 $6, 12$ の要素は存在しなかったから (演習問題 20 参照)、結局位数 $2, 3, 4$ の要素の組合せを考える必要がある。

H がアーベル群だとすれば、可能性としては以下のものに限られる。

(1) 位数 3, 4 の要素 a, b で生成されたアーベル群

$$\langle a, b \mid a^3 = b^4 = 1, ab = ba \rangle = \{1, a, a^2, b, b^2, b^3, ab, ab^2, ab^3, a^2b, a^2b^2, a^2b^3\}$$

(2) 位数 2 の要素 a, b, 位数 3 の要素 c で生成されたアーベル群

$$\begin{aligned}&\langle a, b, c \mid a^2 = b^2 = c^3 = 1, ab = ba, ac = ca, bc = cb\rangle\\ =\ &\{1, a, b, c, c^2, ab, ac, ac^2, bc, bc^2, abc, abc^2\}\end{aligned}$$

しかし、そのようなものは存在しない。

演習問題 22. そのことを確かめよ。(ヒント：位数 2,3,4 の要素の間に積の交換法則が成り立つかどうか確かめればよい。例えば、位数 3 の要素は 4 個（とその二乗）で異数 4 の要素は 3 個（とその三乗）だったから、合計 12 個の組合せで交換法則を確かめなければならない。)

実際、位数 12 の部分群は次のようなもので、これは「**4 次交代群**」と呼ばれている。Klein の 4 元群に位数 3 の元 c を付け加えた次のような群を考えええよう：

$$\langle a, b, c \mid a^2 = b^2 = c^3 = 1, ab = ba, cb = ac, ca = abc\rangle$$

この中で a, b だけで生成された部分群 $\mathfrak{B}_4 = \langle a, b\rangle$ が Klein の 4 元群であることに注意しよう。そこで例えば

$$a = (12)(34),\ b = (13)(24),\ c = (123)$$

とおいてみれば、

$$\begin{aligned}\mathfrak{A}_4 &= \langle a, b, c\rangle\\ &= \left\{\begin{array}{l}1,\ a = (12)(34),\ b = (13)(24),\ ab = ba = (14)(23),\\ c = (123) = (13)(12),\ c^2 = (132) = (12)(13),\\ ac = cb = (243) = (23)(24),\ ac^2 = (143) = (13)(14),\\ bc = (142) = (12)(14),\ bc^2 = (24)(23),\\ abc = ca = (132) = (12)(13),\ abc^2 = (124) = (14)(12)\end{array}\right\}\end{aligned}$$

すべての要素が互換偶数個の互換の積で書けているところが特徴である（単位元はゼロ個の互換の積と考えれば、やはり偶数個の積)。

演習問題 23. $\mathfrak{S}_4$ の要素で $\mathfrak{A}_4$ に含まれないものは合計１２個ある。これらが互換の偶数個の積では書けないことを確かめよ。（ヒント：命題 80 より、対称群の任意の要素は互換の積として下記表せるが、それは一通りではない。しかし必要となる互換の数が偶数個か奇数個かは個々の要素ごとに決まっている。そのことは命題 98 によって保障される。そこで $\mathfrak{A}_4$ に含まれない１２個の元を適当に互換の積に分解してみて、互換が奇数個使われたことを確認すればよい。）

演習問題 24. 上に示した $\mathfrak{A}_4 = \langle a, b, c\rangle$ に対して

$$\mathfrak{A}_4 = \mathfrak{B}_4 \cup c\mathfrak{B}_4 \cup c^2\mathfrak{B}_4$$

となっていることを確かめよ。(ヒント：$a = (12)(34)$, $b = (13)(24)$, $c = (123)$ を使って計算すればよい。)

後に命題 100 で示されるように、対称群 $\mathfrak{S}_2$ の任意の要素 σ について、それが何個の互換の積で書けるかは（幾通りも書き方があるため）決まらないが、互換の個数が偶数か奇数かは σ を決めれば１つに決まる。

6.4. **４次対称群の正規部分群.** 上で求めた $\mathfrak{S}_4$ の真の部分群のうち、正規部分群になるものは、実は $\mathfrak{B}_4$ (Klein の４元群) と $\mathfrak{A}_4$ (４次交代群) のみである。また、正規部分以外の部分群の間には、ある種の関係がある場合がある。これらのことを見通し良く調べるために、いくつかの概念を導入する。

6.4.1. 準同型写像の核. ２つのベクトル空間 V, W の間の線形写像 $f : V \to W$ に対して、「核」$\operatorname{Ker} f$ とは

$$\operatorname{Ker} f = \{\mathbf{v} \in V \mid f(\mathbf{v}) = \mathbf{0}\}$$

となるような V の部分線形空間で、V, W の次元などを比較する際に重要な役割を果たしていたことを思い出そう。

２つの群の間の準同型写像にも、やはり「核」とう概念を考えることができて、群論では非常に重要な役割を果たす。

定義 87 (準同型写像の核)**.** 群の準同型写像 $f : G \to H$ に対し、G の部分集合

$$\operatorname{Ker} f = \{x \in G \mid f(x) = 1_H\}$$

を f の「**核** (kernel)」と呼ぶ。

命題 84(i) より、どんな準同型写像 $f : G \to H$ に対しても、必ず

$$1_G \in \operatorname{Ker} f$$

が成り立つことに注意しよう。つまり、$\operatorname{Ker} f$ は空ではなく、実は G の正規部分群であり、特に $\{1_G\} = \operatorname{Ker} f$ なる場合は f の単射性を意味する。すなわち、

命題 88. 群 $(G, \cdot, 1_G)$ と $(H, *, 1_H)$ の間の準同型 $f : G \to H$ に対して、
(i) $\operatorname{Ker} f \triangleleft G$ (正規部分群)
(ii) $\operatorname{Ker} f = \{1_G\}$ であることと f が単射であることは同値である。

Proof. (i) の証明：$\{1_H\}$ は H の部分群で $\operatorname{Ker} f$ はその逆像だから命題 85(i) により G の部分群である。次に正規部分群であることを示すには、任意の $x \in G$ に対して $x \cdot \operatorname{Ker} f \cdot x^{-1} = \operatorname{Ker} f$ であることを言えばよい。実際、任意の $y \in \operatorname{Ker} f$ に対して、

$$\begin{aligned} f(xyx^{-1}) &= f(x) * f(y) * f(x^{-1}) \\ &= f(x) * f(y) * f(x)^{-1} \quad (\text{命題 84(ii) による}) \\ &= f(x) * 1_H * f(x)^{-1} \quad (y \in \operatorname{Ker} f \text{ だから}) \\ &= f(x) * f(x)^{-1} = 1_H \end{aligned}$$

だから、$xyx^{-1} \in \operatorname{Ker} fF$. よって ($y \in \operatorname{Ker} f$ を任意に動かすことにより)

$$x \cdot \operatorname{Ker} f \cdot x^{-1} \subseteq \operatorname{Ker} f$$

とわかる。逆に、

$$\operatorname{Ker} f \ni y = 1_G \cdot y \cdot 1_G = (x \cdot x^{-1}) \cdot y \cdot (x \cdot x^{-1}) = x \cdot (x^{-1} \cdot y \cdot x) \cdot x^{-1}$$

で、上と同様にして $x^{-1} \cdot y \cdot x \in \operatorname{Ker} f$ だから、結局 $y \in x \cdot \operatorname{Ker} f \cdot x^{-1}$ となるから、

$$x \cdot \operatorname{Ker} f \cdot x^{-1} \supseteq \operatorname{Ker} f$$

とわかる。よって $x \cdot \operatorname{Ker} f \cdot x^{-1} = \operatorname{Ker} f$.

(ii) の証明：まず $\mathrm{Ker}\, f = \{1_G\}$ として f が単射であることを示そう。$x, y \in G$ に対して $f(x) = f(y)$ であるとする。このとき命題 84(ii) より

$$1_H = f(x) * f(y)^{-1} = f(x) * f(y^{-1}) = f(x \cdot y^{-1})$$

となるから、$x \cdot y^{-1} \in \mathrm{Ker}\, f = \{1_G\}$. 従って、$x \cdot y^{-1} = 1_G$ から $x = y$ を得る。すなわち f は単射である。逆に f が単射であると仮定しよう。$x \in \mathrm{Ker}\, f$ を任意にとると、$f(x) = 1_H$. 一方、命題 84(i) より $f(1_G) = 1_H$. よって f の単射性より $x = 1_G$ でなければならない。すなわち $\mathrm{Ker}\, f = \{1_G\}$. □

準同型写像の最も重要な例は、次の**自然準同型写像** (natural homomorphism または natural surjection) で、代数学の中で頻繁に使われる概念である。

命題 89. 群 G とその正規部分群 $N \triangleleft G$ に対して、写像

$$\varphi : G \to G/N, \quad x \longmapsto xN$$

は群の全射準同型写像になっている。また、$\mathrm{Ker}\, \varphi = N$ となる。

Proof. $x, y \in G$ に対して $\varphi(xy) = xyN$. 一方、$N \triangleleft G$ であることより、$\varphi(x) \cdot \varphi(y) = (xN)(yN) = x(Ny)N = x(yN)N = x \cdot yN$ となるから、結局 $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$ となり、φ は準同型である。 □

よく使われる自然準同型として、群 G とその正規部分群 $H \triangleleft G$, $K \triangleleft G$, $K \subset H$ に対し、

$$\varphi : G/K \longrightarrow (G/K)/(H/K)$$

というものがある。これは $(H/K) \triangleleft (G/K)$ であることから、命題 89 によって構成される。すなわち、

補題 90. 群 G とその正規部分群 $H \triangleleft G$, $K \triangleleft G$, $K \subset H$ に対し、

$$(H/K) \triangleleft (G/K)$$

である。

Proof. $K \triangleleft H$ だから（証明：$K \triangleleft G$ ゆえ、任意の $g \in G$ に対して $gKg^{-1} = K$. 特に $g \in H(\subset G)$ をとることにより、$K \triangleleft H$ を得る）、剰余群 H/K を考えることができる。そこで

$$\psi : H/K \longrightarrow G/K, \quad hK \longmapsto hK$$

なる写像を考える。ここで、$H \subset G$ であることから、ψ で写す前の hK における h は H の元と考え、ψ の像 hK における h は G の元と考えている。

この時、$1_{G/K} = 1_G K = K = 1_H K = 1_{H/K}$ であることに注意して、

$$\begin{aligned} \mathrm{Ker}\, \psi &= \{hK \mid \psi(hK) = 1_{G/K}\} = \{hK \mid \psi(hK) = K\} \\ &= \{hK \mid hK = K\} \\ &= \{hK \mid h \in K\} (\text{補題 45 より}) \\ &= K = 1_{H/K} \end{aligned}$$

となるから、命題 88 より ψ は単射となり、これによって

$$H/K \subset G/K$$

とみなせる。さらに、$(H/K) \triangleleft (G/K)$ であることを示そう。任意の $gK \in (G/K)$ に対して、$K \triangleleft G$ $H \triangleleft G$, $K \triangleleft H$ であることを使って、

$$\begin{aligned} & gK \cdot (hK) \cdot g^{-1}K \\ = \;& Kg \cdot (hK) \cdot g^{-1}K = K(gh)K \cdot g^{-1}K \\ = \;& K(h'g)K \cdot g^{-1}K \quad (H \triangleleft G \text{ ゆえ、} ghg^{-1} = h' \text{ となる } h' \in H \text{ が存在する}) \\ = \;& Kh'(gKg^{-1})K = Kh'KK = Kh'K = h'KK \\ = \;& h'K \in H/K \end{aligned}$$

だから、$gK(H/K)g^{-1}K \subset H/K$. 従って $(H/K) \triangleleft (G/K)$ となる。 □

さらに、次の結果は基本的である。

命題 91. 群 G とその正規部分群 $H \triangleleft G$, $K \triangleleft G$, $K \subset H$ に対し、

$$(G/K)/(H/K) \cong G/H.$$

Proof. 対応 $\varepsilon : (G/K)/(H/K) \to G/H$ を

$$(G/K)/(H/K) \ni \bar{a} := (aK)(H/K) \mapsto aH \in G/H$$

と定義する。まずこれが写像として well-defined であること、すなわち、$(G/K)/(H/K)$ の同じ元の異なる表現 $\bar{a} = \bar{b}$ に対して、ε がただ一つの値を決めること（$\varepsilon(\bar{a}) = \varepsilon(\bar{b})$）を示そう。$\bar{a} = \bar{b}$, すなわち $(aK)(H/K) = (bK)(H/K)$ (in H/K) であることから、$(aK)(bK)^{-1} \subset K$. つまり $ab^{-1}K \subset K$ だから $ab^{-1} \in K \subset H$. よって $a \in bH$ となり、これより $aH = bH$ となり $\varepsilon(\bar{a}) = \varepsilon(\bar{b})$ を得る。ε が準同型写像であることは、

$$\begin{aligned} \varepsilon(\bar{a} \cdot \bar{b}) &= \varepsilon((aK)(H/K) \cdot (bK)(H/K)) = \varepsilon((abK)(H/K)) \\ &= abH = (aH) \cdot (bH) = \varepsilon(\bar{a}) \cdot \varepsilon(\bar{b}) \end{aligned}$$

よりわかる。さらに、任意の $aH \in G/H$ に対して $\varepsilon(\bar{a}) = aH$ となるから、ε は全射準同型である。ε の核を計算すると

$$\begin{aligned} \operatorname{Ker}\varepsilon &= \{\bar{a} \mid \varepsilon(\bar{a} = 1_{G/H})\} = \{\bar{a} \mid aH \subset H\} = \{\bar{a} \mid a \in H\} \\ &= \{(aK)(H/K) \mid a \in H\} = \{(H/K) \mid a \in H\} \\ &= \{1_{(G/K)/(H/K)}\} \end{aligned}$$

となるから、命題 88 より ε は単射でもあり、結局群の同型写像とわかる。 □

命題 91 より直ちに以下を得る。

系 92. 群 G の $K \subset H$ なる 2 つの正規部分群 K, H に対して、

$$\varphi : G/K \longrightarrow G/H$$

なる自然準同型がつくれる。

6.4.2. 部分群の共役. 正規部分群でない部分群は、以下に示すような「共役」という関係にある場合がある。

定義 93 (共役)**.** 群 G の任意の要素 $g \in G$ と任意の部分群 $H \subset G$ に対し、部分集合（後述するように、これは実は部分群になる）$gHg^{-1}(\subset G)$ のことを H の「**共役** (conjugate)」と呼ぶ。また、$h, h' \in G$ が「**共役**」(conjugate) であるとは、適当な $g \in G$ によって $gHg^{-1} = h'$ となる場合をいう。

共役部分群を作り出す同型写像は、群論では一般によく使われる。

命題 94. 群 G の任意の部分群 H とその共役の間には同型写像が存在する:$H \cong gHg^{-1}$ $(g \in G)$. 特に、共役 gHg^{-1} は G の部分群である。

Proof. $g \in G$ に対して次のような写像 ψ を考えると、これは同型写像になっている。

$$\begin{array}{rccc} \psi: & H & \longrightarrow & gHg^{-1} \\ & x & \longmapsto & gxg^{-1} \end{array}$$

実際、$\psi(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = \psi(x)\psi(y)$ となるから、ψ は準同型写像である。そこで ψ の核を計算してみよう。$x \in \mathrm{Ker}\,\psi$ とすると $1_G = \psi(x) = gxg^{-1}$ となるから、両辺に左右から g^{-1} および g を掛ければ $x = g^{-1}g = 1_G$ を得る。すなわち $\mathrm{Ker}\,\psi = \{1_G\}$ となり、命題 88 より ψ は単射。最後に、任意の元 $a \in gHg^{-1}$ をとると、gHg^{-1} の定義により、$a = gxg^{-1}$, $x \in H$, と書き表せる。すると $\psi(x) = a$ となり、ψ は全射となる。以上により、ψ は全単射な準同型だから同型写像であり、従って $H \cong gHg^{-1}$ となる。最後の主張は、命題 85(ii) による。 □

系 95. 正規部分群 $H \triangleleft G$ と任意の $g \in G$ に対して、共役写像

$$\begin{array}{rccc} \psi: & H & \longrightarrow & H \\ & x & \longmapsto & gxg^{-1} \end{array}$$

は自分自身から自身への同型写像（**自己同型写像**とよぶ）になっている。

Proof. $H \triangleleft G$ だから $gHg^{-1} = H$ になることに注意すれば、命題 94 の証明から直ちにわかる。 □

6.4.3. $\mathfrak{S}_4$ の共役部分群. $\mathfrak{S}_4$ の正規でない部分群に対して、それらの共役関係を調べてみよう。

命題 96. $\mathfrak{S}_4$ において

(*i*) 位数 *8* の部分群 P_1, P_2, P_3 は互いに共役である。

(*ii*) 位数 *3* の部分群 D_1, D_2, D_3, D_4 は互いに共役である。

従って、とくにこれらの部分群は正規部分群ではない。

Proof. P_i, D_j はそれぞれ 2-Sylow 群、3-Sylow 群と呼ばれる特殊なタイプの部分群で、Sylow 群の一般理論（後述の 12 章参照）により互いに共役なことが分かる。 □

演習問題 25. 位数 *6* の部分群 C_1, C_2, C_3, C_4 が互いに共役であることを示せ。(ヒント：簡単な計算によって $(1i)C_1(1i) = C_i$, $i = 2, 3, 4$, であることが確かめらえる。)

演習問題 26. 位数 4 の部分群 Z_1, Z_2, Z_3 （４次巡回部分群）が互いに共役であることを示せ。(ヒント：$(12)Z_1(12) = Z_2$, $(14)Z_1(14) = Z_3$ であることを確かめよ。)

演習問題 27. 位数 4 の部分群 V_1, V_2, V_3 （*Klein* の４元群以外の $\langle a, b \mid a^2 = b^2 = 1, ab = ba\rangle$ 型アーベル部分群）が互いに共役であることを示せ。(ヒント:$(13)V_1(13) = V_3$, $(12)V_3(12) = V_2$ であることを確かめよ。)

演習問題 28. 任意の $i = 1, 2, 3$, $j = 2, 3, 4$ に対して Z_i と V_j は決して共役にならない。このことを実際に計算せずに示せ。(ヒント：共役ならば同型のはずである。しかし Z_i には位数 4 の元があるが、V_j には位数 4 の元は含まれていない。そのことが同型写像の存在と矛盾することを見ればよい。)

演習問題 29. 位数 2 の部分群 $\langle(12)\rangle, \langle(13)\rangle, \langle(14)\rangle, \langle(23)\rangle, \langle(24)\rangle, \langle(34)\rangle$ は互いに共役であることを示せ。(ヒント：例えば、$(23)(12)(23) = (13)$, $(24)(12)(24) = (14)$, $(13)(12)(13) = (23)$, $(14)(12)(14) = (24)$, $(13)(14)(13) = (34)$ であることを確かめよ。)

演習問題 30. 位数 2 の部分群 $\langle(12)(34)\rangle, \langle(13)(24)\rangle, \langle(14)(23)\rangle$ は互いに共役であることを示せ。(ヒント:例えば、$(13)\underline{(14)(23)}(13) = \underline{(12)(34)}$, $(12)\underline{(14)(23)}(12) = \underline{(13)(24)}$ であることを確かめよ。)

疑問 1. 同じ位数 2 の部分群なのに、演習 29 で扱った部分群と演習 30 で扱った部分群は、決して共役にはならない。それは何故か？(注意 101 参照)

6.4.4. $\mathfrak{S}_4$ の正規部分群. 残る、$\mathfrak{B}_4$ (Klein の４元群) と $\mathfrak{A}_4$ (４次交代群) が正規部分群になるが、全ての共役が自分自身と一致すること (命題 94 参照) を直接計算で確かめるかわりに、もっと見通しの良い別の方法を考えよう。

定義 97. n 次対称群の任意の元 $\sigma \in \mathfrak{S}_n$ に対して、

$$\operatorname{sgn}\sigma = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j}$$

とおく。これは 1 または -1 をとる。$\operatorname{sgn}\sigma = 1$ の場合 σ は「**偶置換** (even permutation)」と呼ばれ、$\operatorname{sgn}\sigma = -1$ の場合 σ は「**奇置換** (odd permutation)」と呼ばれる。

命題 98. 集合 $\{1, -1\}$ は、整数の掛け算を演算とし 1 を単位元とする位数 2 のアーベル群であり、写像

$$\begin{array}{rccc} \operatorname{sgn}: & \mathfrak{S}_n & \longrightarrow & \{1, -1\} \\ & \sigma & \longmapsto & \operatorname{sgn}\sigma \end{array}$$

は群の全射準同型である。

Proof. 準同型写像であることだけ示せばよい。それは以下の計算によりわかる：

$$\begin{aligned} \operatorname{sgn}\sigma\tau &= \prod_{i<j} \frac{\sigma\circ\tau(i) - \sigma\circ\tau(j)}{i - j} \\ &= \prod_{i<j} \frac{\sigma\circ\tau(i) - \sigma\circ\tau(j)}{\tau(i) - \tau(j)} \cdot \frac{\tau(i) - \tau(j)}{i - j} \\ &= (\operatorname{sgn}\sigma) \cdot (\operatorname{sgn}\tau) \end{aligned}$$

□

$\mathfrak{A}_4$ が $\mathfrak{S}_4$ の正規部分群であることは、次の一般的事実からしたがう。（演習 23 参照）

定義 99 (交代群)**.** n 次対称群 $\mathfrak{A}_n$ の要素で偶数個の互換の積で書けるもの（単位元は 0 個の互換の積と考える）を全て集めた部分集合 $\mathfrak{A}_n$ を「n **次交代群** (alternative group)」と呼ぶ。

演習問題 31. 例 59 で考察した $\mathfrak{A}_3$ は、上の定義のものと一致することを確かめよ。(ヒント：$\mathfrak{A}_3$ の全ての要素が偶数個の互換の積であり、$\mathfrak{A}_3$ に入っていない $\mathfrak{G}_3$ の要素が奇数個の互換の積であることを確かめよ。あるいは、次の命題 100 を参考に sgn 関数の値を計算してもよい。)

命題 100. $\mathfrak{A}_n = \mathrm{Ker}(\mathrm{sgn}) = \{\sigma \in \mathfrak{S}_n \mid \mathrm{sgn}\,\sigma = 1\}$. 従って、命題 *88* より $\mathfrak{A}_n \triangleleft \mathfrak{S}_n$ である。

Proof. sgn の定義より、σ が偶数個の互換の積ならば $\mathrm{sgn}(\sigma) = 1$ となり、奇数個の互換の積なら $\mathrm{sgn}(\sigma) = -1$ となることがわかる。従って、$\mathrm{Ker}(\mathrm{sgn}) = \mathfrak{A}_n$ となる。 □

注意 101 (疑問 1 の答)**.** 演習 30 で扱った部分群の *(*単位元以外の*)* 要素は全て互換 2 つの積。従って、これらは全て $\mathfrak{A}_4$ の部分群である。ところが、$\mathfrak{A}_4$ は正規部分群だから、結局演習 *30* で扱った部分群の共役は $\mathfrak{A}_4$ の部分群に限られる。一方、演習 29 で扱った部分群の（単位元以外の）要素は全て互換 1 つで成り立っているから、$\mathfrak{A}_4$ には含まれない。よってこれらは演習 30 で扱った部分群の共役にはなりえない。

次に、$\mathfrak{B}_4 \triangleleft \mathfrak{S}_4$ を示そう。

命題 102. 長さ k の巡回置換 $\pi = (i_1\ i_2\ \ldots\ i_k)$ と、任意の $\sigma \in \mathfrak{S}_n$ に対して、

$$\sigma\pi\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \ldots,\ \sigma(i_k))$$

Proof. 任意の $j \in \{1, \ldots, n\}$ をとると、

$$\sigma\pi\sigma^{-1}(j) = (\sigma \circ \pi)(\sigma^{-1}(j)).$$

もし $\sigma^{-1}(j) \notin \{i_1\ i_2\ \ldots\ i_k\}$, すなわち、$j \notin \{\sigma(i_1)\ \sigma(i_2)\ \ldots\ \sigma(i_k)\}$ ならば、これは π によって不変だから $(\sigma \circ \pi)(\sigma^{-1}(j)) = \sigma(\sigma^{-1}(j) = j$ となり、結局

$$\sigma\pi\sigma^{-1}(j) = j \quad (j \notin \{\sigma(i_1)\ \sigma(i_2)\ \ldots\ \sigma(i_k)\}\sigma(i_k)\} \text{ のとき.}) \tag{9}$$

次に、もし $\sigma^{-1}(j) \in \{i_1\ i_2\ \ldots\ i_k\}$, すなわち、$j \in \{\sigma(i_1)\ \sigma(i_2)\ \ldots\ \sigma(i_k)\}$ ならば、$j = \sigma(i_p)$ $(1 \leq p \leq k)$ の形で書け、

$$(\sigma \circ \pi)(\sigma^{-1}(j)) = (\sigma \circ \pi)(i_p) = \sigma(\pi(i_p)) = \sigma(i_{p+1}) \text{ または } p = k \text{ の場合は } \sigma(i_1).$$

すなわち

$$\sigma\pi\sigma^{-1}(\sigma(i_p)) = \sigma(i_{p+1}) \text{ またはは} \sigma(i_1). \tag{10}$$

(9) と (10) は、まさに $\sigma\pi\sigma^{-1}$ が $(\sigma(i_1)\ \sigma(i_2)\ \ldots,\ \sigma(i_k))$ で表される巡回置換であることを意味している。 □

系 103. *Klein* の 4 元群は 4 次対称群の正規部分群である：$\mathfrak{B}_4 \triangleleft \mathfrak{S}_4$.

Proof. $\mathfrak{B}_4 = \{1, (12)(34), (13)(24), (14)(23)\}$ だが、任意の $\sigma \in \mathfrak{S}_4$ に対して、

$$\sigma(12)(34)\sigma^{-1} = (\sigma(12)\sigma^{-1})(\sigma(34)\sigma^{-1}) = (\sigma(1)\sigma(2))(\sigma(3)\sigma(4))$$

σ を動かせば $\sigma(1)\sigma(2)\sigma(3)\sigma(4)$ は $1, 2, 3, 4$ の全ての並べ換えを動くが、互換については $(ij) = (ji)$ であること、$\{i, j\} \cap \{k, l\} = \emptyset$ ならば $(ij)(kl) = (kl)(ij)$ であることに注意すれば、それは $\sigma(12)(34)\sigma^{-1}$ が $\mathfrak{B}_4$ の他の要素を動くことを意味する。$\sigma(13)(24)\sigma^{-1}$, $\sigma(14)(23)\sigma^{-1}$ についても全く同様。よって、任意の $\sigma \in \mathfrak{S}_4$ に対して $\sigma\mathfrak{B}_4\sigma^{-1} = \mathfrak{B}_4$ となる。 □

6.4.5. $\mathfrak{S}_4$ が可解群であること.

演習問題 32. 群 G とその部分群 $H \subset K$ に対し、$H \triangleleft G$ ならば $H \triangleleft K$ であることを示せ。(ヒント：補題 90 の証明をみよ。)

演習問題 33. アーベル群 G の任意の部分群 H に対して、$H \triangleleft G$ であることを示せ。

演習問題 34. クラインの 4 元群 $\mathfrak{B}_4$ はアーベル群であることを確かめよ。

演習 32, 演習 33, 演習 34 を命題 100 と系 103 に適用すれば、正規鎖

$$0 \subset \langle(12)(34)\rangle \subset \mathfrak{B}_4 \subset \mathfrak{A}_4 \subset \mathfrak{S}_4$$

が存在することがわかる。後は剰余群

$$\mathfrak{S}_4/\mathfrak{A}_4, \quad \mathfrak{A}_4/\mathfrak{B}_4, \quad \mathfrak{B}_4/\langle(12)(34)\rangle, \quad \langle(12)(34)\rangle$$

が巡回群であることが言えればよい。しかし、Lagrange の公式 (系 50) より $\sharp\mathfrak{S}_4/\mathfrak{A}_4 = 2$, $\sharp\mathfrak{A}_4/\mathfrak{B}_4 = 3$, $\sharp\mathfrak{B}_4/\langle(12)(34)\rangle = 2$ だから、命題 51 より、いずれも巡回群だとわかる。

以上により、以下が示された。

命題 104. $\mathfrak{S}_4$ は可解群である。

7. 準同型定理

群の準同型 $f : G \to H$ が全射のとき、

$$1 \longrightarrow \operatorname{Ker} f \longrightarrow G \xrightarrow{f} H \longrightarrow 1$$

という風に書き表し、これを「**短完全列** (short exact sequence)」と呼ぶ。(短) 完全列はもっと一般の定義があるが、ここでは単に「全射準同型 f とその核を纏めて図式化して表したもの」と理解しておけばよい。

さて、命題 88 より $\operatorname{Ker} f \triangleleft G$ であり、また、命題 60 より $G/\operatorname{Ker} f$ という剰余群が作れるのであった。では、$G/\operatorname{Ker} f$ と H の間にどんな関係があるのか？答は以下の通りである。

定理 105 (準同型定理)**.** 群の単完全列

$$1 \longrightarrow \operatorname{Ker} f \longrightarrow G \xrightarrow{f} H \longrightarrow 1$$

に対し、同型

$$H \cong G/\operatorname{Ker} f$$

が成り立つ。

Proof. 剰余群 $G/\operatorname{Ker} f = \{x \operatorname{Ker} f \mid x \in G\}$ から H への写像 φ を次のように構成する：

$$\varphi(x \operatorname{Ker} f) = f(x).$$

- φ が well-defined であること: ところが、$G/\operatorname{Ker} f$ の要素は $x \operatorname{Ker} f$ と一意的に表せるわけではなく、異なる $x, y \in G$ に対して $x \operatorname{Ker} f$ と $y \operatorname{Ker} f$ が $G/\operatorname{Ker} f$ の元としては同じものを表すことがある（例えば、補題 45 より任意の $x \in \operatorname{Ker} f$ に対して $x \operatorname{Ker} f = 1_G \operatorname{Ker} f$ となる)。写像とは 1 つの要素に対して 1 つの値を対応させるものだから、$\varphi(g \operatorname{Ker} f)$ の値は x の取り方によらず一定であることを保障しなければならない。しかしそれは実際に保障されている。なぜならば、$x \operatorname{Ker} f = y \operatorname{Ker} f$ だとすると $\operatorname{Ker} f = x^{-1} \cdot y \operatorname{Ker} f$. 従って $1_G \operatorname{Ker} f$ だから、$x^{-1} \cdot y = z$ なる $z \in \operatorname{Ker} f$ が存在する。そこで命題 84 を使って

  $$1_H = f(z) = f(x^{-1}) \cdot y) = f(x^{-1}) * f(y) = f(x)^{-1} * f(y)$$

  となるから、$f(x) = f(y)$ を得る。よって φ の値は $x \operatorname{Ker} f = y \operatorname{Ker} f$ となる x, y の取り方によらず 1 つに決まることが示された（この性質のことを「f **は well-defined である**」と呼ぶ)。
- φ が準同型であること：任意の $x, y \in G$ に対して

$$\begin{aligned}
&\varphi(x \operatorname{Ker} f \cdot y \operatorname{Ker} f) \\
&= \varphi(x \cdot y \operatorname{Ker} f) \quad (\text{正規部分群だから } \operatorname{Ker} f y = y \operatorname{Ker} f) \\
&\qquad (\operatorname{Ker} f \operatorname{Ker} f = \operatorname{Ker} f \text{ であることは補題 45 による}) \\
&= f(x \cdot y) = f(x) * f(y) \\
&= \varphi(x \operatorname{Ker} f) \cdot \varphi(y \operatorname{Ker} f).
\end{aligned}$$

- φ が全射であること：任意の $\alpha \in H$ に対して、$f : G \to H$ が全射であることから適当な $x \in G$ があって $f(x) = \alpha$ となる。そこで $x \operatorname{Ker} f \in G/\operatorname{Ker} f$ をとれば $\varphi(x \operatorname{Ker} f) = f(x) = \alpha$ となるから、φ は全射である。
- φ が単射であること：命題 88 より、$\operatorname{Ker} \varphi = \{1_{G/\operatorname{Ker} f}\}$ であることを言えば良い。$\operatorname{Ker} \varphi \supseteq \{1_{G/\operatorname{Ker} f}\}$ は命題 84 より保障されているから、逆の包含関係を示せば十分である。すなわち、任意の $x \operatorname{Ker} f \in \operatorname{Ker} \varphi$ に対し、$x \operatorname{Ker} f = \operatorname{Ker} f (= 1_{G/\operatorname{Ker} f})$ であることを言えばよい。実際、

$$1_H = \varphi(x \operatorname{Ker} f) = f(x)$$

だから、$x \in \operatorname{Ker} f$. よって補題 45 より $x \operatorname{Ker} f = \operatorname{Ker} f$ となる。

□

8. ５次以上の代数方程式論と５次以上の対称群

8.1. 交換子群と可解群.

定義 106 (交換子群)**.** 群 G の元 $a, b \in G$ に対し、

$$[a, b] = aba^{-1}b^{-1}$$

を a, b の「**交換子**」**(commutator)** と呼ぶ。また、部分群 $H, K \subset G$ に対し、

$$[H, K] = \{[a, b] \mid a \in H,\ b \in K\} \text{ で生成された群}$$

を H, K の「**交換子群**」**(commutator group)** と呼ぶ。特に $[G, G]$ を G の交換子群と呼ぶ。

次の補題は、交換子が可換性を計る尺度であることを表している。

補題 107. $[a, b] = 1_G$ は a, b が可換であること、すなわち $ab = ba$ であることと同値。また、G がアーベル群であることと、交換子群が自明 $[G, G] = \{1\}$ であることは同値。

Proof. $[a, b] = 1_G \Leftrightarrow aba^{-1}b^{-1} = 1_G \Leftrightarrow ab = ba$ より明らか。後半は前半より明らか □

命題 108. 部分群 $H, K \subset G$ に対し、

(i) 交換子群 $[H, K]$ は G の部分群である。
(ii) 剰余群 $G/[G, G]$ はアーベル群である。
(iii) 正規部分群 $L \triangleleft G$ に対して、G/L がアーベル群だとすると、$L \supset [G, G]$.

Proof. (i) 任意の $[a, b] \in [G, G]$ と $g \in G$ に対して

$$g^{-1}[a, b]g = (g^{-1}ag)(g^{-1}bg)(g^{-1}a^{-1}g)(g^{-1}b^{-1}g) = [g^{-1}ag, g^{-1}bg] \in [G, G]$$

だから、$g^{-1}[G, G]g \subset [G, G]$. これより $[G, G] \triangleleft G$ とわかる。

(ii) 剰余群 $G/[G, G]$ の任意の元 $\bar{a} := a[G, G],\ \bar{b} := b[G, G]$ に対し、(i) より $a[G, G] = [G, G]a,\ b[G, G] = [G, G]b$ だから $a^{-1}[G, G] = [G, G]a^{-1},\ b^{-1}[G, G] = [G, G]b^{-1}$ だから

$$\begin{aligned} &\bar{a}\bar{b}\bar{a}^{-1}\bar{b}^{-1} \\ &= a[G, G]b[G, G]a^{-1}[G, G]b^{-1}[G, G] = aba^{-1}b^{-1}[G, G] = [G, G] \\ &= 1_{[G,G]} \end{aligned}$$

従って、$\bar{a}\bar{b} = \bar{b}\bar{a}$ を得る。すなわち $G/[G, G]$ は可換である。

(iii) 剰余群 G/L がアーベル群だとすると、$L \triangleleft G$ だから、(ii) と同様に計算して、

$$(aL)(bL)(aL)^{-1}(bL)^{-1} = [a, b]L = L$$

となるはずである。すなわち、任意の $a, b \in G$ に対して $[a, b] \in L$. 従って $[G, G] \subset L$. □

定義 109. 群 G に対して、$D^nG\ n = 0, 1, 2, \ldots$ を次のように定義する：

$$D^0G = G, \quad D^{i+1}G = [D^iG, D^iG]$$

命題 110. 群 G に対して部分群の下降列

$$G = D^0G \supseteq D^1G \supseteq \cdots \supseteq D^iG \supseteq \cdots$$

が存在し、各 i に対し $D^iG \triangleright D^{i+1}G$ であり、剰余群 $D^iG/D^{i+1}G$ はアーベル群である。

Proof. 命題 108 より直ちに従う。 □

命題 111. 有限群 G について、下記は同値である。

- (i) G は可解群
- (ii) 正規鎖 $G = G_0 \supset G_1 \supset \cdots G_n = \{1\}$ で、剰余群 G_i/G_{i+1}, $i = 0, 1, \ldots, k-1$, が全て アーベル群 になるものが存在する。
- (iii) $D^nG = 1$ となる $n \in \mathbb{N}$ が存在する。

注意 112. 命題 111(ii) が可解群の本来の定義である。

Proof. $(ii) \Rightarrow (iii)$: i に関する数学的帰納法で $D^iG \subset G_i$ $i = 0, \ldots, n$ を示せば、特に $i = n$ とすることにより $D^nG = \{1\}$ を得る。$i = 0$ の場合、定義よりただちに $D^0G = G \subset G_0 = G$ を得る。次に $i < k$ に対して $D^iG \subset G_i$ が成り立つと仮定して $D^kG \subset G_k$ を示そう。(ii) より G_{k-1}/G_k がアーベル群だから、命題 108(iii) より $[G_{k-1}, G_{k-1}] \subset G_k$. そこで

$$D^kG = [D^{k-1}G, D^{k-1}G] \subset [G_{k-1}, G_{k-1}] \subset G_k$$

を得る。

$(iii) \Rightarrow (ii)$: 交換子列

$$G = D^0G \supset D^1G \supset D^2G \supset \cdots$$

を作れば、命題 108 より、これは正規列で各 $D^iG/D^{i+1}G$ はアーベル群になる。さらに (iii) より、この列は最後には $D^nG = \{1\}$ になる。

$(i) \Rightarrow (ii)$: (i) ならば、正規列 $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$ で各 G_i/G_{i+1} が巡回群になるものが存在するが、巡回群はアーベル群だから、ただちに (ii) を得る。

$(ii) \Rightarrow (i)$: (ii) より正規列 $G_0 \supset \cdots \supset G_n$ で各 G_i/G_{i+1} がアーベル群になるものが存在する。ここである G_i/G_{i+1} が巡回群でないとする。このとき、単位元でない任意の元 $\bar{a} \in G_i/G_{i+1}$ をとる。今、G は有限群だから、G_i/G_{i+1} の位数も有限であり、従って $\bar{a}$ の位数は有限である。この位数がもし合成すうならば、$\bar{a}$ を適当な冪 $\bar{a}^\ell$ と取り替えることによって、最初から $\bar{a}$ の位数が素数だと考えることができる (cf. 演習問題 5)。すると部分群

$$\langle \bar{a} \rangle \subset G_i/G_{i+1}$$

は巡回群である（命題 51). 仮定により G_i/G_{i+1} 自身は巡回群ではないのだから、$\langle \bar{a} \rangle$ は真の部分群である。そこで、自然準同型写像

$$\varphi : G_i \longrightarrow G_i/G_{i+1} \quad x \longmapsto \bar{x} = xG_{i+1}$$

による逆像 $\varphi^{-1}(\langle \bar{a} \rangle)(\subset G_i)$ を H とおくと、

$$G_i \supset H \supset G_{i+1}.$$

ここで $\bar{a} \neq 1_{G_i/G_{i+1}}$ だから $H \neq G_{i+1}$ であり、$\langle \bar{a} \rangle \neq G_i/G_{i+1}$ だから $G_i \neq H$ となる。また、G_i/G_{i+1} はアーベル群だから、$\langle \bar{a} \rangle \triangleleft G_i/G_{i+1}$. よってその準同型による

逆像もまた正規部分群になる: $H \triangleleft G_i$. また、$G_{i+1} \triangleleft G_i$ だから $G_{i+1} \triangleleft H$ を得る。また、自然準同型

$$\psi : G_i/G_{i+1} \longrightarrow (G_i/G_{i+1})/(H/G_{i+1}) = G_i/H$$

を考えることにより (cf. 命題 91)、G_i/H はアーベル群とわかる。実際、ψ は全射だから G_i/H の任意の 2 つの元は $\psi(\bar{a}), \psi(\bar{b})$ と表せるから、G_i/G_{i+1} がアーベル群であることを使えば

$$\psi(\bar{a}) \cdot \psi(\bar{b}) = \psi(\bar{a} \cdot \bar{b}) = \psi(\bar{b} \cdot \bar{a}) = \psi(barb) \cdot \psi(\bar{a})$$

を得る。また、$H/G_{i+1} = \langle \bar{a} \rangle$ はアーベル群（巡回群だから）である。以上により、我々は新しい正規列

$$G = G_0 \supset \cdots G_i \supset H \supset G_{i+1} \supset \cdots$$

で、各 G_i/G_{i+1} はアーベル群で、特に H/G_{i+1} が巡回群になるものを得た。この列の中で巡回群にならない剰余群 G_i/G_{i+1} があれば、上で行った議論を繰り返して新しい部分群を付け加えることにより、最後には G_i/G_{i+1} が全て巡回群になっているような正規列を作ることができる。 □

8.2. $\mathfrak{S}_n$ $(n \geq 5)$ **の非可解性.** ここでは、5 次以上の対称群の非可解性を示す。

補題 113. $n \geq 3$ の時、$\mathfrak{A}_n$ の任意の元は、長さ 3 の巡回置換 (3-cycle) の積で表せる。

Proof. $x_1, x_2, x_3, x_4 \in \{1, 2, 3, \ldots, n\}$ をとり、すくなくとも x_1, x_2, x_3 は互いに相異なるものとする。このとき、

$$(x_1 x_2) \circ (x_2 x_3) = (x_1 x_2 x_3)$$

すなわち、任意の 3-cycle は $\mathfrak{A}_n$ の元であり、従って、3-cycle の積でかける $\mathfrak{S}_n$ の元は全て $\mathfrak{A}_n$ に含まれる。次に、逆の包含関係を示そう。x_1, x_2, x_3, x_4 が互いに相異なるとすると、

$$(x_1 x_2) \circ (x_3 x_4) = (x_1 x_3 x_2) \circ (x_1 x_3 x_4).$$

となるから、上の結果と合わせれば、偶数個の互換の積で表される $\mathfrak{S}_n$ の任意の元は $\mathfrak{A}_n$ の要素であることがわかる。 □

命題 114. 対称群と交代群の交換子群ついて、以下が成り立つ。

(i) $n \geq 2$ に対して $[\mathfrak{S}_n, \mathfrak{S}_n] = \mathfrak{A}_n$,

(ii)

$$[\mathfrak{A}_n, \mathfrak{A}_n] = \begin{cases} \mathfrak{A}_n & n \geq 5 \text{ のとき} \\ \mathfrak{D}_4 & n = 4 \text{ のとき} \\ \{1\} & n = 2, 3 \text{ のとき} \end{cases}$$

Proof. (i) 命題 **??**と準同型定理 105 より、$\mathfrak{S}_n/\mathfrak{A}_n$ は位数 2 のアーベル群だから、命題 111 より

$$[\mathfrak{S}_n, \mathfrak{S}_n] \subset \mathfrak{A}_n$$

である。特に $\mathfrak{A}_2 = \{1\}$ だから、$[\mathfrak{S}_2, \mathfrak{S}_2] = \mathfrak{A}_1 (= \{1\}$ を得る。あとは $n \geq 3$ に対して $[\mathfrak{S}_n, \mathfrak{S}_n] \supset \mathfrak{A}_n$ を示せば良い。$a \in \mathfrak{A}_n$ を任意にとる。補題 113 より、任意の $\mathfrak{A}_n$ の元

は長さ 3 の巡回置換 (3-cycle) の積で書き表せる。ところが、任意の 3-cycle$(x_1\ x_2\ x_3)$ $(1 \le x_1 < x_2 < x_3 \le n)$ は

$$(x_1\ x_2\ x_3) = (x_1x_3)(x_2x_3)(x_1x_3)^{-1}(x_2x_3)^{-1} \in [\mathfrak{A}_n, \mathfrak{A}_n]$$

となっているから、結局 $a \in [\mathfrak{A}_n, \mathfrak{A}_n]$. よって $[\mathfrak{S}_n, \mathfrak{S}_n] \supset \mathfrak{A}_n$ を得る。

(ii) $\sharp\mathfrak{A}_2 = 2$, $\sharp\mathfrak{A}_3 = 3$ ゆえ、命題 51 より、これらはアーベル群（巡回群)。従って補題 107 より

$$[\mathfrak{A}_n, \mathfrak{A}_n] = \{1\} \quad (n = 2, 3).$$

次に $n = 4$ の場合を考えよう。$\mathfrak{B}_4 \triangleleft \mathfrak{A}_4$ で、$\sharp\mathfrak{A}_4 = 12$, $\sharp\mathfrak{B}_4 = 4$ だから (cf. 6.4.5 節)、Lagrange の公式 (系 50) と命題 51 より、$\mathfrak{A}_4/\mathfrak{B}_4$ は位数 3 のアーベル群（巡回群）である。従って、命題 111 より

$$[\mathfrak{A}_4, \mathfrak{A}_4] \subset \mathfrak{B}_4.$$

一方、相異なる $x_1, x_2, x_3, x_4 \in \{1, 2, 3, 4\}$ に対して、

$$(x_1x_2)(x_3x_4) = (x_1x_2x_3)(x_1x_2x_4)(x_1x_2x_3)^{-1}(x_1x_2x_4)^{-1}$$

だから、補題 113 より $(x_1x_2)(x_3x_4) \in [\mathfrak{A}_4, \mathfrak{A}_4]$. $\mathfrak{B}_4$ は $(x_1x_2)(x_3x_4)$ 型の要素と単位元で作られた群だから、上とは逆の包含関係

$$[\mathfrak{A}_4, \mathfrak{A}_4] \supset \mathfrak{B}_4$$

が得られた。

最後に $n \ge 5$ の場合を示そう。$x_1, x_2, x_3, x_4, x_5 \in \{1, \ldots, n\}$ とし、x_1, x_2, x_3 は相異なるとする。このとき、

$$(x_1x_2x_3) = (x_1x_2x_4)(x_1x_3x_5)(x_1x_2x_4)^{-1}(x_1x_3x_5)^{-1}.$$

だから、補題 113 より、これは

$$\mathfrak{A}_n \subset [\mathfrak{A}_n, \mathfrak{A}_n]$$

を意味する。また、逆の包含関係は明らかだから、$\mathfrak{A}_n = [\mathfrak{A}_n, \mathfrak{A}_n]$ を得る。 □

系 115. 対称群 $\mathfrak{S}_n$ $(n \ge 5)$ は非可解である。

Proof. 命題 114 より、交換子列は

$$\mathfrak{S}_n = D^0\mathfrak{S}_n \supset D^1\mathfrak{S}_n = [\mathfrak{S}_n, \mathfrak{S}_n] = \mathfrak{A}_n \supset D^2\mathfrak{S}_n = [\mathfrak{A}_n, \mathfrak{A}_n] = \mathfrak{A}_n \cdots$$

となり、$D^i\mathfrak{S}_n = \mathfrak{A}_n (\neq \{1\})$ $i = 1, 2, \ldots$. 従って、命題 111 より、$\mathfrak{S}_n$ $(n \ge 5)$ は可解群ではありえない。 □

8.3. **代数方程式の可解性.** 系 115 は、５次以上の代数方程式の「解の公式」がつくれないこと、すなわち、係数の冪根で解を表す一般的な公式がつくれないことを意味する。この節の内容は「環・体論 II」で詳しく習うので、ここでは概略程度にとどめる。

次の定義で使われている「ガロア拡大」とは、「自己同型群 $Aut_K(L)$ がうまく定義できる拡大体」と考えておけばよい。ある代数方程式の解を全て付け加えてできる拡大体は「ガロア拡大」体の典型例である。

定義 116 (可解な拡大)**.** 有限次拡大 L/K が「可解」であるとは、適当なガロア拡大 E/K, $E \subset L$ があって、そのガロア群 Gal (E/K) が可解群である場合をいう。

定義 117 (冪根による拡大)**.** 有限次拡大 L/K が「冪根による拡大」であるとは、適当な拡大 E/L と拡大体列

$$K = E_0 \subset E_1 \subset \cdots \subset E_m = E$$

があって、各 E_{i+1} は E_i に次のような元を付け加えた拡大体になっている場合をいう：

(1) 1 の原始 n 乗根
(2) 方程式 $X^n - a = 0$ $(a \in E_i)$ の根の全て。

定理 118. 有限次拡大 L/K が可解であるための必要十分条件は、それが冪根による拡大であることである。

従って、系 115 により、$\mathfrak{S}_n$ をガロア群にもつ 5 次以上の方程式は冪根では解けない。$\mathfrak{S}_n$ $(n \geq 5)$ は非可解だが、$\mathfrak{S}_n$ の真部分群では可解なものが存在する（例えば、巡回部分群 $\langle(12345)\rangle \in \mathfrak{S}_5$). 従って、5 次以上の方程式でも、そのガロア群が $\mathfrak{S}_n$ の可解な真部分群になるものをとれば、その解を係数の冪根で表すことができるのである。（例えば $X^5 - a = 0$, $a \in \mathbb{Q}$)

9. 有限生成 $\mathbb{Z}$-加群

アーベル群は $\mathbb{Z}$-加群とみなして考える方が便利な場合が多い。ここでは $\mathbb{Z}$-加群の概念について基本的なことを述べる。いずれも $\mathbb{Z}$-加群よりも一般的な R-加群（R は環）の概念に拡張できるが、それについては 3 回生「環・体論 I」に譲る。

9.1. **アーベル群と $\mathbb{Z}$-加群.** 群 $(G, \cdot, 1_G)$ の演算"$\cdot$" は、通常は積のように書き表すが、特にアーベル群の場合は積 $(\cdot)$ の代わりに和 $(+)$ を使って書き表す方が便利な場合が多い。すなわち、群の演算を

$$a \cdot a \cdot a \cdot b \cdot c = a^3bc \quad (\text{右辺では} \cdot \text{記号を省略した書いた})$$

のように書くかわりに、

$$a + a + a + b + c = 3a + b + c$$

のように加法的に書きあらわすのである。この時、逆元も a^{-1} ではなく、$-a$ という風に書き、単位元も 1_G や 1_G ではなく、加法風に 0 (または 0_M) と書き表す。

アーベル群 G を特に加法に関する群のように書き表したとき、G は **$\mathbb{Z}$-加群** ($\mathbb{Z}$-module)、（あるいは単に加群）であるという。記号としては G (群 group の頭文字) の代わりに M (module の頭文字）を使うことが多い。以下でもその流儀に従うことにする。

アーベル群を加法的に記述すると、群の元 $a \in G$ を整数倍 na することができる。つまり $n \geq 0$ ならば

$$na = \underbrace{a + \cdots + a}_{n} \in M$$

なる元を表し、$n < 0$ ならば

$$na = \underbrace{-a \cdots - a}_{-n} \in M$$

を表している。これは体 K 上のベクトル空間 V において、任意のベクトル $\mathbf{a} \in V$ と $\alpha \in K$ に対して、スカラー倍 $\alpha\mathbf{a}$ が定義できたのと似ている。つまり、ベクトル空間においては

$$\begin{array}{rccc} \nu: & K \times V & \longrightarrow & V \\ & (\alpha, \mathbf{a}) & \mapsto & \nu(\alpha, \mathbf{a}) = \alpha\mathbf{a} \end{array}$$

なるスカラー倍写像 ν を考えることができて、

(1) $\nu(0, \mathbf{a}) = \mathbf{0}$ (零ベクトル)
(2) $\nu(\alpha, \nu(\beta, \mathbf{a})) = \nu(\alpha\beta, \mathbf{a})$
(3) $\nu(\alpha + \beta, \mathbf{a}) = \nu(\alpha, \mathbf{a}) + \nu(\beta, \mathbf{a})$
(4) $\nu(\alpha, \mathbf{a} + \mathbf{b}) = \nu(\alpha, \mathbf{a}) + \nu(\alpha, \mathbf{a})$

が成り立っていた。同様に、$\mathbb{Z}$-加群 M においては $\mathbb{Z}$ の M に対する **作用** (action)ν

$$\begin{array}{rccc} \nu: & \mathbb{Z} \times M & \longrightarrow & M \\ & (n, a) & \mapsto & \nu(n, a) = na \end{array}$$

が定義されて

(1) $\nu(0, a) = 0_M$ (加群の単位元)
(2) $\nu(n_1, \nu(n_2, a)) = \nu(n_1n_2, aa)$
(3) $\nu(n_1 + n_2, a) = \nu(n_1, a) + \nu(n_2, a)$

(4) $\nu(n, a+b) = \nu(n,a) + \nu(n,a)$

となっている。

演習問題 35. このことを確かめよ。(ヒント：上の４つの条件を全て乗法的に書き換え、通常のアーベル群で成り立っているかどうかを確かめればよい。)

演習問題 36. $\mathbb{Z}$ の作用 ν をもつ群 G に対して、$\nu(n,-x) = -\nu(n,x)$ $(n \in \mathbb{Z}, x \in G)$ が成り立つことを示せ。(ヒント：上の ν の条件より $\nu(n, 0+0) = \nu(n,0) + \nu(n,0)$ および $\nu(n, x+(-x)) = \nu(n,x) + \nu(n,-x)$ を導け。)

また、加群 M の部分集合 $N \subset M$ が**部分加群** (submodule) であるとは、N 自身も M の加法演算と単位元 0 によって加群になっている場合をいう。

アーベル群の準同型写像 $f : G \longrightarrow H$ も、加群として表記した場合には次のようなものになる。すなわち、$x, y \in G$ と $n \in \mathbb{Z}$ に対して、

$$f(x+y) = f(x) + f(y) \quad f(nx) = nf(x)$$

すなわち、ベクトル空間の間の線形写像と同じ形をしていることに注意しよう。

注意 119 (R-加群)**.** 有理整数全体の集合 $\mathbb{Z}$ や実数係数の 1 変数多項式全体の集合 $\mathbb{R}[x]$ のように、加法、減法、乗法（除法はのぞく）の演算を自由に行うことができる集合を（可換）環と呼ぶ。**加法群** G に適当な環 R が作用するものを R-加群と呼ぶ。例えば、任意の体は可換環であるが、体 K 上の任意のベクトル空間 V は、K-加群である。実際、V はベクトルの加法によってアーベル群になっているし、各ベクトルに体 K の元が「スカラー倍」として作用するからである。ここでは $R = \mathbb{Z}$ の場合だけを考え、R を色々変えて R-加群を考えることはしない。

9.2. (**有限生成**) $\mathbb{Z}$**-自由加群.**

定義 120 (有限生成加群)**.** $\mathbb{Z}$-加群 M が**有限生成** (finitely generated) であるとは、有限個の元 $x_1, \ldots, x_n \in M$ によって、M の全ての元 $y \in M$ が $y = \sum_{i=1}^n \alpha_i x_i$ $(\alpha_i \in \mathbb{Z})$ と書き表せる場合をいう（ただし、$\alpha_1, \ldots, \alpha_n$ のとり方は一通りとは限らない)。このことを、$M = \sum_{i=1}^n \mathbb{Z}x_i$ と書き表す。すなわち、

$$\sum_{i=1}^n \mathbb{Z}x_i = \left\{ \sum_{i=1}^n \alpha_i x_i \mid \alpha_i \in \mathbb{Z} \right\}$$

と定義される。

定義 121 (加群の和)**.** 集合 M が部分加群 $N_1, \ldots, N_r$ の**和** (sum) であるとは、M の任意の元 $y \in M$ が $y = \sum_{i=1}^r x_i$ $(x_i \in N_i)$ の形に書き表せる場合をいう。ただし、この書き表し方は一意的とは限らない。$y = \sum_{i=1}^r x_i, w = \sum_{i=1}^r y_i \in M$ に対して、$y + w = \sum_{i=1}^r (x_i + y_i)$ *(ただし、$x_i + y_i$ は加群 N_i における加法)* と定義することにより、M 自身も加群となる。加群の和を

$$M = \sum_{i=1}^r N_i = N_1 + \cdots + N_r$$

と書き表す。

定義 122 (直和)**.** 加群の和 $M = \sum_{i=1}^{r} N_i = N_1 + \cdots + N_r$ が**直和** (direct sum) であるとは、M の任意の元 $y \in M$ が $y = \sum_{i=1}^{r} x_i$ $(x_i \in N_i)$ の形に一意的に書き表せる場合をいう。この時、

$$M = \bigoplus_{i=1}^{r} N_i = N_1 \oplus \cdots \oplus N_r$$

と書き表す。

次の命題は、加群の和が直和であることを示す時に良く使われる。

命題 123. 部分加群の和 $M = N_1 + N_2$ が直和になるための必要十分条件は、単射

$$N_1 \ni x \mapsto x + 0 \in N_1 + N_2 = M$$

および

$$N_2 \ni y \mapsto 0 + y \in N_1 + N_2 = M$$

を考えることにより $N_1, N_2 \subseteq M$ とみなしたとき、$N_1 \cap N_2 = \{0_M\}$ となることである。

Proof. $N_1 \cap N_2 = \{0_M\}$ だとする。このとき、$y \in M$ が

$$y = x_1 + x_2 = u_1 + u_2 \quad (x_1, u_1 \in N_1, x_2, u_2 \in N_2)$$

と二通りに書き表せたとしよう。すると、上の式を移項して $x_1 - u_1 = u_2 - x_2 \in N_1 \cap N_2$ となるから、$x_1 - u_1 = u_2 - x_2 = 0_M$, すなわち、$x_1 = u_1, x_2 = u_2$ となり、$y = x_1 + x_2$ という表し方は一意的となるから、$M = N_1 \oplus N_2$ となる。逆に $M = N_1 \oplus N_2$ であるとしよう。このとき、$y \in N_1 \cap N_2$ は、適当な $x_1 \in N_1$, $x_2 \in N_2$ によって $y = x_1 + 0 = 0 + x_2$ と書ける。しかるに直和だから、この表し方は一意的であるはずで、$x_1 = 0$, $0 = x_2$ を得る。すなわち $y = 0$. よって $N_1 \cap N_2 = \{0_M\}$ □

自由加群の概念は有限生成加群に限らないが、ここでは有限生成の場合だけ考えることにする。

定義 124 (自由加群)**.** 有限生成 $\mathbb{Z}$-加群 $M = \sum_{i=1}^{n} \mathbb{Z}x_i$ に対し、任意の元 $y \in M$ のが一意的に $y = \sum_{i=1}^{n} \alpha_i x_i$ $(\alpha_i \in \mathbb{Z})$ と書き表せる時、M は**基底** (basis) $\{x_1, \ldots, x_n\}$ をもつ $\mathbb{Z}$-**自由加群** (free module) であるという。すなわち、$M = \bigoplus_{i=1}^{n} \mathbb{Z}x_i$ と直和の形で書き表せる場合をいう。

例 125. 自由加群の基底のとりかたは一意的ではない。例えば、有限生成 $\mathbb{Z}$-加群 $M = \mathbb{Z}(1,0) + \mathbb{Z}(0,1)$ は、$\{(1,0),(0,1)\}$) を基底にもつ自由加群だが、

$$(0,1) = -(1,-1) + (1,0) \quad (1,-1) = (1,0) - (0,1)$$

に注意すれば $M = \mathbb{Z}(1,0) + \mathbb{Z}(1,-1)$, すなわち $\{(1,0),(1,-2)\}$ も基底であることがわかる。

例 126. $\mathbb{Z}$-加群ではあるが、$\mathbb{Z}$-自由加群の例として、たとえば

$$M = \mathbb{Z} \cdot \frac{1}{2} + \mathbb{Z} \cdot \frac{1}{3}.$$

実際、

$$\frac{1}{3} \notin \mathbb{Z} \cdot \frac{1}{2}, \quad \frac{1}{2} \notin \mathbb{Z} \cdot \frac{1}{3}$$

だから、$\mathbb{Z}\cdot\frac{1}{2}\neq M$ かつ $\mathbb{Z}\cdot\frac{1}{3}\neq M$. すなわち、$\frac{1}{2},\frac{1}{3}$ はどちらも M の生成元として必要である。しかるに、

$$1=2\cdot\frac{1}{2}+0\cdot\frac{1}{3}=0\cdot\frac{1}{2}+3\cdot\frac{1}{3}$$

と $1\in M$ が 2 通りに表されるから、$\{\frac{1}{2},\frac{1}{3}\}$ は基底にはならず、M は $\mathbb{Z}$-自由加群ではない。

9.3. **$\mathbb{Z}$-加群 $\mathbb{Z}/n\mathbb{Z}$.**

演習問題 37. 任意の自然数 $n\in\mathbb{N}$ に対して、$n\mathbb{Z}=\{nx\mid x\in\mathbb{Z}\}$ は $(\mathbb{Z},\times,1)$ に関しては部分群にはなっていない *(*従って、とくに $\mathbb{Z}/n\mathbb{Z}$ を積演算に関する剰余群として定義できない*)*。このことを示せ。

$(\mathbb{Z},+,0)$ はアーベル群だから、その任意の部分群は正規部分群である（演習 33).
例えば、任意の $n\in\mathbb{N}$ に対し

$$n\mathbb{Z}=\{nk\mid k\in\mathbb{Z}\}=\{\ldots,-2n,-n,0,n,2n,3n,\ldots\}$$

は正規部分群になる $(n\mathbb{Z}\triangleleft\mathbb{Z})$. 従って剰余群 $\mathbb{Z}/n\mathbb{Z}$ をつくることができる（命題 60).
ここで、

$$\mathbb{Z}/n\mathbb{Z}=\{n\mathbb{Z},1+n\mathbb{Z},2+n\mathbb{Z},\ldots,(n-1)+n\mathbb{Z}\}$$

ただし、$j+n\mathbb{Z}=\{i+nk\mid k\in\mathbb{Z}\}$, となり、足し算演算は

$$(i+n\mathbb{Z})+(j+n\mathbb{Z})=(i+j)=\begin{cases}(i+j)+n\mathbb{Z} & i+j<n\text{ の場合;}\\ (i+j-n)+n\mathbb{Z} & \text{それ以外}\end{cases}$$

と定義でき、単位元は $0+n\mathbb{Z}=n\mathbb{Z}$ であり、逆元 $(j+n\mathbb{Z})^{-1}$ $(0\leq j<n)$ は $-(j+n\mathbb{Z})$ と書き、

$$-(j+n\mathbb{Z}):=(n-j)+n\mathbb{Z}$$

と定義する。また、$\mathbb{Z}$ の作用 ν を

$$\begin{array}{rccc}\nu: & \mathbb{Z}\times\mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/nZZ\\ & (m,a+n\mathbb{Z}) & \mapsto & \nu(m,a+n\mathbb{Z})=ma+n\mathbb{Z}\end{array}$$

と定めることにより、$\mathbb{Z}$-加群とみなすことができる。すると $\mathbb{Z}/n\mathbb{Z}$ は $1+n\mathbb{Z}$ で生成された $\mathbb{Z}$-加群である。これが $\mathbb{Z}$-自由加群でないことは、任意の $a\in\mathbb{Z}$ に対して

$$0+n\mathbb{Z}=n(a+n\mathbb{Z})$$

と 2 通り以上の表現をもつことからわかる。

9.4. **加群の階数.** 体 K 上のベクトル空間 V においては、線形独立の概念があり、V の中で K 上線形独立なベクトルの個数の最大値のことを V の次元と呼び $\dim_K V$ と書き表した。$\mathbb{Z}$-加群においても同様の概念を考えることができ、それを「次元」とは呼ばずに 階数と呼ぶ。すなわち、

定義 127 (加群の階数)**.** $\mathbb{Z}$-加群 M の部分集合 $\{x_1,\ldots,x_n\}(\subset M-\{0_M\})$ が一次独立であるとは、

$$\alpha_1x_1+\cdots+\alpha_nx_n=0_M$$

となるような α_j $(j=1,\ldots,n)$ は

$$\alpha_1=\cdots=\alpha_n=0$$

だけに限られる場合をいう。また、一次独立な部分集合の要素の数として最も大きなものを「**階数**」(rank) と呼び、$\operatorname{rank} M$ と書く。

$$\operatorname{rank} M = \max\{\sharp\{x_1, \ldots, x_n\} \mid \{x_1, \ldots, x_n\} \text{は一次独立}\}$$

$\mathbb{Z}$-加群 M の階数は、次のように $\mathbb{Q}$-ベクトル空間の次元として求めることができる。まず、M をもとにして $\mathbb{Q}$-ベクトル空間 $\mathbb{Q} \otimes_{\mathbb{Z}} M$ を次のように定義する：

$$\mathbb{Q} \otimes_{\mathbb{Z}} M = \left\{ \frac{x}{n} \mid x \in M,\ n \in \mathbb{Z} - \{0\} \right\}$$

これは、整数係数である M の要素を零でない整数 n で割った元を新たに考えることを意味する。整数の割り算、すなわち分数においては、一見形が異なる分数が通分によって等しいとされることがあるが、それと同様のことを考える。すなわち、

$$\frac{x}{n} = \frac{y}{m} \Leftrightarrow mx - ny = 0$$

によって $\mathbb{Q} \otimes_{\mathbb{Z}} M$ における等号を定義する。さらに、加法演算は

$$\frac{x}{n} + \frac{y}{m} = \frac{mx + ny}{mn}$$

と通常の分数の足し算のように定義する。さらに M の任意の要素 $x \in M$ を $\frac{x}{1}$ と同一視することにより、

$$M \subset \mathbb{Q} \otimes_{\mathbb{Z}} M$$

とみなす。このとき、

命題 128. $\operatorname{rank} M = \dim_{\mathbb{Q}} \mathbb{Q} \otimes_{\mathbb{Z}} M$

Proof. まず

$$\operatorname{rank} M \leq \dim_{\mathbb{Q}} \mathbb{Q} \otimes_{\mathbb{Z}} M \tag{11}$$

を示そう。そのためには、$x_1, \ldots, x_n \in M$ が一次独立ならば、$\frac{x_1}{1}, \ldots, \frac{x_n}{1}$ が $\mathbb{Q} \otimes_{\mathbb{Z}} M$ の中で $\mathbb{Q}$ 上一次独立であることが言えればよい。もし $\frac{x_1}{1}, \ldots, \frac{x_n}{1}$ が $\mathbb{Q} \otimes_{\mathbb{Z}} M$ で一次独立でないとすれば、

$$\zeta_1 \cdot \frac{x_1}{1} + \cdots + \zeta_n \cdot \frac{x_n}{1} = 0$$

となるような $\zeta_j \in \mathbb{Q}$, $j = 1, \ldots, n$, で $\zeta_1 = \cdots = \zeta_n = 0$ 以外のものが存在する。そこで適当な整数 N で ζ_j の分母を払えば、$\alpha_j := N\zeta_j \in \mathbb{Z}\ j = 1, \ldots, n)$ とできる。すなわち、

$$\alpha_1 \cdot x_1 + \cdots + \alpha_n \cdot x_n = 0$$

で $(\alpha_1, \ldots, \alpha_n) \neq (0, \ldots, 0)$ なる $\alpha_j \in \mathbb{Z}\ j = 1, \ldots, n$ が存在することになり、$x_1, \ldots, x_n$ が一次独立であることに反する。よって、$\frac{x_1}{1}, \ldots, \frac{x_n}{1}$ が $\mathbb{Q} \otimes_{\mathbb{Z}} M$ の中で $\mathbb{Q}$ 上一次独立でなければならない。

次に

$$\operatorname{rank} M \geq \dim_{\mathbb{Q}} \mathbb{Q} \otimes_{\mathbb{Z}} M \tag{12}$$

を示そう。$d = \dim_{\mathbb{Q}} \mathbb{Q} \otimes_{\mathbb{Z}} M$ とし、$\mathbb{Q}$-ベクトル空間としての基底を $\frac{x_1}{n_1}, \ldots, \frac{x_d}{n_d}$ $(x_1, \ldots, x_d \in M,\ n_1, \ldots, n_d \in \mathbb{Z} - \{0\})$ とする。このとき、$N := n_1 \times \cdots \times n_d$ とおき、これを上の基底に掛けて分母を払う：

$$y_j := N \cdot \frac{x_j}{n_j} = \frac{N}{n_j} x_j \in \mathbb{Z} x_j \subset M.$$

すると、$y_1, \ldots, y_d \in M$ は一次独立である。実際、もしそうでなければ

$$\alpha_1 y_1 + \cdots + \alpha_d y_d = 0_M$$

となる $(\alpha_1, \ldots, \alpha_d) \in \mathbb{Z}^d - \{(0, \ldots, 0)\}$ が存在するが、この式を書き直すを

$$\alpha_1 N \cdot \frac{x_1}{n_1} + \cdots + \alpha_d N \cdot \frac{x_d}{n_d} = 0_{\mathbb{Q} \otimes_{\mathbb{Z}} M}$$

で $(\alpha_1 N, \ldots, \alpha_d N) \neq (0, \ldots, 0)$. これは $\frac{x_1}{n_1}, \ldots, \frac{x_d}{n_d}$ が $\mathbb{Q}$-上一次独立であるという仮定に反する。よって $y_1, \ldots, y_d \in M$ は一次独立でなければならない。

$()()$ により、$\operatorname{rank} M = \dim_{\mathbb{Q}} \mathbb{Q} \otimes_{\mathbb{Z}}$ を得る。 □

$\mathbb{Z}$-自由加群の階数とは基底の個数に他ならない。

命題 129. $\mathbb{Z}$-自由加群 M の基底の集合を $\mathcal{B}$ とすると、$\operatorname{rank} M = \sharp\mathcal{B}$ である。

Proof. $\mathcal{B} = \{x_1, \ldots, x_n\}$ とすると、M の任意の要素 y は $y = \sum_{i=1}^{n} \alpha_i x_i$ $(\alpha_j \in \mathbb{Z})$ の形に一意的に書き表せる。すると、$\frac{x_1}{1}, \ldots, \frac{x_n}{1}$ は、$\mathbb{Q}$-ベクトル空間 $\mathbb{Q} \otimes_{\mathbb{Z}} M$ の基底である。実際、

- $\frac{x_1}{1}, \ldots, \frac{x_n}{1}$ は $\mathbb{Q}$ 上一次独立である：実際、

  $$\zeta_1 \frac{x_1}{1} + \cdots + \zeta_n \frac{x_n}{1} = 0_{\mathbb{Q} \otimes_{\mathbb{Z}} M} \qquad (\zeta_j \in \mathbb{Q})$$

  とすると、適当な整数を両辺に掛けて ζ_j の全ての分母を払えば

  $$\alpha_1 x_1 + \cdots + \alpha_n x_n = 0_M (= 0x_1 + \cdots + 0x_n) \qquad (\alpha_j \in \mathbb{Z})$$

  の形になる。すなわち 0_M が見かけ上二通りに表されているが、$x_1, \ldots, x_n$ は基底だから 0_M は x_j の線形結合として一意的に書き表されるはずで、結局 $\alpha_i = 0$ $i = 1, \ldots, n$ でなければならない。従って、ζ_i も全て 0 となり、結局 $\frac{x_1}{1}, \ldots, \frac{x_n}{1}$ は $\mathbb{Q}$ 上一次独立である。
- $\mathbb{Q} \otimes_{\mathbb{Z}} M$ の任意の要素は $\frac{x_1}{1}, \ldots, \frac{x_n}{1}$ の $\mathbb{Q}$ 上の線形結合で書き表せる：実際、$\mathbb{Q} \otimes_{\mathbb{Z}} M$ の任意の要素は $\frac{y}{n}$ $(y \in M, n \in \mathbb{Z} - \{0\})$ の形をしているが、$y = \sum_{i=1}^{n} \alpha_i x_i$ と書き表せるので、結局

  $$\frac{y}{n} = \sum_{i=1}^{n} \frac{\alpha_i}{n} \cdot \frac{x_i}{1} \quad \left(\frac{\alpha_i}{n} \in \mathbb{Q}, i = 1, \ldots, n \right)$$

  の形で書ける。

従って、命題 128 より、$\operatorname{rank} M = \dim_{\mathbb{Q}} \mathbb{Q} \otimes_{\mathbb{Z}} M = n = \sharp\mathcal{B}$ となる。 □

しかしながら、自由加群以外の一般の加群に対しては、$\operatorname{rank} M$ は生成元の個数よりは一般に小さい値をとる。

例 130. $M = \mathbb{Z}\cdot\frac{1}{2} + \mathbb{Z}\cdot\frac{1}{3}$ は自由加群ではないが、2 の生成元 $\frac{1}{2}, \frac{1}{3}$ で生成される $\mathbb{Z}$-加群である。しかるに、$\frac{1}{2} = \frac{3}{2}\cdot\frac{1}{3}$ および $\frac{1}{3} = \frac{2}{3}\cdot\frac{1}{2}$ だから、

$$\mathbb{Q}\otimes_{\mathbb{Z}} M = \mathbb{Q}\cdot\frac{1}{2} + \mathbb{Q}\cdot\frac{1}{3} = \mathbb{Q}\cdot\frac{1}{2} = \mathbb{Q}\cdot\frac{1}{3} (= \mathbb{Q}\cdot 1)$$

となり、従って命題 *9.4* より $\operatorname{rank} M = \dim_{\mathbb{Q}} \mathbb{Q}\otimes_{\mathbb{Z}} M = 1$ となる。

9.5. **加群の長さ.** 加群の「長さ」は、階数と混同しやすいが、階数よりも抽象的な概念でわかりにくい。しかし加群の構造を調べる時に無くてはななならない重要な量である。

定義 131 (加群の長さ)**.** $\mathbb{Z}$-加群 M の長さ $\ell(M)$ は、部分加群列の長さの最小上界 *(* つまり、有限の時は最大値、無限の時は ∞*)* をいう。すなわち、

$$\ell(M) := \sup\left\{ \ell \;\middle|\; \begin{array}{l} 0 \subset M_1 \subset M_2 \subset \cdots \subset M_\ell = M, \\ \text{ここで } M_j \subset M \text{ は部分加群で} \\ M_i \neq M_{i+1}, i = 1, \ldots, \ell - 1 \end{array} \right\}$$

加群の長さを計算するとき、次の命題 132 および命題 136 は大変有用である。

命題 132. $M = N_1 \oplus N_2$ のとき、$\ell(M) = \ell(N_1) + \ell(N_2)$.

Proof. $r = \ell(N_1)$, $s = \ell(N_2)$ とすれば、

$$0 \subset N_{11} \subset N_{12} \subset \cdots \subset N_{1r} = N_1$$

および

$$0 \subset N_{21} \subset N_{22} \subset \cdots \subset N_{2s} = N_2$$

なる（最大長の）部分加群列が存在する。これを使って、

$$\begin{aligned} 0 \subset N_{11}\oplus 0 \subset N_{12}\oplus 0 \subset \cdots \subset & \quad N_{1r}\oplus 0 \\ \subset & \quad N_{1r}\oplus N_{21} \quad \subset N_{1r}\oplus N_{22} \subset \cdots \subset N_{1r}\oplus N_{2s} = M \end{aligned}$$

と、長さ $r+s$ の M の部分加群列がつくれる。従って、

$$\ell(M) \geq \ell(N_1) + \ell(N_2)$$

である。

次に逆の不等式を示そう。まず、第 2 成分への射影

$$\pi_2 : M = N_1 \oplus N_2 \to N_2 \qquad (\pi_2(x,y) = y)$$

は明らかに加群の準同型で $\operatorname{Ker}\pi_2 = N_1$ である。そこで、M の部分加群列

$$0 \subset M_1 \subset M_2 \subset \cdots \subset M_\ell = M$$

が与えられたとき、各 $0 \leq i < \ell$ に対して、以下のすくなくともいずれか一方が成り立つ

条件（$*$）

- $M_i \cap N_1 \subset M_{i+1} \cap N_1$, かつ $M_i \cap N_1 \neq M_{i+1} \cap N_1$
- $\pi_2(M_i) \subset \pi_2(M_{i+1})$ かつ $\pi_2(M_i) \neq \pi_2(M_{i+1})$.

が成り立つ。

条件（∗）の証明. 実際、もしそうでなければ、$M_i \cap \mathrm{Ker}\,\pi_2 = M_{i+1} \cap \mathrm{Ker}\,\pi_2$, $\pi_2(M_i) = \pi_2(M_{i+1})$ となるから、２つの短完全列をふくむ以下の図式を得る。

$$\begin{array}{ccccccc} 0 & \longrightarrow & M_i \cap \mathrm{Ker}\,\pi_2 & \xrightarrow{\eta_i} & M_i & \xrightarrow{\pi_2} & \pi_2(M_i) & \longrightarrow 0 \\ & & \| & & & & \| & \\ 0 & \longrightarrow & M_{i+1} \cap \mathrm{Ker}\,\pi_2 & \xrightarrow{\eta_{i+1}} & M_{i+1} & \xrightarrow{\pi_2} & \pi_2(M_{i+1}) & \longrightarrow 0 \end{array}$$

ここで η_i, η_{i+1} は包含写像である。仮定より $M_i \subset M_{i+1}$ であるが、この図式から $M_{i+1} \subset M_i$ が言えてしまい、$M_i \neq M_{i+1}$ という仮定に反してしまうことを示せば良い。任意の元 $y = y_1 + y_2 \in M_{i+1} \subset N_1 \oplus N_2$ $(y_1 \in N_1, y_2 \in N_2)$ に対して、$\pi_2(y) = y_2 \in \pi_2(M_{i+1}) = \pi_2(M_i)$ となり、$\pi_2 : M_i \to \pi_2(M_i)$ は全射だから、適当な $w = w_1 + w_2 \in M_i \subset N_1 \oplus N_2$ $(w_1 \in N_1, w_2 \in N_2)$ によって

$$\pi_2(w) = w_2 = y_2 = \pi_2(y)$$

となる。一方、$y_1 \in M_i \cap \mathrm{Ker}\,\pi_2 = M_{i+1} \cap \mathrm{Ker}\,\pi_2 \ni w_1$ だから、必要ならば w_1 を y_1 に取り替えれば（たとえそうしても $\pi_2(w) = \pi_2(y)$ という性質は変わらないことに注意）、結局

$$w_1 = y_1$$

と考えることができる。従って、$y = w \in M_i$. つまり $M_{i+1} \subset M_i$ となった。 □

さて、条件（∗）を使えば、

$$0 \subseteq M_1 \cap N_1 \subseteq M_2 \cap N_2 \subseteq \cdots \subseteq M_\ell \cap N_1 = N_1$$

から $M_i \cap N_1 = M_{i+1} \cap N_1$ となってしまうものを除いてできた部分加群列の長さ r と

$$0 \subseteq \pi_2(M_1) \subseteq \pi_2(M_2) \subseteq \cdots \subseteq \pi_2(M_\ell) = N_2$$

から $\pi_2(M_i) = \pi_2(M_{i+1})$ となってしまうものを除いてできた部分加群列の長さ s の和が丁度 ℓ になる。ところが、$r \leq \ell(N_1)$, $s \leq \ell(N_2)$ だから、結局

$$\ell(M) = \ell = r + s \leq \ell(N_1) + \ell(N_2)$$

を得る。 □

命題 136 を示す前に、次の補題を準備しておく。

補題 133 (中国人剰余定理). 自然数 $n \in \mathbb{N}$ が $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ と素因数分解されているとする。ここで $p_1, \ldots, p_r$ は相異なる素数とする。この時、

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_r^{\nu_r}.$$

Proof. 写像 $\varphi : \mathbb{Z}/n\mathbb{Z} \to \bigoplus_{i=1}^r \mathbb{Z}/p_i^{\nu_i}\mathbb{Z}$ を任意の $a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ に対して

$$\varphi(a + n\mathbb{Z}) = (a + p_1^{\nu_1}\mathbb{Z}, \ldots, a + p_r^{\nu_r}\mathbb{Z})$$

と定義する。φ が同型写像であることを言えばよい。まずこれが $\mathbb{Z}$-加群準同型であること、すなわち、

$$\varphi((a + n\mathbb{Z}) + (b + n\mathbb{Z})) = \varphi(a + n\mathbb{Z}) + \varphi(b + n\mathbb{Z})$$

かつ

$$\varphi(\alpha(a + n\mathbb{Z})) = \alpha \cdot \varphi(a + n\mathbb{Z}) \qquad (\alpha \in \mathbb{Z})$$

であることは、直接計算で確かめられる。また、

$$\begin{aligned}\operatorname{Ker}\varphi &= \{a+n\mathbb{Z} \mid a+p_i^{\nu_i}\mathbb{Z}=p_i^{\nu_i},\ i=1,\dots,r\}\\ &= \{a+n\mathbb{Z} \mid a\in p_i^{\nu_i}\mathbb{Z}\ (\text{つまり } a \text{ は } p_i^{\nu_i} \text{ の倍数}),\ i=1,\dots,r\}\end{aligned}$$

となるが、p_i $(i=1,\dots,r)$ は互いに異なる素数だから、a が $p_i^{\nu_i}$ $(i=1,\dots,r)$ の倍数であるとは、結局 a が $\prod_{i=1}^r p_i^{\nu_i}=n$ の倍数であることにほかならない。従って $a+n\mathbb{Z}=\mathbb{Z}$ となり、$\ker\varphi=0$. よって φ は単射である (命題 88). 最後に φ の全射性を示そう。$\overline{a}:=(a_1+p_1^{\nu_1}\mathbb{Z},\dots,a_r+p_r^{\nu_1}\mathbb{Z})\in\bigoplus_{i=1}^r\mathbb{Z}/p_i^{\nu_i}\mathbb{Z}$ を任意にとる。任意の $i\neq j$ に対して、$(p_i^{\nu_i},\prod_{j\neq i}p_j^{\nu_j})=1$ だからユークリッドの互除法定理により

$$y_ip_i^{\nu_i}+x_i\prod_{j\neq i}p_j^{\nu_j}=1$$

なる $x_i,y_i\in\mathbb{Z}$ が存在する。そこで、

$$a=\sum_{i=1}^r a_ix_i\prod_{j\neq i}p_j^{\nu_j}$$

と置けば、$i=1,\dots,r$ に対して

$$a_ix_i\prod_{j\neq i}p_j^{\nu_j}+p_i^{\nu_i}=a_i-a_iy_ip_i^{\nu_i}+p_i^{\nu_i}=a_i+p_i^{\nu_i}$$

であり、また、$k\neq i$ に対して

$$a_ix_i\prod_{j\neq i}p_j^{\nu_j}+p_k^{\nu_k}=p_k^{\nu_k}$$

となるから、結局 $\varphi(a)=\overline{a}$ となる。 □

補題 134. $\mathbb{Z}$ は階数 *1* の $\mathbb{Z}$-自由加群である。また、$\mathbb{Z}$ の部分加群は適当な $a\in\mathbb{Z}$ によって $\mathbb{Z}\cdot a$ の形に限られる。これもまた階数 1 の $\mathbb{Z}$-自由加群である。

Proof. 部分加群が $\mathbb{Z}\cdot a$ の形に限られることだけを示せば、あとは明らか。部分加群 $N\subset\mathbb{Z}$ を任意にとり。$a=\min\{|x|\ 0\neq x\in N\}$, すなわち、$a$ は N の 0 以外の要素で絶対値が最小のものをとる。N 自身も $\mathbb{Z}$-加群ゆえ、任意の $n\in\mathbb{Z}$ に対して $na\in N$. すなわち、$\mathbb{Z}\cdot a\subseteq N$ である。逆に、$x\in N$ を任意にとると、$a\leq|x|$ ゆえ、a で割り算をして

$$x=q\cdot a+r\qquad(q\in\mathbb{Z},\ 0\leq r<a)$$

となる。ここでもし $r\neq0$ ならば、$x,q\cdot a\in N$ ゆえ

$$(0\neq)r=x-q\cdot a\in N$$

となる。すると $r<a$ となってしまい、a の最小性に反する。よって $r=0$ でなければならず、$x\in\mathbb{Z}\cdot a$. つまり $N\subseteq\mathbb{Z}\cdot a$. 従って結局 $N=\mathbb{Z}\cdot a$ となる。 □

注意 135 (単項イデアル整域)**.** 補題 134 はより一般的で重要な定理「Euclid 環は単項イデアル整域である」の特殊な場合になっている。つまり、補題 134 は「$\mathbb{Z}$ は単項イデアル整域である」ということを言っている。詳しくは 3 回生「環・体論 I」で学べ。

命題 136. $n \in \mathbb{Z} - \{0\}$ が $n = p_1 \cdots p_r$ $(p_1 \leq \cdots \leq p_r)$ と素因数分解されているとする。このとき、$\ell(\mathbb{Z}/n\mathbb{Z}) = r$.

Proof. $n = p_1^{\nu_1} \cdots p_s^{\nu_s}$, $p_1 < \cdots < p_s$, $\nu_j \in \mathbb{N}$, $j = 1, \ldots, s$, $r = \nu_1 + \cdots + \nu_s$ と因数分解されたとする。中国人剰余定理 (補題 133) より

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\nu_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_s^{\nu_s}\mathbb{Z}.$$

従って、補題 136 より

$$\ell(\mathbb{Z}/n\mathbb{Z}) = \sum_{i=1}^{s} \ell(\mathbb{Z}/p_i^{\nu_i}).$$

そこで、一般に素数 p と $\nu \in \mathbb{N}$ に対し、$\ell(\mathbb{Z}/p^\nu\mathbb{Z}) = \nu$ であることが言えれば、$\ell(\mathbb{Z}/n\mathbb{Z}) = r$ が言えたことになる。このことを言うためには、$\mathbb{Z}/p^\nu\mathbb{Z}$ の部分加群がどんな形をしているかを考えなければならない。そこで自然準同型写像 (命題 89 参照)

$$\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}/p^\nu\mathbb{Z} \qquad s.t. \quad \varphi(a) = a + p^\nu\mathbb{Z}$$

を考える。任意の部分加群 $M \subset \mathbb{Z}/p^\nu\mathbb{Z}$ に対して、その逆像 $\varphi^{-1}(M)$ は $\varphi^{-1}(0) = p^\nu\mathbb{Z}$ を含む $\mathbb{Z}$ の部分加群である (命題 85 参照)。補題 134 よりそれは $\mathbb{Z}a = a\mathbb{Z}$ $(a \in \mathbb{Z})$ の形をしている。つまり、

$$p^\nu\mathbb{Z} \subseteq a\mathbb{Z} = \varphi^{-1}(M) \qquad (a \in \mathbb{Z})$$

である。そのような a は明らかに $a = p^i$, $i = 0, p, p^2, \ldots, p^\nu$ に限られる。このことから、

$$0 = p^\nu\mathbb{Z}/p^\nu\mathbb{Z} \subset p^{\nu-1}\mathbb{Z}/p^\nu\mathbb{Z} \subset \cdots \subset p^2\mathbb{Z}/p^\nu\mathbb{Z} \subset p\mathbb{Z}/p^\nu\mathbb{Z} \subset \mathbb{Z}/p^\nu\mathbb{Z}$$

が最長の部分加群列になる。したがって $\ell(\mathbb{Z}/p^\nu\mathbb{Z}) = \nu$ となる。 □

注意 137 (ベクトル空間との比較)**.** 加群の「階数」は体 K 上のベクトル空間 V の次元の概念の一般化であった。加群の「長さ」もやはり次元の概念の一般化で、実際、「階数」と「長さ」の概念を体上のベクトル空間の場合に特殊すると、どちらも次元の概念と一致する。しかしながら加群の場合、「階数」と「長さ」は一般に別の値になる。例えば、

$$M = \mathbb{Z} \cdot \frac{1}{2} + \mathbb{Z} \cdot \frac{1}{3}$$

は $\operatorname{rank} M = 1$ であるが $\ell M = 2$ となる。

9.6. 捩れ元、捩れ部分群、捩れの無い加群.

定義 138 (捩れ元)**.** $\mathbb{Z}$-加群 M の元 $x \in M$ が「捩れ元」(torsion element) であるとは、$nx = 0_M$ となる $n \in \mathbb{Z} - \{0\}$ が存在する場合をいう。

命題 139. $\mathbb{Z}$-加群 M の捩れ元全体の集合 $T(M)$ は、M の部分 $\mathbb{Z}$-加群になる。

Proof. **定義** *32* より[4]

(1) $0 \in T(M)$

[4]命題 33 を使った証明に変更すべきである。

(2) $x, y \in T(M)$ ならば $x + y \in T(M)$
(3) $x \in T(M)$ ならば $-xinT(M)$

を示せばよい。実際、任意の $n \in \mathbb{Z} - \{0\}$ に対して $n0 = 0$ だから 1．は明らか。$x, y \in T(M)$ とすると、$nx = my = 0$ となる $n, m \in \mathbb{Z} - \{0\}$ が存在する。すると $(nm)x = n(mx) = n0 = 0$ となるから 2．がいえた。また $nx = 0$ $n \in \mathbb{Z} - \{0\}$ ならば $n(-x) = 0$ だから、3．もいえた。 □

定義 140. 命題 139 の記号のもとで、

- $T(M) \subset M$ のことを「**捩れ部分加群** (torsion subgroup, torsion submodule)」と呼び、
- $T(M) = \{0\}$ の場合、M を**「捩れのない加群」** (torsion free module) と呼ぶ。
- また、$T(M) = M$ の場合、M を**「捩れ加群」** (torsion module)) と呼ぶ。

命題 141. $\mathbb{Z}$-自由加群 M（およびその部分加群）は、捩れのない $\mathbb{Z}$-加群である。

Proof. もし $T(M) \neq \{0\}$ ならば、ある元 $x \in T(M) - \{0\}$ とある $n \in \mathbb{Z} - \{0\}$ によって、$nx = 0$ となる。M の自由基底を $b_1, \ldots, b_r$ とすると、適当な $n_1, \ldots, n_r \in \mathbb{Z}$ によって

$$x = n_1 b_1 + \ldots + n_r b_r$$

と書き表せるから、両辺に上で選んだ n を掛けて

$$0 = nx = (nn_1)b_1 + \ldots + (nn_r)b_r.$$

すると $b_1, \ldots, b_r$ は自由基底だったから、

$$nn_1 = \cdots = nn_r = 0$$

でなければならない。しかるに $n \neq 0$ だから

$$n_1 = \cdots = n_r = 0$$

すなわち、$x = 0$ となり、$x \in T(M) - \{0\}$ であることに反する。よって $T = \{0\}$, すなわち M は捩れのない加群でなければならない。 □

例 142. 命題 *141* の逆は成り立たない。例えば、$M = \mathbb{Z} \cdot \frac{1}{2} + \mathbb{Z} \cdot \frac{1}{2}$ は自由加群ではないが、$T(M) = \{0\}$ である。

命題 143. M が捩れ加群 (i.e. $T(M) = M$) ならば $\operatorname{rank} M = 0$.

Proof. もし $r = \operatorname{rank} M > 0$ ならば、一次独立な要素 $x_1, \ldots, x_r \in M$ がとれるはず。しかし、$M = T(M)$ だから、適当な要素 $_i \in \mathbb{Z} - \{0\}$ $(i = 1, \ldots, r)$ が存在して $n_i x_i = 0_M$ となる。すなわち、

$$n_1 x_1 + \cdots + n_r x_r = 0_M \qquad (n_1, \ldots, n_r) \neq (0, \ldots, 0).$$

これは $x_1, \ldots, x_r$ が一次独立であることに反する。よって $\operatorname{rank} M = 0$ でなければならない。 □

注意 144 (階数と長さの違い)**.** 命題 *136* より、長さ $\ell(\mathbb{Z}/n\mathbb{Z}) = r$, $(n = p_1 \cdots p_r)$ であった。しかし階数は $\mathrm{rank}(\mathbb{Z}/n\mathbb{Z}) = 0$ となる。実際、任意の要素 $a + n\mathbb{N} \in \mathbb{Z}/n\mathbb{Z}$ に対して

$$\nu(n, a + n\mathbb{N}) = na + n\mathbb{N} = n\mathbb{N} = 0_{\mathbb{Z}/n\mathbb{Z}}$$

となるから、全ての元は捩れ元である。つまり $\mathbb{Z}/n\mathbb{Z}$ は捩れ加群であり、命題 *143* より $\operatorname{rank}\mathbb{Z}/n\mathbb{Z} = 0$ となる。

命題 145. M が捩れの無い $\mathbb{Z}$-加群 (i.e. $T(M) = \{0\}$) だとする。このとき、$\operatorname{rank} M = 0$ であることと、$M = \{0\}$ であることは同値である。

Proof. $M = \{0\}$ ならば、一次独立な部分集合が作れないから、$\operatorname{rank} M = 0$ となることは明らかである (定義 127 参照)。逆に、$\operatorname{rank} M = 0$ と仮定する。もし $M = \{0\}$ ならば、$0_M \neq x \in M$ なる元 x がとれるが、$T(M) = \{0\}$ だから x は捩れ元ではない。つまり $nx = 0_M$ となる $n \in \mathbb{Z}$ は $n = 0$ に限られる。これは $\{x\}$ が一次独立な集合であることにほかならない。つまり $\operatorname{rank} M \geq 1$ となり仮定に反する。よって $M = \{0\}$ でなければならない。 □

10. 有限生成 $\mathbb{Z}$-自由加群の部分加群の構造定理

ここでは、有限生成アーベル群の構造定理を証明するための準備として、次の定理 146 を証明する。これは一言で言って、「$\mathbb{Z}$-自由加群の部分加群はいつも $\mathbb{Z}$-自由加群である」ことを主張している。これは当たり前のように見えて、実は全く当たり前ではなく、証明は難しい。また、「$\mathbb{Z}$-自由加群」の $\mathbb{Z}$ を一般の環 R に代えて「R-自由加群」にすると、この定理は成り立たない。ある意味で有理整数環 $\mathbb{Z}$ の特異な性質を現した定理とも言える。

定理 146. F を有限生成 $\mathbb{Z}$-自由加群、$M \subset F$ を $\mathrm{rank}(M) = n$ なる部分加群とする。このとき

- F の自由基底の一部 $x_1, \ldots, x_n$
- 数列 $0 < \alpha_1 \leq \cdots \leq \alpha_n \in \mathbb{Z}$

で、次のような性質をもつものが存在する：

(1) $\alpha_1 x_1, \ldots, \alpha_n x_n$ は M の自由基底となる（特に、M は $\mathbb{Z}$-自由加群となる）
(2) $\alpha_i \mid \alpha_{i+1}$, $1 \leq i < n$

また、この正整数列 $\alpha_1, \ldots, \alpha_n$ は $x_1, \ldots, x_n$ の選び方によらず、M のみによって一意的に決まる。

証明は非常に長いので、いくつかのステップに分割して述べる。

10.1. $\mathrm{cont}(x)$ とその性質.

$\mathbb{Z}$-自由加群 $F = \mathbb{Z}y_1 \oplus \cdots \mathbb{Z}y_r$ の任意の元 $x = \sum_{j=1}^{r} c_j y_j$ を考える。これは（体上のベクトル空間のときと同じ流儀で）座標表示をすれば $x = (c_1, \ldots, c_r)$ とも表せる。この x に対して

$$\mathrm{cont}(x) = (c_1, \ldots, c_r) \quad [c_1, \ldots, c_r \text{ の GCD(自然数値)}]$$

と定義する。以下に cont の基本性質をいくつか示す。

補題 147. 任意の $x = (x_1, \ldots, c_r) \in F$ に対して、$\varphi(x) = a_1 c_1 + \cdots a_r c_r = \mathrm{cont}(x)$ となるような一次式 $\varphi(X) = a_1 X_1 + \cdots + a_r X_r$ が存在する。

Proof. ユークリッドの互除法定理を繰り返し適用することにより

$$c_1 a_1 + \cdots c_r a_r = (c_1, \ldots, c_r)$$

となるような $a_1, \ldots, a_r \in \mathbb{Z}$ の存在がわかる。従って r 個の変数 $X_1, \ldots, X_r$ についての一次式

$$\varphi(X) = a_1 X_1 + \cdots + a_r X_r \quad (a_1, \ldots, a_r \in \mathbb{Z})$$

をとり、$x = (c_1, \ldots, c_r)$ と座標表示で考えれば、$\varphi(x) = a_1 c_1 + \cdots a_r c_r = \mathrm{cont}(x)$ となる。 □

補題 148. 任意の一次式 $\psi(X)$ に対して $\mathrm{cont}(x) | \psi(x)$.

Proof. 各 j に対して $c_j = c'_j(c_1, \ldots, c_r)$, $c'_j \in \mathbb{Z}$, と書き表すと、$\varphi(X)$ 以外の任意の一次式

$$\psi(X) = b_1 X_1 + \cdots + b_r X_r \quad (b_1, \ldots, b_r \in \mathbb{Z})$$

に対して、

$$\psi(x) = b_1 c_1 + \cdots + b_r c_r = (b_1 c'_1 + \cdots + b_r c'_r)(c_1, \ldots, c_r) = (b_1 c'_1 + \cdots + b_r c'_r)\,\mathrm{cont}(x)$$

だから、任意の一次式 $\psi(X)$ に対して $\mathrm{cont}(x) | \psi(x)$ を得る。 □

集合

$$\mathfrak{Z} = \{\mathrm{cont}(y) \mid y \in F\}$$

は自然数全体の集合 $\mathbb{N}$ の部分集合だから、その最小値が存在する。それを $\mathrm{cont}(x) = \min \mathfrak{Z}$ とおく。このとき

補題 149. 上のようにとった $x \in F$ と任意の $y \in M$ に対して $\mathrm{cont}(x) | \mathrm{cont}(y)$.

Proof. もし、

(*)「任意の一次式 $\psi(X)$ と任意の $y \in M$ に対して、$\varphi(x)|\psi(y)$ であること」

が言えれば、任意の $y \in M$ に対して、補題 147 より $\mathrm{cont}(y) = \psi(y)$ となるような一次式 $\psi(X)$ をとば、ただちに補題 149 を得る。

そこで $(*)$ を示そう。

(1) 任意の $y \in M$ に対して、 $\varphi(x)|\varphi(y)$ である。

Proof. $y \in M$ を任意にとり

$$d = (\varphi(x), \varphi(y))$$

とおく。ユークリッドの互除法定理により $d = a\varphi(x) + b\varphi(y) (= \varphi(ax + by))$ なる $a, b \in \mathbb{Z}$ が存在する。補題 148 より $\mathrm{cont}(ax + by)|\varphi(ax + by)$ だから

$$\mathrm{cont}(ax + by)|d$$

となるが、$d|\varphi(x)$ で、かつ、$\varphi(x) = \mathrm{cont}(x)$ だから、さらに $\mathrm{cont}(ax+by)| \mathrm{cont}(x)$ をえる。従ってとくに $\mathrm{cont}(ac + by) \leq \mathrm{cont}(x)$ だが、$\mathrm{cont}(x) = \min \mathfrak{Z}$ だから結局

$$\mathrm{cont}(ac + by) = \mathrm{cont}(x).$$

したがって $\mathrm{cont}(x)|d$. さらに $d|\varphi(y)$ だから、結局 $\mathrm{cont}(x) = \varphi(x)|\varphi(y)$ をえる。 □

(2) 以下の同値性がいえる：$\varphi(x)|\psi(y) \Leftrightarrow \varphi(x)|\psi\left(y - \frac{\varphi(y)}{\varphi(x)}x\right)$.

Proof. 任意の一次式 $\psi(X)$ に対し、

$$\psi\left(y - \frac{\varphi(y)}{\varphi(x)}x\right) = \psi(y) - \frac{\varphi(y)}{\varphi(x)}\psi(x) = \psi(y) - \frac{\psi(x)}{\varphi(x)}\varphi(y)$$

であることから、補題 147, 補題 148 より $\varphi(x)|\psi(x)$ であることと、1. の結果を使えばよい。 □

(3) しかるに $\varphi\left(y - \frac{\varphi(y)}{\varphi(x)}x\right) = 0$ だから、y を $y - \frac{\varphi(y)}{\varphi(x)}x$ にとりかえることにより、最初から $\varphi(y) = 0$ と思ってよい。(つまり、そのような場合だけ証明しておけば、一般の場合もただちに従うわけである。)

(4) さらに、以下の同値性がいえる：$\varphi(x)|\psi(y) \Leftrightarrow \varphi(x)|\Psi(y)$, ただし、$\Psi(X) = \psi(X) - \frac{\psi(x)}{\varphi(x)}\varphi(X)$

Proof. 上に示した 2. の証明と同様に, 1. より $\varphi(x)|\varphi(y)$, また補題 147, 補題 148 より $\varphi(x)|\psi(x)$ であることを使えば、ただちに分かる。 □

(5) しかるに $\Psi(x) = 0$ だから、ψ を Ψ にとりかえることにより、最初から $\psi(x) = 0$ だと思ってよい。(つまり、そのような場合だけ証明しておけば、一般の場合もただちに従うわけである。)
(6) 上で得られた 3. 5. により $(*)$ のかわりに以下の $(**)$ を示せばよいことがわかった：
　　$(**)$ $\psi(x) = 0$ となる任意の一次式 $\psi(X)$ と $\varphi(y) = 0$ となる任意の $y \in M$ に対して、$\varphi(x)|\psi(y)$.
(7) $(**)$ が成り立つ。

Proof. $d = (\varphi(x), \psi(y))$ とおくと、ユークリッドの互除法定理により $d = a\varphi(x) + b\psi(y)$ となる $a, b \in \mathbb{Z}$ が存在する。そこで

$$\begin{aligned}
&(\varphi + \psi)(ax + by) \\
&= \varphi(ax + by) + \psi(ax + by) = a\varphi(x) + b\varphi(y) + a\psi(x) + b\psi(y) \\
&= a\varphi(x) + b\psi(y) \quad (\varphi(y) = \psi(x) = 0) \\
&= d
\end{aligned}$$

となるから、

$$\mathrm{cont}(ax + by)|d.$$

さらに $d|\varphi(x)$ だから、$\mathrm{cont}(ax + by)|\varphi(x)$ となり、$\mathrm{cont}(ax + by) \leq \varphi(x)$. ところが、補題 147 より $\varphi(x) = \mathrm{cont}(x) = \min \mathfrak{Z}$ だったから、結局

$$\varphi(x) = \mathrm{cont}(ax + by).$$

よって $\varphi(x)|d$. そして $d|\psi(y)$ だから、結局 $\varphi(x)|\psi(y)$ となり $(**)$ を得た。 □

□

10.2. M **の自由基底** $\{\alpha_i x_i\}_i$ **の存在証明.** $n = \mathrm{rank}(M)$ についての数学的帰納法によって、M の $\mathbb{Z}$-自由基底の存在を示そう。

$n = 0$ の時、定理 146 の主張は $M = \{0\}$ であることに他ならない。しかるに、命題 141 より M は捩れの無い加群だから、命題 145 より $M = \{0\}$ となり、確かに $n = 0$ の場合は定理 146 が成り立つことがわかった。

次に $n > 0$ の場合を証明しよう。帰納法の仮定は以下の通り：

> F' を任意の有限生成 $\mathbb{Z}$-自由加群、$M' \subset F$ を $\mathrm{rank}(M) = n - 1$ なる任意の部分加群とする。このとき
> - F' の自由基底の一部 $x_1, \ldots, x_{n-1}$
> - 数列 $0 < \alpha_1 \leq \cdots \leq \alpha_{n-1} \in \mathbb{Z}$
>
> で、次のような性質をもつものが存在する：
> (1) $\alpha_1 x_1, \ldots, \alpha_{n-1} x_{n-1}$ は M' の自由基底となる
> (2) $\alpha_i \mid \alpha_{i+1}$, $1 \leq i < n - 1$

補題 149 より、全ての $y \in M$ に対して $\mathrm{cont}(x)|\,\mathrm{cont}(y)$ となるような $x \in M$ が存在する。そこで補題 147 より、$\varphi(x) = \mathrm{cont}(x)$ となるような一次式 $\varphi(X)$ をとると、

$$x = \varphi(x)x_1 \quad (x_1 \in F)$$

と書ける。さて、F の部分加群 $\mathrm{Ker}\,\varphi = \{y \in F \mid \varphi(y) = 0\}$ を考え $M' = M \cap \mathrm{Ker}\,\varphi$ とおく。この時、

補題 150. $M = \mathbb{Z}x \oplus M'$

Proof. 任意の $y \in M$ に対し

$$y = \frac{\varphi(y)}{\varphi(x)}x + (y - \frac{\varphi(y)}{\varphi(x)}x)$$

と書けるが、補題 149 の証明の 1. で示したように

$$\frac{\varphi(y)}{\varphi(x)}x \in \mathbb{Z}x.$$

また、φ を適用してみれば容易に

$$y - \frac{\varphi(y)}{\varphi(x)}x \in M'$$

とわかる。以上で $M = \mathbb{Z}x + M'$ であることがわかった。

あと、$\mathbb{Z}x \cap M' = \{0\}$ であることを示せばよい（命題 123 参照)。そこで $y \in \mathbb{Z}x \cap M'$ とすると、$y = cx$ $(c \in \mathbb{Z})$ で、かつ、$\varphi(cx) = c\varphi(x) = 0$ となるはずである。さて、命題 141 より M は捩れのない $\mathbb{Z}$-加群であるが、今 $n = \mathrm{rank}(M) > 0$ と仮定しているから、命題 145 により $M \neq 0$ となる。よって $\mathrm{cont}(x) = \varphi(x) \neq 0$ でなければならない（$\mathrm{cont}(x) = \min \mathfrak{Z}$ から、すくなくとも $1 \leq \mathrm{cont}(x)$ とわかる)。従って $c = 0$, すなわち $y = 0$ に限られる。よって $\mathbb{Z}x \cap M' = \{0\}$ となり、$M = \mathbb{Z}x \oplus M'$ であることがわかった。 □

補題 151. $F = \mathbb{Z}x_1 \oplus \mathrm{Ker}\,\varphi$

Proof. 任意の $y \in F$ に対し

$$y = \frac{\varphi(y)}{\varphi(x_1)}x_1 + (y - \frac{\varphi(y)}{\varphi(x_1)}x_1)$$

と書けるが、$x = \varphi(x)x_1$ に φ を作用させると $(\varphi(x) \in \mathbb{Z}$ に注意して$)$ $\varphi(x) = \varphi(x)\varphi(x_1)$ だから、$\varphi(x_1) = 1$ である。従って、

$$\frac{\varphi(y)}{\varphi(x_1)}x_1 = \varphi(y)x_1 \in \mathbb{Z}x_1.$$

また、φ を適用してみることにより、$\varphi(x_1) = 1$ を使えば、容易に

$$y - \frac{\varphi(y)}{\varphi(x_1)}x_1 \in \mathrm{Ker}\,\varphi$$

とわかる。以上で $F = \mathbb{Z}x_1 + \mathrm{Ker}\,\varphi$ であることがわかった。さらに、$y \in \mathbb{Z}x_1 \cap \mathrm{Ker}\,\varphi$ とすると、$y = cx_1$ $(c \in \mathbb{Z})$ で、かつ、$\varphi(cx_)) = c\varphi(x_) = c = 0$ となるはずである。すなわち $y = 0$ に限られる。よって $\mathbb{Z}x_1 \cap \mathrm{Ker}\,\varphi' = \{0\}$ となり、$F = \mathbb{Z}x_\oplus \mathrm{Ker}\,\varphi$ であることがわかった（命題 123 参照)。 □

以上の準備のもとで、$n = \mathrm{rank}\,M > 0$ の場合の証明を行おう。

(1) 補題 150 において $x \neq 0$ だから、$\mathrm{rank}\,M' < n(= \mathrm{rank}\,M)$. 従って、帰納法の仮定により M' は $\mathbb{Z}$-自由加群で $\mathrm{rank}\,M' = n - 1$. 従って再び補題 150 により M は $\mathbb{Z}$-自由加群となる。

(2) また、上と同様に補題 151 に帰納法の仮定を使って $\mathrm{Ker}\,\varphi$ は F の $\mathbb{Z}$-部分自由加群となる。
(3) さらに $M' \subset \mathrm{Ker}\,\varphi$ に帰納法の仮定を適用すれば、$\mathrm{Ker}\,\varphi$ の $\mathbb{Z}$-自由基底 $x_2, \ldots, x_n$ と $\alpha_2, \ldots, \alpha_n \in \mathbb{Z} - \{0\}$ で $\alpha_i | \alpha_{i+1}$ $(2 \leq i < n)$ なるものがあって、$\alpha_2 x_2, \ldots, \alpha_n x_n$ が M' の $\mathbb{Z}$-自由基底になる。
(4) 従って、$x_1, x_2, \ldots, x_n$ が $F = \mathbb{Z}x_1 \oplus \mathrm{Ker}\,\varphi$ の $\mathbb{Z}$-自由基底になり、$\alpha_1 = \varphi(x)$ とおけば、$\alpha_1 x_1, \alpha_2 x_2, \ldots, \alpha_n x_n$ が $M = \mathbb{Z}x \oplus M'$ の $\mathbb{Z}$-自由基底になっている。
(5) あとは、$\alpha_1 | \alpha_2$ であることだけ示せばよい。
(6) x_2 は自由基底のひとつだから、$\varphi_2(x_2) = 1$ となる一次式 φ_2 が存在する。

Proof. x_2 を座標表示すれば $x_2 = (0, 1, 0, \ldots, 0)$ だから、$\varphi_2(X) = X_2$ とおけば $\varphi_2(x_2) = 1$ となる。 □

(7) 補題 148, 補題 149 により、$\varphi(x) | \varphi_2(\alpha_2 x_2)$, すなわち $\alpha_1 | \alpha_2$ を得る

10.3. $\{\alpha_i\}_i$ **の一意性の証明.** M は $\mathrm{rank}\, M = n$ なる $\mathbb{Z}$-自由加群であることが既に示されているので、$\{\alpha_i\}_i$ として異なるものが取れるとすれば、次のような状況である：
F の自由基底の一部が $x_1, \ldots, x_n$ および $y_1, \ldots, y_n$ と 2 通り選べ、それに応じて自然数列 $\{\alpha_i\}_{i=1}^n$ および $\{\beta_i\}_{i=1}^n$ がとれて、

$$M = \bigoplus_{i=1}^{n} \mathbb{Z} \cdot \alpha_i x_i = \bigoplus_{i=1}^{n} \mathbb{Z} \cdot \beta_i y_i.$$

F の自由基底を、上でとったものの残りを埋めて $x_1, \ldots, x_n, x_{n+1}, \ldots, x_r$ または $y_1, \ldots, y_n, y_{n+1}, \ldots, y_r$ ととれば、$F = \bigoplus_{i=1}^{r} \mathbb{Z}x_i = \bigoplus_{i=1}^{r} \mathbb{Z}y_i$ となるから、任意の $a \in \mathbb{Z}$ に対して、$ax_i \leftrightarrow x_i$, $a\alpha_i x_i \leftrightarrow a\alpha_i$ なる対応を考えることにより

$$\mathbb{Z}x_i / \mathbb{Z} \cdot \alpha_i x_i \cong \mathbb{Z}/\alpha_i\mathbb{Z} \qquad (i = 1, \ldots, n)$$

同様に

$$\mathbb{Z}y_i / \mathbb{Z} \cdot \beta_i y_i \cong \mathbb{Z}/\beta_i\mathbb{Z} \qquad (i = 1, \ldots, n)$$

と考えることができる。従って、

$$F/M \cong \left(\bigoplus_{i=1}^{n} \mathbb{Z}/\alpha_i\mathbb{Z} \right) \oplus \bigoplus_{i=n+1}^{r} \mathbb{Z}x_i \cong \left(\bigoplus_{i=1}^{n} \mathbb{Z}/\beta_i\mathbb{Z} \right) \oplus \bigoplus_{i=n+1}^{r} \mathbb{Z}y_i$$

このことから

$$\bigoplus_{i=1}^{n} \mathbb{Z}/\alpha_i\mathbb{Z} \cong \bigoplus_{i=1}^{n} \mathbb{Z}/\beta_i\mathbb{Z} \tag{13}$$

を言うためには、次の補題 152 のようなもう少し精密な議論が必要になる。ポイントは、上の議論で F を使ったかわりに、もう少し小さい $M_{sat} (\subset F)$ という部分加群を考えることにある。

補題 152. 有限生成 $\mathbb{Z}$-自由加群 F とその $\mathbb{Z}$-部分加群 $M \subset F$ に対し、F の自由基底の一部 $x_1, \ldots, x_n$ と $1 < \alpha_1 \leq \cdots \leq \alpha_n \in \mathbb{Z}$ で $\alpha_1 x_1, \ldots, \alpha_n x_n$ が M の $\mathbb{Z}$-自由基底になったとする。この時、$\bigoplus_{i=1}^n \mathbb{Z}x_i \subset F$ は M によって一意的に決まる。すなわち、

$$\bigoplus_{i=1}^n \mathbb{Z}x_i = M_{sat} := \{y \in F \mid \text{適当な } 0 \neq a \in \mathbb{Z} \text{ によって } ay \in M\}$$

となる。さらに

$$M_{sat}/M \cong \bigoplus_{i=1}^n \mathbb{Z}/\alpha_i\mathbb{Z}.$$

Proof. $\alpha_i | \alpha_n$ $1 \leq i < n$ だから、

$$\alpha_n \cdot (\bigoplus_{i=1}^n \mathbb{Z}x_i) = \bigoplus_{i=1}^n \mathbb{Z}\frac{\alpha_n}{\alpha_i}\alpha_i x_i \subset \bigoplus_{i=1}^n \mathbb{Z}\alpha_i x_i = M$$

従ってとくに

$$\bigoplus_{i=1}^n \mathbb{Z}x_i \subseteq M_{sat}$$

となる。逆に、$y \in M_{sat}$ を任意にとる。適当な $0 \neq a \in \mathbb{Z}$ によって $ay \in M$ となる。$x_1, \ldots, x_n$ は F の自由基底の一部だったから、残りを埋めて $x_1, \ldots, x_n, x_{n+1}, \ldots, x_r$ とすると、$y = \sum_{j=1}^r a_j x_j$ と書けるから、

$$ay = \sum_{j=1}^r aa_j x_j \in M = \bigoplus_{j=1}^n \mathbb{Z}\alpha_j x_j$$

となる。従って $aa_{n+1} = \cdots = aa_r = 0$, すなわち $a_{n+1} = \cdots = a_r = 0$ となり、$y \in \bigoplus_{i=1}^n \mathbb{Z}\alpha_i$, i.e.,

$$M_{sat} \subseteq \bigoplus_{i=1}^n \mathbb{Z}x_i.$$

以上により、$M_{sat} = \bigoplus_{i=1}^n \mathbb{Z}x_i$ が得られた。そこで、

$$M_{sat}/M = \bigoplus_{i=1}^n \mathbb{Z}x_i/M = \bigoplus_{i=1}^n \mathbb{Z}x_i/\bigoplus_{i=1}^n \mathbb{Z}\alpha_i x_i = \bigoplus_{i=1}^n (\mathbb{Z}x_i/\mathbb{Z}\alpha_i x_i) \cong \bigoplus_{i=1}^n (\mathbb{Z}/\alpha_i\mathbb{Z})$$

を得る。 □

以上により、(13) の場合に $\alpha_i = \beta_i$ $1 \leq i \leq n$ であることを示せば良いとわかった。そのことは、以下の補題 153 からしたがう。

補題 153. $\mathbb{Z}$-加群 $Q \cong \bigoplus_{i=1}^n \mathbb{Z}/\alpha_i\mathbb{Z}$, $1 < \alpha_1, \ldots, \alpha_n \in \mathbb{Z}$, $\alpha_{i+1} | \alpha_i$ $(\leq i < n)$ を考える。このとき、α_i は、Q によって一意的に決まる。(証明をやりやすくする都合上 α_i の添え字が逆順にしてあることに注意)

Proof. 二通りの選び方があって、

$$Q \cong \bigoplus_{i=1}^{n} \mathbb{Z}/\alpha_i\mathbb{Z} \cong \bigoplus_{j=1}^{m} \mathbb{Z}/\beta_j\mathbb{Z}$$

$\alpha_{i+1}|\alpha_i$ $(\leq i < n)$ および $\beta_{j+1}|\beta_j$ $(\leq j < n)$, となっているとする。

今、仮に

$$k \leq \min\{m, n\}, \quad \alpha_k\mathbb{Z} \neq \beta_k\mathbb{Z}$$

となる k が存在するとしよう。k としてはそのようなものの最小のものをとると、$\alpha_i\mathbb{Z} = \beta_i\mathbb{Z}$ $(1 \leq i < k)$ であり、かつ、

$$\alpha_j|\alpha_k \quad (j = k+1, \ldots, n)$$

となる。従って、

$$\alpha_k Q \cong \bigoplus_{i=1}^{k-1} \alpha_k \cdot (\mathbb{Z}/\alpha_i\mathbb{Z}) \cong \bigoplus_{i=1}^{k-1} \alpha_k \cdot (\mathbb{Z}/\alpha_i\mathbb{Z}) \oplus \bigoplus_{j=k}^{m} \alpha_k \cdot (\mathbb{Z}/\beta_j\mathbb{Z})$$

今 $\ell(Q) < \infty$ だから、上の式より

$$\ell(\bigoplus_{i=1}^{k-1} \alpha_k \cdot (\mathbb{Z}/\alpha_i\mathbb{Z})) = \ell(\bigoplus_{i=1}^{k-1} \alpha_k \cdot (\mathbb{Z}/\alpha_i\mathbb{Z})) + \sum_{j=k}^{m} \ell(\alpha_k \cdot (\mathbb{Z}/\beta_j\mathbb{Z}))$$

すなわち、$\ell(\alpha_k \cdot (\mathbb{Z}/\beta_k\mathbb{Z})) = 0$ となり、、$\alpha_k \cdot (\mathbb{Z}/\beta_k\mathbb{Z}) = 0$ を得る。すなわち、$\alpha_k\mathbb{Z} \subseteq \beta_k\mathbb{Z}$. 同様にして $\beta_k\mathbb{Z} \subseteq \alpha_k\mathbb{Z}$ も示せるから、$\alpha_k\mathbb{Z} = \beta_k\mathbb{Z}$. これは k のとりかたに矛盾する。従って、

$$\alpha_i\mathbb{Z} \neq \beta_i\mathbb{Z} \quad (1 \leq i \leq \min\{m, n\})$$

でなければならない。

ここで $m \leq n$ と仮定しても一般性は失われない。そこで上の議論と同様に

$$\ell(\bigoplus_{j=m+1}^{n} \mathbb{Z}/\alpha_i\mathbb{Z}) = 0$$

となるが、これより $\bigoplus_{j=m+1}^{n} \mathbb{Z}/\alpha_i\mathbb{Z} = 0$ となり、結局 $m = n$ を得る。 □

11. 有限生成アーベル群の基本定理

ここでは 9 章と 10 章の結果を使って、有限生成アーベル群の基本定理を証明する。この定理は特に有限アーベル群の構造を記述するものである。

11.1. **群の直和.** 9.2 節では加群の直和について述べたが、そこでは部分加群の直和の形で述べた。ここでは部分群とは限らない群 $G_1, \ldots, G_n$ をいくつか持ってきて、それらから直和 $G = \bigoplus_{i=1}^n G_i$ をつくる定式化を述べる。一度直和群 G を作ってしまえば、各 G_i は G の部分群になるので、9.2 で述べた定式化と本質的に同じことになる点に注意する。

二つの群 $(G_1, *, 1_{G_1})$, $(G_2, \cdot, 1_{G_1})$ に対して、直積集合

$$G_1 \times G_2 = \{(x, y) \mid x \in G_1,\ y \in G_2\}$$

に対して演算を

$$(x, y) \bullet (x', y') = (x * x', y \cdot y') \qquad (x, y), (x', y') \in G_1 \times G_2$$

と定義すれば、$(1_{G_1}, 1_{G_2})$ が単位元、逆元は $(x, y)^{-1} = (x^{-1}, y^{-1})$ となり、この演算に関して $G_1 \times G_2$ は群になる。このようにして作られた新しい群を

$$G_1 \oplus G_2 := (G_1 \times G_2, \bullet, (1_{G_1}, 1_{G_2})$$

と書き表し、G_1 と G_2 の「**直和 (群)**」と呼ぶ。また、3 個以上の群に対しても同様に直和

$$\bigoplus_{i=1}^n G_i = G_1 \oplus \cdots \oplus G_n$$

を定義することができる。

演習問題 38. 直和群 $G = \bigoplus_{i=1}^n G_i$ の演算を定義せよ。その単位元 1_G や逆元を求めよ。

群の直和 $G = \bigoplus_{i=1}^n G_i$ に対し、群の単射準同型

$$\begin{array}{rccc} \psi_i : & G_i & \longrightarrow & G \\ & x & \longmapsto & (1_{G_1}, \ldots, 1_{G_{i-1}}, x, 1_{G_{i+1}}, \ldots, 1_{G_n}) \end{array} \qquad (i = 1, \ldots, n)$$

によって $G_i \subset G$ と考えることができる。

演習問題 39. 上の ψ_i が群の単射準同型になっていることを確かめよ。

直和については以下の性質が基本的である。

命題 154. 群の直和 $G = \bigoplus_{i=1}^n G_i$ に対し、

(*i*) 任意の $i \neq j$ に対して $G_i \cap G_j = \{1_G\}$

(*ii*) 任意の要素 $g \in G$ は $g = (x_1, \ldots, x_n)$, $x_i \in G_i$, $i = 1, \ldots, n$ の形に一意的に書き表すことができる。

Proof. (*i*) 簡単のため、$i = 1, j = 2$ の場合だけ示そう（一般の場合も同様に示せる）。上に定義した単射準同型 ψ_i によって、

$$\begin{aligned} G_1 &= \{(x, 1_{G_2}, 1_{G_3}, \ldots, 1_{G_n}) \mid x \in G_1\} \\ G_2 &= \{(1_{G_1}, y, 1_{G_3}, \ldots, 1_{G_n}) \mid y \in G_2\} \end{aligned}$$

と書き表せるから、$G_1 \cap G_2 = \{(1_{G_1}, \ldots, 1_{G_n})\} = \{1_G\}$ とわかる。
(ii) 直和の定義から $g \in G$ が $g = (x_1, \ldots, x_n)$, $x_i \in G_i$, $i = 1, \ldots, n$ の形に表せることは明らかだから、一意性の証明をしよう。

$$g = (x_1, \ldots, x_n) = (y_1, \ldots, y_n) \qquad x_i, y_i \in G_i \ (i = 1, \ldots, n)$$

と二通りに表せたとすると、

$$\begin{aligned} 1_G &= gg^{-1} = (x_1, \ldots, x_n)(y_1, \ldots, y_n)^{-1} = (x_1, \ldots, x_n)(y_1^{-1}, \ldots, y_n^{-1}) \\ &= (x_1 y^{-1}, \ldots, x_n y_n^{-1}) \end{aligned}$$

となる（演習 38 参照)。従って、単位元の一意性（命題 24）より、

$$1_{G_i} = x_i y_i^{-1} \quad (i = 1, \ldots, n)$$

でなければならず、これより $x_i = y_i$ $(i = 1, \ldots, n)$ が直ちに従う。 □

11.2. **有限生成アーベル群.** 有限生成アーベル群とは、有限生成 $\mathbb{Z}$-加群 (定義 120) と本質的に同じもので、表記法が乗法的になっているだけである。

定義 155 (有限生成アーベル群)**.** アーベル群 G が「**有限生成** (finitely generated)」であるとは、G の全ての要素 x が、適当な有限個の元 $g_1, \ldots, g_r \in G$ によって

$$x = g_1^{n_1} \cdots g_r^{n_r} \qquad (n_1, \ldots, n_r \in \mathbb{Z})$$

の形で書き表せる場合をいう。特に、有限アーベル群は有限生成アーベル群である (有限生成アーベル群が有限群とは限らないことに注意！)。

例 156 (有限生成の有限アーベル群の例)**.** $\mathbb{Z}/4\mathbb{Z} = \{0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\}$ は全ての要素が、有限個の元 $4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}$ を使って（そのまんま）書き表されるから、有限生成である。あるいは、全ての要素が $1 + 4\mathbb{Z}$ だけを使って書き表せるとも考えらえる。すなわち、

$$\begin{aligned} 0 + 4\mathbb{Z} &= (1 + 4\mathbb{Z}) + (1 + 4\mathbb{Z}) + (1 + 4\mathbb{Z}) + (1 + 4\mathbb{Z}) \\ 1 + 4\mathbb{Z} &= 1 + 4\mathbb{Z} \quad (\text{そのまんま}) \\ 2 + 4\mathbb{Z} &= (1 + 4\mathbb{Z}) + (1 + 4\mathbb{Z}) \\ 3 + 4\mathbb{Z} &= (1 + 4\mathbb{Z}) + (1 + 4\mathbb{Z}) + (1 + 4\mathbb{Z}) \end{aligned}$$

演習問題 40. $\mathbb{Z}/6\mathbb{Z}$ は一つの要素 $j + 6\mathbb{Z}$ だけで生成することができる。このとき j の値として可能なものは何か？(ヒント：$j = 1, 5$ のみが可能。では、$j = 0, 1, 2, 3, 4$ だとどの要素が書き表せないか？)

演習問題 41. 直和群 $G = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ は有限アーベル群だから有限生成である。G が $(1 + 4\mathbb{Z}, 0 + 6\mathbb{Z})$ と $(0 + 4\mathbb{Z}, 1 + 6\mathbb{Z})$ の 2 つの元で生成されることを示せ。

例 157 (有限生成の無限アーベル群の例)**.** 無限アーベル群 $(\mathbb{Z}, +, 0)$ の $d(\geq 1)$ 個の直和

$$\mathbb{Z}^d = \{(x_1, \ldots, x_d) \mid x_i \in \mathbb{Z},\ i = 1, \ldots, d\}$$

はやはり無限アーベル群であり、それらは有限個の要素

$$x_i = (0, \ldots, 0, 1, 0, \ldots, 0) \qquad i \text{ 番目以外は全て } 0)$$

で生成されている。

例 158 (有限生成の無限アーベル群の例)**.** 無限アーベル群 $\mathbb{Z}$ と有限アーベル群の直和

$$\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$$

は無限アーベル群であるが、これらは有限個の要素

$$\begin{aligned} x_1 &= (1, 0+3\mathbb{Z}, 0+4\mathbb{Z}) \\ x_2 &= (0, 1+3\mathbb{Z}, 0+4\mathbb{Z}) \\ x_3 &= (0, 0+3\mathbb{Z}, 1+4\mathbb{Z}) \end{aligned}$$

で生成されているから、有限生成アーベル群である。

定義 159 (自由群)**.** 有限生成 $\mathbb{Z}$-自由加群を乗法的に書き表したものを**自由群** *(free group)* と呼ぶ。すなわち、有限生成アーベル群 G が**自由群**であるとは、適当な生成元 $g_1, \ldots, g_r$ が存在して、

$$g_1^{n_1} \cdot g_2^{n_2} \cdots g_r^{n_r} = 1_G$$

となるような $(n_1, n_2, \ldots, n_r) \in \mathbb{Z}^r$ は

$$(0, 0, \ldots, 0) \in \mathbb{Z}^r$$

に限られる場合、つまり「生成元（またはその逆元）を 1 つ以上使って単位元を表すことはできない」場合をいう。

有限生成アーベル群の構造以下の通り。

定理 160 (有限生成アーベル群の基本定理)**.** 任意の有限生成アーベル群 G に対して、

(1) $d \in \mathbb{N} \cup \{0\}$
(2) 素数 $p_1, \ldots, p_r$
(3) 各 $i = 1, \ldots, r$ に対して、自然数列 $1 \leq \nu(i,1) \leq \cdots \leq \nu(i, q_i)$

が一意的に決まり

$$G \cong F \oplus \bigoplus_{i=1}^{r} \bigoplus_{j=1}^{q_i} G_{i,j}$$

但し、F は d 個の元で生成された自由群で、$G_{i,j}$ は $p_i^{\nu(p_i,j)}$-次の巡回群。特に、G が有限アーベル群の場合は、自由群 F の部分が存在せず、G は素数冪位数の巡回群の直和になっている。

例 161 ($\mathfrak{S}_4$ の位数 2 の部分群)**.** (6.3.1 節参照)

$$\langle (12) \rangle = \{1, (12)\} \xrightarrow{\varphi} \mathbb{Z}/2\mathbb{Z}$$

を $\varphi((12)) = 1 + 2\mathbb{Z}$ と定義すると、これは明らかに全射であり

$$\begin{aligned} \varphi(1) &= \varphi((12)^2) = \varphi((12)) + \varphi((12)) = (1+2\mathbb{Z}) + (1+2\mathbb{Z}) \\ &= 0 + 2\mathbb{Z} \quad (\mathbb{Z}/2\mathbb{Z} \text{ の単位元}) \\ \varphi((12)) &= 1 + 2\mathbb{Z} \neq 0 + 2\mathbb{Z} \end{aligned}$$

となる。従って、

$$\operatorname{Ker} \varphi = \{x \in \langle (12) \rangle \mid \varphi(x) = 0 + 2\mathbb{Z}\} = \{1\}$$

よって、短完全列

$$1 \longrightarrow \{1\} \longrightarrow \langle(12)\rangle \xrightarrow{\varphi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1$$

を得る。剰余群の同型 $\langle(12)\rangle/\{1\} \cong \langle(12)\rangle$ を使って、準同型定理により

$$\langle(12)\rangle \cong \mathbb{Z}/2\mathbb{Z}$$

を得る。同様にして、

$$\langle(13)\rangle \cong \langle(14)\rangle \cong \langle(23)\rangle \cong \langle(24)\rangle \cong \langle(34)\rangle \cong \mathbb{Z}/2\mathbb{Z}$$

を得る。

演習問題 42. 例 161 に出てきた、以下の同型を示せ。

$$\langle(12)\rangle/\{1\} \cong \langle(12)\rangle.$$

(ヒント:一般に群 G と単位元だけからなる群 $N = \{1_G\}$ に対して、$G/N = G/\{1_G\} = \{g_1N, g_2N, \ldots\} = \{\{g_1\}, \{g_2\}, \ldots,\}$. そこで、$\{g_i\} \in G/N$ に $g_i \in G$ を対応させる写像を ψ とすれば、これは群の同型になる。)

演習問題 43. $\mathfrak{S}_4$ の位数 *2* の部分群は、例 161 に出てきたものの他に、

$$\langle(12)(34)\rangle, \langle(13)(24)\rangle, \langle(14)(23)\rangle$$

があった、これらも $\mathbb{Z}/2\mathbb{Z}$ と同型であることを示せ。(ヒント： 例 161 の方法を真似ればよい。)

演習問題 44 ($\mathfrak{S}_4$ の位数 3 の部分群)**.** (6.3.2 節参照) $\mathfrak{S}_4$ の位数 *4* のアーベル部分群

$$\begin{aligned} D_1 &= \langle(234)\rangle = \{1, (234), (243)\}, \\ D_2 &= \langle(134)\rangle = \{1, (134), (143)\}, \\ D_3 &= \langle(124)\rangle = \{1, (124), (142)\}, \\ D_4 &= \langle(123)\rangle = \{1, (123), (132)\} \end{aligned}$$

について、

$$D_1 \cong D_2 \cong D_3 \cong D_4 \cong \mathbb{Z}/3\mathbb{Z}$$

であることを示せ。(ヒント：D_i は全て 3 次の巡回群だったが、その生成元を $\mathbb{Z}/3\mathbb{Z}$ の生成元に対応される写像 φ を作り、それが同型写像になっていることを示す。例えば、$\varphi : D_1 \to \mathbb{Z}/3\mathbb{Z}$ は $\varphi((234)) = 1 + 3\mathbb{Z}$ として、φ が全射で $\operatorname{Ker}\varphi = \{1\}$ であることを示せば、準同型定理により $D_1 \cong \mathbb{Z}/3\mathbb{Z}$ がいえる。)

演習問題 45 ($\mathfrak{S}_4$ の位数 4 の部分群 (1))**.** (6.3.3 節参照) $\mathfrak{S}_4$ の位数 *4* の部分群

$$\begin{aligned} Z_1 &= \langle(1234)\rangle = \{1, (1234), (13)(24), (1432)\} \\ Z_2 &= \langle(1342)\rangle = \{1, (1342), (14)(23), (1243)\} \\ Z_3 &= \langle(1423)\rangle = \{1, (1423), (12)(34), (1324)\} \end{aligned}$$

はいずれも $\mathbb{Z}/4\mathbb{Z}$ に同型であることを示せ。(ヒント：Z_i はいずれも巡回群だから、その生成元を $\mathbb{Z}/4\mathbb{Z}$ の生成元 $1 + 4\mathbb{Z}$(または $3 + 4\mathbb{Z}$) に対応させる写像 φ を考え、それが全射であること $\operatorname{Ker}\varphi = \{1\}$ であることを確かめ、準同型定理をつかう。)

演習問題 46. $\mathfrak{S}_3$ の $\{1\}$ 以外の真の部分アーベル群は、全て $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ であることを示せ。(ヒント：4.1 節参照。)

巡回部分群以外の例として、次のものを考えてみよう。

例 162 ($\mathfrak{S}_4$ の位数 4 の部分群 (2))**.** (6.3.3 節参照) クラインの 4 元群

$$\mathfrak{B}_4 = \{1, (12)(34), (13)(24), (14)(23)\}$$

に対して、

$$\begin{array}{rccc} \varphi: & \mathfrak{B}_4 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \\ & (12)(34) & \longmapsto & (1+2\mathbb{Z}, 0+2\mathbb{Z}) \\ & (13)(24) & \longmapsto & (0+2\mathbb{Z}, 1+2\mathbb{Z}) \end{array}$$

と置けば、準同型写像であること、および $(14)(23) = (12)(34)(13)(24)$ と $1 = (12)(34)(12)(34)$ を使って

$$\begin{array}{rcl} \varphi((14)(23)) & = & \varphi((12)(34)(13)(24)) = \varphi((12)(34)) + \varphi((13)(24)) \\ & = & (1+2\mathbb{Z}, 0+2\mathbb{Z}) + (0+2\mathbb{Z}, 1+2\mathbb{Z}) \\ & = & (1+2\mathbb{Z}, 1+2\mathbb{Z}) \\ \varphi(1) & = & \varphi((12)(34)(12)(34)) = \varphi((12)(34)) + \varphi((12)(34)) \\ & = & (1+2\mathbb{Z}, 0+2\mathbb{Z}) + (1+2\mathbb{Z}, 0+2\mathbb{Z}) \\ & = & (0+2\mathbb{Z}, 0+2\mathbb{Z}) \quad (\text{単位元}) \end{array}$$

を得る。従って、φ は全射、かつ、$\operatorname{Ker}\varphi = \{1\}$ となり、準同型定理より

$$\mathfrak{B}_4 \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

を得る。

演習問題 47. $\mathfrak{S}_4$ の位数 *4* の他のアーベル部分群

$$\begin{array}{rcl} V_1 & = & \{1, (12), (34), (12)(34)\} \\ V_2 & = & \{1, (13), (24), (13)(24)\} \\ V_3 & = & \{1, (14), (23), (14)(23)\} \end{array}$$

についても、$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ であることを示せ。(ヒント：例 162 の方法を真似る。)

11.3. **基本定理の証明.** 基本定理を $\mathbb{Z}$-加群の言葉で言い換えた下記のものを証明する。

定理 163 (有限生成アーベル群の基本定理 ($\mathbb{Z}$-加群版))**.** 任意の有限生成 $\mathbb{Z}$-加群 M に対して、

(1) $d \in \mathbb{N} \cup \{0\}$
(2) 素数 $p_1, \ldots, p_r$
(3) 各 $i = 1, \ldots, r$ に対して、自然数列 $1 \leq \nu(i,1) \leq \cdots \leq \nu(i,q_i)$

が一意的に決まり

$$M \cong \mathbb{Z}^d \oplus \bigoplus_{i=1}^{r} G_i, \qquad \text{ただし} \quad M_i = \bigoplus_{j=1}^{q_i} \mathbb{Z}/p_i^{\nu(i,j)}\mathbb{Z}$$

となる。

この定理は以下の 2 つの命題から直ちに得られる。

命題 164. 有限生成 $\mathbb{Z}$-加群 M とその捩れ部分加群 $T(M) \subset M$ を考える。このとき、
(i) $T(M)$ は有限生成である
(ii) ある部分自由加群 $F \subset M$ が存在して、
(a) $M = T(M) \oplus F$
(b) $\operatorname{rank} M = \operatorname{rank} F$
となる。特に $T(M) = \{0\}$ ならば、M は自由加群になる。

Proof. M の生成元集合を $z_1, \ldots, z_r$ とする：$M = \mathbb{Z}z_1 + \cdots \mathbb{Z}z_r$. そこで $\mathbb{Z}$-自由加群からの全射 $\mathbb{Z}$-準同型写像 f を

$$\begin{array}{rccl} f: & \bigoplus_{i=1}^{r} \mathbb{Z}e_i & \longrightarrow & M \\ & e_i & \longmapsto & z_i \quad (i = 1, \ldots, n) \end{array}$$

と定義すると、準同型定理 (定理 105) により

$$M \cong \bigoplus_{i=1}^{n} \mathbb{Z}e_i / \operatorname{Ker} f.$$

そこで、$\operatorname{Ker} f \subset \mathbb{Z}^r$ に定理 146 を適用すると、数列 $0 < \alpha_1 < \cdots < \alpha_n \in \mathbb{Z}$ が一意的に存在して $(n \leq r)$

$$\operatorname{Ker} f = \bigoplus_{i=1}^{n} \mathbb{Z}\alpha_i e_i$$

と書ける。従って、

$$\begin{aligned} M &\cong \bigoplus_{i=1}^{r} \mathbb{Z}e_i / \bigoplus_{i=1}^{n} \mathbb{Z}\alpha_i e_i \cong \bigoplus_{i=n+1}^{r} \mathbb{Z}e_i \oplus \bigoplus_{i=1}^{n} \mathbb{Z}e_i / \bigoplus_{i=1}^{n} \mathbb{Z}\alpha_i e_i \\ &\cong \bigoplus_{i=n+1}^{r} \mathbb{Z}e_i \oplus \bigoplus_{i=1}^{n} (\mathbb{Z}e_i / \mathbb{Z}\alpha_i e_i) \cong \bigoplus_{i=n+1}^{r} \mathbb{Z}e_i \oplus \bigoplus_{i=1}^{n} \mathbb{Z}/\mathbb{Z}\alpha_i. \end{aligned}$$

ここで $T(M) = \bigoplus_{i=1}^{n} \mathbb{Z}/\mathbb{Z}\alpha_i$, および、$\operatorname{rank} M = \bigoplus_{i=r+1}^{n} \mathbb{Z}e_i$ を得る。 □

命題 165. 有限生成な捩れ $\mathbb{Z}$-加群 M と素数 p に対して

$$M_p = \{x \in M \mid \text{適当な } n \in \mathbb{N} \text{ に対して } p^n x = 0\}$$

とすると、

$$M = \bigoplus_{p:\text{素数}} M_p$$

となる。ただし、有限個の p を除いて $M_p = \{0\}$ となり、上の直和は有限和になっている。さらに、$M_p \neq \{0\}$ となる各素数 p に対して、整数列

$$1 \leq \nu(p,1) \leq \cdots \leq \nu(p,r_p)$$

と自然数 r_p が一意的に存在して、

$$M_p \cong \bigoplus_{j_p=1}^{r_p} \mathbb{Z}/p^{\nu(p,j_p)}\mathbb{Z}$$

と書き表される。

Proof. 命題 164 により、

$$M \cong \bigoplus_{i=1}^{n} \mathbb{Z}/\alpha_i\mathbb{Z}.$$

そこで $\alpha_i = \prod_{p:\text{素数}} p^{\nu(p,i)}$ と素因数分解すると、中国人剰余定理 (補題 133) より

$$\mathbb{Z}/\alpha_i\mathbb{Z} \cong \bigoplus_{p:\text{素数}} \mathbb{Z}/p^{\nu(p,i)}\mathbb{Z}$$

となるから、

$$M \cong \bigoplus_{p:\text{素数}} \bigoplus_{i=1}^{n} \mathbb{Z}/p^{\nu(p,i)}\mathbb{Z}.$$

ここで明らかに $\bigoplus_{i=1}^{n} \mathbb{Z}/p^{\nu(p,i)}\mathbb{Z} \subset M_p$. 一方、素数 $q \neq p$ に対して、$p \in \mathbb{Z}$ の自然準同型

$$\mathbb{Z} \longrightarrow \mathbb{Z}/q^r\mathbb{Z}$$

による像 $p + q^{\mathbb{Z}}$ は可逆元である（実際、$(p, q^r) = 1$ だから、ユークリッドの互除法により $xp + yq^r = 1$ となる $x, y \in \mathbb{Z}$ が存在するから、$\mathbb{Z}/q^r\mathbb{Z}$ の中で $xp = 1$ が成り立つから)。従って $\bigoplus_{i=1}^{n} \mathbb{Z}/p^{\nu(p,i)}\mathbb{Z} \supset M_p$ を得、結局

$$\bigoplus_{i=1}^{n} \mathbb{Z}/p^{\nu(p,i)}\mathbb{Z} \cong M_p$$

となる。ここで $\nu(p,i) = 0$ となる項に対しては $ZZ/p^{\nu(p,i)}\mathbb{Z} = ZZ/\mathbb{Z} = 0$ となるから、上の直和から除いてしまってもよいから、

$$M_p \cong \bigoplus_{i=j_p}^{r_p} \mathbb{Z}/p^{\nu(p,j_p)}\mathbb{Z} \qquad (1 \leq \nu(p,1) \leq \cdots \leq \nu(p,r_p))$$

とできる。一意性については補題 153 から従う。 □

12. Sylow 群

12.1. **p-群、p-Sylow 群、Sylow の定理.** 有限生成アーベル群の基本定理 (定理 160) は、特に有限アーベル群の構造を明らかにするものであった。ここでは、アーベル群とは限らない有限群の構造を示す重要な結果として、Sylow の定理を証明する。

定義 166 (p-群)**.** 有限群 G が「**p-群** (p-group)」であるとは、位数が p の冪 $\sharp G = p^k$ $(\mathbb{Z} \ni k \geq 0)$, である場合をいう。(特に、単位元だけからなる部分群 $\{1_G\}$ も p-群と考える)。

定義 167 (p-Sylow 群)**.** 有限群 G の部分群 $H \subset G$ が「**p-Sylow 群** (p-Sylow group)」であるとは、H が p-群であり、$\sharp H = p^k$ とすると $\sharp G = p^k m$ で $p \nmid m$, すなわち指数 $(G : H)$ が p で割り切れない場合をいう。

演習問題 48. p-群 G の任意の要素の位数は常に p の冪であることを示せ。(ヒント: $x \in G$ を任意にとり、x で生成された巡回部分群 $\langle x \rangle \subset G$ を考え、Lagrange の公式 (系 50) を使う。)

演習問題 49. 有限群 G の *p-Sylow* 群 $H \subset G$ に対し、H を真に含む p-群は存在しないことを示せ。(ヒント：$\sharp H = p^k$ および $\sharp G = p^k m$, $p \nmid m$ と考えてよい。そこで、K が H を真に含む p-群だとすると、$H \subset K$ かつ $\sharp K^\ell$, $k < \ell$ となるが、Lagrange の公式 (系 50) よりそれは矛盾とわかる。)

定義 168 (内部自己同型)**.** (有限とは限らない) 群 G と任意の要素 $g \in G$ に対して、写像

$$int_g : \begin{array}{ccc} G & \longrightarrow & G \\ h & \mapsto & ghg^{-1} \end{array}$$

のことを「**内部自己同型（写像）**」(inner automorphism) と呼ぶ。任意の部分群 $H \subset G$ の int_g による像は H と共役であり *(*定義 *93* 参照)、特に命題 *94* により int_g は同型写像である。

定理 169 (Sylow)**.** 有限群 G と素数 p に対し

- (i) G は *p-Sylow* 群を含む。さらに、任意の p-部分群 H は、ある *p-Sylow* 群 S に含まれる：$H \subset S \subset G$.
- (ii) G の全ての *p-Sylow* 群は互いに共役である。
- (iii) G に含まれる *p-Sylow* 群の個数を s とすると、$s | \sharp G$ かつ $s \equiv 1 \pmod{p}$ となる。

例 170. 4 次置換群 $\mathfrak{S}_4$ の位数は $4! = 2^3 3$ だったから、*Sylow* の定理より位数 8 の *2-Sylow* 群と位数 3 の *3-Sylow* 群が存在するはずである。実際、位数 8 の部分群は P_1, P_2, P_3 と呼ばれる部分群の合計 *3* 個 $(3 \equiv 1 \pmod 2)$ であり (6.3.5 節参照)、これらは命題 *96* によれば互いに共役であった。また、位数 3 の部分群は D_1, D_2, D_3, D_4 と呼ばれる部分群の合計 *4* 個 $(4 \equiv 1 \pmod 3)$ であり (6.3.2 節参照)、これらも命題 *96* によれば互いに共役であった。

12.2. **群の集合への作用.** ここでは Sylow の定理の証明で重要な役割を果たす「群の集合への作用」という概念を定義する。この概念は、Sylow の定理だけではなく、数学のはば広い分野で現れる基本概念である。

定義 171 (群の集合への作用)**.** 集合 X に対する群 G の「**作用**」(action) とは、次のような写像

$$\begin{array}{rccc} \mu: & G\times X & \longrightarrow & X \\ & (g,x) & \longmapsto & \mu(g,x) \end{array}$$

のことをいう：

(i) 任意の $x\in X$ に対して $\mu(1_G,x)=x$

(ii) 任意の $g,h\in G,\ x\in X$ に対して $\mu(gh,x)=\mu(g,\mu(h,x))$.

このとき、$x\in X$ に対して

$$G(x):=\{\mu(g,x)\mid g\in G\}\ (\subset X)$$

のことを x の G による「**軌道**」(orbit) と呼ぶ。また、

$$G_x:=\{g\in G\mid \mu(g,x)x=x\}\ (\subset G)$$

のことを x の「**不変部分群**」(isotropy group) と呼ぶ。

上の定義で、単に $g\cdot x$ と書いたものが実際何であるかによって、色々な作用を定義することができる。

例 172 (自明な作用)**.**

$$\begin{array}{rccc} \mu: & G\times X & \longrightarrow & X \\ & (g,x) & \longmapsto & x \end{array}$$

すなわち、$\mu(g,x)=x\ (g\in G)$ と定義したものを「**自明な作用**」(trivial action) と呼ぶ。これはどんな群 G と集合 X についても考えることができる。

例 173. 任意の群 G に対して $X:=G$ として、

$$\begin{array}{rccc} \mu_l: & G\times G & \longrightarrow & X \\ & (g,h) & \longmapsto & \mu_l(g,h)=gh \end{array}$$

を**左変換** (left translation) と呼び、

$$\begin{array}{rccc} \mu_r: & G\times G & \longrightarrow & X \\ & (g,h) & \longmapsto & \mu_r(g,h)=hg \end{array}$$

を**右変換** (right translation) 呼ぶ。いずれも群の作用になっていることがわかる。

例 174 (内部自己同型)**.** 群 G に対して、内部自己同型写像を使って

$$\begin{array}{rccc} int: & G\times G & \longrightarrow & X \\ & (g,h) & \longmapsto & int_g(h)=ghg^{-1} \end{array}$$

なる写像を考えれば、これも群 G の集合 $X:=G$ への作用になっている。

X として群以外の集合を考える典型例として、以下のものがある。

例 175 (ガロア群の拡大体への作用)**.** (有理数体 $\mathbb{Q}$ を含む) 基礎体 K の上の n 次の代数方程式 $f(x)=0$ の解 $\alpha_1,\dots,\alpha_n$ によって、分解体 $L=K(\alpha_1,\dots,\alpha_n)$ を考える。この時、$G:=\mathrm{Gal}\,(L/K),\ X:=L$ とおけば、ガロア群 G の分解体 X への作用は、まさにここで定義した群の作用になっている。

例 176 (線形変換群)**.** 幾何学でよく考えられる群の作用として、例えば次のようなものがある。

$$\begin{aligned} G &= GL(2,\mathbb{R}) \\ &= \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \mid a_{11}a_{22} \neq a_{12}a_{21}, a_{ij} \in \mathbb{R}, 1 \leq i,j \leq 2 \right\}, \end{aligned}$$

および、$X = \mathbb{R}^2$ とし、

$$\begin{array}{ccc} GL(2,\mathbb{R}) \times \mathbb{R}^2 & \longrightarrow & \mathbb{R}^2 \\ (g, \mathbf{x}) & \longmapsto & g\mathbf{x} \end{array}$$

を考えると、これは G の X に対する作用になっている。ただし、ここで $g\mathbf{x}$ は行列 g と列ベクトル $\mathbf{x}$ の積とする。$GL(2,\mathbb{R})$ は 2 次の**一般線形群** (general linear group) と呼ばれ、行列の積に関する群である。

演習問題 50 (特殊線形群)**.**

$$SL(2,\mathbb{R}) = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \mid a_{11}a_{22} - a_{12}a_{21} = 1, a_{ij} \in \mathbb{R}, 1 \leq i,j \leq 2 \right\}$$

は 2 次の**特殊線形群** (special linear grou) と呼ばれる。$SL(2,\mathbb{R})$ が行列の積に関して群になっていることを示せ。(ヒント：行列の積によって「行列式 $= 1$」という性質が保存されることに注意。)

軌道の性質として以下重要であり、軌道に関するあらゆる考察の基礎になる。

命題 177. 群 G が集合 X に作用しているとする。このとき、$X = \bigcup_{x \in X} G(x)$ となり、これは *disjunctive union,* すなわち相異なる軌道 $G(x)$, $G(y)$ は交わらない：$G(x) \cap G(y) = \emptyset$ (if $x \neq y$).

Proof. $G(x)$ の定義より $G(x) \subset X$ だから、$\bigcup_{x \in X} G(x) \subset X$ は明らか。逆に、任意の $x \in X$ に対して $G(x) \ni \mu(x, 1_G) = x$ だから、$x \in \bigcup_{x \in X} G(x)$. すなわち $X \subset \bigcup_{x \in X} G(x)$. よって $X = \bigcup_{x \in X} G(x)$.

次に、$G(x) \cap G(y) \neq \emptyset$ だと仮定する。$z \in G(x) \cap G(y)$ を任意のとると、軌道の定義より $z = \mu(g,x) = \mu(h,y)$ となるような $g, h \in G$ が存在する。すると、

$$\mu(h^{-1}, z) = \mu(h^{-1}, \mu(h,y)) = \mu(h^{-1}h, y) = \mu(1_G, y) = y$$

となるから、

$$\mu(h^{-1}g, x) = \mu(h^{-1}, \mu(g,x)) = \mu(h^{-1}, z) = y.$$

すると、任意の $w \in G(y)$ に対して、$w = \mu(k,y)$ $(k \in G)$ と書けるが、さらに上の結果を使うと

$$w = \mu(k,y) = \mu(k, \mu(h^{-1}g, x)) = \mu(kh^{-1}g, x)$$

となり、結局 $w \in G(x)$, すなわち $G(y) \subseteq G(x)$ となる。同様にして逆の包含関係 $G(x) \subseteq G(y)$ も言えるから、$G(x) = G(y)$ となり、$G(y)$ と $G(y)$ が相異なるという仮定に反する。従って、$G(x) \cap G(y) = \emptyset$ でなければならない。 □

命題 178. 有限群 G が有限集合 X に作用しているとする。命題 177 より $X = \bigcup_{x\in G} G(x)$ となるが、X は有限だから、和集合をとる $G(x)$ としては有限個のもの $G(x_1), \ldots, G(x_n)$ で十分である。このとき、

$$\sharp X = \sum_{i=1}^{n} \sharp G(x_i) = \sum_{i=1}^{n} (G : G_{x_i}).$$

Proof. 各 $x \in G$ に対して $\sharp G(x) = (G : G_x)$ であることを示せばよい。写像 φ を

$$\varphi : G \longrightarrow G(x), \quad g \longmapsto gx \tag{14}$$

と定義する。この時、

$$\begin{aligned} \varphi(g) = \varphi(h) &\Leftrightarrow gx = hx \Leftrightarrow h^{-1}gx = x \Leftrightarrow h^{-1}g \in G_x \Leftrightarrow g \in hG_x \\ &\Leftrightarrow gG_x = hG_x \end{aligned}$$

となる (最後の $\Leftrightarrow$ については演習問題 51 参照)。従って、$G/G_x x$ (G_x の G における左剰余類の集合) に対して、

$$G/G_x \ni gG_x \overset{\tilde{\varphi}}{\mapsto} \varphi(g) \in G(x)$$

なる対応 $\tilde{\varphi}$ を考えると、左剰余類の代表限 g の取り方によらずに写像の値 $\varphi(g)$ がきまる（つまり写像は写像として正しく定義される)。

この写像 $\tilde{\varphi}$ が単射であることは、上に示した $\varphi(g) = \varphi(h)$ の同値条件から明らか。また、任意の $gx \in G(x)$ に対して $gG_x \in G/G_x$ をとれば $\tilde{\varphi}(gG_x) = gx$ となることから、全射であることもわかる。よって、

$$G/G_x \cong G(x) \quad (\text{全単射})$$

となり、これから直ちに

$$(G : G_x) = \sharp(G/G_x) = \sharp G(x)$$

を得る。 □

演習問題 51. 群 G の部分群 $H \subset G$ を考える。$g \in H$ に対して $gH = H$ であることを示せ。また、$g, h \in G$ に対して、$h \in gH$ ならば、$hH = gH$ であることを示せ。(ヒント：前半は、任意の $k \in H$ に対して $k = gg^{-1}k \in gH$ であることを使う。後半は、$HH \subset H$ より $hH \subset gH$ が従うが、逆の包含関係は $h \in gH$ であることから $h = gk$ $(k \in H)$ と書き表せるから $g = hk^{-1}$ となるが、このことから $g \in hH$ を導く。)

12.3. **Sylow の定理の証明.** いくつかのステップの分けて証明する。

12.3.1. p-部分群の個数. ここでは以下の補題を証明する。

補題 179. 有限群 G と素数 p に対して、$n = \sharp G = p^k m$ （ただし、$p \mid m$ であってもよい）とする。このとき、$\sharp H = p^k$ なる p-部分群 $H \subset G$ の個数を s とすると

$$s \equiv \binom{n-1}{p^k - 1} = \frac{1}{m}\binom{n}{p^k} \pmod{p}.$$

補題 179 の証明. **Step 1:** G の部分集合（部分群とは限らない!）U で、$\sharp U = p^k$ なるものを全て集めた集合を X とおく: $X = \{U \mid U \subset G(\text{部分集合}),\ \sharp U = p^k\}$. このとき、

$$\sharp X = \binom{n}{p^k}.$$

G の X への左作用

$$G \times X \ni (g, U) \longmapsto gU = \{gu \mid u \in G\} \in X$$

を考える。すると U の不変部分群は $G_U = \{g \in G \mid gU = U\}$ となるから、G_U は U に次のように作用していることになる：

$$G_U \times U \ni (g, u) \longmapsto gu \in U.$$

この作用において $g \in G_U$ を動かすことにより、$G_U u \subset U$ とわかる。また、$1_G \in G_U$ だから任意の $u \in U$ に対して $G_U u \ni u$. すなわち、$G_U U \supset U$. 以上により、左分解

$$U = \bigcup_{u \in U} G_U u$$

が得られ、命題 46 よりこれは disjoint union であり、また、$\sharp G_U u = \sharp G_U$. ここで $\sharp U = p^k$ だったから、$\sharp G_U = p^{k'}$ $(k' \leq k)$ となっていることがわかる。特に、上の左分解の左剰余類が 1 つだけならば、$\sharp G_U = \sharp U = p^k$ となる。

Step 2: 次に、G の X への作用による軌道分解

$$X = \bigcup_{U \in X} G \cdot U = \bigcup_{i=1}^{r} G \cdot U_i$$

を考える。ここで、X は有限集合だから、最初の和集合の中から相異なる $G \cdot U$ だけを取ってくると有限個になる。そのことを 2 番目の和集合で表している。すると命題 178 より

$$\binom{n}{p^k} = \sharp X = \sum_{i=1}^{n} \sharp G(U_i) = \sum_{i=1}^{r} (G : G_{U_i}).$$

Step 3: Step 1 でみたように、$\sharp G_{U_i} = p^{k_i}$, $(k_i \leq k)$ とおくことができるから、Lagrange の公式 (系 50) より

$$(G : G_{U_i}) = \sharp G / p^{k_i} = p^{k - k_i} m.$$

そこで、$I = \{i \mid 1 \leq i \leq r, k_i = k\}$ とおくと、$i \in I$ に対して $(G : G_{U_i}) = m$ となるから

$$\sharp I \cdot m = \sum_{i \in I} (G : G_{U_i}) \equiv \binom{n}{p^k} \pmod{pm}$$

となる（実際、上式の右辺から左辺を引いた式は $\sum_{i \notin I} (G : G_{U_i})$ であるが、これは $p^t m$ $(t \geq 1)$ の形をした値の和に他ならないから、pm の倍数になって

いる)。従って、この式の両辺を m で割って $n = p^k m$ を使って二項係数を計算すると

$$\sharp I \equiv \frac{1}{m}\binom{n}{p^k} = \frac{1}{m} \cdot \frac{p^k m \cdot (n-1)!}{p^k(p^k-1)!(n-p^k)} = \binom{n-1}{p^k-1} \pmod{p}$$

従って、あとは $\sharp I$ が位数 p^k の p-部分群の個数であることを示せばよい。

Step 4: $\sharp H = p^k$ なる任意の p-群 $H \subset G$ に対して、G の左分解 $G = \bigcup_{g\in G} gH$ が disjoint union で $\sharp gH = \sharp H = p^k$ (命題 46) だから、軌道 $G(H) = \{gH \mid g \in G\}$ はちょうど m 個の要素を持つはずである (Lagrange の公式 (系 50))．また、$\sharp H = \sharp H'$ なる相異なる p-群 $H, H' \subset G$ に対して、仮に $g'H = g''H' \in G(H) \cap G(H')$ $(g', g'' \in G)$ が成り立っているとする。すると、$gH = H'$ $(g := g'g''^{-1} \in G)$. そこで $1_G \in H' = gH$ より $1_G = gg^{-1}$, $g^{-1} \in H$. そして H は部分群だから $g \in H$. よって $gH = H = H'$ となってしまい、仮定に反する。従って $G(H) \cap G(H') = \emptyset$ でなければならない。以上により、$i \in I$ に対して $\sharp G(U_i) = (G : G_{U_i}) = m$ だったが、$\sharp H = p^k$ なる p-群 H はこのような $G(U_i)$ のいずれかに 1 つだけ含まれている：$G(H) = G(U_i)$.

Step 5: 逆に、任意の U_i $(i \in I)$ に対して、$\sharp H = p^k$ なる p-群が存在して、$G(U_i) = G(H)$ であることを示そう。$(G : G_{U_i}) = m$ で $\sharp G = p^k m$ だから、(Lagrange の公式 (系 50)) より $\sharp G_{U_i} = p^k$. いっぽう、**Step 1** でみたように、$U_i = \bigcup_{u\in U_i} G_{U_i} \cdot u$ (disjoint union) だが、$\sharp U_i = p^k = \sharp G_{U_i} \cdot u$ $(u \in U_i)$ より、結局 $U_i = G_{U_i} \cdot u_i$ $(u_i \in U_i)$ となる。そこで、

$$G(U_i) = G(u_i^{-1} \cdot U_i) = G(u_i^{-1} \cdot G_{U_i} \cdot u_i)$$

となるが、$H := u_i^{-1} \cdot G_{U_i} \cdot u_i (\cong G_{U_i})$ とおけば、これは位数 p^k の p-部分群である。

□

12.3.2. 巡回群の部分群と *p-Sylow* 群の個数. ここでは補題 179 をより精密化するために、下記の結果を示す。

命題 180. 有限群 G が巡回群であるとする。この時、任意の自然数 d で $d|\sharp G$ なるものに対して、$H \subset G$, $\sharp H = d$, となるような部分群 H が必ず唯一つ存在する。

Proof. $G = \langle a \rangle$ で $\sharp G = n$ であるとすると。$a^n = 1_G$. そこで $d|n$ とすれば、$b := a^{\frac{n}{d}} \in G$ は位数 d の元である。従って、$H = \langle b \rangle (\subset G)$ とおけば、これは位数 d の部分群。逆に、部分群 $K \subset G$ の位数 $\sharp K = d$ だとする。巡回群はアーベル群だから、剰余群 G/K が作れ、その位数は (Lagrange の公式 (系 50)) より $\frac{n}{d}$, そして自然準同型

$$\varphi : G = \langle a \rangle \longrightarrow G/K$$

を考えれば、$G/K = \langle \varphi(a) \rangle$ となっている。$\varphi(a)^{\frac{n}{d}} = 1_{G/K}$ だから、$a^{\frac{n}{d}} \in K$. ところがこれは上で考えた b と同じ元である。つまり、この元だけで d 次巡回群が作れてしまう：$\langle a^{\frac{n}{d}} \langle \subset K$ かつ $\sharp \langle a^{\frac{n}{d}} \langle = \sharp K = d$. つまり、$K = \langle b \rangle$ となり、位数 d の部分群はこの 1 つに限られる。 □

補題 179 で得られた式、

$$s \equiv \binom{n-1}{p^k-1} = \frac{1}{m}\binom{n}{p^k} \pmod{p}.$$

において、右辺は群 G の構造には全く関係なく、位数 $\sharp G = p^k m$ のみで決まる量である。しかるに s は群 G の構造によって変わりうる値である。そして補題 179 は、いかに G の構造が変わって s の値が変化しようと、mod p では必ず等しいことを主張する。従って、特に G が巡回群でも上の式が成り立つはずである。この場合は補題 180 により $s = 1$. すなわち、

$$1 \equiv \binom{n-1}{p^k-1} = \frac{1}{m}\binom{n}{p^k} \pmod{p}.$$

この式はもはや、位数を除いて G の構造に依存する値は何もなく、結局群には関係なく一般に成り立つ、純粋に初等整数論的な公式になっていることに注意しよう。このことから、ただちに以下を得る。

命題 181. 有限群 G の位数を $p^k m$ としたとき、$H \subset G$, $\sharp H = p^k$, なる p-部分群 H の個数を s とすると、$s \equiv 1 \pmod{p}$. 特に $s \neq 0$ である。特に、$p \nmid m$ とすれば、s は *p-Sylow* 群である。

Sylow の定理 169(i) の前半（p-Sylow 群が必ず存在すること）、および、(iii) の後半（$s \equiv 1 \pmod{p}$) は、命題 181 より直ちに従う。

12.3.3. 共役な p-部分群. Sylow の定理 169(i) の後半（任意の p-部分群が p-Sylow 群に含まれること）と (ii) は、次の補題から直ちに従う。

補題 182. 有限群 G と p-部分群 $H \subset G$, および、*p-Sylow* 群 $S \subset G$ が与えられたとする。このとき、適当な $g \in G$ によって $H \subset gSg^{-1}$ となる。

Proof. G の S による左分解 G/S に対して、H は次のように作用する：

$$H \times G/S \longrightarrow G/S, \quad (h, gS) \longmapsto (hg)S.$$

任意の H-軌道 $H(gS) = \{(hg)S \mid h \in H\}$ $(g \in S)$ に対して、$\sharp H(gS)$ は $\sharp H$ の約数、すなわち p の冪である (cf. 命題 178 の証明)。しかしながら、S は p-Sylow 群だから、(Lagrange の公式 (系 50)) より $\sharp G/S$ は p で割り切れない。ところが、命題 178 より

$$\sharp G/S = \sum_{g \in G} \sharp H(gS)$$

だから、結局、$\sharp H(gS) = p^0 = 1$, すなわち、任意の $h \in H$ に対して $hgS = gS$ となるような H-軌道が含まれていなければならない。特に $1 \in S$ だから、$hg \in gS$, i.e., $h \in gSg^{-1}$. よって $H \subset gGg^{-1}$ を得る。 □

12.3.4. *p-Sylow* 群の正規化群.

定義 183. 群 G の部分群 $H \subset G$ に対して、

$$N_H = \{g \in G \mid gHg^{-1} \ H\}$$

を H の「**正規化群**」(normalizer) と呼ぶ。

命題 184. 群 G の部分群 $H \subset G$ に対して、
(i) N_H は G の部分群である。
(ii) $N_G \triangleright H$.

Proof. (i) $1_G \in N_H$ は明らか。$g, h \in N_H$ に対して、

$$\begin{aligned}(gh)H(gh)^{-1} &= (gh)H(h^{-1}g^{-1}) = g(hHh^{-1})g^{-1} \\ &= gHg^{-1} \quad (h \in N_H \text{ ゆえ}) \\ &= H \quad (g \in N_H \text{ ゆえ})\end{aligned}$$

ゆえ、$gh \in N_H$ となる。さらに、$g \in N_H$ ならば、$gHg^{-1} = H$ だが、両辺に左から g^{-1}, 右から g を掛ければ、$H = g^{-1}H(g^{-1})^{-1}$ を得るから、$g^{-1} \in N_H$. よって、N_H は G の部分群である。また、(ii) は N_G の定義から明らかである。 □

Sylow の定理 169 の最後に残った部分、すなわち (iii) の前半「$s|\sharp G$」は、以下の補題と補題 184(i), および、Lagrange の公式 (系 50) より直ちに従う。

補題 185. 有限群 G と p-*Sylow* 群 $S \subset G$ が与えられたとする。このとき、$(G : N_S)$ は G に含まれる p-*Sylow* 群の個数を表す。

Proof. X を G の p-Sylow 群全体の集合とする。既に示されたように、任意の 2 つ p-Sylow 群は互いに共役だから、G の X に対する共役作用

$$\mu : G \times X \longrightarrow X, \quad (g, S') \longmapsto \mu(g, S') = gS'g^{-1}$$

は**推移的** *(transitive)* である：すなわち、任意の $S, S' \in X$ に対して、適当な $g \in G$ によって $\mu(g, S) = S'$ とできる。従って、$X = G(S)$. さらに $\sharp G(S) = (G : G_S)$ となる。実際、$(G : G_S) = \sharp(G/G_S))$ に注意して

$$G/G_S \ni gG_S \leftrightarrow gS \in G(S)$$

なる対応を考えれば、これが全単射であることは容易にわかる。よって、

$$\sharp X = (G : G_S)$$

を得る。さらに μ が共役作用だから

$$G_S = \{g \in G \mid \mu(g, S) = S\} = \{g \in G \mid gSg^{-1} = S\} = N_S \tag{15}$$

となり、結局 $\sharp X = (G : N_S)$ となる。 □

13. 有限群の分類

命題 186. 位数が素数 p の有限群 G は巡回群である。

Proof. 命題 51 □

命題 187. $p < q$ が素数で $p \nmid (q-1)$ ならば、位数 pq の有限群 G は pq 次の巡回群である。

Proof. Satz 5.3/12 [1]. □

References

[1] S. Bosch, *Algebra*, 4. Auflage, Springer, 2001.
[2] 藤崎源二朗、「体とガロア理論」（岩波基礎数学選書）岩波書店、1991.

Appendix A. ユークリッドの互除法

定義 188 (最大公約数と最小公倍数)**.** 正整数 $a,\ b$ に対し、

- (a,b)
  $a,\ b$ の最大公約数
- $(a,b)=1$
  $a,\ b$ の最大公約数が *1* であること. このことを特に「a と b は互いに素である」という。
- $LCM(a,b)$
  $a,\ b$ の最小公倍数. 適当な正整数 $M,\ N$ によって $LCM(a,b)=M\times a=N\times b$ と書けることに注意する。

命題 189. $a>b$ なる任意の整数を考え、a を b で割った余りを r とする：

$$a=q\times b+r\quad 0\le r<b.$$

このとき、$(a,b)=(b,r)$ である。

Proof. $a=q\times b+r$ だから、$(b,r)\mid a$. よって (b,r) は a と b の公約数。つまり、

$$(b,r)\mid(a,b) \tag{16}$$

$r=a-q\times b$ だから、$(a,b)\mid r$. よって (a,b) は b と r の公約数。つまり、

$$(a,b)\mid(b,r) \tag{17}$$

である。(16) と (17) より $(a,b)=(b,r)$. □

Euclud の互除法とは、最大公約数 (a,b) を計算する高速アルゴリズムである。このアルゴリズムは、$a,\ b$ をそれぞれ素因数分解して共通因子を捜す方法よりも一般の効率が良い。

Euclud の互除法:

Step 0: $a=b$ ならば、$(a,b)=a=b$ として計算終了。さもなくば、Step 1 に進む。以下、必要ならば a と b を入れ替えて、$a>b$ と思ってよい。
Step 1: a を b で割ってみる：$a=q\times b+r,\ 0\le r<b$.
(このとき、上の命題より $(a,b)=(b,r)$ である！)
Step 2: $r=0$ ならば $(a,b)=b$ として計算終了。さもなくば、a,b を b,r に置き換えて Step 1 に戻る。

Euclid の互除法は、次の重要な定理の証明にも使われる。

定理 190 (Euclid の定理)**.** 任意の整数 a,b に対し、適当な整数 x,y が存在して、

$$xa+yb=(a,b).$$

Proof. Euclid の互除法を実行すると、次のような式が出てくる。

$$\begin{aligned} a &= q \times b + r_1 \quad (b > r_1) \\ b &= q_1 \times r_1 + r_2 \quad (r_1 > r_2) \\ r_1 &= q_2 \times r_2 + r_3 \quad (r_2 > r_3) \\ &\cdots \\ r_{k-2} &= q_{k-1} \times r_{k-1} + r_k \quad (r_{k-1} > r_k) \\ r_{k-1} &= q_k \times r_k \end{aligned}$$

割り算の余りは $r_1 > r_2 > r_3 > \cdots > r_k$ と単調現象するから、最後には余りが零になる。最後の式はそのことを表している。そして命題 189 より $r_k = (a, b)$ である。

そこで、上の式を下から順番に見て行って、$r_{k-1}, r_{k-2}, \ldots, r_2, r_1$ の順に消去していく。この時、一番下の式は使わないので除外しておき、また、最後から 2 番目の式は適当に移項して

$$\begin{aligned} a &= q \times b + r_1 \\ b &= q_1 \times r_1 + r_2 \\ r_1 &= q_2 \times r_2 + r_3 \\ &\cdots \\ r_{k-4} &= q_{k-3} \times r_{k-3} + r_{k-2} \\ r_{k-3} &= q_{k-2} \times r_{k-2} + r_{k-1} \\ (a, b) &= r_{k-2} - q_{k-1} \times r_{k-1} \end{aligned}$$

を考える。下から 2 番目の式を使って、最後の式の r_{k-1} を消去し、この式はもう不要なので除外する：

$$\begin{aligned} a &= q \times b + r_1 \\ b &= q_1 \times r_1 + r_2 \\ r_1 &= q_2 \times r_2 + r_3 \\ &\cdots \\ r_{k-4} &= q_{k-3} \times r_{k-3} + r_{k-2} \\ (a, b) &= r_{k-2} - q_{k-1} \times \underline{(r_{k-3} - q_{k-2} \times r_{k-2})} \end{aligned}$$

同様に、下から 2 番目の式を使って、最後の式の r_{k-2} を消去し、この式はもう不要なので除外する：

$$\begin{aligned} a &= q \times b + r_1 \\ b &= q_1 \times r_1 + r_2 \\ r_1 &= q_2 \times r_2 + r_3 \\ &\cdots \\ (a, b) &= \underline{(r_{k-4} - q_{k-3} \times r_{k-3})} - q_{k-1} \times (r_{k-3} - q_{k-2} \times \underline{(r_{k-4} - q_{k-3} \times r_{k-3})}) \end{aligned}$$

最後の式を少し整理すると、

$$\begin{aligned} a &= q \times b + r_1 \\ b &= q_1 \times r_1 + r_2 \\ r_1 &= q_2 \times r_2 + r_3 \\ &\cdots \\ (a,b) &= (1 + q_{k-1} \times q_{k-2}) \times \underline{r_{k-4}} - (q_{k-3} \times + q_{k-1} \times + q_{k-1} \times q_{k-2} \times q_{k-3}) \times \underline{r_{k-3}} \end{aligned}$$

となるので、最後の式の r_{k-3} と r_{k-4} を順番に消去していけば良い。同様の計算を続けていけば、最後には

$$(a,b) = xa + yb \quad x, y \in \mathbb{Z}$$

なる形の式を得る。 □

例 191 (Euclid の互除法の仕組み (1))**.** $a = 12,\ b = 42$ とする. $b > a$ だから、b を a で割ってみる。

$$b = 3 \times a + 6 \qquad (*)$$

ここで次の事に注意する。

$$\boxed{(a,b) = (a, b - 3 \times a) = (a, 6)}$$

ところが、a は *6* で割り切れる。

$$a = 2 \times 6$$

従って、$(a,b) = (a,6) = 6$ となる。すると、式 $(*)$ は

$$b = 3 \times a + (a,b) \qquad \text{つまり} \qquad (-3)a + b = (a,b)$$

となる。従って、定理 *190* の整数 $x,\ y$ としては、$x = -3,\ y = 1$ とすればよい。

例 192 (Euclid の互除法の仕組み (2))**.** $a = 142,\ b = 36$ とする. $a > b$ だから、a を b で割ってみる。

$$a = 3 \times b + 34 \qquad (*)$$

ここで次の事に注意する。

$$\boxed{(a,b) = (b, a - 3 \times b) = (b, 34)}$$

$b = 36 > 34$ だから、b を *34* で割ってみる。

$$b = 1 \times 34 + 2 \qquad (**)$$

ここで次の事に注意する。

$$\boxed{(b,34) = (34, b - 1 \times 34) = (34, 2)}$$

ところが、34 は *2* で割り切れる。

$$34 = 17 \times 2$$

つまり、$(34,2) = 2$ とわかる。以上によって、

$$(a,b) = (b,34) = (34,2) = 2$$

とわかった。このことから、式 $(*)$ は式 $(**)$ を使って

$$b = 1 \times 34 + 2 = 1 \times 34 + (a,b) = 1 \times (a - 3 \times b) + (a,b) = a - 3 \times b + (a,b)$$

従って $x=-1,\ y=4$ とおけば、

$$ax+by=(a,b)$$

となる。

例 193 (Euclid の互除法の仕組み (3))**.** $a=53,\ b=17$ とする。$a>b$ なので、a を b で割ってみる。

$$a=3\times b+2 \qquad (*)$$

ここで次の事に注意する。

$$\boxed{(a,b)=(b,a-3\times b)=(b,2)}$$

$b>2$ なので、b を 2 で割ってみる。

$$b=8\times 2+1 \qquad (**)$$

ここで次の事に注意する。

$$\boxed{(b,2)=(2,b-8\times 2)=(2,1)=1}$$

以上から、次のことがわかった。

$$(a,b)=(b,2)=(2,1)=1$$

つまり、a と b は互いに素である。また、式 $(**)$ は式 $(*)$ を使って

$$b=8\times 2+1=8\times(a-3\times b)+1=8\times a-24\times b+1$$

従って、$x=-8,\ y=25$ とおけば、

$$ax+by=(a,b)=1$$

となる。

Contents

Yukihide Takayama, Department of Mathematical Sciences, Ritsumeikan University, 1-1-1 Nojihigashi, Kusatsu, Shiga 525-8577, Japan
E-mail address: takayama@se.ritsumei.ac.jp