代数基礎 1

松井紘樹

目次

第 6 章の内容は講義では扱いません.

約束事，よく使う記号

- $\mathbb{N}$ は自然数全体の集合（この講義では 0 も自然数に含めることにする），$\mathbb{Z}$ は整数全体の集合，$\mathbb{Q}$ は有理数全体の集合，$\mathbb{R}$ は実数全体の集合，$\mathbb{C}$ は複素数全体の集合を表す[*1]．
- $\emptyset$ は空集合（一つも元を持たない集合）を表す．
- 記号 $:=$ で「左辺を右辺で定義する」ことを表す
  （例：$n! := 1 \cdot 2 \cdots (n-1)n$）
- $:\Longleftrightarrow$ と書いたら「左側を右側で定義する」を意味する．
  （例：p が素数 $:\Longleftrightarrow$ p は 2 以上の自然数で 1 と自分自身以外に約数を持たない）
- 「$\forall x,\ P$」は「任意の[*2]x に対して命題 P が真である」を表す[*3]．
  （例：「$\forall x \in \mathbb{R}, x^2 \geq 0$」は「任意の実数 x に対して $x^2 \geq 0$ が成り立つ」を意味する）
- 「$\exists x$ s.t. P」は「命題 P が真であるような x が存在する」を表す[*4]．
  （例：「$\exists x \in \mathbb{R}$ s.t. $x^2 - 3x + 1 < 0$」は「$x^2 - 3x + 1 < 0$ となるような実数 x が存在する」を意味する）
- ギリシャ文字：

α, A：アルファ	η, H：エータ	ν, N：ニュー	τ, T：タウ
β, B：ベータ	θ, Θ：シータ	ξ, Ξ：グザイ，クシー	υ, Υ：ウプシロン
γ, Γ：ガンマ	ι, I：イオタ	o, O：オミクロン	ϕ, φ, Φ：ファイ
δ, Δ：デルタ	κ, K：カッパ	π, Π：パイ	χ, X：カイ
ϵ, E：イプシロン	λ, Λ：ラムダ	ρ, P：ロー	ψ, Ψ：プサイ
ζ, Z：ゼータ	μ, M：ミュー	σ, Σ：シグマ	ω, Ω：オメガ

[*1] $\mathbb{N}$ は Natural number（英語で自然数），$\mathbb{Z}$ は Zhalen（ドイツ語で整数），$\mathbb{Q}$ は Quoziente（イタリア語で比），$\mathbb{R}$ は Real number（英語で実数），$\mathbb{C}$ は Complex number（英語で複素数）の頭文字

[*2] 「任意の」は「全ての」と読み替えると分かりやすい

[*3] $\forall$ は All（全て）の頭文字の A をひっくり返したもの

[*4] $\exists$ は Exist（存在する）の頭文字の E をひっくり返したもの，s.t. は such that の頭文字を取ったもの

第 1 章

集合と写像

集合と写像は分野を問わず数学における共通の言語である．この章では集合と写像の基本事項について復習する．

1.1　集合と写像

集合

集合とは「**要素**または**元**と呼ばれる “もの”の集まり」である[*1]．x が集合 A の元であることを $x \in A$ で，x が A の元でないことを $x \notin A$ で表す．

集合 A の表し方には主に以下の 2 通りがある：

- **外延的記法**：集合の元を列挙する方法

$$A = \{x_1, x_2, \ldots, x_n\} \quad (A \text{ は元 } x_1, x_2, \ldots, x_n \text{ を持つ集合})$$

  例： $\{1,2,3,4\},\ \{1,3,5,7,\ldots\},\ \{\ldots,-2,-1,0,1,2,\ldots\}$

- **内包的記法** $\cdots$ 集合を元の満たす条件を用いて表す方法

$$A = \{x \in E \mid P(x)\} \qquad (A \text{ は集合 } E \text{ の元で条件 } P(x) \text{ を満たすもの全体の集合})$$

  例： $\{x \in \mathbb{Z} \mid 1 \leq x \leq 4\},\ \{x \in \mathbb{N} \mid x \text{ は奇数 }\},\ \{x \in \mathbb{R} \mid x \text{ は整数 }\}$

（元の個数が無限個だと基本的に外延的記法では表せないので内包的記法に慣れよう[*2]）

集合に関する以下の記号はよく使われる：

- $A \subseteq B :\Longleftrightarrow$ 全ての A の元 a は B の元である　（A は B の**部分集合**）
- $A = B :\Longleftrightarrow A \subseteq B$ かつ $B \subseteq A$　（A と B は**等しい**）
- $A \cup B := \{x \mid x \in A \text{ または } x \in B\}$　（A と B の**和集合**）
- $A \cap B := \{x \mid x \in A \text{ かつ } x \in B\}$　（A と B の**共通集合**）
- $A \setminus B := \{x \mid x \in A \text{ かつ } x \notin B\}$　（A と B の**差集合**）
- $A \times B := \{(a,b) \mid a \in A \text{ かつ } b \in B\}$[*3]　（$A$ と B の**直積集合**）
  （$A \times B$ の元は「$(a,b) = (a',b') \Longleftrightarrow a = a' \text{かつ } b = b'$」を満たす）

[*1] 厳密な定義はこの講義の範疇を超えるので省略するが，単にものの集まりだと思っても支障はない

[*2] 実数全体の集合 $\mathbb{R}$ は外延的記法で書ける?

[*3] $\mathbb{R}^2 := \mathbb{R} \times \mathbb{R}$ やをイメージすると良い

写像

A, B を集合とする．A の各元 a に対して B の元 b をただ一つ対応させる規則 f を A から B への**写像**という．このとき，$a \in A$ に対応する B の元を $f(a)$ と書き，写像 f を

$$f : A \to B,\ a \mapsto f(a) \quad \text{または単に} \quad f : A \to B$$

と表す．写像 $f : A \to B$ に対して，集合 A を写像 f の**定義域**，集合 B を写像 f の**値域**と呼ぶ．

A の部分集合 A' に対して，B の部分集合

$$f(A') := \{f(a) \in B \mid a \in A'\}$$

を f による A' **の像**と呼ぶ．f による A の像 $f(A)$ は単に f **の像**と呼ぶ．

B の部分集合 B' に対して，A の部分集合

$$f^{-1}(B') := \{a \in A \mid f(a) \in B'\}$$

を f による B' **の逆像**という[*4]．

二つの写像 $f, g : A \to B$ が**等しい**とは，「任意の $a \in A$ に対して $f(a) = g(a)$」が成り立つときに言い，$f = g$ と表す．

例 1.1.1. (1) 集合 $A = \{1, 2, 3, 4\}$，$B = \{5, 6, 7, 8\}$ に対して元の対応

$$1 \mapsto 7,\ 2 \mapsto 6,\ 3 \mapsto 5,\ 4 \mapsto 6$$

で写像 $f : A \to B$ が定め（つまり，$f(1) = 7, f(2) = 6, f(3) = 5, f(4) = 6$），$f$ の定義域は $A = \{1, 2, 3, 4\}$，値域は $B = \{5, 6, 7, 8\}$ である．

また，f の像は $f(A) = \{f(1), f(2), f(3), f(4)\} = \{5, 6, 7\}$，$f$ による $B' = \{5, 6\}$ の逆像は $f^{-1}(B') = \{2, 4, 6\}$ である．

(2) $\mathbb{R}$ 上で定義された関数 $f(x)$ は写像

$$f : \mathbb{R} \to \mathbb{R},\ x \mapsto f(x)$$

を定め，f の定義域は $\mathbb{R}$，値域は $\mathbb{R}$ となる．

また，f の像は $f(\mathbb{R}) = \{f(x) \mid x \in \mathbb{R}\}$ である．

(3) $m \times n$ 型行列 A に対して，写像 $f_A : \mathbb{R}^n \to \mathbb{R}^m$ が

$$f_A(\boldsymbol{x}) = A\boldsymbol{x} \quad (\boldsymbol{x} \in \mathbb{R}^n)$$

で定め（f_A は A を表現行列にもつ線型写像），f_A の定義域は $\mathbb{R}^n$，値域は $\mathbb{R}^m$ である．つまり，線型写像は写像である．

また，f の像は $f_A(\mathbb{R}^n) = \{A\boldsymbol{x} \mid \boldsymbol{x} \in \mathbb{R}^n\}$ であり，f による $\{\boldsymbol{0}\}$ の逆像は $f_A^{-1}(\{\boldsymbol{0}\}) = \{\boldsymbol{x} \in \mathbb{R}^n \mid A(x) = \boldsymbol{0}\}$ である．

従って，写像は関数や線型写像の概念を拡張したものである．

定義 1.1.2. (1) 集合 A に対して，A の**恒等写像** $\mathrm{id}_A : A \to A$ を

$$\mathrm{id}_A(a) := a \quad (a \in A)$$

[*4] 後で定義する逆写像と混同しないようにしましょう

で定義する．

(2) 写像 $f : A \to B$, $g : B \to C$ に対して，f と g の**合成写像** $g \circ f : A \to B$ を

$$(g \circ f)(a) := g(f(a)) \quad (a \in A)$$

で定義する．

命題 1.1.3. $f : A \to B$, $g : B \to C$, $h : C \to D$ を写像とする．

(1) $(h \circ g) \circ f = h \circ (g \circ f)$ が成り立つ．

(2) $f \circ \mathrm{id}_A = f$ と $\mathrm{id}_B \circ f = f$ が成り立つ．

証明. (1) A の各元 a に対して合成写像の定義から

$$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$$
$$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a)))$$

となる．従って，任意の $a \in A$ に対して $((h \circ g) \circ f)(a) = (h \circ (g \circ f))(a)$ が示されたので $(h \circ g) \circ f = h \circ (g \circ f)$.

(2) A の任意の元 a に対して

$$(f \circ \mathrm{id}_A)(a) = f(\mathrm{id}_A(f)) = f(a)$$

が成り立つので $f \circ \mathrm{id}_A = f$ が成り立つ．同様に $\mathrm{id}_B \circ f = f$. ■

例 1.1.4. (1) $\mathbb{R}$ の恒等写像は関数 $f(x) = x$ で与えられる．

$\mathbb{R}$ で定義された関数 $f(x)$, $g(x)$ に対して，写像 f と g の合成写像は f と g の合成関数 $(g \circ f)(x) = g(f(x))$ で与えられる．

(2) $\mathbb{R}^n$ の恒等写像は f_{E_n} である．

行列 $l \times m$ 型行列 A と $m \times n$ 型行列 B に対して

$$(f_A \circ f_B)(\boldsymbol{x}) = f_A(f_B(\boldsymbol{x}))f_A(B\boldsymbol{x}) = A(B\boldsymbol{x}) = (AB)\boldsymbol{x} = f_{AB}(\boldsymbol{x})$$

となる．従って，$f_A \circ f_B = f_{AB}$.

定義 1.1.5. $f : A \to B$ を写像とする．写像 $g : B \to A$ が f の逆写像であるとは，

$$g \circ f = \mathrm{id}_A \quad \text{かつ} \quad f \circ g = \mathrm{id}_B$$
（つまり，「任意の $a \in A$ に対して $g(f(a)) = a$ かつ任意の $b \in B$ に対して $f(g(b)) = b$」）

が成り立つ時に言う．この g を f^{-1}（f **インバース**と読む）と書く．

注意. 逆写像の定義より，$a \in A$ と $b \in B$ に対して

$$f(a) = b \Longleftrightarrow f^{-1}(b) = a$$

が成り立つ．

例 1.1.6. (1) $g(x)$ が $f(x)$ の逆関数のとき，g は f の逆写像である．

例えば，$f:\mathbb{R}\to\mathbb{R},\ x\mapsto 2x+1$ は逆写像 $g:\mathbb{R}\to\mathbb{R},\ x\mapsto \frac{x-1}{2}$ を持つ．ここで，$\mathbb{R}_{>0}:=\{x\in\mathbb{R}\mid x>0\}$.

(2) A が n 次の正則行列のとき，例 1.1.4(2) により

$$f_A\circ f_{A^{-1}}=f_{AA^{-1}}=f_{E_n}=\mathsf{id}_{\mathbb{R}^n}$$
$$f_{A^{-1}}\circ f_A=f_{A^{-1}A}=f_{E_n}=\mathsf{id}_{\mathbb{R}^n}$$

従って，f_A は逆写像 $f_{A^{-1}}$ を持つ．

命題 1.1.7. 写像 $f:A\to B$ と $g:B\to C$ を考える．

(1) f と g が逆写像を持つとき $g\circ f$ も逆写像を持ち，$(g\circ f)^{-1}=f^{-1}\circ g^{-1}$ が成り立つ．

(2) f が逆写像を持つとき f^{-1} も逆写像を持ち，$(f^{-1})^{-1}=f$ が成り立つ．

証明. (1) f と g が逆写像 f^{-1}, g^{-1} を持つとする．このとき，$f^{-1}\circ g^{-1}$ が $g\circ f$ の逆写像であることを確かめれば良い．これは

$$(f^{-1}\circ g^{-1})\circ(g\circ f)=f^{-1}\circ(g^{-1}\circ g)\circ f=f^{-1}\circ\mathsf{id}_B\circ f=f^{-1}\circ f=\mathsf{id}_A$$
$$(g\circ f)\circ(f^{-1}\circ g^{-1})=g\circ(f\circ f^{-1})\circ g^{-1}=g\circ\mathsf{id}_B\circ g^{-1}=g\circ g^{-1}=\mathsf{id}_C$$

となることから従う．

(2) f が逆写像 f^{-1} を持つとする．このとき，f が f^{-1} の逆写像であることを確かめれば良い．f^{-1} が f の逆写像なので

$$f\circ f^{-1}=\mathsf{id}_B,\quad f^{-1}\circ f=\mathsf{id}_A$$

成り立っているが，これは f が f^{-1} の逆写像であることを意味している． ■

定義 1.1.8. $f:A\to B$ を写像とする．

(1) f が**単射**とは，「任意の $a,a'\in A$ に対して，$f(a)=f(a')$ ならば $a=a'$ となる」が成り立つときに言う．

(2) f が**全射**とは，「任意の $b\in B$ に対して，$b=f(a)$ となる $a\in A$ が存在する」が成り立つときに言う．

(3) f が**全単射**とは，f が単射かつ全射（つまり，「任意の $b\in B$ に対して，$b=f(a)$ となる $a\in A$ がただ一つ存在する」）のときに言う．

例 1.1.9. (1) 関数 $f(x)=x^2$ を考える．

- $f:\mathbb{R}\to\mathbb{R},\ x\mapsto x^2$ は単射でも全射でもない．
- $f:\mathbb{R}\to[0,\infty),\ x\mapsto x^2$ は全射であるが単射ではない．
- $f:[0,\infty)\to\mathbb{R},\ x\mapsto x^2$ は単射であるが全射ではない．
- $f:[0,\infty)\to[0,\infty),\ x\mapsto x^2$ は全単射である．

(2) n 次の正方行列 A を考える．

- A が正則行列のとき，$f:\mathbb{R}^n\to\mathbb{R}^n,\ \boldsymbol{x}\mapsto A\boldsymbol{x}$ は全単射である．
- A が正則行列でないとき，$f:\mathbb{R}^n\to\mathbb{R}^n,\ \boldsymbol{x}\mapsto A\boldsymbol{x}$ は全射でも単射でもない．

定理 1.1.10. 写像 $f : A \to B$ に対して，

$$f \text{ が逆写像を持つ} \iff f \text{ が全単射}$$

証明. （$\Longrightarrow$）と（$\Longleftarrow$）をそれぞれ示す．

f が逆写像をもつなら f は全単射：

f が逆写像 $g : B \to A$ を持つとする．まずは f が単射であることを示す．A の元 a, a' が $f(a) = f(a')$ を満たすとする．このとき，

$$a = g(f(a)) = g(f(a')) = a'$$

となるので，f が単射であることが示された（一つ目と三つ目の等号に逆写像の定義 $g \circ f = \mathsf{id}_A$ を用いた）．

次に f が全射であることを示す．任意の B の元 b に対して，A の元 $a = g(b)$ を考えると，

$$f(a) = f(g(b)) = b$$

となるので f が全射であることも示された（二つ目の等号に逆写像の定義 $f \circ g = \mathsf{id}_B$ を用いた）．

f が全単射なら f は逆写像をもつ：

f が全単射なので，各 $b \in A$ に対して $f(a) = b$ となる $a \in A$ がただ一つ存在する．この a を $g(b)$ と書くことにする．この対応で，写像

$$g : B \to A,\ b \mapsto g(b)$$

を得る．定義より，任意の $b \in B$ に対して $f(g(b)) = b$ が成り立つ．一方で，任意の $a \in A$ に対して $f(g(f(a))) = f(a)$ であるが，f が単射なので $g(f(a)) = a$ が従う．よって，$f \circ g = \mathsf{id}_B$ と $g \circ f = \mathsf{id}_A$ が示されたので g は f の逆写像である． ■

演習問題

問題 1.1.1. $A = \{1, 2, 3, 4, 5\}$, $B = \{a, b, c\}$ とし，写像 $f : A \to B$ を

$$f(1) = a,\ f(2) = b,\ f(3) = b,\ f(4) = a,\ f(5) = b$$

このとき，以下の集合を求めよ：

(1) $f(A)$

(2) $f(\{1, 2\})$

(3) $f(\{1, 4\})$

(4) $f^{-1}(a)$

(5) $f^{-1}(c)$

(6) $f^{-1}(\{a, c\})$

問題 1.1.2. 例 1.1.9(1) を確かめよ．

問題 1.1.3. 次の写像が全射，単射，全単射，どれでもない，のいずれか答えよ．また，全単射の場合はその逆写像も求めよ．

(1) $f : \mathbb{R} \to \mathbb{R},\ x \mapsto e^x$

(2) $f : \mathbb{R} \to \mathbb{R}_{>0},\ x \mapsto e^x$　（ただし，$\mathbb{R}_{>0} := \{x \in \mathbb{R} \mid x > 0\}$）

(3) $f : \mathbb{R} \to \mathbb{R},\ x \mapsto x^3 - x$

(4) $f : \mathbb{R}^2 \to \mathbb{R}^2,\ \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} 3x+5y \\ 4x+7y \end{smallmatrix}\right)$

(5) $f : \mathbb{R}^2 \to \mathbb{R}^2,\ \left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} 4x+2y \\ 2x+y \end{smallmatrix}\right)$

(6) $x \in \{0, 1, 2, 3, 4\}$ に対して x^3 を 5 で割った余り $f(x)$ を対応させる写像

$$f : \{0, 1, 2, 3, 4\} \to \{0, 1, 2, 3, 4\}$$

問題 1.1.4. 写像 $f : A \to B$ と $g : B \to C$ に対して以下を示せ.

(1) f と g が単射ならば $g \circ f$ は単射

(2) $g \circ f$ が単射ならば f は単射

(3) f と g が全射ならば $g \circ f$ は全射

(4) $g \circ f$ が全射ならば f は全射

1.2　同値関係

集合 X 上の同値関係とは大雑把に言えば X をいくつかの互いに交わらないグループに分けるものである．例えば，

- 代数基礎 1 の受講者全体の集合 X を誕生月によって

  「1 月生まれのグループ」,「2 月生まれのグループ」, . . . ,「12 月生まれのグループ」

  に分ける
- 整数全体の集合 $\mathbb{Z}$ を 6 で割った余りによって 6 個のグループ

  「余りが 0 のグループ」,「余りが 1 のグループ」, . . . ,「余りが 5 のグループ」

  に分ける

といったものである．このように集合 X のグループ分けを考えたいとき，初めからグループ達を定めてもよいが，それよりも X の 2 つの元がいつ同じグループに属するかを表す**関係**を定めたほうが扱いやすいことが多い．これが**同値関係**である．

同値関係

定義 1.2.1. X を集合とする．

(1) X 上の**関係** $\sim$ とは，X の任意の 2 元 x, y に対して，
- x と y に関係がある（$x \sim y$ と書く）
- x と y には関係が無い（$x \not\sim y$ と書く）

のいずれか一方のみが定められているもの．

(2) X 上の関係 $\sim$ が**同値関係**であるとは，以下の 3 条件が成り立つ時に言う．

（反射律）任意の $x \in X$ に対して，$x \sim x$ となる．
（対称律）任意の $x, y \in X$ に対して，$x \sim y$ ならば $y \sim x$ となる．
（推移律）任意の $x, y, z \in X$ に対して，$x \sim y$ かつ $y \sim z$ ならば $x \sim z$ となる．

コメント. (1) より厳密には，集合 X 上の関係とは $X \times X$ の部分集合 R のことである．このとき，$(x, y) \in R$ のとき $x \sim y$ と定めると，X の任意の 2 元 x, y に対して，$x \sim y$（つまり $(x, y) \in R$）と $x \not\sim y$（つまり $(x, y) \notin R$）のいずれか一方のみが成り立つ．

(2) 集合の元をグループに分けるという観点からは，同値関係 $\sim$ は

$$x \sim y \Longleftrightarrow x \text{ は } y \text{ と同じグループに属する}$$

を意味している．すると，反射律，対称律，推移律はそれぞれ

（反射律）X の元 x は x 自身と同じグループに属する．
（対称律）X の元 x が y と同じグループに属するならば，y は x と同じグループに属する．
（推移律）X の元 x が y と同じグループに属し，y が z と同じグループに属するならば，x は z と同じグループに属する．

という当たり前の性質を意味している．

例 1.2.2. (1) $\mathbb{R}$ 上の関係 $\sim$ を

$$x \sim y :\Longleftrightarrow x \leq y$$

で定める．これを $\mathbb{R}$ 上の**順序関係**という．

$\mathbb{R}$ 上の順序関係は同値関係ではない．実際，反射律，推移律は成り立つが，対称律は成り立たない（$1 \leq 2$ だが $2 \leq 1$ ではない）．

(2) X を代数基礎 1 の受講者全体の集合とし，$x, y \in X$ に対して

$$x \sim y :\Longleftrightarrow x \text{ と } y \text{ の誕生月が同じ}$$

と定めると，$\sim$ は X 上の同値関係である：

（反射律）代数基礎 1 の受講者 x に対して，x と x の誕生月は同じ．

（対称律）代数基礎 1 の受講者 x, y に対して，x と y の誕生月が同じならば y と x の誕生月が同じ．

（推移律）代数基礎 1 の受講者 x, y, z に対して，x と y の誕生月が同じで y と z の誕生月が同じならば，x と z の誕生月は同じ．

(3) $n \in \mathbb{Z}$（$n \geq 1$）とする．$\mathbb{Z}$ 上の関係 $\sim$ を

$$x \sim y :\Longleftrightarrow x - y \text{ が } n \text{ の倍数}$$

で定めると，$\sim$ は $\mathbb{Z}$ 上の同値関係である：

（反射律）任意の $x \in \mathbb{Z}$ に対して，$x - x = 0$ は n の倍数なので $0 \sim 0$ となる．

（対称律）$x \sim y$ のとき，$x - y$ は n の倍数なので $y - x = -(x - y)$ も n の倍数．従って，$y \sim x$.

（推移律）$x \sim y$, $y \sim z$ とする．$x - y$ と $y - z$ が n の倍数なので，$x - z = (x - y) + (y - z)$ も n の倍数．従って，$x \sim z$.

(4) $\mathbb{R}$ 上の関係 $\sim$ を

$$x \sim y :\Longleftrightarrow x - y \in \mathbb{Z}$$

で定めると，$\sim$ は $\mathbb{R}$ 上の同値関係である．

（反射律）任意の $x \in \mathbb{R}$ に対して，$x - x = 0 \in \mathbb{Z}$ より $x \sim x$.

（対称律）$x, y \in \mathbb{R}$ が $x \sim y$ を満たすとする．このとき，$x - y \in \mathbb{Z}$ なので $y - x = -(x - y) \in \mathbb{Z}$ となる．従って，$y \sim x$.

（推移律）$x, y, z \in \mathbb{R}$ が $x \sim y$, $y \sim z$ を満たすとする．このとき，$x - y$, $y - z \in \mathbb{Z}$ なので $x - z = (x - y) + (y - z) \in \mathbb{Z}$ となる．従って，$x \sim z$.

それでは，同値関係から集合のグループ分けを実際に与えよう．

定義 1.2.3. $\sim$ を集合 X 上の同値関係とする．$x \in X$ に対して，X の部分集合

$$[x] := \{y \in X \mid x \sim y\}$$

を x **を代表元とする同値類**という．

X の同値類を元とする集合

$$X/\sim := \{[x] \mid x \in X\}$$

を X の同値関係 $\sim$ による**商集合**という．

$C \in X/\sim$ に対して，C の元 x を C の**代表**と呼ぶ．

例 1.2.4. (1) X を代数基礎 1 の受講者全体の集合とし，例 1.2.2(2) の同値関係を考える．このとき，代数基礎 1 の受講者 x に対して，

$$[x] = \{y \in X \mid x \text{ と } y \text{ の誕生月が同じ }\}$$

である．従って，x が i 月生まれならば，

$$[x] = \{y \in X \mid y \text{ は } i \text{ 月生まれ }\}$$

と表せる．このことから，X_i を i 月生まれの受講生全体の集合とすると，商集合

$$X/\sim = \{[x] \mid x \in X\} = \{X_1, X_2, \ldots, X_{12}\}$$

は X を誕生月でグループ分けしたときのグループの集合である．

(2) $n \in \mathbb{Z}$（$n \geq 1$）とし，例 1.2.2(3) で考えた $\mathbb{Z}$ 上の同値関係

$$x \sim y :\Longleftrightarrow x - y \text{ が } n \text{ の倍数}$$

を考える．このとき，$x \in \mathbb{Z}$ に対して

$$[x] = \{y \in \mathbb{Z} \mid x - y \text{ が } n \text{ の倍数 }\}$$

である．$x - y$ が n の倍数とは x と y を n で割ったあまりが等しいということなので，x を n で割った余りを r とすると，

$$[x] = r + n\mathbb{Z} = \{y \in \mathbb{Z} \mid y \text{ を } n \text{ で割った余りが } r\}$$

となる．従って，$\mathbb{Z}$ の $\sim$ による商集合

$$\mathbb{Z}/\sim = \{[x] \mid x \in \mathbb{Z}\} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$$

は $\mathbb{Z}$ を n で割った余りでグループ分けしたときのグループの集合である．

(3) 例 1.2.2(4) で考えた $\mathbb{R}$ 上の同値関係

$$x \sim y :\Longleftrightarrow x - y \in \mathbb{Z}$$

を考える．このとき，$x \in \mathbb{R}$ に対して

$$[x] = \{y \in \mathbb{R} \mid y - x \in \mathbb{Z}\} = \{x + n \mid n \in \mathbb{Z}\} =: x + \mathbb{Z}$$

である．$x \sim y$ は x と y の小数部分が等しいことを意味するので，x の小数部分を $r \in [0, 1)$ とすれば，

$$[x] = r + \mathbb{Z} = \{y \in \mathbb{R} \mid y \text{ の小数部分は } r\}$$

となる．従って，$\mathbb{R}$ の $\sim$ による商集合

$$\mathbb{R}/\sim = \{[x] \mid x \in \mathbb{R}\} = \{r + \mathbb{Z} \mid r \in [0, 1)\}$$

は $\mathbb{R}$ を同じ小数部分を持つ実数にグループ分けしたときのグループの集合である．

集合の同値関係による同値類は以下の性質を満たす：

命題 1.2.5. $\sim$ を X 上の同値関係とする．このとき，以下が成り立つ：

(1) 任意の $x \in X$ に対して $x \in [x]$ となる．特に，$[x] \neq \emptyset$.
(2) $X = \bigcup_{x \in X} [x]$

(3) $x, y \in X$ に対して，以下の 3 条件は互いに同値：
  (i) $x \sim y$
  (ii) $[x] \cap [y] \neq \emptyset$
  (iii) $[x] = [y]$

証明. (1) 反射律より任意の $x \in X$ に対して $x \sim x$ が成り立つ．従って，$x \in [x]$ となり，特に $[x] \neq \emptyset$ となる．

(2) $[x]$ は X の部分集合なので $\bigcup_{x \in X} [x] \subseteq X$ である．一方で，任意の $x \in X$ は $[x]$ の元なので $X \subseteq \bigcup_{x \in X} [x]$ となる．従って，$X = \bigcup_{x \in X} [x]$ が示された．

(3)(i) $\Rightarrow$ (ii)：
$x \sim y$ として $[x] = [y]$ となることを示す．$z \in [x]$ とすると，$x \sim z$ である．対称律より $y \sim x$ となるので，推移律を用いて $y \sim z$ となる．従って，$z \in [y]$ が成り立つ．以上より，$[x] \subseteq [y]$ が示された．全く同様にして $[y] \subseteq [x]$ も示されるので，$[x] = [y]$ が分かる．

(ii) $\Rightarrow$ (iii)：
$[x] \cap [y] \neq \emptyset$ とし，$[x] = [y]$ を示す．$z \in [x] \cap [y]$ とすると，$x \sim z$ かつ $y \sim z$ が成り立つ．対称律より $z \sim y$ となるので，推移律より $x \sim y$．従って，上で示したことから $[x] = [y]$ となる．

(iii) $\Rightarrow$ (i)：$[x] = [y]$ のとき，(1) より $y \in [y] = [x]$ となるので $x \sim y$. ■

この命題により，X は互いに交わらない同値類達の和集合となる．そこで，その各同値類から一つずつ代表を取ってきたものとして以下の概念を考える．

定義 1.2.6. 集合 X 上の同値関係 $\sim$ を考える．X の部分集合 $\{x_i\}_{i \in I}$ が次の条件を満たすとき，$\{x_i\}_{i \in I}$ を $X/\sim$ の**完全代表系**と呼ぶ：

(i) $X/\sim = \bigcup_{i \in I} [x_i]$
(ii) $x_i \neq x_j$ ならば $[x_i] \cap [x_j] = \emptyset$

例 1.2.7. (1) X を代数基礎 1 の受講者全体の集合とし，例 1.2.2(2) の同値関係を考える．代数基礎 1 の受講者から 1 月生まれの x_1, 2 月生まれの $x_2, \ldots$, 12 月生まれの x_{12} を一人ずつ選んでくると，

$$\{x_1, x_2, \ldots, x_{12}\}$$

は $X/\sim$ の完全代表系である．
(2) 例 1.2.2(3) で考えた $\mathbb{Z}$ の同値関係を考える．このとき，$0, 1, \ldots, n-1$ は $\mathbb{Z}/\sim$ の完全代表系である．
(3) 例 1.2.2(4) で考えた $\mathbb{R}$ の同値関係を考える．このとき，$[0, 1)$ は $\mathbb{R}/\sim$ の完全代表系である．

well-defined 性

集合 X 上の同値関係と写像 $f : X \to Y$ が与えられたとする．このとき，写像 $\overline{f} : X/\sim \to Y$ を

$$\overline{f}([x]) = f(x)$$

で定義したい．しかし，この定義には問題がある：

$x \sim y$ かつ $f(x) \neq f(y)$ となる元 x, y が存在したとしよう．このとき，$[x] = [y]$ であるにも関わらず

$$\overline{f}([x]) = f(x) \neq f(y) = \overline{f}([y])$$

というおかしなことが起こってしまう．

このような状況では $\overline{f} : X/\sim \to Y$ の定義は矛盾をはらんでいる悪い定義（**ill-defined**）であると言える．このような矛盾が生じないとき，$\overline{f} : X/\sim \to Y$ は **well-defined** であるという：

定義 1.2.8. $\sim$ を集合 X 上の同値関係とする．写像 $f : X \to Y$ が条件

任意の $x, y \in X$ に対して，$x \sim y$ ならば $f(x) = f(y)$

を満たすとき，写像

$$\overline{f} : X/\sim \to Y,\ [x] \mapsto f(x)$$

が定まる．このとき，$\overline{f} : X/\sim \to Y$ は **well-defined** であるという．

例 1.2.9. (1) 例 1.2.2(2) で定義した $\mathbb{Z}$ 上の同値関係 $\sim$ を考える．

- $\overline{f} : \mathbb{Z}/\sim \to \mathbb{Z}/\sim,\ [x] \mapsto [x^2]$ は well-defined である：

  (∵) $x \sim y$ のとき $x - y = nq$ $(\exists q \in \mathbb{Z})$ と表せるが，このとき

  $$x^2 - y^2 = (x-y)(x+y) = nq(x+y)$$

  は n の倍数なので $x^2 \sim y^2$ となる．よって，命題 1.2.5(3) より $[x^2] = [y^2]$ である．

- $\zeta_n := e^{\frac{2\pi i}{n}}$ を 1 の原始 n 乗根とすると，

  $$\overline{f} : \mathbb{Z}/\sim \to \mathbb{C} - \{0\},\ [x] \mapsto \zeta_n^x$$

  は well-defined である：

  (∵) $x \sim y$ のとき $x - y = nq$ $(\exists q \in \mathbb{Z})$ と表せるが，このとき

  $$e^{\frac{2\pi x i}{n}} = e^{\frac{2\pi (y+nq) i}{n}} = e^{\frac{2\pi y i}{n}} \cdot e^{2\pi q i} = e^{\frac{2\pi y i}{n}}$$

  となる．

- n が奇数のとき，

  $$\overline{f} : \mathbb{Z}/\sim \to \mathbb{C} - \{0\},\ [x] \mapsto (-1)^x$$

  は well-defined ではない：

  (∵) $0 \sim n$ であるが $(-1)^0 = 1 \neq -1 = (-1)^n$ である．

(2) 例 1.2.2(4) で考えた $\mathbb{R}$ 上の同値関係 $\sim$ を考える．

- $\overline{f} : \mathbb{R}/\sim \to \mathbb{R}/\sim,\quad [x] \mapsto [2x]$ は well-defined である：

  (∵) $x \sim y$ のとき，$x - y \in \mathbb{Z}$ である．従って，$2x - 2y = 2(x-y) \in \mathbb{Z}$ となり，$2x \sim 2y$．よって，命題 1.2.5(3) より $[2x] = [2y]$ である．

- $\overline{f} : \mathbb{R}/\sim \to \mathbb{R}/\sim,\quad [x] \mapsto [x^2]$ は well-defined でない：

  (∵) $\sqrt{2}$ と $\sqrt{2} - 1$ の小数部分は等しいので，$\sqrt{2} \sim \sqrt{2} - 1$ である．一方で，$(\sqrt{2})^2 - (\sqrt{2}-1)^2 = 2\sqrt{2} - 1 \notin \mathbb{Z}$ なので，命題 1.2.5(3) より $[(\sqrt{2})^2] \neq [(\sqrt{2}-1)^2]$.

演習問題

問題 1.2.1. 以下の集合 X 上の関係 $\sim$ が同値関係であることを確かめよ．

(1) $\mathbb{Z}_{\neq 0} := \{x \in \mathbb{Z} \mid x \neq 0\}$ とする．
$X := \mathbb{Z} \times \mathbb{Z}_{\neq 0}$，$(x, y) \sim (u, v) :\Longleftrightarrow xv = yu$

(2) $X := \mathsf{M}_2(\mathbb{R})$（2 次の実正方行列の集合），$A \sim B :\Longleftrightarrow \forall \boldsymbol{v} \in \mathbb{R}^2, A\boldsymbol{v} = B\boldsymbol{v}$

(3) X は実数列全体の集合．
$\{a_n\}_{n=1}^{\infty} \sim \{b_n\}_{n=1}^{\infty} :\Longleftrightarrow \exists N \in \mathbb{N}$ s.t. $\forall n \geq N, a_n = b_n$

問題 1.2.2. X を集合，$\sim$ を X 上の関係とする．$\sim$ が

(i) 任意の $x \in X$ に対して，$x \sim x$
(ii) 任意の $x, y, z \in X$ に対して，$x \sim y$ かつ $x \sim z$ ならば $y \sim z$

を満たすとき，$\sim$ は X 上の同値関係であることを示せ．

問題 1.2.3. $\mathsf{M}_n(\mathbb{C})$ で n 次の複素正方行列の集合を表し，$\mathsf{M}_n(\mathbb{C})$ 上の関係

$$A \sim B :\Longleftrightarrow \text{ある正方行列 } P \text{ が存在して } B = PAP^{-1}$$

を考える．

(1) $\sim$ が同値関係であることを示せ．
(2) 以下の $\overline{f}$ が *well-defined* かどうか答えよ：
(i) $\overline{f} : \mathsf{M}_n(\mathbb{C})/\sim \to \mathbb{C}$，$[A] \mapsto A_{11}$
（ただし，A_{11} は行列 A の $(1, 1)$ 成分を意味する）
(ii) $\overline{f} : \mathsf{M}_n(\mathbb{C})/\sim \to \mathbb{C}$，$[A] \mapsto \mathsf{det}(A)$
(iii) $\overline{f} : \mathsf{M}_n(\mathbb{C})/\sim \to \mathbb{C}$，$[A] \mapsto \mathrm{Tr}(A)$
(iv) $\overline{f} : \mathsf{M}_n(\mathbb{C})/\sim \to \mathbb{C}^n$，$[A] \mapsto A_1$
（ただし，A_1 は行列 A の 1 列目を意味する）
(v) $\overline{f} : \mathsf{M}_n(\mathbb{C})/\sim \to \mathsf{M}_n(\mathbb{C})/\sim$，$[A] \mapsto [A^2]$

問題 1.2.4. $m, n \in \mathbb{Z}\,(m, n \geq 1)$ とする．このとき，$\mathbb{Z}$ 上の同値関係 $\sim_m$ と $\sim_n$ をそれぞれ

$$x \sim_m y :\Longleftrightarrow x - y \text{ が } m \text{ の倍数}$$
$$x \sim_n y :\Longleftrightarrow x - y \text{ が } n \text{ の倍数}$$

で定め，

$$\overline{f} : \mathbb{Z}/\sim_m \to \mathbb{Z}/\sim_n,\ [x]_m \mapsto [x]_n$$

を考える（$[x]_m$ は $\sim_m$ に関する同値類，$[x]_n$ は $\sim_n$ に関する同値類を表している）．

(1) m が n の倍数のとき，$\overline{f}$ は *well-defined* であることを確かめよ．
(2) m が n の倍数でないとき，$\overline{f}$ は *well-defined* でないことを確かめよ．

以上のことから，

$$\overline{f} \text{ が } \textit{well-defined} \Longleftrightarrow m \text{ が } n \text{ の倍数}$$

が分かる．

問題 1.2.5. 写像 $f : X \to Y$ に対して，X 上の関係

$$x \sim y :\Longleftrightarrow f(x) = f(y)$$

を考える．

(1) $\sim$ が同値関係であることを示せ.
(2) $\overline{f} : X/\sim \to Y,\ [x] \mapsto f(x)$ が *well-defined* であることを示せ.
(3) 写像 $\overline{f} : X/\sim \to Y$ が単射であることを示せ.
(4) f が全射のとき，写像 $\overline{f} : X/\sim \to Y$ が全単射であることを示せ.

第 2 章

整数の剰余

この章ではウォーミングアップとして整数とその剰余について復習する．

2.1 整数の剰余

次の命題は a が自然数の場合には中学校か高校で習っている（はず）．

命題 2.1.1 (除法の原理)．$a, n \in \mathbb{Z}$（$n \neq 0$）とする．このとき，

$$a = qn + r, \quad 0 \leq r < |n|$$

を満たすような整数 q, r がただ一組存在する．

q, r をそれぞれ a を n で割った**商**，**余り**と呼ぶ．

証明. $n < 0$ のときは n の代わりに $-n$ を考えレバ良いので，$n \geq 1$ として示せば良い．

存在すること：

数直線を左半開区間

$$\ldots,\ [-2n, -n),\ [-n, 0),\ [0, n),\ [n, 2n),\ \ldots$$

に分割する．すると，整数 a はいずれかの左半開区間 $[qn, (q+1)n)$ $(q \in \mathbb{Z})$ に含まれる．このとき，$qn \leq a < (q+1)n$ となるので，$r = a - qn$ と置くと

$$a = qn + r, \quad 0 \leq r < n$$

が成り立つ．

ただ一組であること：

$a = qn + r = q'n + r',\ 0 \leq r, r' < n$ となる整数の組 $(q, r), (q', r')$ を考える．このとき $q = q',\ r = r'$ を示せば良い．等式 $qn + r = q'n + r'$ より $(q - q')n = qn - q'n = r' - r$ となる．今，仮定 $0 \leq r, r' < n$ から $|r' - r| < n$ となることに注意すると，$(q - q')n = qn - q'n = r' - r$ を満たすのは $q - q' = 0,\ r' - r = 0$ となるときのみである．従って $q = q',\ r = r'$. ■

定義 2.1.2. a を n で割った余りが 0 のとき，n を a **の約数**と言い，$n|a$ と書く：

$$n|a :\Longleftrightarrow \exists q \in \mathbb{Z} \text{ s.t. } a = qn$$

全ての整数 $n \in \mathbb{Z}$ に対して $0 = 0 \cdot n$ となるので，全ての整数は 0 の約数であると約束する．

定義 2.1.3. a, b を 0 でない整数とする．

(1) $0 \neq n \in \mathbb{Z}$ が a と b の約数のとき，n を a と b **の公約数**と呼ぶ．
(2) a と b の公約数のうちで最大のものを $\gcd(a, b)$ と書き，a と b **の最大公約数（great common divisor）**と言う．

以下，$\gcd(a, 0) = a$, $\gcd(0, b) = b$, $\gcd(0, 0) = 0$ と約束することにする．

定理 2.1.4. （ユークリッドの互除法） $a, n \in \mathbb{Z}$（$n \neq 0$）とし，a を n で割った余りを r とする．このとき，

$$\gcd(a, n) = \gcd(n, r)$$

が成り立つ．

証明. a を n で割った余りが r なので，$a = qn + r$ $(q, r \in \mathbb{Z}, 0 \leq r < |n|)$ と表せる．

$c := \gcd(a, n)$, $d := \gcd(n, r)$ と置いたとき，$c \leq d$ と $d \leq c$ を示せば良い．

$c \leq d$ について：

c は a と n の公約数なので $a = uc$, $n = vc$ $(u, v \in \mathbb{Z})$ と書ける．このとき，

$$r = a - qn = uc - qvc = (u - qv)c$$

となり，c は r の約数である．特に，c が r と n の公約数であることも分かった．d は r と n の最大公約数なので，最大性から $c \leq d$ となる．

$d \leq c$ について：

d は n と r の公約数なので $n = ud$, $r = vd$ $(u, v \in \mathbb{Z})$ と書ける．このとき，

$$a = qn + r = qud + vd = (qu + v)d$$

となり，d は a の約数である．また，d は n の約数でもあるので，結局 d は a と n の公約数である．c は a と n の最大公約数なので，最大性により $d \leq c$ となる．

$c \leq d$ と $d \leq c$ が示されたので，$c = d$ が分かった． ■

例 2.1.5. (1) ユークリッドの互除法（定理 2.1.4）を用いて 39 と 25 の最大公約数を求める．

$39 = 1 \cdot 25 + 14$ なので，$\gcd(39, 25) = \gcd(25, 14)$
$25 = 1 \cdot 14 + 11$ なので，$\gcd(25, 14) = \gcd(14, 11)$
$14 = 1 \cdot 11 + 3$ なので，$\gcd(14, 11) = \gcd(11, 3)$
$11 = 3 \cdot 3 + 2$ なので，$\gcd(11, 3) = \gcd(3, 2)$
$3 = 1 \cdot 2 + 1$ なので，$\gcd(3, 2) = \gcd(2, 1)$
ここで，$\gcd(2, 1) = 1$ より $\gcd(39, 25) = 1$ となる．

(2) ユークリッドの互除法（定理 2.1.4）を用いて 1071 と 1029 の最大公約数を求める．

$1071 = 1 \cdot 1029 + 42$ なので，$\gcd(1071, 1029) = \gcd(1029, 42)$
$1029 = 24 \cdot 42 + 21$ なので，$\gcd(1029, 42) = \gcd(42, 21)$
$42 = 2 \cdot 21 + 0$ なので，$\gcd(42, 21) = \gcd(21, 0)$
ここで，$\gcd(21, 0) = 21$ より $\gcd(1071, 1029) = 21$ となる．

この例では 1 または 0 が現れるまでユークリッドの互除法を繰り返し用いたが，もちろん最大公約数が簡単に求められるようになったらそこで終了しても良い．

命題 2.1.6 (ベズーの補題)．a, b を 0 でない整数で $d = \mathsf{gcd}(a, b)$ とする．このとき，

$$ua + vb = d$$

を満たす整数 u, v が存在する．

証明. a, b の符号を適当に変えることで，$a \geq b > 0$ として示せば十分である．このとき，b に関する数学的帰納法で証明する．

- $b = 1$ のとき， $d = 1$ なので $u = 0, v = 1$ とすれば
$$0 \cdot a + 1 \cdot 1 = 1$$
となる．
- $b > 1$ とし，$a' \geq b' > 0$, $b' < b$ を満たす全ての整数 a', b' に対して主張が正しいと仮定する（$\exists u, v \in \mathbb{Z}$ s.t. $ua' + b'v = \mathsf{gcd}(a', b')$）．
命題 2.1.1 より，
$$a = qb + r, \quad 0 \leq r < b$$
となる整数 q, r が存在する．従って，ユークリッドの互除法（定理 2.1.4）により $d = \mathsf{gcd}(a, b) = \mathsf{gcd}(b, r)$ が成立する．ここで，$b \geq r > 0$, $r < b$ なので数学的帰納法の仮定により
$$ub + vr = d$$
となる整数 u, v が存在する．$r = a - qb$ を代入することで
$$va + (u - qv)b = d$$
と表すことができる．

数学的帰納法により，$a \geq b > 0$ なる全ての整数に対して主張が正しいことが示された． ■

コメント. a, b を 0 でない自然数で $d = \mathsf{gcd}(a, b)$ とする．このとき，任意の整数 u, v に対して $d|(ua + vb)$ となる．特に，$ua + vb = 1$ を満たす整数 u, v が存在すれば $d|1$，つまり $d = 1$ となる．従って，命題 2.1.6 と合わせて
$$\exists u, v \in \mathbb{Z} \text{ s.t. } ua + vb = 1 \Longleftrightarrow \mathsf{gcd}(a, b) = 1$$
が分かる．

命題 2.1.6 の u, v は以下のようにユークリッドの互除法を逆に辿っていくことで求めることができる：

例 2.1.7. (1) $a = 39$, $b = 25$ とする．このとき，例 2.1.5(1) より $\mathsf{gcd}(39, 25) = 1$ となる．
例 2.1.5(1) で計算した割り算の式を繰り返し用いると，
$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (11 - 3 \cdot 3) = -11 + 4 \cdot 3 \\ &= -11 + 4 \cdot (14 - 1 \cdot 11) = 4 \cdot 14 - 5 \cdot 11 \\ &= 4 \cdot 14 - 5 \cdot (25 - 1 \cdot 14) = -5 \cdot 25 + 9 \cdot 14 \\ &= -5 \cdot 25 + 9 \cdot (39 - 1 \cdot 25) = 9 \cdot 39 - 14 \cdot 25 \end{aligned}$$
となり，$9 \cdot 39 - 14 \cdot 25 = 1$ と表せる．

(2) $a = 1071$, $b = 1029$ とする．このとき，例 2.1.5(1) より $\mathsf{gcd}(1071, 1029) = 21$ となる．

例 2.1.5(2) で計算した割り算の式を繰り返し用いると，

$$\begin{aligned} 21 &= 1029 - 24 \cdot 42 \\ &= 1029 - 24 \cdot (1071 - 1 \cdot 1029) = (-24) \cdot 1071 + 25 \cdot 1029 \end{aligned}$$

となり，$(-24) \cdot 1071 + 25 \cdot 1029 = 21$ と表せる．

演習問題

問題 2.1.1. 以下の整数 a, b に対して，最大公約数 $\gcd(a, b)$ および $ua + vb = \gcd(a, b)$ を満たすような u, v を一組求めよ．

(1) $(a, b) = (729, 1000)$
(2) $(a, b) = (323, 374)$
(3) $(a, b) = (858, 1914)$

2.2　合同式

以後，整数 $n > 0$ を一つ固定する．

定義 2.2.1. a, b を整数とする．a と b を n で割った余りが等しいとき，a と b は n を法として合同であるといい

$$a \equiv b \bmod n$$

と表す．

定義から，

$$a \equiv b \bmod n \iff \exists q \in \mathbb{Z} \text{ s.t. } a - b \in qn$$

である．

コメント． 例 1.2.2(2) より，$a \equiv b \bmod n$ は $\mathbb{Z}$ 上の同値関係である．

合同関係は以下のように和，積と相性が良い．

命題 2.2.2. $a \equiv b \bmod n$ かつ $a' \equiv b' \bmod n$ とする．このとき，

(1) $a + a' \equiv b + b' \bmod n$
(2) $aa' \equiv bb' \bmod n$

証明. 仮定より，ある整数 q, q' を用いて $a - b = qn$, $a' - b' = q'n$ とできる．

(1) $(a + a') - (b + b') = (a - b) + (a' - b') = qn + q'n = (q + q')n$ は n の倍数なので，$a + a' \equiv b + b' \bmod n$.

(2) $aa' - bb' = (a - b)a' + b(a' - b') = qna' + bq'n = (qa' + q'b)n$ の倍数なので，$aa' \equiv bb' \bmod n$. ■

例 2.2.3. $(m+1)$ 桁の自然数 N は

$$N = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 \cdot 10 + a_0$$
$$(0 \leq a_0, a_1, \ldots, a_m \leq 9,\ a_m \neq 0)$$

と表せる（a_i は N の i の位の数字）.
$n = 3$ のとき，$10 \equiv 1 \mod 3$ なので $10^i \equiv 1^i = 1 \mod 3$ となる．従って，

$$\begin{aligned} N &\equiv a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 \cdot 10 + a_0 \\ &\equiv a_m \cdot 1 + a_{m-1} \cdot 1 + \cdots + a_1 \cdot 1 + a_0 \\ &\equiv a_m + a_{m-1} + \cdots + a_1 + a_0 \mod 3 \end{aligned}$$

となる．このことから，N を 3 で割った余りと N の各桁の和 $a_m + a_{m-1} + \cdots + a_1 + a_0$ を 3 で割った余りは等しい.
$n = 9$ のときも $10 \equiv 1 \mod 9$ なので上と全く同様にして

$$N \equiv a_m + a_{m-1} + \cdots + a_1 + a_0 \mod 9$$

となる．従って，N を 9 で割った余りと N の各桁の和 $a_m + a_{m-1} + \cdots + a_1 + a_0$ を 9 で割った余りは等しい．例えば,

$$\begin{aligned} 1859135 &\equiv 1 + 8 + 5 + 9 + 1 + 3 + 5 \\ &\equiv 32 \\ &\equiv 3 + 2 \\ &\equiv 5 \\ &\equiv \begin{cases} 2 \mod 3 \\ 5 \mod 9 \end{cases} \end{aligned}$$

となり，1859135 を 3 で割った余りは 2，9 で割った余りは 5 となることが分かる.

整数 a, b に対して

$$ax \equiv b \mod n$$

の形の整数 x に関する方程式を **1 次合同式**と呼ぶ.

通常の 1 次方程式 $ax = b$（ただし $a \neq 0$）の場合，両辺に a の逆数を掛けることで

$$x = 1 \cdot x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}b$$

と解を求めることができる．同様に考えて，$au \equiv 1 \mod n$ となる整数 u を見つけることができれば

$$x = 1 \cdot x \equiv (au)x = u(ax) \equiv ub \mod n$$

となり，$x = ub + kn$ $(k \in \mathbb{Z})$ がこの方程式の一般解となる.

もちろんいつでも $au \equiv 1 \mod n$ なる u が存在するわけではない（$2u \equiv 1 \mod 4$ となる整数 u は存在しない）．このような u が存在するための条件は以下の命題で与えられる：

命題 2.2.4. a を整数とする．このとき，

$$au \equiv 1 \mod n \text{ となる整数 } u \text{ が存在する} \iff \gcd(a, n) = 1$$

証明. $(\Longrightarrow)$: $au \equiv 1 \mod n$ とすると，ある整数 q が存在して，$au - 1 = qn$ となる．このとき，$au - qn = 1$ となるので $\gcd(a, n) = 1$.

($\Longleftarrow$) : $\gcd(a,n)=1$ とすると，命題 2.1.6 より $ua+vn=1$ となる整数 u,v が存在する．このとき，$ua-1=vn$ なので $au\equiv 1 \bmod n$．■

コメント. 証明から分かるように，命題 2.1.6 を用いて $au+nv=1$ となる整数 u,v を見つければ，$au\equiv 1 \bmod n$ となる．

例 2.2.5. (1) $\gcd(39,25)=1$ なので $39u\equiv 1 \bmod 25$ となる整数 u が存在する．

実際，例 2.1.7(1) より $9\cdot 39-14\cdot 25=1$ なので $9\cdot 39\equiv 1 \bmod 25$.

(2) $\gcd(51,49)=1$ なので $51u\equiv 1 \bmod 49$ となる整数 u が存在する．

実際，例 2.1.7 のようにユークリッドの互除法を用いて計算すると，例えば $51\cdot 25+49\cdot(-26)=1$ が成り立つことが分かる．従って，$51\cdot 25\equiv 1 \bmod 49$.

1 次合同式

$$ax\equiv b \bmod n$$

に話を戻そう．$d=\gcd(a,n)$ と置いたとき，以下のようにしてこの方程式の一般解を求めることができる：

- b が d で割り切れないとき，$ax-b$ は n の倍数ではないので解は存在しない．
- b が d の倍数のとき，$a=a'd$, $b=b'd$, $n=n'd$ と表せる．上の 1 次合同式の両辺を d で割ると

$$ax\equiv b \bmod n \Longleftrightarrow a'x\equiv b' \bmod n'$$

となる．$\gcd(a',n')=1$ なので，定理 2.2.7 より $a'u\equiv 1 \bmod n'$ となる u が存在する．この u を用いると，この方程式の一般解は

$$x=ub'+kn' \quad (k\in\mathbb{Z})$$

で与えられる．

例 2.2.6. (1) $4x\equiv -12 \bmod 28$ の一般解を求める．

$d=\gcd(4,28)=4$ は -12 を割り切るので，この方程式は解を持つ．
$4x\equiv -12 \bmod 28$ の両辺を $d=4$ で割って，

$$x\equiv -3\equiv 7$$

を得る．従って，この 1 次合同式の一般解は

$$x=-3+7k \quad (k\in\mathbb{Z}).$$

(2) $1071x\equiv 42 \bmod 1029$ の一般解を求める．

$d=\gcd(1071,1029)=21$ は 42 を割り切るので，この方程式は解を持つ．
$1071x\equiv 42 \bmod 1029$ の両辺を 21 で割って，

$$51x\equiv 2 \bmod 49$$

を得る．例 2.2.5(2) より，$51\cdot 25\equiv 1 \bmod 49$ となるので，両辺を 25 で割って，

$$x\equiv 25\cdot 51x\equiv 25\cdot 2=50 \bmod 49$$

以上より，この方程式の一般解は

$$x=50+49k \quad (k\in\mathbb{Z}).$$

中国式剰余定理

3〜5 世紀ごろ，中国において孫子[*1]は以下のような問題に対する解放を与えた：

「25 で割ると 2 余り，7 で割ると 6 余る数は何か？」

例えば 27 はこの問題の答えとなる．

これを一般化したものが以下の定理である：

定理 2.2.7 (中国式剰余定理)．m, n を 0 でない互いに素な整数とする．任意の整数 a, b に対して，連立合同式

$$\begin{cases} x \equiv a \bmod m \\ x \equiv b \bmod n \end{cases}$$

を満たす整数 $0 \leq x_0 < mn$ がただ一つ存在する．また，この連立合同式の一般解はこの x_0 を用いて $x_0 + kmn$ $(k \in \mathbb{Z})$ と表せる．

証明．命題 2.1.6 により $mu + nv = 1$ となる整数 m, n が存在する．この u, v を用いて

$$y := anv + bmu$$

と置く．このとき，

- $mu \equiv (mu + nv) \equiv 1 \bmod n$ より $y \equiv bmu \equiv b \bmod n$.
- $nv \equiv (mu + nv) \equiv 1 \bmod m$ より $y \equiv anv \equiv a \bmod m$.

従って，この y は

$$\begin{cases} y \equiv a \bmod m \\ y \equiv b \bmod n \end{cases}$$

を満たす．

y を mn で割った余りを $0 \leq x_0 < mn$ とすれば，x_0 は

$$\begin{cases} x_0 \equiv a \bmod m \\ x_0 \equiv b \bmod n \end{cases}$$

を満たす．あとは問題の連立合同式の解が $x_0 + kmn$ $(k \in \mathbb{Z})$．の形になることを示せば良い．整数 z が

$$\begin{cases} z \equiv a \bmod m \\ z \equiv b \bmod n \end{cases}$$

を満たすとする．このとき，

- $z - x_0 \equiv a - a \equiv 0 \bmod m$ より $z - x_0$ は m の倍数
- $z - x_0 \equiv b - b \equiv 0 \bmod n$ より $z - x_0$ は n の倍数

m と n は互いに素なので，$z - x_0$ は mn の倍数である．従って，$z = x_0 + kmn$ $(k \in \mathbb{Z})$ と表せる． ■

[*1] 「兵法」を書いた孫子とは別人

コメント. m, n を 0 でない互いに素な整数とする．定理 2.2.7 の証明から，連立合同式

$$\begin{cases} x \equiv a \mod m \\ x \equiv b \mod n \end{cases}$$

の一般解は以下のように求めることができる：

(i) $mu + nv = 1$ となるような整数 u, v を見つける（命題 2.1.6 参照）
(ii) $y = bmu + anv$ と置くと $y \equiv a \mod m$, $y \equiv b \mod n$ が成り立つ．
(iii) y を mn で割った余りを x_0 とすれば，上の連立合同式の一般解は $x_0 + kmn$ $(k \in \mathbb{Z})$ である．

例 2.2.8. 連立合同式

$$\begin{cases} x \equiv 2 \mod 25 \\ x \equiv 6 \mod 7 \end{cases}$$

の一般解を求める．

(i) ユークリッドの互除法より

$$\begin{aligned} \gcd(25, 7) &= \gcd(7, 4) \quad (25 = 3 \cdot 7 + 4) \\ &= \gcd(4, 3) \quad (7 = 1 \cdot 4 + 3) \\ &= \gcd(3, 1) \quad (4 = 1 \cdot 3 + 1) \end{aligned}$$

となるので，

$$\begin{aligned} 1 &= 4 - 3 \\ &= 4 - (7 - 4) = (-1) \cdot 7 + 2 \cdot 4 \\ &= (-1) \cdot 7 + 2 \cdot (25 - 3 \cdot 7) = 2 \cdot 25 + (-7) \cdot 7 \end{aligned}$$

と表せる．
(ii) $y = 6 \cdot 2 \cdot 25 + 2 \cdot (-7) \cdot 7 = 300 - 98 = 202$ とすると，$y \equiv 2 \mod 25$, $y \equiv 6 \mod 7$ が成り立つ．
(iii) $y = 202$ を $25 \cdot 7 = 175$ で割った余りは $x_0 = 27$ なので，この連立合同式の一般解は $27 + 175k$ $(k \in \mathbb{Z})$.

フェルマーの小定理

最後に，整数のべきの余りを計算する強力な方法であるフェルマーの小定理を紹介する．

定理 2.2.9 (フェルマーの小定理)**.** p を素数とする．このとき，整数 $x \in \{1, 2 \ldots, p-1\}$ に対して，

$$x^{p-1} \equiv 1 \mod p$$

証明. まず最初に，$x, 2x, \ldots (p-1)x$ を p で割った余りは全て異なることに注意しておく．実際，$1 \le i < j \le p-1$ に対して，$0 < j - i \le p-2$ かつ x は p と互いに素なので，

$$jx - ix = (j - i)x$$

は p の倍数になり得ない．従って，jx と ix を p で割った余りは全て異なる．

このことから，$x, 2x, \ldots (p-1)x$ を p で割った余りには $1, 2, \ldots, p-1$ がひとつずつ現れる．従って，

$$x \cdot (2x) \cdots ((p-1)x) \equiv 1 \cdot 2 \cdots (p-1) \mod p$$

となり，

$$(p-1)!x^{p-1} \equiv (p-1)! \bmod p$$

$(p-1)!$ は p と互いに素なので，

$$x^{p-1} \equiv 1 \bmod p$$

を得る．■

フェルマーの小定理の一般化（おまけ）

定義 2.2.10. 整数 n に対して，

$$\varphi(n) := (n \text{ と互いに素な整数 } 1 \leq a \leq n \text{ の個数})$$

と定義する．この関数 φ を**オイラー関数**と呼ぶ．

例 2.2.11. (1) 小さな整数 n について $\varphi(n)$ は以下のようになる：

n	1	2	3	4	5	6	7	8	9	10	$\cdots$
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	$\cdots$

(2) p が素数のとき，$\varphi(p) = p-1$ となる．

フェルマーの小定理と全く同様にして以下の定理を示すことができる．

定理 2.2.12 (オイラーの定理)**.** n を正の整数とする．このとき，n と互いに素な整数 x に対して，

$$x^{\varphi(n)} \equiv 1 \bmod n$$

が成り立つ．

オイラーの定理は公開鍵暗号と呼ばれる暗号方式に用いられている．例えばインターネット上の電子署名などでこの暗号方式は使われている．公開鍵暗号の安全性の根拠は相異なる素数 p, q に対して，$\varphi(pq)$ を計算すること（$\fallingdotseq n$ を素因数分解を計算すること）が経験上難しいということにあるが，近年では量子コンピュータ等の発展によりその安全性が揺らいでいる．

演習問題

問題 2.2.1. 以下の 1 次合同式の一般解を求めよ：

(1) $39x \equiv 3 \bmod 25$
(2) $12x \equiv 18 \bmod 30$
(3) $201x \equiv 2 \bmod 2839$
(4) $129x \equiv 21 \bmod 1566$

問題 2.2.2. 以下の連立合同式の一般解を求めよ：

(1) $\begin{cases} x \equiv 3 \bmod 7 \\ x \equiv 2 \bmod 5 \end{cases}$

(2) $\begin{cases} x \equiv 2 \bmod 9 \\ x \equiv 3 \bmod 11 \end{cases}$

(3) $\begin{cases} x \equiv 15 \bmod 23 \\ x \equiv 6 \bmod 17 \end{cases}$

(4) $\begin{cases} x \equiv 24 \bmod 37 \\ x \equiv 19 \bmod 25 \end{cases}$

第 3 章

群と準同型写像

この章では群の定義とその基本的な性質を扱う．

3.0　群とは

群とは，和や積などの演算を一つ備えた集合のことであり，大きく分けると以下の二つの側面がある：

- 和や積の性質を一般化/抽象化する（様々な対象を同時に扱うことができる）
- 様々な対称性（何らかの性質を保つ全単射）を記述する
  - 代数方程式の解の公式の理論（解の入れ替えに関する対称性）
  - 図形の対称性（合同変換に関する対称性）

数の演算の一般化としての群

整数，有理数，実数，複素数などの和，積は似た性質を持っている．例えば，整数の和は以下の性質を持っている：

- （結合法則）$(x+y)+z=x+(y+z)$
- （単位元）$x+0=x+0=x$
- （逆元）$x+(-x)=(-x)+x=0$

従って，整数の集合 $\mathbb{Z}$ **は加法に関して群である**[*1]．有理数，実数，複素数の和も同様の性質を持っており，$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ も加法に関して群となる．

また，0 でない実数の積は以下の性質を持つ：

- （結合法則）$(xy)z=x(yz)$
- （単位元）$x\cdot 1=1\cdot x=x$
- （逆元）$x\cdot x^{-1}=x^{-1}\cdot x=1$

従って，0 でない実数の集合 $\mathbb{R}\setminus\{0\}$ **は乗法に関して群である**．0 でない有理数，0 でない複素数の積も同様の性質を持っており，$\mathbb{Q}\setminus\{0\}$, $\mathbb{C}\setminus\{0\}$ も乗法に関して群となる．

これらは和と積という異なる演算についての性質であるが，

$$x+y\longleftrightarrow xy,\quad 0\longleftrightarrow 1,\quad -x\longleftrightarrow x^{-1}$$

と読み替えると同じことを述べていることが分かる．これらの演算の持つ性質を抽象化したものが**群**である．

群という抽象的な概念を考えるメリットを述べるために，以下の二つの定理を紹介する：

[*1] 群の正確な定義はこれからしていく

定理 3.0.1. n を正整数とする．このとき，整数 $x \in \{0, 1, \ldots, n-1\}$ に対して，

$$n \cdot x \equiv 0 \mod n$$

定理 3.0.2 (フェルマーの小定理（系 4.1.11）)**.** n を素数とする．このとき，整数 $x \in \{1, 2 \ldots, n-1\}$ に対して，

$$x^{n-1} \equiv 1 \mod n$$

この二つの定理は主張の形は似ているが，全く異なることを述べている．従って，その証明もそれぞれ別々に与えられる（一つ目の定理は当たり前の主張であるが）．しかし，群という側面からみると，これらは一般の群に対する次の定理を特別な群に適用したものとして得られる：

定理 3.0.3. G を元の個数が n 個の有限群とする．このとき，G の元 x に対して

$$x^n = 1$$

が成り立つ．

このように群という抽象的な対象を考えることで，無数に存在する具体的な群に対して個別に議論をする必要が無くなる．

方程式の解の対称性

n 次代数方程式

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

を考える．この方程式には解の公式が存在するだろうか？より正確には，全ての解が a_0, a_1, …, a_{n-1} から四則演算とべき根を用いて表せるだろうか？ 2 次の場合は高校学んだように平方完成をすることで容易に解の公式を得る．3 次と 4 次の場合も，2 次の場合と比べると非常に複雑であるが，それぞれタルタリア[*2]およびフェラーリ[*3]により解の公式が発見された．それでは 5 次以上の場合の解の公式についてはどうか？

解の公式の研究から群がどのように現れたかざっくりと説明する．ここでは簡単のために $n = 3$ の場合を考える．方程式の左辺を

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = (x - \beta_1)(x - \beta_2)\cdots(x - \beta_n)$$

と因数分解すると，解と係数の関係により

$$\begin{aligned} a_{n-1} &= -(\beta_1 + \beta_2 + \cdots + \beta_n), \\ a_{n-2} &= (-1)^2 \sum_{i<j} \beta_i \beta_j, \\ &\vdots \\ a_0 &= -\beta_1 \beta_2 \cdots \beta_n \end{aligned}$$

と表せる．この右辺に現れる式は β_1, β_2, …, β_n を入れ替えても変わらない式である．このような式のことを β_1, β_2, …, β_n の**対称式**と呼ぶ．実は，β_1, β_2, …, β_n の対称式は $a_0, a_1, \ldots, a_{n-1}$ から四則演算を用いて得られることが分かる．

ここで，

$$S_n := \{\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} \mid \sigma \text{ は全単射 }\}$$

[*2] Tartaglia (∼1557)
[*3] Ferrari (1522∼1565)

と置くと，S_n の写像の合成は以下の性質を満たす

- （結合法則）$(\sigma \circ \tau) \circ \rho = \sigma \circ (\tau \circ \rho)$
- （単位元）$\sigma \circ \mathsf{id}_{\{1,2,\dots,n\}} = \mathsf{id}_{\{1,2,\dots,n\}} \circ \sigma = \sigma$
- （逆元）$\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathsf{id}_{\{1,2,\dots,n\}}$ が成り立つ．

従って，**S_n は写像の合成により群となる．**

群 S_n を用いると，上に述べた事実は以下のように述べることができる：β_1, β_2, …, β_n の式 $f(\beta_1, \beta_2, \dots, \beta_n)$ に対して，

$$
\begin{aligned}
&f(\beta_1, \beta_2, \dots, \beta_n) \text{ が対称式} \\
&\quad \Longleftrightarrow \text{任意の } \sigma \in S_n \text{ に対して } f(\beta_{\sigma(1)}, \beta_{\sigma(2)}, \dots, \beta_{\sigma(n)}) = f(\beta_1, \beta_2, \dots, \beta_n) \\
&\quad \Longleftrightarrow f(\beta_1, \beta_2, \dots, \beta_n) \text{ は } a_0, a_1, \dots, a_{n-1} \text{ から四則演算を用いて得られる}
\end{aligned}
$$

この議論を発展させると，「$a_0, a_1, \dots, a_{n-1}$ から四則演算とべき根を用いてどのような複素数が表せるか」が S_n の群構造を見ることで理解することができる．この考え方でアーベル[*4]は以下の定理を示した．

定理 3.0.4.　（アーベル）5 次以上の代数方程式には解の公式が存在しない（つまり，$n \geq 5$ のとき S_n は可解群[a]ではない）．

[a] この講義では扱わない

その後，ガロア[*5]は与えられた n 次代数方程式が四則演算とべき根を用いて解けるための条件を**ガロア群**と呼ばれる群を用いて与えた[*6]．ガロアの理論は今日**ガロア理論**と呼ばれている．

図形の対称性

図形の対称性からも群の概念は自然に現れる．

平面 $\mathbb{R}^2$ から自分自身への全単射 $f : \mathbb{R}^2 \to \mathbb{R}^2$ であり，2 点間の距離を保つものを**合同変換**と呼ぶ：

$$|f(\boldsymbol{x}) - f(\boldsymbol{y})| = |\boldsymbol{x} - \boldsymbol{y}| \quad (\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^2)$$

例えば，平行移動，回転，鏡映（= ある直線についての反転）は合同変換である．実は，すべての合同変換は平行移動，回転，鏡映を有限回繰り返すことで得られる．

平面内の図形 X に対して，X を動かさない合同変換の集合を $\mathsf{E}(X)$ と表す：

$$\mathsf{E}(X) := \{f : \mathbb{R}^2 \to \mathbb{R}^2 \mid f \text{ は合同変換で } f(X) = X\}$$

$\mathsf{E}(X)$ の元の合成は以下の性質を満たす：

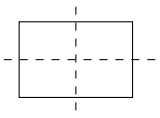
- （結合法則）$(h \circ g) \circ f = h \circ (g \circ f)$
- （単位元）$f \circ \mathsf{id}_{\mathbb{R}^2} = \mathsf{id}_{\mathbb{R}^2} \circ f = f$
- （逆元）$f \circ f^{-1} = f^{-1} \circ f = \mathsf{id}_{\mathbb{R}^2}$

従って，**$\mathsf{E}(X)$ は変換の合成により群となる．**

$\mathsf{E}(X)$ の元は図形 X の平行移動対称性，回転対称性，鏡映対称性を表している．従って，$\mathsf{E}(X)$ に多くの元が含まれるほどその図形は対称性が高いと言える．

[*4] Abel (1802～1829)
[*5] Galois (1811～1832)
[*6] 詳しくは代数学 2 で扱う

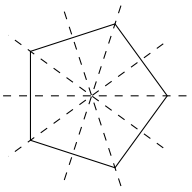
- 平面内の長方形 R を考える：



このとき，$\mathsf{E}(R)$ の元は
  - 動かさない変換 $\mathsf{id}_{\mathbb{R}^2}$
  - 中心の周りに π だけ回転させる変換
  - 点線に関して反転

の 4 個からなる．

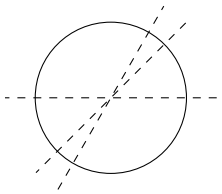
- 平面内の正五角形 P を考える：



このとき，$\mathsf{E}(P)$ の元は
  - 動かさない変換 $\mathsf{id}_{\mathbb{R}^2}$
  - 中心の周りに $2\pi/5$, $4\pi/5$, $8\pi/5$, $8\pi/5$ だけ回転させる変換
  - 点線に関して反転

の 10 個からなる．

- 平面内の円 C を考える：



このとき，$\mathsf{E}(C)$ の元は
  - 動かさない変換 $\mathsf{id}_{\mathbb{R}^2}$
  - 円の中心の周りに任意の角度だけ回転させる変換（無限個）
  - 任意の直径に関する反転（無限個）

の無限個からなる．

以上のことから，長方形，正五角形，円の順に対称性が高いと考えることができる．図形の変換のなす群を用いることで，とらえどころのない直感的な概念である図形の対称性を数学的に扱うことができるようになる．

群は一つの演算のみを扱う最も単純な代数系のひとつである．従ってその適用範囲はとても広く，数学以外にも様々な分野において重要な役割を果たす：

- 化学（結晶，分子構造の対称性）
- 物理学（対称性と保存量（ネーターの定理），素粒子の対称性）
- コンピュータサイエンス，暗号理論（楕円曲線暗号，RSA 暗号）
- 人文科学（ムルンギン族の婚姻体系）

3.1　群の定義

群の定義は抽象的で最初は分かりにくく感じるかもしれないが，以下の例 3.1.4 に挙げるような具体的な例を常に頭に浮かべておくと良い．

X を集合とする．X 上の**演算**とは，X の全ての 2 元 x, y に一つの X の元 $x * y$ を対応させる規則（言い換えれば，写像 $X \times X \to X,\ (x, y) \mapsto x * y$）のことである．一見難しく見えるが以下のようなものをイメージすると良い．

例 3.1.1. (1) 実数の加法，減法，乗法

$$a + b, \quad a - b, \quad ab$$

は $\mathbb{R}$ 上の演算である（0 による割り算は定義されていないので除法は $\mathbb{R}$ 上の演算ではない）．

(2) 行列の加法，減法，乗法

$$A + B, \quad A - B, \quad AB$$

は n 次の実正方行列全体の集合 $\mathsf{M}_n(\mathbb{R})$ 上の演算である．

定義 3.1.2 (群の定義)**.** (1) 空集合でない集合 G 上の演算

$$a * b \quad (a, b \in G)$$

を考える．G がこの演算 $*$ に関して**群**であるとは，以下の条件が満たされるときに言う：

(i)（結合法則）
全ての $a, b, c \in G$ に対して $a * (b * c) = (a * b) * c$ が成り立つ．

(ii)（単位元の存在）
G の元 e_G が存在して，全ての $a \in G$ に対して $a * e_G = e_G * a = a$ を満たす．
この e_G を G の**単位元**と呼ぶ．

(iii)（逆元の存在）
G の各元 a に対して，$a * a' = a' * a = e_G$ を満たす G の元 a' が存在する．
この a' を a の**逆元**と呼ぶ．

(2) G の元の個数を $|G|$ と書き，G の**位数**と呼ぶ．$|G| < \infty$ のとき，G を**有限群**と呼ぶ．

定義 3.1.3. 群 G は条件

(iv) 全ての $a, b \in G$ に対して $a * b = b * a$ が成り立つ．

を満たすとき，**可換群**または**アーベル群**と呼ぶ．

群の演算は，積 ab または和 $a + b$ で表すことが多い．

- 積 ab で表すとき G を**乗法群**と呼び，単位元，逆元をそれぞれ 1_G, a^{-1} と表す．
- 和 $a + b$ で表すとき G を**加法群**と呼び，単位元，逆元をそれぞれ 0_G, $-a$ と表す． また，演算を和で表す場合は可換群であることを仮定するのが普通である．

以下，この講義では**特に断らない限り群の演算は積で表すことにする．**

例 3.1.4. (1) 一つの元からなる集合 $G = \{1_G\}$ は演算

$$1_G \cdot 1_G := 1_G$$

により可換群となる．これを**自明群**と呼ぶ．

(2) 整数全体の集合 $\mathbb{Z}$ は加法 $+$ により可換群となる：

実際，$a, b, c \in \mathbb{Z}$ に対して以下が成り立つ：

(i) $(a+b)+c = a+(b+c)$

(ii) $a+0 = 0+a = 0$

(iii) $a+(-a) = (-a)+a = 0$

(iv) $a+b = b+a$

特に，$\mathbb{Z}$ の単位元は 0，$a \in \mathbb{Z}$ の逆元は $-a$ である．

同様に，$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ も加法により可換群となる（$\mathbb{N}$ は加法では群にならない[a]）．

(3) 0 でない実数全体の集合 $\mathbb{R} \setminus \{0\}$ は乗法 $\cdot$ により可換群となる：

実際，$a, b, c \in \mathbb{R} \setminus \{0\}$ に対して以下が成り立つ：

(i) $(ab)c = a(bc)$

(ii) $a1 = 1a = 0$

(iii) $aa^{-1} = a^{-1}a = 1$

(iv) $ab = ba$

特に，$\mathbb{R} \setminus \{0\}$ の単位元は 1，$a \in \mathbb{R} \setminus \{0\}$ の逆元は $a^{-1} = 1/a$ である．

同様に，$\mathbb{Q} \setminus \{0\}, \mathbb{C} \setminus \{0\}$ も乗法により可換群となる（$\mathbb{Z} \setminus \{0\}$ は乗法で群にならない[b]）．

(4)（**一般線形群（General Linear Group）**）

n 次実正則行列全体の集合 $\mathsf{GL}_n(\mathbb{R})$ は行列の積により群となる：

実際，$A, B, C \in \mathsf{GL}_n(\mathbb{R})$ に対して以下が成り立つ：

(i) $(AB)C = A(BC)$

(ii) $AE_n = E_nA = A$

(iii) $AA^{-1} = A^{-1}A = E_n$

特に，$\mathsf{GL}_n(\mathbb{R})$ の単位元は単位行列 E_n，$A \in \mathsf{GL}_n(\mathbb{R})$ の逆元は逆行列 A^{-1} である．

また，$n \geq 2$ のとき $\mathsf{GL}_n(\mathbb{R})$ は可換群ではない：

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} \neq \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

n 次複素正則行列の集合 $\mathsf{GL}_n(\mathbb{C})$ も同様に行列の積により群となる．

(5)（**クラインの四元群**）

4 つの文字 $1, i, j, k$ からなる集合 $G = \{1, i, j, k\}$ を考える．集合 G に演算を以下の様に定義する：

	1	i	j	k
1	1	i	j	k
i	i	1	k	j
j	j	k	1	i
k	k	j	i	1

（この表の見方：第 x 列第 y 行の成分には x と y の積 xy を書いている）

この演算により G が群となることが容易にチェックできる．

(6)（**直積群**）

G_1, G_2 を群とする．このとき，直積集合

$$G_1 \times G_2 := \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$$

は成分ごとの演算

$$(g_1, g_2)(g_1', g_2') := (g_1 g_1', g_2 g_2')$$

で群となる．この群の単位元は $(1_{G_1}, 1_{G_2})$，(g_1, g_2) の逆元は $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$ である．

直積する群の数を増やして

$$G_1 \times G_2 \times \cdots \times G_n := \{(g_1, g_2, \ldots, g_n) \mid g_1 \in G_1, g_2 \in G_2, \ldots, g_n \in G_n\}$$

を考えても成分ごとの演算

$$(g_1, g_2, \ldots, g_n)(g_1', g_2', \ldots, g_n') := (g_1 g_1', g_2 g_2', \ldots, g_n g_n')$$

により群となる．

例えば，$\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}$ はベクトルの和で群になる．

[a] $-3 \notin \mathbb{N}$
[b] $3^{-1} \notin \mathbb{Z} \setminus \{0\}$

以下，例などで現れた群は特に断らない限りそこの演算で群になっていると思うことにする．例えば，$\mathbb{Z}$ と書いたら何も言わなくても加法で群に，$\mathbb{R} \setminus \{0\}$ と書いたら何も言わなくても乗法で群になっていると思う．

注意. 同じ集合が異なる演算で群になることはあり得る（問題 3.1.3 を見よ）．

コメント. G を群とする．結合法則を用いると $a, b, c, d \in G$ に対して，

$$((ab)c)d,\ (a(bc))d,\ a((bc)d),\ a(b(cd)),\ (ab)(cd)$$

は全て等しいことが分かる．そこで，これらを単に $abcd$ と書く．もっと一般に，n 個の元 $a_1, a_2, \ldots, a_n \in G$ をこの順番に掛け算したとき，その結果はどこから掛け算を始めても同じものになる[*7]．それを括弧をつけずに単に

$$a_1 a_2 \cdots a_n$$

と書く（加法群のときは $a_1 + a_2 + \cdots + a_n$ と書く）．

定義 3.1.5. G を群とする．$a \in G$ と自然数 n に対して，a の **n 乗** a^n を以下の様に定義する：

$$a^n := \begin{cases} \overbrace{a \cdot a \cdot \cdots \cdot a}^{n\text{ 個}} & (n > 0 \text{ のとき}) \\ 1_G & (n = 0 \text{ のとき}) \\ (a^{-n})^{-1} & (n < 0 \text{ のとき}) \end{cases}$$

[*7] $a_1, a_2, \ldots, a_n$ の積は括弧の付け方により $\frac{(2n-2)!}{n!(n-1)!}$ 通りあるがそれらは全て等しくなる．この個数 $\frac{(2n-2)!}{n!(n-1)!}$ はカタラン数と呼ばれ，それだけで一冊の本があるほど重要な数である．

G が加法群のときは加法を使うので n 乗ではなく n **倍** na で表す：

$$na := \begin{cases} \overbrace{a+a+\cdots+a}^{n\text{ 個}} & (n>0 \text{ のとき}) \\ 0_G & (n=0 \text{ のとき}) \\ -((-n)a) & (n<0 \text{ のとき}) \end{cases}$$

となる．

注意. 上の定義は $\mathbb{Q}-\{0\}, \mathbb{R}-\{0\}, \mathbb{C}-\{0\}$ や $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ の場合には通常の n 乗や n 倍と同じものになっている．

以下の事実は線形代数学で学んだ逆行列の性質を思い出すと分かりやすい：

命題 3.1.6. G を群とする．

(1) $a, b \in G$ に対して，$(ab)^{-1} = b^{-1}a^{-1}$.

(2) $a \in G$ に対して，$(a^{-1})^{-1} = a$.

（加法群の場合は $-(a+b) = (-a)+(-b)$, $-(-a) = a$ を意味する）．

証明. (1) $b^{-1}a^{-1}$ が ab の逆元であることを確かめれば良い．これは

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}1b = b^{-1}b = 1_G$$
$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a1a^{-1} = aa^{-1} = 1_G$$

から分かる．

(2) a が a^{-1} の逆元であることを確かめれば良い．a^{-1} が a の逆元なので $aa^{-1} = a^{-1}a = 1_G$ が成り立っている．このことから，a は a^{-1} の逆元である． ■

この命題を繰り返し用いることで，通常の数の指数法則が群に対しても成り立つことが確かめられる：

系 3.1.7 (指数法則)． G を群とする．$a \in G$ と $m, n \in \mathbb{Z}$ に対して，

$$a^m \cdot a^n = a^{m+n},\ (a^m)^n = a^{mn}$$

が成り立つ（加法群の場合は $ma+na = (m+n)a$, $n(ma) = (mn)a$ を意味する）．

演習問題

問題 3.1.1. $G = \{1, i, j, k\}$ をクラインの四元群とする．

(1) i^{-1}, j^{-1}, k^{-1} が何か答えよ．

(2) G が可換群かどうか答えよ．

問題 3.1.2. 以下の群 G と $a, b, c \in G$ に対して，ac^2 と $ab^{-1}c^2b$ を計算せよ．

(1) $G = \mathsf{GL}_2(\mathbb{R})$, $a = \begin{pmatrix} 3 & -1 \\ 2 & 2 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$, $c = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$

(2) $G=\mathbb{Z}$, $a=-1$, $b=2$, $c=4$

(3) G はクラインの四元群，$a=i$, $b=j$, $c=k$

ここで，G の演算は 例 3.1.4 のものを考えている（(2) の G は加法群であることに注意!!）.

問題 3.1.3. 集合 $\mathbb{Z}$ が演算

$$x*y:=x+y+1 \quad (x,y\in\mathbb{Z})$$

で群となることを以下のように示せ：

(i) 演算 $x*y$ が結合法則を満たすことを示せ.

(ii)「任意の $x\in\mathbb{Z}$ に対して $x*a=x$」を満たすような a を見つけよ.

(iii) $x\in\mathbb{Z}$ に対して，$x*x'=a$ を満たす x' を見つけよ.

問題 3.1.4. 集合 $G:=\mathbb{R}\setminus\{-1\}$（$-1$ 以外の実数全体の集合）上の演算

$$x*y:=x+y+xy \quad (x,y\in G)$$

を考える.

(1) $x,y\in G$ に対して，$x*y\in G$ を示せ.

(2) G がこの演算に関して群となることを示せ.

(3) G における 3, 9 の逆元をそれぞれ求めよ.

(4) $3*x*5=9$ を満たすような $x\in G$ を求めよ.

問題 3.1.5. 集合 $G:=\{(a,b)\in\mathbb{R}^2 \mid a\neq 0\}$ 上の演算

$$(a,b)*(c,d):=(ac,ad+b)$$

を考える.

(1) G がこの演算で群になることを示せ.

(2) G が可換群かどうか答えよ.

問題 3.1.6. G を群とし，$a,b,c\in G$ とする.

(1) $ac=bc$ ならば $a=b$ となることを示せ.

(2) $ab=ba$ ならば $ab^{-1}=b^{-1}a$ となることを示せ.

問題 3.1.7. G を群とする．G の元 a,b に対して $[a,b]:=aba^{-1}b^{-1}$ と置き，これを a と b の**交換子**と呼ぶ.

(1) $a,b\in G$ に対して

$$[a,b]=1_G \Longleftrightarrow ab=ba$$

を示せ.

(2) $a,b\in G$ に対して

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

を示せ.

(3) $a, b, g \in G$ に対して

$$g[a,b]g^{-1} = [gag^{-1}, gbg^{-1}]$$

を示せ.

3.2　整数の剰余群と対称群

この節では重要な群の例である，整数の剰余のなす群，数の置換のなす群を紹介する．

整数の剰余群

以下，正の整数 n を一つ固定する．
整数 a に対して記号 $\overline{a}$ を導入する．この記号は

$$\overline{a} = \overline{b} :\Longleftrightarrow a \equiv b \bmod n$$

を満たすものと約束する．また，

$$\mathbb{Z}/n\mathbb{Z} := \{\overline{a} \mid a \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

と定める．２つ目の等式は，整数 a を n で割った余りが $r \in \{0, 1, \ldots, n-1\}$ のときに $\overline{a} = \overline{r}$ となることから分かる．

例 3.2.1. (1) $n = 3$ のとき，

$$\cdots = \overline{-9} = \overline{-6} = \overline{-3} = \overline{0} = \overline{3} = \overline{6} = \overline{9} = \cdots$$
$$\cdots = \overline{-8} = \overline{-5} = \overline{-2} = \overline{1} = \overline{4} = \overline{7} = \overline{10} = \cdots$$
$$\cdots = \overline{-7} = \overline{-4} = \overline{-1} = \overline{2} = \overline{5} = \overline{8} = \overline{11} = \cdots$$

となるので $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$.

(2) $n = 4$ のとき，

$$\cdots = \overline{-12} = \overline{-8} = \overline{-4} = \overline{0} = \overline{4} = \overline{8} = \overline{12} = \cdots$$
$$\cdots = \overline{-11} = \overline{-7} = \overline{-3} = \overline{1} = \overline{5} = \overline{9} = \overline{13} = \cdots$$
$$\cdots = \overline{-10} = \overline{-6} = \overline{-2} = \overline{2} = \overline{6} = \overline{10} = \overline{14} = \cdots$$
$$\cdots = \overline{-9} = \overline{-5} = \overline{-1} = \overline{3} = \overline{7} = \overline{11} = \overline{15} = \cdots$$

となるので $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$.

定義 3.2.2. $a, b \in \mathbb{Z}$ に対して，$\overline{a}$ と $\overline{b}$ の和，積をそれぞれ

$$\overline{a} + \overline{b} := \overline{a+b}$$
$$\overline{a} \cdot \overline{b} := \overline{ab}$$

で定義する．

$\mathbb{Z}/n\mathbb{Z}$ の一つの元には複数の表し方がある（$\overline{a+nk}$ $(k \in \mathbb{Z})$ は全て $\overline{a}$ と一致する）．上の和と積の定義はこの表し方に依存するような定義であるが，結果が表し方に依存してしまうと問題である．しかし，以下の命題によりこのような心配はない．

命題 3.2.3. (1) $\overline{a} = \overline{a'}$, $\overline{b} = \overline{b'}$ ならば $\overline{a} + \overline{b} = \overline{a'} + \overline{b'}$
(2) $\overline{a} = \overline{a'}$, $\overline{b} = \overline{b'}$ ならば $\overline{a} \cdot \overline{b} = \overline{a'} \cdot \overline{b'}$

証明. これは命題 2.2.2 の言い換えである． ■

定理 3.2.4. $\mathbb{Z}/n\mathbb{Z}$ は定義 3.2.2 で定義した加法 $\overline{a}+\overline{b}:=\overline{a+b}$ により可換群となる．

証明. 可換群の定義の (i), (ii), (iii), (iv) を確かめる．

(i) $\overline{a},\overline{b},\overline{c}\in\mathbb{Z}/n\mathbb{Z}$ に対して，

$$(\overline{a}+\overline{b})+\overline{c}=\overline{a+b}+\overline{c}=\overline{(a+b)+c}=\overline{a+(b+c)}=\overline{a}+\overline{b+c}=\overline{a}+(\overline{b}+\overline{c})$$

が成り立つ．

(ii) $\overline{a}\in\mathbb{Z}/n\mathbb{Z}$ に対して，

$$\overline{a}+\overline{0}=\overline{a+0}=\overline{a}$$
$$\overline{0}+\overline{a}=\overline{0+a}=\overline{a}$$

が成り立つ．従って，$\overline{0}$ が $\mathbb{Z}/n\mathbb{Z}$ の単位元である．

(iii) $\overline{a}\in\mathbb{Z}/n\mathbb{Z}$ に対して，

$$\overline{a}+\overline{-a}=\overline{a+(-a)}=\overline{0}$$
$$\overline{-a}+\overline{a}=\overline{(-a)+a}=\overline{0}$$

が成り立つ．従って，$\overline{-a}$ が $\mathbb{Z}/n\mathbb{Z}$ における $\overline{a}$ の逆元である．

(iv) $\overline{a},\overline{b}\in\mathbb{Z}/n\mathbb{Z}$ に対して，

$$\overline{a}+\overline{b}=\overline{a+b}=\overline{b+a}=\overline{b}+\overline{a}$$

が成り立つ．

以上のことから，$\mathbb{Z}/n\mathbb{Z}$ が加法群であることが示された． ■

次に $\mathbb{Z}/n\mathbb{Z}$ の積を考える．$\mathbb{Z}/n\mathbb{Z}$ の元 $\overline{a}$ は一般に積に関する逆元（$\overline{a}\cdot\overline{b}=\overline{1}$ となる $\overline{b}$）を持たない．例えば $n=6$ のとき，$\overline{2}$ は掛け算に関する逆元を持たない．逆元を持つための条件は以下の命題により分かる．

命題 3.2.5. $\overline{a}\in\mathbb{Z}/n\mathbb{Z}$ に対して，以下が成り立つ：

$$\text{ある } \overline{b}\in\mathbb{Z}/n\mathbb{Z} \text{ が存在して } \overline{a}\cdot\overline{b}=\overline{1} \text{ が成り立つ} \iff \mathsf{gcd}(a,n)=1$$

$\overline{a}$ の積に関する逆元（$\overline{a}\cdot\overline{b}=\overline{1}$ を満たす $\overline{b}$）を $\overline{a}^{-1}$ と書く．

証明. これは定理 2.2.7 の言い換えである． ■

例 3.2.6. (1) $n=25$ とすると，例 2.2.5(1) より $\overline{39}^{-1}=\overline{9}$.
(2) $n=49$ とすると，例 2.2.5(2) より $\overline{51}^{-1}=\overline{25}$.

定義 3.2.7. $\mathbb{Z}/n\mathbb{Z}$ の可逆元（積に関して逆元を持つ元）の集合を

$$(\mathbb{Z}/n\mathbb{Z})^{\times}:=\{\overline{a}\in\mathbb{Z}/n\mathbb{Z}\mid \mathsf{gcd}(a,n)=1\}$$

と表す．

例 3.2.8. (1) $n=2$ のとき，$(\mathbb{Z}/2\mathbb{Z})^\times=\{\overline{1}\}$．また，$\overline{1}^{-1}=\overline{1}$.
(2) $n=3$ のとき，$(\mathbb{Z}/3\mathbb{Z})^\times=\{\overline{1},\overline{2}\}$．また，$\overline{1}^{-1}=\overline{1}$, $\overline{2}^{-1}=\overline{2}$.
(3) $n=4$ のとき，$(\mathbb{Z}/4\mathbb{Z})^\times=\{\overline{1},\overline{3}\}$．また，$\overline{1}^{-1}=\overline{1}$, $\overline{3}^{-1}=\overline{3}$.
(4) $n=6$ のとき，$(\mathbb{Z}/6\mathbb{Z})^\times=\{\overline{1},\overline{5}\}$．また，$\overline{1}^{-1}=\overline{1}$, $\overline{5}^{-1}=\overline{5}$.
(5) p が素数のとき，$(\mathbb{Z}/p\mathbb{Z})^\times=\{\overline{1},\overline{2},\dots,\overline{p-1}\}$（$\rightsquigarrow$ フェルマーの小定理）.

定理 3.2.9. $(\mathbb{Z}/n\mathbb{Z})^\times$ は定義 3.2.2 で定義された乗法 $\overline{a}\cdot\overline{b}:=\overline{ab}$ により可換群となる．

証明. まずはこの積が $(\mathbb{Z}/n\mathbb{Z})^\times$ 上の演算を定めること，つまり $\overline{a}$, $\overline{b}\in(\mathbb{Z}/n\mathbb{Z})^\times$ に対して $\overline{a}\cdot\overline{b}\in(\mathbb{Z}/n\mathbb{Z})^\times$ となることに注意しておく．実際，$\overline{a},\overline{b}$ に対して $\gcd(a,n)=\gcd(b,n)=1$ なので $\gcd(ab,n)=1$ である．従って，$\overline{a}\cdot\overline{b}=\overline{ab}\in(\mathbb{Z}/n\mathbb{Z})^\times$.

次に，可換群の定義の (i), (ii), (iii), (iv) を確かめる．

(i) $\overline{a},\overline{b},\overline{c}\in(\mathbb{Z}/n\mathbb{Z})^\times$ に対して，

$$(\overline{a}\cdot\overline{b})\cdot\overline{c}=\overline{ab}\cdot\overline{c}=\overline{(ab)c}=\overline{a(bc)}=\overline{a}\cdot\overline{bc}=\overline{a}\cdot(\overline{b}\cdot\overline{c})$$

が成り立つ．

(ii) $\overline{a}\in(\mathbb{Z}/n\mathbb{Z})^\times$ に対して，

$$\overline{a}\cdot\overline{1}=\overline{a\cdot1}=\overline{a}$$
$$\overline{1}\cdot\overline{a}=\overline{1\cdot a}=\overline{a}$$

が成り立つ．従って，$\overline{1}$ が $(\mathbb{Z}/n\mathbb{Z})^\times$ の単位元である．

(iii) 逆元の存在は定理 3.2.17 より分かる．

(iv) $\overline{a},\overline{b}\in\mathbb{Z}/n\mathbb{Z}$ に対して，

$$\overline{a}\cdot\overline{b}=\overline{a\cdot b}=\overline{b\cdot a}=\overline{b}\cdot\overline{a}$$

が成り立つ．

以上のことから，$(\mathbb{Z}/n\mathbb{Z})^\times$ が可換群であることが示された． ■

置換群と対称群

この章の最初に述べたように群とは何らかの物の対称性を表している．そのうちで，集合の元の入れ替えに関する対称性を表すものが置換群および対称群である．

X を空集合でない集合とする．このとき，X から X への全単射全体の集合

$$S(X):=\{f:X\to X\mid f\text{ は全単射}\}$$

を考える．$S(X)$ の元は集合 X の元 x を X の元 $f(x)$ に置換する操作と思うことができる．

定理 3.2.10. $S(X)$ は写像の合成 $\circ$ で群となる．

証明. 全単射の合成も全単射なので $f,g\in S(X)$ に対して $f\circ g\in S(X)$ であることに注意しておく．つまり，写像の合成は $S(X)$ の演算を定めている．

群の定義の (i) は命題 1.1.3(1) より従う．(ii) は命題 1.1.3(2) より従う（恒等写像 id_X が単位元）．(iii) は定理 1.1.10 より従う（$f\in S(X)$ の逆元は f の逆写像 f^{-1}）． ■

定義 3.2.11 (置換群)**.** 群 $S(X)$ を X の**置換群**と呼ぶ．$S(X)$ の元を X の**置換**，$S(X)$ の単位元（恒等写像 id_X）を**恒等置換**，$f \in S(X)$ の逆元（f の逆写像 f^{-1}）を f の**逆置換**という． また，X の置換 f, g に対して，合成 $f \circ g$ を単に fg と書く．

置換群の中でも $X = \{1, 2, \ldots, n\}$ の場合が特に重要である．

定義 3.2.12 (対称群)**.** $S(\{1, 2, \ldots, n\})$ を n **次対称群**といい，S_n と書く．また，$\{1, 2, \ldots, n\}$ の恒等置換は 1_n と表すことにする．

S_n の元 σ が $1, 2, \ldots, n$ をそれぞれ $k_1, k_2, \ldots, k_n$ に移すとする（つまり $\sigma(i) = k_i$）．このとき，

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$$

と表すことにする[*8]．この表記を使うと恒等置換は

$$1_n = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

と表される．

σ は $\{1, 2, \ldots, n\}$ から $\{1, 2, \ldots, n\}$ への全単射なので，$(k_1, k_2, \ldots, k_n)$ は $(1, 2, \ldots, n)$ の順番を並び替えたものである．つまり，置換は $1, 2, \ldots, n$ の順番を並び替える操作であると思える．

命題 3.2.13. S_n の元の個数は $n!$ である．

証明. 上で説明したように，S_n の元は $1, 2, \ldots, n$ の順番を並び替える操作であり，その方法は全部で ${}_nP_n = n!$ 通りある． ■

例 3.2.14. (1) S_1 の元は恒等置換 1_1 のみである．

(2) $(1, 2)$ の順番を入れ替えたものは $(1, 2)$, $(2, 1)$ の 2 つなので，S_2 の元は

$$1_2 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix},\ \sigma := \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

の 2 個．

(3) $(1, 2, 3)$ の順番を入れ替えたものは

$$(1, 2, 3),\ (1, 3, 2),\ (2, 1, 3),\ (2, 3, 1),\ (3, 1, 2),\ (3, 2, 1)$$

の 6 つなので，S_3 の元は

$$1_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

の 6 個．

例 3.2.15. S_4 の元

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

を考える．

[*8] 行列と同じ記号だが全く異なる意味を持つので注意

(1) σ の逆置換を求める．

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

なので

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

となる．従って，

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

(2) $\sigma\tau$ を計算する．

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

なので

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

(3) $\tau\sigma$ を計算する．

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

なので

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

注意. $n=1,2$ のとき S_n は可換群，$n\geq 3$ のとき S_n は非可換群である．
例えば，上の (1)(2) より $\sigma\tau\neq\tau\sigma$ となるので S_4 は可換群ではない．

定義 3.2.16. $1\leq i\neq j\leq n$ に対して，i と j を入れ替える操作は $\{1,2,\dots,n\}$ の置換である． これを $(i\ j)$ と書く:

$$(i\ j)=\begin{pmatrix}1&2&\cdots&i&\cdots&j&\cdots&n\\1&2&\cdots&j&\cdots&i&\cdots&n\end{pmatrix}$$

このように，二つの数を入れ替える置換を**互換**と呼ぶ．特に，隣り合う数を入れ替える互換 $(1\ 2),(2\ 3),\dots,(n-1\ n)$ を**隣接互換**と呼ぶ．

注意. i と j を入れ替える操作は 2 回繰り返すと元に戻る．つまり，$(i\ j)(i\ j)=1_n$ となるので，$(i\ j)=(i\ j)^{-1}$ が分かる．

次の定理は対称群の重要な性質である．

定理 3.2.17. S_n の元はいくつかの互換の積で表される．もっと強く，S_n の元はいくつかの隣接互換の積で表される．つまり，$(1,2,\dots,n)$ のどんな並び替えも隣り合う数の入れ替えを繰り返すことで得られる．

証明. $\sigma\in S_n$ を考える．以下のステップを繰り返していく：

- $\sigma(n)=i$ のとき，

$$\sigma':=(n-1\ n)\cdots(i+1\ i+2)(i\ i+1)\sigma$$

と置く．$(n-1\ n)\cdots(i+1\ i+2)(i\ i+1)$ で i は n に移るので，

$$\sigma'(n)=(n-1\ n)\cdots(i+1\ i+2)(i\ i+1)\sigma(n)=(n-1\ n)\cdots(i+1\ i+2)(i\ i+1)(i)=n$$

となる．（最初から $\sigma(n)=n$ ならば $\sigma':=\sigma$ として次のステップへ進む）

- $\sigma'(n-1)=j$ のとき，

$$\sigma'':=(n-2\ n-1)\cdots(j+1\ j+2)(j\ j+1)\sigma'$$

と置く．$(n-2\ n-1)\cdots(j+1\ j+2)(j\ j+1)$ で j は $n-1$ に移るので，

$$\begin{aligned}\sigma''(n-1)&=(n-2\ n-1)\cdots(j+1\ j+2)(j\ j+1)\sigma'(n-1)\\&=(n-2\ n-1)\cdots(j+1\ j+2)(j\ j+1)(j)\\&=n-1\end{aligned}$$

となる．また，σ' に掛けた隣接互換には n が出てこないので $\sigma''(n)=n$ となる．
（最初から $\sigma'(n-1)=n-1$ ならば $\sigma'':=\sigma'$ として次のステップへ進む）

- $\sigma''(n-2)=k$ のとき，

$$\sigma''':=(n-3\ n-2)\cdots(k+1\ k+2)(k\ k+1)\sigma''$$

と置く．$(n-3\ n-2)\cdots(k+1\ k+2)(k\ k+1)$ で k は $n-2$ に移るので，

$$\begin{aligned}\sigma'''(n-2)&=(n-3\ n-2)\cdots(k+1\ k+2)(k\ k+1)\sigma''(n-2)\\&=(n-3\ n-2)\cdots(k+1\ k+2)(k\ k+1)(k)\\&=n-2\end{aligned}$$

となる．また，σ'' に掛けた隣接互換には $n-1$,n が出てこないので $\sigma'''(n-1)=n-1$, $\sigma'''(n)=n$ となる．
（最初から $\sigma''(n-2)=n-2$ ならば $\sigma''':=\sigma''$ として次のステップへ進む）

以後同様のステップを繰り返していくと，最終的にいくつかの隣接互換 $\tau_1,\tau_2,\ldots,\tau_N$ を用いて

$$\tau_1\tau_2\cdots\tau_N\sigma=1_n$$

と表せることが分かる．従って，左から $\tau_N\cdots\tau_2\tau_1$ を掛けることで

$$\sigma=\tau_N\cdots\tau_2\tau_1$$

となり，σ は隣接互換の積となる． ■

例 3.2.18. (1) $\sigma=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$ を隣接互換の積で表す．

$\sigma(4)=2$ なので，

$$\sigma'=(3\ 4)(2\ 3)\sigma$$

と置くと，

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

となる．

$\sigma'(3)=1$ なので，

$$\sigma''=(2\ 3)(1\ 2)\sigma'$$

と置くと，

$$\sigma''=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=1_4$$

となる．

従って，

$$(2\ 3)(1\ 2)(3\ 4)(2\ 3)\sigma=1_4$$

となり，左から $(2\ 3)(3\ 4)(1\ 2)(2\ 3)$ を掛けて

$$\sigma = (2\ 3)(3\ 4)(1\ 2)(2\ 3)$$

となる．

(2) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$ を互換の積で表す．

$\sigma(5) = 1$ なので

$$\sigma' := (4\ 5)(3\ 4)(2\ 3)(1\ 2)\sigma$$

と置くと

$$\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}$$

となる．

$\sigma'(4) = 4$ なので

$$\sigma'' := \sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix} = (2\ 3)$$

と置く．

$\sigma''(3) = 2$ なので

$$\sigma''' := (2\ 3)\sigma'' = 1_5$$

と置く．

これらのことから，

$$(2\ 3)(4\ 5)(3\ 4)(2\ 3)(1\ 2)\sigma = 1_5$$

となる．従って，左から $(1\ 2)(2\ 3)(3\ 4)(4\ 5)(2\ 3)$ を掛けて

$$\sigma = (1\ 2)(2\ 3)(3\ 4)(4\ 5)(2\ 3)$$

となる．

定理 3.2.17 により全ての置換は互換の積で表せるが，その方法は一通りではない：

$$(1\ 2) = (1\ 2)(2\ 3)(2\ 3)$$

しかし，その個数の偶奇は表し方によらないことが示される（上の場合どちらの表示でも奇数個）．

定理 3.2.19. 置換 σ を互換の積で表す時，その個数の偶奇は表し方によらない．

証明. 置換 σ に対して， n 次の正方行列

$$E_\sigma := (\boldsymbol{e}_{\sigma(1)}, \boldsymbol{e}_{\sigma(2)}, \ldots, \boldsymbol{e}_{\sigma(n)}) = (\delta_{\sigma(i)j})_{1 \le i,j \le n}$$

を考える．ここで，$\boldsymbol{e}_1, \boldsymbol{e}_2, \ldots, \boldsymbol{e}_n$ は $\mathbb{R}^n$ の標準基底であり，δ_{kl} はディラックのデルタ

$$\delta_{kl} = \begin{cases} 1 & (k = l) \\ 0 & (k \neq l) \end{cases}$$

である．例えば $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$ のとき

$$E_\sigma = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

互換 $(i\ j)$ と置換 σ に対して，$E_{(i\ j)\sigma}$ は行列 E_σ の i 列目と j 列目を入れ替えて得られる行列に他ならない．よって，

$$\det(E_{(i\ j)\sigma}) = -\det(E_\sigma) \tag{$*$}$$

が成り立つ．

σ を $\sigma = \tau_1\tau_2\cdots\tau_t$ と互換の積で表したとき，$(*)$ を繰り返し用いて

$$\det(E_\sigma) = \det(E_{\tau_1\tau_2\cdots\tau_t}) = -\det(E_{\tau_2\cdots\tau_t}) = (-1)^2\det(E_{\tau_3\cdots\tau_t}) = \cdots = (-1)^t\det(E_{1_n}) = (-1)^t$$

となる．もちろん $\det(E_\sigma)$ は σ を互換の積で表す方法によらないので，$(-1)^t$ は σ を互換の積で表す方法にはよらない．従って，σ を互換の積で表したときの個数 t の偶奇は表し方によらない． ■

この定理により，以下の定義をすることができる．

定義 3.2.20. (1) 置換 $\sigma \in S_n$ に対してその**符号**（**signature**）$\mathrm{sgn}(\sigma)$ を

$$\mathrm{sgn}(\sigma) := \begin{cases} 1 & (\sigma \text{ が偶数個の互換の積}) \\ -1 & (\sigma \text{ が奇数個の互換の積}) \end{cases}$$

で定義する．

(2) $\mathrm{sgn}(\sigma) = 1$ のとき，σ を**偶置換**，$\mathrm{sgn}(\sigma) = -1$ のとき，σ を**奇置換**という．
偶置換の全体のなす S_n の部分集合を A_n と書いて n **次交代群**と呼ぶ（これが実際に群になることは例 3.3.3(5) で示す）．

例 3.2.21. (1) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$ とすると，例 3.2.18(1) より

$$\sigma = (2\ 3)(3\ 4)(1\ 2)(2\ 3)$$

となり，偶数個の互換の積である．従って，$\mathrm{sgn}(\sigma) = 1$ であり σ は偶置換．

(2) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$ とすると，例 3.2.18(2) より

$$\sigma = (1\ 2)(2\ 3)(3\ 4)(4\ 5)(2\ 3)$$

となり，奇数個の互換の積である．従って，$\mathrm{sgn}(\sigma) = -1$ であり σ は奇置換．

命題 3.2.22. (1) $\mathrm{sgn}(1_n) = 1$.

(2) $\sigma, \tau \in S_n$ に対して $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau)$ が成り立つ．

(3) $\sigma \in S_n$ に対して $\mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}(\sigma)^{-1}$ が成り立つ．

証明. (1) $1_n = (1\ 2)(1\ 2)$ は偶置換なので $\mathrm{sgn}(1_n) = 1$.

(2) σ, τ が

$$\sigma = \sigma_1\sigma_2\cdots\sigma_s, \quad \tau = \tau_1\tau_2\cdots\tau_t$$

のようにそれぞれ s 個，t 個の互換の積で表されたとする．このとき，

$$\sigma\tau = (\sigma_1\sigma_2\cdots\sigma_s)(\tau_1\tau_2\cdots\tau_t)$$

は $s+t$ 個の互換の積となる．

$\mathsf{sgn}(\sigma)=1$, $\mathsf{sgn}(\tau)=1$ のとき s,t は偶数なので $s+t$ も偶数．従って，$\mathsf{sgn}(\sigma\tau)=1=\mathsf{sgn}(\sigma)\,\mathsf{sgn}(\tau)$．他の 3 パターン $(\mathsf{sgn}(\sigma),\mathsf{sgn}(\tau))=(-1,1),(1,-1),(-1,-1)$ の場合も同様.

(3) σ が

$$\sigma=\sigma_1\sigma_2\cdots\sigma_s$$

のように s 個の互換の積で表されたとする．このとき，

$$\sigma^{-1}=\sigma_s\cdots\sigma_2\sigma_1$$

となり，σ は s 個の互換の積である．

$\mathsf{sgn}(\sigma)=1$ のとき s は偶数なので $\mathsf{sgn}(\sigma^{-1})=1$．$\mathsf{sgn}(\sigma)=-1$ のとき s は奇数なので $\mathsf{sgn}(\sigma^{-1})=-1$．　■

演習問題

問題 3.2.1. $\mathbb{Z}/12\mathbb{Z}$ において $\overline{2}\overline{x}=\overline{6}$ となるような $0\le x<12$ を全て求めよ．

問題 3.2.2. (1)　(i) $\overline{a}\in(\mathbb{Z}/8\mathbb{Z})^\times$ となるような $0\le a<8$ を全て求めよ．
(ii) (i) で求めた各 a に対して $\overline{a}^{-1}=\overline{b}$ となる $0\le b<8$ を求めよ．

(2)　(i) $\overline{a}\in(\mathbb{Z}/12\mathbb{Z})^\times$ となるような $0\le a<12$ を全て求めよ．
(ii) (i) で求めた各 a に対して $\overline{a}^{-1}=\overline{b}$ となる $0\le b<12$ を求めよ．

(3)　(i) $\overline{a}\in(\mathbb{Z}/15\mathbb{Z})^\times$ となるような $0\le a<15$ を全て求めよ．
(ii) (i) で求めた各 a に対して $\overline{a}^{-1}=\overline{b}$ となる $0\le b<15$ を求めよ．

(4)　(i) $\overline{a}\in(\mathbb{Z}/20\mathbb{Z})^\times$ となるような $0\le a<20$ を全て求めよ．
(ii) (i) で求めた各 a に対して $\overline{a}^{-1}=\overline{b}$ となる $0\le b<20$ を求めよ．

(5)　(i) $\overline{a}\in(\mathbb{Z}/24\mathbb{Z})^\times$ となるような $0\le a<24$ を全て求めよ．
(ii) (i) で求めた各 a に対して $\overline{a}^{-1}=\overline{b}$ となる $0\le b<24$ を求めよ．

問題 3.2.3. S_4 の元を全て列挙せよ．

問題 3.2.4. 以下の置換を計算せよ．

(1) $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}^{-1}$

(2) $\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}$

コメント. 一般に S_n の隣接互換 $\sigma_i=(i\ i+1)$ $(i=1,2,\ldots,n-1)$ は

(1) $\sigma_i\sigma_{i+1}\sigma_i=\sigma_{i+1}\sigma_i\sigma_{i+1}$

(2) $|i-j|\neq1$ のとき $\sigma_i\sigma_j=\sigma_j\sigma_i$

を満たす．これらの関係式は**組み紐関係式**と呼ばれる重要な式である．

問題 3.2.5. 以下の置換を隣接互換の積で表し，その符号を求めよ．

(1) $\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}$

(2) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$

(3) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$

(4) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}$

3.3　部分群

$\mathbb{R}$ は加法により群になることは例 3.1.4(2) で述べた通りである．また，$\mathbb{R}$ の部分集合 $\mathbb{Z}$ も群となっているが，その演算は $\mathbb{R}$ と全く同じものであった．同様に例 3.1.4(3) により $\mathbb{R}\setminus\{0\}$ は乗法により群となっているが，その部分集合 $\mathbb{Q}\setminus\{0\}$ は $\mathbb{R}\setminus\{0\}$ と全く同じ演算で群となっている．

このように，群 G の部分集合 H が G と同じ演算で群となっているとき，H を G の部分群であるという．部分群は群の例を豊富に作り出すだけでなく，G の構造を把握する上でも部分群は重要な役割を果たす．

定義 3.3.1. G を群，H を G の部分集合とする．H が G の**部分群**であるとは，以下の条件を満たすときに言う：

(i) $1_G \in H$
(ii) 全ての $a,b \in H$ に対して，$ab \in H$
(iii) 全ての $a \in H$ に対して，$a^{-1} \in H$

名前の通り，部分群は群となる：

命題 3.3.2. G を群，H を G の部分群とする．このとき，H は G と同じ演算で群となる．さらに，以下が成り立つ：

- 「H の単位元」＝「G の単位元」
- $a \in H$ に対して，「a の H における逆元」＝「a の G における逆元」

証明. 条件 (ii) から $a,b \in H$ に対して $ab \in H$ となるので，G の演算は H の演算を定める．

以下，H が群の定義の (i), (ii), (iii) を満たすことを確かめる．

(i) G の演算が結合法則を満たすことから従う．

(ii) 部分群の定義の (i) より $1_G \in H$ であるが，1_G が H の単位元になることは 1_G が G の単位元であることから従う：

$$\text{全ての } a \in H \text{ に対して } a1_G = 1_G a = a$$

(iii) $a \in H$ に対して，部分群の定義の (iii) より $a^{-1} \in H$ である．a^{-1} が H における a の逆元になることは a^{-1} が G における a の逆元であることから従う：

$$aa^{-1} = a^{-1}a = 1_G$$

以上より，G が H と同じ演算で群になることが示された． ■

例 3.3.3. (1) G を群とする．このとき，G の部分集合 $\{1_G\}$ と G は定義 3.3.1(i)(ii)(iii) を満たすことが容易に分かるので，G の部分群となる．これらを G の**自明な部分群**という．

(2) $n \in \mathbb{Z}$ に対して，$\mathbb{Z}$ の部分集合

$$n\mathbb{Z} := \{nx \mid x \in \mathbb{Z}\} \quad (n \text{ の倍数の集合})$$

は $\mathbb{Z}$ の部分群である．

実際，定義 3.3.1(i)(ii)(iii) が成り立つ：
(i) $0 = n \cdot 0 \in n\mathbb{Z}$.
(ii) $nk, nl \in n\mathbb{Z}$ に対して，$nk + nl = n(k+l) \in n\mathbb{Z}$.

(iii) $nk \in n\mathbb{Z}$ に対して，$-nk = n(-k) \in n\mathbb{Z}$.

(3) 整数 $n \geq 1$ に対して 1 の n 乗根の集合

$$H := \{x \in \mathbb{C} \setminus \{0\} \mid x^n = 1\}$$

は $\mathbb{C} \setminus \{0\}$ の部分群である．

実際，定義 3.3.1(i)(ii)(iii) が成り立つ：

(i) $1^n = 1$ より $1 \in H$.

(ii) $x, y \in H$ とする．$x^n = y^n = 1$ より $(xy)^n = x^n y^n = 1$ となるので，$xy \in H$.

(iii) $x \in H$ とする．$x^n = 1$ より $(x^{-1})^n = (x^n)^{-1} = 1$ となるので，$x^{-1} \in H$.

(4) 以下の一般線形群 $\mathsf{GL}_n(\mathbb{R})$（または $\mathsf{GL}_n(\mathbb{C})$）部分集合は部分群である：

(a)（**特殊線形群（Special Linear Group）**）

$\mathsf{GL}_n(\mathbb{R})$ の部分集合

$$\mathsf{SL}_n(\mathbb{R}) := \{A \in \mathsf{GL}_n(\mathbb{R}) \mid \det(A) = 1\}$$

は $\mathsf{GL}_n(\mathbb{R})$ の部分群である．

実際，定義 3.3.1 の (i)(ii)(iii) が成り立つ：

(i) $\det(E_n) = 1$ より，$\mathsf{GL}_n(\mathbb{R})$ の単位元 E_n は $\mathsf{SL}_n(\mathbb{R})$ の元である．

(ii) $A, B \in \mathsf{SL}_n(\mathbb{R})$ とする．$\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$ となるので，$AB \in \mathsf{SL}_n(\mathbb{R})$.

(iii) $A \in \mathsf{SL}_n(\mathbb{R})$ とする．$\det(A^{-1}) = \det(A)^{-1} = 1^{-1} = 1$ となるので，$A^{-1} \in \mathsf{SL}_n(\mathbb{R})$.

同様に，$\mathsf{SL}_n(\mathbb{C}) := \{A \in \mathsf{GL}_n(\mathbb{C}) \mid \det(A) = 1\}$ は $\mathsf{GL}_n(\mathbb{C})$ の部分群である．

(b)（**直交群（Orthogonal Group）**）

$\mathsf{GL}_n(\mathbb{R})$ の部分集合

$$\begin{aligned}\mathsf{O}(n) &:= \{A \in \mathsf{GL}_n(\mathbb{R}) \mid {}^tAA = A{}^tA = E_n\} \\ &= \{A \in \mathsf{GL}_n(\mathbb{R}) \mid {}^tA = A^{-1}\}\end{aligned}$$

は $\mathsf{GL}_n(\mathbb{R})$ の部分群である（${}^tA$ は A の転置行列）．

実際，定義 3.3.1(i)(ii)(iii) が成り立つ：

(i) ${}^tE_n = E_n = E_n^{-1}$ より，$\mathsf{GL}_n(\mathbb{R})$ の単位元 E_n は $\mathsf{O}(n)$ の元である．

(ii) $A, B \in \mathsf{O}(n)$ とする．${}^t(AB) = {}^tB{}^tA = B^{-1}A^{-1} = (AB)^{-1}$ となるので，$AB \in \mathsf{O}(n)$.

(iii) $A \in \mathsf{O}(n)$ とする．${}^t(A^{-1}) = ({}^tA)^{-1} = (A^{-1})^{-1}$ となるので，$A^{-1} \in \mathsf{O}(n)$.

(c)（**特殊直交群（Special Orthogonal Group）**）

$\mathsf{GL}_n(\mathbb{R})$ の部分集合

$$\mathsf{SO}(n) := \mathsf{SL}_n(\mathbb{R}) \cap \mathrm{O}(n) := \{A \in \mathsf{GL}_n(\mathbb{R}) \mid {}^tA = A^{-1} \text{ かつ } \det(A) = 1\}$$

は次の命題 3.3.4 から $\mathsf{GL}_n(\mathbb{R})$ の部分群である．

(d)（**ユニタリ群（Unitary Group）**）

$\mathsf{GL}_n(\mathbb{C})$ の部分集合

$$\begin{aligned}\mathsf{U}(n) &:= \{A \in \mathsf{GL}_n(\mathbb{C}) \mid A^*A = AA^* = E_n\} \\ &= \{A \in \mathsf{GL}_n(\mathbb{C}) \mid A^* = A^{-1}\}\end{aligned}$$

は $\mathsf{GL}_n(\mathbb{C})$ の部分群である（$A^* := \overline{{}^tA}$ は A の随伴行列）．

実際，定義 3.3.1(i)(ii)(iii) が成り立つ：

(i) $E_n^* = \overline{{}^tE_n} = E_n = E_n^{-1}$ より，$\mathsf{GL}_n(\mathbb{C})$ の単位元 E_n は $\mathsf{U}(n)$ の元である．

(ii) $A, B \in \mathsf{U}(n)$ とする．$(AB)^* = B^*A^* = B^{-1}A^{-1} = (AB)^{-1}$ となるので，$AB \in \mathsf{U}(n)$.

(iii) $A \in \mathsf{U}(n)$ とする．$(A^{-1})^* = (A^*)^{-1} = (A^{-1})^{-1}$ となるので，$A^{-1} \in \mathsf{U}(n)$.

(e)（**特殊ユニタリ群（Special Unitary Group）**）

$\mathsf{GL}_n(\mathbb{C})$ の部分集合

$$\mathsf{SU}(n) := \mathsf{SL}_n(\mathbb{C}) \cap \mathrm{U}(n)$$

は命題 3.3.4 により $\mathsf{GL}_n(\mathbb{C})$ の部分群となる．

(5) n 次交代群 A_n は n 次対称群 S_n の部分群である．

実際，定義 3.3.1(i)(ii)(iii) が成り立つ：

(i) $1_n = (1\ 2)(1\ 2)$ は偶置換なので $1_n \in A_n$.

(ii) $\sigma, \tau \in A_n$ に対して，σ と τ は偶数個の互換の積なので $\sigma\tau$ も偶数個の互換の積である．従って，$\sigma\tau \in A_n$.

(iii) $\sigma \in A_n$ に対して，σ は偶数個の互換の積なので σ^{-1} も偶数個の互換の積である．従って，$\sigma^{-1} \in A_n$.

(6)（**n 次二面体群（Dihedral Group）**）

(a) $n \geq 3$ を整数とする．このとき，$\mathsf{GL}_2(\mathbb{R})$ の元

$$T := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad R := \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix}$$

を考える（T は x 軸に関する反転，R は原点を中心に反時計回りに $2\pi/n$ だけ回転させる操作を表す行列である）．このとき，$\mathsf{GL}_2(\mathbb{R})$ の $2n$ 個の元からなる部分集合

$$D_n := \{E_2, R, R^2, \ldots, R^{n-1}, T, TR, TR^2, \ldots, TR^{n-1}\}$$

は $\mathsf{GL}_2(\mathbb{R})$ の部分群である．

実際，これらの行列は関係式

$$T^2 = E_2, \quad R^n = E_2, \quad R^kT = TR^{n-k} \quad (k \in \mathbb{Z})$$

を満たしているので，定義 3.3.1(i)(ii)(iii) が容易に確かめられる．

(b) $n \geq 3$ を整数とする．S_n の元

$$\tau := \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{pmatrix}, \quad \rho := \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix}$$

を考える（$\tau(i) = n - i + 1$, $\rho(i) = i + 1$ $(1 \leq i \leq n-1)$, $\rho(n) = 1$ ）．このとき，S_n の $2n$ 個の元からなる部分集合

$$D_n := \{1_n, \rho, \rho^2, \ldots, \rho^{n-1}, \tau, \tau\rho, \tau\rho^2, \ldots, \tau\rho^{n-1}\}$$

は S_n の部分群である．

実際，これらの置換は関係式

$$\tau^2 = 1_n, \quad \rho^n = 1_n, \quad \rho^k\tau = \tau\rho^{n-k} \quad (k \in \mathbb{Z})$$

を満たしているので定義 3.3.1(i)(ii)(iii) が確かめられる．

コメント. $\mathsf{GL}_2(\mathbb{R})$ は $\mathbb{R}^2$ 上の可逆な線型変換の全体であった．例 3.3.3(4)(6) で紹介した $\mathsf{GL}_2(\mathbb{R})$ の部分群は以下のような意味を持つ：

- $\mathsf{SL}_2(\mathbb{R})$：面積と向きを変えない可逆な線形変換の全体
- $\mathsf{O}(2)$：内積を変えない（従って，長さと角度を変えない）可逆な線形変換の全体
- $\mathsf{SO}(2)$：面積，向き，内積を変えない可逆な線形変換の全体 $=$ 回転変換全体
- D_n：原点を中心とする正 n 角形 X の合同変換の全体（$=\mathsf{E}(X)$）

コメント. 座標平面内の n 個の点

$$\boldsymbol{x}_k := \left(\cos\left(\frac{(2k-1)\pi}{n}\right), \sin\left(\frac{(2k-1)\pi}{n}\right)\right) \quad (k=1,2,\dots,n)$$

を頂点とする正 n 角形を考える．例 3.3.3(6)(a) の D_n はこの正 n 角形の合同変換の集まりである．
行列 T により頂点 $\boldsymbol{x}_k$ は $\boldsymbol{x}_{n-k}$ に移され，R により頂点 $\boldsymbol{x}_1, \boldsymbol{x}_2, \dots, \boldsymbol{x}_{n-1}, \boldsymbol{x}_n$ はそれぞれ $\boldsymbol{x}_2, \boldsymbol{x}_3, \dots, \boldsymbol{x}_n, \boldsymbol{x}_1$ に移される．従って，例 3.3.3(6)(b) の置換 τ, ρ を用いると

$$T\boldsymbol{x}_k = \boldsymbol{x}_{\tau(k)}, \quad R\boldsymbol{x}_k = \boldsymbol{x}_{\rho(k)}$$

と表される．一般に，D_n の元 T^sR^t $(s=0,1,\ t=0,1,2,\dots,n-1)$ に対して

$$(T^sR^t)\boldsymbol{x}_k = \boldsymbol{x}_{(\tau^s\rho^t)(k)}$$

が成り立つ．
この様に，正 n 角形の頂点の変換を通して正 n 角形の合同変換と n 文字の置換は対応している．この元の対応により，例 3.3.3 の (6)$(a)(b)$ の部分群は**群として同じ構造を持っている**ことが分かる[a]．これが (6) と (7) の部分群を同じ記号 D_n を用いて表す理由である．例 3.3.3 の (6)$(a)(b)$ で導入した 2 つの群は正 n 角形の変換を「合同変換」,「頂点の変換」という二通りの見方により群とみなしたものなので，本質的には同じものであるということは納得できるのではないかと思う．

[a] 「群として同じ構造を持っている」ことの正確な意味は第 3.6 節で説明される

群 G の部分群が二つあると，それらの共通集合も再び部分群となる．

命題 3.3.4. *G を群，H_1, H_2 を G の部分群とする．このとき，$H_1 \cap H_2$ も G の部分群である．*

証明. 定義 3.3.1(i)(ii)(iii) を確かめる．

(i) H_1 と H_2 が部分群なので，$1_G \in H_1$ かつ $1_G \in H_2$．従って，$1_G \in H_1 \cap H_2$ となる．

(ii) $a, b \in H_1 \cap H_2$ とする．$a, b \in H_1$ なので，H_1 が部分群であることから $ab \in H_1$．$a, b \in H_2$ なので，H_2 が部分群であることから $ab \in H_2$．従って，$ab \in H_1 \cap H_2$ となる．

(iii) $a \in H_1 \cap H_2$ とする．$a \in H_1$ なので，H_1 が部分群であることから $a^{-1} \in H_1$．$a \in H_2$ なので，H_2 が部分群であることから $a^{-1} \in H_2$．従って，$a^{-1} \in H_1 \cap H_2$ となる．

(i)(ii)(iii) が示されたので，$H_1 \cap H_2$ は G の部分群となる． ■

この命題により，群 G の部分群 H_1, H_2 に対して，$H_1 \cap H_2$ は H_1, H_2 に含まれる部分群の中で最大のものであることが分かる：

部分群 $K \leq G$ に対して

$$K \subseteq H_1 \text{かつ } K \subseteq H_2 \Longrightarrow K \subseteq H_1 \cap H_2 \quad \text{（共通集合の定義から明らか）}$$

それでは，H_1 と H_2 を含む最小の部分群はどうなるだろうか．それについては第 3.4 節で扱う．

注意. H_1, H_2 が G の部分群でも $H_1 \cup H_2$ は一般に G の部分群とはならない．例えば，$G = \mathbb{Z}$, $H_1 = 2\mathbb{Z}$, $H_2 = 3\mathbb{Z}$ とすると，$2, 3 \in H_1 \cup H_3$ であるが，$2 + 3 \notin H_1 \cup H_2$ である．

演習問題

問題 3.3.1. H を G の空集合でない部分集合とする．このとき，H が G の部分群であることと条件

(iv) 任意の $x, y \in H$ に対して，$xy^{-1} \in H$

が成り立つことは同値であることを示せ．

問題 3.3.2. (1) 例 3.3.3(6)(a) において $n = 3$ とし，以下を示せ．
- (i) 関係式 $T^2 = E_2$, $R^3 = E_2$, $R^k T = TR^{3-k}$ $(k = 0, 1, 2)$ を確かめよ．
- (ii) D_3 の乗積表を書け．
- (iii) D_3 が $\mathsf{GL}_2(\mathbb{R})$ の部分群となることを確かめよ．

(2) 例 3.3.3(6)(b) において $n = 3$ とし，以下を示せ．
- (i) 関係式 $\tau^2 = 1_3$, $\rho^3 = 1_3$, $\rho^k \tau = \tau \rho^{3-k}$ $(k = 0, 1, 2)$ を確かめよ．
- (ii) D_3 の乗積表を書け．
- (iii) D_3 が S_3 の部分群となることを確かめよ．

問題 3.3.3. 以下の群 G と G の部分集合 H に対して，H が G の部分群であるかどうか理由も合わせて答えよ：

(1) $G = \mathbb{Z}$, $H := \{2n + 3 \mid n \in \mathbb{Z}\}$

(2) $G = \mathbb{R} - \{0\}$, $H := (0, \infty)$

(3) $G = \mathbb{R} - \{0\}$, $H := \{2^n \mid n \in \mathbb{N}\}$

(4) $G = \mathbb{Q} - \{0\}$, $H = \{2^k 3^l \mid k, l \in \mathbb{Z}\}$

(5) n を 2 以上の整数とする．
$G = \mathbb{C} - \{0\}$, $H = \{x \in G \mid x^n = 1\}$

(6) $G = \mathsf{GL}_2(\mathbb{R})$, $H = \{A \in \mathsf{GL}_2(\mathbb{R}) \mid \forall B \in \mathsf{GL}_2(\mathbb{R}), AB = BA\}$.

(7) $G = \mathsf{GL}_2(\mathbb{R})$, $H = \{A \in \mathsf{GL}_2(\mathbb{R}) \mid |A| \in \mathbb{Z}\}$.

(8) $G = \mathsf{GL}_2(\mathbb{R})$,

$$H := \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \middle| \, \theta \in \mathbb{R} \right\}$$

(9) $G = S_4$,

$$H := \left\{ 1_4, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \right\}$$

(10) $G = S_4$,

$$H := \left\{ 1_4, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \right\}$$

(11) $G = S_5$, $H := \{\sigma \in S_5 \mid \sigma(5) = 5\}$

問題 3.3.4. 群 G と G の空集合でない部分集合 S を考える．

(1) $\mathrm{Z}_G(S) := \{x \in G \mid \forall a \in S,\ xa = ax\}$ が G の部分群であることを示せ．
$\mathrm{Z}_G(S)$ を S の**中心化群**という．また，$\mathrm{Z}(G) := \mathrm{Z}_G(G) = \{x \in G \mid \forall a \in G,\ xa = ax\}$ を G の**中心**という．

(2) $\mathrm{N}_G(S) := \{x \in G \mid xS = Sx\}$ が G の部分群であることを示せ．
（ただし，$xS := \{xa \mid a \in S\},\ Sx := \{ax \mid a \in S\}$）
$\mathrm{N}_G(S)$ を S の**正規化群**という．

3.4　群の生成

例 3.3.3(6)(a) で定義した二面体群 D_n は

$$D_n := \{E_2,\, R,\, R^2,\, \ldots,\, R^{n-1},\, T,\, TR,\, TR^2,\, \ldots,\, TR^{n-1}\}$$

という $2n$ 個の元からなる部分群である．しかし，群の元をよく見ると全ての元は T と R から何回かの積によって得られている．従って，D_n は T と R という 2 つの元から作られていると言える．これを D_n は T と R **で生成される**という．群 G 全体を作り出すより少ない元の集合 S が見つかれば，その群がどういう元からなるかより分かりやすくなる．

G を群，S を G の空集合でない部分集合とする．まずは S を含む部分群 H にどのような元が含まれるか見ていく：

- 定義 3.3.1(i) により $1_G \in H$
- $x \in S$ に対して，定義 3.3.1(iii) により $x^{-1} \in H$
- $x_1, x_2, \ldots, x_n \in S$ に対して，$x_i^{\pm 1} \in H$ $(i = 1, 2, \ldots, n)$ なので，定義 3.3.1(ii) により $x_1^{\pm 1} x_2^{\pm 1} \cdots x_n^{\pm 1} \in H$（複合任意）．

そこで，$x_1^{\pm 1} x_2^{\pm 1} \cdots x_n^{\pm 1}$ $(x_1, \ldots, x_n \in S)$ の形の元を集めた G の部分集合を考える：

定義 3.4.1. G を群，S を G の空集合でない部分集合とする．このとき，G の部分集合

$$\langle S \rangle := \{x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n} \mid n \in \mathbb{N},\ x_1, x_2, \ldots, x_n \in S,\ e_1, e_2, \ldots, e_n \in \{1, -1\}\}$$

を S **で生成された** G **の部分群**といい，S を $\langle S \rangle$ **の生成系**と呼ぶ．
S が有限集合 $S = \{x_1, x_2, \ldots, x_n\}$ のとき，$\langle \{x_1, x_2, \ldots, x_n\} \rangle$ の $\{,\}$ を省略して単に $\langle x_1, x_2, \ldots, x_n \rangle$ と書く．
また，有限個の元で生成される群は**有限生成**であるという．

次の命題により，S で生成される部分群 $\langle S \rangle$ は実際に G の部分群となっていること，さらにそれが S を含む部分群の中で最も小さいものであることが分かる．

命題 3.4.2. G を群，S を G の空集合でない部分集合とする．

(1) $\langle S \rangle$ は G の部分群である．
(2) $\langle S \rangle$ は S を含む G の部分群の中で最小のものである：
　　H が G の部分群で $S \subseteq H$ ならば $\langle S \rangle \subseteq H$ となる

証明. (1) 定義 3.3.1(i)(ii)(iii) を確かめる．

(i) 1_G は $\langle S \rangle$ の元である．例えば，$x \in S$ に対して $1_G = x^0 = xx^{-1} \in \langle S \rangle$.

(ii) $\langle S \rangle$ の 2 元 $x_1^{c_1} x_2^{c_2} \cdots x_m^{c_m}$, $y_1^{e_1} y_2^{e_2} \cdots y_n^{e_n}$ $(x_i, y_j \in S,\, c_i, e_j \in \{1, -1\})$ に対して，

$$(x_1^{c_1} x_2^{c_2} \cdots x_m^{c_m})(y_1^{e_1} y_2^{e_2} \cdots y_n^{e_n}) = x_1^{c_1} x_2^{c_2} \cdots x_m^{c_m} y_1^{e_1} y_2^{e_2} \cdots y_n^{e_n}$$

は $\langle S \rangle$ の元である．

(iii) $\langle S \rangle$ の元 $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ $(x_i \in S,\, e_i \in \{1, -1\})$ に対して，系 3.1.7 より

$$(x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n})^{-1} = x_n^{-e_n} \cdots x_2^{-e_2} x_1^{-e_1}$$

となるが，これも再び $\langle S \rangle$ の元である．

(2) H を G の部分群で $S \subseteq H$ とする．このとき，定義 3.4.1 の前の議論から，$\langle S \rangle$ の任意の元 $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ ($x_i \in S$, $e_i \in \{1, -1\}$) は H の元になる．従って，$\langle S \rangle \subseteq H$ が示された． ■

注意. $\langle S \rangle$ の元 $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ において，$x^{\pm 1} x^{\pm 1} \cdots x^{\pm 1}$ の形の部分を x^k ($k \in \mathbb{Z}$) とまとめると，$\langle S \rangle$ の元は

$$x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} \quad (x_i \in S,\ k_i \in \mathbb{Z},\ x_i \neq x_{i+1}^{\pm 1})$$

と表せる．
例えば $S = \{x, y, z\}$ のとき，

$$xxxyyy^{-1}y^{-1}yz = x^3yz$$
$$z^{-1}z^{-1}zzyyyxxx^{-1}x^{-1}x^{-1}x^{-1}yy = z^0y^3x^{-2}y^2 = y^3x^{-2}y^2$$

特別な状況で $\langle S \rangle$ がどのような集合となるのか見ていく．

例 3.4.3. G を群とする．

(1) $x \in G$ に対して，$\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$ となる．これは上のコメントから分かる．

(2) $x, y \in G$ に対して，

$$\langle x, y \rangle = \{x^{m_1} y^{n_1} x^{m_2} y^{n_2} \cdots x^{m_k} y^{n_k} \mid k \in \mathbb{N},\ m_1, n_1, m_2, n_2, \ldots, m_k, n_k \in \mathbb{Z}\}$$

となる．これも上のコメントから分かる（$y^2x^3y^{-2}x^2$ などは $x^0y^2x^3y^{-2}x^2y^0$ とみなす）．

(3) G が可換群のとき，$x_1, x_2, \ldots, x_n \in G$ に対して

$$\langle x_1, x_2, \ldots, x_n \rangle = \{x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} \mid k_1, k_2, \ldots, k_n \in \mathbb{Z}\}$$

となる．
これは G が可換群なので積の順番を入れ替えても良いことから分かる．例えば，

$$x_3x_2^3x_1^{-2}x_2^2x_1^3 = x_1^{-2}x_1^3x_2^3x_2^2x_3 = x_1y_2^5x_3$$

ちなみに，G が加法群の場合は

$$\langle x_1, x_2, \ldots, x_n \rangle = \{k_1x_1 + k_2x_2 + \cdots + k_nx_n \mid k_1, k_2, \ldots, k_n \in \mathbb{Z}\}$$

である．

以上の状況は非常によく現れるので是非覚えてほしい．

例 3.4.4. (1) $n \in \mathbb{Z}$ に対して，例 3.3.3(2) において考えた $\mathbb{Z}$ の部分群 $n\mathbb{Z}$ は例 3.4.3(1) または (3) により n で生成されることが分かる：

$$n\mathbb{Z} = \langle n \rangle$$

(2) 整数 $n \geq 1$ に対して，例 3.3.3(3) において考えた $\mathbb{C} \setminus \{0\}$ の部分群 $H = \{x \in \mathbb{C} \setminus \{0\} \mid x^n = 1\}$ は 1 の原始 n 乗根 $\zeta_n := e^{\frac{2\pi\sqrt{-1}}{n}}$ で生成される：

$$H = \langle \zeta_n \rangle$$

実際，$\zeta_n \in H$ なので命題 3.4.2(2) より $H \supseteq \langle \zeta_n \rangle$ となる．一方で，方程式 $x^n = 1$ の解は

$$\zeta_n^0 = 1,\ \zeta_n = e^{\frac{2\pi\sqrt{-1}}{n}},\ \zeta_n^2 = e^{\frac{4\pi\sqrt{-1}}{n}},\ \zeta_n^{n-1} = e^{\frac{2(n-1)\pi\sqrt{-1}}{n}}$$

の n 個であるが，これらは全て $\langle\zeta_n\rangle$ の元なので $H \subseteq \langle\zeta_n\rangle$ も分かる．従って，$H = \langle\zeta_n\rangle$ が示された．

(3) 定理 3.2.17 により任意の置換は隣接互換の積となるので，

$$S_n = \langle (1\ 2), (2\ 3), \cdots, (n-1\ n) \rangle$$

となる（定理 3.2.17 より $\subseteq$ が分かり，命題 3.4.2(2) より $\supseteq$ が分かる）．

(4) 定理 3.2.17 により任意の偶置換は偶数個の隣接互換の積となるので，

$$A_n = \langle \{ \sigma\tau \mid \sigma, \tau \text{は隣接互換} \} \rangle$$

となる（定理 3.2.17 より $\subseteq$ が分かり，命題 3.4.2(2) より $\supseteq$ が分かる）．
例えば，$n = 3$ のとき

$$A_3 = \langle (1\ 2)(2\ 3) \rangle$$

となり，$n = 4$ のとき

$$\begin{aligned} A_4 &= \langle (1\ 2)(2\ 3), (1\ 2)(3\ 4), (2\ 3)(3\ 4) \rangle \\ &= \left\langle \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \right\rangle \end{aligned}$$

となる．

(5) $n \geq 3$ を整数とし，$\mathsf{GL}_2(\mathbb{R})$ の元

$$T := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad R := \begin{pmatrix} \cos\left(\frac{2\pi}{n}\right) & -\sin\left(\frac{2\pi}{n}\right) \\ \sin\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi}{n}\right) \end{pmatrix}$$

を考える．このとき，例 3.3.3(6)(a) で考えた部分群

$$D_n = \{E_2, R, R^2, \ldots, R^{n-1}, T, TR, TR^2, \ldots, TR^{n-1}\}$$

は T と R で生成される：

$$D_n = \langle T, R \rangle$$

（命題 3.4.2(2) より $\supseteq$ が従い，$\langle T, R \rangle$ の定義から $\subseteq$ が分かる）．

(6) $n \geq 3$ を整数とし，S_n の元

$$\tau := \begin{pmatrix} 1 & 2 & \cdots & n-2 & n-1 \\ n-1 & n-2 & \cdots & 2 & 1 \end{pmatrix}, \quad \rho := \begin{pmatrix} 1 & 2 & \cdots & n-2 & n-1 \\ 2 & 3 & \cdots & n-1 & 1 \end{pmatrix}$$

を考える．このとき，例 3.3.3(6)(b) で考えた部分群

$$D_n = \{1_n, \rho, \rho^2, \ldots, \rho^{n-1}, \tau, \tau\rho, \tau\rho^2, \ldots, \tau\rho^{n-1}\}$$

は τ と ρ で生成される：

$$D_n = \langle \tau, \rho \rangle$$

（命題 3.4.2(2) より $\supseteq$ が従い，$\langle \tau, \rho \rangle$ の定義から $\subseteq$ が分かる）．

例 3.4.5. 整数 $m, n \in \mathbb{Z}$ に対して $d = \mathsf{gcd}(m, n)$ と置く．このとき，命題 2.1.6 により

$$\langle m, n \rangle = d\mathbb{Z}$$

が分かる（($\subseteq$) は m, n が d の倍数であることから，($\supseteq$) は命題 2.1.6 より従う）．

一般に $m_1, m_2, \ldots, m_k \in \mathbb{Z}$ の最大公約数を $d = \mathsf{gcd}(m_1, m_2, \ldots, m_k)$ と置いたとき，

$$\langle m_1, m_2, \ldots, m_k \rangle = d\mathbb{Z}$$

が成り立つ．

演習問題

問題 3.4.1. G を群，x を G の元とする．このとき，

$$G_x := \{y \in G \mid xy = yx\}$$

が G の部分群となることを示せ．

問題 3.4.2. $\mathsf{GL}_2(\mathbb{R})$ の以下の部分群の元を全て求めよ．

(1) $\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$

(2) $\left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle$

問題 3.4.3. $\mathbb{Z}/12\mathbb{Z}$ を考える．このとき，

$$\langle \overline{a} \rangle = \mathbb{Z}/12\mathbb{Z}$$

を満たすような整数 $0 \leq a < 12$ を全て求めよ．

問題 3.4.4. 例 3.3.3(6)(a) の

$$D_3 := \langle T, R \rangle$$

を考える．D_3 の以下の部分群の元を全て求めよ．

(1) $\langle R \rangle$
(2) $\langle T \rangle$
(3) $\langle TR^2 \rangle$
(4) $\langle TR, TR^3 \rangle$

問題 3.4.5. 例 3.3.3(6)(b) の

$$D_3 := \langle \tau, \rho \rangle$$

を考える．D_3 の以下の部分群の元を全て求めよ．

(1) $\langle \rho \rangle$
(2) $\langle \tau \rangle$
(3) $\langle \tau\rho \rangle$
(4) $\langle \tau\rho, \rho \rangle$

問題 3.4.6. G が部分集合 S で生成されているとする：$G = \langle S \rangle$．このとき，以下を示せ：

(1) $a \in S$ が「任意の $b \in S$ に対して $ab = ba$」を満たすならば，任意の $b \in G$ に対して $ab = ba$ を満たす．
(2)「任意の $a, b \in S$ に対して $ab = ba$」が成り立つならば G は可換群である．

3.5　元の位数と巡回群

巡回群は最も簡単な群のクラスである一方で，理論上・応用上も非常に重要な群でもある．この節では巡回群とその位数と密接な関わりがある群の元の位数について考える．

元の位数

定義 3.5.1. G を群，$x \in G$ とする．このとき，x の**位数（order）**$\mathsf{ord}(x)$ を次で定義する：

$$\mathsf{ord}(x) := \begin{cases} x^n = 1_G \text{ となる最小の正の整数 } n & (\text{「}\exists n \geq 1 \text{ s.t. } x^n = 1_G\text{」のとき}) \\ \infty & (\text{「}\forall n \geq 1, x^n \neq 1_G\text{」のとき}) \end{cases}$$

$\mathsf{ord}(x) < \infty$ のとき，x は**有限位数**を持つといい，$\mathsf{ord}(x) = \infty$ のとき，x は**無限位数**を持つという．

コメント. $x \in G$ の位数は以下の様に求めることができる：

> x のべき $x, x^2, x^3, \ldots$ を順に計算していき，最初に $x^n = 1_G$ となった n が $\mathsf{ord}(x)$．すべての $n \geq 1$ に対して $x^n \neq 1_G$ となるとき，$\mathsf{ord}(x) = \infty$ ．

例 3.5.2. (1) $\mathbb{C} \setminus \{0\}$ の元 $i = \sqrt{-1}$ を考える．i のべきを順に計算していくと

$$\begin{aligned} i &\neq 1 \\ i^2 &= -1 \neq 1 \\ i^3 &= -i \neq 1 \\ i^4 &= 1 \end{aligned}$$

となるので，$\mathsf{ord}(\sigma) = 4$.

(2) 整数 $n \geq 1$ に対して 1 の原始 n 乗根 $\zeta_n := e^{\frac{2\pi i}{n}} \in \mathbb{C} \setminus \{0\}$ を考える．原始 n 乗根の定義から ζ_n は n 乗して初めて 1 になるので，$\mathsf{ord}(\zeta_n) = n$（$n = 4$ の場合が (1)）.

(3) $z \in \mathbb{C} \setminus \{0\}$ が $|z| \neq 1$ を満たすとき $\mathsf{ord}(z) = \infty$ となる．

z^n の絶対値を考えれば，すべての整数 $n \geq 1$ に対して $z^n \neq 1$ が分かる（$|z^n| = |z|^n \neq 1$ より）．従って，$\mathsf{ord}(z) = \infty$.

(4) $\mathsf{GL}_2(\mathbb{R})$ の元 $A = \begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}$ を考える．A のべきを順に計算していくと

$$\begin{aligned} A &= \begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix} \neq E_2 \\ A^2 &= \begin{pmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{pmatrix} \neq E_2 \\ A^3 &= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \neq E_2 \\ A^4 &= \begin{pmatrix} -1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & -1/2 \end{pmatrix} \neq E_2 \\ A^5 &= \begin{pmatrix} 1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & 1/2 \end{pmatrix} \neq E_2 \\ A^6 &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E_2 \end{aligned}$$

となるので，$\mathsf{ord}(A) = 6$.

(5) $\mathsf{GL}_2(\mathbb{R})$ の元 $A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ を考えると，$\mathsf{ord}(A) = \infty$.

実際，A^n の行列式を考えればすべての $n \geq 1$ に対して $A^n \neq E_2$ が分かる（$\mathsf{det}(A^n) = \mathsf{det}(A)^n = 3^n$ より）．従って，$\mathsf{ord}(A) = \infty$.

(6) $(\mathbb{Z}/11\mathbb{Z})^\times$ の元 $\overline{3}$ を考える．$\overline{3}$ のべきを順に計算していくと

$$\begin{aligned} \overline{3} &\neq \overline{1} \\ \overline{3}^2 &= \overline{9} \neq \overline{1} \\ \overline{3}^3 &= \overline{27} = \overline{5} \neq \overline{1} \\ \overline{3}^4 &= \overline{81} = \overline{4} \neq \overline{1} \\ \overline{3}^5 &= \overline{243} = \overline{1} \end{aligned}$$

となるので，$\mathsf{ord}(\overline{3}) = 5$.

(7) S_4 の元 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ を考える．σ のべきを順に計算していくと

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \neq 1_4 \\ \sigma^2 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \neq 1_4 \\ \sigma^3 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \neq 1_4 \\ \sigma^4 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = 1_4 \end{aligned}$$

となるので，$\mathsf{ord}(\sigma) = 4$.

次の命題により $(\mathbb{Z}/n\mathbb{Z})^\times$ や S_n の元は全て有限位数を持つことが分かる．

命題 3.5.3. 有限群 G の任意の元は有限位数を持つ．

証明. $n := |G|$ とする．このとき，$x \in G$ に対して，$n+1$ 個の元 $x^0 = 1_G, x, x^2, \ldots, x^n$ は G の元なので，ある

$0 \leq i < j \leq n$ が存在して $x^i = x^j$ となる[*9]．このとき，$x^{j-i} = 1_G$ となるので $\mathrm{ord}(x) \leq j - i < \infty$． ■

注意． この証明から，位数が n の有限群の元の位数は必ず n 以下であることが分かる．実はもっと強く，位数が n の有限群の元の位数は必ず n の約数となる（ラグランジュの定理（定理 4.1.8））．

巡回群

定義 3.5.4. 群 G が巡回群であるとは，ある $x \in G$ を用いて

$$G = \langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$$

と表せるときにいう．

注意． $G = \langle x^n \rangle$ が巡回群のとき，G の任意の元 x^m, x^n に対して

$$x^m x^n = x^{m+n} = x^n x^m$$

となる（系 3.1.7 より）．従って，巡回群は可換群である．

巡回群の生成元の位数が有限のとき，その相異なる元が完全に分かる．

命題 3.5.5. G を群，$x \in G$ を有限位数 n を持つ元とする．このとき，

$$x^k = x^l \Longleftrightarrow k \equiv l \bmod n$$

となる．特に，

$$\langle x \rangle = \{1_G, x, x^2, \ldots, x^{n-1}\}$$

かつ $|\langle x \rangle| = \mathrm{ord}(x) = n$ が成り立つ．

証明． まず初めに，整数 m が $x^m = 1_G$ を満たすとき，$n|m$ となることを示す．命題 2.1.1 より

$$m = qn + r \quad (0 \leq r < n)$$

を満たす整数 q, r が存在する．このとき，系 3.1.7 より

$$x^m = x^{qn+r} = x^{qn}x^r = (x^n)^q x^r = 1_G^q x^r = x^r \quad (x \text{ の位数が } n \text{ なので } x^n = 1_G)$$

となるので，$x^r = 1_G$．$r > 0$ と仮定すると，$n = \mathrm{ord}(x)$ が $x^n = 1_G$ なる最小の整数 $n \geq 1$ であることに矛盾する．従って $r = 0$ となり，$m = qn$．

「$x^k = x^l \Longrightarrow k \equiv l \bmod n$」の証明：

$x^k = x^l$ のとき，$x^{k-l} = x^k(x^l)^{-1} = 1_G$ となるので，上で示したことから $n|(k-l)$ となる．従って，$k \equiv l \bmod n$．

「$k \equiv l \bmod n \Longrightarrow x^k = x^l$」の証明：

$k \equiv l \bmod n$ のとき，$k - l = qn$ $(q \in \mathbb{Z})$ と書ける．このとき，

$$x^k = x^{qn+l} = x^{qn}x^l = (x^n)^q x^l = 1_G^q x^l = x^l$$

[*9] このような議論を鳩の巣原理という：n 羽の鳩を m 個の巣に入れる時，$m < n$ ならばいずれかの巣には 2 羽以上の鳩が入る

となる．

次に，$\langle x\rangle = \{1_G, x, x^2, \ldots, x^{n-1}\}$ を示す．$\langle x\rangle$ の任意の元は x^m の形だが，m を n で割った余りを $r \in \{0, 1, \ldots, n-1\}$ とすると

$$x^m = x^r \in \{1_G, x, x^2, \ldots, x^{n-1}\}$$

となる．従って，$\langle x\rangle \subseteq \{1_G, x, x^2, \ldots, x^{n-1}\}$ が分かる．逆の包含 $\{1_G, x, x^2, \ldots, x^{n-1}\} \subseteq \langle x\rangle$ は定義より明らか．よって，等号 $\langle x\rangle = \{1_G, x, x^2, \ldots, x^{n-1}\}$ が示された．

最後に，$|\langle x\rangle| = n$ を示す．そのためには $1_G, x, x^2, \ldots, x^{n-1}$ が全て異なることを示せばよい．$k, l \in \{0, 1, \ldots, n-1\}$ が $k \neq l$ となるとき，$k \not\equiv l \bmod n$ なので上で示したことから $x^k \neq x^l$．以上のことから $|\langle x\rangle| = n$ が示された． ■

例 3.5.6. (1) $n \geq 1$ とする．例 3.5.2(2) より $\mathbb{C} \setminus \{0\}$ の元 ζ_n の位数は n なので，命題 3.5.5 より

$$\langle \zeta_n\rangle = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}$$

かつ $|\langle \zeta_n\rangle| = n$ となる．

(2) 例 3.5.2(4) より $\mathrm{GL}_2(\mathbb{R})$ の元 $A = \begin{pmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{pmatrix}$ の位数は 6 なので，命題 3.5.5 より

$$\langle A\rangle = \{E_2, A, A^2, A^3, A^4, A^5\}$$

かつ $|\langle A\rangle| = 6$ となる．

(3) 例 3.5.2(6) より $(\mathbb{Z}/11\mathbb{Z})^\times$ の元 $\overline{3}$ の位数は 5 なので，命題 3.5.5 より

$$\langle \overline{3}\rangle = \{\overline{1}, \overline{3}, \overline{4}, \overline{5}, \overline{9}\}$$

かつ $|\langle \overline{3}\rangle| = 5$ となる．

(4) 例 3.5.2(7) より S_4 の元 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ の位数は 4 なので，命題 3.5.5 より

$$\langle \sigma\rangle = \{1_4, \sigma, \sigma^2, \sigma^3\}$$

かつ $|\langle \sigma\rangle| = 4$ となる．

巡回群の生成元の位数が無限のときは以下のことが分かる：

命題 3.5.7. G を群，$x \in G$ を無限位数を持つ元とする．このとき，$m, n \in \mathbb{Z}$ に対して，

$$x^m = x^n \Longrightarrow m = n$$

が成り立つ（$\langle x\rangle$ の元 x^n は全て異なる）．特に，$|\langle x\rangle| = \mathrm{ord}(x) = \infty$ が成り立つ．

証明. $x^m = x^n$ とする．対称性により $m \leq n$ としても良い．このとき，$x^{n-m} = x^n(x^m)^{-1} = 1_G$ となる．もし $n - m \geq 1$ ならば $\mathrm{ord}(x) \leq n - m$ となり，x が無限位数を持つことに矛盾．従って，$m = n$ となる． ■

例 3.5.8. (1) 例 3.5.2(3) より，$z \in \mathbb{C} - \{0\}$ が $|z| \neq 1$ を満たすとき z は無限位数を持つので命題 3.5.7 により z^n $(n \in \mathbb{Z})$ は全て異なり，$|\langle z\rangle| = \infty$ となる．

(2) 例 3.5.2(5) より $A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$ は無限位数を持つので命題 3.5.7 により A^n $(n \in \mathbb{Z})$ は全て異な

り，$|\langle A\rangle| = \infty$ となる．

コメント． 命題 *3.5.5 and 3.5.7* を合わせて，群 G の任意の元 x に対して

$$|\langle x\rangle| = \mathsf{ord}(x)$$

となることが分かる．

最後に，元の位数の応用として巡回群の部分群について以下の事実を示す：

命題 3.5.9. *G を巡回群とすると，G の部分群も再び巡回群となる．*

証明. 巡回群 $G = \langle x\rangle$ の部分群 H を考える．$H = \{1_G\}$ ならば H は巡回群 $\langle 1_G\rangle$ となるので $H \neq \{1_G\}$ として示せば良い．

H の元は全て x^k $(k \in \mathbb{Z})$ の形をしているので，$x^n \in H$ となる最小の正の整数 n を取る．このとき $H = \langle x^n\rangle$ を示す．H の任意の元 x^k $(k \in \mathbb{Z})$ に対して，命題 2.1.1 より

$$k = qn + r \quad (0 \leq r < n)$$

となる整数 q, n が存在する．このとき，

$$x^r = x^{k-qn} = x^k x^{-qn} = x^k (x^n)^{-q} = x^k 1_G^{-q} = x^k \in H$$

となる．もし $r \geq 1$ ならば n が $x^n \in H$ となる最小の正の整数であることに矛盾する．従って $r = 0$ となり，$x^k = x^{qn} = (x^n)^q$ となる．このことから $H \subseteq \langle x^n\rangle$ が示された．逆の包含はすぐ分かるので $H = \langle x^n\rangle$ となり，H も巡回群となる． ■

コメント． $\mathbb{Z}$ は巡回群なので，その部分群も巡回群である．従って，命題 3.5.9 より $\mathbb{Z}$ の部分群はすべて $n\mathbb{Z}$ $(n \in \mathbb{Z})$ の形をしている[a]．

[a] この事実は環 $\mathbb{Z}$ が単項イデアル整域（PID）であることを意味している（代数基礎 2 で学ぶ）

演習問題

問題 3.5.1. 例 3.3.3(6)(a) の $D_3 \subseteq \mathsf{GL}_2(\mathbb{R})$ を考える．D_3 の以下の元の位数を求めよ：

(1) R
(2) T
(3) TR^2
(4) TR^3

問題 3.5.2. 例 3.3.3(6)(a) の $D_3 \subseteq S_3$ を考える．D_3 の以下の元の位数を求めよ：

(1) ρ
(2) τ
(3) $\tau\rho$
(4) $\tau\rho^5$

問題 3.5.3. (1) $G = \langle \zeta_4\rangle$ を位数 4 の巡回群とする．G の元 $1, \zeta_4, \zeta_4^2, \zeta_4^3$ の位数をそれぞれ求めよ．

(2) $G = \langle \zeta_6 \rangle$ を位数 6 の巡回群とする．G の元 $1, \zeta_6, \zeta_6^2, \zeta_6^3, \zeta_6^4, \zeta_6^5$ の位数をそれぞれ求めよ．

問題 3.5.4. $G = \langle x \rangle$ を位数 n の巡回群，m を n の約数，$l = n/m$ とする．このとき，$\langle x^l \rangle$ は位数 m の巡回群であることを示せ．

3.6　準同型写像と同型写像

2 つの群 G と H が与えられたとき，それらが一見異なるものでも “群として同じ構造を持っている” ことがあり得る．例えば，剰余群 $\mathbb{Z}/2\mathbb{Z}$ と $\mathbb{C} - \{0\}$ の部分群 $\{1, -1\}$ の乗積表を書いてみると，それぞれ

	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

	1	-1
1	1	-1
-1	-1	1

となり，$\overline{0} \leftrightarrow 1$ と $\overline{1} \leftrightarrow -1$ という元の対応で演算も対応していることが分かる．従って，一見全く異なる集合である $\mathbb{Z}/2\mathbb{Z}$ と $\{1, -1\}$ は群として同じ構造を持っていると言える．同様に，例 3.3.3(6) の群

$$D_n = \{E_2, R, R^2, \ldots, R^{n-1}, T, TR, TR^2, \ldots, TR^{n-1}\}$$
$$D_n = \{1_n, \rho, \rho^2, \ldots, \rho^{n-1}, \tau, \tau\rho, \tau\rho^2, \ldots, \tau\rho^{n-1}\}$$

も $T \leftrightarrow \tau$ と $R \leftrightarrow \rho$ という元の対応で演算も対応していることが分かる（$T^2 = E_2, R^n = E_2, R^k T = TR^{n-k}$ と $\tau^2 = 1_n, \rho^n = 1_n, \rho^k\tau = \tau\rho^{n-k}$ により）．この場合も 2 つの群は群として同じ構造を持っていると言える．このように 2 つの群が同じ構造を持つとき，「同型」であるという．

さらに「同型」の拡張として「準同型」という概念がある．これは 2 つの群が同じ構造を持つとまでは言えないまでも何らかの関係があることを意味する．群論では「準同型」や「同型」という概念を用いて様々な群の間の関係を調べることが重要になる．

準同型写像

定義 3.6.1. G, H を群とし，$f : G \to H$ を写像とする．

(1) $f : G \to H$ が**準同型写像**であるとは，

「任意の $x, y \in G$ に対して $f(xy) = f(x)f(y)$ が成り立つ」

を満たすときに言う．

(2) $f : G \to H$ が**同型写像**であるとは，以下の 2 条件を満たすときに言う．
- f は準同型写像である．
- 準同型写像 $g : H \to G$ が存在して $g \circ f = \mathrm{id}_G$, $f \circ g = \mathrm{id}_H$ が成り立つ．

(3) 群 G から H への同型写像が存在するとき，G と H **は同型**であるという．このとき $G \cong H$ と表す．

コメント. (1) G または H が加法群のとき，演算が積ではなく和で書かれるので準同型写像の定義は以下の様になる：
- G が加法群のとき：

任意の $x, y \in G$ に対して $f(x + y) = f(x)f(y)$ が成り立つ

- H が加法群のとき：

$$\text{任意の } x, y \in G \text{ に対して } f(xy) = f(x) + f(y) \text{ が成り立つ}$$

- G, H が加法群のとき：

$$\text{任意の } x, y \in G \text{ に対して } f(x+y) = f(x) + f(y) \text{ が成り立つ}$$

(2) 二つの群 G と H は同型であるとき，群として同じものとみなすことが出来る．

準同型写像 $f : G \to H$ が同型写像であるとは，定義より「f が逆写像 $f^{-1} : H \to G$ を持ち，かつ f^{-1} が準同型写像である」を意味する．実は f が逆写像を持つとき，f^{-1} は自動的に準同型写像になることが分かる：

命題 3.6.2. $f : G \to H$ を準同型写像とする． このとき，次の条件は同値である．

(1) f は同型写像
(2) f は全単射

証明. (1) $\Rightarrow$ (2) は定義からすぐに分かる．

(2) $\Rightarrow$ (1) : f は全単射なので定理 1.1.10 より f は逆写像 f^{-1} を持つ．$x, y \in H$ に対して，

$$f(f^{-1}(xy)) = xy = f(f^{-1}(x))f(f^{-1}(y)) = f(f^{-1}(x)f^{-1}(y))$$

となる（3 つ目の等号で f が準同型であることを使っている）．f は単射なので

$$f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$$

となる．従って，f の逆写像 f^{-1} は準同型写像である．このことから f は同型写像であることが示された． ■

例 3.6.3. (1) G を群とする．このとき，恒等写像

$$\mathrm{id}_G : G \to G,\ x \mapsto x$$

は準同型写像である．また，恒等写像は全単射なので id_G は同型写像である．

(2) G が群，H が G の部分群のとき，

$$i : H \to G,\ x \mapsto x$$

は準同型写像である．これは H が G と同じ演算で群になることから分かる．

(3) 巡回群 $G = \langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$ を考える．

このとき，

$$f : \mathbb{Z} \to G,\ k \mapsto x^k$$

は準同型写像である．

実際，$k, l \in \mathbb{Z}$ に対して

$$f(k+l) = x^{k+l} = x^k x^l = f(k)f(l)$$

が成り立つ（$\mathbb{Z}$ が加法群であることと上のコメントの (1) に注意）．

x の位数が無限のとき命題 3.5.7 より f は全単射となる．従って，f は同型写像となり，G と $\mathbb{Z}$ は同型である．

x の位数が $\mathrm{ord}(x) = n < \infty$ のとき，上と同様に

$$\overline{f} : \mathbb{Z}/n\mathbb{Z} \to G,\ \overline{k} \mapsto x^k$$

は準同型写像となる．

実際，$\overline{k}, \overline{l} \in \mathbb{Z}/n\mathbb{Z}$ に対して

$$\overline{f}\left(\overline{k}+\overline{l}\right) = x^{k+l} = x^k x^l = \overline{f}\left(\overline{k}\right)\overline{f}\left(\overline{l}\right)$$

が成り立つ．

さらに，命題 3.5.5 より $\overline{f}$ は全単射となる．従って，$\overline{f}$ は同型写像となり，G と $\mathbb{Z}/n\mathbb{Z}$ は同型である．

(4) $\mathsf{det} : \mathsf{GL}_n(\mathbb{R}) \to \mathbb{R} \setminus \{0\},\ A \mapsto \mathsf{det}(A)$ は準同型写像である．

実際，任意の $A, B \in \mathsf{GL}_n(\mathbb{R})$ に対して，

$$\mathsf{det}(AB) = \mathsf{det}(A)\,\mathsf{det}(B)$$

が成り立っている．

(5) $\mathsf{sgn} : S_n \to \mathbb{R} \setminus \{0\},\ \sigma \mapsto \mathsf{sgn}(\sigma)$ は準同型写像である．

実際，任意の $\sigma, \tau \in S_n$ に対して，命題 3.2.22 より

$$\mathsf{sgn}(\sigma\tau) = \mathsf{sgn}(\sigma)\,\mathsf{sgn}(\tau)$$

が成り立っている．

(6) $\mathbb{R} \setminus \{-1\}$ は演算

$$x * y := xy + x + y$$

で群となる（問題 3.1.4 参照）．このとき，写像

$$f : \mathbb{R} \setminus \{-1\} \to \mathbb{R} \setminus \{0\},\ x \mapsto x + 1$$

は準同型写像となる．

実際，$x, y \in \mathbb{R} \setminus \{-1\}$ に対して

$$f(x * y) = f(xy + x + y) = xy + x + y + 1 = (x + 1)(y + 1) = f(x)f(y)$$

となる．

また，f は全単射であることが容易に分かり，f は同型写像である．従って，$\mathbb{R} \setminus \{-1\}$ と $\mathbb{R} \setminus \{0\}$ は同型である．

(7) $f : \mathbb{Z}/2\mathbb{Z} \to \{1, -1\}$ を

$$f(\overline{0}) = 1 \quad f(\overline{1}) = -1$$

と定めると f は準同型写像である．

実際，

$$\begin{aligned}
f(\overline{0}+\overline{0}) &= f(\overline{0}) = 1 = f(\overline{0})f(\overline{0}) \\
f(\overline{0}+\overline{1}) &= f(\overline{1}) = -1 = 1(-1) = f(\overline{0})f(\overline{1}) \\
f(\overline{1}+\overline{0}) &= f(\overline{1}) = -1 = (-1)1 = f(\overline{1})f(\overline{0}) \\
f(\overline{1}+\overline{1}) &= f(\overline{0}) = 1 = (-1)(-1) = f(\overline{1})f(\overline{1})
\end{aligned}$$

が成り立っている．

また，明らかに f は全単射なので f は同型写像である．従って，$\mathbb{Z}/2\mathbb{Z}$ と $\{1, -1\}$ は同型である．

(8) 例 3.3.3(6) の群

$$G = \{E_2, R, R^2, \ldots, R^{n-1}, T, TR, TR^2, \ldots, TR^{n-1}\}$$
$$H = \{1_n, \rho, \rho^2, \ldots, \rho^{n-1}, \tau, \tau\rho, \tau\rho^2, \ldots, \tau\rho^{n-1}\}$$

を考える（そこではどちらも D_n と書いていたが区別のため G と H で表す）．写像

$$f : G \to H$$

を

$$f(R^i) = \rho^i \quad (i \in \mathbb{Z})$$
$$f(TR^i) = \tau\rho^i \quad (i \in \mathbb{Z})$$

で定義する．
このとき，関係式

$$T^2 = E_2,\ R^n = E_2,\ TR^i = R^{n-i}T,\ \tau^2 = 1_n,\ \rho^n = 1_n,\ \tau\rho^i = \rho^{n-i}\tau$$

により

$$\begin{aligned}
&f(R^iR^j) = f(R^{i+j}) = \rho^{i+j} = \rho^i\rho^j = f(R^i)f(R^j)\\
&f(R^i(TR^j)) = f(TR^{n-i}R^j) = f(TR^{n-i+j})\\
&\qquad = \tau\rho^{n-i+j} = \tau\rho^{n-i}\rho^j = \rho^i(\tau\rho^j) = f(R^i)f(TR^j)\\
&f((TR^i)R^j) = f(TR^{i+j}) = \tau\rho^{i+j} = (\tau\rho^i)\rho^j = f(TR^i)f(R^j)\\
&f((TR^i)(TR^j)) = f(TTR^{n-i}R^j) = f(R^{n-i+j})\\
&\qquad = \rho^{n-i+j} = \tau\tau\rho^{n-i}\rho^j = (\tau\rho^i)(\tau\rho^j) = f(TR^i)f(TR^j)
\end{aligned}$$

が分かる．従って，f は準同型写像．
また，明らかに f は全単射なので f は同型写像である．従って，G と H は同型である．つまり，G と H は群として同じものとみなすことが出来る．これが例 3.3.3(6) の群を同じ記号 D_n を使って書いた理由である．

準同型写像は群の演算を保つことが定義であるが，この定義から自動的に単位元，逆元を保つことが従う．

命題 3.6.4. $f : G \to H$ を準同型写像とする．このとき，以下が成り立つ．

(1) $f(1_G) = 1_H$
(2) $x \in G$ に対して $f(x^{-1}) = f(x)^{-1}$

証明. (1) $1_G = 1_G1_G$ より，

$$f(1_G) = f(1_G1_G) = f(1_G)f(1_G)$$

となる．両辺に左（または右）から $f(1_G)$ の逆元を掛けて

$$1_H = f(1_G)^{-1}f(1_G) = f(1_G)^{-1}f(1_G)f(1_G) = 1_Hf(1_G) = f(1_G)$$

となる．

(2) $xx^{-1} = 1_G$ なので，

$$1_H = f(1_G) = f(xx^{-1}) = f(x)f(x^{-1})$$

となる．両辺に左から $f(x)$ の逆元を掛けて，

$$f(x)^{-1} = f(x)^{-1}1_H = f(x)^{-1}f(x)f(x^{-1}) = f(x^{-1})$$

となる． ■

準同型写像の合成も再び準同型写像となる．

命題 3.6.5. (1) $f : G \to H$, $g : H \to I$ が (準) 同型写像のとき，$g \circ f : G \to I$ も (準) 同型写像．
(2) $f : G \to H$ が同型写像のとき，f の逆写像 $f^{-1} : H \to G$ も同型写像．

証明. (1) $f : G \to H$, $g : H \to I$ が準同型写像とする．このとき，任意の $x, y \in G$ に対して，

$$(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y)$$

となる（2 つ目の等号は f が準同型写像であることを，3 つ目の等号は g が準同型写像であることを使っている）．従って，$g \circ f : G \to I$ も準同型写像．

$f : G \to H$, $g : H \to I$ が同型写像のとき，$g \circ f$ は全単射であり前半の証明より $g \circ f$ は準同型写像なので命題 3.6.2 より $g \circ f$ は同型写像．

(2) : 命題 3.6.2 の証明により f^{-1} は準同型写像であり，全単射でもある．従って，命題 3.6.2 より f^{-1} は同型写像． ■

核と像

命題 3.6.2 により，準同型写像が同型かどうか知るためには単射性および全射性が問題になる．準同型写像の核および像とは，その準同型写像が単射および全射からどれぐらい離れているかを測る部分群である．

定義 3.6.6. $f : G \to H$ を準同型写像とする．

(1) G の部分集合

$$\mathrm{Ker}\, f := f^{-1}(\{1_H\}) = \{x \in G \mid f(x) = 1_H\}$$

を f の**核**（Kernel）という．

(2) H の部分集合

$$\mathrm{Im}\, f := f(G) = \{f(x) \mid x \in G\}$$

を f の**像**（Image）という．

命題 3.6.7. $f : G \to H$ を準同型写像とする．

(1) f の核 $\mathrm{Ker}\, f$ は G の部分群
(2) f の像 $\mathrm{Im}\, f$ は H の部分群

証明. (1) 定義 3.3.1 の (i)(ii)(iii) を確かめる：

(i) 命題 3.6.4(1) より $f(1_G) = 1_H$ なので $1_G \in \mathrm{Ker}\, f$.

(ii) $x, y \in \mathrm{Ker}\, f$ とする．このとき $f(x) = f(y) = 1_H$ となるので

$$f(xy) = f(x)f(y) = 1_H 1_H = 1_H$$

となる（1 つ目の等号で f が準同型写像であることを使っている）．従って，$xy \in \mathrm{Ker}\, f$.

(iii) $x \in \mathsf{Ker}\, f$ とする．このとき $f(x) = 1_H$ なので，命題 3.6.4(2) より

$$f(x^{-1}) = f(x)^{-1} = 1_H^{-1} = 1_H$$

となる．従って，$x^{-1} \in \mathsf{Ker}\, f$．

以上より，$\mathsf{Ker}\, f$ は G の部分群となる．

(2) 定義 3.3.1 の (i)(ii)(iii) を確かめる：

(i) 命題 3.6.4(1) より $1_H = f(1_G) \in \mathsf{Im}\, f$．

(ii) $f(x), f(y) \in \mathsf{Im}\, f$ とする．このとき，

$$f(x)f(y) = f(xy) \in \mathsf{Im}\, f$$

となる．

(iii) $f(x) \in \mathsf{Im}\, f$ とする．このとき，命題 3.6.4(2) より

$$f(x)^{-1} = f(x^{-1}) \in \mathsf{Im}\, f$$

となる．

以上より，$\mathsf{Im}\, f$ は H の部分群となる． ■

例 3.6.8. (1) G を群とし，$x \in G$ が $\mathsf{ord}(x) = n < \infty$ とする．このとき，準同型写像

$$f : \mathbb{Z} \to G,\ k \mapsto x^k$$

に対して，

$$\begin{aligned} \mathsf{Ker}\, f &= n\mathbb{Z} \quad (\text{命題 3.5.5 より}) \\ \mathsf{Im}\, f &= \langle x \rangle \quad (\text{巡回群 } \langle x \rangle \text{ の定義より}) \end{aligned}$$

となる．

(2) 準同型写像 $\det : \mathsf{GL}_n(\mathbb{R}) \to \mathbb{R} \setminus \{0\},\ A \mapsto \det(A)$ に対して，

$$\begin{aligned} \mathsf{Ker}(\det) &= \mathsf{SL}_n(\mathbb{R}) \\ \mathsf{Im}(\det) &= \mathbb{R} \setminus \{0\} \end{aligned}$$

となる．$\mathsf{Ker}(\det) = \mathsf{SL}_n(\mathbb{R})$ は特殊線形群の定義より分かる．$\mathsf{Im}(\det) = \mathbb{R} - \{0\}$ の方は任意の $a \in \mathbb{R} - \{0\}$ に対して正則行列

$$E(a) := \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

を考えると $\det(E(a)) = a$ となることから分かる．

(3) 準同型写像 $\mathsf{sgn} : S_n \to \mathbb{R} \setminus \{0\},\ \sigma \mapsto \mathsf{sgn}(\sigma)$ に対して，

$$\begin{aligned} \mathsf{Ker}(\mathsf{sgn}) &= A_n \quad (\text{交代群 } A_n \text{ の定義より}) \\ \mathsf{Im}(\mathsf{sgn}) &= \{1, -1\} \quad (\mathsf{sgn}(1\ 2) = -1,\ \mathsf{sgn}\, 1_n = 1 \text{ より}) \end{aligned}$$

となる．

準同型写像の単射性，全射性はそれぞれ核と像を用いて特徴づけられる：

命題 3.6.9. $f : G \to H$ を準同型写像とする．このとき，以下のことが成り立つ：

(1) 次の 2 条件は同値：
　(i) f は単射
　(ii) $\mathrm{Ker}\, f = \{1_G\}$
(2) 次の 2 条件は同値：
　(i) f は全射
　(ii) $\mathrm{Im}\, f = H$

証明. (1)(i) $\Rightarrow$ (ii)：($\supseteq$) の方は命題 3.6.4(1) で示されているので ($\subseteq$) を示せば良い．

$x \in \mathrm{Ker}\, f$ とする．このとき $f(x) = 1_H$ である．命題 3.6.4(1) より，$f(x) = 1_H = f(1_G)$ となるが，f が単射なので $x = 1_G$ となる．従って，$\mathrm{Ker}\, f \subseteq \{1_G\}$ が示された．

(ii) $\Rightarrow$ (i)：$x, y \in G$ が $f(x) = f(y)$ を満たすとする．両辺に $f(y)$ の逆元を右から掛けて

$$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = f(y)f(y)^{-1} = 1_H$$

となる（1 つ目の等号は f が準同型写像であることを，2 つ目の等号は命題 3.6.4(2) を使っている）．従って，$xy^{-1} \in \mathrm{Ker}\, f$ となる．ここで，$\mathrm{Ker}\, f = \{1_G\}$ なので $xy^{-1} = 1_G$ となり，$x = y$ が示された．このことから，f が単射となる．

(2) はほぼ全射の定義である． ■

注意. $\{1_G\}$ は G の最も小さい部分群なので，命題 3.6.9(1) により $\mathrm{Ker}\, f$ が小さいほど単射に近いと考えることができる．
同様に，H は H の最も大きい部分群なので，命題 3.6.9(2) により $\mathrm{Im}\, f$ が大きいほど全射に近いと考えることができる．

命題 3.6.2 と命題 3.6.9 を合わせて次のことが分かる：

命題 3.6.10. $f : G \to H$ を準同型写像とする．このとき，次の 3 条件は同値：

(1) f は同型写像
(2) f は全単射
(3) $\mathrm{Ker}\, f = \{1_G\}$ かつ $\mathrm{Im}\, f = H$

演習問題

問題 3.6.1. 以下の写像が準同型写像であるかどうか答えよ．また，準同型写像である場合はその核と像も求めよ．ただし，以下では $(0, \infty)$ は $\mathbb{R} - \{0\}$ の部分群と思っている．

(1) $f : \mathbb{R} - \{0\} \to \mathbb{R} - \{0\},\ x \mapsto x^2$
(2) $f : \mathbb{R} \to \mathbb{R},\ x \mapsto \sin x$
(3) $f : (0, \infty) \to \mathbb{R},\ x \mapsto \log x$
(4) $f : \mathbb{R} \to (0, \infty),\ x \mapsto e^x$
(5) $f : \mathbb{R} - \{0\} \to (0, \infty),\ x \mapsto e^x$
(6) $f : \mathbb{Z} \to \mathbb{Z},\ x \mapsto x + 1$

(7) $f : \mathbb{Z} \to \mathbb{Z},\ x \mapsto x^3$
(8) $f : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z},\ \overline{x} \mapsto \overline{x}^3$
(9) $f : \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z},\ \overline{x} \mapsto 3\overline{x}$
(10) $f : \mathbb{R} \to \mathbb{C} - \{0\},\ x \mapsto e^{ix} = \cos x + i \sin x$
(11) $f : \mathbb{R} \to \mathsf{GL}_2(\mathbb{R}),\ x \mapsto \begin{pmatrix} \cos x & -\sin x \\ \sin x & \cos x \end{pmatrix}$
(12) $f : \mathsf{GL}_2(\mathbb{R}) \to \mathbb{R},\ A \mapsto \mathrm{Tr}A$
(13) $f : \mathsf{GL}_2(\mathbb{R}) \to \mathsf{GL}_2(\mathbb{R}),\ A \mapsto {}^tA$
(14) $f : S_3 \to S_3,\ \sigma \mapsto (1\ 2)\sigma$
(15) $f : S_3 \to S_3,\ \sigma \mapsto (1\ 2)\sigma(1\ 2)$

問題 3.6.2. G を群とする．このとき，写像

$$f : G \to G,\ x \mapsto x^{-1}$$

は一般に準同型写像ではない．

(1) f が準同型写像となる G の例を一つ挙げよ．
(2) f が準同型写像とはならない群 G の例を一つ挙げよ．
(3) f が準同型写像となるための必要十分条件を求めよ．

問題 3.6.3. G, H を群，$f : G \to H$ を準同型写像とする．このとき，H の部分集合 $S \subseteq H$ に対して S の f による逆像

$$f^{-1}(S) := \{y \in H \mid f(y) \in S\}$$

が G の部分群となることを示せ（$S = \{1_H\}$ とすればこれは 命題 3.6.7(1) に他ならない）．

問題 3.6.4. G を群，$g \in G$ とする．このとき，

$$f_g : G \to G\ \ x \mapsto gxg^{-1}$$

が準同型写像となることを示せ．

第 4 章

剰余類と剰余群

$n \geq 1$ を整数とする．$\mathbb{Z}$ 上の同値関係

$$x \sim y :\Longleftrightarrow x \equiv y \bmod n$$

により，$\mathbb{Z}$ は n で割った余りで n 個のグループ

$$n\mathbb{Z},\ 1+n\mathbb{Z},\ 2+n\mathbb{Z}, \ldots,\ (n-1)+n\mathbb{Z}$$

に分けられた．この章ではもっと一般に群 G とその部分群 H に対して，G の元を H で割った “余り”のグループ：

$$xH \quad (x \in G)$$

で類別することを考える（$G = \mathbb{Z}$, $H = n\mathbb{Z}$ の場合が上記に相当する）．さらに，H が正規部分群と呼ばれる良い部分群のとき，このグループ達の集合 $G/H = \{xH \mid x \in G\}$ は自然に群とみなすことができる．大雑把に言えば，G の構造は H と G/H というより小さな二つの群の構造を用いて理解することができる．

4.1 剰余類

以下 G を群，H を G の部分群とする．

補題 4.1.1. (1) G 上の関係 $x \equiv_l y \bmod H$ を

$$x \equiv_l y \bmod H :\Longleftrightarrow y^{-1}x \in H\ (\Longleftrightarrow \exists h \in H \text{ s.t. } x = yh)$$

で定義すると，これは同値関係である．
また，この同値関係による $x \in G$ の同値類は

$$xH := \{xy \mid y \in H\}$$

である．

(2) G 上の関係 $x \equiv_r y \bmod H$ を

$$x \equiv_r y \bmod H :\Longleftrightarrow xy^{-1} \in H\ (\Longleftrightarrow \exists h \in H \text{ s.t. } x = hy)$$

で定義すると，これは同値関係である．
また，この同値関係による $x \in G$ の同値類は

$$Hx := \{xy \mid y \in H\}$$

である．

証明. (1) （反射律）$x \in G$ に対して，$x^{-1}x = 1_G \in H$ なので $x \equiv_l x \bmod H$.

（対称律）$x \equiv_l y \bmod H$ のとき $y^{-1}x \in H$ である．このとき，$x^{-1}y = (y^{-1}x)^{-1}$ なので $y \equiv_l x \bmod H$.

（推移律）$x \equiv_l y \bmod H$ かつ $y \equiv_l z \bmod H$ のとき，$y^{-1}x, z^{-1}y \in H$ である．このとき，$z^{-1}x = (z^{-1}y)(y^{-1}x) \in H$ なので $x \equiv_l z \bmod H$.

以上より，$x \equiv_l y \bmod H$ は G 上の同値関係である．

次に，この同値関係による $x \in G$ の同値類が xH であることを示す．$y \in G$ に対して

$$\begin{aligned} y \in [x] &\iff x \equiv_l y \bmod H \\ &\iff y \equiv_l x \bmod H \\ &\iff \exists h \in H \text{ s.t. } y = xh \\ &\iff y \in xH \end{aligned}$$

が成り立つので，$[x] = xH$.

(2) も全く同様に示される． ■

定義 4.1.2. $x \in G$ とする．

(1) 集合 $xH = \{xy \mid y \in H\}$ を H **を法とする** x **の左剰余類**と呼ぶ．また，H を法とする左剰余類全体の集合（同値関係 $x \equiv_l y \bmod H$ による商集合）を

$$G/H := \{xH \mid x \in G\}$$

と書き，G の H **による左剰余集合**と呼ぶ．

(2) 集合 $Hx = \{yx \mid y \in H\}$ を H **を法とする** x **の右剰余類**と呼ぶ．また，H を法とする右剰余類全体の集合（同値関係 $x \equiv_r y \bmod H$ による商集合）を

$$H\backslash G := \{Hx \mid x \in G\}$$

と書き，G の H **による右剰余集合**と呼ぶ．

コメント. $G = \mathbb{Z}$, $H = n\mathbb{Z}$ のとき，

$$x \equiv_l y \bmod n\mathbb{Z} \iff x \equiv_r y \bmod n\mathbb{Z} \iff x \equiv y \bmod n$$

である．従って，同値関係 $x \equiv_l y \bmod H$, $x \equiv_r y \bmod H$ は $\mathbb{Z}$ 上の合同式 $x \equiv y \bmod n$ を一般の群に拡張したものである．

注意. (1) G が可換群ならば任意の $x, y \in G$ に対して $xy = yx$ が成り立つので，$xH = Hx$ となる．従って，G が可換群ならば $G/H = H\backslash G$ も従う．
一方で，可換群とは限らない場合，一般に $xy \neq yx$ であることから，

$$xH \neq Hx$$

である．全ての $x \in G$ に対してこれが等号になるような部分群 H は**正規部分群**と呼ばれ，重要な役割を果たす（第 4.2 節）．

(2) G の 2 元 x, y に対して，$x \neq y$ でも $xH \neq yH$ とは限らない．ざっくり言えば，異なる G の元も集合 G/H において同一視される．どのような元が同一視されるかは次の命題から分かる．

命題 4.1.3. (1) $x, y \in G$ に対して次の 3 条件は全て互いに同値である：

(i) $xH \cap yH \neq \emptyset$

(ii) $xH = yH$

(iii) $y^{-1}x \in H$

特に，$x \in G$ に対して

$$xH = H \iff x \in H$$

(2) $x, y \in G$ に対して次の 3 条件は全て互いに同値である：

(i) $Hx \cap Hy \neq \emptyset$

(ii) $Hx = Hy$

(iii) $yx^{-1} \in H$

特に，$x \in G$ に対して

$$Hx = H \iff x \in H$$

証明. (1)(2) はそれぞれ同値関係 $x \equiv_l y \bmod H$, $x \equiv_r y \bmod H$ に対して命題 1.2.5(3) を用いることで得られる． ■

例 4.1.4. (1) $G = \mathbb{Z}$, $H = n\mathbb{Z}$ とする．$x \in \mathbb{Z}$ の $n\mathbb{Z}$ を法とする左剰余類は

$$x + n\mathbb{Z} = \{x + nq \mid q \in \mathbb{Z}\}$$

となり，$\mathbb{Z}$ の $n\mathbb{Z}$ による左剰余集合は

$$\begin{aligned}\mathbb{Z}/n\mathbb{Z} &= \{x + n\mathbb{Z} \mid x \in \mathbb{Z}\} \\ &= \begin{cases} \{n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\} & (n \neq 0 \text{ のとき}) \\ \{\{x\} \mid x \in \mathbb{Z}\} & (n = 0 \text{ のとき}) \end{cases}\end{aligned}$$

となる．

また，$\mathbb{Z}$ は可換群なので $\mathbb{Z}/n\mathbb{Z} = n\mathbb{Z}\backslash\mathbb{Z}$ である．

(2) $G = \mathsf{GL}_n(\mathbb{R})$, $H = \mathsf{SL}_n(\mathbb{R})$ とする．$A \in \mathsf{GL}_n(\mathbb{R})$ の $\mathsf{SL}_n(\mathbb{R})$ による左剰余類および右剰余類はそれぞれ

$$\begin{aligned}A\mathsf{SL}_n(\mathbb{R}) &= \{AB \mid B \in \mathsf{SL}_n(\mathbb{R})\} \\ \mathsf{SL}_n(\mathbb{R})A &= \{BA \mid B \in \mathsf{SL}_n(\mathbb{R})\}\end{aligned}$$

であり，$\mathsf{GL}_n(\mathbb{R})$ の $\mathsf{SL}_n(\mathbb{R})$ による左剰余集合および右剰余集合はそれぞれ

$$\begin{aligned}\mathsf{GL}_n(\mathbb{R})/\mathsf{SL}_n(\mathbb{R}) &= \{A\mathsf{SL}_n(\mathbb{R}) \mid A \in \mathsf{GL}_n(\mathbb{R})\} \\ \mathsf{SL}_n(\mathbb{R})\backslash\mathsf{GL}_n(\mathbb{R}) &= \{\mathsf{SL}_n(\mathbb{R})A \mid A \in \mathsf{GL}_n(\mathbb{R})\}\end{aligned}$$

となる．

以下，左剰余集合 $\mathsf{GL}_n(\mathbb{R})/\mathsf{SL}_n(\mathbb{R})$ についてもう少し詳しく見ていく（右剰余集合 $\mathsf{SL}_n(\mathbb{R})\backslash\mathsf{GL}_n(\mathbb{R})$ についても同様のことが言える）．

実数 $a \in \mathbb{R} \setminus \{0\}$ に対して行列 $E(a) \in \mathsf{GL}_n(\mathbb{R})$ を

$$E(a) := \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

と定める．

$A \in \mathsf{GL}_n(\mathbb{R})$ の行列式を $a = \det(A)$ とする．$\det(E(a)) = a$ に注意すると

$$A^{-1}E(a) \in \mathsf{SL}_n(\mathbb{R})$$

が成り立ち，

$$A\mathsf{SL}_n(\mathbb{R}) = I(a)\mathsf{SL}_n(\mathbb{R})$$

が分かる．このことから集合の等号

$$\mathsf{GL}_n(\mathbb{R})/\mathsf{SL}_n(\mathbb{R}) = \{E(a)\mathsf{SL}_n(\mathbb{R}) \mid a \in \mathbb{R} \setminus \{0\}\}$$

が言えるので，全単射

$$f : \mathbb{R} \setminus \{0\} \to \mathsf{GL}_n(\mathbb{R})/\mathsf{SL}_n(\mathbb{R}),\ a \mapsto I(a)\mathsf{SL}_n(\mathbb{R})$$

を得る（全射になることは上の議論から分かり，単射になることは $E(a)\mathsf{SL}_n(\mathbb{R})$ の元の行列式を見ることで分かる）．

(3) $G = S_n$, $H = A_n$ とする．$\sigma \in S_n$ の A_n による左剰余類および右剰余類はそれぞれ

$$\sigma A_n := \{\sigma\tau \mid \tau \in A_n\}$$
$$A_n\sigma := \{\tau\sigma \mid \tau \in A_n\}$$

であり，S_n の A_n による左剰余集合および右剰余集合はそれぞれ

$$S_n/A_n := \{\sigma A_n \mid \sigma \in S_n\}$$
$$A_n\backslash S_n := \{A_n\sigma \mid \sigma \in S_n\}$$

である．

以下，集合 S_n/A_n についてもう少し詳しく見ていく（右剰余集合 $A_n\backslash S_n$ についても同様のことが言える）．$\sigma \in S_n$ が偶置換のとき，$\sigma \in A_n$ なので $\sigma A_n = A_n$ となる，一方で，$\sigma \in S_n$ が奇置換のとき $\sigma^{-1}(1\ 2) \in A_n$ なので $\sigma A_n = (1\ 2)A_n$ となる．以上より

$$S_n/A_n = \{A_n, (1\ 2)A_n\}$$

が分かるので，全単射

$$f : \{1, -1\} \to S_n/A_n$$

が $f(1) = A_n$, $f(-1) = (1\ 2)A_n$ で与えられる．

(4) 例 3.3.3(6)(a) の群 $D_3 = \{E_2, R, R^2, T, TR, TR^2\}$ および D_3 の部分群 $H = \langle R\rangle$ を考える．このとき，D_3 の $\langle R\rangle$ による左剰余集合 $D_3/\langle R\rangle$ について考える．

まず，命題 3.5.5 により $\langle R\rangle = \{E_2, R, R^2\}$ となることに注意しておく．$\langle R\rangle$ を法とする左剰余類

$$E_n\langle R\rangle,\ R\langle R\rangle,\ R^2\langle R\rangle,\ T\langle R\rangle,\ TR\langle R\rangle,\ TR^2\langle R\rangle$$

がそれぞれどのような集合か計算すると，

$$\begin{aligned}
E_n\langle R\rangle &= \langle R\rangle = \{E_2, R, R^2\}\\
R\langle R\rangle &= \{RE_2, RR, RR^2\} = \{R, R^2, R^3\} = \{E_2, R, R^2\}\\
R^2\langle R\rangle &= \{R^2E_2, R^2R, R^2R^2\} = \{R^2, R^3, R^4\} = \{E_2, R, R^2\}\\
T\langle R\rangle &= \{TE_2, TR, TR^2\} = \{T, TR, TR^2\} = \{T, TR, TR^2\}\\
TR\langle R\rangle &= \{TRE_2, TRR, TRR^2\} = \{TR, TR^2, TR^3\} = \{T, TR, TR^2\}\\
TR^2\langle R\rangle &= \{TR^2E_2, TR^2R, TR^2R^2\} = \{TR^2, TR^3, TR^4\} = \{T, TR, TR^2\}
\end{aligned}$$

のようになる．従って，$\langle R\rangle = E_n\langle R\rangle = R\langle R\rangle = R^2\langle R\rangle$, $T\langle R\rangle = TR\langle R\rangle = TR^2\langle R\rangle$ なので

$$D_3/\langle R\rangle = \{\langle R\rangle, T\langle R\rangle\}$$

となる．

同様に右剰余類を計算すると，

$$\begin{aligned}\langle R\rangle E_2 &= \langle R\rangle = \{E_2, R, R^2\}\\ \langle R\rangle R &= \{E_2, R, R^2\}\\ \langle R\rangle R^2 &= \{E_2, R, R^2\}\\ \langle R\rangle T &= \{T, TR, TR^2\}\\ \langle R\rangle TR &= \{T, TR, TR^2\}\\ \langle R\rangle TR^2 &= \{T, TR, TR^2\}\end{aligned}$$

となるので

$$\langle R\rangle\backslash D_3 = \{\langle R\rangle, \langle R\rangle T\}$$

である．

上の計算から，任意の D_3 の元 A に対して $A\langle R\rangle = \langle R\rangle A$ となることが分かる．特に，

$$D_3/\langle TR\rangle = \langle TR\rangle\backslash D_3$$

である．

(5) 例 3.3.3(6)(a) の群 $D_3 = \{E_2, R, R^2, T, TR, TR^2\}$ および D_3 の部分群 $H = \langle TR\rangle$ を考える．このとき，D_3 の $\langle TR\rangle$ による左剰余集合 $D_3/\langle TR\rangle$ について考える．
まず，$(TR)^2 = TRTR = TTR^2R = E_2$ なので命題 3.5.5 により $\langle TR\rangle = \{E_2, TR\}$ となることに注意しておく．$\langle TR\rangle$ による左剰余類

$$E_n\langle TR\rangle,\ R\langle TR\rangle,\ R^2\langle TR\rangle,\ T\langle TR\rangle,\ TR\langle TR\rangle,\ TR^2\langle TR\rangle$$

がそれぞれどのような集合か計算すると，

$$\begin{aligned}E_n\langle TR\rangle &= \langle TR\rangle = \{E_2, TR\}\\ R\langle TR\rangle &= \{RE_2, RTR\} = \{R, T\}\\ R^2\langle TR\rangle &= \{R^2E_2, R^2TR\} = \{R^2, TR^2\}\\ T\langle TR\rangle &= \{TE_2, TTR\} = \{R, T\}\\ TR\langle TR\rangle &= \{TRE_2, (TR)^2\} = \{E_2, TR\}\\ TR^2\langle TR\rangle &= \{TR^2E_2, TR^2TR\} = \{R^2, TR^2\}\end{aligned}$$

従って，$\langle TR\rangle = E_n\langle TR\rangle = TR\langle TR\rangle$, $R\langle TR\rangle = T\langle TR\rangle$, $R^2\langle TR\rangle = TR^2\langle TR\rangle$ なので

$$D_3/\langle TR\rangle = \{\langle TR\rangle, R\langle TR\rangle, R^2\langle TR\rangle\}$$

となる．

同様に右剰余類を計算すると，

$$\begin{aligned}\langle TR\rangle E_2 &= \langle TR\rangle = \{E_2, TR\}\\ \langle TR\rangle R &= \{E_2R, TRR\} = \{R, TR^2\}\\ \langle TR\rangle R^2 &= \{E_2R^2, TRR^2\} = \{R^2, T\}\\ \langle TR\rangle T &= \{E_2T, TRT\} = \{R^2, T\}\\ \langle TR\rangle TR &= \{E_2TR, (TR)^2\} = \{E_2, TR\}\\ \langle TR\rangle TR^2 &= \{E_2TR^2, TRTR^2\} = \{R, TR^2\}\end{aligned}$$

となるので

$$\langle TR\rangle\backslash D_3 = \{\langle TR\rangle, \langle TR\rangle R, \langle TR\rangle R^2\}$$

である．

以上の計算から $D_3/\langle TR\rangle \neq \langle TR\rangle\backslash D_3$ となることが分かる．

コメント． n を 1 以上の整数とする． 第 3.2 節 において

$$\overline{a} = \overline{b} \Longleftrightarrow a \equiv b \bmod n$$

なる記号 $\overline{a}$ を導入した．命題 4.1.3 により $n\mathbb{Z}$ を法とする左剰余類は

$$a + n\mathbb{Z} = b + n\mathbb{Z} \Longleftrightarrow a - b \in n\mathbb{Z} \Longleftrightarrow a \equiv b \bmod n$$

を満たすので，$\overline{a} = a + n\mathbb{Z}$ と思うことにする．特に，第 3.2 節 で導入した $\mathbb{Z}/n\mathbb{Z}$ は $\mathbb{Z}$ の $n\mathbb{Z}$ による左剰余集合と同じものと思う．

左剰余類と右剰余類および左剰余集合と右剰余集合は集合としては一般に異なるものだが，それらの元の個数は等しい．

命題 4.1.5. G を群，H を G の部分群とする．このとき，

(1) $|G/H| = |H\backslash G|$
(2) 任意の $x \in G$ に対して，$|xH| = |Hx| = |H|$

証明. 2 つの集合 X, Y について，$|X| = |Y|$ である（つまり X と Y の元の個数が等しい）ためには，ある全単射 $f : X \to Y$ が存在すれば良い．

(1) 全単射 $f : G/H \to H\backslash G$ を見つける．写像 $f : G/H \to H\backslash G$ を

$$f(xH) = Hx^{-1}$$

と定める．このとき，f は well-defined である．実際，$xH = x'H$ のとき $x^{-1}x' \in H$ であるが，これは $Hx^{-1} = Hx'^{-1}$ を意味する．この写像 $f : G/H \to H\backslash G$ は $g : H\backslash G \to G/H$, $Hx \mapsto x^{-1}H$ を逆写像としてもつので（g の well-defined 性も要チェック!!），f は全単射．

(2) 全単射 $f : H \to xH$ を見つければ $|xH| = |H|$ が示される（$|Hx| = |H|$ も同様）．$f : H \to xH$ を $f(y) = xy$ で定義すると，f は $g : xH \to H$, $xy \mapsto y$ を逆写像として持つので，f は全単射． ■

定義 4.1.6. G を群，H を G の部分群とする．このとき，H の G における指数を

$$[G : H] := |G/H|$$

で定義する．定義により $[G : H]$ は 1 以上の整数または ∞ となる．命題 4.1.5 より $[G : H] = |H\backslash G|$ でもある．

例 4.1.7. 例 4.1.4 より以下のことが分かる．

(1) $[\mathbb{Z} : n\mathbb{Z}] = \begin{cases} n & (n \neq 0 \text{ のとき}) \\ \infty & (n = 0 \text{ のとき}) \end{cases}$
(2) $[\mathsf{GL}_n(\mathbb{R}) : \mathsf{SL}_n(\mathbb{R})] = \infty$

(3) $[S_n : A_n] = 2$

(4) $[D_3 : \langle R \rangle] = 2$

(5) $[D_3 : \langle TR \rangle] = 3$

ラグランジュの定理

群論における最も重要な定理の一つとして以下のラグランジュの定理がある：

定理 4.1.8. （ラグランジュの定理） G を群，H を G の部分群とする．このとき，

$$|G| = [G : H]|H|$$

が成り立つ（ここで，$\infty \cdot n = n \cdot \infty = \infty \cdot \infty = \infty$ としている）．特に $|G| < \infty$ のとき，以下が成り立つ：

- $[G : H]$ は 1 以上の整数
- $|H|$ は $|G|$ の約数
- $[G : H] = |G|/|H|$

証明. 簡単のため $|G| < \infty$ の場合を考える．G/H の元の個数を m とし，その相異なる元を $x_1H, x_2H, \ldots, x_mH$ とする（つまり，$x_1, x_2, \ldots, x_m$ は G/H の完全代表系）．このとき，命題 4.1.3 より $i \neq j$ のとき $x_iH \cap x_jH = \emptyset$ である．G は $x_1H, x_2H, \ldots, x_mH$ の和集合でどの二つも交わらないので，

$$|G| = |x_1H| + |x_2H| + \cdots + |x_mH|$$

となる．ここで，命題 4.1.5(2) より $|x_iH| = |H|$ となり，

$$|G| = \overbrace{|H| + |H| + \cdots + |H|}^{m \text{ 個}} = m|H| = [G : H]|H|$$

が示された．

後半の主張は等式 $|G| = [G : H]|H|$ よりすぐに分かる． ■

例 4.1.9. (1) $G = \mathbb{Z}$, $H = n\mathbb{Z}$ の場合を考える．

$n \in \mathbb{Z}$（$n \neq 0$）とすると，$|\mathbb{Z}| = |n\mathbb{Z}| = \infty$, $[\mathbb{Z} : n\mathbb{Z}] = n$ より

$$\infty = n \cdot \infty$$

となり，確かにラグランジュの定理が成り立っている．

$n = 0$ のとき，$|\mathbb{Z}| = [\mathbb{Z} : 0\mathbb{Z}] = \infty$, $|0\mathbb{Z}| = 1$ より

$$\infty = \infty \cdot 1$$

となり，確かにラグランジュの定理が成り立っている．

(2) $G = \mathsf{GL}_n(\mathbb{R})$, $H = \mathsf{SL}_n(\mathbb{R})$ のとき，$|\mathsf{GL}_n(\mathbb{R})| = |\mathsf{SL}_n(\mathbb{R})| = [\mathsf{GL}_n(\mathbb{R}) : \mathsf{SL}_n(\mathbb{R})] = \infty$ より

$$\infty = \infty \cdot \infty$$

となり，確かにラグランジュの定理が成り立っている．

(3) $G = S_n$, $H = A_n$ のとき，$|S_n| = n!$, $[S_n : A_n] = 2$ なのでラグランジュの定理より

$$|A_n| = |S_n|/[S_n : A_n] = \frac{n!}{2}$$

となる．

(4) $G = D_3$, $H = \langle R \rangle$ のとき $|D_3| = 6$, $|\langle R \rangle| = 3$, $[D_3 : \langle R \rangle] = 2$ なので

$$6 = 2 \cdot 3$$

となり，確かにラグランジュの定理が成り立っている．

(5) $G = D_3$, $H = \langle TR \rangle$ のとき $|D_3| = 6$, $|\langle TR \rangle| = 2$, $[D_3 : \langle TR \rangle] = 3$ なので

$$6 = 3 \cdot 2$$

となり，確かにラグランジュの定理が成り立っている．

ラグランジュの定理の重要性は以下の様々な応用を見れば納得できるであろう．

系 4.1.10. G を有限群，x を G の元とする．このとき，$\mathrm{ord}(x)$ は $|G|$ の約数である．特に，$x^{|G|} = 1_G$ が成り立つ．

証明. $\langle x \rangle$ は G の部分群なのでラグランジュの定理より $|\langle x \rangle|$ は $|G|$ の約数である．命題 3.5.5 より $\mathrm{ord}(x) = |\langle x \rangle|$ となるので系の主張が示される． ■

フェルマーの小定理（定理 2.2.9）は定理 4.1.8 からすぐに従う：

系 4.1.11. （フェルマーの小定理） p を素数とする．このとき，p と互いに素な整数 x に対して，

$$x^{p-1} \equiv 1 \bmod p$$

が成り立つ．

証明. $G = (\mathbb{Z}/p\mathbb{Z})^\times$（定義 3.2.7 で定義した群）は位数 $p-1$ の有限群である．従って，$\overline{x} \in (\mathbb{Z}/p\mathbb{Z})^\times$ に対して系 4.1.10 を用いると

$$\overline{x}^{p-1} = \overline{1}$$

となるが，これは

$$x^{p-1} \equiv 1 \bmod p$$

を意味する． ■

同様に，$G = (\mathbb{Z}/n\mathbb{Z})^\times$ を考えることでオイラーの定理（定理 2.2.12）も示される：

系 4.1.12. （オイラーの定理）n を正の素数とする．このとき，n と互いに素な整数 x に対して，

$$x^{\varphi(n)} \equiv 1 \bmod n$$

が成り立つ．

また，以下の系もラグランジュの定理の重要な応用である．

系 4.1.13. G を有限群で位数が素数 p であるとする．このとき，G は巡回群である．

証明. G の元 x で単位元でないものを取る（$|G| = p \geq 2$ なのでこのような x がある）．このとき，$|\langle x \rangle|$ は 1 でない $|G| = p$ の約数なので，$|G| = |\langle x \rangle|$ となる．従って，$G = \langle x \rangle$ ■

演習問題

問題 4.1.1. 以下の群 G と G の部分群 H に対して左剰余集合 G/H および指数 $[G : H]$ を求めよ．ただし，G/H はその元を重複しないように全て求めよ（つまり，$[G : H]$ 個の異なる元を求める）．

(1) $G = \mathbb{Z}/15\mathbb{Z}$, $H = \langle \overline{3} \rangle$

(2) $G = (\mathbb{Z}/16\mathbb{Z})^{\times}$, $H = \langle \overline{7} \rangle$

(3) $G = \langle \zeta_{24} \rangle$, $H = \langle \zeta_{24}^6 \rangle$
ただし，$\zeta_{24} = e^{\frac{2\pi}{24}}$ は 1 の原始 24 乗根.

(4) $D_3 = \{E_2, R, R^2, T, TR, TR^2\}$, $H = \langle T \rangle$

(5) $D_4 = \{E_2, R, R^2, R^3, T, TR, TR^2, TR^3\}$, $H = \langle TR^2 \rangle$

(6) $G = S_3$, $H = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\rangle$

(7) $G = S_4$, $H = \{1_4, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$

(8) $G = S_4$, $H = \{1_4, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$

問題 4.1.2. S_3 の元 $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ および S_3 の部分群 $H = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\rangle$ を考える．このとき，G の元 σ, σ' であって，

- $\sigma H = \sigma' H$
- $\sigma\tau H \neq \sigma'\tau H$

を両方満たすような σ, σ' の例を一組見つけよ．

問題 4.1.3. G を群，H をその部分群とする．このとき，

$$f : G/H \to H\backslash H,\ xH \mapsto Hx$$

が *well-defined* でないような例を見つけよ（例えば $G = S_3$, $H = \langle (2\ 3) \rangle$ ではどうか）.

問題 4.1.4. G を群とする．このとき，以下の 2 条件が同値であることを示せ.

(1) G はアーベル群

(2) 任意の $x \in G$ に対して $xH = Hx$.

4.2　正規部分群と剰余群

$\mathbb{Z}$ の $n\mathbb{Z}$ による左剰余集合 $\mathbb{Z}/n\mathbb{Z}$ は $\mathbb{Z}$ の加法から自然に定まる加法により群となっていた（命題 3.2.13）．$\mathbb{Z}$ の代わりに $\mathbb{Z}/n\mathbb{Z}$ を考えることで，整数 x を n で割った余りというより簡単な/小さい整数に取り替えることができ，色々な計算が簡単になった（例 2.2.3）．

一般の群 G の部分群 H による左剰余集合 G/H においても，G の元 x は G/H において $y^{-1}x \in H$ を満たす元 y に自由に取り替えることができる（命題 4.1.3 より $xH = yH$ なので）．従って，G の代わりに G/H を用いることで計算が簡単になると期待できる．そのためには G/H が G から自然に定まる演算

$$(xH)(yH) := xyH$$

で群になっていて欲しい．群の定義 3.1.2(i)(ii)(iii) は G が群であることから自動的に従うが，問題となるのはこの演算の well-defined 性：

$$xH = x'H,\ yH = y'H \Longrightarrow (xH)(yH) = (x'H)(y'H) \quad （つまり\ xyH = x'y'H）$$

である．残念ながら，これは一般に成り立たない：

$G = S_3$, $H = \langle(1\ 3)\rangle$, $\sigma = (1\ 3)$, $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ としたとき，$1_3H = \sigma H$ かつ $\tau H = \tau H$ であるが，

$$(1_3H)(\tau H) = 1_3\tau H \neq \sigma\tau H = (\sigma H)(\tau H)$$

である（$\tau^{-1}\sigma\tau = (2\ 3) \notin H$ より（問題 4.1.2 参照））

この演算が well-defined になるような部分群は正規部分群と呼ばれ，群論において重要な役割を果たす．

正規部分群

定義 4.2.1.　G を群，N を G の部分群とする．条件

「任意の $x \in G$ と $y \in N$ に対して $xyx^{-1} \in N$ が成り立つ」

が成り立つとき，G は N の**正規部分群（normal subgroup）**であるという．N が G の正規部分群であるとき $N \triangleleft G$ と書く．

注意. (1) 自明な部分群 $\{1_G\}$ と G は定義より明らかに正規部分群である．

(2) $xNx^{-1} := \{xyx^{-1} \mid y \in N\}$ と置いたとき $N \triangleleft G$ は「任意の $x \in G$ に対して $xNx^{-1} \subseteq N$ が成り立つ」を意味している．実は，

$$N \triangleleft G \Longleftrightarrow \text{「任意の } x \in G \text{ に対して } xNx^{-1} = N \text{ が成り立つ」}$$

を示すことができる（各自チェックせよ）．

この他にも $N \triangleleft G$ の様々な言い換えがある（問題 4.2.1 参照）．

正規部分群の典型例は準同型写像の核である．

命題 4.2.2.　$f : G \to H$ を準同型写像とする．このとき，$\mathrm{Ker}\, f$ は G の正規部分群である．

証明. 任意の $x \in G$ と $y \in \mathsf{Ker}\, f$ に対して $xyx^{-1} \in \mathsf{Ker}\, f$ を示す．実際，

$$f(xyx^{-1}) = f(x)f(y)f(x)^{-1} = f(x)1_H f(x)^{-1} = 1_H$$

となるので $xyx^{-1} \in \mathsf{Ker}\, f$ となる． ■

注意. 一般に準同型写像 $f : G \to H$ の像 $\mathsf{Im}\, f$ は H の正規部分群とは限らない．

例 4.2.3. (1) G が可換群ならば，G の全ての部分群は正規部分群である．

実際，N を可換群 G の部分群とすると，任意の $x \in G$ と $y \in N$ に対して G の可換性により

$$xyx^{-1} = yxx^{-1} = y \in N$$

となる．従って，N は G の正規部分群．

特に，$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q} - \{0\}$, $\mathbb{R} - \{0\}$, $\mathbb{C} - \{0\}$, $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^\times$ の部分群は全て正規部分群である．

(2) $\mathsf{GL}_n(\mathbb{R})$ の部分群 $\mathsf{SL}_n(\mathbb{R})$ は正規部分群である．

実際，$\mathsf{SL}_n(\mathbb{R})$ は準同型写像

$$\det : \mathsf{GL}_n(\mathbb{R}) \to \mathbb{R} - \{0\},\ A \mapsto \det(A)$$

の核なので命題 4.2.2 より正規部分群である．

(3) S_n の部分群 A_n は正規部分群である．

実際，A_n は準同型写像

$$\mathsf{sgn} : S_n \to \{1, -1\},\ \sigma \mapsto \mathsf{sgn}(\sigma)$$

の核なので命題 4.2.2 より正規部分群である．

(4) $\mathsf{GL}_2(\mathbb{R})$ の部分群

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| a, b, d \in \mathbb{R}, a \neq 0, d \neq 0 \right\}, \quad N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| b \in \mathbb{R} \right\}$$

を考える（G, N が $\mathsf{GL}_2(\mathbb{R})$ の部分群になることは各自チェックせよ）．このとき，N は G の正規部分群である．

実際，任意の

$$\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \in G, \quad \begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix} \in N$$

に対して

$$\begin{aligned} \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}^{-1} &= \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_1^{-1} & -a_1^{-1}b_1d_1^{-1} \\ 0 & d_1^{-1} \end{pmatrix} \\ &= \begin{pmatrix} 1 & a_1b_2d_1^{-1} \\ 0 & 1 \end{pmatrix} \in N \end{aligned}$$

となるので，N は G の正規部分群である．

(5) S_4 の部分群 $N = \{1_4, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ は正規部分群である．

実際，任意の $\sigma \in S_4$ に対して

$$\begin{aligned}\sigma 1_4 \sigma^{-1} &= 1_4 \in N \\ \sigma(1\ 2)(3\ 4)\sigma^{-1} &= (\sigma(1),\ \sigma(2))(\sigma(3)\ \sigma(4)) \in N \\ \sigma(1\ 3)(2\ 4)\sigma^{-1} &= (\sigma(1),\ \sigma(3))(\sigma(2)\ \sigma(4)) \in N \\ \sigma(1\ 4)(2\ 3)\sigma^{-1} &= (\sigma(1),\ \sigma(4))(\sigma(2)\ \sigma(3)) \in N\end{aligned}$$

が成り立つことが分かる．よって，N は S_4 の正規部分群．

(6) $\mathsf{GL}_2(\mathbb{R})$ の部分群 $H = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle = \left\{ E_2, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$ は正規部分群ではない．

実際，$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in \mathsf{GL}_2(\mathbb{R}),\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in H$ に対して

$$\begin{aligned}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{-1} &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix} \notin H\end{aligned}$$

となるので H は $\mathsf{GL}_2(\mathbb{R})$ の正規部分群ではない．

(7) S_3 の部分群 $H = \langle (1\ 2) \rangle = \{1_3, (1\ 2)\}$ は正規部分群ではない．

実際，

$$(1\ 3)(1\ 2)(1\ 3)^{-1} = (1\ 3)(1\ 2)(1\ 3) = (2\ 3) \notin H$$

となるので H は S_3 の正規部分群ではない．

命題 4.2.4. *N を群 G の正規部分群とする．このとき，任意の $x \in G$ に対して $xN = Nx$ が成り立つ．特に，$G/N = N\backslash G$ が成り立つ．*

証明. $xN \subseteq Nx$ を示す（逆の包含 $Nx \subseteq xN$ も全く同様に示される）．任意の $xn \in xN$（$n \in N$）を取ると，N が正規部分群なので $xnx^{-1} \in N$ となる．$n' := xnx^{-1} \in N$ とおけば $xn = n'x \in Nx$ となる．このことから，$xN \subseteq Nx$ が示された． ■

この命題により正規部分群 N に対してはその左剰余集合および右剰余集合が一致するので，以降では左剰余集合 G/N のみを考えることにする．

剰余群

次に，正規部分群 N に対して G/N の演算

$$(xN)(yN) := xyN$$

が well-defined であることおよびこの演算で G/N が群になることを確かめていく．well-defined であることは次の補題から分かる．

補題 4.2.5. *G を群，N を G の正規部分群とする．このとき，$x, x'y, y' \in G$ に対して，$xN = x'N$ かつ $yN = y'N$ ならば $xyN = x'y'N$ が成り立つ．*

証明. $xyN \subseteq x'y'N$ を示す（逆の包含 $x'y'N \subseteq xyN$ も全く同様）．つまり，任意の $xyn \in xyN$ $(n \in N)$ に対して $xyn \in x'y'N$ を示せばよい．

$x = x1_G \in xN = x'N$, $y = y1_N \in yN = y'N$ より $x = x'n'$, $y = y'n''$（$n', n'' \in N$）と表せる．従って，$xyn = x'n'y'n''n$ となる．ここで，N が正規部分群であることを用いると $\tilde{n} := y'^{-1}n'y' \in N$ となるが，$n'y' = y'\tilde{n}$ であることから

$$xyn = x'n'y'n''n = x'y'\tilde{n}n''h \in x'y'N$$

が分かる．よって，$xyN \subseteq x'y'N$ が示された． ■

この補題により，N が群 G の正規部分群のとき G/N 上の well-defined な演算

$$G/N \times G/N \to G/H,\ (xN, yN) \mapsto (xN)(yN) := xyN$$

が定まる．

定理 4.2.6. *G を群，N を G の正規部分群とする．このとき，G/N は上記の演算により群となる．*

証明. 上で定義した演算 $(xN)(yN) := xyN$ が定義 3.1.2 の (i)(ii)(iii) を満たすことを確かめる．

(i)（結合法則）

任意の $xN, yN, zN \in G/N$ に対して，

$$((xN)(yN))(zN) = (xyN)(zN) = (xy)zN = x(yz)N = (xN)(yzN) = (xN)((yN)(zN))$$

が成り立つ．

(ii)（単位元の存在）

任意の $xN \in G/N$ に対して，

$$(1_GN)(xN) = (1_Gx)N = xN$$
$$(xN)(1_GN) = (x1_G)N = xN$$

が成り立つので，1_GN が G/N の単位元となる．

(c)（逆元の存在）

任意の $xN \in G/N$ に対して，

$$(x^{-1}N)(xN) = (x^{-1}x)N = 1_GN$$
$$(xN)(x^{-1}N) = (xx^{-1})N = 1_GN$$

となるので，$x^{-1}N$ が xN の逆元である． ■

定義 4.2.7. 定理 4.2.6 で得られた群 G/N を G の N による**剰余群**または**商群**という．

注意. 定理 4.2.6 の証明より，

- G/N の単位元は $1_{G/N} = 1_GN$ $(= N)$
- $xN \in G/N$ の逆元は $(xN)^{-1} = x^{-1}N$

命題 4.2.8. *G を群，N を G の正規部分群とする．このとき，自然な写像*

$$\pi : G \to G/N,\ x \mapsto xN$$

は全射準同型写像で $\mathrm{Ker}\ \pi = N$ となる．

証明. 任意の $x, y \in G$ に対して $\pi(xy) = xyN = (xN)(yN) = \pi(x)\pi(y)$ となるので，π は準同型写像である．
全射であることは任意の $xN \in G/N$ が $\pi(x) = xN$ と書けることから分かる．一方で，$x \in G$ に対して

$$\begin{aligned} x \in \mathrm{Ker}\,\pi &\iff xN = \pi(x) = N \\ &\iff x \in N \quad (\text{命題 4.1.3 より}) \end{aligned}$$

となるので $\mathrm{Ker}\ \pi = N$．■

演習問題

問題 4.2.1. 群 G と G の部分群 N に対して，以下の条件が全て互いに同値であることを確かめよ．

(1) H が G の正規部分群
(2) 任意の $x \in G$ に対して，$xNx^{-1} = N$
(3) 任意の $x \in G$ に対して，$xNx^{-1} \subseteq N$
(4) 任意の $x \in G$ に対して，$xNx^{-1} \supseteq N$
(5) 任意の $x \in G$ に対して，$xN = Nx$
(6) 任意の $x \in G$ に対して，$xN \subseteq Nx$
(7) 任意の $x \in G$ に対して，$xN \supseteq Nx$

問題 4.2.2. 二面体群 $D_4 = \{E_2, R, R^2, R^3, T, TR, TR^2, TR^3\}$ を考える

(1) D_4 の以下の部分群が正規部分群であることを確かめよ．
  (i) $\{E_2, R^2\}$
  (ii) $\{E_2, R, R^2, R^3\}$
  (iii) $\{E_2, R^2, T, TR^2\}$
  (iv) $\{E_2, R^2, TR, TR^3\}$
(2) D_4 の以下の部分群が正規部分群でないことを確かめよ．
  (i) $\{E_2, T\}$
  (ii) $\{E_2, TR\}$
  (iii) $\{E_2, TR^2\}$
  (iv) $\{E_2, TR^3\}$

ちなみに，D_4 の部分群は上記 8 個と自明な部分群 $\{E_2\}, D_4$ の 10 個しかないので（これまでの講義で学んだ内容で示すことができるので，興味があれば各自確かめよ），D_4 の全ての部分群に対して正規部分群であるかそうでないかが分かったことになる．

問題 4.2.3. 以下の群 G の部分群 H が正規部分群かどうか答えよ．

(1) $G = \mathrm{GL}_2(\mathbb{R})$, $H = \{aE_2 \mid a \in \mathbb{R} \setminus \{0\}\}$
(2) $G = \mathrm{GL}_2(\mathbb{R})$, $H = \mathrm{O}(2)$
(3) $G = S_3$, $H = \langle (1\ 2) \rangle = \{1_3, (1\ 2)\}$
(4) $G = S_3$, $H = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\rangle = \left\{ 1_3, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 21 \end{pmatrix} \right\}$

問題 4.2.4. G を群とする．G の中心

$$Z(G) := \{x \in G \mid \forall y \in G,\ xy = yx\}$$

が G の正規部分群であることを示せ．

問題 4.2.5. G を群，H, K を G の部分群とする．このとき，以下の主張を証明せよ

(1) H と K が G の正規部分群のとき，$H \cap K$ は G の正規部分群である．

(2) H が G の部分群で K が G の部分群のとき，HK は G の部分群である．

(3) H と K が G の部分群のとき，HK は G の正規部分群である．

問題 4.2.6. $f : G \to H$ を群の準同型写像，K, L をそれぞれ G, H の部分群とする．

(1) K の f による像 $f(K) := \{f(x) \mid x \in K\}$ が H の部分群であることを示せ．
(2) L の f による逆像 $f^{-1}(L) := \{x \in G \mid f(x) \in L\}$ が G の部分群であることを示せ．
(3) L が H の正規部分群であるとき，$f^{-1}(L)$ が G の正規部分群となることを示せ．
(4) f が全射で K が G の正規部分群のとき，$f(K)$ は H の正規部分群であることを示せ．

問題 4.2.7. $\mathsf{GL}_2(\mathbb{C})$ の部分群

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| a, b, d \in \mathbb{C}, a, d \neq 0 \right\}, N = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| a, b \in \mathbb{C}, a \neq 0 \right\}$$

を考える（部分群になることをは各自チェックせよ）．

(1) N が G の正規部分群であることを示せ．

(2) $A = \begin{pmatrix} -2 & 1 \\ 0 & 2 \end{pmatrix} \in G$ について，$AN \in G/N$ の位数を求めよ．

(3) $A = \begin{pmatrix} -2i & 1 \\ 0 & -2 \end{pmatrix} \in G$ について，$AN \in G/N$ の位数を求めよ．

(4) $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G$ に対して，$\mathsf{ord}(AN) < \infty$ となるための必要十分条件を求めよ．

4.3　準同型定理

準同型定理は群の間の同型を作り出す重要な定理であり，群以外にも環や加群（代数基礎 2，代数学 1 で扱う）に対しても成り立つなど，群論というよりは代数学における中心的な定理である．

準同型写像 $f : G \to H$ に対して，何らかの同型写像を作りたい．命題 3.6.10 より全単射な準同型写像を見つければ良いことになるが，f の値域を $\mathrm{Im}\, f$ に制限すれば全射準同型写像 $f : G \to \mathrm{Im}\, f$ を得る．一方で，単射を作るためには命題 3.6.9 により核が自明な部分群になるようにすれば良い．もちろん f の核 $\mathrm{Ker}\, f$ は一般には自明な部分群ではない（単位元以外の元を含む）が，G の $\mathrm{Ker}\, f$ による商群 $G/\mathrm{Ker}\, f$ を考えれば，この群の中で f の核 $\mathrm{Ker}\, f$ の任意の元 x は単位元となる：$x\,\mathrm{Ker}\, f = \mathrm{Ker}\, f = 1_{G/\mathrm{Ker}\, f}$．

従って，直感的には $f : G \to H$ の値域を $\mathrm{Im}\, f$ に，定義域を $G/\mathrm{Ker}\, f$ に置き換えれば全単射な準同型写像，つまり，同型写像が得られる．これを正当化するのが準同型定理である．

以下の定理は準同型写像を証明するための重要なステップである．

定理 4.3.1.　$f : G \to H$ を準同型写像，N を G の正規部分群とする．さらに，$f(N) = \{1_H\}$（$\Longleftrightarrow$ 任意の $x \in N$ に対して $f(x) = 1_H \Longleftrightarrow N \subseteq \mathrm{Ker}\, f$）が成り立つとする．このとき，well-defined な準同型写像

$$\overline{f} : G/N \to H,\ xN \mapsto f(x)$$

が定まり，$\overline{f} \circ \pi = f$ が成り立つ．

証明.　well-defined であること：

$xN = yN$ のときに $f(x) = f(y)$ を示せば良い．$xN = yN$ のとき $y^{-1}x \in N$ であるが，仮定より $f(y^{-1}x) = 1_H$ となる．f が準同型写像なので $f(y)^{-1}f(x) = f(y^{-1}x) = 1_H$ となり，$f(x) = f(y)$ が示された．

準同型写像であること：

任意の $xN, yN \in G/N$ に対して

$$\overline{f}((xN)(yN)) = \overline{f}(xyN) = f(xy) = f(x)f(y) = \overline{f}(xN)\overline{f}(yN)$$

が成り立つので $\overline{f}$ は準同型写像である．

$\overline{f} \circ \pi = f$：

任意の $x \in G$ に対して

$$(\overline{f} \circ \pi)(x) = \overline{f}(\pi(x)) = \overline{f}(xN) = f(x)$$

となるので，$\overline{f} \circ \pi = f$．　■

定理 4.3.2 (準同型定理（第一同型定理）)．　$f : G \to H$ を準同型写像とする．このとき，well-defined な同型写像

$$\overline{f} : G/\mathrm{Ker}\, f \xrightarrow{\cong} \mathrm{Im}\, f,\ xN \mapsto f(x)$$

が定まる．

証明.　定理 4.3.1 を写像 $f : G \to \mathrm{Im}\, f,\ x \mapsto f(x)$ と $N = \mathrm{Ker}\, f$ に適用すると，well-defined な準同型写像 $\overline{f} : G/\mathrm{Ker}\, f \to \mathrm{Im}\, f,\ x\,\mathrm{Ker}\, f \mapsto f(x)$ が定まる．命題 3.6.10 より $\mathrm{Ker}\, \overline{f} = \{1_{G/\mathrm{Ker}\, f}\}$ かつ $\overline{f}$ が全射であることを示せば良い．

$\overline{f}$ が全射であること：

任意の $\mathrm{Im}\, f$ の元は $f(x)$ $(x \in G)$ の形をしているが，$\overline{f}$ の定義より $\overline{f}(x\,\mathrm{Ker}\, f) = f(x)$．従って，$\overline{f}$ は全射．

$\mathrm{Ker}\,\overline{f} = \{1_{G/\mathrm{Ker}\,f}\}$ であること：

任意の $x\,\mathrm{Ker}\,f \in \mathrm{Ker}\,\overline{f}$ を考える．このとき $f(x) = \overline{f}(x\,\mathrm{Ker}\,f) = 1_H$ が成り立つので $x \in \mathrm{Ker}\,f$．したがって，$x\,\mathrm{Ker}\,f = \mathrm{Ker}\,f = 1_{G/\mathrm{Ker}\,f}$ となる．よって，$\mathrm{Ker}\,\overline{f} = \{1_{G/\mathrm{Ker}\,f}\}$ が成り立つ．

命題 3.6.10 より $\overline{f}$ は同型写像となることが示された． ■

準同型定理より，任意に与えられた準同型写像 $f : G \to H$ にから同型 $G/\mathrm{Ker}\,f \cong \mathrm{Im}\,f$ を作ることができる．以下の例では様々な準同型写像に対して準同型定理を適用することで群の同型を見つける．

例 4.3.3. (1) 準同型写像 $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R} - \{0\}$ に対して

$$\mathrm{Ker}(\det) = \mathrm{SL}_n(\mathbb{R}), \quad \mathrm{Im}(\det) = \mathbb{R} \setminus \{0\}$$

となるので，準同型定理より同型写像

$$\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \xrightarrow{\cong} \mathbb{R} \setminus \{0\},\ A\mathrm{SL}_n(\mathbb{R}) \mapsto \det(A)$$

を得る．この同型写像の逆写像は例 4.1.4(2) で得られた全単射である．

(2) 準同型写像 $\mathrm{sgn} : S_n \to \mathbb{R} \setminus \{0\}$ に対して

$$\mathrm{Ker}(\mathrm{sgn}) = A_n, \quad \mathrm{Im}(\mathrm{sgn}) = \{1, -1\}$$

となるので，準同型定理より同型写像

$$S_n/A_n \xrightarrow{\cong} \{1, -1\},\ \sigma A_n \mapsto \mathrm{sgn}(\sigma)$$

を得る．この同型写像の逆写像は例 4.1.4(3) で得られた全単射である．

(3) $G = \langle x \rangle$ を巡回群とする．このとき，準同型写像

$$f : \mathbb{Z} \to G,\ k \mapsto x^k$$

が定まる．定義から f は全射（$\mathrm{Im}\,f = G$）である．一方で，x の位数の定義から

$$\mathrm{Ker}\,f = \begin{cases} n\mathbb{Z} & (\mathrm{ord}(x) = n < \infty \text{ のとき}) \\ \{0\} & (\mathrm{ord}(x) = \infty \text{ のとき}) \end{cases}$$

となる．従って，準同型定理より同型写像

$$\begin{cases} \mathbb{Z}/n\mathbb{Z} \xrightarrow{\cong} G,\ k + n\mathbb{Z} \mapsto x^k & (\mathrm{ord}(x) = n < \infty \text{ のとき}) \\ \mathbb{Z} \xrightarrow{\cong} G,\ k \mapsto x^k & (\mathrm{ord}(x) = \infty \text{ のとき}) \end{cases}$$

を得る．この同型写像は例 3.6.3(3) で得られたものと同じである．

(4) 準同型写像

$$f : \mathbb{C} \setminus \{0\} \to \mathbb{C} \setminus \{0\},\ z \mapsto z/|z|$$

を考える．このとき，

$$\mathrm{Ker}\,f = \mathbb{R}_{>0} := \{x \in \mathbb{R} \mid x > 0\}, \quad \mathrm{Im}\,f := \mathbb{T} := \{z \in \mathbb{C} \setminus \{0\} \mid |z| = 1\}$$

である．準同型定理より，同型写像

$$(\mathbb{C} \setminus \{0\})/\mathbb{R}_{>0} \xrightarrow{\cong} \mathbb{T},\ z\mathbb{R}_{>0} \mapsto z/|z|$$

を得る．$(\mathbb{C} \setminus \{0\})/\mathbb{R}_{>0}$ の元 $z\mathbb{R}_{>0}$ は複素平面内の z 方向の半直線であり，対応する元 $z/|z|$ は半直線 $z\mathbb{R}_{>0}$ 方向の長さ 1 の複素数である．

(5) 準同型写像

$$f : \mathbb{R} \mapsto \mathbb{C} \setminus \{0\},\ x \mapsto e^{2\pi x\sqrt{-1}}$$

を考える．このとき，

$$\mathsf{Ker}\, f = \mathbb{Z}, \quad \mathsf{Im}\, f = \mathbb{T}$$

である．準同型定理より同型写像

$$\mathbb{R}/\mathbb{Z} \xrightarrow{\cong} \mathbb{T},\ x\mathbb{Z} \mapsto e^{2\pi xi}$$

を得る．

任意の整数 n と実数 x に対して $(x+n)\mathbb{R} = x\mathbb{R}$ となるので，任意の実数は $\mathbb{R}/\mathbb{Z}$ において閉区間 $[0,1]$ の点と同一視される．さらに，0 と 1 も同様に $\mathbb{R}/\mathbb{Z}$ にいて同一視される．すると上の同型は閉区間 $[0,1]$ の端の点をくっつけて円周にするという操作を表している．

準同型定理の応用

上で紹介した準同型定理は群論において最も重要な定理の一つであるが，他にも同型定理と名付けられた様々な定理がある．どれも準同型定理から従う主張であるが，よく使うので紹介する．

定理 4.3.4 (第二同型定理)．G を群，H を G の部分群，N を G の正規部分群とする．このとき，以下のことが成り立つ：

(1) $HN := \{xy \mid x \in H, y \in N\}$ は G の部分群
(2) $H \cap N$ は H の正規部分群
(3) N は HN の正規部分群
(4) well-defined な同型写像

$$H/H \cap N \xrightarrow{\cong} HN/N,\ x(H \cap N) \mapsto xN$$

が定まる．

証明. (1) 定義 3.3.1 の (i)(ii)(iii) を確かめる．

(i) $1_G = 1_G 1_G \in HN$.

(ii) $x_1y_1, x_2y_2 \in HN$ $(x_1, x_2 \in H, y_1, y_2 \in N)$ を考える．N が G の正規部分群なので，$y' := x_2^{-1}y_1x_2 \in N$ となる．このとき，$y_1x_2 = x_2y'$ なので

$$(x_1y_1)(x_2y_2) = (x_1x_2)(y'y_2) \in HN$$

が成り立つ．

(iii) $xy \in HN$ $(x \in H, y \in N)$ を考える．N が G の正規部分群なので，$y' := xy^{-1}x^{-1} \in N$ となる．このとき，$y^{-1}x^{-1} = x^{-1}y'$ なので

$$(xy)^{-1} = y^{-1}x^{-1} = x^{-1}y' \in HN$$

が成り立つ．

(2) 任意の $x \in H$, $y \in H \cap N$ に対して，N が G の正規部分群なので $xyx^{-1} \in N$ となる．一方で，$x, y \in H$ なので $xyx^{-1} \in H$ となる．これらのことから $xyx^{-1} \in H \cap N$ が成り立つ．したがって，$H \cap N$ は H の正規部分群となる．

(3) は容易に分かる．

(4) 写像 $f : H \to HN/N,\ x \mapsto xN$ は全射準同型写像であり，その核は $H \cap N$ となる．したがって，準同型定理より well-defined な同型写像

$$H/H \cap N \xrightarrow{\cong} HN/N,\ x(H \cap N) \mapsto xN$$

が定まる． ■

例 4.3.5. $0 \neq m, n \in \mathbb{Z}$ とする．

(1) 写像

$$\mathbb{Z} \to m\mathbb{Z}/mn\mathbb{Z},\ x \mapsto mx + mn\mathbb{Z}$$

は全射準同型写像であり，その核は $n\mathbb{Z}$ である．準同型定理より同型写像

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\cong} m\mathbb{Z}/mn\mathbb{Z},\ x + n\mathbb{Z} \mapsto mx + mn\mathbb{Z}$$

を得る（直感的には $m\mathbb{Z}/mn\mathbb{Z}$ を m で約分している）．

(2) $g = \mathsf{gcd}(m, n)$（m と n の最大公約数），$l = \mathsf{lcm}(m, n)$（m と n の最小公倍数）とすると，

$$m\mathbb{Z} + n\mathbb{Z} = g\mathbb{Z} \quad \text{（命題 2.1.6 より分かる）}$$
$$m\mathbb{Z} \cap n\mathbb{Z} = l\mathbb{Z} \quad \text{（容易）}$$

が成り立つ．このとき，第二同型定理（定理 4.3.4）より同型写像

$$m\mathbb{Z}/m\mathbb{Z} \cap n\mathbb{Z} \xrightarrow{\cong} (m\mathbb{Z} + n\mathbb{Z})/n\mathbb{Z}$$

を得る．上の等式と合わせて同型写像

$$m\mathbb{Z}/l\mathbb{Z} \xrightarrow{\cong} g\mathbb{Z}/n\mathbb{Z},\ mx + l\mathbb{Z} \mapsto ma + n\mathbb{Z}$$

を得る．

例 4.3.6. S_4 の部分群

$$N = \{1_4, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$
$$H = \left\langle \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \right\rangle = \left\{ 1_4, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \right\}$$

を考える．例 4.2.3(5) より N は S_4 の正規部分群である．このとき，

- $H \cap N = \{1_4, (1\ 3)(2\ 4)\}$
- $HN = \left\{ 1_4, (1\ 3), (2\ 4), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \right\}$

であり，第二同型定理（定理 4.3.4）より同型写像

$$H/(H \cap N) \cong HN/N$$

を得る．

定理 4.3.7 (第三同型定理)．G を群，N, K を G の正規部分群で $K \subseteq N \subseteq G$ を満たすとする．このとき，以下のことが成り立つ：

(1) N/K は G/K の正規部分群
(2) well-defined な同型写像

$$(G/K)/(N/K) \xrightarrow{\cong} G/N,\ (xK)(N/K) \mapsto xN$$

が定まる

証明. (1) 任意の $xN \in G/K$, $yN \in N/K$ に対して，

$$(xK)(yK)(xK)^{-1} = (xyx^{-1})K$$

であるが，N が G の正規部分群なので $xyx^{-1} \in N$ となるので $(xK)(yK)(xK)^{-1} = (xyx^{-1})K \in N/K$．従って，$N/K$ は G/K の正規部分群である．

(2) 自然な写像 $\pi : G \to G/N,\ x \mapsto xN$ を考える．このとき，$K \subseteq N = \mathrm{Ker}\ \pi$ なので定理 4.3.1 より well-defined な準同型写像 $\overline{\pi} : G/K \to G/N,\ xK \mapsto xN$ が定まる．$\overline{\pi}$ は全射であり，$\mathrm{Ker}\ \overline{\pi} = N/K$ であることを用いると，準同型定理により well-defined な同型写像

$$(G/K)/(N/K) \xrightarrow{\cong} G/N,\ (xK)(N/K) \mapsto xN$$

が定まる． ■

一般に，群 G よりも剰余群 G/N の方が簡単である（例えば，有限群の場合は G/N の位数は G の位数以下である）．次の定理を用いると，G の部分群の情報とより簡単な群である G/N の部分群の情報を結びつけることができる．

定理 4.3.8 (対応定理（第四同型定理）)．G を群，N を G の正規部分群とし，次の集合を考える：

- $\mathcal{X} := \{H \mid H \text{ は } G \text{ の部分群で } N \subseteq H\}$
- $\mathcal{Y} := \{K \mid K \text{ は } G/N \text{ の部分群 }\}$

このとき，互いに逆写像である全単射

$$f : \mathcal{X} \leftrightarrows \mathcal{Y} : g$$

が存在する．ここで，f と g は

$$f(H) := \pi(H) = H/N, \quad g(K) := \pi^{-1}(K) := \{x \in G \mid xH \in K\}$$

で与えられる．

証明. $H \in \mathcal{X}$ に対して $f(H) = H/N \in \mathcal{Y}$ となること：
$H/N \subseteq G/N$ が定義 3.3.1 の (i)(ii)(iii) を満たすことを確かめる．
(i) $1_G \in H$ より $H \in H/N$．
(ii) $xN, yN \in H/N$ $(x, y \in H)$ とすると，$xy \in H$ なので $(xN)(yN) = xyN \in H/N$．
(iii) $xN \in H/N$ $(x \in H)$ とすると，$x^{-1} \in H$ なので $(xN)^{-1} = x^{-1}N \in H/N$．
従って，$H/N \in \mathcal{Y}$ となる．

$K \in \mathcal{Y}$ に対して $g(H) = \pi^{-1}(K) \in \mathcal{X}$ となること：
任意の $x \in N$ に対して $\pi(x) = xN = N = 1_{G/N}$ となるので $x \in \pi^{-1}(K)$．よって，$N \subseteq \pi^{-1}(K)$ が分かる．一方で，$\pi^{-1}(K)$ は G の部分群である（問題 3.6.3）．従って，$\pi^{-1}(K) \in \mathcal{X}$ となる．

任意の $H \in \mathcal{X}$ に対して $g(f(H)) = \pi^{-1}(\pi(H)) = H$ となること：

一般に $H \subseteq \pi^{-1}(\pi(H))$ が成り立つことは容易に分かる．一方で，$x \in \pi^{-1}(\pi(H))$ に対して $\pi(x) \in \pi(H) = H/N$ となるので，ある $y \in H$ が存在して $\pi(x) = \pi(y)$ が成り立つ．このとき命題 4.1.3 より $y^{-1}x \in \mathrm{Ker}\ \pi = N \subseteq H$ となるが，$y, y^{-1}x \in H$ なので $x = y(y^{-1}x) \in H$ となる．従って，逆の包含 $\pi^{-1}(\pi(H)) \subseteq H$ も示された．

任意の $K \in \mathcal{Y}$ に対して $f(g(K)) = \pi(\pi^{-1}(K)) = K$ となること：

これは π が全射であることから分かる．

以上より，f と g が互いに逆な全単射を与えることが示された． ■

例 4.3.9. $n \geq 1$ を整数とする．対応定理（定理 4.3.8）により，集合

- $\mathcal{X} := \{H \mid H \text{ は } \mathbb{Z} \text{ の部分群で } n\mathbb{Z} \subseteq H\}$
- $\mathcal{Y} := \{K \mid K \text{ は } \mathbb{Z}/n\mathbb{Z} \text{ の部分群 }\}$

の間には全単射が存在する．

命題 3.5.9 より $\mathbb{Z}$ の部分群は全て $k\mathbb{Z}$（$k \in \mathbb{N}$）の形をしているが，

$$n\mathbb{Z} \subseteq k\mathbb{Z} \Longleftrightarrow n \in k\mathbb{Z} \Longleftrightarrow k|n$$

が成り立つことが分かる．従って，

$$\mathcal{X} = \{k\mathbb{Z} \mid k \text{ は } n \text{ の約数 }\}$$

となり，

$$\mathcal{Y} = \{k\mathbb{Z}/n\mathbb{Z} \mid k \text{ は } n \text{ の約数 }\}$$

が分かる．

$\mathbb{Z}/n\mathbb{Z}$ の部分群 $k\mathbb{Z}/n\mathbb{Z} \in \mathcal{Y}$ に対して，第三同型定理（定理 4.3.7）により

$$(\mathbb{Z}/n\mathbb{Z})/(k\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/k\mathbb{Z}$$

が成り立つ．

例えば，$n = 6$ のとき $\mathbb{Z}/6\mathbb{Z}$ の部分群は

$$6\mathbb{Z}/6\mathbb{Z} = \{6\mathbb{Z}\},\quad 3\mathbb{Z}/6\mathbb{Z},\quad 2\mathbb{Z}/6\mathbb{Z},\quad \mathbb{Z}/6\mathbb{Z}$$

の 4 個であり，$n = 12$ のとき $\mathbb{Z}/12\mathbb{Z}$ の部分群は

$$12\mathbb{Z}/12\mathbb{Z} = \{12\mathbb{Z}\},\quad 6\mathbb{Z}/12\mathbb{Z},\quad 4\mathbb{Z}/12\mathbb{Z},\quad 3\mathbb{Z}/12\mathbb{Z},\quad 2\mathbb{Z}/12\mathbb{Z},\quad \mathbb{Z}/12\mathbb{Z}$$

の 6 個である．

演習問題

問題 4.3.1. 以下の準同型写像に準同型定理（定理 4.3.2）を適用することでどのような同型写像が得られるか答えよ．

(1) $f : \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z},\ k + 6\mathbb{Z} \mapsto 2k + 6\mathbb{Z}$

(2) $f : \mathbb{Z}/12\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z},\ k + 12\mathbb{Z} \mapsto 3k + 12\mathbb{Z}$

(3) $f : \mathbb{Z} \to (\mathbb{Z}/7\mathbb{Z})^{\times},\ k \mapsto \overline{3^l}$

(4) $f : \mathbb{R} - \{0\} \to \mathbb{R} - \{0\},\ x \mapsto x/|x|$

(5) $f : \mathbb{R} - \{0\} \to \mathbb{R} - \{0\},\ x \mapsto x^2$

(6) $f : \mathbb{C} - \{0\} \to \mathbb{R} - \{0\},\ z \mapsto |z|$

(7) $G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbb{R}, a, d \neq 0 \right\} \leq \mathsf{GL}_2(\mathbb{R})$ としたとき，

$f : G \to \mathsf{GL}_2(\mathbb{R}),\ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \to \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$

(8) $f : S_4 \mapsto S_3,\ \sigma \mapsto \sigma|_{\{1,2,3\}}$

ここで，$\sigma|_{\{1,2,3\}}$ は $\sigma|_{\{1,2,3\}}(1) = \sigma(1)$, $\sigma|_{\{1,2,3\}}(2) = \sigma(2)$, $\sigma|_{\{1,2,3\}}(3) = \sigma(3)$ なる S_3 の元．

問題 4.3.2. (2) $\mathbb{Z}/18\mathbb{Z}$ の部分群を全て求めよ．

(2) $\mathbb{Z}/24\mathbb{Z}$ の部分群を全て求めよ．

問題 4.3.3. $f : G \to H$ を準同型写像，$|G| = n < \infty$ とする．このとき，$|\mathsf{Ker}\, f||\mathsf{Im}\, f|$ を n を用いて表せ．

問題 4.3.4. G を有限群，H を G の部分群，N を G の正規部分群とする．このとき，等式 $|H||N| = |HN||H \cap N|$ を示せ．

問題 4.3.5. $\mathsf{GL}_2(\mathbb{C})$ の部分群

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| a, b, d \in \mathbb{C}, a, d \neq 0 \right\}, N = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| a, b \in \mathbb{C}, a \neq 0 \right\},$$

を考える（問題 4.2.7 参照）．

(1) G の部分群

$$H = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \middle| a, d \in \mathbb{C} - \{0\} \right\}$$

に対して，$G = HN$ を示せ．

(2) $H \cap N = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \middle| a \in \mathbb{C} - \{0\} \right\}$ を示せ．

(3) $H \to \mathbb{C} - \{0\},\ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mapsto \dfrac{a}{d}$ が群の準同型写像であることを示し，その核を求めよ．

(4) 第二同型定理（定理 4.3.4）を用いて G/N がどのような群と同型となるか答えよ．

問題 4.3.6. G を可換群とし，自然数 $n \geq 1$ を一つ固定する．

(2) G の部分集合

$$G^n := \{x^n \mid x \in G\}, \quad G_n := \{x \in G \mid x^n = 1_G\}$$

が G の部分群であることを示せ．

(3) 同型 $G/G_n \cong G^n$ を示せ．

4.4　直積群

次に，準同型定理を用いて直積群についてもう少し詳しく調べる．

中国式剰余定理

第 2.2 節で述べた中国式剰余定理（定理 2.2.7）は群の言葉を用いると以下のように表現できる：

定理 4.4.1 (中国式剰余定理)．m, n を 0 でない互いに素な整数とする．このとき，well-defined な同型写像

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},\ x + mn\mathbb{Z} \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$$

を得る．

証明．準同型写像

$$f : \mathbb{Z} \mapsto \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},\ x \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$$

を考える．このとき，$\mathrm{Ker}\, f = mn\mathbb{Z}$ かつ f が全射（$\mathrm{Im}\, f = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$）であることが示されれば準同型定理（定理 4.3.2）より主張の同型写像を得る．

$\mathrm{Ker}\, f = mn\mathbb{Z}$ であること：

任意の $x \in \mathbb{Z}$ に対して

$$\begin{aligned} x \in \mathrm{Ker}\, f &\iff (x + m\mathbb{Z}, x + n\mathbb{Z}) = f(x) = (m\mathbb{Z}, n\mathbb{Z}) \\ &\iff x \in m\mathbb{Z} \text{ かつ } x \in n\mathbb{Z} \\ &\iff m|x \text{ かつ } n|x \\ &\iff mn|x \qquad (m \text{ と } n \text{ が互いに素なので}) \\ &\iff x \in mn\mathbb{Z} \end{aligned}$$

が成り立つので，$\mathrm{Ker}\, f = mn\mathbb{Z}$ が示される．

f が全射であること：

任意の $(a + m\mathbb{Z}, b + n\mathbb{Z}) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ を考える．$\gcd(m, n) = 1$ なので定理 2.2.7 より，

$$\begin{cases} x \equiv a \bmod m \\ x \equiv b \bmod n \end{cases}$$

となる整数 x が存在する．このとき，$f(x) = (a + m\mathbb{Z}, b + n\mathbb{Z})$ となるので，f は全射．

f に準同型定理を用いることで同型写像

$$\mathbb{Z}/mn\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},\ x \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$$

を得る． ■

例 4.4.2. (1) $\mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$

(2) $\mathbb{Z}/84\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times 7\mathbb{Z}$

(3) $\mathbb{Z}/4\mathbb{Z} \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

（(∵) $\mathbb{Z}/4\mathbb{Z}$ の元 $1 + 4\mathbb{Z}$ は位数 4 を持つが，$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ の任意の元は位数 2 以下である．）

つまり，定理 4.4.1 において n_1 と n_2 が互いに素であるという仮定は必要である．

直積群の応用

正の整数 n に対して，オイラー関数 $\varphi(n)$ が

$$\varphi(n) = (n \text{ と互いに素な整数 } 1 \leq a \leq n \text{ の個数}) = |(\mathbb{Z}/n\mathbb{Z})^\times|$$

で定義されていた．n が素数の場合は $\varphi(n) = n - 1$ だったが，一般の整数 n に対して $\varphi(n)$ はどのように計算されるだろうか？中国式剰余定理の応用として $\varphi(n)$ の公式を与える．

以下の定理は中国式剰余定理（定理 4.4.1）の乗法群版である：

定理 4.4.3. m, n を 0 でない互いに素な整数とする．このとき，定理 4.4.1 の同型写像は同型写像

$$(\mathbb{Z}/mn\mathbb{Z})^\times \xrightarrow{\cong} (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times,\ x + mn\mathbb{Z} \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$$

に制限される．

証明. 整数 $x \in \mathbb{Z}$ に対して，

$$\mathsf{gcd}(x, mn) = 1 \Longleftrightarrow \mathsf{gcd}(x, m) = \mathsf{gcd}(x, n) = 1$$

が成り立つので，定理 4.4.1 の同型写像は全単射

$$(\mathbb{Z}/mn\mathbb{Z})^\times \xrightarrow{\cong} (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times,\ x + mn\mathbb{Z} \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$$

に制限される． また，この写像が積を保つことが容易に分かるので，これは乗法群の同型写像である． ■

整数の素因数分解を考えることで，以下のオイラー関数の式から一般の公式を導く事ができる：

補題 4.4.4. (1) p を素数，k を正の整数とすると，

$$\varphi(p^k) = p^k - p^{k-1}.$$

(2) m, n を互いに素な正の整数とすると，

$$\varphi(mn) = \varphi(m)\varphi(n).$$

証明. (1) $1 \sim p^k$ の中で p^k と互いに素でない（つまり p の倍数）のは

$$jp \quad (1 \leq j \leq p^{k-1})$$

の p^{k-1} 個．従って，$1 \sim p^k$ の中で p^k と互いに素なものは $p^k - p^{k-1}$ 個となり，$\varphi(p^k) = p^k - p^{k-1}$．

(2) 定理 4.4.3 より，

$$\varphi(mn) = |(\mathbb{Z}/mn\mathbb{Z})^\times| = |(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times| = |(\mathbb{Z}/m\mathbb{Z})^\times||(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(m)\varphi(n)$$

■

定理 4.4.5. 正の整数 n が $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ と素因数分解されるとき，

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

証明. 補題 4.4.4 より，

$$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{k_i}) = \prod_{i=1}^{r} (p_i^{k_i} - p_i^{k_i - 1}) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

■

例 4.4.6. $20916 = 2^2 \cdot 3^3 \cdot 11 \cdot 17$ より

$$\varphi(20916) = 20916\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{11}\right)\left(1-\frac{1}{17}\right) = 5760$$

結果だけ述べるに留めるが，オイラー関数 $\varphi(n)$ は正多角形の作図問題に応用される（証明は代数学 2 で学ぶガロア理論を用いる）．

定理 4.4.7. （ガウス）正の整数 n に対して，

$$\text{正 } n \text{ 角形が定規とコンパスを使って作図できる} \iff \varphi(n) \text{ が 2 のべき}$$

n を $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$ $(p_1 = 2)$ と素因数分解したとき，定理 4.4.5 より

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right) = p_1^{k_1-1}p_2^{k_2-1}\cdots p_r^{k_r-1}(p_1-1)(p_2-1)\cdots(p_r-1)$$

となる．これが 2 のべきになるためには，

$$k_i = 1 \text{ かつ } p_i = 2^{l_i}+1 \quad (i = 2, 3, \ldots, r)$$

が必要十分である．2^l+1 の形の素数は**フェルマー素数**と呼ばれる[*1]．従って，ガウスの定理は以下のように言い換えることができる：

$$\begin{aligned}&\text{正 } n \text{ 角形が定規とコンパスを使って作図できる}\\ &\iff n = 2^k p_2\cdots p_r \quad (k \geq 0,\ p_i \text{ は相異なるフェルマー素数})\end{aligned}$$

$n = 17$ の場合がガウスが 19 歳のときに発見した事実である．

内部直積

次に，群 G と部分群 G_1, G_2 に対して，G がいつ直積群 $G_1 \times G_2$ と同型となるか考える．
まずは $G = G_1 \times G_2$ のときにどのようなことが成り立つか考える．写像

$$\begin{aligned}i_1 &: G_1 \to G_1 \times G_2,\ x_1 \mapsto (x_1, 1_{G_2})\\ i_2 &: G_2 \to G_1 \times G_2,\ x_2 \mapsto (1_{G_1}, x_2)\end{aligned}$$

は単射準同型写像である．従って，同型写像

$$\begin{aligned}i_1 &: G_1 \xrightarrow{\cong} \mathsf{Im}(i_1) := \{(x_1, 1_{G_2}) \mid x_1 \in G_1\}\\ i_2 &: G_2 \xrightarrow{\cong} \mathsf{Im}(i_2) := \{(1_{G_1}, x_2) \mid x_2 \in G_2\}\end{aligned}$$

を得る．G_1 と G_2 をそれぞれ $\mathsf{Im}(i_1)$ と $\mathsf{Im}(i_2)$ と同一視することで $G_1 \times G_2$ の部分群とみなす．

命題 4.4.8. 群 G_1,G_2 に対して以下が成り立つ．

(1) $G_1, G_2 \triangleleft G_1 \times G_2$
(2) $G_1 \cap G_2 = \{1_{G_1 \times G_2}\}$
(3) $G_1 \times G_2 = G_1G_2$

[*1] フェルマー素数は $3, 5, 17, 257, 65537$ しか見つかっていない

証明. G_1, G_2 の元 x_1, x_2 はそれぞれ $G_1 \times G_2$ の元

$$(x_1, 1_{G_2}), (1_{G_1}, x_2)$$

と同一視することで G_1, G_2 を $G_1 \times G_2$ とみなしていたことに注意しておく．

(1) $G_1 \triangleleft G_1 \times G_2$ のみ示す（$G_2 \triangleleft G_1 \times G_2$ も同様）．

任意の $(x_1, 1_{G_2}) \in G_1$ と $(y_1, y_2) \in G_1 \times G_2$ に対して，

$$\begin{aligned}(y_1, y_2)^{-1}(x_1, 1_{G_2})(y_1, y_2) &= (y_1^{-1}, y_2^{-1})(x_1, 1_{G_2})(y_1, y_2)\\ &= (y_1^{-1}x_1y_1, y_2^{-1}y_2)\\ &= (y_1^{-1}x_1y_1, 1_{G_2}) \in G_1\end{aligned}$$

より G_1 は $G_1 \times G_2$ の正規部分群である．

(2) $(x_1, x_2) \in G_1 \cap G_2$ とすると，$(x_1, x_2) \in G_1$ より $x_2 = 1_{G_2}$ であり，$(x_1, x_2) \in G_2$ より $x_1 = 1_{G_1}$ となる．従って，$G_1 \cap G_2 = \{1_{G_1 \times G_2}\}$ が成り立つ．

(3) 任意の $(x_1, x_2) \in G_1 \times G_2$ に対して

$$(x_1, x_2) = (x_1, 1_{G_2})(1_{G_1}, x_2) \in G_1G_2$$

となる．従って，$G_1 \times G_2 = G_1G_2$ が成り立つ． ■

実は群 G の部分群 G_1, G_2 が命題 4.4.8 の 3 条件を満たせば G は $G_1 \times G_2$ と同型となる．

定理 4.4.9. *G を群とする．G の部分群 G_1, G_2 が以下の条件を満たすとする：*

(1) $G_1, G_2 \triangleleft G$
(2) $G_1 \cap G_2 = \{1_G\}$
(3) $G = G_1G_2$

このとき，同型写像

$$G_1 \times G_2 \xrightarrow{\cong} G,\ (x_1, x_2) \mapsto x_1x_2$$

が存在する．

証明. (i) 任意の $x \in G_1$, $y \in G_2$ に対して，$xy = yx$：

G_1 が G の正規部分群なので $yxy^{-1} \in G_1$ であり，$x \in G_1$ と合わせて $xyxy^{-1} = x(yxy^{-1}) \in G_1$ である．また，G_2 が G の正規部分群なので $xyx^{-1} \in G_2$ であり，$y \in G_2$ と合わせて $xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} \in G_2$ である．

以上より $xyx^{-1}y^{-1} \in G_1 \cap G_2$ となるが，(2) より $xyx^{-1}y^{-1} = 1_G$ が分かる．従って，$xy = yx$ が成り立つ．

(ii) $f : G_1 \times G_2 \to G,\ (x_1, x_2) \mapsto x_1x_2$ は準同型写像：

$(x_1, x_2), (y_1, y_2) \in G_1 \times G_2$ に対して，

$$\begin{aligned}f((x_1, x_2)(y_1, y_2)) &= f((x_1y_1, x_2y_2))\\ &= x_1y_1x_2y_2\\ &= x_1x_2y_1y_2 \quad ((\text{i}) \text{ より } y_1x_2 = x_2y_1)\\ &= f((x_1, x_2))f((y_1, y_2))\end{aligned}$$

が成り立つので f は準同型写像．

(iii) $f : G_1 \times G_2 \to G,\ (x_1, x_2) \mapsto x_1x_2$ は全単射：

(3) より f は全射．従って，命題 3.6.10 により，$\mathrm{Ker}\, f = \{1_{G_1 \times G_2}\}$ を示せば十分である．任意の $(x_1, x_2) \in \mathrm{Ker}\, f$ を考える．このとき，$x_1x_2 = f((x_1, x_2)) = 1_G$ であるが，このことから $x_1 = x_2^{-1}$ となる．すると，$x_1 \in G_1$,

$x_2^{-1} \in G_2$ より $x_1 = x_2^{-1} \in G_1 \cap G_2$ となり，(2) から $x_1 = x_2^{-1} = 1_G$ が従う．よって，$(x_1, x_2) = 1_{G_1 \times G_2}$ が示された．以上より $\mathrm{Ker}\, f = \{1_{G_1 \times G_2}\}$ となったので，f は同型写像である． ■

例 4.4.10. S_5 の部分群

$$G := \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & c & d & e \end{pmatrix} \middle| \, a, b \text{ は } 1, 2 \text{ の並べ替え}，c, d, e \text{ は } 3, 4, 5 \text{ の並べ替え} \right\}$$

$$G_1 := \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ a & b & 3 & 4 & 5 \end{pmatrix} \middle| \, a, b \text{ は } 1, 2 \text{ の並べ替え} \right\}$$

$$G_2 := \left\{ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & c & d & e \end{pmatrix} \middle| \, c, d, e \text{ は } 3, 4, 5 \text{ の並べ替え} \right\}$$

を考える．このとき，G_1, G_2 は定理 4.4.9 の条件 (1)(2)(3) を満たし，同型写像

$$f : G_1 \times G_2 \xrightarrow{\cong} G,\ (\sigma, \tau) \mapsto \sigma\tau$$

を得る．

有限生成アーベル群の構造定理

最後に，有限生成アーベル群の構造に関する定理を紹介する．

定理 4.4.11. G を有限生成アーベル群とする．このとき，ある整数 $r \geq 0$, $e_1, e_2, \ldots, e_t \geq 1$, 素数 $p_1, p_2, \ldots, p_t$ と同型

$$G \cong \mathbb{Z}^r \times \mathbb{Z}/p_1^{e_1}\mathbb{Z} \times \mathbb{Z}/p_2^{e_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_t^{e_t}\mathbb{Z}$$

が存在する（$p_1, p_2, \ldots, p_t$ には同じものが現れても良い）．

（証明のスケッチ）．G の生成系を $S = \{x_1, x_2, \ldots, x_n\}$ とする：$G = \langle x_1, x_2, \ldots, x_n \rangle$．このとき，$G$ がアーベル群（可換群）なので，例 3.4.3(3) より

$$G = \{x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} \mid k_1, k_2, \ldots, k_n \in \mathbb{Z}\}$$

と表せる．そこで，全射準同型写像

$$f : \mathbb{Z}^n \to G,\ (k_1, k_2, \ldots, k_n) \mapsto x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$$

を考える．

Step 1：

ある整数を成分に持つ $n \times m$ 行列 A が存在して，

$$\mathrm{Ker}\, f = \mathrm{Im}\ A := \{A\boldsymbol{x} \mid \boldsymbol{x} \in \mathbb{Z}^m\}$$

が成り立つ．

Step 1 により，f に準同型定理を用いることで同型

$$\mathbb{Z}^n / \mathrm{Im}\ A = \mathbb{Z}^n / \mathrm{Ker}\, f \cong G$$

を得る．従って，$\mathbb{Z}^n / \mathrm{Im}\ A$ が定理の主張の右辺の形の群と同型になることを示せば良い．

Step 2（ここが証明で本質的な部分（単因子論））:

行列 A を基本変形することでブロック行列

$$B = \begin{pmatrix} B_{11} & \boldsymbol{O} \\ \boldsymbol{O} & \boldsymbol{O} \end{pmatrix}$$

の形にできる．ここで，

$$B_{11} = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_t \end{pmatrix} \quad (d_1, d_2, \ldots, d_t \in \mathbb{N} - \{0\},\ d_i | d_{i+1})$$

ただし，許される基本変形は「行（または列）の入れ替え」,「行（または列）を ± 1 倍する」,「ある行（または列）の整数倍を別の行（または列）に加える」の 3 種類.

Step 3 :

上の基本変形に対応する正則行列 P, Q をとる．つまり，$PAQ = B$ を満たすとする．このとき，同型写像

$$\mathbb{Z}^n / \mathsf{Im}\ A \xrightarrow{\cong} \mathbb{Z}^n / \mathsf{Im}\ B,\ \boldsymbol{x} + \mathsf{Im}\ A \mapsto P\boldsymbol{x} + \mathsf{Im}\ B$$

が存在する.

Step 3 より，$\mathbb{Z}^n / \mathsf{Im}\ B$ が定理の主張の右辺の形の群と同型であることを示せば良い．Step 2 を用いると

$$\mathsf{Im}\ B = d_1\mathbb{Z} \oplus d_2\mathbb{Z} \oplus \cdots \oplus d_t\mathbb{Z} \oplus \{0\}^{n-t} \subseteq \mathbb{Z}^n$$

と表せるので，$\mathbb{Z}^n / \mathsf{Im}\ B$ は成分ごとの剰余群を考えることで

$$\mathbb{Z}^n / \mathsf{Im}\ B \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_t\mathbb{Z} \oplus \mathbb{Z}^{n-t} \qquad (*)$$

となる.

最後に，0 でない自然数 d の素因数分解 $d = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$ を考えたとき，中国式剰余定理を用いることで同型

$$\mathbb{Z}/d\mathbb{Z} \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{k_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_l^{k_l}\mathbb{Z}$$

を得る．$(*)$ に現れる各 $\mathbb{Z}/d_i\mathbb{Z}$ をこの様に表すことで $G \cong \mathbb{Z}^n / \mathsf{Im}\ B$ は定理の主張の右辺の形の群と同型となる． ■

演習問題

問題 4.4.1. 以下の群を $\mathbb{Z}/p^k\mathbb{Z}$（p は素数で $k \geq 1$）の形の群のいくつかの直積で表せ.

(1) $\mathbb{Z}/24\mathbb{Z}$
(2) $\mathbb{Z}/120\mathbb{Z}$
(3) $\mathbb{Z}/220\mathbb{Z}$

問題 4.4.2. 自然数 $n \geq 1$ に対して S_n で n 次対称群を表す．写像

$$f : S_3 \times S_5 \to S_8$$

を以下のように定義する：$\sigma \in S_3$, $\tau \in S_5$ に対して $f(\sigma,\tau) \in S_8$ を

$$f(\sigma,\tau)(i) = \begin{cases} \sigma(i) & (i = 1,2,3) \\ \tau(i-3)+3 & (i = 4,5,6,7,8) \end{cases}$$

で定める．

(1) $f(\sigma,\tau)$ が実際に S_8 の元であること，つまり写像

$$f(\sigma,\tau) : \{1,2,3,4,5,6,7,8\} \to \{1,2,3,4,5,6,7,8\}$$

が全単射であることを示せ．

(2) この写像 $f : S_3 \times S_5 \to S_8$ が準同型写像であることを示せ．

(3) f が単射であることを示せ．

問題 4.4.3. (1) $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ が巡回群であるかどうか答えよ．

(2) $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ が巡回群であるかどうか答えよ．

(3) 正の整数 m, n に対して，$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ が巡回群であるための必要十分条件を答えよ．

第 5 章

群の作用

群 $\mathrm{GL}_n(\mathbb{R})$ の元は $\mathbb{R}^n$ 上の全単射な線形変換を与え，S_n の元は $\{1, 2, \ldots, n\}$ という集合の元の変換（置き換え）を与える．もっと一般に群 G の元が集合 X の元の何らかの変換を与えているときに G が集合 X に作用しているという．この節では群の作用について考える．

5.1　群の作用

群の作用

定義 5.1.1. G を群，X を集合とする．このとき，G の X への**左作用**とは，写像

$$\alpha : G \times X \to X,\ (g, x) \mapsto \alpha(g, x)$$

であって以下の条件を満たすものである（以後，$g \in G$ と $x \in X$ に対して $g \cdot x := \alpha(g, x)$ と表すことにする）：

(i) 任意の $x \in X$ に対して $1_G \cdot x = x$
(ii) 任意の $g, h \in G$ と $x \in X$ に対して $g \cdot (h \cdot x) = (gh) \cdot x$

また，このとき G は X へ**左作用している**という．

名前から推測できるように G の X への右作用も定義されるが，左作用と右作用は本質的に同じものであり，この講義では左作用のみしか扱わないので左作用を単に**作用**と呼ぶことにする．

定理 5.1.2. 群 G が集合 X に作用しているとする．$g \in G$ に対して写像

$$\lambda_g : X \to X,\ x \mapsto g \cdot x$$

を考える．

(1) λ_g は全単射
(2) $\lambda : G \to S(X),\ g \mapsto \lambda_g$ は準同型写像

証明. (1) 最初に任意の $x \in X$ に対して

$$\begin{aligned} g \cdot (g^{-1} \cdot x) &= (gg^{-1}) \cdot x = 1_G \cdot x = x \\ g^{-1} \cdot (g \cdot x) &= (g^{-1}g) \cdot x = 1_G \cdot x = x \end{aligned} \qquad (*)$$

が成り立つことに注意しておく．ここで，一つ目の等号は定義 5.1.1(ii) より，三つ目の等号は定義 5.1.1(i) より従う．

全射性を示す．任意の $x \in X$ に対して，$(*)$ より

$$\lambda_g(g^{-1} \cdot x) = g \cdot (g^{-1} \cdot x) = x$$

が成り立つので，λ_g は全射．

次に単射性を示す．$x, y \in X$ が $\lambda_g(x) = \lambda_g(y)$ を満たすとする．このとき $g \cdot x = g \cdot y$ であるが，$(*)$ より

$$x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot y) = y$$

が成り立つので，λ_g は単射．

(2) $S(X) := \{f : X \to X \mid f \text{ は全単射 }\}$ は写像の合成により群となっていたことに注意しておく（命題 3.2.3）．

$g, g' \in G$ に対して，$\lambda(gg') = \lambda(g) \circ \lambda(g')$，つまり，$\lambda_{gg'} = \lambda_g \circ \lambda_{g'}$ を示す．任意の $x \in X$ に対して

$$\lambda_{gg'}(x) = (gg') \cdot x = g \cdot (g' \cdot x) = \lambda_g(g' \cdot x) = \lambda_g(\lambda_{g'}(x)) = (\lambda_g \circ \lambda_{g'})(x)$$

が成り立つので，$\lambda_{gg'} = \lambda_g \circ \lambda_{g'}$ が示された．ここで，二つ目の等号では定義 5.1.1(ii) を用いている． ■

注意． 定理 5.1.2 とは逆に，群 G，集合 X および準同型写像 $\lambda : G \to S(X)$ を考えたとき，写像

$$G \times X \to X,\ (g, x) \mapsto \lambda(g)(x)$$

は G の X への作用を与える（問題 5.1.2）．
従って，G の X への作用を与えることと準同型写像 $\lambda : G \to S(X)$ を与えることは同値である．

例 5.1.3. (1) X を集合とする．このとき，群 $S(X)$ は X に写像

$$\alpha : S(X) \times X \mapsto X,\ (f, x) \mapsto f \cdot x := f(x)$$

により作用する．

実際，以下の様に定義 5.1.1 の条件 (i)(ii) が成り立つ．

(i) 任意の $x \in X$ に対して $\mathsf{id}_X \cdot x = \mathsf{id}_X(x) = x$

(ii) 任意の $f, g \in S(X)$ および $x \in X$ に対して

$$f \cdot (g \cdot x) = f \cdot g(x) = f(g(x)) = (f \circ g)(x) = (f \circ g) \cdot x$$

この作用について，定理 5.1.2 により得られる準同型写像

$$\lambda : S(X) \to S(X)$$

は恒等写像である．

特に，$X = \{1, 2, \ldots, n\}$ を考えれば，S_n が $\{1, 2, \ldots, n\}$ に

$$\alpha : S_n \times \{1, 2, \ldots, n\} \mapsto \{1, 2, \ldots, n\},\ (\sigma, i) \mapsto \sigma \cdot i := \sigma(i)$$

で作用する．

(2) 群 $\mathsf{GL}_n(\mathbb{R})$ は集合 $\mathbb{R}^n$ に写像

$$\alpha : \mathsf{GL}_n(\mathbb{R}) \times \mathbb{R}^n \to \mathbb{R}^n,\ (A, \boldsymbol{x}) \mapsto A \cdot \boldsymbol{x} := A\boldsymbol{x}$$

により作用する．

実際，以下の様に定義 5.1.1 の条件 (i)(ii) が成り立つ．

(i) 任意の $\boldsymbol{x} \in \mathbb{R}^n$ に対して $E_n \cdot \boldsymbol{x} = E_n\boldsymbol{x} = \boldsymbol{x}$

(ii) 任意の $A, B \in \mathsf{GL}_n(\mathbb{R})$ および $\boldsymbol{x} \in \mathbb{R}^n$ に対して

$$A \cdot (B \cdot \boldsymbol{x}) = A \cdot B\boldsymbol{x} = A(B\boldsymbol{x}) = (AB)\boldsymbol{x} = (AB) \cdot \boldsymbol{x}$$

この作用について，定理 5.1.2 により得られる準同型写像

$$\lambda : \mathsf{GL}_n(\mathbb{R}) \to S(\mathbb{R}^n)$$

は単射準同型写像であり，その像は

$$\mathsf{Im}\ \lambda = \{ f : \mathbb{R}^n \to \mathbb{R}^n \mid f \text{ は全単射な線形変換 } \}$$

である．従って，同型写像

$$\lambda : \mathsf{GL}_n(\mathbb{R}) \xrightarrow{\cong} \mathsf{Im}\ \lambda$$

が存在し，この同型写像で $A \in \mathsf{GL}_n(\mathbb{R})$ と A を表現行列として持つ線型写像 $f : \mathbb{R}^n \to \mathbb{R}^n$ が対応する．

(3) G を群とする．このとき，写像

$$\alpha : G \times G \to G,\ (g, x) \mapsto g \cdot x := gx$$

により G は G 自身に作用する．

実際，以下の様に定義 5.1.1 の条件 (i)(ii) が成り立つ．

(i) 任意の $x \in G$ に対して $1_G \cdot x = 1_G x = x$

(ii) 任意の $g, h \in G$ および $x \in G$ に対して

$$g \cdot (h \cdot x) = g \cdot hx = g(hx) = (gh)x$$

この作用について，定理 5.1.2 により得られる準同型写像は

$$\lambda : G \to S(G),\ g \mapsto \lambda_g$$

である．ここで，λ_g は左から g を掛ける写像：$\lambda_g(x) := gx$.

以下の定理により，全ての群はある集合 X の置換群 $S(X)$ の部分群とみなすことができる．特に，位数が n の有限群 G は対称群 S_n の部分群とみなすことができる．

定理 5.1.4 (ケーリーの定理)．G を群とする．このとき，例 5.1.3(3) の準同型写像 $\lambda : G \to S(G)$ は単射である．従って，G は $S(G)$ の部分群 $\mathsf{Im}\ \lambda$ と同型である．
特に，$|G| = n < \infty$ の場合 G は S_n の部分群と同型である．

証明. $g, g' \in G$ が $\lambda(g) = \lambda(g')$，つまり，$\lambda_g = \lambda_{g'}$ を満たしているとする．このとき，

$$g = g1_G = \lambda_g(1_G) = \lambda_{g'}(1_G) = g'1_G = g'$$

となるので，$\lambda : G \to S(G)$ は単射．

次に，$|G| = n < \infty$ と仮定する．G は n 個の元を持つので，$G = \{g_1, g_2, \ldots, g_n\}$ と書ける．全単射

$$\varphi : \{1, 2, \ldots, n\} \to G,\ i \mapsto g_i$$

を用いて写像

$$\Phi : S(G) \to S_n,\ f \mapsto \varphi^{-1} \circ f \circ \varphi$$

を定義する（$\Phi(f)$ は $\{1,2,\dots,n\} \xrightarrow{\varphi} G \xrightarrow{f} G \xrightarrow{\varphi^{-1}} \{1,2,\dots,n\}$ という合成写像）．この Φ が単射準同型写像であることを示す．

まず単射性を示す．$f, f' \in S(G)$ が $\Phi(f) = \Phi(f')$ を満たすとき $\varphi^{-1} \circ f \circ \varphi = \varphi^{-1} \circ f' \circ \varphi$ が成り立つが，この両辺に左から φ を，右から φ^{-1} を合成することで $f = f'$ が従う．よって，Φ は単射．

次に準同型写像であることを示す．$f, f' \in S(G)$ に対して，

$$\Phi(f' \circ f) = \varphi^{-1} \circ (f' \circ f) \circ \varphi = (\varphi^{-1} \circ f' \circ \varphi) \circ (\varphi^{-1} \circ f \circ \varphi) = \Phi(f') \circ \Phi(f)$$

となるので Φ は準同型写像．

$\lambda : G \to S(G)$ と $\Phi : S(G) \to S_n$ は単射準同型写像なので，これらの合成写像

$$\Psi := \Phi \circ \lambda : G \to S_n$$

も再び単射準同型写像となる．従って，G は S_n の部分群 $\mathsf{Im}\ \Psi$ と同型となる． ■

コメント． G が位数 n の有限群のとき，上の定理より単射準同型写像

$$\Psi : G \to S_n$$

が存在することが分かる．
G の元に $g_1, g_2, \dots, g_n$ と番号を振ったとき，$g_i \in G$ に対応する置換 $\sigma_i := \Psi(g_i) \in S_n$ は

$$\sigma_i(j) = k \Longleftrightarrow g g_j = g_k \quad (1 \le j, k \le n)$$

で与えられる．従って，G は S_n の部分群 $\{\sigma_1, \sigma_2, \dots, \sigma_n\}$ と同型になる．
上の σ_i の定め方から，G の元の番号の振り方を変えると異なる置換が対応する．

例 5.1.5. 二面体群 $D_3 = \{E_2, R, R^2, T, TR, TR^2\}$ を考える（例 3.3.3(6) 参照）．D_3 の元に $g_1 = E_2$, $g_2 = R$, $g_3 = R^2$, $g_4 = T$, $g_5 = TR$, $g_6 = TR^2$ と番号を振る．このとき，G の乗積表を書くと

	g_1	g_2	g_3	g_4	g_5	g_6
g_1	g_1	g_2	g_3	g_4	g_5	g_6
g_2	g_2	g_3	g_1	g_6	g_4	g_5
g_3	g_3	g_1	g_2	g_5	g_6	g_4
g_4	g_4	g_5	g_6	g_1	g_2	g_3
g_5	g_5	g_6	g_4	g_3	g_1	g_2
g_6	g_6	g_4	g_5	g_2	g_3	g_1

となる（上から i 行目，左から j 列目には $g_i g_j$ の結果が書かれている）．
上のコメントより単射準同型 $\Psi : D_3 \to S_6$ が定まるが，$g_i \in D_3$ に対応する置換 $\sigma_i := \Psi(g_i) \in S_6$ は

$$\sigma_i(j) = k \Longleftrightarrow g_i g_j = g_k$$

を満たしている．
上の乗積表の 1 行目をみると，

$$g_1 g_1 = g_1,\ g_1 g_2 = g_2,\ g_1 g_3 = g_3,\ g_1 g_4 = g_4,\ g_1 g_5 = g_5,\ g_1 g_6 = g_6$$

となっているので

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = 1_6$$

となる.
上の乗積表の 2 行目をみると,

$$g_1g_1 = g_2,\ g_1g_2 = g_3,\ g_1g_3 = g_1,\ g_1g_4 = g_6,\ g_1g_5 = g_4,\ g_1g_6 = g_5$$

となっているので

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 4 & 5 \end{pmatrix}$$

となる.
上の乗積表の 3 行目をみると,

$$g_1g_1 = g_3,\ g_1g_2 = g_1,\ g_1g_3 = g_2,\ g_1g_4 = g_5,\ g_1g_5 = g_6,\ g_1g_6 = g_4$$

となっているので

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 6 & 4 \end{pmatrix}$$

となる.
以下同様にして,

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}, \sigma_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 3 & 1 & 2 \end{pmatrix}, \sigma_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 2 & 3 & 1 \end{pmatrix}$$

となる. このようにして, 単射準同型写像

$$\Psi : G \to S_6,\ g_i \mapsto \sigma_i$$

が得られ, G は S_6 の部分群

$$\{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$$

と同型になる.

軌道と安定化群

以下, G を群とし, G が集合 X に作用しているとする.

定義 5.1.6. $x \in X$ とする.

(1) X の部分集合

$$G \cdot x := \{g \cdot x \mid g \in G\}$$

を x の G **軌道**または単に**軌道**という.

(2) G の部分集合

$$G_x := \{g \in G \mid g \cdot x = x\}$$

を x の**安定化群**という.

以下の命題により, 安定化群 G_x が実際に G の部分群となることが分かる.

命題 5.1.7. $x \in X$ とする．このとき，以下のことが成り立つ：

(1) x の安定化群 G_x は G の部分群である．
(2) 全単射

$$G/G_x \xrightarrow{\cong} G \cdot x,\ gG_x \mapsto g \cdot x$$

が存在する．特に，$|G \cdot x| = [G : G_x] = |G|/|G_x|$ が成り立ち，この値は $|G|$ の約数である．

証明. (1) 定義 3.3.1 の条件 (i)(ii)(iii) を確かめる：
(i) 定義 5.1.1 の (i) より $1_G \cdot x = x$ なので，$1_G \in G_x$.
(ii) $g, h \in G_x$ に対して，定義 5.1.1 の (ii) より

$$(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$$

となるので $gh \in G_x$.
(iii) $g \in G_x$ に対して $g \cdot x = x$ より

$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = 1_G \cdot x = x$$

が成り立つので，$g^{-1} \in G_x$．ここで，一つ目の等号は $g \cdot x = x$ を，二つ目の等号は定義 5.1.1 の (ii) を，最後の等号は定義 5.1.1 の (i) を用いている．

以上より，G_x は G の部分群となる．

(2) 最初に写像 $f : G/G_x \to G \cdot x,\ gG_x \mapsto g \cdot x$ が well-defined であること，つまり，

「$gG_x, g'G_x \in G/G_x$ が $gG_x = g'G_x$ を満たすとき $g \cdot x = g' \cdot x$ が成り立つ」

を確かめる．

$gG_x, g'G_x \in G/G_x$ が $gG_x = g'G_x$ を満たすとする．このとき，命題 4.1.3 より $g^{-1}g' \in G_x$ となり，$(g^{-1}g') \cdot x = x$ が成り立つ．左から g を掛けることで

$$g' \cdot x = (g(g^{-1}g')) \cdot x = g \cdot ((g^{-1}g') \cdot x) = g \cdot x$$

となり，f が well-defined であることが示された．ここで，二つ目の等号で作用の定義の (ii) を，最後の等号では $g^{-1}g' \in G_x$ であることを用いている．

次に，f が全射であることを確かめる．これは任意の $g \cdot x \in G \cdot x$ が $g \cdot x = f(gG_x)$ を満たすことから分かる．

最後に，f が単射であることを確かめる．$gG_x, g'G_x \in G/G_x$ が $f(gG_x) = f(g'G_x)$ を満たすとする．このとき，$g \cdot x = g' \cdot x$ なので

$$x = 1_G \cdot x = (g^{-1}g) \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g' \cdot x) = (g^{-1}g') \cdot x$$

となり，$g^{-1}g' \in G_x$．従って，$gG_x = g'G_x$ が示された．

以上より，f は全単射となる．特に，$|G/G_x| = |G \cdot x|$ が成り立つことも分かる． ■

例 5.1.8. (1) 例 5.1.3(1) で考えた S_n の $\{1, 2, \ldots, n\}$ への作用を考える．このとき，$n \in \{1, 2, \ldots, n\}$ の軌道と安定化群を求める．

- 任意の $i \in \{1, 2, \ldots, n\}$ に対して $(i\ n) \cdot n = (i\ n)(n) = i$ となるので，n の軌道は

$$S_n \cdot x = \{\sigma(n) \mid \sigma \in S_n\} = \{1, 2, \ldots, n\}$$

- n の安定化群は
$$(S_n)_n = \{\sigma \in S_n \mid \sigma(n) = n\}$$

$(S_n)_n$ の元は n を動かさずに $1, 2, \ldots, n-1$ を入れ替える置換なので，S_{n-1} の元と同一視できる：

$$S_{n-1} \xrightarrow{\cong} (S_n)_n,\ \begin{pmatrix} 1 & 2 & \cdots & n-1 \\ k_1 & k_2 & \cdots & k_{n-1} \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ k_1 & k_2 & \cdots & k_{n-1} & n \end{pmatrix}$$

この同一視を用いると，命題 5.1.7(2) により全単射

$$S_n/S_{n-1} \xrightarrow{\cong} \{1, 2, \ldots, n\},\ \sigma S_{n-1} \mapsto \sigma(n)$$

を得る．

(2) 例 5.1.3(3) で考えた群 G の自分自身への作用を考える．このとき，$x \in G$ の軌道と安定化群を調べる．

- 任意の $y \in G$ に対して，$(yx^{-1}) \cdot x = (yx^{-1})x = y$ が成り立つので
$$G \cdot x = \{gx \mid g \in G\} = G$$
- $g \in G$ が $gx = x$ を満たすとき，両辺に右から x^{-1} を掛けることで $g = 1_G$ となる．従って，x の安定化群は
$$G_x = \{g \in G \mid gx = x\} = \{1_G\}$$

(3) 実数 θ に対して反時計周りに θ 回転する行列を

$$R_\theta := \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

と置き，回転行列のなす $\mathsf{GL}_2(\mathbb{R})$ の部分群

$$G := \{R_\theta \mid \theta \in \mathbb{R}\}$$

を考える（実は G は特殊直交群 $\mathsf{SO}(2)$ と同じものである）．このとき，例 5.1.3(2) と同様にして G は $\mathbb{R}^2$ に作用する．

この作用について，$\boldsymbol{v} \in \mathbb{R}^2$ の軌道および安定化群は以下の様になる：

$\boldsymbol{v} \neq 0$ のとき，

- $G \cdot \boldsymbol{v} = \{R_\theta \boldsymbol{v} \mid \theta \in \mathbb{R}\}$ = 半径 $|\boldsymbol{v}|$ の円周
- $G_{\boldsymbol{v}} = \{R_\theta \in G \mid R_\theta \boldsymbol{v} = \boldsymbol{v}\} = \{R_{2n\pi} \mid n \in \mathbb{Z}\}$
（$\boldsymbol{v}$ を θ 回転して元に戻るとき θ は 2π の倍数となる）

$\boldsymbol{v} = \boldsymbol{0}$ のとき，

- $G \cdot \boldsymbol{0} = \{R_\theta \boldsymbol{0} \mid \theta \in \mathbb{R}\} = \{\boldsymbol{0}\}$
- $G_{\boldsymbol{0}} = \{R_\theta \in G \mid R_\theta \boldsymbol{0} = \boldsymbol{0}\} = G$

群 G が集合 X に作用しているとき，この作用を用いて X をいくつかの軌道に分解することができる．これを示すために以下の補題を用意する．

補題 5.1.9. (1) X 上の関係
$$x \sim_G y :\Longleftrightarrow \exists g \in G \text{ s.t. } y = g \cdot x$$

は同値関係となる．

(2) (1) の同値関係による $x \in G$ の同値類は

$$[x] := \{y \in X \mid x \sim_G y\} = G \cdot x$$

となる．

証明. (1) 定義 1.2.1(2) の 3 条件を確かめる．

(i)（反射律）

任意の x に対して，定義 5.1.1 の (i) より $1_G \cdot x = x$ となるので，$x \sim_G x$.

(ii)（対称律）

$x, y \in X$ が $x \sim_G y$ を満たしているとする．このとき，ある $g \in G$ が存在して $g \cdot x = x$ となる．両辺に左から g^{-1} を作用させて，

$$x = 1_G \cdot x = (g^{-1}g) \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x$$

が成り立つので，$y \sim_G x$ となる．ここで，一つ目の等号では作用の定義の (i) を，三つ目の等号では作用の定義の (ii) を，最後の等号では $g \cdot x = x$ を用いている．

(iii)（推移律）

$x, y, z \in X$ が $x \sim_G y$, $y \sim_G z$ を満たしているとする．このとき，ある $g, h \in G$ が存在して $g \cdot x = y$, $h \cdot y = z$ が成り立つ．このとき，

$$z = h \cdot y = h \cdot (g \cdot x) = (hg) \cdot x$$

が成り立つので，$x \sim_G z$ となる．ここで，最後の等号では作用の定義の (ii) を用いた．

以上より，$\sim_G$ は同値関係となる．

(2) は軌道 $G \cdot x$ の定義より従う． ■

上記の同値関係による商集合 $X/\sim_G$ の完全代表系を $\{x_i\}_{i \in I} \subseteq X$ とする．このとき，$\{G \cdot x_i \mid i \in I\}$ は集合 X の分割を与える：

$$X = \bigcup_{i \in I} G \cdot x_i \quad (\text{どの二つも交わらない和集合})$$

これを G の X への作用による**軌道分解**という．

さらに，G と X が有限集合のとき，完全代表系を $\{x_1, x_2, \ldots, x_n\}$ と表すと，軌道分解の元の個数を比べて，

$$|X| = \sum_{i=1}^{n} |G \cdot x_i|$$

と表せる．ここで，命題 5.1.7(2) とラグランジュの定理（定理 4.1.8）により $|G \cdot x_i|$ は $|G|$ の約数となる．

例 5.1.10. (1) 例 5.1.3(1) で与えた作用を用いることで，S_4 の部分群

$$G := \{1_4, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$$

は $\{1, 2, 3, 4\}$ に作用する（$\sigma \cdot i = \sigma(i)$）．

このとき，$1, 2, 3, 4$ の軌道をそれぞれ求めると，

- $G \cdot 1 = \{1_4(1), (1\ 2)(1), (3\ 4)(1), (1\ 2)(3\ 4)(1)\} = \{1, 2\}$
- $G \cdot 2 = \{1_4(2), (1\ 2)(2), (3\ 4)(2), (1\ 2)(3\ 4)(2)\} = \{1, 2\}$
- $G \cdot 3 = \{1_4(3), (1\ 2)(3), (3\ 4)(3), (1\ 2)(3\ 4)(3)\} = \{3, 4\}$
- $G \cdot 4 = \{1_4(4), (1\ 2)(4), (3\ 4)(4), (1\ 2)(3\ 4)(4)\} = \{3, 4\}$

となる．従って，$X/\sim_G$ の完全代表系として $\{1,3\}$ を取ることができ，軌道分解

$$\{1,2,3,4\} = \{1,2\} \cup \{3,4\} = (G\cdot 1) \cup (G\cdot 3)$$

を得る．

(2) 例 5.1.8(3) で与えた G の $\mathbb{R}^2$ への作用を考える．このとき，$\{(r,0) \in \mathbb{R}^2 \mid r \geq 0\}$ は $\mathbb{R}^2/\sim$ の完全代表系となる．従って，軌道分解

$$\mathbb{R}^2 = \bigcup_{r\geq 0} G\cdot(r,0) \quad (\text{どの二つも交わらない和集合})$$

を得る．ここで，$G\cdot(r,0)$ を半径 r の円周となるので，上の軌道分解は $\mathbb{R}^2$ を原点を中心とする同心円達に分解している．

演習問題

問題 5.1.1. 以下の群 G，集合 X，写像

$$\alpha : G \times X \to X$$

に対して，α が G の X への作用を与えることを確かめよ．

(1) $G = \mathbb{R}$, $X = \mathbb{C}$,

$$\alpha : \mathbb{R} \times \mathbb{C} \to \mathbb{C},\ (x,z) \mapsto e^{ix}z$$

(2) $G = \mathsf{GL}_2(\mathbb{R})$, $X = \mathrm{M}_2(\mathbb{R})$: 2 次の実正方行列の集合，

$$\mathsf{GL}_2(\mathbb{R}) \times \mathrm{M}_2(\mathbb{R}) \to \mathrm{M}_2(\mathbb{R}),\ (P,A) \mapsto PAP^{-1}$$

(3) $G = \mathsf{SL}_2(\mathbb{R})$, $\mathbb{H} := \{z \in \mathbb{C} \mid z \text{ の虚部が正 }\}$,

$$\mathsf{SL}_2(\mathbb{R}) \times \mathbb{H} \to \mathbb{H},\ \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z\right) \mapsto \frac{az+b}{cz+d}$$

問題 5.1.2. 群 G，集合 X および準同型写像 $\lambda : G \to S(X)$ を考える．このとき，写像

$$G \times X \to X,\ (g,x) \mapsto \lambda(g)(x)$$

が G の X への左作用を与えることを示せ．

問題 5.1.3. 写像

$$\alpha : S_3 \times S_3 \to S_3,\ (\sigma,\tau) \mapsto \sigma\tau\sigma^{-1}$$

を考える．

(1) α が S_3 の S_3 への作用を与えることを確かめよ．

(2) $(1\ 2)$ の安定化群 $(S_3)_{(1\ 2)}$ を求めよ．

(3) $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 1 \end{pmatrix}$ の安定化群 $(S_3)_\sigma$ を求めよ．

問題 5.1.4. S_5 の部分群 G は 例 5.1.3(1) と同様の作用により $\{1,2,3,4,5\}$ に作用する．以下の各 G について，G の $\{1,2,3,4,5\}$ の作用による軌道分解を求めよ．

(1) $G = \left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \right\rangle$

(2) $G = \left\langle \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \right\rangle$

(3) $G = \left\{ 1_5,\ (1\ 2),\ (1\ 2)(4\ 5),\ (1\ 3)(4\ 5),\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix},\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix} \right\}$

(4) $G = A_5$

問題 5.1.5. 群 G が集合 X に作用しているとする.

(1) $g \in G$ に対して，$G \cdot (g \cdot x) = G \cdot x$ が成り立つことを示せ.

(2) $g \in G$ と $x \in X$ に対して，$gG_xg^{-1} = G_{gx}$ が成り立つことを示せ.

5.2　共役作用

線型写像 $f : \mathbb{R}^n \to \mathbb{R}^n$ を考える．$\mathbb{R}^n$ の基底 $\boldsymbol{v}_1, \boldsymbol{v}_2 \ldots, \boldsymbol{v}_n$ に関する表現行列を $A = (a_{ij})$ とする：

$$f(\boldsymbol{v}_j) = a_{1j}\boldsymbol{v}_1 + a_{2j}\boldsymbol{v}_2 + \cdots + a_{nj}\boldsymbol{v}_n.$$

また，$\mathbb{R}^n$ の別の基底 $\boldsymbol{w}_1, \boldsymbol{w}_2 \ldots, \boldsymbol{w}_n$ に関する表現行列を $B = (b_{ij})$ とする：

$$f(\boldsymbol{w}_j) = b_{1j}\boldsymbol{w}_1 + b_{2j}\boldsymbol{w}_2 + \cdots + b_{nj}\boldsymbol{w}_n.$$

さらに，基底 $(\boldsymbol{v}_1, \boldsymbol{v}_2 \ldots, \boldsymbol{v}_n)$ から $(\boldsymbol{w}_1, \boldsymbol{w}_2 \ldots, \boldsymbol{w}_n)$ への変換行列を $P = (p_{ij})$ とする：

$$\boldsymbol{v}_j = p_{1j}\boldsymbol{w}_1 + p_{2j}\boldsymbol{w}_2 + \cdots + p_{nj}\boldsymbol{w}_n.$$

このとき，$B = PAP^{-1}$ が成り立っていた．従って，A で表現される線形写像は $\mathbb{R}^n$ の基底を取り替えることで PAP^{-1} という行列に変換される．このことから，PAP^{-1} という行列は行列 A を視点（基底）を変えて見直したものと思うことができる．この様な操作を一般化したものが**共役作用**である．

この節では群 G を共役作用の基本性質を述べたあと，対称群の場合に詳しく調べる．

群の共役作用

補題 5.2.1. G を群とする．写像

$$G \times G \to G,\ (g, x) \mapsto g \cdot x := gxg^{-1}$$

は G の G 自身への作用を与える．

証明. (1) 定義 5.1.1 の (i)(ii) を確かめる．

(i) 任意の x に対して，

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

となる．

(ii) 任意の $g, h \in G$ と $x \in X$ に対して，

$$g \cdot (h \cdot x) = g \cdot (hxh^{-1}) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = (gh) \cdot x$$

が成り立つ． ■

定義 5.2.2. G を群とする．

(1) 補題 5.2.1 で与えられる G の G 自身への作用を G の**共役作用**という．また，G の共役作用による $x \in G$ の軌道を

$$C(x) := \{gxg^{-1} \mid g \in G\}$$

と書き，x の**共役類**という．

(2) $x, y \in G$ に対して，ある $g \in G$ が存在して $y = gxg^{-1}$ となるとき，x と y は**共役である**という．
命題 1.2.5(3) より「x と y が共役である $\iff C(x) = C(y)$ 」が成り立つ．

コメント. (1) G の共役作用による $x \in G$ の安定化群は

$$G_x = \{g \in G \mid gx = xg\}$$

となる.

(2) 補題 5.1.9(1) により，G 上の関係

$$x \sim y :\Longleftrightarrow \text{「ある } g \in G \text{ が存在して } y = gxg^{-1} \text{ となる}$$

は同値関係となる．従って，以下のことが成り立つ：

(i) 任意の $x \in G$ に対して，x と x は共役である.

(ii) 任意の $x, y \in G$ に対して，x と y が共役ならば，y と x は共役である.

(iii) 任意の $x, y, z \in G$ に対して，x と y が共役かつ y と z が共役ならば，x と z は共役である.

例 5.2.3. (1) $A = \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \in \mathsf{GL}_2(\mathbb{R})$ に対して，$P = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$ と置くと

$$PAP^{-1} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = B$$

が成り立つので，A と B は共役である.

(2) $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ に対して，

$$(1\ 2)\sigma(1\ 2)^{-1} = \tau$$

が成り立つので，σ と τ は共役である.

コメント. $\mathsf{GL}_n(\mathbb{C})$ における共役作用は線形代数において重要な役割を果たす：
任意の n 次複素正方行列 A はある行列 $P \in \mathsf{GL}_n(\mathbb{R})$ を用いて

$$PAP^{-1} = \begin{pmatrix} \lambda_1 & * & 0 & \cdots & 0 \\ 0 & \lambda_2 & * & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & * \\ 0 & 0 & 0 & \cdots & \lambda_n \end{pmatrix}$$

と表すことができる（$*$ の部分には 1 か 0 のいずれかが入る）．この右辺の形の行列を A の**ジョルダン標準形**と呼ぶ.

従って，$A, B \in \mathsf{GL}_n(\mathbb{C})$ に対して，

$$A \text{ と } B \text{ が共役} \Longleftarrow A \text{ と } B \text{ は “同じ”ジョルダン標準形を持つ}$$

となる.

例えば，$n = 2$ の場合のジョルダン標準形は

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}, \quad \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \quad (\lambda_1, \lambda_2, \lambda \in \mathbb{C})$$

の形である．
正方行列は必ずしも対角化可能でないことを考えると，ジョルダン標準形が必ず存在するという事実は特筆すべきことである．

G を有限群とするとき，G の共役作用に関する軌道分解

$$G = \bigcup_{i=1}^{t} C(x_i) \quad (\text{どの二つも交わらない})$$

において両辺の集合の元の個数を考えると

$$|G| = \sum_{i=1}^{t} |C(x_i)|$$

と書くことができる．これを G の**類等式**と呼ぶ．

例 5.2.4. S_3 に対してその類等式を求める．そのために S_3 の元の共役類を全て計算していく．S_3 の共役作用は以下の表（乗積表ではない）にまとめられる：

	1_3	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	σ	τ
1_3	1_3	$(1\ 2)$	$(1\ 3)$	$(2\ 3)$	σ	τ
$(1\ 2)$	1_3	$(1\ 2)$	$(2\ 3)$	$(1\ 3)$	τ	σ
$(1\ 3)$	1_3	$(2\ 3)$	$(1\ 3)$	$(1\ 2)$	τ	σ
$(2\ 3)$	1_3	$(1\ 3)$	$(1\ 2)$	$(2\ 3)$	τ	σ
σ	1_3	$(2\ 3)$	$(1\ 2)$	$(1\ 3)$	σ	τ
τ	1_3	$(1, 3)$	$(2\ 3)$	$(1\ 2)$	σ	τ

ここで，

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

であり，例えば σ 行 $(1\ 3)$ 列の部分には $\sigma \cdot (1\ 3) = \sigma(1\ 2)\sigma^{-1} = (1\ 2)$ が，$(1\ 2)$ 行 τ 列の部分には $(1\ 2) \cdot \tau = (1\ 2)\tau(1\ 2)^{-1} = \sigma$ が書いてある．
このことから，S_3 の共役類は

$$\begin{aligned} C(1_3) &= \{1_3\} \\ C((1\ 2)) &= \{(1\ 2), (1\ 3), (2\ 3)\} \\ C((1\ 3)) &= \{(1\ 2), (1\ 3), (2\ 3)\} \\ C((2\ 3)) &= \{(1\ 2), (1\ 3), (2\ 3)\} \\ C(\sigma) &= \{\sigma, \tau\} \\ C(\tau) &= \{\sigma, \tau\} \end{aligned}$$

となる．従って，S_3 の軌道分解はこれらから異なるものを考えればよいので，

$$S_3 = \{1_3\} \cup \{(1\ 2), (1\ 3), (2\ 3)\} \cup \{\sigma, \tau\}$$

が S_3 の共役作用に関する軌道分解である．このことから，S_3 の類等式は

$$|S_3| = 1 + 3 + 2$$

となる．

コメント． 命題 5.1.7 より $|C(x)| = [G : G_x]$ となるので，ラグランジュの定理（定理 4.1.8）より $|C(x)|$ は $|G|$ の約数である．また，1_G の共役類は $\{1_G\}$ なので類等式には必ず 1 が現れる．この事実は類等式に制約を課している．例えば $|G| = 6$ の場合，その類等式としてあり得るのは

$$\begin{aligned}
|G| &= 1 + 2 + 3 \\
|G| &= 1 + 1 + 1 + 3 \\
|G| &= 1 + 1 + 2 + 2 \\
|G| &= 1 + 1 + 1 + 1 + 2 \\
|G| &= 1 + 1 + 1 + 1 + 1 + 1
\end{aligned}$$

の 5 パターンのみである[a]．
類等式は有限群の構造を理解する上でしばしば重要な役割を果たす．

[a] 実は位数 6 の群は S_3 か $\mathbb{Z}/6\mathbb{Z}$ のいずれかに同型なのでその類等式は $1+2+3$ か $1+1+1+1+1+1$ のいずれか

S_n の共役類

S_n の場合には二つの元が共役かどうかの簡単な判定法がある．以下それを解説する．

定義 5.2.5. $\sigma \in S_n$ が**長さ l の巡回置換**であるとは，ある l 個の相異なる $i_1, i_2, \ldots, i_l \in \{1, 2, \ldots, n\}$ が存在して

- $\sigma(i_1) = i_2,\ \sigma(i_2) = i_3, \cdots, \sigma(i_{l-1}) = i_l,\ \sigma(i_l) = i_1$
- j が $i_1, i_2, \ldots, i_l$ とは異なるとき $\sigma(j) = j$

が成り立つときに言う．このような置換を $(i_1\ i_2\ \cdots\ i_l)$ と表す．また，$i_1, i_2, \ldots, i_l$ をこの巡回置換 $(i_1\ i_2\ \cdots\ i_l)$ の**成分**と呼ぶことにする．
定義より，長さ 2 の巡回置換 $(i\ j)$ は i と j の互換に他ならない．また，長さ 1 の巡回置換 (i) とは恒等置換 1_n のことである．

例 5.2.6. (1) S_4 の巡回置換 $(1\ 4\ 2)$ は

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

である．
(2) S_6 の巡回置換 $(4\ 3\ 6\ 2)$ は

$$(4\ 3\ 6\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 6 & 3 & 5 & 2 \end{pmatrix}$$

である．

命題 5.2.7. 任意の置換 $\sigma \in S_n$ は巡回置換の積として

$$\sigma = \sigma_1\sigma_2\cdots\sigma_t$$

と表せる．ただし，

- σ_k は長さ l_k の巡回置換（長さ 1 の巡回置換の OK）
- $i \neq j$ に対して，σ_i と σ_j の成分には同じ数は現れない
- $l_1 \geq l_2 \geq \cdots \geq l_t$ かつ $l_1 + l_2 + \cdots + l_t = n$

さらに，ベクトル $(l_1, l_2, \ldots, l_t)$ はこの表し方によらない．

このとき，$\sigma = \sigma_1\sigma_2\cdots\sigma_t$ を σ の**サイクル分解**，ベクトル $(l_1, l_2, \ldots, l_t)$ を σ の**型**という．

証明. 以下の操作を繰り返して得られる．

(1) $\sigma(i) \neq i$ となる最小の数 i_1 を考える．
(2) i_1 を i_1 に戻るまで σ で繰り返し送る：

$$i_2 := \sigma(i_1),\ i_3 := \sigma(i_2), \ldots, i_{l_1} := \sigma(i_{l_1-1}),\ \sigma(i_{l_1}) = i_1$$

(3) このとき，

$$\sigma_1 = (i_1\ i_2\ \ldots\ i_{l_1})$$

は長さ l の巡回置換である．
(4) $\sigma' := \sigma_1^{-1}\sigma$ と置くと，

$$\sigma'(i_1) = i_1,\ \sigma'(i_2) = i_2, \cdots, \sigma'(i_l) = i_l,$$

が成り立つ．
(5) $\sigma_1^{-1}\sigma$ に対して (1),(2),(3),(4) を繰り返す．

上の操作 (1)〜(5) を繰り返すと，ある巡回置換 $\sigma_1, \sigma_2, \ldots, \sigma_t$ を用いて

$$\sigma_t^{-1}\cdots\sigma_2^{-1}\sigma_1^{-1}\sigma = 1_n$$

と表せる．従って，

$$\sigma = \sigma_1\sigma_2\cdots\sigma_t$$

となる．あとは $\sigma_1, \sigma_2, \ldots, \sigma_t$ を長さが大きい順になる様に並べ替えれば良い（$i \neq j$ に対して σ_i, σ_j の成分には同じものが現れないので $\sigma_i\sigma_j = \sigma_j\sigma_i$ となり，並び替えても問題ない）． ■

例 5.2.8. (1) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$ を考える．命題 5.2.7 の証明の様にして σ のサイクル分解および型を求める．

- $\sigma(1) = 4 \neq 1$ であり，

$$\sigma(1) = 4,\ \sigma(4) = 5,\ \sigma(5) = 1$$

となるので，

$$\sigma' := (1\ 4\ 5)^{-1}\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}$$

と置く．

- $\sigma'(2) = 3 \neq 2$ であり，

$$\sigma(2) = 3,\ \sigma(3) = 2$$

となるので，

$$(2\ 3)^{-1}\sigma' = 1_5$$

となる．

以上より，$(2\ 3)^{-1}(1\ 4\ 5)^{-1}\sigma = 1_5$ であり，

$$\sigma = (1\ 4\ 5)(2\ 3)$$

と表せる．従って，σ の型は $(3, 2)$ となる．

(2) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 4 & 8 & 2 & 6 & 1 & 3 \end{pmatrix}$ を考える．命題 5.2.7 の証明の様にして σ のサイクル分解および型を求める．

- $\sigma(1) = 5 \neq 1$ であり，

$$\sigma(1) = 5,\ \sigma(5) = 2,\ \sigma(2) = 7,\ \sigma(7) = 1$$

となるので，

$$\sigma' := (1\ 5\ 2\ 7)^{-1}\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 4 & 8 & 5 & 6 & 7 & 3 \end{pmatrix}$$

と置く．

- $\sigma'(3) = 4 \neq 3$ であり，

$$\sigma'(3) = 4,\ \sigma'(4) = 8,\ \sigma'(8) = 3$$

となるので，

$$(3\ 4\ 8)^{-1}\sigma' = 1_5 = (6)$$

となる（巡回置換 (6) は 1_8 だが，命題 5.2.7 の形に合わせるために (6) を用いる）．
以上より，$(3\ 4\ 8)^{-1}(1\ 5\ 2\ 7)^{-1}\sigma = (6)$ であり，

$$\sigma = (1\ 5\ 2\ 7)(3\ 4\ 8)(6)$$

と表せる．従って，σ の型は $(4, 3, 1)$ となる．

以下の命題により，置換の型は共役作用で変わらないことが分かる．

命題 5.2.9. 巡回置換 $(i_1\ i_2 \cdots i_l)$ と $\sigma \in S_n$ に対して

$$\sigma(i_1\ i_2 \cdots i_l)\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2) \cdots \sigma(i_l))$$

となる．特に，$\sigma, \tau \in S_n$ に対して，σ と $\sigma\tau\sigma^{-1}$ の型は等しい．

証明. $j \notin \{\sigma(i_1), \sigma(i_2), \ldots, \sigma(i_l)\}$ のとき，

$$(\sigma(i_1\ i_2 \cdots i_l)\sigma^{-1})(j) = \sigma(i_1\ i_2 \cdots i_l)(\sigma^{-1}(j)) = \sigma(\sigma^{-1}(j)) = j$$

となる．一方で $j=\sigma(i_k)$ のとき

$$\begin{aligned}(\sigma(i_1\ i_2\cdots i_l)\sigma^{-1})(j)&=\sigma((i_1\ i_2\cdots i_l)(i_k))\\&=\begin{cases}\sigma(i_{k+1}) & (k=1,2,\dots,l-1\text{ のとき})\\ \sigma(i_1) & (k=l\text{ のとき})\end{cases}\end{aligned}$$

となる．以上のことから

$$\sigma(i_1\ i_2\cdots i_l)\sigma^{-1}=(\sigma(i_1)\ \sigma(i_2)\cdots\sigma(i_l))$$

が示された．

τ の型を $(l_1,l_2,\dots,l_k)$ とし，$\tau=\tau_1\tau_2\cdots\tau_t$ をサイクル分解とする．上で示したことから $\sigma\tau_k\sigma^{-1}$ は長さ l_k の巡回置換となる．従って，

$$\sigma\tau\sigma^{-1}=\sigma(\tau_1\tau_2\cdots\tau_t)\sigma^{-1}=(\sigma\tau_1\sigma^{-1})(\sigma\tau_2\sigma^{-1})\cdots(\sigma\tau_t\sigma^{-1})$$

は $\sigma\tau\sigma^{-1}$ のサイクル分解を与えるので，$\sigma\tau\sigma^{-1}$ は型 $(l_1,l_2,\dots,l_k)$ を持つことが分かる． ■

この命題を用いて以下の共役の判定法を得る．

定理 5.2.10. $\sigma,\tau\in S_n$ に対して，

$$\sigma\text{ と }\tau\text{ が共役}\iff\sigma\text{ と }\tau\text{ は同じ型を持つ}$$

証明. $(\Longrightarrow)$ は命題 5.2.9 で示されている．

$(\Longleftarrow)$: σ の型が $(l_1,l_2,\dots,l_t)$ のとき，σ が

$$\rho:=(1\ 2\cdots m_1)(m_1+1\ m_1+2\cdots m_2)\cdots(m_{t-1}+1\ m_{t-1}+2\cdots m_t)$$

と共役であることを示せば良い．ここで，$m_1=l_1,m_2=l_1+l_2,\dots,m_t=\sum_{k=1}^{t}l_k$ と置いている．これが示されれば，σ,τ が同じ型 $(l_1,l_2,\dots,l_t)$ を持つとき σ と τ はどちらも ρ と共役となるので，σ と τ は共役となる．

σ がサイクル分解

$$\sigma=(i_{11}\ i_{12}\cdots i_{1m_1})(i_{21}\ i_{22}\cdots i_{2m_2})\cdots(i_{t1}\ i_{t2}\cdots i_{tm_t})$$

を持つとする．このとき，置換 ω を

$$\omega(j)=\begin{cases}i_{1j} & (1\le j\le m_1)\\ i_{2,j-m_1} & (m_1+1\le j\le m_2+1)\\ \quad\vdots & \\ i_{t,j-m_{t-1}} & (m_{t-1}+1\le j\le m_t)\end{cases}$$

で定めると，命題 5.2.9 により

$$\omega\rho\omega^{-1}=\sigma$$

が成り立つので σ と ρ は共役である． ■

例 5.2.11. (1) S_3 の元の型は

$$(1,1,1),\ (2,1),\ (3)$$

のいずれかである．それぞれの型を持つ元は以下の様になる：

- 型 $(1,1,1)$: 1_3
- 型 $(2,1)$: $(1\ 2),(1\ 3),(2\ 3)$
- 型 (3) : $(1\ 2\ 3),(1\ 3\ 2)$

従って，S_3 の共役類は

$$\{1_3\}, \{(1\ 2), (1\ 3), (2\ 3)\}, \{(1\ 2\ 3), (1\ 3\ 2)\}$$

の 3 つで，S_3 の類等式は

$$|S_3| = 1 + 3 + 2$$

である（これは例 5.2.3 で求めたものと一致している）．

(2) S_4 の元の型は

$$(1,1,1,1),\ (2,1,1),\ (2,2),\ (3,1),\ (4)$$

のいずれかである．それぞれの型を持つ元は以下の様になる：

- 型 $(1,1,1,1)$: 1_4
- 型 $(2,1,1)$: $(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)$
- 型 $(3,1)$: $(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)$
- 型 $(2,2)$: $(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$
- 型 (4) : $(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)$

従って，S_4 の共役類は

$$\begin{aligned}
&\{1_4\},\\
&\{(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)\},\\
&\{(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\},\\
&\{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\},\\
&\{(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)\}
\end{aligned}$$

の 4 つで，S_4 の類等式は

$$|S_4| = 1 + 6 + 8 + 3 + 6$$

である．

最後に，S_n の共役類の個数について考察する．定理 5.2.10 により共役類の個数は型の個数と同じなので，型の個数が分かれば良い．S_n の元の型は n の分割と呼ばれるものになっている．

定義 5.2.12. 整数 $n \geq 1$ に対して，1 以上の整数の組 $(l_1, l_2, \ldots, l_t)$ が

- $l_1 \geq l_2 \geq \cdots \geq l_t$
- $l_1 + l_2 + \cdots + l_t = n$

を満たすとき，$(l_1, l_2, \ldots, l_t)$ を n **の分割**という．n の分割の個数を $p(n)$ と書いて，n **の分割数**という．

例 5.2.13. 小さい n についてその分割は以下の様になる：

- 1 の分割は (1) のみ
- 2 の分割は $(2), (1,1)$ の 2 個
- 3 の分割は $(3), (2,1), (1,1,1)$ の 3 個
- 4 の分割は $(4), (3,1), (2,1,1), (2,2)(1,1,1,1)$ の 5 個
- 5 の分割は $(5), (4,1), (3,1,1), (3,2)(2,1,1,1), (2,2,1), (1,1,1,1,1)$ の 7 個

従って，小さな n の分割数は

n	1	2	3	4	5	$\cdots$
$p(n)$	1	2	3	5	7	$\cdots$

定理 5.2.10 により以下のことが分かる．

定理 5.2.14. *S_n の共役類の個数は $p(n)$ である．*

演習問題

問題 5.2.1. (1) D_3 の共役類および類等式を求めよ．

(2) D_4 の共役類および類等式を求めよ．

(3) A_4 の共役類および類等式を求めよ．

問題 5.2.2. 以下の置換のサイクル分解および型を求めよ．

(1) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 3 & 4 & 5 \end{pmatrix}$

(2) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 8 \\ 3 & 8 & 7 & 4 & 5 & 1 & 2 \end{pmatrix}$

(3) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 2 & 8 & 6 & 1 & 10 & 9 & 4 & 7 & 3 \end{pmatrix}$

(4) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 10 & 4 & 2 & 8 & 1 & 5 & 7 & 3 & 9 \end{pmatrix}$

問題 5.2.3. (1) 型 $(3,3)$ を持つ S_6 の元を全て求めよ

(2) 型 $(3,2,1)$ を持つ S_6 の元を全て求めよ

(3) 型 $(4,3)$ を持つ S_7 の元を全て求めよ

(4) 型 $(3,2,2)$ を持つ S_7 の元を全て求めよ

問題 5.2.4. S_6, S_7, S_8 の共役類の個数を求めよ．

問題 5.2.5. G を有限群とする．

(1) $x \in G$ に対して「$|C(x)| = 1 \iff x \in \mathrm{Z}(G)$」を示せ．ここで，$\mathrm{Z}(G)$ は G の中心である（問題 3.3.4 参照）．
従って，G の類等式は $|G| = |\mathrm{Z}(G)| + \sum_{i=1}^{n} |C(x_i)|$ の形である．

(2) G の位数が素数 p のべき p^n $(n \geq 1)$ ならば，G の中心 $\mathrm{Z}(G)$ は単位元以外の元を含むことを示せ．

第 6 章

有限群の分類*

n を自然数とする．n 個の元を持つ集合 $G = \{g_1, g_2, \ldots, g_n\}$ に対して，その上の演算

$$G \times G \to G$$

は，各組 (g_i, g_j) $(i, j = 1, 2, \ldots, n)$ に一つの元 $g_i * g_j \in G$ を指定してあげれば定まるので，高々 n^{n^2} 個である．従って，これらの演算の中で群の定義定義 3.1.2(i)(ii)(iii) を満たすものも高々 n^{n^2} 個しかない．このことから，位数が n の群は同型の差を除くと有限個しか無いことが分かる．そこで，以下の問題を考える：

問題 (位数 n の群の分類)**.** 位数が n の群で，互いに同型でないもののリストを作れ[*1]．

有限群の分類は群論のみならず数学全体，果ては数学以外においても重要なものである．例えば，有限群は数学やそれ以外の分野でも良く現れるが，そのような有限群に対してある性質を示したいとする．このとき，もし上記の様なリストができていれば，あとはそのリストに現れる群に対して虱潰しにその性質を調べるという方法が使える．実際，このような虱潰しによる方法で証明された事実も多い．

この節では，有限群を分類するための重要な道具であるシローの定理を紹介し，それを用いていくつかの具体的な n に対して位数 n を持つ群を実際に分類する．

6.1 シローの定理

この節で述べるシローの定理は有限群のシロー部分群と呼ばれる群に対する定理である．

定義 6.1.1. G を有限群，p を $|G|$ の素因数とし，$|G| = p^r m$（$\gcd(p, m) = 1$）と表す．

(1) 位数が p のベキである G の部分群を G の **p 部分群**と呼ぶ．
(2) 位数 p^r の G の部分群を G の**シロー p 部分群**と呼ぶ[a]．

[a] シロー（Sylow）は人名

群 G の部分集合 X, X' が**共役である**とは，ある $g \in G$ が存在して

$$X' = gXg^{-1} := \{gxg^{-1} \mid x \in X\}$$

が成り立つことを言う．

[*1] 問題を有限単純群という有限群の最小の構成要素のようなものに限ると，その分類は 100 人以上の研究者による成果の下，最終的に 2004 年に完成した．この分類の証明をまとめた本が 2023 年までに 10 分冊出版されていて，最終的には 5000 ページ程になるらしい

定理 6.1.2 (シローの定理)．G を有限群，p を $|G|$ の素因数とし，$|G| = p^r m$（$\gcd(p, m) = 1$）と表す．

(1) G のシロー p 部分群は少なくとも一つ存在する．
(2) G の任意の p 部分群はあるシロー p 部分群に含まれる．
(3) G のシロー p 部分群は全て互いに共役である．
(4) G のシロー p 部分群の個数を n_p とすると，以下が成り立つ：
　(i) $n_p | m$
　(ii) $n_p \equiv 1 \bmod p$

コメント． G のシロー p 部分群 S と $x \in G$ に対して，命題 4.1.5(2) より $|xSx^{-1}| = |S| = p^r$ となるので，xSx^{-1} もシロー p 部分群となる．従って，G のシロー p 部分群の個数が一つのとき，任意の $x \in G$ に対して $xSx^{-1} = S$ が成り立つ．よって，$n_p = 1$ のとき S は G の正規部分群となる．

証明は大変なの（と余り重要でないの）で後回しにして，シローの定理を用いた小さい位数の有限群の分類を次の節で紹介する．

6.2　位数 n を持つ群 G の分類

まずは，位数の素因数分解が単純な場合に有限群の分類をいくつか紹介する．

命題 6.2.1.　位数が素数 p の群は全て $\mathbb{Z}/p\mathbb{Z}$ と同型である．

証明. 位数が素数 p の群は系 4.1.13 より巡回群しか無いので，全て $\mathbb{Z}/p\mathbb{Z}$ と同型である． ■

命題 6.2.2.　p を素数とする．位数が p^2 の群は全て $\mathbb{Z}/p^2\mathbb{Z}$ または $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ と同型である．

証明. 位数が p^2 の群が可換群であることが示されれば，定理 4.4.11 よりそれは $\mathbb{Z}/p^2\mathbb{Z}$ または $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ と同型になる．

以下，位数 p^2 の群 G が可換群であることを示す．G の中心 $\mathrm{Z}(G):=\{x\in G\mid \forall y\in G,\ xy=yx\}$ を考える（問題 4.2.7 よりこれは G の正規部分群である）．問題 5.2.5 より $|\mathrm{Z}(G)|>1$ なので，ラグランジュの定理（定理 4.1.8）より $|G/\mathrm{Z}(G)|$ は $1, p$ のいずれかである．

- $|G/\mathrm{Z}(G)|=1$ のとき，$G=\mathrm{Z}(G)$ となるので G は可換群である．
- $|G/\mathrm{Z}(G)|=p$ のとき，系 4.1.13 より $G/\mathrm{Z}(G)$ は巡回群である．つまり，ある $x\in G$ を用いて

  $$G/\mathrm{Z}(G)=\langle x\mathrm{Z}(G)\rangle=\{x^k\mathrm{Z}(G)\mid k\in\mathbb{Z}\}$$

  と表せる．G の任意の元 y はいずれかの $x^k\mathrm{Z}(G)$ に含まれるので，$y=x^ka$ $(k\in\mathbb{Z}, a\in\mathrm{Z}(G))$ の形で表せる．すると，G の任意の 2 元 $y=x^ka$, $z=x^kb$ $(k,l\in\mathbb{Z}, a,b\in\mathrm{Z}(G))$ に対して

  $$yz=(x^ka)(x^lb)=x^kx^lab=x^lx^kba=(x^lb)(x^ka)=zy$$

  となるので，G は可換群となる（2 つ目，3 つ目，4 つ目の等号において a,b が G の任意の元と可換であることを使った）．

■

命題 6.2.3.　p, q を $p<q$ なる素数で，$q\not\equiv 1 \bmod p$ とする．このとき，位数が pq の群は全て $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$ と同型である（中国式剰余定理（定理 4.4.1）より $\mathbb{Z}/pq\mathbb{Z}$ と同型）．

証明. A を G のシロー q 部分群とする．定理 6.1.2(4) より，G のシロー q 部分群の個数 n_q は p の約数かつ $n_q\equiv 1 \bmod q$ なので，$n_q=1$ となる（$p<q$ に注意）．また，B を G のシロー p 部分群とする．定理 6.1.2(4) より，G のシロー p 部分群の個数 n_p は q の約数かつ $n_p\equiv 1 \bmod p$ なので，仮定（$q\not\equiv 1 \bmod p$）より $n_p=1$ である．定理 6.1.2 の後のコメントより，A, B は G の正規部分群となる．

$A\cap B$ は A の部分群かつ B の部分群なので，ラグランジュの定理（定理 4.1.8）より $|A\cap B|$ は $|A|=q$ の約数かつ $|B|=p$ の約数．従って，$|A\cap B|=1$ となり，$A\cap B=\{1_G\}$ である．

以上のことを用いると，定理 4.4.9 より，同型写像

$$G\cong A\times B$$

が存在することが分かる．命題 6.2.1 より $A\cong\mathbb{Z}/p\mathbb{Z}$ かつ $B\cong\mathbb{Z}/q\mathbb{Z}$ なので，

$$G\cong\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/q\mathbb{Z}$$

が示された． ■

命題 6.2.4. p を奇素数とする．このとき，位数が $2p$ の群は全て $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ ($\cong \mathbb{Z}/2p\mathbb{Z}$) または D_p と同型である．

証明. A を G のシロー 2 部分群，B を G のシロー p 部分群とする．このとき，定理 6.1.2(4) より

- $n_2 \equiv 1 \bmod 2$ かつ n_2 は p の約数となるので，n_2 は 1 または p
- $n_p \equiv 1 \bmod p$ かつ n_p は 2 の約数となるので，$n_p = 1$

$n_p = 1$ なので，B は G の正規部分群であることに注意しておく（定理 6.1.2 の後のコメント参照）．

$A \cap B$ は A, B の部分群なのでラグランジュの定理（定理 4.1.8）より $|A \cap B|$ は $|A| = 2, |B| = p$ の約数である．従って，$|A \cap B| = 1$ となり，$A \cap B = \{1_G\}$ である．

A, B はそれぞれ位数が素数 $2, p$ なので命題 6.2.1 より巡回群であり，位数 2 の元 t, 位数 p の元 r を用いて

$$A = \langle t \rangle = \{1_G, t\}, \quad B = \langle r \rangle = \{1_G, r, r^2, \dots, r^{p-1}\}$$

と表せる．

B は正規部分群より $trt^{-1} \in B$ となるため，$trt^{-1} = r^k$ となる $0 \leq k < p$ が存在する．このとき，$r = t^{-1}r^k t$ より

$$r = t^{-1}r^k t = (t^{-1}rt)^k = (r^k)^k = r^{k^2}$$

となるので，$r^{k^2-1} = 1_G$ となる．すると，r の位数が p なので命題 3.5.5 より $k^2 - 1$ は p の倍数である．ここで，$\overline{k}^2 = \overline{1}$ となる $(\mathbb{Z}/p\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \dots, \overline{p-1}\}$ の元が $\overline{1}$ または $\overline{p-1}$ であることに注意すると，k は 1 または $p-1$ となることが分かる．

$\underline{k = 1 \text{ のとき}}$：

$trt^{-1} = r$ となるので，任意の $j \in \mathbb{Z}$ に対して $tr^j t^{-1} = (trt^{-1})^l = r^j$ となる．従って，任意の $i, j \in \mathbb{Z}$ に対して $t^i r^j = r^j t^i$ が成り立つ．このことから，写像

$$f : A \times B \to G,\ (t^i, r^j) \mapsto t^i r^j$$

が準同型写像となることが分かる．$A \cap B = \{1_G\}$ により f は単射となるが，$|A \times B| = |A||B| = 6 = |G|$ なので f は同型写像である．命題 6.2.1 より A は $\mathbb{Z}/2\mathbb{Z}$ と，B は $\mathbb{Z}/p\mathbb{Z}$ と同型なので，G は $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/2p\mathbb{Z}$ と同型である．

$\underline{k = p-1 \text{ のとき}}$：

$trt^{-1} = r^{p-1}$ となるので，任意の $j \in \mathbb{Z}$ に対して $tr^j t^{-1} = (trt^{-1})^l = r^{j(p-1)} = r^{p-j}$ となる．従って，任意の $j \in \mathbb{Z}$ に対して $tr^j = r^{p-j}t$ が成り立つ．このことから，写像

$$f : D_p \to G,\ T^i R^j \mapsto t^i r^j$$

が準同型写像となることが分かる．上と同様に $A \cap B = \{1_G\}$ なので f は単射となり，$|D_p| = |G| = 2p$ なので f は同型写像となる．従って，G は D_p と同型である． ■

これまで示したことを使うと，$n \leq 15$ の場合の位数 n の有限群の分類は以下のようになる（位数が n の群はリストに書いてある群のいずれかと同型になる）．

n	位数 n の群のリスト	理由
1	$\mathbb{Z}/\mathbb{Z}$	位数 1 の群は単位元のみからなるので
2	$\mathbb{Z}/2\mathbb{Z}$	命題 6.2.1 より
3	$\mathbb{Z}/3\mathbb{Z}$	命題 6.2.1 より
4	$\mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$	命題 6.2.2 より
5	$\mathbb{Z}/5\mathbb{Z}$	命題 6.2.1 より
6	$\mathbb{Z}/6\mathbb{Z},\ D_3\ (\cong S_3)$	命題 6.2.4 より
7	$\mathbb{Z}/7\mathbb{Z}$	命題 6.2.1 より
8	?	
9	$\mathbb{Z}/9\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$	命題 6.2.2 より
10	$\mathbb{Z}/10\mathbb{Z},\ D_5$	命題 6.2.4 より
11	$\mathbb{Z}/11\mathbb{Z}$	命題 6.2.1 より
12	?	
13	$\mathbb{Z}/13\mathbb{Z}$	命題 6.2.1 より
14	$\mathbb{Z}/14\mathbb{Z},\ D_7$	命題 6.2.4 より
15	$\mathbb{Z}/15\mathbb{Z}$	命題 6.2.3 より

$n = 8, 12$ の場合については若干大変なので省略する（問題 6.3.3 を見よ）．一般に，n の素因数の数が多くなるほど位数 n の群の分類は複雑になっていく．

6.3　シローの定理の証明

この節では先延ばしにしていたシローの定理の証明を与える．まずは次の補題を示す．

補題 6.3.1. p を素数，r, m を 1 以上の自然数で $\gcd(p, m) = 1$ とする．このとき，二項係数 $\binom{p^r m}{p^r}$ は p で割り切れない．

証明. 二項係数の定義より

$$\begin{aligned}\binom{p^r m}{p^r} &= \frac{(p^r m)!}{p^r!\,(p^r(m-1))!} \\ &= \frac{p^n m(p^r m - 1)(p^r m - 2)\cdots(p^r m - p^r + 1)}{p^r(p^r - 1)(p^n - 2)\cdots 1} \\ &= m\prod_{k=1}^{p^r-1}\frac{p^r m - k}{p^r - k}\end{aligned}$$

と変形できる．ここで，$1 \leq k < p^r$ を $k = p^i l$（$\gcd(p, l) = 1$）と表すと，

$$\frac{p^r m - k}{p^r - k} = \frac{p^i(p^{r-i}m - l)}{p^i(p^{r-i} - l)} = \frac{p^{r-i}m - l}{p^{r-i} - l}$$

となり，既約分数で表したときに分子分母は p で割り切れない．従って，

$$\prod_{k=1}^{p^r-1}\frac{p^r m - k}{p^r - k}$$

を既約分数 $\frac{a}{b}$ で表したとき，a, b は p で割り切れない．すると，等式

$$\binom{p^r m}{p^r} b = am$$

において，a, b, m は p で割り切れないので，$\binom{p^r m}{p^r}$ も p で割り切れない． ■

定理 6.3.2 (シローの定理 I（定理 6.1.2(1)）)．G を有限群，p を $|G|$ の素因子，$|G| = p^r m$ $(\gcd(p, m) = 1)$ とする．このとき，G のシロー p 部分群が存在する．

証明. p^r 個の元を持つ G の部分集合全体の集合を T と書く：

$$T := \{X \subseteq G \mid |X| = p^n\}$$

このとき，G は集合 T に

$$g \cdot X := gX := \{gx \mid x \in X\}$$

により作用する．この作用の軌道分解

$$T = \bigcup_{i=1}^{t} G \cdot X_i \quad (\text{互いに交わらない和集合})$$

を考えたとき，両辺の元の個数を考えると命題 5.1.7(2) より

$$\binom{p^n m}{p^n} = |T| = \sum_{i=1}^{t} |G \cdot X_i| = \sum_{i=1}^{t} |G|/|G_{X_i}|$$

となる（$G_{X_i} := \{g \in G \mid gX_i = X_i\}$ は上の作用による X_i の安定化群）．

補題 6.3.1 により左辺は p で割り切れないので，いずれかの $|G|/|G_{X_i}|$ は p で割り切れない．ラグランジュの定理（定理 4.1.8）より $|G_{X_i}|$ は $|G| = p^r m$ の約数なので，$|G_{X_i}|$ は p^r の倍数である．勝手な $x \in X_i$ を取ると，任意の $g \in G_{X_i}$ に対して $gx \in X_i$ となるので，$G_{X_i} \cdot x \subseteq X_i$ が従う．よって，命題 4.1.5(2) より，$|G_{X_i}| = |G_{X_i} \cdot x| \leq |X_i| = p^r$ となる．以上より $|G_{X_i}| = p^r$ となるので，G_{X_i} が G のシロー p 部分群である．■

定理 6.3.3 (シローの定理 II（定理 6.1.2(2)(3)）)．G を有限群，p を $|G|$ の素因子，$|G| = p^r m$ $(\gcd(p, m) = 1)$ とする．

(2) G の任意の p 部分群はあるシロー p 部分群に含まれる．
(2) G のシロー p 部分群は全て互いに共役である．

証明．S を G のシロー p 部分群とする．このとき，以下の主張を示せば良い：

$$H \text{ を位数が } p \text{ のべき } p^s \text{ の } G \text{ の部分群とする．このとき，ある } x \in G \text{ が存在して } x^{-1}Hx \subseteq S \text{ となる．}$$

実際，これが示されると $H \subseteq x^{-1}Sx$ となり，H はシロー p 部分群 $g^{-1}Sg$ に含まれる．また，H がシロー p 部分群のとき，$|H| = p^r = |xSx^{-1}|$ なので $H = xSx^{-1}$ となり，H と S は共役である．

以下，上の主張を示す．$X := G/S$ と置くと，ラグランジュの定理（定理 4.1.8）より $|X| = |G|/|S| = p^r m/p^r = m$ である．H の X への作用

$$H \times X \to X,\ (h, xS) \mapsto h \cdot xH := (hx)S$$

を考える．この作用による X の軌道分解

$$X = \bigcup_{i=1}^{t} H \cdot x_i S \quad (\text{互いに交わらない和集合})$$

を考えると，

$$|X| = \sum_{i=1}^{t} |H \cdot x_i S|$$

が成り立つ．命題 5.1.7(2) より $|H \cdot x_i S| = |H|/|H_{x_i S}|$ は $|H| = p^s$ の約数であるが，$|X| = m$ は p を約数に持たないので，ある i について $|H \cdot x_i S| = 1$ となる．このとき，任意の $h \in H$ に対して

$$h \cdot x_i S = x_i S$$

が成り立つ．つまり，任意の $h \in H$ に対して $x_i^{-1} h x_i \in S$ となるが，これは $x_i^{-1} H x_i \subseteq S$ を意味する．■

定理 6.3.4 (シローの定理 I（定理 6.1.2(4)）)．G を有限群，p を $|G|$ の素因子，$|G| = p^r m$ $(\gcd(p, m) = 1)$ とする．G のシロー p 部分群の個数を n_p とすると，以下が成り立つ：

(i) $n_p | m$
(ii) $n_p \equiv 1 \bmod p$

証明．Y を G のシロー p 部分群全体の集合とする．G は Y に

$$G \times Y \to Y,\ (x, H) \mapsto xHx^{-1}$$

で作用する．S をシロー p 部分群とする．定理 6.1.2(3) より S の G 軌道は Y 全体となるので，命題 5.1.7(2) より

$$|Y| = |G \cdot S| = |G|/|G_S|$$

となる（$G_S = \{x \in G \mid xSx^{-1} = S\}$ はこの作用による S の安定化群）．ここで，$x \in S$ に対して $xSx^{-1} = S$ が成り立つので $S \subseteq G_S$．ラグランジュの定理（定理 4.1.8）より $|G_S|$ は $|S| = p^r$ の倍数．従って，$|Y| = |G|/|G_S|$ は $m = |G|/p^r$ の約数である．

次に，$n_p \equiv 1 \bmod p$ を示すために，作用

$$S \times Y \to Y,\ (x, H) \mapsto xHx^{-1}$$

を考える（上の作用と同じだが作用する群が S に制限されている）．この作用の軌道分解

$$Y = \bigcup_{i=1}^{t} S \cdot H_i \quad （互いに交わらない和集合）$$

を考えると，

$$|Y| = \sum_{i=1}^{t} |S \cdot H_i|$$

が成り立つ．また，命題 5.1.7(2) より $|S \cdot H_i|$ は $|S| = p^r$ の約数である．

ここで，Y の元 S を含む S 軌道 $S \cdot H_i$ を考えると $S = xH_ix^{-1}$ $(x \in S)$ と表せるが，$x \in S$ なので $H_i = x^{-1}Sx = S$ となる．従って，$S \cdot H_i = \{S\}$ が成り立つ．逆に，$|S \cdot H_j| = 1$ のとき，次の補題により $S = H_j \in S \cdot H_j$ が分かるので，$i = j$ が従う．

以上のことより，$|S \cdot H_i| = 1$ かつ $|S \cdot H_j|$ $(j \neq i)$ は 1 より大きい p のべきとなるので，それらの和 $n_p = |Y|$ は p で割って 1 余る整数である．■

補題 6.3.5. G を有限群，p を $|G|$ の素因子，$|G| = p^r m$ $(\gcd(p, m) = 1)$ とし，S, S' を G のシロー p 部分群とする．任意の $x \in S$ に対して $xS'x^{-1} = S'$ が成り立つならば，$S = S'$．

証明. 定理 6.3.4 の証明で考えた作用 $G \times Y \to Y,\ (x, H) \mapsto xHx^{-1}$ による $S' \in Y$ の安定化群 $G_{S'} = \{x \in G \mid xS'x^{-1} = S'\}$ を考える．すると，定理 6.3.4 の前半で使った議論と同様にして，$|G_{S'}|$ は p^r の倍数であり，$|G_{S'}| = p^r m'$ $(\gcd p, m' = 1)$ と表せる．

ここで，仮定より $S \subseteq G_{S'}$ である．また，任意の $x \in S'$ も $xS'x^{-1} = S'$ を満たすので，$S \subseteq G_{S'}$ も成り立つ．今，$|G_{S'}| = p^r m'$ $(\gcd p, m' = 1)$ かつ $|S| = |S'| = p^r$ なので，S と S' は $G_{S'}$ のシロー p 部分群でもある．従って，定理 6.1.2(3) より，ある $x \in G_{S'}$ が存在して $S = xS'x^{-1}$ が成り立つ．すると，$G_{S'}$ の定義より $S = xS'x^{-1} = S'$ が示される．■

演習問題

問題 6.3.1. (1) $\mathbb{Z}/36\mathbb{Z}$ のシロー 3 部分群を一つ見つけよ．
(2) $(\mathbb{Z}/11\mathbb{Z})^\times$ のシロー 5 部分群を一つ見つけよ．
(3) $(\mathbb{Z}/13\mathbb{Z})^\times$ のシロー 2 部分群を一つ見つけよ．
(4) D_6 のシロー 2 部分群を一つ見つけよ．

問題 6.3.2. p を素数とする．

(1) 位数が p^2 の有限群 G には位数 p の元が存在することを示せ．
(2) 位数が $2p$ の有限群 G には位数 p の元が存在することを示せ．
(3) 位数が p の倍数である有限群 G には位数 p の元が存在することを示せ．

問題 6.3.3. $\mathsf{GL}_2(\mathbb{C})$ の元

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

を考える.

(1) $Q := \{E_2, -E_2, I, -I, J, -J, K, -K\}$ が $\mathsf{GL}_2(\mathbb{C})$ の部分群であることを確かめよ.
(2) Q がアーベル群であることを確かめよ.
(3) Q の中心 $\mathsf{Z}(Q)$ を計算せよ.
(4) D_4 の中心 $\mathsf{Z}(D_4)$ を計算せよ.
(5) $D_4 \ncong Q$ を示せ.
(6) 位数 8 の群が全て $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, D_4, Q のいずれかと同型となることを何らかの文献（群論の本など）を参照して示せ.

ちなみに，(5) より D_4 と Q は同型でないので，(6) の 5 個の群はどの二つも同型ではない.