

定理 (準同型定理) . 群の準同型写像 $f: G \rightarrow G'$ は, 同型写像 $\varphi: G/\text{Ker} f \rightarrow \text{Im} f, g \text{Ker} f \mapsto f(g)$ を引き起こす .

例 . $\text{GL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\}$, $\text{SL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A = 1\}$ とする . $\det: \text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^\times = \mathbb{R} \setminus \{0\}, A \mapsto \det A$ は全射準同型写像 . 準同型定理より $\text{GL}_n(\mathbb{R})/\text{SL}_n(\mathbb{R}) \cong \mathbb{R}^\times$.

例 . $\text{sgn}: S_n \rightarrow \{\pm 1\}, \sigma \mapsto \text{sgn}(\sigma)$ は全射準同型写像であり, $\text{Ker sgn} = A_n$. よって, 準同型定理より $S_n/A_n \cong \{\pm 1\}$ が得られる .

定義 (X 上の対称群) . $S(X) := \{\sigma: X \rightarrow X \mid \sigma: \text{全単射}\}$ は写像の合成 $\sigma \circ \tau := \sigma(\tau(x)), \forall x \in X$ に関して群をなす . $(S(X), \circ)$ を X 上の対称群, $\sigma \in S(X)$ を置換, $G \subset S(X)$ を置換群という .

定理 . 位数 n の有限群は S_n のある部分群と同型である .

定義 (群が集合に作用する) . G を群とする . 集合 X に対して, 写像 $G \times X \rightarrow X, (g, x) \mapsto g \circ x$ が次の 2 つの条件, (1) $(\sigma \circ \tau)(x) = \sigma \circ (\tau \circ x)$, (2) $1_G \circ x = x$ を満たすとき, G は X に作用しているといい, $G \curvearrowright X$ とかく . このとき, G を X の変換群, X を G -集合という .

定義 1 (元 x の G -軌道) . $G \curvearrowright X$ とする . X の部分集合 $\{g \circ x \mid g \in G\}$ を x の G -軌道 (G -orbit) といい, $\text{Orb}_G(x)$ とかく .

命題 2 . $G \curvearrowright X$ のとき, $x \sim y \Leftrightarrow \exists g \in G \text{ s.t. } g \circ x = y$ とすれば, $\sim$ は X 上の同値関係を与える .

定義 3 (共役作用, 共役類, 類等式) . $G \times G \rightarrow G, (g, x) \mapsto g \circ x := gxg^{-1}$ による, G の G 自身への作用 ($G \curvearrowright G$) を共役作用, 共役作用による軌道 $\text{Orb}_G(x)$ を x の共役類, 共役類による類別 $G = C_1 \cup \dots \cup C_k$ の各類の位数を表わした等式 $\#G = \#C_1 + \#C_2 + \dots + \#C_k$ を類等式という .

定義 4 (x の G における固定群) . $G \curvearrowright X$ とする . $x \in X$ に対し, $\text{Stab}_G(x) := \{g \in G \mid g \circ x = x\}$ を x の G における固定群 (stabilizer), または等方群 (isotropy group) という .

定理 5 (Orbit-Stabilizer Theorem) . $G \curvearrowright X$ に対し, $\#\text{Orb}_G(x) = |G : \text{Stab}_G(x)|$. 特に, $\#\text{Orb}_G(x) \mid \#G$

定義 6 (中心化群, 中心) . 空でない部分集合 $S \subset G$ に対し, $Z_G(S) := \{g \in G \mid gsg^{-1} = s, (\forall s \in S)\} = \{g \in G \mid gs = sg, (\forall s \in S)\}$ を S の中心化群という . $S = \{a\}$ のとき, $Z_G(\{a\}) = Z_G(a)$ とかく . $Z_G(G)$ は単に $Z(G)$ とかき, G の中心という .

命題 7 . (1) $Z_G(S) \subset G$; 部分群, (2) x と共役な G の元の個数は $|G : Z_G(x)|$, (3) $\text{Orb}_G(x) = \{x\} \Leftrightarrow Z_G(x) = G \Leftrightarrow x \in Z(G)$.

命題 8 . S_n の 2 つの元 σ, τ が共役 $\Leftrightarrow \sigma$ と τ は同じ型 (サイクルタイプ).

命題 9 . $N \triangleleft G$ とすると, N はいくつかの共役類の和集合である .

- [1] $T := \{z \in \mathbb{C}^\times \mid |z| = 1\}$ とする .
 (i) $f: \mathbb{C}^\times \rightarrow \mathbb{R}_{>0}, z \mapsto |z|$ は全射準同型写像である事を示せ . また, 準同型定理を用いると準同型写像 f からどのような同型が得られるか?
 (ii) $g: \mathbb{R} \rightarrow \mathbb{C}^\times, x \mapsto \cos 2\pi x + i \sin 2\pi x$ は準同型写像である事を示せ . また, 準同型定理を用いると準同型写像 g からどのような同型が得られるか?

[2] $n = 3, 4, 5$ に対して, S_n の類等式を求めよ .

[3] $n = 3, 4, 5$ に対して, A_n の類等式を求めよ .

[4] $n = 3, 4, 5$ に対して, D_n の類等式を求めよ .

[5] A_4 の類等式 $12 = 1 + 3 + 4 + 4$ を使って, A_4 には指数 2 の部分群 H が存在しない事を示せ . (ヒント H の存在を仮定すると, $H \triangleleft A_4$ となり, 命題 9 から矛盾が導かれる)

[6] A_5 の類等式 $60 = 1 + 15 + 20 + 12 + 12$ を使って, A_5 が単純群である (自明群 $\{1\}$ と A_5 以外には正規部分群はない) ことを示せ . (ヒント 命題 9 を使う)

定義 10 (群の (外部) 直積, 直和) . $G_1, \dots, G_n$ を群とする . 直積集合 $G_1 \times \dots \times G_n = \{(x_1, \dots, x_n) \mid x_i \in G_i\}$ は二項演算 $(x_1, \dots, x_n) \circ (y_1, \dots, y_n) := (x_1 y_1, \dots, x_n y_n)$ により群をなす .
群 $(G_1 \times \dots \times G_n, \circ)$ を $G_1, \dots, G_n$ の (外部) 直積 という . 特に , 各 G_i が加群 $(G_i, +)$ のときには , $G_1, \dots, G_n$ の 直和 といい $G_1 \oplus \dots \oplus G_n$ とかく .

命題 11 . (1) $G_1 \times G_2 \cong G_2 \times G_1$. 一般に , $G_1 \times \dots \times G_n$ の順序をどう入れ替えても同型 .
(2) $G = G_1 \times G_2$ のとき , $G'_1 := \{(g_1, 1_{G_2}) \mid g_1 \in G_1\}, G'_2 := \{(1_{G_1}, g_2) \mid g_2 \in G_2\}$ とおくと , $G'_1 \triangleleft G, G'_2 \triangleleft G$ であり , $G_1 \cong G'_1, G_2 \cong G'_2, G = G'_1 G'_2, G'_1 \cap G'_2 = \{1_G\}$.
(3) G'_1 の元と G'_2 の元は交換可能 .

定義 12 (内部直積) . $N_1 \triangleleft G, N_2 \triangleleft G$ に対し ,

(1) $G = N_1 N_2$, (2) $N_1 \cap N_2 = \{1_G\}$

が成り立つとき、 G は N_1 と N_2 の 内部直積 といい , $G = N_1 \dot{\times} N_2$ とかく .

命題 13 . $G = N_1 \dot{\times} N_2$ のとき , N_1 の元と N_2 の元は交換可能 .

命題 14 . $N_1, N_2 \triangleleft G$ に対し , $G = N_1 \dot{\times} N_2 \Leftrightarrow \forall g \in G, g = ab, (a \in N_1, b \in N_2)$ と一意的に書ける .

命題 15 . $G = N_1 \dot{\times} N_2 \implies G \cong N_1 \times N_2$ (外部直積).

コメント . 前命題 (命題 15) と命題 11, $G = G_1 \times G_2 \implies \exists N_1, \exists N_2 \triangleleft G$ s.t. $N_1 \cong G_1, N_2 \cong G_2$ かつ $G = N_1 \dot{\times} N_2$ より , 外部直積と内部直積は同型を同一視すれば , 同じものである . よって今後は区別せずに , 単に直積といい , $G = G_1 \times G_2$ とかく . また , $G = G_1 \times \dots \times G_n$ の場合にも , $N_i \triangleleft G$ に対し , (1) $G = N_1 \dots N_n$, (2) $(H_1 \dots H_i) \cap H_{i+1} = \{1_G\}, (1 \leq i \leq n-1)$ によって内部直積を定義すれば , 同様の結果が得られる .

定理 16 (中国の剰余定理, Chinese Remainder Theorem) .

$m, n \in \mathbb{Z}, (m, n) = 1$ とする . このとき , $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. ($C_{mn} \cong C_m \times C_n$)

系 17 . $n_1, \dots, n_r \in \mathbb{N}$ に対して , どの 2 つも互いに素とし , $n = n_1 \dots n_r$ とおく .

$a_1, \dots, a_r \in \mathbb{Z}$ に対し , $\exists x \in \mathbb{Z}$ s.t. $x \equiv a_1 \pmod{n_1}, \dots, x \equiv a_r \pmod{n_r}$.

解の 1 つを x_0 とすると , 全ての解は $x = x_0 + kn, (k \in \mathbb{Z})$ で与えられる .

命題 18 . $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ の元 $[a]$ に逆元が存在 $\Leftrightarrow (a, n) = 1$.

定義 19 (既約剰余類群, オイラー関数) . $(\mathbb{Z}/n\mathbb{Z})^\times := \{[a] \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}$ は乗法群であり , n を法とする既約剰余類群という . $\varphi(n) := \#(\mathbb{Z}/n\mathbb{Z})^\times$ を オイラー関数 という .

定理 20 (オイラーの定理) . $n \in \mathbb{N}, (a, n) = 1$ とすると , $a^{\varphi(n)} \equiv 1 \pmod{n}$.

系 21 (フェルマーの小定理) . p ; 素数 , $(a, p) = 1$ とすると , $a^{p-1} \equiv 1 \pmod{p}$.

よって , $\forall a \in \mathbb{Z}$ に対し , $a^p \equiv a \pmod{p}$.

Fact 22 . $(m, n) = 1$ ならば , $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$

命題 23 (オイラー関数の計算) .

(1) 素数 p と $r \in \mathbb{N}$ に対して , $\varphi(p^r) = p^{r-1}(p-1)$

(2) $(m, n) = 1$ ならば , $\varphi(mn) = \varphi(m)\varphi(n)$.

Fact 24 . G を位数 n の有限群とする . $G \cong C_n \iff \forall d \mid n$ に対し , $\#\{a \in G \mid a^d = 1\} \leq d$

Fact 25 . $((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$ は位数 $p-1$ の巡回群 . $(\mathbb{Z}/p\mathbb{Z})^\times = \langle g \rangle$ なる $g \in \mathbb{N}$ を法 p の原始根という .

[1] 3 で割ると余りが 2, 5 で割ると余りが 4 となるような整数をすべて求めよ .

[2] 19^{1219} を 29 で割った余りは?

[3] $10^k \equiv 1 \pmod{17}$ となる $k \in \mathbb{N}$ は存在するか? また存在すれば , 最小の k を答えよ .

[4] $2 \leq n \leq 30$ に対し , $\varphi(n)$ を求めよ .