代数学 C・代数学特論 III　2023 年度前期

コスキヴィルタ・ジャンステファン

埼玉大学

目次

数学記号一覧

	記号	説明
数論	$\gcd(a,b)$	a と b の最大公約数
	$\mathrm{lcm}(a,b)$	a と b の最小公倍数
集合論	id_X	集合 X の恒等写像
	$f \circ g$	写像 f, g の合成写像
	f^{-1}	全単射 $f\colon X \to Y$ の逆写像
	$f^{-1}(A)$	写像 f による集合 A の逆像
	$\lvert X \rvert$	集合 X の元の個数
	$\emptyset$	空集合
	$X \setminus Y$	X から Y を引いた差集合
	$\mathcal{F}(X,X)$	写像 $X \to X$ 全体の集合
線形代数	$\det(A)$	行列 A の行列式
	$\det(f)$	ベクトル空間 V の線形変換 $f\colon V \to V$ の行列式
	$\chi_A(X)$	行列 A の固有多項式
	$\chi_f(X)$	ベクトル空間 V の線形変換 $f\colon V \to V$ の固有多項式
	E_n	n 次正方単位行列
	$W_1 \oplus W_2$	線形部分空間 W_1, W_2 の直和
	$\mathrm{Span}(u_1,\ldots,u_n)$	ベクトル $u_1,\ldots,u_n$ の線形結合全体のなす部分空間
	$\mathrm{M}_n(\mathbb{K})$	可換体 $\mathbb{K}$ を成分とする n 次正方行列全体の集合
	$\mathrm{GL}_n(\mathbb{K})$	可換体 $\mathbb{K}$ の元を成分とする n 次正則行列全体のなす群
	$\lVert x \rVert$	ベクトル x のノルム
	$\mathrm{O}_n(\mathbb{R})$	n 次直交行列全体の群
	$\mathrm{SO}_n(\mathbb{R})$	行列式が 1 である n 次直交行列全体の群
	$W^{\perp}$	ユークリッド空間の線形部分空間 W の直交補空間
	$\mathbb{F}_p$	可換体 $\mathbb{Z}/p\mathbb{Z}$ (p：素数)
群論	$x \cdot y$, xy	乗法的に書かれた演算
	$x + y$	加法的に書かれた演算
	$\langle x \rangle$	x で生成される巡回部分群
	x^{-1}	x の逆元
	Ker	核
	Im	像
	$Z(G)$	群 G の中心
	xH	部分群 H による x の左剰余類
	Hx	部分群 H による x の右剰余類
	G/H	部分群 H による G の左剰余類全体の集合 (または剰余群)
	$H\backslash G$	部分群 H による G の右剰余類全体の集合
	$H \triangleleft G$	H が G の正規部分群であることを意味する記号
	$G \times H$	G と H の直積
	$\mathrm{Aut}(G)$	G の自己同型群
	$N_G(H)$	G における部分群 H の正規化群
	G_x	x の安定化部分群

Gx	G による x の軌道
$[G : H]$	部分群 H の G における指数
X^G	G の X への作用に関する固定点全体の集合
X^g	g で固定される元全体の集合
X/G	G の作用による X の軌道全体の集合
$\mathfrak{S}_n$	n 次対称群
$\mathfrak{S}(X)$	集合 X の次対称群
$\mathfrak{A}_n$	n 次交代群
$(a_1 \cdots a_k)$	長さ k の巡回置換
n_p	p シロー部分群の個数
$N \rtimes_\varphi H$	$\varphi\colon H \to \mathrm{Aut}(N)$ に関する外部半直積
$G = N \rtimes H$	G が部分群 N と H の半直積であることを意味する記号
$\mathbb{Z}/n\mathbb{Z}$	n を法とする剰余類群
$(\mathbb{Z}/n\mathbb{Z})^\times$	剰余環 $\mathbb{Z}/n\mathbb{Z}$ の乗法群
D_n	n 次二面体群
$D(G)$	群 G の導来部分群
$[G, G]$	同上
$[x, y]$	x と y の交換子
G^{ab}	G のアーベル化
$\mathrm{ord}(x)$	x の位数
$\mathrm{sgn}(\sigma)$	置換 σ の符号
$\mathrm{Cent}_G(x)$	G における x の中心化群
$\mathrm{Inn}(G)$	G の内部自己同型全体のなす群
$\lim$	極限

解析

1　群

1.1　モノイド, 半群, 群

X を空でない集合とする．X 上の演算とは, 写像 $X \times X \to X$ のことである．例えば, $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, $(x, y) \mapsto x + y$ は $\mathbb{Z}$ 上の演算である．演算 $f\colon X \times X \to X$ が与えられているとき, $f(x, y)$ を単に $x \cdot y$ または xy と表す．任意の $x, y, z \in G$ に対し

$$(xy)z = x(yz)$$

が成り立つとき, 演算が結合的である (または結合法則を満たす) という．演算が結合法則を満たすときに G が半群であるという．結合法則が成り立つときに, 有限個の元 $x_1, \ldots, x_n$ の積はカッコの入れ方に依らないので, 単に

$$x_1 x_2 \ldots x_n$$

と表す．各 x_i が x に等しい場合, 上の積を x^n と書き, x の n 乗という．G の元 e が単位元であるとは, 任意の $x \in G$ に対し

$$ex = xe = x$$

であることをいう．

補題 1.1　単位元が高々一つ存在する．

証明

e, e' を G の単位元とする．このとき, $e = ee' = e'$ となり, 主張が従う．

定義 1.2　単位元を持つ半群をモノイドという．

G をモノイドとする．$x \in G$ が可逆元であるとは,

$$xy = yx = e \tag{1.1}$$

を満たす元 $y \in G$ が存在することをいう．上の条件を満たす元 y を x の逆元という．

補題 1.3　$x \in G$ が可逆元ならば, x の逆元は一意的に存在する．

証明

$y, y' \in G$ を x の逆元とする (つまり, $e = xy = yx = xy' = y'x$ とする)．このとき,

$$y = ye = y(xy') = (yx)y' = ey' = y'$$

である．主張が従う．

x の逆元を x^{-1} とおく．逆元の定義より $xx^{-1} = x^{-1}x = e$ が成り立つ．

命題 1.4

(1) 単位元 e は可逆元であり, $e^{-1} = e$ である．
(2) $x \in G$ を可逆元とする．このとき, x^{-1} も可逆元であり, $(x^{-1})^{-1} = x$ である．
(3) $x, y \in G$ が可逆元ならば, xy も可逆元である．さらに $(xy)^{-1} = y^{-1}x^{-1}$ が成り立つ．

証明

- (1) は $ee = e$ から分かる.
- (2) を示す. $xx^{-1} = x^{-1}x = e$ より, x^{-1} も可逆元であり, その逆元は x である.
- (3) を示す. x, y を可逆元とする. このとき

$$xy(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xx^{-1} = e$$
$$(y^{-1}x^{-1})xy = y^{-1}(x^{-1}x)y = y^{-1}y = e$$

よって, xy は可逆元であり, その逆元は $y^{-1}x^{-1}$ である.

例 1.5.

- $(\mathbb{Z}_{\geq 0}, +)$ はモノイドであり, その単位元は 0 である. 可逆元は 0 のみである.
- $(\mathbb{Z}/n\mathbb{Z}, +)$ は $\overline{0}$ を単位元とするモノイドである. 全ての元が可逆元である.
- $(\mathbb{Z}/n\mathbb{Z}, \times)$ は $\overline{1}$ を単位元とするモノイドである. 以下が成り立つ.

$$\overline{k} \text{ が可逆元である} \iff \gcd(k, n) = 1.$$

実際, $\overline{k}$ が可逆元になるためには, $ak + bn = 1$ となる $a, b \in \mathbb{Z}$ が存在することは必要十分である (このとき, $\overline{a}\overline{k} = \overline{1}$ となり, $\overline{k}$ の逆元は $\overline{a}$ である).

- $(\mathrm{M}_n(\mathbb{C}), \times)$ は単位行列を単位元とするモノイドである. 可逆元は正則行列である.
- X を集合とし, $\mathcal{F}(X, X)$ を写像 $f\colon X \to X$ 全体の集合とする. 写像の合成 $(f, g) \mapsto f \circ g$ に関して $\mathcal{F}(X, X)$ はモノイドをなす (その単位元は恒等写像である). $f\colon X \to X$ が可逆元であるためには, f が全単射であることが必要十分である.

x が可逆元ならば, x のべき乗「x^n」の定義を $n \in \mathbb{Z}$ の場合に拡張する. すなわち, $n = 0$ のとき $x^0 = e$ と約束し, $n < 0$ のとき

$$x^n := (x^{-1})^{-n}$$

と定める. n, m が任意の整数ならば, 以下が成り立つ.

(1) $x^{n+m} = x^n x^m$,

(2) $x^{nm} = (x^n)^m$,

(3) $x^{-n} = (x^{-1})^n = (x^n)^{-1}$.

定義 1.6 G がモノイドで, G の全ての元が可逆元であるとき, G を群という.

さらに, 任意の $x, y \in G$ に対し

$$xy = yx$$

が成り立つときに, G が可換群またはアーベル群であるという.

例 1.7.

- $(\mathbb{Z}, +)$ と $(\mathbb{Z}/n\mathbb{Z}, +)$ はアーベル群である.
- $(\mathbb{C}^*, \times)$ はアーベル群である.

補題 1.8 H がモノイドで,

$$G = \{x \in H \mid x \text{ が可逆元である}\}$$

とおくと, G は H の演算に関して群をなす.

証明

命題 1.4(3) より, $x, y \in G$ ならば $xy \in G$ である. よって, H の演算は G 上の演算 $G \times G \to G$, $(x, y) \mapsto xy$ を引き起こす. $e \in G$ であるので, G は明らかにモノイドである. また, $x \in G$ とする. このとき, 命題 1.4 により $x^{-1} \in G$ である. ゆえに, x は G 内に可逆元を持つ. したがって G は群である.

例 1.9.

- モノイド $(\mathbb{Z}/n\mathbb{Z}, \times)$ を考える. 補題 1.8 により以下の部分集合は掛け算に関して群をなす.

$$(\mathbb{Z}/n\mathbb{Z})^{\times} = \left\{ \overline{k} \in \mathbb{Z}/n\mathbb{Z} \;\middle|\; \gcd(k, n) = 1 \right\}.$$

- モノイド $(\mathrm{M}_n(\mathbb{C}), \times)$ を考える. 補題 1.8 により $\mathrm{GL}_n(\mathbb{C}) = \{A \in \mathrm{M}_n(\mathbb{C}) \mid \text{正則行列}\}$ は行列の積に関して群をなす. $n \geq 2$ のとき $\mathrm{GL}_n(\mathbb{C})$ はアーベル群でない.
- モノイド $(\mathcal{F}(X, X), \circ)$ を考える. 補題 1.8 により

$$\mathfrak{S}(X) = \{f \colon X \to X \mid \text{全単射}\}.$$

は写像の合成に関して群をなす. $\mathfrak{S}(X)$ を X の対称群といい, その元を X の置換という. $|X| \geq 3$ のとき $\mathfrak{S}(X)$ はアーベル群でない. $X = \{1, 2, \ldots, n\}$ のとき, $\mathfrak{S}(X) = \mathfrak{S}_n$ と書く.

定義 1.10 G, H を群とする. $G \times H$ の 2 つの元 $(g_1, h_1), (g_2, h_2)$ に対し

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$$

とおくと, $G \times H$ 上の演算が定まり, $G \times H$ が群になる. この群を G と H の直積という.

1.2 部分群

G を群とし, その単位元を e とおく.

定義 1.11 部分集合 $H \subset G$ が G の部分群であるとは, 以下を満たすことをいう.

(a) $e \in H$.

(b) $x, y \in H$ ならば, $xy \in H$ である.

(c) $x \in H$ ならば, $x^{-1} \in H$ である.

$\{e\}$ 及び G は明らかに G の部分群である.

例 1.12. $(\mathbb{Z}, +)$ の部分群 $n\mathbb{Z}$ $(n \geq 0)$ である.

命題 1.13 H が部分群である $\iff$ H が空でなく, かつ任意の $x, y \in H$ に対し $xy^{-1} \in H$ である.

証明

- 「$\Longrightarrow$」は明らかである.
- 「$\Longleftarrow$」を示す. $H \neq \emptyset$ より $x \in H$ が取れる. 仮定より, $xx^{-1} = e \in H$ となり, H は定義 1.11 の条件 (a) を満たす. 次に, 定義 1.11 の (c) が成り立つことを確認する. $x \in H$ とする. $x^{-1} = ex^{-1}$ と書ける. $e \in H$ を示したので, 仮定より $x^{-1} \in H$ となる. 最後に, 定義 1.11 の (b) を示す. $x, y \in H$ とする. $xy = x(y^{-1})^{-1}$ と書ける. 一方, 以上より $y^{-1} \in H$ が成り立つ. ゆえに, $xy \in H$ がいえる. したがって, H は部分群である.

命題 1.14　G を群とし, $S \subset G$ を空でない部分集合とする. S を含む G の部分群のうちに最小のものが存在する. それを $\langle S \rangle$ とおくと,

$$\langle S \rangle = \{ s_1^{k_1} \dots s_m^{k_m} \mid s_i \in S,\ k_i \in \mathbb{Z} \} \tag{1.2}$$

が成り立つ. 任意の部分群 $H \subset G$ に対し, $S \subset H \iff \langle S \rangle \subset H$.

証明

上記の集合 (1.2) が部分群であることを示す. $S \neq \emptyset$ より $\langle S \rangle \neq \emptyset$ である. また, $x, y \in \langle S \rangle$ とし, $x = s_1^{k_1} \dots s_m^{k_m}$, $y = t_1^{r_1} \dots t_d^{r_d}$ $(s_i, t_i \in S,\ k_i, r_i \in \mathbb{Z})$ とする. このとき,

$$xy^{-1} = s_1^{k_1} \dots s_m^{k_m} t_d^{-r_d} \dots t_1^{-r_1}$$

となる. とくに $xy^{-1} \in \langle S \rangle$ である. したがって, $\langle S \rangle$ は部分群である. H を部分群とし, $S \subset H$ とする. このとき, 任意の $s_1, \dots, s_m \in S$ 及び $k_1, \dots, k_m \in \mathbb{Z}$ に対し $s_1^{k_1} \dots s_m^{k_m} \in H$ である. よって, $\langle S \rangle \subset H$ となる. ゆえに, $\langle S \rangle$ は S を含む部分群の中で最小のものである. また,「$S \subset H \iff \langle S \rangle \subset H$」が示された.

定義 1.15

(a) $\langle S \rangle$ は S で生成される部分群と呼ばれる.

(b) $\langle S \rangle = G$ のとき, S が G を生成する (または, S が G の生成系である) という.

(c) $S = \{x_1, \dots, x_n\}$ のとき, $\langle S \rangle$ を単に $\langle x_1, \dots, x_n \rangle$ と書く.

命題 1.14 により, 一つの元 $x \in G$ で生成された部分群は以下のように書ける.

$$\langle x \rangle = \{ x^k \mid k \in \mathbb{Z} \}.$$

定義 1.16　$G = \langle x \rangle$ となる $x \in G$ が存在するとき, G を巡回群という. また, $G = \langle x \rangle$ を満たす元 x は G の生成元と呼ばれる.

例えば, $\mathbb{Z}/n\mathbb{Z}$ は $\overline{1}$ で生成されるので, 巡回群である. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ は巡回群でない.

命題 1.17　$G = \mathbb{Z}/n\mathbb{Z}$ とする. $k \in \mathbb{Z}$ に対し, 以下が同値である.

(i) k と n が互いに素である.

(ii) $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$ である.

(iii) $\overline{k}$ が $(\mathbb{Z}/n\mathbb{Z}, +)$ の生成元である.

証明

「(i) $\iff$ (ii)」は既に知っている. (ii) ならば, $\overline{k}\overline{m} = \overline{1}$ となる $m \in \mathbb{Z}$ が存在する. よって, 任意の $d \in \mathbb{Z}$ に対し, $\overline{d} = (dm)\overline{k}$ となる ゆえに, $\overline{d}$ は $\mathbb{Z}/m\mathbb{Z}$ において $\overline{k}$ で生成される部分群に属する. よって, $\overline{k}$ は $\mathbb{Z}/m\mathbb{Z}$ を生成する. 逆に, $\overline{k}$ が $(\mathbb{Z}/n\mathbb{Z}, +)$ の生成元ならば, $m\overline{k} = \overline{1}$ となる $m \in \mathbb{Z}$ が存在する. よって, $\overline{m}\overline{k} = \overline{1}$ となり, $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$ である.

定義 1.18　G を群とする.

$$Z(G) := \{x \in G \mid \text{任意の } y \in G \text{ に対し}, xy = yx\}$$

とおき, G の中心という.

補題 1.19　$Z(G)$ は G の部分群である.

証明

明らかに, $e \in Z(G)$ である. $x, x' \in Z(G)$ とすると, 任意の $y \in G$ に対し

$$(xx')y = x(x'y) = x(yx') = (xy)x' = (yx)x' = y(xx')$$

である. よって, $xx' \in Z(G)$ である. また, $x \in Z(G)$ ならば, $xy = yx$ より,

$$x^{-1}y = x^{-1}(yx)x^{-1} = x^{-1}(xy)x^{-1} = yx^{-1}$$

となり, $x^{-1} \in Z(G)$ である. 主張が従う.

明らかに, G がアーベル群である $\iff$ $Z(G) = G$ が成り立つ.

例 1.20. $\mathbb{K}$ を可換体とする. $\mathrm{GL}_n(\mathbb{K})$ の中心は

$$Z(\mathrm{GL}_n(\mathbb{K})) = \{\lambda E_n \mid \lambda \in \mathbb{K}^*\}$$

2　準同型

2.1　定義

定義 2.1　G, G' を群とし, $f\colon G \to G'$ を写像とする. f が群準同型であるとは, 任意の $x, y \in G$ に対し

$$f(x \cdot y) = f(x) \cdot f(y)$$

が成り立つことをいう.

例 2.2.

- $(\mathbb{R}, +)$ と $(\mathbb{R}^*, \times)$ は明らかにアーベル群である. 写像 $\exp\colon \mathbb{R} \to \mathbb{R}^*,\ x \mapsto \exp(x)$ は $\exp(x+y) = \exp(x)\exp(y)$ を満たすので, $(\mathbb{R}, +)$ から $(\mathbb{R}^*, \times)$ への群準同型である.
- $\mathbb{K}$ を可換体とする. 行列式は群の準同型 $\det\colon \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^*$ である.

補題 2.3　$f\colon G \to G'$ を群準同型とする. G, G' の単位元をそれぞれ e, e' とおく.
(1) $f(e) = e'$ である.
(2) 任意の $x \in G$ に対し $f(x^{-1}) = f(x)^{-1}$ である.

証明

- $f(e) = f(ee) = f(e)f(e)$ である. よって, 両辺に $f(e)$ をかけると, $f(e) = e'$ となる.
- $f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = e'$ である. よって, $f(x^{-1}) = f(x)^{-1}$ である.

命題 2.4　$f\colon G \to G'$ を群準同型とする．

(1) $H \subset G$ が部分群ならば，$f(H)$ は G' の部分群である．

(2) $H' \subset G'$ が部分群ならば，$f^{-1}(H') = \{x \in G \mid f(x) \in H'\}$ は G の部分群である．

証明

- (1) を示す．$f(e) = e'$ かつ $e \in H$ より $e' \in f(H)$ である．また，$x, y \in f(H)$ とし，$x = f(a)$, $y = f(b)$ $(a, b \in H)$ とする．このとき，$xy^{-1} = f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$ となる．H が部分群だから，$ab^{-1} \in H$ であり，ゆえに $xy^{-1} \in f(H)$ である．したがって，$f(H)$ は G' の部分群である．
- (2) 示す．$f(e) = e'$ かつ $e' \in H'$ より，$e \in f^{-1}(H')$ である．また，$a, b \in f^{-1}(H')$ ならば，$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1}$ である．$f(a), f(b) \in H'$ より，$f(ab^{-1}) \in H'$ となる．よって，$ab^{-1} \in f^{-1}(H')$ である．以上より，$f^{-1}(H')$ は G の部分群である．

命題 2.5　$f\colon G \to G'$ を群準同型とし，$S \subset G$ を空でない部分群とする．以下が成り立つ．

$$f(\langle S \rangle) = \langle f(S) \rangle.$$

証明

$$\begin{aligned} f(\langle S \rangle) &= \{f(s_1^{k_1} \dots s_m^{k_m}) \mid s_i \in S,\ k_i \in \mathbb{Z}\} \\ &= \{f(s_1)^{k_1} \dots f(s_m)^{k_m}) \mid s_i \in S,\ k_i \in \mathbb{Z}\} \\ &= \langle f(S) \rangle. \end{aligned}$$

系 2.6　$f\colon G \to G'$ を全射群準同型とする．G が巡回群ならば，G' も巡回群である．

証明

$G = \langle x \rangle$ とする．命題 2.5 により，$G' = f(G) = f(\langle x \rangle) = \langle f(x) \rangle$ となるので，G' は $f(x)$ によって生成される．

2.2　準同型の核・像

定義 2.7　$f\colon G \to G'$ を群準同型とする．G, G' の単位元をそれぞれ e, e' と表す．

(a) $\mathrm{Ker}(f) := \{x \in G \mid f(x) = e'\}$ とおき，f の核という．

(b) $\mathrm{Im}(f) := \{f(x) \mid x \in G\}$ とおき，f の像という．

補題 2.8　$\mathrm{Ker}(f)$ は G の部分群であり，$\mathrm{Im}(f)$ は G' の部分群である．

証明

$\mathrm{Ker}(f) = f^{-1}(\{e'\})$, $\mathrm{Im}(f) = f(G)$ であるので，主張が命題 2.4 から従う．

例 2.9. $f(x) = \exp(ix)$ で定まる群準同型 $f\colon \mathbb{R} \to \mathbb{C}^*$ を考える.

$$\mathrm{Ker}(f) = \{x \in \mathbb{R} \mid f(x) = 1\} = 2\pi\mathbb{Z}$$

である. また,

$$\mathrm{Im}(f) = \{z \in \mathbb{C}^* \mid |z| = 1\}$$

が成り立つ.

例 2.10. 置換の符号は群の準同型 $\mathrm{sgn}\colon \mathfrak{S}_n \to \{\pm 1\}, \sigma \mapsto \mathrm{sgn}(\sigma)$ を与える. その核の元は偶置換と呼ばれ, $\mathfrak{A}_n = \{\sigma \in \mathfrak{S}_n \mid \mathrm{sgn}(\sigma) = 1\}$ は交代群と呼ばれる.

定義 2.11

(a) 群準同型 $f\colon G \to G'$ が全単射であるとき, f を群同型という.

(b) 群準同型 $G \to G$ のことを G の自己準同型という.

(c) 群同型 $G \to G$ のことを G の自己同型という.

G_1, G_2 が群で, 群同型 $G_1 \to G_2$ が存在するときに, $G_1 \simeq G_2$ と表す.

補題 2.12 $f\colon G \to G'$ が群同型ならば, $f^{-1}\colon G' \to G$ も群同型である.

証明

f^{-1} は明らかに全単射であるので, f^{-1} が群準同型であることを示せば十分である. つまり, $f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$ $(x, y \in G')$ を示せば良い.

$$f(f^{-1}(xy)) = xy = f(f^{-1}(x))f(f^{-1}(y)) = f(f^{-1}(x)f^{-1}(y))$$

が成り立つ. f が単射だから, $f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$ となる.

例 2.13. 指数関数 $\exp\colon (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \times)$ は群同型であり, その逆写像は $\ln\colon (\mathbb{R}_{>0}, \times) \to (\mathbb{R}, +)$ である.

2.3 剰余類

定義 2.14 G を群とし, H を G の部分群とする. $x \in G$ に対し,

$$xH := \{xh \mid h \in H\}$$
$$Hx := \{hx \mid h \in H\}.$$

とおき, それぞれ x の左剰余類, 右剰余類という.

補題 2.15 $x, x' \in G$ に対し, 以下が同値である.

(i) $xH = x'H$

(ii) $x \in x'H$

(iii) $x' \in xH$

(iv) $xH \cap x'H \neq \emptyset$

証明

(i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iv), 及び (i) $\Longrightarrow$ (iii) $\Longrightarrow$ (iv) は明らかである. 最後に, (iv) $\Longrightarrow$ (i) を示す. $y \in xH \cap x'H$ とする. このとき, $y = xh = x'h'$ となる $h, h' \in H$ が取れる. よって, 任意の $k \in H$ に対し,

$$xk = (xh)h^{-1}k = (x'h')h^{-1}k = x'(h'h^{-1}k) \in x'H$$

となる. ゆえに, $xH \subset x'H$ である. 同様の議論で x, x' の役割を交換することで, $x'H \subset xH$ が分かる. ゆえに, $xH = x'H$ である.

左剰余類全体の集合, 右剰余類全体の集合をそれぞれ G/H, $H\backslash G$ と表す.

命題 2.16 G が左剰余類に分割される. つまり, G の元の族 $\{x_i\}_{i\in I}$ が存在し,

$$G = \bigsqcup_{i\in I} x_i H \tag{2.1}$$

が成り立つ (記号 $\bigsqcup$ は共通部分を持たない和集合を意味する). 同様に, G が右剰余類に分割される.

証明

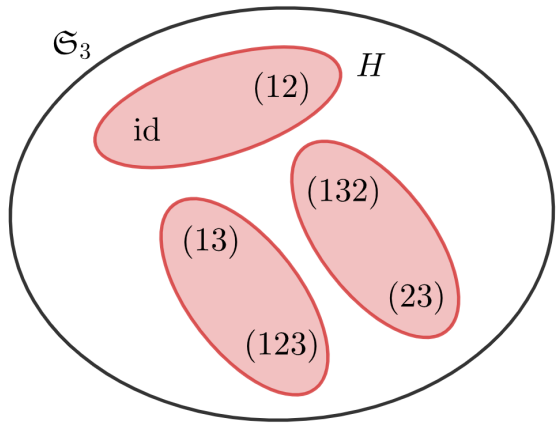
左剰余類全体の族を $(C_i)_{i\in I}$ とおく. 各 $i \in I$ に対し, 代表元 $x_i \in C_i$ を取る. とくに, $C_i = x_i H$ である. 任意の $x \in G$ に対し, $x \in xH$ であるので, $G = \bigcup_{i\in I} C_i$ である. また, 補題 2.15 により, $i \neq j$ ならば $C_i \cap C_j = \emptyset$ である. 主張が従う.

(2.1) を満たす G の元の族 $\{x_i\}_{i\in I}$ を左剰余類の代表系という. 右剰余類の代表系は同様に定義されている.

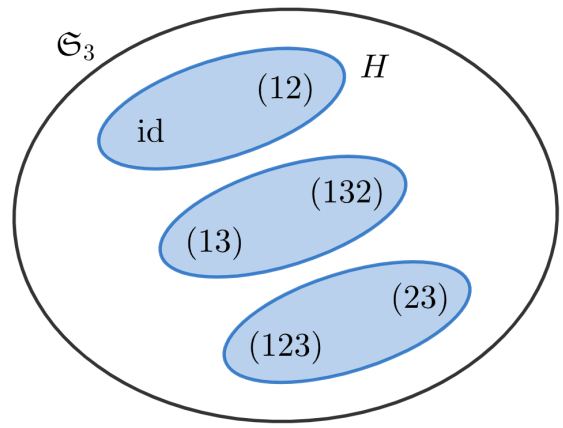
例 2.17. $G = \mathfrak{S}_3$ で, $H = \{\mathrm{id},\ (12)\}$ とする. 明らかに, H は G の部分群である. H による左剰余類, 右剰余類はそれぞれ以下の通りである.

$$\begin{aligned}
\mathrm{id}\, H &= \{\mathrm{id},\ (12)\} = (12)H = H \\
(13)H &= \{(13)\,\mathrm{id}, (13)(12)\} = \{(13), (123)\} = (123)H \\
(23)H &= \{(23)\,\mathrm{id}, (23)(12)\} = \{(23), (132)\} = (132)H
\end{aligned}$$

$$\begin{aligned}
H\,\mathrm{id} &= \{\mathrm{id},\ (12)\} = H(12) = H \\
H(13) &= \{\mathrm{id}(13), (12)(13)\} = \{(13), (132)\} = H(132) \\
H(23) &= \{\mathrm{id}(23), (12)(23)\} = \{(23), (123)\} = (123)H.
\end{aligned}$$



左剰余類



右剰余類

補題 2.18　以下の写像は well-defined であり, 全単射である.

$$\psi\colon G/H \longrightarrow H\backslash G, \quad xH \mapsto Hx^{-1}.$$

証明

- ψ が well-defined であることを示す. $xH = x'H$ $(x, x' \in G)$ のとき, $Hx^{-1} = Hx'^{-1}$ を示せば良い. 写像 $\iota\colon G \to G$, $g \mapsto g^{-1}$ による xH の像は

$$\iota(xH) = \{h^{-1}x^{-1} \mid h \in H\} = Hx^{-1}$$

  ゆえに, $Hx^{-1} = \iota(xH) = \iota(x'H) = Hx'^{-1}$ となる.
- ψ の単射性を示す. $Hx^{-1} = Hx'^{-1}$ $(x, x' \in G)$ と仮定する. このとき $\iota(xH) = \iota(x'H)$ であるので, ι の単射性より $xH = x'H$ である. よって, ψ は単射である.
- ψ の全射性を示す. $y \in G$ ならば, $\psi(y^{-1}H) = H(y^{-1})^{-1} = Hy$ である. ゆえに, ψ は全射である.

定義 2.19　G/H が有限集合のとき, H を有限指数の部分群という. G/H の元の個数を G における H の指数といい, $[G : H]$ と表す. 補題 2.18 により,

$$[G : H] = |G/H| = |H\backslash G|.$$

2.4　正規部分群・剰余群

定義 2.20　G を群とし, $H \subset G$ を部分群とする. H が正規部分群であるとは,

$$g \in G,\ h \in H \quad \Longrightarrow \quad ghg^{-1} \in H.$$

が成り立つことをいう. このとき, $H \triangleleft G$ と表す.

$g \in G$ に対し,

$$gHg^{-1} := \{ghg^{-1} \mid h \in H\}$$

とおく. gHg^{-1} は G の部分群であることは容易に確認できる. H が正規部分群であることは, 任意の $g \in G$ に対し $gHg^{-1} \subset H$ であることを意味する. このとき, g と g^{-1} を入れ替えて, $g^{-1}Hg \subset H$ も成り立つ. ゆえに,

$H \subset gHg^{-1}$ である. まとめると, 以下が成り立つ.

$$\begin{aligned} H \text{ が } G \text{ の正規部分群である} &\iff \text{任意の } g \in G \text{ に対し, } gHg^{-1} = H \\ &\iff \text{任意の } g \in G \text{ に対し, } gH = Hg. \end{aligned}$$

例 2.21.

- $\{e\}$ と G は G の正規部分群である.
- $Z(G) \subset G$ を G の中心とし, H を $Z(G)$ に含まれる部分群とする. このとき, H が G の正規部分群である. 実際, このとき $g \in G$, $h \in H$ に対し $ghg^{-1} = gg^{-1}h = h \in H$ である.
- G がアーベル群ならば, G の全ての部分群が正規部分群である.

命題 2.22 $f\colon G \to G'$ を群準同型とする. このとき, $\mathrm{Ker}(f)$ は G の正規部分群である. また, $H' \subset G'$ が G' の正規部分群ならば, $H := f^{-1}(H')$ は G の正規部分群である.

証明

$H' \triangleleft G'$ とし, $H := f^{-1}(H')$ とおく. $g \in G$, $h \in H$ のとき,

$$f(ghg^{-1}) = f(g)f(h)f(g)^{-1}$$

である. $f(h) \in H'$ であるので, 正規性より $f(g)f(h)f(g)^{-1} \in H'$ である. ゆえに $ghg^{-1} \in H$ となり, H が正規部分群である. $\mathrm{Ker}(f) = f^{-1}(\{e\})$ であるので, 正規部分群である.

H を G の正規部分群とする. このとき, 左剰余類全体の集合 G/H に自然な演算を入れることができる. $g, g' \in G$ に対し,

$$(gH)(g'H) := (gg')H \tag{2.2}$$

とおくことで, G/H の演算を定義する. この演算が well-defined であることを確認しよう. 結果が剰余類の代表元の取り方に依らないことを示せば良い. $g_1, g_2, g_1', g_2' \in G$ で, $g_1H = g_2H$, $g_1'H = g_2'H$ とする. このとき, $g_1g_2H = g_1'g_2'H$ を示せば良い. G の元 g, g' に対し,

$$gHg' := \{ghg' \mid h \in H\}$$

とおくことで部分集合 gHg' を定義する (一般には部分群でない). H の正規性より, 以下が成り立つ.

$$g_1g_1'H = g_1g_2'H = g_1Hg_2' = g_2Hg_2' = g_2g_2'H.$$

ゆえに, (2.2) で定まる G/H の演算は well-defined である.

命題 2.23

(1) この演算に関して G/H は群をなす.
(2) $\pi(x) = xH$ で定まる写像 $\pi\colon G \to G/H$ は群準同型である.
(3) $\mathrm{Ker}(\pi) = H$ である.

証明

- 結合法則は容易に確認できる. また, $eH = H$ は明らかに単位元である. 最後に, $x \in G$ のとき $(xH)(x^{-1}H) = (x^{-1}H)(xH) = eH = H$ であるので, 全ての元が可逆元である.
- $x, y \in G$ のとき, $\pi(xy) = xyH = (xH)(yH) = \pi(x)\pi(y)$ であり, π は群準同型である.
- $\pi(x) = H \iff xH = H \iff x \in H$ である.

π は「自然な射影」と呼ばれる.

命題 2.24　G を群とし, H を G の部分群とする. $[G:H]=2$ ならば, H が G の正規部分群である.

証明

$g \notin H$ とする. 仮定より $G = H \sqcup gH = H \sqcup Hg$ が成り立つ. ゆえに $gH = Hg$ である. よって, H が正規部分群である.

2.5　準同型定理

定理 2.25: (準同型定理)　$f\colon G \to G'$ を群準同型とする. このとき, 写像

$$\widetilde{f}\colon G/\operatorname{Ker}(f) \to \operatorname{Im}(f), \quad x\operatorname{Ker}(f) \mapsto f(x)$$

は well-defined であり, 群同型写像である.

証明

- $\widetilde{f}$ が well-defined であることを示す. $x\operatorname{Ker}(f) = y\operatorname{Ker}(f)$ $(x,y \in G)$ のとき, $f(x)=f(y)$ を示せば良い. $y = xz$ となる $z \in \operatorname{Ker}(f)$ が存在する. ゆえに, $f(y) = f(xz) = f(x)f(z) = f(x)e' = f(x)$ となる.
- $\widetilde{f}$ が単射であることを示す. $f(x)=f(y)$ $(x,y \in G)$ と仮定する. $z = x^{-1}y$ とおくと, $f(z) = f(x^{-1})f(y) = f(x)^{-1}f(y) = e'$ となる. よって, $z \in \operatorname{Ker}(f)$ である. $y = xz$ より, $x\operatorname{Ker}(f) = y\operatorname{Ker}(f)$ である.
- $\widetilde{f}$ が全射であることと, 群準同型写像であることは明らかである. 以上より, $\widetilde{f}$ は群同型である.

注意 2.26.　$f\colon G \to G'$ を群準同型とする. $\iota\colon \operatorname{Im}(f) \to G'$ を自然な包含写像とし, $\pi\colon G \to G/\operatorname{Ker}(f)$ を自然な射影とする. また, $\widetilde{f}\colon G/\operatorname{Ker}(f) \to \operatorname{Im}(f)$ を準同型定理で与えられた群同型写像とする. このとき, $f = \iota \circ \widetilde{f} \circ \pi$ と分解できる.

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & G' \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ G/\operatorname{Ker}(f) & \xrightarrow[\widetilde{f}]{} & \operatorname{Im}(f) \end{array}$$

例 2.27.　$f\colon \mathbb{R} \to \mathbb{C}^*$, $x \mapsto \exp(2i\pi x)$ を考える. 明らかに, f は $(\mathbb{R},+)$ から $(\mathbb{C}^*,\times)$ への準同型である. また, f の像は $U = \{z \in \mathbb{C} \mid |z| = 1\}$ であり, f の核は $\mathbb{Z}$ である. よって群同型

$$\mathbb{R}/\mathbb{Z} \simeq U, \quad x + \mathbb{Z} \mapsto \exp(2i\pi x)$$

が存在する.

系 2.28　$f\colon G \to G'$ を全射準同型とし, $H' \subset G'$ を正規部分群とする. このとき, $H = f^{-1}(H')$ で, 群同型

$$G/H \simeq G'/H', \qquad gH \mapsto f(g)H'$$

が存在する.

証明

$\pi' \colon G' \to G'/H'$ を自然な射影とし, $\alpha \colon \pi' \circ f$ とおく. f が全射より, α も全射である. $\mathrm{Ker}(\alpha) = f^{-1}(H') = H$ であるので, 準同型定理により

$$G/H \to G'/H', \quad gH \mapsto \alpha(g) = f(g)H'$$

が存在する.

2.6 自己準同型群

G を群とする. G の自己同型 $G \to G$ 全体の集合を $\mathrm{Aut}(G)$ で表す. $f, f' \colon G \to G$ が G の自己同型ならば, $f \circ f'$ も自己準同型である. また, 補題 2.12 により f^{-1} も自己同型である. ゆえに, $\mathrm{Aut}(G)$ は $\mathfrak{S}(G)$ の部分群をなす. $\mathrm{Aut}(G)$ は G の自己同型群と呼ばれる. $g \in G$ とする. $x \in G$ に対し $\varphi_g(x) = gxg^{-1}$ とおくことによって, 写像

$$\varphi_g \colon G \to G$$

を定める. $x, y \in G$ に対し $\varphi_g(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = \varphi_g(x)\varphi_g(y)$ であるので, φ_g は準同型写像である. また,

$$\varphi_g \circ \varphi_{g^{-1}} = \varphi_{g^{-1}} \circ \varphi_g = \mathrm{id}_G$$

が成り立つので, φ_g は全単射であり, G の自己同型である. φ_g $(g \in G)$ という形の自己同型を G の内部自己同型という. $g, g' \in G$ に対し,

$$\varphi_{gg'} = \varphi_g \circ \varphi_{g'}$$

である. ゆえに, 写像 $\varphi \colon G \to \mathrm{Aut}(G)$, $g \mapsto \varphi_g$ は群準同型である. φ の像を $\mathrm{Inn}(G)$ とおき, G の内部自己同型群という. また,

$$\begin{aligned}
\mathrm{Ker}(\varphi) &= \{g \in G \mid \varphi_g = \mathrm{id}_G\} \\
&= \{g \in G \mid \text{全ての } x \in G \text{ に対し}, gxg^{-1} = x\} \\
&= \{g \in G \mid \text{全ての } x \in G \text{ に対し}, gx = xg\} \\
&= Z(G)
\end{aligned}$$

が成り立つ. ゆえに, 準同型定理により, 以下のような同型写像が存在する.

$$G/Z(G) \simeq \mathrm{Inn}(G).$$

$\mathrm{Inn}(G)$ に属さない G の自己同型を G の外部自己同型という.

補題 2.29 $\mathrm{Inn}(G)$ が $\mathrm{Aut}(G)$ の正規部分群である.

証明

$\sigma \in \mathrm{Aut}(G)$ とする. このとき, 任意の $g, x \in G$ に対し,

$$\begin{aligned}
(\sigma \circ \varphi_g \circ \sigma^{-1})(x) &= \sigma(g\sigma^{-1}(x)g^{-1}) \\
&= \sigma(g)\sigma(\sigma^{-1}(x))\sigma(g)^{-1} \\
&= \sigma(g)x\sigma(g)^{-1} \\
&= \varphi_{\sigma(g)}(x).
\end{aligned}$$

よって, $\sigma \circ \varphi_g \circ \sigma^{-1} = \varphi_{\sigma(g)}$ が成り立つ. とくに, $\sigma \circ \varphi_g \circ \sigma^{-1} \in \mathrm{Inn}(G)$ である.

例 2.30. $G = \mathbb{Z}/n\mathbb{Z}$ の自己同型群について考える．以下の群同型が存在することを示す．

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^{\times}. \tag{2.3}$$

まず, $k \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ に対し, $f_k(m) = km$ $(m \in \mathbb{Z}/n\mathbb{Z})$ とおくことによって, 写像 $f_k \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ を定める．k が可逆元であるので, f_k は明らかに $\mathbb{Z}/n\mathbb{Z}$ の自己同型である．また, $f_{kk'} = f_k \circ f_{k'}$ $(k, k' \in (\mathbb{Z}/n\mathbb{Z})^{\times})$ より, 写像 $k \mapsto f_k$ は群準同型 $(\mathbb{Z}/n\mathbb{Z})^{\times} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ である．明らかに, $k \mapsto f_k$ は単射である．最後に, 全射性について考える．$f \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ とする．$\overline{1}$ が $\mathbb{Z}/n\mathbb{Z}$ の生成元だから, 系 2.6 により $f(\overline{1})$ も生成元である．ゆえに, $f(\overline{1}) = k$, $k \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ である．よって, 任意の $m \in \mathbb{Z}/n\mathbb{Z}$ に対し, $f(m) = mf(\overline{1}) = km$ である．したがって, $f = f_k$ となり, 主張が従う．

2.7 導来部分群

G を群とする．

定義 2.31 $x, y \in G$ に対し, $[x, y] := xyx^{-1}y^{-1}$ とおき, x と y との交換子という．交換子全体の集合で生成される部分群を G の導来部分群といい, $D(G)$ または $[G, G]$ と表す．

$$x, y \text{ が交換する} \quad \Longleftrightarrow \quad [x, y] = e \tag{2.4}$$

が成り立つことに注意する．

命題 2.32

(1) $D(G)$ を含む任意の部分群 H は G の正規部分群であり, 剰余群 G/H はアーベル群である．

(2) 逆に, $H \subset G$ を正規部分群とし, G/H がアーベル群であるとする．このとき, $D(G) \subset H$ である．

証明

- $D(G) \subset H$ とする．$g \in G$, $h \in H$ とする．仮定より, $[g, h] = ghg^{-1}h^{-1} \in H$ である．よって, $ghg^{-1} = [g, h]h \in H$ となり, ゆえに H が正規部分群である．$g \in G$ に対し, $\overline{g} := gH$ とおく．$g \mapsto \overline{g}$ が群準同型 $G \to G/H$ であるので, $g, g' \in G$ に対し, $[\overline{g}, \overline{g'}] = \overline{[g, g']}$ である．$[g, g'] \in H$ より, $\overline{[g, g']} = \overline{e}$ となる．したがって, $[\overline{g}, \overline{g'}] = \overline{e}$ となり, (2.4) により $\overline{g}$ と $\overline{g'}$ が交換する．
- 自然な射影 $\pi \colon G \to G/H$, $g \mapsto \overline{g}$ を考える．任意の $g, h \in G$ に対し $\pi([g, g']) = [\overline{g}, \overline{g'}] = \overline{e}$ である．ゆえに, $[g, g'] \in \mathrm{Ker}(\pi) = H$ となる．よって, $D(G) \subset H$ である．

$G/D(G)$ は群 G のアーベル化と呼ばれ, G^{ab} と表される．

定義 2.33 H を G の部分群とする．H が特性部分群であるとは, G の任意の自己同型 $\varphi \colon G \to G$ に対し $\varphi(H) \subset H$ であることをいう．

また, このとき仮定より $\varphi^{-1}(H) \subset H$ も成り立つので, $\varphi(H) = H$ となる．H が特性部分群ならば, 正規部分群でもある．なぜならば, $g \in G$ とし, 内部自己同型 $\varphi_g \colon x \mapsto gxg^{-1}$ を考える．仮定より $\varphi_g(H) = gHg^{-1} = H$ であるので, H が正規である．

命題 2.34 $D(G)$ は G の特性部分群である．

証明

$\varphi\colon G \to G$ を自己同型とし, $g, h \in G$ とする. このとき, $\varphi([g,h]) = [\varphi(g), \varphi(h)]$ が成り立つ. よって, $\varphi(D(G)) \subset D(G)$ である.

3 位数

3.1 定義

定義 3.1 G を有限群とする. G の位数とは, G の元の個数のことである.

定義 3.2 G を群とし, $x \in G$ とする.
(a) 部分群 $\langle x \rangle$ が有限ならば, $\mathrm{ord}(x) = |\langle x \rangle|$ とおき, x の位数という.
(b) 部分群 $\langle x \rangle$ が無限ならば, x の位数が無限であるという.

命題 3.3 x の位数が $n \in \mathbb{N}$ であるとする. このとき,

$$\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}$$

が成り立つ (ただし, $e, x, \ldots, x^{n-1}$ は相異なる). さらに, $\langle x \rangle \simeq \mathbb{Z}/n\mathbb{Z}$ である.

証明

写像 $\varphi\colon \mathbb{Z} \to G$, $k \mapsto x^k$ を考える. 明らかに φ は群 $(\mathbb{Z}, +)$ から G への準同型である. $\mathrm{Im}(\varphi) = \langle x \rangle$ である. $\mathrm{Ker}(\varphi)$ は $\mathbb{Z}$ の部分群であるので, $\mathrm{Ker}(\varphi) = m\mathbb{Z}$ となる $m \in \mathbb{Z}_{\geq 0}$ が存在する. 準同型定理により同型写像 $\mathbb{Z}/m\mathbb{Z} \simeq \langle x \rangle$ が存在する. とくに $n = |\langle x \rangle| = |\mathbb{Z}/m\mathbb{Z}| = m$ となる. $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$ より, $\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}$ である.

系 3.4 x の位数が $n \in \mathbb{N}$ であるとする. このとき, 任意の整数 $m \in \mathbb{Z}$ に対し, 以下が成り立つ.

$$x^m = e \iff n \mid m.$$

証明

準同型 $\varphi\colon \mathbb{Z} \to \langle x \rangle$, $k \mapsto x^k$ を考える. 命題 3.3 により $\mathrm{Ker}(\varphi) = \{m \in \mathbb{Z} \mid x^m = e\} = n\mathbb{Z}$ である. 主張が従う.

例 3.5. $G = \mathrm{GL}_2(\mathbb{C})$ とし, $x = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$, $y = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ とする.

$$x^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \quad x^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

より, x の位数は 3 である. 同様に, $y^2 = -E_2$, $y^3 = -y$, $y^4 = E_2$ より y の位数は 4 である. 一方,

$$xy = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

より, xy の位数は無限である.

$n, m \in \mathbb{Z}$ とする．このとき，$n\mathbb{Z} + m\mathbb{Z}$ が $\mathbb{Z}$ の部分群であるので，$n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$ を満たす $d \geq 0$ が一意的に存在する．$d = \gcd(n, m)$ とおき，n, m の最大公約数という．

命題 3.6　x が位数 $n \in \mathbb{N}$ の元とする．このとき，任意の $k \in \mathbb{Z}$ に対し，

$$\mathrm{ord}(x^k) = \frac{n}{\gcd(k, n)}$$

である．とくに，$k \geq 1$ が n の約数ならば，$\mathrm{ord}(x^k) = \frac{n}{k}$ である．

証明

$d = \gcd(k, n)$ とおく．$n = dn'$，$k = dk'$ となる互いに素な整数 n', k' が存在する．とくに $kn' = k'n$ である．ゆえに，

$$(x^k)^{n'} = x^{kn'} = x^{k'n} = e$$

である．ゆえに，$\mathrm{ord}(x^k) \mid n'$ である．逆に，$(x^k)^m = e$ ならば，$x^{km} = e$ となり，ゆえに $n \mid km$ である．よって，$n' \mid k'm$ となる．n'，k' が互いに素だから，$n' \mid m$ となる．とくに，$m = \mathrm{ord}(x^k)$ とおけば，$n' \mid \mathrm{ord}(x^k)$ がいえる．以上より，

$$\mathrm{ord}(x^k) = n' = \frac{n}{\gcd(k, n)}.$$

命題 3.7　$x, y \in G$ が交換する元で，$n = \mathrm{ord}(x)$ と $m = \mathrm{ord}(y)$ が互いに素であるとする．このとき，$\mathrm{ord}(xy) = nm$ である．

証明

x, y が交換するので，$(xy)^{mn} = x^{mn}y^{mn} = e$ である．また，$(xy)^k = e$ とすると，

$$e = (xy)^{km} = x^{km}y^{km} = x^{km}$$

である．ゆえに，$n \mid km$ となる．$\gcd(n, m) = 1$ より，$n \mid k$ である．同様に，$m \mid k$ であることが分かる．n と m が互いに素だから，$nm \mid k$ となる．とくに，$nm \mid \mathrm{ord}(xy)$ である．以上より，$\mathrm{ord}(xy) = nm$ が成り立つ．

3.2　ラグランジュの定理

定理 3.8: (ラグランジュ定理)　G を有限群とし，H を G の部分群とする．このとき

$$|G| = |H| \cdot [G : H]$$

が成り立つ．

証明

$\{x_1, \ldots, x_m\}$ を左剰余類の代表系とする．とくに，$m = [G : H]$ である．このとき

$$G = \bigsqcup_{i=1}^{m} x_i H$$

である．ゆえに，$|G| = \sum_{i=1}^{m} |x_i H|$ が成り立つ．次に，任意の $x \in G$ に対し，$|H| = |xH|$ であること

を示す．写像 $\gamma\colon H \to xH$, $h \mapsto xh$ は明らかに全射である．また, $xh = xh'$ ならば x^{-1} をかけることによって $h = h'$ が導ける．ゆえに, γ は全単射であり, とくに $|H| = |xH|$ が成り立つ．したがって, $|G| = m|H|$ となり, 主張が従う．

系 3.9　G を有限群とし, $|G| = n$ とおく．このとき, 任意の $x \in G$ に対し $x^n = e$ が成り立つ．

証明

$H = \langle x \rangle$ とおき, $d = |H|$ とおく．ラグランジュ定理により, $\mathrm{ord}(x) = d$ は n の約数である．系 3.4 により $x^n = e$ である．

例 3.10. $G = (\mathbb{Z}/n\mathbb{Z})^\times$ とする．G が位数 $\varphi(n)$ のアーベル群である．但し, φ はオイラー関数である．系 3.9 により全ての $x \in G$ に対し, $x^{\varphi(n)} = \overline{1}$ が成り立つ．すなわち, $\gcd(k, n) = 1$ を満たす任意の整数 $k \in \mathbb{Z}$ に対し,

$$k^{\varphi(n)} \equiv 1 \pmod{n}$$

が成り立つ．とくに, $n = p$ が素数のとき, フェルマーの小定理が得られる．つまり, p で割り切れない任意の整数 k に対し, $k^{p-1} \equiv 1 \pmod{p}$ である．

3.3　巡回群

定理 3.11　G を巡回群とする．
(1) G が有限ならば, $G \simeq \mathbb{Z}/n\mathbb{Z}$ である (ただし, $n = |G|$ である)．
(2) G が無限ならば, $G \simeq \mathbb{Z}$ である．

証明

(1) は命題 3.3 から分かる．(2) を示す．$G = \langle x \rangle$ となる $x \in G$ が取れる．準同型 $\varphi\colon \mathbb{Z} \to G$, $k \mapsto x^k$ を考える．φ は全射であるので, $\mathbb{Z}/\mathrm{Ker}(\varphi) \simeq G$ である．G が無限だから, $\mathrm{Ker}(\varphi) = 0$ となる．したがって, $G \simeq \mathbb{Z}$ である．

命題 3.12　G を位数 n の巡回群とする．
(1) $H \subset G$ が部分群ならば, H が巡回群である．
(2) 対応 $H \mapsto |H|$ によって, G の部分群は n の正の約数に一対一に対応している．

証明

- $x \in G$ を生成元とし, 準同型 $\phi\colon \mathbb{Z} \to G$, $k \mapsto x^k$ を考える．$\phi^{-1}(H)$ が $\mathbb{Z}$ の部分群だから, $\phi^{-1}(H) = m\mathbb{Z}$ $(m \in \mathbb{N})$ と表せる．ϕ が全射だから,

$$H = \phi(\phi^{-1}(H)) = \phi(m\mathbb{Z}) = \langle x^m \rangle \tag{3.1}$$

  である．ゆえに, H は巡回群である．
- 以下の写像が全単射であることを示す．

$$\{G \text{ の部分群 }\} \to \{n \text{ の正の約数 }\}, \quad H \mapsto |H|. \tag{3.2}$$

  まず, 全射性について考える．d を n の正の約数とする．$m = n/d$ とおくと, 命題 3.6 により $\mathrm{ord}(x^m) = d$ である．よって, $H := \langle x^m \rangle$ は位数 d の部分群であり, 写像 (3.2) は全射である．

最後に, 単射性について考える. H' を位数 d の部分群とし, $m = \frac{n}{d}$ とおく. $\phi^{-1}(H') = r\mathbb{Z}$ となる $r \geq 1$ が存在する. $n\mathbb{Z} \subset \phi^{-1}(H')$ より, r は n の約数である. $H' = \phi(r\mathbb{Z}) = \langle x^r \rangle$ より, $|H'| = d = n/r$, すなわち $r = m$ が成り立つ. したがって, $\langle x^m \rangle$ は位数 d の唯一の部分群である.

命題 3.13 G の位数が素数であるとする. このとき, G は巡回群である.

証明

$x \in G \setminus \{e\}$ で, $H = \langle x \rangle$ とおく. $|H|$ が $|G|$ の約数であり, かつ $|H| > 1$ であるので, $|H| = |G|$ となる. よって, $G = H$ である.

定理 3.14 p を奇素数とする. このとき, $(\mathbb{Z}/p^m\mathbb{Z})^\times$ $(m \geq 1)$ は巡回群である.

証明

レポート 1 参照.

4 群作用

4.1 定義

G を群とし, X を空でない集合とする. 写像 $f\colon G \times X \to X$ が与えられているとする. $g \in G$, $x \in X$ に対し, $f(g, x)$ を単に $g \cdot x$ または gx と表す. G の単位元を e とおく.

定義 4.1 以下が成り立つとき, f が G の X への群作用であるという.

- $g \cdot (g' \cdot x) = (gg') \cdot x, \quad g, g' \in G, x \in X.$
- $e \cdot x = x, \quad x \in X.$

G が X に作用しているとする. このとき, 写像 $\rho(g)\colon X \to X$, $x \mapsto g \cdot x$ は全単射であることに注意する. なぜならば, 定義 4.1 を言い換えれば

- $\rho(gg') = \rho(g) \circ \rho(g'), \quad g, g' \in G.$
- $\rho(e) = \mathrm{id}_X$

である. このことから, $\rho(g) \circ \rho(g^{-1}) = \rho(g^{-1}) \circ \rho(g) = \mathrm{id}_X$ である. ゆえに $\rho(g)$ は全単射である. また, $g \mapsto \rho(g)$ で定まる写像

$$\rho\colon G \to \mathfrak{S}(X)$$

は群準同型である. 逆に, 群準同型 $\rho\colon G \to \mathfrak{S}(X)$ が与えられているとき, 写像 $(g, x) \mapsto \rho(g)(x)$ は定義 4.1 の条件を満たすので, 群作用が定まる.

定義 4.2

(a) $\rho\colon G \to \mathfrak{S}(X)$ が単射であるとき, 作用が忠実であるという.

(b) 任意の $x, y \in X$ に対し $g \in G$ が存在し, $g \cdot x = y$ であるとき, 作用が推移的であるという.

4.2　群作用の例

■自明作用　G を群, X を集合とする. 全ての $g \in G$, $x \in X$ に対し, $g \cdot x = x$ とおくと, G の X への群作用が定まる. この作用は自明作用と呼ばれ, 自明準同型 $G \to \mathfrak{S}(X)$, $g \mapsto \mathrm{id}_X$ に対応している. $|X| > 1$ のとき推移的でない. $|G| > 1$ のとき忠実でない.

■左移動作用　G を群とする. $g, h \in G$ に対し,

$$g \cdot h = gh$$

とおくことによって, G の自分自身への作用が定まる. この作用は「左移動による作用」と呼ばれる. 明らかに推移的な作用である. 実際, $h_1, h_2 \in G$ ならば, $g = h_2 h_1^{-1}$ とおくと $g \cdot h_1 = h_2$ である. この作用で定まる群準同型 $\rho\colon G \to \mathfrak{S}(G)$ を考える. $g \in \mathrm{Ker}(\rho)$ ならば, 任意の $h \in G$ に対し, $g \cdot h = h$ であり, すなわち $gh = h$ である. h の逆元を両辺にかけて, $g = e$ となる. 従って, 作用は忠実である.

今, G が有限群であるとし, $n = |G|$ とおく. 忠実性より, 単射群準同型

$$\rho\colon G \to \mathfrak{S}(X) \simeq \mathfrak{S}_n$$

が得られる. したがって, 以下の定理が分かる.

定理 4.3　G が位数 n の群ならば, G と同型である $\mathfrak{S}_n$ の部分群が存在する.

$\mathfrak{S}_n$ は位数 $n!$ の群であることに注意する.

■右移動作用　G を群とする. $g, h \in G$ に対し,

$$g \cdot h = hg^{-1}$$

とおくことによって, G の自分自身への作用が定まる. この作用は「右移動による作用」と呼ばれ, 左移動と同じ性質を持つ.

■共役作用　$g, h \in G$ に対し,

$$g \cdot h := ghg^{-1}$$

とおくことによって, G の自分自身への群作用が定まる. この作用を「G の共役による作用」という. この作用に対応する群準同型

$$\rho\colon G \to \mathfrak{S}(G), \quad g \mapsto (h \mapsto ghg^{-1})$$

の像は G の自己同型群 $\mathrm{Aut}(G) \subset \mathfrak{S}(G)$ に含まれる. さらに, ρ は §2.6 で定義された群準同型 $G \to \mathrm{Aut}(G)$ に一致する. とくに, $\mathrm{Ker}(\rho) = Z(G)$ が成り立つ.

■部分群の共役　群 G の 2 つの部分群 H, H' が共役であるとは, $H' = gHg^{-1}$ $(g \in G)$ と表せるときにいう. X を G の部分群全体のなす集合とする. $g \in G$, $H \in X$ に対し,

$$g \cdot H := gHg^{-1}$$

とおくことによって, G の X への作用が定まる.

■左剰余類への作用　H を G の部分群とする. $g, x \in G$ に対し, $g \cdot (xH) := gxH$ とおくことで, G の G/H への作用が定まる. この作用は明らかに推移的である.

■作用の制限　群 G が集合 X に作用しているとする. H を G の部分群とする. このとき, $H \times X \to X$, $(h, x) \mapsto h \cdot x$ は H の X への作用である.

一方, $Y \subset X$ を部分集合とする. 任意の $g \in G$ 及び $y \in Y$ に対し $g \cdot y \in Y$ が成り立つと仮定する. このとき, $G \times Y \to Y$, $(g, y) \mapsto g \cdot y$ は G の Y への作用である.

4.3 軌道

群 G が集合 X に作用しているとする. $x, y \in X$ とする. このとき,

$$x \sim y \quad \Longleftrightarrow \quad g \in G \text{ が存在し, } y = g \cdot x$$

とおくことで, X 上の同値関係「$\sim$」が定まる. 実際, 任意の $x, y, z \in X$, $g, g' \in G$ に対し, 以下が成り立つ.

- 反射性：$x = e \cdot x$ より $x \sim x$ である.
- 対称性：$y = g \cdot x$ ならば, $g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$ となる. よって, 「$x \sim y$」 $\Longrightarrow$ 「$y \sim x$」が成り立つ.
- 推移性：$y = g \cdot x$ かつ $z = g' \cdot y$ ならば, $z = g' \cdot (g \cdot x) = (g'g) \cdot x$ となる. ゆえに, 「$x \sim y$」かつ「$y \sim z$」 $\Longrightarrow$ 「$x \sim z$」が成り立つ.

定義 4.4 G による x の軌道とは,

$$Gx = \{g \cdot x \mid g \in G\}$$

で定まる X の部分集合のことをいう.

言い換えれば, x の起動は同値関係「$\sim$」に関する x の同値類にほかならない. とくに, 以下の命題が同値関係の一般的な性質から従う.

命題 4.5 X が軌道に分割される. つまり, $(X_i)_{i \in I}$ を G による全ての軌道とすると, 以下が成り立つ.

$$X = \bigsqcup_{i \in I} X_i \qquad \text{(共通部分のない和集合).}$$

G による軌道全体の集合を X/G とおく. X の元の族 $\{x_i\}_{i \in I}$ が軌道の代表系であるとは, 任意の軌道 $Y \subset X$ に対し $Y = Gx_i$ を満たす $i \in I$ が一意に存在するときにいう. 言い換えれば, 各軌道の中から一つの元を選び, それらの元を集めた集合のことである.

例 4.6. $\mathbb{K}$ を可換体とし, $G = \mathrm{GL}_2(\mathbb{K})$ とおく. G が $\mathrm{M}_2(\mathbb{K})$ に共役により作用している (つまり, $P \in \mathrm{GL}_2(\mathbb{K})$, $M \in \mathrm{M}_2(\mathbb{K})$ に対し, $P \cdot M = PMP^{-1}$ で定まる作用). このとき, 有理標準形の存在定理より, 以下の集合は軌道の代表系をなす.

$$\left\{ \begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix} \;\middle|\; a, b \in \mathbb{K} \right\} \cup \{\lambda E_2 \mid \lambda \in \mathbb{K}\}.$$

例 4.7. G を群とし, $H \subset G$ を部分群とする. H の G への右移動による作用 (すなわち, $h \in H$, $g \in G$ に対し $h \cdot g := hg^{-1}$ で定まる作用) を考える. このとき, $g \in G$ に対し, g の H による起動は左剰余類

$$gH = \{gh \mid h \in H\}$$

に他ならない.

4.4 安定化部分群

定義 4.8 $x \in X$ に対し,

$$G_x = \{g \in G \mid g \cdot x = x\}$$

とおき, x の安定化部分群という.

G_x が G の部分群であることを示す．明らかに $e \in G_x$ である．$g, g' \in G_x$ ならば，$(gg') \cdot x = g \cdot (g' \cdot x) = g \cdot x = x$ となり，$gg' \in G_x$ である．最後に，$g \in G_x$ とする．このとき，$g \cdot x = x$ より $g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$ である．ゆえに $g^{-1} \in G_x$ が成り立つ．以上より G_x は G の部分群である．

命題 4.9　$y = g \cdot x$ $(g \in G)$ とする．このとき，$G_y = gG_xg^{-1}$ が成り立つ．

証明

任意の $h \in G$ に対し，

$$\begin{aligned} h \in G_y &\iff h \cdot y = y \\ &\iff h \cdot (g \cdot x) = g \cdot x \\ &\iff (hg) \cdot x = g \cdot x \\ &\iff (g^{-1}hg)h \cdot x = x \\ &\iff g^{-1}hg \in G_x \\ &\iff h \in gG_xg^{-1}. \end{aligned}$$

例 4.10. G の自分自身への共役による作用を考える．このとき，$x \in G$ の安定化部分群は以下の部分群である．

$$\begin{aligned} G_x &= \{g \in G \mid gxg^{-1} = x\} \\ &= \{g \in G \mid gx = xg\}. \end{aligned}$$

つまり，G_x は x と交換する元全体の部分群である．この部分群を x の中心化群といい，$\mathrm{Cent}_G(x)$ と表す．

例 4.11. G を群とし，$X = \{G \text{ の部分群 }\}$ とする．G が共役により X に作用している (§4.2 参照)．このとき，部分群 $H \subset G$ の安定化部分群は H の正規化群といい，$N_G(H)$ と表す．すなわち，

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}$$

である．明らかに，$H \subset N_G(H)$ である．また，$H \triangleleft N_G(H)$ である．

命題 4.12　G が X に作用しているとする．

$$\text{作用が忠実である} \iff \bigcap_{x \in X} G_x = \{e\}$$

が成り立つ．

証明

G の X への作用に対応する準同型を $\rho\colon G \to \mathfrak{S}(X)$ とおく．このとき，

$$\begin{aligned} \mathrm{Ker}(\rho) &= \{g \in G \mid \text{任意の } x \in X \text{ に対し } g \cdot x = x\} \\ &= \{g \in G \mid \text{任意の } x \in X \text{ に対し } g \in G_x\} \\ &= \bigcap_{x \in X} G_x \end{aligned}$$

である．主張が従う．

命題 4.13　G が X に作用しているとする．$x \in X$ に対し，写像

$$\alpha\colon G/G_x \to Gx, \quad gG_x \mapsto g \cdot x$$

は well-defined であり，全単射である．

証明

- α が well-defined であることを示す．$gG_x = g'G_x$ $(g, g' \in G)$ のとき，$g \cdot x = g' \cdot x$ を示せば良い．仮定より，$g' = gh$ となる $h \in G_x$ が存在する．よって，$g' \cdot x = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot x$ となる．よって，α は well-defined である．
- α が単射であることを示す．$g \cdot x = g' \cdot x$ を仮定する．$h = g^{-1}g'$ とおくと，$h \cdot x = g^{-1} \cdot (g' \cdot x) = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x$ である．よって，$h \in G_x$ である．したがって，$g' = gh$ より $g'G_x = gG_x$ である．ゆえに，α は単射である．
- α が全射であるのは明らかである．

定理 4.14　有限群 G が有限集合 X に作用しているとする．$\{x_1, \ldots, x_m\}$ を X の軌道の代表系とする．このとき，以下が成り立つ．

$$|X| = \sum_{i=1}^{m} [G : G_{x_i}].$$

証明

$X_i = Gx_i$ とおくと，命題 4.5 により，$X = X_1 \sqcup \cdots \sqcup X_m$ である．よって，$|X| = \sum_{i=1}^{m} |X_i|$ である．さらに，命題 4.13 により全単射 $G/G_{x_i} \to X_i$ が存在するので，$|X_i| = |G/G_{x_i}| = [G : G_{x_i}]$ である．主張が従う．

任意の $g \in G$ に対し $g \cdot x = x$ が成り立つとき，x が X の固定点であるという．以下の条件が互いに同値である．

(i)　x が固定点である．

(ii)　$G_x = G$ である．

(iii)　$Gx = \{x\}$.

X の固定点全体の集合を X^G と表す．有限群 G が有限集合 X に作用しているとし，$\{x_1, \ldots, x_m\}$ を軌道の代表系とする．定理 4.14 により $|X| = \sum_{i=1}^{m} [G : G_{x_i}]$ である．また，x_i が固定点ならば，$G_{x_i} = G$ より $[G : G_{x_i}] = 1$ である．よって，

$$|X| = |X^G| + \sum_{x_i \notin X^G} [G : G_{x_i}]. \tag{4.1}$$

4.5　バーンサイドの補題

G を有限群とし，G が有限集合 X に作用しているとする．$g \in G$ に対し，

$$X^g := \{x \in X \mid g \cdot x = x\}$$

とおく．つまり，X^g は g で固定される X の元全体の集合である．バーンサイドの補題と呼ばれる以下の結果は，軌道の個数の公式を与えるものである．

定理 4.15: バーンサイドの補題

$$|X/G| = \frac{1}{|G|}\sum_{g\in G}|X^g| \qquad \text{である.}$$

証明

X_1, X_2 を共通部分を持たない 2 つの部分集合で, G の作用によって保たれているものとする. つまり, 任意の $x \in X_i$, $g \in G$ に対し $g\cdot x \in X_i$ であるとする $(i = 1, 2)$. このとき, $(X_1 \sqcup X_2)/G = (X_1/G) \sqcup (X_2/G)$ かつ $X^g = X_1^g \sqcup X_2^g$ と書けるので, 定理の出張が X_1 及び X_2 の場合に成り立つならば, $X_1 \sqcup X_2$ の場合にも成り立つ. X が軌道に分割されるので, $X = Ga$ $(a \in X)$ の場合に帰着できる. このとき, $|X/G| = 1$ であるので, $\sum_{g\in G}|X^g| = |G|$ を示せば良い. 以下の集合を考える.

$$A := \{(g, x) \in G \times X \mid g\cdot x = x\}$$

第 1 成分に関して数えると, $|A| = \sum_{g\in G}|X^g|$ が成り立つ. 一方, 第 2 成分に関して数えると, $|A| = \sum_{x\in X}|G_x|$ が成り立つ. $X = Ga$ より, X のどの 2 つもの元 x, y の安定化部分群が共役である (命題 4.9 参照). とくに, $|G_x| = |G_y|$ である. よって, $|A| = |Ga||G_a|$ である. $|Ga| = [G : G_a] = \frac{|G|}{|G_a|}$ より, $|A| = |G|$ となる. 主張が従う.

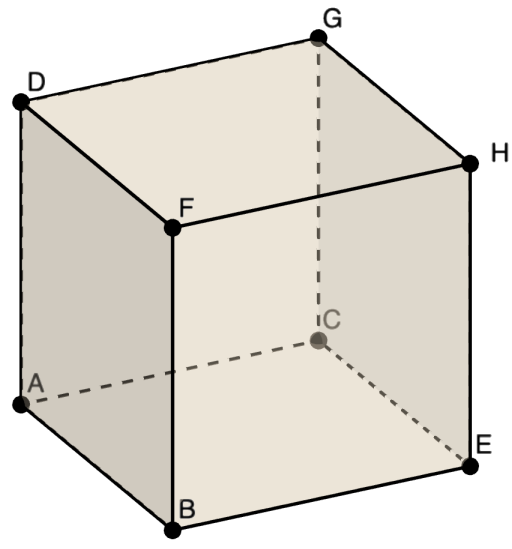
4.6 例：立方体の対称群

$\mathbb{R}^3$ の以下の 8 つの点を考える.

$$A = \begin{pmatrix}-1\\-1\\-1\end{pmatrix}, \quad B = \begin{pmatrix}1\\-1\\-1\end{pmatrix}, \quad C = \begin{pmatrix}-1\\1\\-1\end{pmatrix}, \quad D = \begin{pmatrix}-1\\-1\\1\end{pmatrix},$$

$$E = \begin{pmatrix}1\\1\\-1\end{pmatrix}, \quad F = \begin{pmatrix}1\\-1\\1\end{pmatrix}, \quad G = \begin{pmatrix}-1\\1\\1\end{pmatrix}, \quad H = \begin{pmatrix}1\\1\\1\end{pmatrix}.$$

立方体 $ABCDEFGH$ を X とおく.



$$\Gamma = \{g \in \mathrm{GL}_3(\mathbb{R}) \mid g(X) = X\}$$

とおき, X の変換群という. 明らかに, Γ は有限群である. とくに, $N = |\Gamma|$ とおくと, 任意の $\gamma \in \Gamma$ に対し $\gamma^N = 1$ である. ゆえに, γ の全ての固有値は 1 の冪根である. また, 多項式 $X^N - 1$ が重根を持たないので, g が $\mathbb{C}$ 上対角化可能である. まず, Γ に属する鏡映について考える.

(i) $\alpha = PQ$ を立方体の一辺とし, P, Q, O の 3 点を含む平面を W とおく. 超平面 W に関する直交鏡映 τ_α は明らかに Γ に属する (図 1 参照).

(ii) $i \in \{1, 2, 3\}$ に対し, $x_i = 0$ で定まる平面を W_i とおく. W_i に関する直交鏡映 τ_i は Γ の元である (図 2 参照).

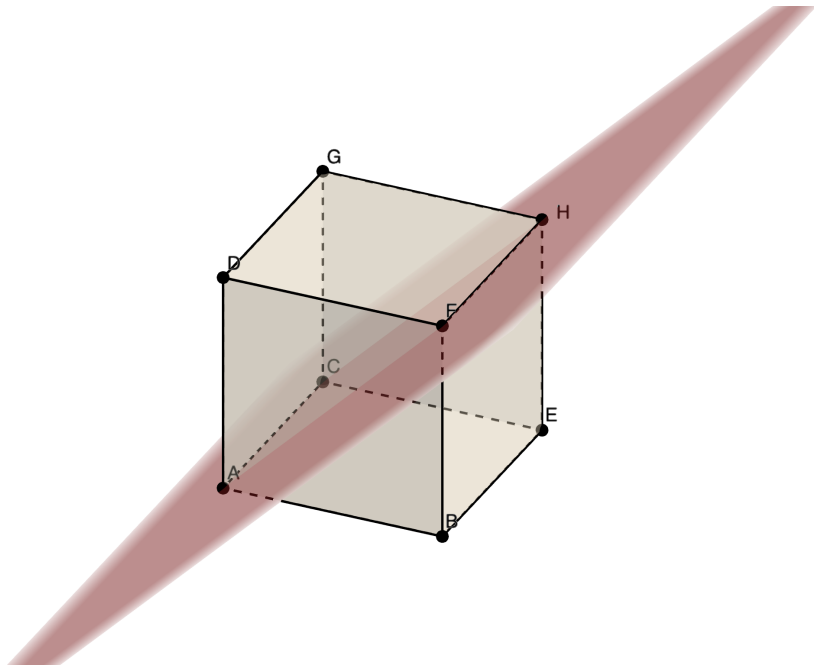


図 1: 鏡映 τ_α

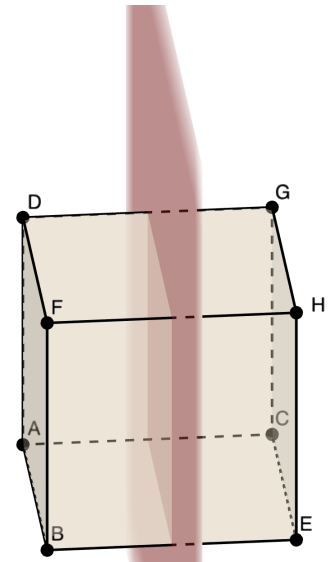


図 2: 鏡映 τ_i

補題 4.16 Γ は

$$\{\pm \mathrm{id}\} \cup \{\tau_\alpha \mid \alpha \text{ が } X \text{ の一辺 }\}$$

によって生成される.

証明

- $\{\pm \mathrm{id}\} \cup \{\tau_\alpha \mid \alpha$ が X の一辺 $\}$ で生成される部分群を Γ' とおく. $\Gamma' = \Gamma$ を示す. $\gamma \in \Gamma$ とし, $\gamma \in \Gamma'$ を示す. 明らかに, Γ' が X の頂点全体の集合に推移的に作用している. よって, $\gamma(A) = \sigma(A)$ となる $\sigma \in \Gamma'$ が存在する. ゆえに, $(\sigma^{-1} \circ \gamma)(A) = A$ である. γ と $\sigma^{-1} \circ \gamma$ を入れ替えて, $\gamma(A) = A$ として良い.
- A を通る 3 つの辺を $\alpha_1 = AB$, $\alpha_2 = AC$, $\alpha_3 = AD$ とおく. 明らかに, τ_{α_i} は α_i を固定し, 他の 2 つの辺を置き換える.

  $$S_A := \langle \tau_{\alpha_1}, \tau_{\alpha_2}, \tau_{\alpha_3} \rangle$$

  と定義する. S_A の全ての元が A と H を固定し, 頂点 $\{B, C, D\}$ を置き換える. 同様に, S_A は頂点 $\{E, F, G\}$ を置き換える.
- 次に, $\gamma(B) \in \{B, C, D\}$ が成り立つことを示す. $\gamma(B) \in \{E, F, G\}$ と仮定する. 以上より, $\gamma(B) = \sigma'(G)$ を満たす $\sigma' \in S_A$ が存在する. $\gamma' = \sigma'^{-1} \circ \gamma$ とおくと, $\gamma'(A) = A$, $\gamma'(B) = G$ である. $H = -A$, $G = -B$ より $\gamma'(H) = H$, $\gamma'(G) = B$ である. ゆえに, $\gamma'(\{A, B, G, H\}) = \{A, B, G, H\}$ かつ $\gamma'(\{C, D, E, F\}) = \{C, D, E, F\}$ が成り立つ. A, B, G, H を含む平面, C, D, E, F を含む平面

をそれぞれ P_1, P_2 とおくと, 以上より $\gamma'(P_i) = P_i$ である. よって, $D = P_1 \cap P_2$ で $\gamma'(D) = D$ が成り立つ. ゆえに, $\gamma'|_D = \mathrm{id}_D$ または $\gamma'|_D = -\mathrm{id}_D$ である. $\gamma'|_D = \mathrm{id}_D$ の場合, $P_1 = \mathbb{R}A \oplus D$ が固有値 1 に対応する固有空間に含まれ, $\gamma'(B) = G$ に矛盾する. $\gamma'|_D = -\mathrm{id}_D$ の場合, $P_1 = \mathbb{R}B \oplus D$ が固有値 -1 に対応する固有空間に含まれ, $\gamma'(A) = A$ に矛盾する. このことから, $\gamma(B) \in \{B, C, D\}$ である.

- 以上より, $\gamma(B) = \sigma''(B)$ となる $\sigma'' \in S_A$ が存在する. γ と $\sigma''^{-1} \circ \gamma$ を入れ替えて, $\gamma(A) = A$ かつ $\gamma(B) = B$ として良い. このとき $\gamma|_{P_1} = \mathrm{id}_{P_1}$ となるので, γ の固有多項式 $\chi_\gamma(X)$ は $\mathbb{R}$ 上分解する. γ の固有値が 1 の冪根であるので, $\chi_\gamma(X) = (X-1)^3$ または $(X-1)^2(X+1)$ である.
  (1) $\chi_\gamma(X) = (X-1)^3$ ならば, γ が対角化可能であるので $\gamma = \mathrm{id}$ となる. $\chi_\gamma(X) = (X-1)^2(X+1)$ ならば, $\det(\gamma) = -1$ である.
  (2) 辺 AB を α とおき, 鏡映 τ_α を考える. $\gamma_0 := \gamma \circ \tau_\alpha$ とおくと, $\gamma_0|_{P_1} = \mathrm{id}_{P_1}$ かつ $\det(\gamma_0) = 1$ である. 上のケース (1) より, $\gamma_0 = \mathrm{id}$ となり, $\gamma = \tau_\alpha$ である.

  いずれの場合 $\gamma \in \Gamma'$ であるので, 主張が従う.

とくに, 補題 4.16 により $\Gamma \subset \mathrm{O}_3(\mathbb{R})$ である. また, 補題 4.16 の証明より, $\gamma \in \Gamma$ で $\gamma(A) = A$ ならば, γ が $\{B, C, D\}$ の置換を引き起こす. このことから,

$$\Gamma_A = \{\gamma \in \Gamma \mid \gamma(A) = A\}$$

とおくと, 群準同型 $u_A \colon \Gamma_A \to \mathfrak{S}(\{B, C, D\})$ が得られる. B, C, D が $\mathbb{R}^3$ を生成するので, u_A は単射である. また, $\mathrm{Im}(u_A)$ が $\{B, C, D\}$ の全ての互換を含むので, u_A は全射である. よって, u_A は群同型となり, とくに $|\Gamma_A| = 6$ である. 命題 4.13 により Γ/Γ_A を A の軌道と同一視できるので, $[\Gamma : \Gamma_A] = 8$ であり, すなわち $|\Gamma| = 8 \times |\Gamma_A| = 8 \times 6 = 48$ である.

$$\Gamma_0 := \Gamma \cap \mathrm{SO}_3(\mathbb{R}) = \{\gamma \in \Gamma \mid \det(\gamma) = 1\}$$

とおく. すなわち, Γ_0 は立方体 X を保つ回転変換全体の部分群である.

命題 4.17 群同型

$$\Gamma \simeq \mathfrak{S}_4 \times \{\pm 1\}$$
$$\Gamma_0 \simeq \mathfrak{S}_4$$

が存在する.

証明

- 立方体の対角線全体の集合を $\mathcal{D}$ とおく. つまり,

$$\mathcal{D} = \{AH, BG, CF, DE\}$$

とおく.

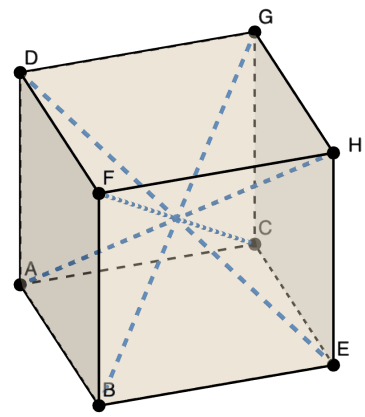


図 3: 立方体の対角

$\Gamma \subset \mathrm{O}_3(\mathbb{R})$ より, 任意の頂点 P, Q に対し $\|\gamma(PQ)\| = \|PQ\|$ $(\gamma \in \Gamma)$ である. ゆえに, Γ は立方体の対角線全体の集合に作用している. この作用に対応する群準同型

$$\rho\colon \Gamma \to \mathfrak{S}(\mathcal{D})$$

を考える. $|\mathcal{D}| = 4$ より, $\mathfrak{S}(\mathcal{D}) \simeq \mathfrak{S}_4$ である.

- $\mathrm{Ker}(\rho) = \{\pm \mathrm{id}\}$ が成り立つことを示す. $\gamma \in \mathrm{Ker}(\rho)$ とすると $\gamma(A) \in \{A, H\}$ である. γ と $-\gamma$ を入れ替えて, $\gamma(A) = A$ として良い. このとき, $\gamma(B) \in \{B, C, D\} \cap \{B, G\}$ より, $\gamma(B) = B$ である. 同様に, $\gamma(C) = C$ となり, $\gamma = \mathrm{id}$ である. したがって, $\mathrm{Ker}(\rho) = \{\pm \mathrm{id}\}$ である.
- 次に, ρ が全単射であることを示す. s_1, s_2 を立方体の 2 つの対角線とし, $P = (s_1 \oplus s_2)^{\perp}$ とおく. P に関する直交鏡映を τ_P とおくと, $\rho(\tau_P)$ は s_1 と s_2 を置き換える $\mathcal{D}$ の互換である. 対称群 $\mathfrak{S}_4$ が互換によって生成されるので, ρ は全単射である.
- $[\Gamma : \Gamma_0] = 2$ であるので, $|\Gamma_0| = 24$ である. $\Gamma_0 \cap \mathrm{Ker}(\rho) = \{\mathrm{id}\}$ より, $\rho\colon \Gamma_0 \to \mathfrak{S}_4$ は単射である. $|\Gamma_0| = |\mathfrak{S}_4|$ より, $\rho\colon \Gamma_0 \to \mathfrak{S}_4$ は群同型である. 最後に, Γ の任意の元が $\pm\gamma$ $(\gamma \in \Gamma_0)$ と表せるので,

$$\Gamma \simeq \{\pm 1\} \times \Gamma_0 \simeq \{\pm 1\} \times \mathfrak{S}_4.$$

$\mathfrak{S}(\mathcal{D})$ の各元について, 群同型 $\Gamma_0 \simeq \mathfrak{S}(\mathcal{D})$ によってそれに対応している Γ_0 の元について考える. 対称群 $\mathfrak{S}(\mathcal{D}) \simeq \mathfrak{S}_4$ の 24 個の元は以下のように 5 つの種類 (共役類) に分類できる.

(i) 長さ 4 の巡回置換 (6 個). それらは立方体の一面の中点を通る直線に関する $\pm\frac{\pi}{2}$ 回転変換に対応している (図 4 参照).

(ii) 長さ 3 の巡回置換 (8 個). それらは立方体の対角線に関する $\pm\frac{2\pi}{3}$ 回転変換に対応している (図 5 参照).

(iii) 互いに素である 2 つの互換の積 (3 個). それらは立方体の一面の中点を通る直線に関する π 回転変換に対応している (図 4 参照).

(iv) 互換 (6 個). それらは立方体の一辺の中点を通る直線に関する π 回転変換に対応している (図 6 参照).

(v) 恒等置換 (1 個). 恒等写像 id に対応している.

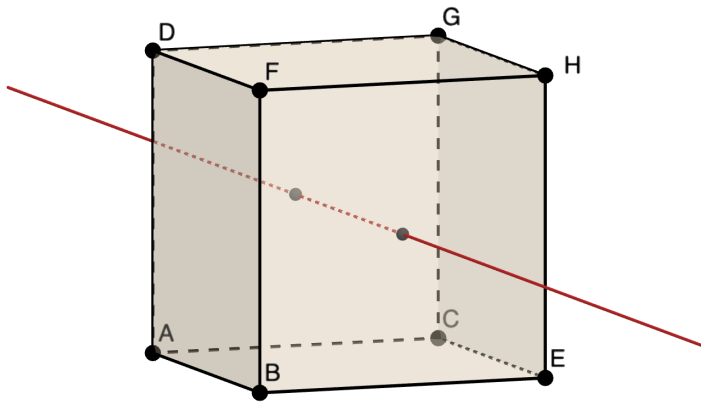


図 4: 回転 (i) と (iii)

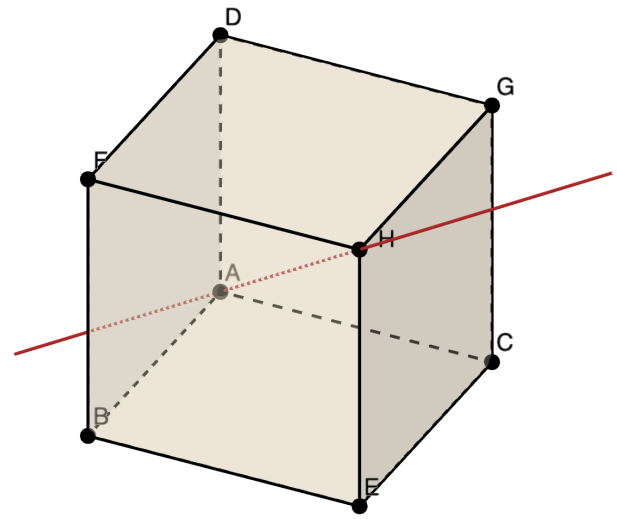


図 5: 回転 (ii)

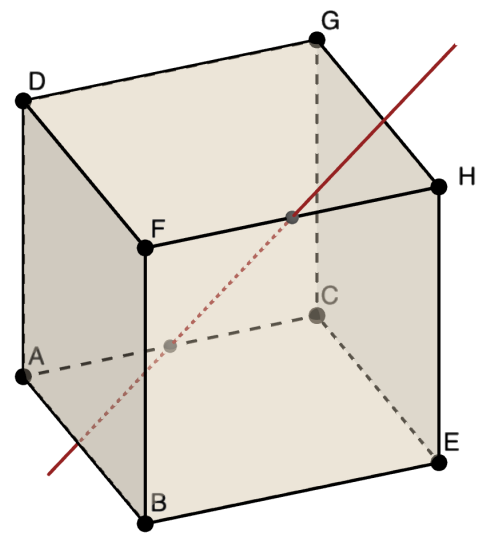


図 6: 回転 (iv)

5　シローの定理

5.1　p 群

定義 5.1　G を有限群とし, p を素数とする. G の位数が p^k $(k \geq 1)$ のとき, G を p 群という.

命題 5.2　G を p 群とし, G が有限集合 X に作用しているとする. このとき, 以下が成り立つ.

$$|X| \equiv |X^G| \pmod{p}.$$

証明

$x_1, \ldots, x_m$ を軌道の代表系とする. (4.1) により

$$|X| = |X^G| + \sum_{x_j \notin X^G} [G : G_{x_j}]$$

である. $x_j \notin X^G$ より, $[G : G_{x_j}] > 1$ である. $[G : G_{x_j}]$ は G の約数だから, p の冪である. 主張が従う.

命題 5.3　G が p 群ならば, G の中心は非自明である.

証明

G の自分自身への共役作用を考える. このとき, 固定点の集合は G の中心 $Z(G)$ に一致する. よって, $0 \equiv |G| \equiv |Z(G)| \pmod{p}$ となる. とくに $Z(G) \neq \{e\}$ である.

定理 5.4　G を p 群とする. このとき, 以下の条件を満たす部分群の列 $\{e\} = G_0 \subsetneq G_1 \subsetneq \cdots \subsetneq G_m = G$ が存在する.
(1) $G_i \triangleleft G$ である $(0 \leq i \leq m)$.
(2) $[G_{i+1} : G_i] = p$ $(0 \leq i \leq m-1)$.

証明

G の位数に関する帰納法によって証明する. $|G| = p$ のとき明らかである. $|G| = p^m$ とおく $(m \geq 2)$. 命題 5.3 により, e とは異なる元 $x \in Z(G)$ が取れる. x の位数を p^k $(k \geq 1)$ とおく. 明らかに, $y = x^{p^{k-1}}$ の位数は p である. $H = \langle y \rangle$ とおく. $H \subset Z(G)$ より, $H \triangleleft G$ である. p 群 $G' = G/H$ を考える. $|G'| = \frac{|G|}{|H|} < |G|$ だから, 帰納法の仮定より条件 (1), (2) を満たす部分群の列 $\{e'\} = G'_0 \subsetneq G'_1 \subsetneq \cdots \subsetneq G'_r = G'$ が存在する. $\pi\colon G \to G'$ を自然な射影とし, $G_i = \pi^{-1}(G'_i)$ とおく. 系 2.28 により $G_{i+1}/G_i \simeq G'_{i+1}/G'_i$ であり, ゆえに $[G_{i+1} : G_i] = p$ $(0 \leq i \leq r-1)$ が成り立つ. また, $G'_i \triangleleft G'$ より $G_i \triangleleft G$ である. 以下の列が得られた.

$$\{e\} \subsetneq H = G_0 \subsetneq \cdots \subsetneq G_r = G. \tag{5.1}$$

ここで, $|G_0| = |H| = p$ である. よって, G の場合も主張が成立する.

例 5.5. p を素数とし, $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ とおく ($\mathbb{F}_p$ は可換体である). $\mathbb{F}_p$ の元を成分とする以下の形の 3 次正方行列を考える.

$$M(a,b,c) = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}, \qquad a,b,c \in \mathbb{F}_p$$

このような行列全体を集めた集合を G とおく. 明らかに, G は $\mathrm{GL}_3(\mathbb{F}_p)$ の位数 p^3 の部分群である. とくに, G は p 群である.

$$\begin{aligned} &M(a,b,c) \times M(a',b',c') = M(a+a', b+b', c+c'+ab') \\ &M(a,b,c)^{-1} = M(-a,-b,ab-c) \\ &[M(a,b,c), M(a',b',c')] = M(0,0,ab'-a'b) \end{aligned}$$

よって,

$$Z(G) = \left\{ \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; c \in \mathbb{F}_p \right\}$$

$H := \{M(0,b,c) \mid b,c \in \mathbb{F}_p\}$ と定義すると, $G_2 \triangleleft G$ である. ゆえに, 以下の列が定理 5.4 の条件を満たす.

$$\{\mathrm{id}\} = G_0 \subsetneq G_1 = Z(G) \subsetneq G_2 \subsetneq G_3 = G.$$

命題 5.6　G を位数 p^2 の群とする. このとき, $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ または $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ である. とくに G はアーベル群である.

証明

命題 5.3 により, $Z(G) \neq \{e\}$ である. ゆえに, $|Z(G)| \in \{p, p^2\}$ である. $|Z(G)| = p$ と仮定する. $x \in G \setminus Z(G)$ とすると, $\langle x, Z(G)\rangle \subset \mathrm{Cent}_G(x)$ である. とくに $|\mathrm{Cent}_G(x)| > p$ であり, ゆえに $\mathrm{Cent}_G(x) = G$ である. よって $x \in Z(G)$ となり, 仮定に矛盾する. したがって, $Z(G) = G$ が成り立つ. すなわち, G はアーベル群である. 位数 p^2 の元が存在する場合は, 命題 3.3 により $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ である. そうでなければ, $G \setminus \{e\}$ の全ての元は位数 p を持つ. $a \in G \setminus \{e\}$, $b \in G \setminus \langle a\rangle$ とすると, 写像

$$\langle a\rangle \times \langle b\rangle \to G, \quad (x, y) \mapsto xy$$

は群同型である. 以上より $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ となる.

5.2 p シロー部分群

G を有限群とし, その位数を n と書く. p を n の素因数とする. $n = p^k m$ と書くことができる. ただし, $k \geq 1$, $\gcd(p, m) = 1$ とする.

定義 5.7 H を G の部分群とする.
(a) $|H| = p^d$ $(d \geq 1)$ のとき, H を p 部分群という.
(b) $|H| = p^k$ のとき, H を G の p シロー部分群という.

すなわち, p シロー部分群は p 部分群の中で最大位数のものである.

例 5.8. $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ とおくと, $\mathbb{F}_p$ は可換体である. 群 $G = \mathrm{GL}_n(\mathbb{F}_p)$ を考える. まず, G の位数を求める. $A \in \mathrm{M}_n(\mathbb{F}_p)$ を n 次正方行列とする. A の列を $x_1, \ldots, x_n$ とおく (ただし, $x_i \in \mathbb{F}_p^n$ である). このとき,

$$A \text{ が正則である} \iff \text{全ての } i = 1, \ldots, n \text{ に対し, } x_i \notin \mathrm{Span}(x_1, \ldots, x_{i-1})$$

が成り立つ (ただし, $i = 1$ のとき $\mathrm{Span}(\emptyset) = \{0\}$ と約束する). 上の条件を満たすベクトルの列 $x_1, \ldots, x_n$ の個数について考える.

- x_1 としては $\mathbb{F}_p^n \setminus \{0\}$ の任意のベクトルが取れるので, ちょうど $p^n - 1$ 個がある.
- x_2 としては $\mathrm{Span}(x_1)$ に属さない $\mathbb{F}_p^n \setminus$ の任意のベクトルが取れるので, ちょうど $p^n - p$ 個がある.
- 帰納法的に $(x_1, \ldots, x_{i-1})$ が線型独立であるように $x_1, \ldots, x_{i-1}$ を取ったとき, $x_i \in \mathbb{F}_p^n \setminus \mathrm{Span}(x_1, \ldots, x_{i-1})$ を満たすベクトルの取り方はちょうど $p^n - p^{i-1}$ 個ある.

以上より,

$$|G| = (p^n - 1)(p^n - p) \ldots (p^n - p^{n-1})$$

が成り立つ. とくに,

$$|G| = p^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} (p^i - 1)$$

と書ける. ここで, $\prod_{i=1}^{n}(p^i - 1)$ は明らかに p で割り切れない. H を以下のような形の行列全体の部分集合とする.

$$\begin{pmatrix} 1 & * & \ldots & * \\ & \ddots & \ddots & \vdots \\ & & \ddots & * \\ & & & 1 \end{pmatrix}, \qquad * \in \mathbb{F}_p.$$

明らかに, H が G の部分群である. また, 対角線の上にある全ての成分を自由に $\mathbb{F}_p$ から取れるので,

$$|H| = p^{\frac{n(n-1)}{2}}$$

が成り立つ. したがって, H は G の p シロー部分群である.

5.3 シローの定理

補題 5.9 G を有限群とし, $H \subset G$ を部分群とする. p を $|H|$ の素因数とする.
(1) G が p シロー部分群を持つならば, H も p シロー部分群を持つ.
(2) さらに, S が G の p シロー部分群ならば, 適当な $a \in G$ が存在し, $H \cap aSa^{-1}$ が H の p シロー部分群である.

証明

明らかに, (2) を示せば十分である. $S \subset G$ を p シロー部分群とする. $h \in H$ 及び $gS \in G/S$ $(g \in G)$ に対し, $h \cdot (gS) = hgS$ とおくことによって, H の $X = G/S$ への群作用を定める. S が G の p シロー部分群だから, $|X| = [G : S]$ は p の倍数でない. よって, その濃度が p の倍数でないような軌道 Hx $(x \in X)$ が存在する. $x = aS$ $(a \in G)$ とおくと, x の安定化部分群は $H_x = H \cap aSa^{-1}$ である. 命題 4.13 により, $|Hx| = [H : H_x]$ である. ゆえに, H における H_x の指数が p の倍数でない. また, S が p 群だから, aSa^{-1} も p 群であり, ゆえに H_x も p 群である. したがって, $H_x = H \cap aSa^{-1}$ は H の p シロー部分群である.

定理 5.10: (シローの定理) G を有限群とし, $|G| = n$ とおく. p を n の約数とする.
(1) G は p シロー部分群を持つ.
(2) K が G の p 部分群ならば, K を含む G の p シロー部分群が存在する.
(3) S, S' が p シロー部分群ならば, $S' = gSg^{-1}$ となる $g \in G$ が存在する.
(4) p シロー部分群の数を n_p とおくと, $n_p \equiv 1 \pmod{p}$ かつ $n_p \mid n$ が成り立つ. また, S が G の p シロー部分群ならば, $n_p = [G : N_G(S)]$ である.

証明

- (1) を示す. 置換 $\sigma \in \mathfrak{S}_n$ に対し, 置換行列 M_σ を $M_\sigma = (\delta_{i,\sigma(j)})_{i,j}$ によって定義する.

$$\gamma \colon \mathfrak{S}_n \to \mathrm{GL}_n(\mathbb{F}_p),\ \sigma \mapsto M_\sigma$$

で定まる写像は明らかに単射群準同型である. 定理 4.3 により, $G \simeq G'$ となる $\mathfrak{S}_n$ の部分群 G' が存在する. $G'' := \gamma(G')$ とおくと, γ の単射性より $G \simeq G' \simeq G''$ となる. 例 5.8 により $\mathrm{GL}_n(\mathbb{F}_p)$ が p シロー部分群を持つので, 補題 5.9 により G'' も p シロー部分群を持つ. G が G'' と同型であるので, G は p シロー部分群を持つ.
- (2) を示す. S を G の p シロー部分群とする. 補題 5.9 により, $a \in G$ が存在し, $H \cap aSa^{-1}$ が H の p シロー部分群である. しかし, H が p 群であるので, その p シロー部分群は H 自身に限る. よって, $H \cap aSa^{-1} = H$ となり, すなわち $H \subset aSa^{-1}$ である. $|aSa^{-1}| = |S|$ より, aSa^{-1} は H を含む G の p シロー部分群である.
- (3) を示す. S, S' を G の p シロー部分群とする. 補題 5.9 で $H = S'$ とすると, 適当な $a \in G$ を用いて $S' \cap aSa^{-1}$ が S' の p シロー部分群である. よって $S' \cap aSa^{-1} = S'$ となり, すなわち $S' \subset aSa^{-1}$ となる. $|S'| = |S| = |aSa^{-1}|$ より, $S' = aSa^{-1}$ が成り立つ.
- 最後に, (4) を示す. X を G の p シロー部分群全体の集合とする. G が共役によって X に作用している. また, S が p シロー部分群ならば, (3) より $X = \{gSg^{-1} \mid g \in G\}$ が成り立つ. よって, G が X に推移的に作用している. S の安定化部分群は $N_G(S)$ であるので, $n_p = |X| = [G : N_G(S)]$ であ

る．とくに，$n_p \mid n$ である．G の作用を S に制限することによって，S の X への作用が定まる．S が p 群だから，$|X| \equiv |X^S| \pmod{p}$ である (命題 5.2 参照)．以下は，$X^S = \{S\}$ であることを示す．明らかに，$S \in X^S$ である．逆に，$S' \in X^S$ とする．このとき，$hS'h^{-1} = S'$ $(h \in S)$ であるので，$S \subset N_G(S')$ である．一方，$S' \subset N_G(S')$ が成り立つ．また，S, S' が $N_G(S')$ の p シロー部分群である．(3) を群 $N_G(S')$ に適用させると，S, S' が $N_G(S')$ において共役である．しかし，$h \in N_G(S')$ のとき，$hS'h^{-1} = S'$ だから，$S = S'$ となる．以上より，$X^S = \{S\}$ である．ゆえに，$|X| \equiv |X^S| = 1 \pmod{p}$ が成り立つ．

注意 5.11. S を G の p シロー部分群とする．定理 5.10(iv) より

$$n_p = 1 \iff N_G(S) = G \iff S \triangleleft G$$

が成り立つ．

系 5.12: (コーシーの定理) G を位数 n の群とし，p を n の素因数とする．このとき，位数 p の元が G 内に存在する．

証明

H を G の p シロー部分群とし，$x \in H$ $(x \neq e)$ とする．x の位数は p^k $(k \geq 1)$ である．ゆえに，$x^{p^{k-1}}$ の位数は p である．

系 5.13 p, q が素数で，$p < q$ かつ $q \not\equiv 1 \pmod{p}$ とする．G を位数 pq の群とする．このとき，G は巡回群である．

証明

n_p, n_q をそれぞれ G の p シロー部分群の個数，q シロー部分群の個数とする．シロー定理より，

$$n_p \equiv 1 \pmod{p} \text{ かつ } n_p \mid pq$$
$$n_q \equiv 1 \pmod{q} \text{ かつ } n_q \mid pq$$

がいえる．ゆえに，$n_p = n_q = 1$ となる．H_p, H_q をそれぞれ p シロー部分群，q シロー部分群とする．$n_p = n_q = 1$ より H_p と H_q は正規部分群である．次に，H_p と H_q の元が交換することを示す．$x \in H_p$，$y \in H_q$ とし，x と y の交換子

$$z = [x, y] = xyx^{-1}y^{-1}$$

を考える．H_q の正規性より，$xyx^{-1} \in H_q$ である．よって，$z \in H_q$ となる．同様に，H_p の正規性より $yxy^{-1} \in H_q$ が成り立つ．よって，$z \in H_p$ となる．したがって，$z \in H_p \cap H_q$ である．H_p と H_q の位数が互いに素だから，ラグランジュ定理より $H_p \cap H_q$ の位数は 1 となり，すなわち $H_p \cap H_q = \{e\}$ である．とくに，$z = e$ となり，ゆえに $xy = yx$ が成立する．よって，H_p と H_q の元が交換する．
最後に，$x \in H_p$，$y \in H_q$ を単位元とは異なるものとする．このとき，$\mathrm{ord}(x) = p$，$\mathrm{ord}(y) = q$ である．x, y が交換し，その位数が互いに素だから，命題 3.7 により $\mathrm{ord}(xy) = pq$ である．ゆえに，xy は G の生成元である．

例 5.14. G を位数 15 の群とする．このとき，G は巡回群である．

6　半直積

6.1　外部半直積

N, H を 2 つの群とし, 群準同型

$$\varphi\colon H \to \mathrm{Aut}(N)$$

が与えられているとする. このとき, φ に関する N と H の半直積を次のように定義する. $G = N \times H$ とおく. G の元 (n_1, h_1) と (n_2, h_2) に対し,

$$(n_1, h_1) \cdot (n_2, h_2) := (n_1 \varphi(h_1)(n_2), h_1 h_2)$$

とおくことによって, G に演算を入れる.

定理 6.1

(1) この演算に関して G は群である.

(2) N, H の単位元をそれぞれ e_N, e_H とおくと, G の単位元は (e_N, e_H) である.

(3) $(n, h) \in G$ の逆元は $(\varphi(h^{-1})(n^{-1}), h^{-1})$ である.

証明

- 演算が結合的であることを確認する. $(n_i, h_i) \in N \times H$ $(i = 1, 2, 3)$ とする. このとき,

$$\begin{aligned}
(n_1, h_1) \cdot ((n_2, h_2) \cdot (n_3, h_3)) &= (n_1, h_1) \cdot (n_2 \varphi(h_2)(n_3), h_2 h_3) \\
&= \left(n_1 \varphi(h_1)\left(n_2 \varphi(h_2)(n_3)\right), h_1 h_2 h_3\right) \\
&= (n_1 \varphi(h_1)(n_2) \varphi(h_1 h_2)(n_3), h_1 h_2 h_3) \\
&= (n_1 \varphi(h_1)(n_2), h_1 h_2) \cdot (n_3, h_3) \\
&= ((n_1, h_1) \cdot (n_2, h_2)) \cdot (n_3, h_3).
\end{aligned}$$

  よって, 演算が結合法則を満たす.

- $\varphi(h)(e_N) = e_N$ かつ $\varphi(e_H) = \mathrm{id}_N$ より, 任意の $(n, h) \in G$ に対し,

$$(n, h) \cdot (e_N, e_H) = (e_N, e_H) \cdot (n, h) = (n, h)$$

  が成り立つ. ゆえに (e_N, e_H) は単位元である.

- 最後に,

$$\begin{aligned}
(n, h) \cdot (\varphi(h^{-1})(n^{-1}), h^{-1}) &= (n \varphi(h)(\varphi(h^{-1})(n^{-1}), h h^{-1}) \\
&= (n \varphi(h h^{-1})(n^{-1}), e_H) \\
&= (n \,\mathrm{id}_N(n^{-1}), e_H) \\
&= (e_N, e_H)
\end{aligned}$$

  である. 一方,

$$\begin{aligned}
(\varphi(h^{-1})(n^{-1}), h^{-1}) \cdot (n, h) &= (\varphi(h^{-1})(n^{-1}) \varphi(h^{-1})(n), h^{-1} h) \\
&= \varphi(h^{-1})(n^{-1} n), e_H) \\
&= \varphi(h^{-1})(e_N), e_H) \\
&= (e_N, e_H)
\end{aligned}$$

  である. よって, (n, h) が逆元として $(\varphi(h^{-1})(n^{-1}), h^{-1})$ を持つ. 以上より, G は群である.

定義 6.2　G を N と H の (外部) 半直積といい, $G = N \rtimes_\varphi H$ と表す.

以下の 2 つの写像を考える.

$$\iota_N \colon N \to G, \quad n \mapsto (n, e_H)$$
$$\iota_H \colon H \to G, \quad h \mapsto (e_N, h)$$

この写像はそれぞれ単射群準同型である. ι_N, ι_H の像をそれぞれ N, H と同一視し, 単に N, H と表す. 第 2 成分への射影

$$\pi_H \colon G \to H, \quad (n, h) \mapsto h$$

を考える. G の演算の定義より, π_H は群準同型である. また, $\mathrm{Ker}(\pi_H)$ が成り立つので, N は G の正規部分群である. しかし, H が正規部分群であるとは限らない. 以下, 「φ が自明な準同型である」とは, 全ての $h \in H$ に対し $\varphi(h) = \mathrm{id}_N$ であることを意味する.

定理 6.3　以下が同値である.
(i)　H が G の正規部分群である.
(ii)　φ が自明な準同型である.
(iii)　G の演算が直積 $N \times H$ の演算と一致する.

証明

「(ii) $\Longrightarrow$ (iii) $\Longrightarrow$ (i)」は明らかである. (i) を仮定する. このとき, 任意の $h, \in H$, $n \in N$ に対し, $(n^{-1}, e_H) \cdot (e_N, h) \cdot (n^{-1}, e_H)^{-1}$ が H に属する.

$$\begin{aligned}(n^{-1}, e_H) \cdot (e_N, h) \cdot (n^{-1}, e_H)^{-1} &= (n^{-1}, h) \cdot (n, e_H) \\ &= (n^{-1}\varphi(h)(n), h)\end{aligned}$$

である. ゆえに, 上の元の第 1 成分が e_N となり, すなわち $\varphi(h)(n) = n$ が成り立つ. したがって, 任意の $h \in H$ に対し $\varphi(h) = \mathrm{id}_N$ である.

6.2　内部半直積

まず, $\varphi \colon H \to \mathrm{Aut}(N)$ を群準同型とし, φ に関する N と H の外部半直積 $G = N \rtimes_\varphi H$ を考える. ι_N, ι_H により, N, H を G の部分群として考える.

補題 6.4　N, H は以下を満たす.
(1)　$N \triangleleft G$ である.
(2)　G の部分群として $N \cap H = \{e_G\}$ である.
(3)　$G = NH$ である.

条件 (3) の集合 NH について補足説明をする. 一般の群 G の 2 つの部分群 K, H に対し,

$$KH = \{kh \mid k \in K,\ h \in H\}$$

とおく. KH は部分群とは限らない. しかし, K, H の一方が他方の正規化部分群に含まれるとき, KH が部分群であることが容易に証明できる. また, そのとき $KH = HK$ も成り立つ. 上の補題を証明する.

証明

(1) と (2) は明らかである. (3) を確認する. $G = N \rtimes_\varphi H$ のとき, 任意の $(n,h) \in G$ に対し $(n,h) = (n,e_H)\cdot(e_N,h)$ と表すことができるので, 条件 (3) が満たされている.

今, 群 G 及び 2 つの部分群 N, H が与えられているとする.

定義 6.5 G が N と H の内部半直積であるとは, N, H が以下の条件を満たすことをいう.
(1) $N \triangleleft G$ である.
(2) G の部分群として $N \cap H = \{e_G\}$ である.
(3) $G = NH$ である.
このとき, $G = N \rtimes H$ と表す.

注意 6.6. 定義 6.5 の 3 つ条件は以下の条件と同値である.
(1) $N \triangleleft G$ である.
(2) G の部分群として $N \cap H = \{e_G\}$ である.
(3') $G = \langle N \cup H \rangle$ である (つまり, G が N と H によって生成される).
実際, $N \triangleleft G$ より, NH は部分群である. ゆえに, $\langle N \cup H \rangle = NH = HN$ が成り立つ.

「外部半直積」と「内部半直積」の関係について説明する.

- 群 N, H 及び準同型 $\varphi\colon H \to \mathrm{Aut}(N)$ が与えられているとし, G を φ に関する外部半直積とする. このとき, N と $\iota_N(N)$ また H と $\iota_H(H)$ を同一視すると, N, H が上の 3 つの条件を満たすので, G は N と H の内部半直積である.
- 逆に, 群 G 及び部分群 N, H が与えられているとし, G が N と H の内部半直積であるとする. とくに, $N \triangleleft G$ であるので, G が共役によって N に作用している. この作用を H に制限し, 以下の準同型を考える.

$$\varphi\colon H \to \mathrm{Aut}(N), \quad h \mapsto (n \mapsto hnh^{-1})$$

φ に関する N と H の外部半直積 $N \rtimes_\varphi H$ を考える.

$$f\colon N \rtimes_\varphi H \to G, \quad (n,h) \mapsto nh$$

と定義する. f が群準同型であることを確認する. 任意の $n_1, n_2 \in N$, $h_1, h_2 \in H$ に対し,

$$\begin{aligned} f((n_1,h_1)\cdot(n_2,h_2)) &= f(n_1\varphi(h_1)(n_2), h_1h_2) \\ &= n_1h_1n_2h_1^{-1}h_1h_2 \\ &= n_1h_1n_2h_2 \\ &= f(n_1,h_1)f(n_2,h_2) \end{aligned}$$

である. ゆえに, f は群準同型である. 条件 (2) より, f は全射である. また, $(n,h) \in \mathrm{Ker}(f)$ ならば, $nh = e_g$ より $n = h^{-1} \in N \cap H$ となる. 条件 (1) より, $n = h = e_G$ となる. よって, f は単射である. 以上より, G と $N \rtimes_\varphi H$ は互いに同型である.

以上より, 「内部半直積」と「外部半直積」の定義は単純に考え方の違いだけで、本質的に同等である。

例 6.7. $a \in \mathbb{C}^*$, $b \in \mathbb{C}$ に対し, $f_{a,b}(z) = az + b$ とおくことで写像 $f_{a,b}\colon \mathbb{C} \to \mathbb{C}$ を定義し,

$$G := \{f_{a,b} \mid a \in \mathbb{C}^*,\ b \in \mathbb{C}\}$$

とおく. $a, a' \in \mathbb{C}^*$, $b, b' \in \mathbb{C}$ のとき,

$$f_{a,b} \circ f_{a',b'} = f_{aa',ab'+b}$$
$$f_{a,b}^{-1} = f_{\frac{1}{a},-\frac{b}{a}}$$

が成り立つ. よって,G は写像の合成に関して群をなす. また,

$$N := \{f_{1,b} \mid b \in \mathbb{C}\}$$
$$H := \{f_{a,0} \mid a \in \mathbb{C}^*\}$$

とおくと, N, H は G の部分群である. 以上より, 写像 $f_{a,b} \mapsto a$ は群準同型 $G \to \mathbb{C}^*$ である. その核は N であるので, N は G の正規部分群となる. $N \cap H = \{\mathrm{id}\}$ は明らかに成り立つ. また, $f_{a,b} = f_{1,b} \circ f_{a,0}$ であるので, G が N と H によって生成される. したがって, $G = N \rtimes H$ が成り立つ. 写像 $a \mapsto f_{a,0}$ と $b \mapsto f_{1,b}$ によって, それぞれ $N \simeq \mathbb{C}$ かつ $H \simeq \mathbb{C}^*$ となる. H の N への共役作用は自然な作用

$$\mathbb{C}^* \to \mathrm{Aut}(\mathbb{C}), \quad a \mapsto (z \mapsto az)$$

に対応する. G は外部半直積 $\mathbb{C} \rtimes \mathbb{C}^*$ と同型である.

6.3 半直積の同型

2 つの群 N, H 及び群準同型 $\varphi\colon H \to \mathrm{Aut}(N)$ が与えられているとする. また, $\gamma \in \mathrm{Aut}(H)$ を H の自己同型とする. 合成写像

$$\varphi \circ \gamma\colon H \to \mathrm{Aut}(N)$$

を考える.

命題 6.8 以下の写像は群同型である.

$$\alpha\colon N \rtimes_{\varphi\circ\gamma} H \to N \rtimes_{\varphi} H, \quad (n,h) \mapsto (n, \gamma(h))$$

証明

上の写像は明らかに全単射であるので, 群準同型であることを示せば十分である. 任意の $n_1, n_2 \in N$, $h_1, h_2 \in H$ に対し, 以下が成り立つ.

$$\begin{aligned}\alpha((n_1,h_1)\cdot(n_2,h_2)) &= \alpha(n_1\varphi(\gamma(h_1))(n_2), h_1h_2)\\ &= (n_1\varphi(\gamma(h_1))(n_2), \gamma(h_1h_2))\\ &= (n_1,\gamma(h_1))\cdot(n_2,\gamma(h_2))\\ &= \alpha(n_1,h_1)\cdot\alpha(n_2,h_2).\end{aligned}$$

主張が従う.

今, $s \in \mathrm{Aut}(N)$ とし,

$$\Gamma_s\colon \mathrm{Aut}(N) \to \mathrm{Aut}(N), \quad f \mapsto s \circ f \circ s^{-1} \tag{6.1}$$

と定義する. 群準同型 $\Gamma_s \circ \varphi\colon H \to \mathrm{Aut}(N)$ を考える.

命題 6.9 以下の写像は群同型である.

$$\beta\colon N \rtimes_{\varphi} H \to N \rtimes_{\Gamma_s\circ\varphi} H, \quad (n,h) \mapsto (s(n), h)$$

証明

上の写像は明らかに全単射であるので, 群準同型であることを示せば十分である. 任意の $n_1, n_2 \in N$, $h_1, h_2 \in H$ に対し, 以下が成り立つ.

$$\begin{aligned}\beta((n_1,h_1)\cdot(n_2,h_2)) &= \beta(n_1\varphi(h_1)(n_2), h_1h_2)\\ &= (s(n_1)s(\varphi(h_1)(n_2)), h_1h_2)\\ &= (s(n_1)\Gamma_s(\varphi(h_1))(s(n_2)), h_1h_2)\\ &= (s(n_1),h_1)\cdot(s(n_2),h_2)\\ &= \beta(n_1,h_1)\cdot\beta(n_2,h_2).\end{aligned}$$

主張が従う.

命題 6.10　p, q を素数とし, $p \mid q-1$ とする. このとき, 位数 pq の群は同型を除いてちょうど 2 つ存在する.

証明

p シロー部分群の個数, q シロー部分群の個数をそれぞれ n_p, n_q とおく.

$$\begin{aligned} n_p &\equiv 1 \pmod{p} \text{ かつ } n_p \mid q\\ n_q &\equiv 1 \pmod{q} \text{ かつ } n_q \mid p\end{aligned}$$

である. $p < q$ より, $n_q = 1$ となる. H_p, H_q をそれぞれ p シロー部分群, q シロー部分群とする. $n_q = 1$ より, H_q は正規部分群である. ラグランジュ定理より $|H_p \cap H_q|$ が p と q の公約数であるので, $H_p \cap H_q = \{e\}$ となる. また, H_qH_p は部分群であり, その位数は $> q$ であるので, $H_qH_p = G$ が成り立つ. したがって,

$$G = H_q \rtimes H_p$$

である. 命題 3.13 により $H_p \simeq \mathbb{Z}/p\mathbb{Z}$, $H_q \simeq \mathbb{Z}/q\mathbb{Z}$ である. よって, $G \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$ と表すことができる. ただし, ここで $\varphi\colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ は群準同型である. φ が自明な準同型ならば, 定理 6.3 により $G \simeq \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/pq\mathbb{Z}$ である.
最後に, 非自明な群準同型 $\varphi\colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ について考える. このとき, φ が単射であるので, $\mathrm{Im}(\varphi)$ は位数 p の部分群である. 例 2.30 により $\mathrm{Aut}(\mathbb{Z}/q\mathbb{Z}) \simeq (\mathbb{Z}/q\mathbb{Z})^\times$ である. また, 定理 3.14 により $(\mathbb{Z}/q\mathbb{Z})^\times$ は巡回群である. $p \mid q-1$ だから, 巡回群 $(\mathbb{Z}/q\mathbb{Z})^\times$ はただ一つの位数 p の部分群を持つ (命題 3.12 参照). ゆえに, φ の像が一意に定まる. よって, $\varphi, \varphi'\colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ が非自明な準同型ならば, $\varphi' = \varphi \circ \gamma$ となる $\gamma \in \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ が存在する. 命題 6.8 により,

$$\mathbb{Z}/q\mathbb{Z} \rtimes_{\varphi'} \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$$

となる. 以上より, 位数 pq の群は同型を除いてちょうど 2 つ存在し, $\mathbb{Z}/pq\mathbb{Z}$ と $\mathbb{Z}/q\mathbb{Z} \rtimes_\varphi \mathbb{Z}/p\mathbb{Z}$ に限る ($\varphi\colon \mathbb{Z}/p\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/q\mathbb{Z})$ は非自明な準同型である).

6.4　二面体群

$n \geq 3$ とする. $k = 0, 1, \ldots, n-1$ に対し,

$$A_k = \begin{pmatrix} \cos(\frac{2k\pi}{n}) \\ \sin(\frac{2k\pi}{n}) \end{pmatrix}$$

とする. $A_0, A_1, \ldots, A_{n-1}$ を頂点とする正 n 角形 P_n を考える.

定義 6.11　正 n 角形 P_n の対称群を D_n とおき, 二面体群という. つまり,

$$D_n := \{f \in \mathrm{GL}_2(\mathbb{R}) \mid f(P_n) = P_n\}.$$

例えば, 以下の線型変換が D_n に属する.

- $\frac{2\pi}{n}$ 回転変換 r (図 7). $r(A_i) = A_{i+1}$ $(0 \leq i \leq n-2)$, $r(A_{n-1}) = A_0$ が成り立つので, $r \in D_n$ である. 明らかに, $\mathrm{ord}(r) = n$ である.
- x 軸に関する鏡映変換 s (図 8, 図 9). つまり,

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

である. $s(A_i) = A_{n-i}$ $(1 \leq i \leq n-1)$, $s(A_0) = A_0$ であるので, $s \in D_n$ である. 明らかに, $\mathrm{ord}(s) = 2$ である.

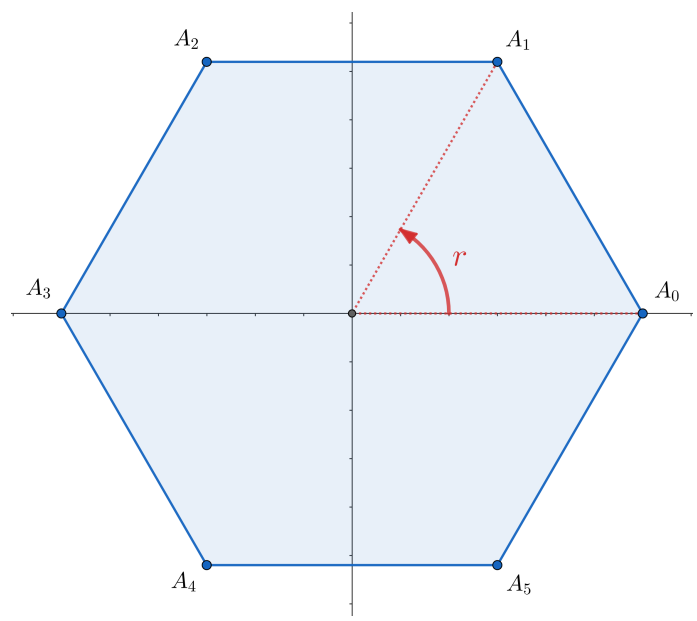


図 7: 回転 r $(n = 6)$

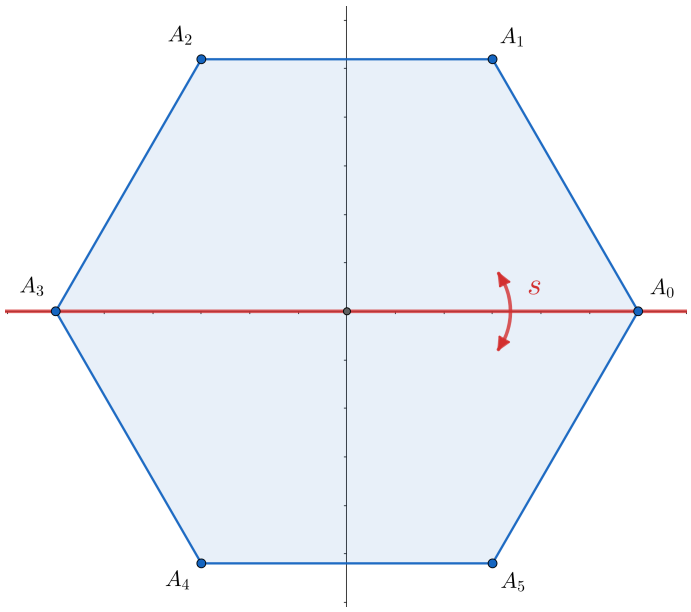


図 8: 鏡映 s $(n = 6)$

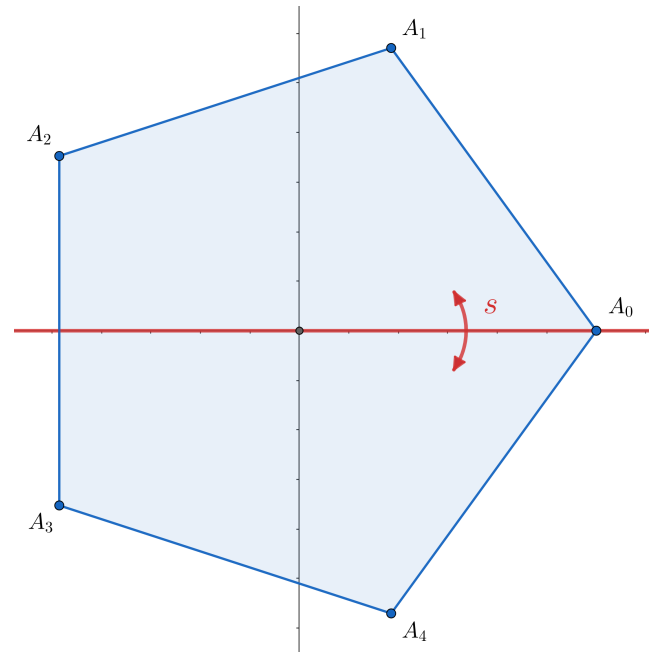


図 9: 鏡映 s $(n = 5)$

D_n は正 n 角形 P_n の頂点全体の集合に作用している. また, この作用は明らかに忠実である. したがって, 単射準同型

$$\iota_n \colon D_n \to \mathfrak{S}(\{A_0, \ldots, A_{n-1}\}) \simeq \mathfrak{S}_n \tag{6.2}$$

が得られる．とくに，D_n は有限群である．

補題 6.12　D_n が s と r で生成される．

証明

- $N = |D_n|$ とおくと，ラグランジュの定理より任意の $f \in D_n$ に対し $f^N = \mathrm{id}$ が成り立つ．多項式 $X^N - 1$ の全ての根が単根であるので，f は $\mathbb{C}$ 上対角可能である．
- $H = \langle r, s \rangle$ とおく．$D_n = H$ であることを示す．$f \in D_n$ とする．明らかに，H が P_n の頂点に推移的に作用している．よって，$f(A_0) = g(A_0)$ を満たす $g \in H$ が存在する．f と $g^{-1} \circ f$ を入れ替えて，$f(A_0) = A_0$ として良い．
- このとき，f は固有値として 1 を持つので，f の固有多項式 χ_f が $\mathbb{R}$ で分解する．よって，f の固有値は 1 の乗根であるので，$\chi_f = (X-1)^2$ または $X^2 - 1$ が成り立つ．
  (1) $\chi_f = (X-1)^2$ ならば，f が対角可能だから $f = \mathrm{id}$ となる．
  (2) $\chi_f = X^2 - 1$ ならば，$\det(f) = -1$, $\det(f \circ s) = 1$ となる．上の (1) より，$f \circ s = \mathrm{id}$ である．したがって $f = s$ である．

  いずれの場合，$f \in H$ となり，主張が従う．

とくに，$D_n \subset \mathrm{O}_2(\mathbb{R})$ である．$\det(sr) = -1$ より，sr は直交鏡映である．とくに $(sr)^2 = srsr = \mathrm{id}$ が成り立つ．よって，

$$srs = r^{-1} \tag{6.3}$$

$$\text{ゆえに} \qquad sr^k s = (srs)^r = r^{-k}, \qquad k \in \mathbb{Z} \tag{6.4}$$

である．とくに $R = \langle r \rangle$ が正規部分群である．D_n/R が s の剰余類で生成されるので，$[D_n : R] = 2$ となる．ゆえに，$|D_n| = 2|R| = 2n$ である．また，以下が成り立つ．

$$D_n = \{\mathrm{id}, r, \dots, r^{n-1}\} \cup \{s, sr, \dots, sr^{n-1}\}.$$

$H = \langle s \rangle$ とおく．以上より，D_n は R と H の内部半直積である．$R \simeq \mathbb{Z}/n\mathbb{Z}$, $H \simeq \mathbb{Z}/2\mathbb{Z}$ と同一視する．このとき，(6.3) により H の R への共役作用は $\overline{1} \mapsto -\mathrm{id}$ で定まる準同型

$$\varphi \colon \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$$

に対応する．ゆえに，

$$D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes_\varphi \mathbb{Z}/2\mathbb{Z}$$

である．

補題 6.13　D_n の中心は以下の通りである．

$$Z(D_n) = \begin{cases} \{\mathrm{id}\} & (n \text{ が奇数}) \\ \{\pm \mathrm{id}\} & (n \text{ が偶数}). \end{cases}$$

証明

まず，r の中心化群について考える．明らかに，$\langle r \rangle \subset \mathrm{Cent}_{D_n}(r)$ である．$[D_n : \langle r \rangle] = 2$ であることと，$s \notin \mathrm{Cent}_{D_n}(r)$ であることより，$\mathrm{Cent}_{D_n}(r) = \langle r \rangle$ がいえる．とくに，$Z(D_n) \subset \langle r \rangle$．$k \geq 1$ で $x = r^k$ とおく．$sxs = x^{-1}$ より，$x = r^k \in Z(D_n) \iff x^2 = \mathrm{id}$ である．n が奇数のとき，$\langle r \rangle$ は位数 2 の元を持たないので，$Z(D_n) = \{\mathrm{id}\}$ となる．n が偶数のとき，巡回群 $\langle r \rangle$ に属する位数 2 の元は $r^{n/2} = -\mathrm{id}$ に限る．主張が従う．

D_n の導来部分群を $[D_n, D_n]$ と表す (定義 2.31 参照).

補題 6.14 $[D_n, D_n] = \langle r^2 \rangle$ である. また,

$$D_n/[D_n, D_n] \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} & (n \text{ が奇数}) \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & (n \text{ が偶数}). \end{cases}$$

証明

$sr^{-1}s = r$ より, $[r, s] = rsr^{-1}s = r^2$ である. ゆえに, $\langle r^2 \rangle \subset [D_n, D_n]$ である. n が奇数のとき, $\langle r^2 \rangle = \langle r \rangle$ が正規部分群であり, さらに $D_n/\langle r \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ がアーベル群である. 命題 2.32(2) より $[D_n, D_n] \subset \langle r \rangle = \langle r^2 \rangle$ であるので, $[D_n, D_n] = \langle r^2 \rangle$ が成り立つ.
n が偶数のとき, $sr^2s = r^{-2} = r^{n-2} = (r^2)^{\frac{n-2}{2}}$ と書けるので, $s \in N_{D_n}(\langle r^2 \rangle)$ である. また, $r \in N_{D_n}(\langle r^2 \rangle)$ も成り立つので, $N_{D_n}(\langle r^2 \rangle) = D_n$ となり, すなわち $\langle r^2 \rangle$ が正規部分群である. また, $D_n/\langle r^2 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ である. 実際, r, s の剰余類は $D_n/\langle r^2 \rangle$ を生成し, それぞれの位数は 2 である. とくに, $D_n/\langle r^2 \rangle$ はアーベル群であるので, $[D_n, D_n] \subset \langle r^2 \rangle$ である. 主張が従う.

次に, D_n の自己同型について考える. 以下の $\mathrm{Aut}(D_n)$ の部分群を考える.

$$\mathrm{Fix}(r) := \{\sigma \in \mathrm{Aut}(D_n) \mid \sigma(r) = r\}$$
$$\mathrm{Fix}(s) := \{\sigma \in \mathrm{Aut}(D_n) \mid \sigma(s) = s\}$$

定理 6.15 $\mathrm{Aut}(D_n) = \mathrm{Fix}(r) \rtimes \mathrm{Fix}(s)$ が成り立つ. つまり,

- $\mathrm{Fix}(r) \triangleleft \mathrm{Aut}(D_n)$ である.
- $\mathrm{Fix}(r) \cap \mathrm{Fix}(s) = \{\mathrm{id}\}$ である.
- $\mathrm{Fix}(r)$ と $\mathrm{Fix}(s)$ が $\mathrm{Aut}(D_n)$ を生成する.

また, 以下が成り立つ.

(1) $\mathrm{Fix}(s) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ である.

(2) $\mathrm{Fix}(r) \simeq \mathbb{Z}/n\mathbb{Z}$ である.

(3) $\mathrm{Fix}(s)$ の $\mathrm{Fix}(r)$ への共役作用は, 掛け算で定まる自然な作用 $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ に対応している.

証明

まず, $\langle r \rangle$ が D_n の特性部分群であることを示す. $\sigma \in \mathrm{Aut}(D_n)$ とする. $\mathrm{ord}(\sigma(r)) = \mathrm{ord}(r) = n \geq 3$ より, $\sigma(r) \in \langle r \rangle$ である. 実際, $D_n \setminus \langle r \rangle$ の全ての元は直交鏡映であるので, その位数は 2 である. よって, $\sigma(\langle r \rangle) = \langle \sigma(r) \rangle = \langle r \rangle$ が成り立つ. つまり, $\langle r \rangle$ が D_n の特性部分群である.
ゆえに, $\sigma\colon D_n \to D_n$ が自己同型ならば, σ が $\langle r \rangle$ の自己同型 $\sigma|_{\langle r \rangle}$ を引き起こす. ゆえに, 以下の群準同型が得られる.

$$\alpha\colon \mathrm{Aut}(D_n) \to \mathrm{Aut}(\langle r \rangle), \quad \sigma \mapsto \sigma|_{\langle r \rangle}.$$

この準同型の核は $\mathrm{Fix}(r)$ である. 実際, $\mathrm{Ker}(\alpha) \subset \mathrm{Fix}(r)$ は明らかである. 逆に, $\sigma(r) = r$ ならば, $\sigma(r^k) = r^k$ $(k \in \mathbb{Z})$ となり, すなわち $\sigma|_{\langle r \rangle} = \mathrm{id}_{\langle r \rangle}$ であり, $\sigma \in \mathrm{Ker}(\alpha)$ である. したがって, $\mathrm{Ker}(\alpha) = \mathrm{Fix}(r)$ である. とくに, $\mathrm{Fix}(r) \triangleleft \mathrm{Aut}(D_n)$ である.
群同型 $\mathbb{Z}/n\mathbb{Z} \to \langle r \rangle$, $\overline{k} \mapsto r^k$ によって, $\langle r \rangle$ と $\mathbb{Z}/n\mathbb{Z}$ を同一視する. 同様に, $\mathrm{Aut}(\langle r \rangle)$ と $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ を同一視する. 具体的に, $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ のとき, a に対応している $\mathrm{Aut}(\langle r \rangle)$ のものは $r^k \mapsto r^{ak}$ で定まる自己同型である. $\sigma \in \mathrm{Fix}(r)$ とする. $\sigma(\langle r \rangle) = \langle r \rangle$ より $\sigma(s) \notin \langle r \rangle$ である. よって, $\sigma(s) = sr^m$

となる $m \in \mathbb{Z}/n\mathbb{Z}$ が存在する. 逆に, $m \in \mathbb{Z}/n\mathbb{Z}$ に対し, D_n の自己同型 τ_m を以下のように定義する.

$$\begin{aligned} &\tau_m(r^k) = r^k, \\ &\tau_m(sr^k) = sr^{m+k} \qquad\qquad k \in 0, 1, \ldots, n-1. \end{aligned}$$

τ_m が準同型であることは, 以下の式から分かる.

$$\begin{aligned} \tau_m(sr^k sr^{k'}) = \tau_m(r^{k'-k}) = r^{k'-k} \\ \text{一方,} \quad \tau_m(sr^k)\ \tau_m(sr^{k'}) = sr^{m+k} sr^{m+k'} = r^{m+k'-m-k} = r^{k'-k} \end{aligned}$$

である. とくに, 以下が成り立つ.

$$\mathrm{Fix}(r) = \{\tau_m \mid m \in \mathbb{Z}/n\mathbb{Z}\}.$$

また, $\tau_{m+m'} = \tau_m \circ \tau_{m'}$ $(m, m' \in \mathbb{Z}/n\mathbb{Z})$ が成り立つので, $\mathbb{Z}/n\mathbb{Z} \to \mathrm{Fix}(r)$, $m \mapsto \tau_m$ は群同型である.
次に, $\mathrm{Fix}(r) \cap \mathrm{Fix}(s) = \{\mathrm{id}\}$ を示す. $\sigma \in \mathrm{Aut}(D_n)$ で $\sigma(r) = r$ かつ $\sigma(s) = s$ とすると, $D_n = \langle r, s \rangle$ より, $\sigma = \mathrm{id}$ である. よって $\mathrm{Fix}(r) \cap \mathrm{Fix}(s) = \{\mathrm{id}\}$ が成り立つ.
次に, $\mathrm{Fix}(s)$ の元について調べる. $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対し, D_n の自己同型 σ_a を次のよう定める.

$$\begin{aligned} \sigma_a(r^k) = r^{ak}, \quad k \in 0, 1, \ldots, n-1 \\ \sigma_a(sr^k) = sr^{ak}. \end{aligned}$$

σ_a が準同型であることは以下の式から分かる.

$$\begin{aligned} \sigma_a(sr^k sr^{k'}) = \sigma_a(r^{k'-k}) = r^{a(k'-k)} \\ \text{一方,} \quad \sigma_a(sr^k)\ \sigma_a(sr^{k'}) = sr^{ak} sr^{ak'} = r^{ak'-ak} = r^{a(k'-k)}. \end{aligned}$$

また, σ_a が全単射であるので, $\sigma_a \in \mathrm{Aut}(D_n)$ である. 定義より $\sigma_a(s) = s$ であるので, $\sigma_a \in \mathrm{Fix}(s)$ である. 逆に, $\sigma \in \mathrm{Fix}(s)$ とすると, $\sigma(r) = r^a$ となる $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ が存在する. ゆえに $\sigma(r) = r^a = \sigma_a(r)$ かつ $\sigma(s) = s = \sigma_a(s)$ である. r, s が D_n の生成系であるので, $\sigma = \sigma_a$ となる. よって, 以下が成り立つ.

$$\mathrm{Fix}(s) = \{\sigma_a \mid a \in (\mathbb{Z}/n\mathbb{Z})^\times\}.$$

また, $\sigma_a \circ \sigma_b = \sigma_{ab}$ $(a, b \in (\mathbb{Z}/n\mathbb{Z})^\times)$ が成り立つので, 写像 $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Fix}(s)$, $a \mapsto \sigma_a$ は群同型である.
任意の $\sigma \in \mathrm{Aut}(D_n)$ に対し $\sigma = \tau_1 \circ \tau_2$ となる $\tau_1 \in \mathrm{Fix}(r)$ 及び $\tau_2 \in \mathrm{Fix}(s)$ が存在することを示す. $\sigma \in \mathrm{Aut}(D_n)$ とする. $\sigma(r) = r^a$ となる $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ が存在する. $\tau := \sigma \circ \sigma_a^{-1}$ とおく. $\sigma|_{\langle r \rangle} = \sigma_a|_{\langle r \rangle}$ より, $\tau|_{\langle r \rangle} = \mathrm{id}$ であり, すなわち $\tau \in \mathrm{Fix}(r)$ である. また, $\sigma = \tau \circ \sigma_a$ が成り立つ. 以上より,

$$\mathrm{Aut}(D_n) = \mathrm{Fix}(r) \rtimes \mathrm{Fix}(s)$$

と書ける. 最後に, $m \in \mathbb{Z}/n\mathbb{Z}$, $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ とすると

$$\sigma_a \circ \tau_m \circ \sigma_a^{-1}(s) = \sigma_a(sr^m) = sr^{am} = \tau_{am}$$

であるので (3) が分かる.

7　対称群

7.1　対称群の復習

置換 $\sigma \in \mathfrak{S}_n$ に対し, その符号 $\mathrm{sgn}(\sigma) \in \{\pm 1\}$ が定義できる. 符号は群準同型

$$\mathrm{sgn}\colon \mathfrak{S}_n \longrightarrow \{\pm 1\}$$

を与える. 符号 1 の置換を偶置換と呼び, 偶置換全体のなす部分群を交代群といい, $\mathfrak{A}_n$ と表す. 準同型の定理により同型写像 $\mathfrak{S}_n/\mathfrak{A}_n \simeq \{\pm 1\}$ が存在するので, $\mathfrak{A}_n$ が指数 2 の部分群である. また, $\mathfrak{A}_n = \mathrm{Ker}(\mathrm{sgn})$ より, $\mathfrak{A}_n$ が $\mathfrak{S}_n$ の正規部分群でる.

同様に, X が有限集合ならば, X の対称群 $\mathfrak{S}(X)$ が定義できる (例 1.9 参照). $X = \{x_1, \ldots, x_n\}$ (ただし $n = |X|$) とおく. $f\colon X \to X$ を全単射とする.

$$f(x_i) = x_{\sigma(i)}, \quad i = 1, \ldots, n$$

を満たす置換 $\sigma \in \mathfrak{S}_n$ が一意的に存在する. このとき, $\mathrm{sgn}(\sigma)$ は X の元の添字の付け方によらないことに注意する. なぜならば, $X = \{x'_1, \ldots, x'_n\}$ とおくと, $x'_i = x_{\tau(i)}$ となる $\tau \in \mathfrak{S}_n$ が存在する. また, $f(x'_i) = x'_{\sigma'(i)}$ で定まる置換 σ' を考える. このとき,

$$\begin{aligned} & f(x_{\tau(i)}) = f(x'_i) = x'_{\sigma'(i)} = x_{\tau(\sigma'(i))} \\ \text{一方}, \quad & f(x_{\tau(i)}) = x_{\sigma(\tau(i))} \end{aligned}$$

である. ゆえに, $\tau(\sigma'(i)) = \sigma(\tau(i))$ であり, すなわち $\sigma' = \tau^{-1}\sigma\tau$ である. とくに, $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\sigma')$ が成り立つ. 以上より,

$$\mathrm{sgn}(f) := \mathrm{sgn}(\sigma)$$

とおくことによって, well-defined な群準同型 $\mathrm{sgn}\colon \mathfrak{S}(X) \to \{\pm 1\}$ が定まり, さらにそれが X の元の添字の付け方によらない. sgn の核を $\mathfrak{A}(X)$ とおく.

$k \geq 2$ とし, $i_1, \ldots, i_k \in \{1, \ldots, n\}$ が相異なるとする. $i_1, \ldots, i_k$ 以外の元を固定する置換で, $\sigma(i_j) = i_{j+1}$ $(1 \leq j < k)$ かつ $\sigma(i_k) = i_1$ を満たすものを

$$(i_1 \ \ldots \ i_k)$$

とおき, 長さ k の巡回置換という. 長さ k の巡回置換の符号は $(-1)^{k+1}$ である. よって, 巡回置換が偶置換であるためには, その長さが奇数であることが必要十分である. $c_1, \ldots, c_r$ を巡回置換とし, $c_i = (a_{i,1} \ \ldots \ a_{i,k_i})$ とおく. 全ての $a_{i,j}$ が相異なるときに, $c_1, \ldots, c_r$ が互いに素であるという.

定理 7.1　$\sigma \in \mathfrak{S}_n$ とする. σ が互いに素な巡回置換の積 $c_1 \ldots c_r$ で表せる. また, c_i の順序を除いてこの分解が一意的である.

例 7.2. 以下の置換を考える.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 6 & 5 & 4 & 7 & 8 & 1 \end{pmatrix}$$

$\sigma = (1\ 3\ 6\ 7\ 8)(4\ 5)$ と分解できる.

定理 7.3　以下の集合はそれぞれ $\mathfrak{S}_n$ の生成系である.

(1) 互換全体の集合：$\{(i\ j) \mid 1 \leq i < j \leq n\}$.

(2) 隣接互換全体の集合：$\{(i\ i+1) \mid 1 \leq i < n\}$.

(3) $\sigma = \{(1\ 2 \ldots\ n)\}$, $\tau = (1\ 2)$ の 2 つの元.

証明

- (1) を示す. 定理 7.1 により, 任意の長さ k の巡回置換が互換の積と分解できることを示せば十分である.

$$(c_1\ \dots\ c_k) = (c_1\ c_k)(c_1\ c_{k-1})\dots(c_1 c_2)$$

が成り立つので, 主張が分かる.

- (2) を示す. (1) より, 任意の互換が隣接互換の積と表せることを示せば十分である. $1 \leq i < j \leq n$ とすると,

$$\begin{aligned}(i\ j) &= (i\ i+1)(i+1\ j)(i\ i+1)\\ (i+1\ j) &= (i+1\ i+2)(i+2\ j)(i+1\ i+2)\\ &\vdots\\ (j-2\ j) &= (j-2\ j-1)(j-1\ j)(j-2\ j-1).\end{aligned}$$

である. 以上より, $(i\ j)$ が $2(j-i)-1$ 個の隣接互換の積で表せる.

- (3) を示す. (2) より, 任意の隣接互換が $\sigma = (1\ 2\dots\ n)$ と $\tau = (1\ 2)$ で生成される部分群に属することを示せば良い. 以下が成り立つ.

$$\begin{aligned}(2\ 3) &= \sigma\tau\sigma^{-1}\\ (3\ 4) &= \sigma(2\ 3)\sigma^{-1}\\ &\vdots\\ (n-1\ n) &= \sigma(n-2\ n-1)\sigma^{-1}.\end{aligned}$$

以上より, 全ての隣接互換が σ と τ で生成されるので, 主張が分かる.

命題 7.4　$n \geq 3$ とする. 長さ 3 の巡回置換全体の集合が $\mathfrak{A}_n$ を生成する.

証明

$\sigma \in \mathfrak{A}_n$ とする. 定理 7.3 により, 互換 $t_1, \dots, t_r$ が存在し, $\sigma = t_1 \dots t_r$ と表せる. また, $\mathrm{sgn}(\sigma) = 1$ より, r が偶数である. よって, 2 つの互換の積が長さ 3 の巡回置換の積と表せることを示せば良い. $t = (ab)$, $t' = (ac)$ のとき, $tt' = (acb)$ より従う. t, t' が互いに素であるとき, $t = (ab)$, $t' = (cd)$ とおく (但し a, b, c, d は相異なる). このとく, $s = (bc)$ とおくと, $tt' = (ts)(st')$ と書ける. 以上より, ts と st' は長さ 3 の巡回置換であるので主張が従う.

系 7.5　$\mathfrak{A}_n$ は $\mathfrak{S}_n$ の指数 2 の唯一の部分群である.

証明

H を $\mathfrak{S}_n$ の指数 2 の部分群とする. 命題 2.24 により, $H \triangleleft \mathfrak{S}_n$ である. よって, $\mathfrak{S}_n/H$ は位数 2 の群である. ゆえに, 任意の $\sigma \in \mathfrak{S}_n$ に対し, $\sigma^2 H = H$ であり, すなわち $\sigma^2 \in H$ が成り立つ. $\tau = (abc)$ が長さ 3 の巡回置換ならば, $\tau = (acb)^2$ と書けるので, $\tau \in H$ である. よって, 長さ 3 の巡回置換の全てが H に属する. 命題 7.4 により, $\mathfrak{A}_n \subset H$ となり, ゆえに $H = \mathfrak{A}_n$ が成り立つ.

命題 7.6　$n \geq 3$ のとき, $\mathfrak{S}_n$ の中心は自明である.

証明

$\sigma \in Z(\mathfrak{S}_n)$ とする．任意の $a, b \in \{1, \ldots, n\}$ に対し，$(ab) = \sigma(ab)\sigma^{-1} = (\sigma(a)\sigma(b))$ が成り立つ．ゆえに，$\sigma(\{a, b\}) = \{a, b\}$ が成り立つ．c を a, b とは異なる元とする．同様に，$\sigma(\{a, c\}) = \{a, c\}$ が成り立つので，$\sigma(a) = a$ である．以上より，$\sigma = \mathrm{id}$ である．

7.2 k-推移的作用

自然数 k 及び集合 X に対し，

$$X_k = \{(x_1, \ldots, x_k) \in X^k \mid x_1, \ldots, x_n \text{ は相異なる } \}.$$

とおく．G を群とし，G が X に作用しているとする．このとき，$(x_1, \ldots, x_k) \in X_k$，$g \in G$ に対し $g \cdot (x_1, \ldots, x_k) = (g \cdot x_1, \ldots, g \cdot x_k)$ とおくことによって，G の X_k への群作用が定まる．

定義 7.7　G の X_k への作用が推移的であるとき，G が X に k-推移的に作用しているという．

$\mathfrak{S}_n$ の $\{1, \ldots, n\}$ への自然な作用 (すなわち $\sigma \cdot k = \sigma(k)$ で定まる作用) を考える．

命題 7.8　$1 \leq k \leq n$ とする．$\mathfrak{S}_n$ が $\{1, \ldots, n\}$ に k-推移的に作用している．

証明

$a = (a_1, \ldots, a_k)$ と $b = (b_1, \ldots, b_k)$ をそれぞれ $\{1, \ldots, n\}$ の相異なる元からなる 2 つの組とする．$\sigma(a_i) = b_i$ とおくと，$\sigma\colon \{a_1, \ldots, a_k\} \to \{b_1, \ldots, b_k\}$ が全単射である．明らかに，σ を全単射 $\{1, \ldots, n\} \to \{1, \ldots, n\}$ に延長できる．$\sigma \cdot a = b$ が成り立つ．よって，$\mathfrak{S}_n$ が $\{1, \ldots, n\}$ に k-推移的に作用している．

命題 7.9　$1 \leq k \leq n-2$ とする．$\mathfrak{A}_n$ が $\{1, \ldots, n\}$ に k-推移的に作用している．

証明

$a = (a_1, \ldots, a_k)$ と $b = (b_1, \ldots, b_k)$ をそれぞれ $\{1, \ldots, n\}$ の相異なる元の組とする．$A = \{a_1, \ldots, a_k\}$ とおく．$k \leq n-2$ という仮定より，$x, y \in \{1, \ldots, n\} \setminus A$ を満たす元 x, y $(x \neq y)$ が取れる．命題 7.8 により $\sigma(a_i) = b_i$ $(i = 1, \ldots, k)$ を満たす置換 $\sigma \in \mathfrak{S}_n$ が存在する．$\sigma \notin \mathfrak{A}_n$ の場合，$\sigma' = \sigma \circ (x\ y)$ を考える．$\sigma' \in \mathfrak{A}_n$ かつ $\sigma'(a_i) = b_i$ が成り立つ．以上より，$\sigma \cdot a = b$ を満たす $\sigma \in \mathfrak{A}_n$ が存在する．主張が従う．

7.3 共役類

$\sigma \in \mathfrak{S}_n$ とし，$\theta = (i_1\ \ldots\ i_k)$ $(k \geq 2)$ を長さ k の巡回置換とする．このとき，

$$\sigma\theta\sigma^{-1} = (\sigma(i_1)\ \ldots\ \sigma(i_k))$$

が成り立つ．とくに，巡回置換の共役元は，同じ長さの巡回置換である．

定理 7.10　$\sigma, \sigma' \in \mathfrak{S}_n$ とする．また, σ, σ' を以下のように互いに素な巡回置換に分解されるとする．

$$\sigma = c_1 \dots c_r$$
$$\sigma' = c'_1 \dots c'_s.$$

このとき, σ と σ' が $\mathfrak{S}_n$ において共役になるためには, 以下の条件が必要十分である．

$$r = s \quad \text{かつ} \quad \text{順序を除いて } c_1, \dots, c_r \text{ の長さは } c'_1, \dots, c'_r \text{ の長さと一致する．} \tag{7.1}$$

証明

- σ, σ' が共役であるとし, $\sigma' = \tau\sigma\tau^{-1}$ $(\tau \in \mathfrak{S}_n)$ とする．このとき,

  $$\sigma' = \tau\sigma\tau^{-1} = (\tau c_1 \tau^{-1}) \dots (\tau c_r \tau^{-1})$$

  である．$\tau c_i \tau^{-1}$ は長さ k_i の巡回置換である．また, $c_1, \dots, c_r$ が互いに素であるので, $\tau c_1 \tau^{-1}, \dots, \tau c_r \tau^{-1}$ も互いに素である．分解の一意性より, 順序を除いて 巡回置換 $\{\tau c_i \tau^{-1}\}_i$ と $\{c'_i\}_i$ が一致する．とくに, $r = s$ であり, かつ順序を除いて c_i と c'_i の長さが一致する．
- 逆に, 条件 (7.1) が成り立つとする．このとき, c_i, c'_i の順序を変えて, 各 c_i の長さが c'_i の長さに等しいとして良い．$c_i = (a_{i,1} \ \dots \ a_{i,k_i})$, $c'_i = (a'_{i,1} \ \dots \ a'_{i,k_i})$ とおく．$\{a_{i,j}\}_{i,j}$, また $\{a'_{i,j}\}_{i,j}$ は相異なる元からなる部分集合で, その濃度が等しい．ゆえに,

  $$\tau(a_{i,j}) = a'_{i,j}, \qquad 1 \le i \le r,\ 1 \le j \le k_i$$

  を満たす置換 $\tau \in \mathfrak{S}_n$ が存在する．ゆえに, $\tau c_i \tau^{-1} = c'_i$ となり, すなわち $\tau\sigma\tau^{-1} = \sigma'$ である．

例 7.11. 以下の置換を考える．

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 8 & 7 & 1 & 4 & 6 & 2 \end{pmatrix}, \quad \sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 8 & 4 & 7 & 6 & 1 & 2 & 3 \end{pmatrix}$$

$\sigma = (1\ 3\ 8\ 2\ 5)(4\ 7\ 6)$ であり, $\sigma' = (1\ 5\ 6)(2\ 8\ 3\ 4\ 7)$ である．よって, σ, σ' は 順序を除いて同じ長さを持つ互いに素な巡回置換の積で表せる．ゆえに, σ と σ' が共役である．

命題 7.12

(1) $2 \le k \le n$ とする．長さ k の巡回置換の全てが $\mathfrak{S}_n$ において共役である．

(2) $n \ge 5$ とする．k が奇数で $3 \le k \le n-2$ とする．このとき, 長さ k の巡回置換の全てが $\mathfrak{A}_n$ において共役である．

証明

(1) は定理 7.10 から分かる．(2) を示す．長さ k の 2 つの巡回置換 $\sigma = (a_1 \ \dots \ a_k)$, $\sigma' = (b_1 \ \dots \ b_k)$ を考える．命題 7.9 により, $\tau(a_i) = b_i$ を満たす $\tau \in \mathfrak{A}_n$ が存在する．$\tau\sigma\tau^{-1} = \sigma'$ となり, 主張が従う．

7.4　$n = 3$ の場合

- $\mathfrak{S}_3$ の位数は $6 = 2 \times 3$ である．正規部分群として $\mathfrak{A}_3$ を持つ．$\mathfrak{S}_3$, $\mathfrak{A}_3$ は以下の元から構成されている．

  $$\mathfrak{S}_3 = \{\mathrm{id}, (12), (23), (13), (123), 132)\}$$
  $$\mathfrak{A}_3 = \{\mathrm{id}, (123), (132)\}.$$

  $\mathfrak{A}_3$ は $\mathfrak{S}_3$ の唯一の 3 シロー部分群である．$\mathfrak{S}_3$ の 2 シロー部分群は $\langle(12)\rangle$, $\langle(23)\rangle$, $\langle(13)\rangle$ の 3 つである．

- $\mathfrak{S}_3$ のそれぞれの元の中心化群を調べる．命題 7.6 により $Z(\mathfrak{S}_3) = \{\mathrm{id}\}$ であるので，任意の $\tau \in \mathfrak{S}_3$ $(\tau \neq \mathrm{id})$ に対し $\mathrm{Cent}_{\mathfrak{S}_3}(\tau) \neq \mathfrak{S}_3$ である．また，$\langle\tau\rangle \subset \mathrm{Cent}_{\mathfrak{S}_3}(\tau)$ が成り立つ．$\langle\tau\rangle$ の指数は 2 または 3 であるので，ラグランジュ定理により $\mathrm{Cent}_{\mathfrak{S}_3}(\tau) = \langle\tau\rangle$ であることが分かる．
- $\mathfrak{S}_3$ の導来部分群について考える．明らかに，$\mathfrak{S}_3/\mathfrak{A}_3$ はアーベル群であるので，$D(\mathfrak{S}_3) \subset \mathfrak{A}_3$ が成り立つ．また，$\mathfrak{S}_3$ がアーベル群でないので，$D(\mathfrak{S}_3) \neq \{\mathrm{id}\}$ である．よって，$D(\mathfrak{S}_3) = \mathfrak{A}_3$ である．
- $N = \mathfrak{A}_3$, $H = \langle(12)\rangle$ とおくと，
$$\mathfrak{S}_3 = N \rtimes H$$
が成り立つ．
- 位数 6 の群について考える．(6.2) より，$n \geq 3$ のとき単射準同型 $D_n \to \mathfrak{S}_n$ が存在する．$n = 3$ のとき，$|\mathfrak{S}_3| = |D_3| = 6$ より，この写像は群同型である．また，命題 6.10 より，位数 $6 = 2 \times 3$ の群は同型を除いてちょうど 2 つ存在する．以下の命題が分かる．

命題 7.13　G を位数 6 の群とする．
(1) G がアーベル群ならば，$G \simeq \mathbb{Z}/6\mathbb{Z}$ である．
(2) G がアーベル群でない場合は，$G \simeq \mathfrak{S}_3$ である．

7.5　$n = 4$ の場合

7.5.1　シロー部分群

- $\mathfrak{A}_4$, $\mathfrak{S}_4$ の位数はそれぞれ $12 = 2^2 \times 3$, $24 = 2^3 \times 3$ である．$\mathfrak{A}_4$, $\mathfrak{S}_4$ はそれぞれ，以下のような形の元から構成されている．ただし，以下は a, b, c, d を $\{1, 2, 3, 4\}$ の相異なるものとする．
$$\mathfrak{A}_4 \ : \quad \mathrm{id},\ (abc),\ (ab)(cd)$$
$$\mathfrak{S}_4 \ : \quad \mathrm{id},\ (ab),\ (abc),\ (ab)(cd),\ (abcd)$$
$\mathfrak{A}_4$ の 2 シロー部分群は位数 4 の部分群である．(abc) という形の置換は位数 3 の元だから，2 シロー部分群に属さない．ゆえに，
$$H_2 := \{\mathrm{id}, (12)(23), (13)(24), (14)(23)\}$$
は $\mathfrak{A}_4$ の唯一の 2 シロー部分群である．とくに，$H_2 \triangleleft \mathfrak{A}_4$ である．長さ 3 の巡回置換の各元は 3 シロー部分群を生成する．ゆえに，3 シロー部分群の個数は 4 である．それらは $\mathfrak{S}_4$ の 3 シロー部分群でもある．
- 次に，$\mathfrak{S}_4$ の 2 シロー部分群について考える．τ を H_2 の元とする $(\tau \neq \mathrm{id})$．定理 7.10 により，$\mathfrak{S}_4$ における τ の共役類は $H_2 \setminus \{\mathrm{id}\}$ である．ゆえに，命題 4.13 により，
$$3 = [\mathfrak{S}_4 : \mathrm{Cent}_{\mathfrak{S}_4}(\tau)] = \frac{|\mathfrak{S}_4|}{|\mathrm{Cent}_{\mathfrak{S}_4}(\tau)|}$$
が成り立つ．よって，$|\mathrm{Cent}_{\mathfrak{S}_4}(\tau)| = 8$ であり，すなわち $\mathrm{Cent}_{\mathfrak{S}_4}(\tau)$ は $\mathfrak{S}_4$ の 2 シロー部分群である．シローの定理より全ての 2 シロー部分群が互いに共役であるので，$\mathfrak{S}_4$ の 2 シロー部分群は
$$\mathrm{Cent}_{\mathfrak{S}_4}(\tau), \qquad \tau \in H_2 \setminus \{\mathrm{id}\}$$
の 3 つである．明らかに，$H_2 \subset \mathrm{Cent}_{\mathfrak{S}_4}(\tau)$ である．さらに，$\tau = (ab)(cd)$ と書くと，(ab) と (cd) が τ と交換する (ただし，a, b, c, d が相異なるとする)．ゆえに，$\mathrm{Cent}_{\mathfrak{S}_4}(\tau) = \langle(ab), H_2\rangle = \langle(cd), H_2\rangle$ である．

7.5.2　元の中心化部分群

以下の表は，$\mathfrak{S}_4$, $\mathfrak{A}_4$ の元の中心化部分群をまとめたものである．

元	$\mathrm{Cent}_{\mathfrak{S}_4}(\tau)$
id	$\mathfrak{S}_4$
(ab)	$\langle (ab), (cd) \rangle$
$(ab)(cd)$	$\langle H_2, (ab) \rangle$
(abc)	$\langle (abc) \rangle$
$(abcd)$	$\langle (abcd) \rangle$

表 2: $\mathfrak{S}_4$ の元の中心化部分群

元	$\mathrm{Cent}_{\mathfrak{A}_4}(\tau)$
id	$\mathfrak{A}_4$
(abc)	$\langle (abc) \rangle$
$(ab)(cd)$	H_2

表 3: $\mathfrak{A}_4$ の元の中心化部分群

証明

$\tau \in \mathfrak{A}_4$ のとき, $\mathrm{Cent}_{\mathfrak{A}_4}(\tau) = \mathrm{Cent}_{\mathfrak{S}_4}(\tau) \cap \mathfrak{A}_4$ と書けるので, $\mathfrak{S}_4$ における中心化群のみについて考えれば十分である. ただし, a, b, c, d は $\{1, 2, 3, 4\}$ の相異なるものとする.

- $\mathfrak{S}_4$ の互換の数は 6 である. 全ての互換が互いに共役であるので, 任意の互換 τ に対し,

$$6 = \frac{|\mathfrak{S}_4|}{|\mathrm{Cent}_{\mathfrak{S}_4}(\tau)|}$$

  が成り立つ. ゆえに, $|\mathrm{Cent}_{\mathfrak{S}_4}(\tau)| = 4$ である. $\tau = (ab)$ とおき, $\{1, 2, 3, 4\} \setminus \{a, b\} = \{c, d\}$ とおく. 明らかに $(cd) \in \mathrm{Cent}_{\mathfrak{S}_4}(\tau)$ である. ゆえに, $\mathrm{Cent}_{\mathfrak{S}_4}(\tau) = \langle (ab), (cd) \rangle$ である.
- $\tau = (ab)(cd)$ とする (ただし, a, b, c, d は相異なる). このとき, $\mathrm{Cent}_{\mathfrak{S}_4}(\tau) = \langle H_2, (ab) \rangle$ が成り立つことは既に §7.5.1 で示した.
- 次に, $\tau = (abc)$ とする (ただし, a, b, c は相異なるとする). $\mathfrak{S}_4$ では, 長さ 3 の巡回置換はちょうど 8 個があり, それが全て共役である. よって,

$$8 = \frac{|\mathfrak{S}_4|}{|\mathrm{Cent}_{\mathfrak{S}_4}(\tau)|}$$

  であり, すなわち $|\mathrm{Cent}_{\mathfrak{S}_4}(\tau)| = 3$ が成り立つ. したがって, $\mathrm{Cent}_{\mathfrak{S}_4}(\tau) = \langle \tau \rangle$ である.
- $\tau = (abcd)$ とする (ただし, a, b, c, d は相異なるとする). $\mathfrak{S}_4$ では, 長さ 4 の巡回置換はちょうど 6 個があり, それが全て共役である. よって,

$$6 = \frac{|\mathfrak{S}_4|}{|\mathrm{Cent}_{\mathfrak{S}_4}(\tau)|}$$

  であり, すなわち $|\mathrm{Cent}_{\mathfrak{S}_4}(\tau)| = 4$ が成り立つ. したがって, $\mathrm{Cent}_{\mathfrak{S}_4}(\tau) = \langle \tau \rangle$ である.

7.5.3 部分群一覧

以下の表は, $\mathfrak{S}_4$, $\mathfrak{A}_4$ の部分群及びそれぞれの正規化群を位数別にまとめたものである.
さらに, $D(\mathfrak{S}_4) = D(\mathfrak{A}_4) = H_2$ が成り立つ.

証明

- $\mathfrak{A}_4$ の場合を考える. 位数 6 の部分群が存在しないことのみ確認する. 他の位数の部分群の形は既に知っている. H を $\mathfrak{A}_4$ の部分群とし, $|H| = 6$ とする. 命題 2.24 により, $H \triangleleft \mathfrak{A}_4$ となる. H に含まれる 3 シロー部分群が存在する. $\mathfrak{A}_4$ の 3 シロー部分群が全て共役であることと, H が $\mathfrak{A}_4$ の正規部分群であることから, 全ての 3 シロー部分群が H に含まれ, $|H| = 6$ に矛盾する. ゆえに, $\mathfrak{A}_4$ の中で位数 6 の部分群が存在しない.
  $H \subset \mathfrak{A}_n$ が $\mathfrak{A}_n$ の部分群ならば, $N_{\mathfrak{A}_n}(H) = N_{\mathfrak{S}_n}(H) \cap \mathfrak{A}_n$ と書けるので, $\mathfrak{S}_n$ における正規化群のみについて考えれば十分である. 以下, $\mathfrak{S}_4$ の部分群及びそれらの正規化群を求める. $H \subset \mathfrak{S}_n$ を部

位数	$\mathfrak{S}_4$ の部分群	正規化群
1	$\{\mathrm{id}\}$	$\mathfrak{S}_4$
2	$\langle(ab)\rangle$	$\langle(ab),(cd)\rangle$
	$\langle(ab)(cd)\rangle$	$\langle H_2,(ab)\rangle$
3	$\langle(abc)\rangle$	$\langle(ab),(bc)\rangle$
4	$\langle(abcd)\rangle$	$\langle H_2,(ac)\rangle$
	$\langle(ab),(cd)\rangle$	$\langle H_2,(ab)\rangle$
	H_2	$\mathfrak{S}_4$
6	$\langle(ab),(bc)\rangle$	$\langle(ab),(bc)\rangle$
8	$\langle H_2,(ab)\rangle$	$\langle H_2,(ab)\rangle$
12	$\mathfrak{A}_4$	$\mathfrak{S}_4$
24	$\mathfrak{S}_4$	$\mathfrak{S}_4$

表 4: $\mathfrak{S}_4$ の部分群

位数	部分群	正規化群
1	$\{\mathrm{id}\}$	$\mathfrak{A}_4$
2	$\langle(ab)(cd)\rangle$	H_2
3	$\langle(abc)\rangle$	$\langle(abc)\rangle$
4	H_2	$\mathfrak{A}_4$
6	なし	なし
12	$\mathfrak{A}_4$	$\mathfrak{A}_4$

表 5: $\mathfrak{A}_4$ の部分群

分群とする.

- $|H|=1$ のとき, $H=\{\mathrm{id}\}$ であり, $N_{\mathfrak{S}_n}(\{\mathrm{id}\})=\mathfrak{S}_n$ である.
- $|H|=2$ とする. このとき, $H=\langle\tau\rangle$, $\tau=(ab)$ または $\tau=(ab)(cd)$ と書ける. ただし, a,b,c,d が相異なるとする. 明らかに, $N_{\mathfrak{S}_4}(\langle\tau\rangle)=\mathrm{Cent}_{\mathfrak{S}_4}(\tau)$ となり, 主張が表 1 から従う.
- $|H|=3$ とする. このとき, $\tau=(abc)$ で $H=\langle\tau\rangle$ と表すことができる (ただし, a,b,c が相異なる). 位数 3 の部分群はちょうど 4 個が存在し, シロー定理より全てが共役である. ゆえに, $[\mathfrak{S}_4:N_{\mathfrak{S}_4}(H)]=4$, すなわち $N_{\mathfrak{S}_4}(H)=6$ である. 明らかに, $\langle(ab),(bc)\rangle\subset N_{\mathfrak{S}_4}(H)$ である. よって, $N_{\mathfrak{S}_4}(H)=\langle(ab),(bc)\rangle$ が成り立つ.
- $|H|=4$ とする. このとき, 以下の 3 つの場合に分けて考える.
  (a) まず, $H=\langle(abcd)\rangle$ の場合を考える. この形の部分群はちょうど 3 つ存在する. また, 長さ 4 の巡回置換は全て $\mathfrak{S}_4$ において互いに共役であるので, それら共役である. ゆえに, $[\mathfrak{S}_4:N_{\mathfrak{S}_4}(H)]=3$ であり, すなわち $N_{\mathfrak{S}_4}(H)=8$ である. よって, $N_{\mathfrak{S}_4}(H)$ は 2 シロー部分群である. 明らかに, $(ac)\in N_{\mathfrak{S}_4}(H)$ であるので, $N_{\mathfrak{S}_4}(H)=\langle H_2,(ac)\rangle$ が成り立つ.
  (b) $H=H_2$ の場合は, $H\triangleleft\mathfrak{S}_4$ であるので $N_{\mathfrak{S}_4}(H)=\mathfrak{S}_4$ である.
  (c) 最後に, H の中で互換 $\tau=(ab)$ が存在する場合を考える. H が可換群であるので, $H\subset\mathrm{Cent}_{\mathfrak{S}_4}(\tau)$ である. 表 1 により, $\mathrm{Cent}_{\mathfrak{S}_4}(\tau)=\langle(ab),(cd)\rangle$ (a,b,c,d が相異なる) が成り立つ. よって $H=\langle(ab),(cd)\rangle$ である. この形の部分群は全て共役であり, ちょうど 3 つが存在する. ゆえに, $N_{\mathfrak{S}_4}(H)$ の指数が 3 となり, すなわち $|N_{\mathfrak{S}_4}(H)|=8$ である. ゆえに $N_{\mathfrak{S}_4}(H)$ は 2 シロー部分群である. 明らかに $(ab)\in N_{\mathfrak{S}_4}(H)$ であるので, $N_{\mathfrak{S}_4}(H)=\langle H_2,(ab)\rangle$ が成り立つ.
- $|H|=6$ とする. このとき, H の中で長さ 3 の巡回置換 (abc) が存在する. $H'=\langle(abc)\rangle$ とおくと $[H:H']=2$ であるので, $H'\triangleleft H$ である. よって, $H\subset N_{\mathfrak{S}_4}(H')$ である. $N_{\mathfrak{S}_4}(H')=\langle(ab),(bc)\rangle$ であり, 位数 6 の部分群である. ゆえに $H=\langle(ab),(bc)\rangle$ が成り立つ. $\{1,2,3,4\}\setminus\{a,b,c\}=\{d\}$ とおくと, H は d を固定する置換全体の部分群である. ゆえに, $\sigma H\sigma^{-1}$ ($\sigma\in\mathfrak{S}_4$) は $\sigma(d)$ の固定部分群である. よって, H の共役類の濃度は 4 となり, $N_{\mathfrak{S}_4}(H)$ の指数も 4 である. すなわち, $|N_{\mathfrak{S}_4}(H)|=6$ である. したがって, $N_{\mathfrak{S}_4}(H)=H$ が成り立つ.
- 位数 8 の部分群は 2 シロー部分群である. §7.5.1 により, それらは $\langle H_2,(ab)\rangle$ という形である. $\mathfrak{S}_4$ の 2 シロー部分群の個数は 3 であるので, $N_{\mathfrak{S}_4}(H)$ の指数は 3 である. ゆえに, $N_{\mathfrak{S}_4}(H)=H$ が成り立つ.
- 位数 12 の部分群は系 7.5 により $\mathfrak{A}_4$ に限る. $\mathfrak{A}_n$ が正規部分群だから, その正規化群は $\mathfrak{S}_4$ である.

- $|H| = 24$ のとき, $H = \mathfrak{S}_4$, $N_{\mathfrak{S}_4}(H) = \mathfrak{S}_4$ である.

7.6 単純群

定義 7.14 G を群とする. G が単純であるとは, G が非自明な正規部分群を持たないとき (すなわち, G の正規部分群が $\{e\}$ と G に限るとき) にいう.

定理 7.15 $n \geq 5$ のとき, $\mathfrak{A}_n$ が単純群である.

証明

(1) まず, $n = 5$ のときに定理の主張を証明する. $\mathfrak{A}_5$ の位数は 60 である. $\mathfrak{A}_5$ の置換は以下のように分類できる.

- 単位元 (1 個).
- $(ab)(cd)$ という形の置換 (但し, $a, b, c, d \in \{1, 2, 3, 4, 5\}$ は相異なる). このようなものは位数 2 の元であり, ちょうど 15 個が存在する.
- 長さ 3 の巡回置換 (20 個). このような元の位数は 3 である.
- 長さ 5 の巡回置換 (24 個). このような元の位数は 5 である.

命題 7.12 により, 長さ 3 の巡回置換の全てが $\mathfrak{A}_5$ において共役である. 同様に, $(ab)(cd)$ という形の元の全てが $\mathfrak{A}_5$ において共役である. なぜならば, $\sigma = (ab)(cd)$, $\sigma' = (a'b')(c'd')$ とおき, σ, σ' の唯一の固定点をそれぞれ e, e' とおく. 命題 7.9 により $\tau(a) = a'$, $\tau(b) = b'$, $\tau(e) = e'$ を満たす $\tau \in \mathfrak{A}_5$ が存在する. ゆえに, $\{\tau(c), \tau(d)\} = \{c', d'\}$ であり, $\tau\sigma\tau^{-1} = \sigma'$ となる.

$H \subset \mathfrak{A}_5$ $(H \neq \{\mathrm{id}\})$ を正規部分群とする. 正規性より $\sigma \in H$ ならば σ の全ての共役元が H に属する. よって, $(ab)(cd)$ という形の元が H に属するならば, この形の元の全てが H に属する. (abc) という形の元の場合も同様である. また, σ を長さ 5 の巡回置換とし, $\sigma \in H$ とする. このとき, $\langle\sigma\rangle \subset H$ であるので, H が $\mathfrak{A}_5$ の 5 シロー部分群を含む. 5 シロー部分群が互いに共役であるので, 全ての長さ 5 の巡回置換が H に属する.

H には少なくとも 2 種類の元が存在する. なぜならば, 単位元を含めて $1 + 15 = 16$, $1 + 20 = 21$, $1 + 24 = 25$ のいずれも $60 = |\mathfrak{A}_5|$ の約数でないからである. よって, $|H| \geq 1 + 15 + 20 = 36$ となる. したがって, $|H| = 60$ となり, $H = \mathfrak{A}_5$ が成り立つ.

(2) 次に, $n > 5$ の場合を考える. $H \subset \mathfrak{A}_n$ $(H \neq \{\mathrm{id}\})$ を正規部分群とし, $\sigma \in H$ $(\sigma \neq \mathrm{id})$ とする. $\sigma(a) \neq a$ を満たす $a \in \{1, \ldots, n\}$ をとり, $b = \sigma(a)$ とおく. また, $c \notin \{a, b, \sigma(b)\}$ を満たす元 c が存在する. $\tau = (acb)$ とおき, $\gamma = [\tau, \sigma] = \tau\sigma\tau^{-1}\sigma^{-1}$ とおく. H が正規部分群より, $\tau\sigma\tau^{-1} \in H$ である. ゆえに, $\gamma \in H$ である. また, $\tau^{-1} = (abc)$ より, $\sigma\tau^{-1}\sigma^{-1} = (\sigma(a)\ \sigma(b)\ \sigma(c))$ である. $A := \{a, b, c, \sigma(a), \sigma(b), \sigma(c)\}$ と定める. $b = \sigma(a)$ より, $|A| \leq 5$ が成り立つ. $\gamma = (acb)(\sigma(a)\ \sigma(b)\ \sigma(c))$ より, 任意の $k \in \{1, \ldots, n\} \setminus A$ に対し, $\gamma(k) = k$ が成り立つ. $|A| < 5$ の場合は A に元を付け加えて $|A| = 5$ として良い. 以下の群を考える:

$$G = \{\theta \in \mathfrak{A}_n \mid \text{全ての } k \notin A \text{ に対し, } \theta(k) = k\}.$$

$|A| = 5$ より $G \simeq \mathfrak{A}_5$ である. また, $H' := H \cap G$ とおくと $H' \triangleleft G$ である. 以上より $\gamma \in G$ が成り立つ. $n = 5$ のケースより G は単純群であるので, $H' = G$ となる. とくに, $(abc) \in H' \subset H$ である. 長さ 3 の巡回置換の全てが $\mathfrak{A}_n$ において互いに共役である (7.12 参照). ゆえに, H の正規性より, それらが全て H に属する. また, 長さ 3 の巡回置換全体が $\mathfrak{A}_n$ を生成するので, $H = \mathfrak{A}_n$ となる.

系 7.16　$n \geq 5$ とし, $\sigma \in \mathfrak{A}_n$ $(\sigma \neq \mathrm{id})$ とする. σ の共役元全体の集合を $S := \{\tau\sigma\tau^{-1} \mid \tau \in \mathfrak{S}_n\}$ とおく. このとき, S が $\mathfrak{S}_n$ を生成する.

証明

任意の $\sigma \in \mathfrak{A}_n$ に対し, $\sigma S \sigma^{-1} = S$ である. ゆえに, $H := \langle S \rangle$ とおくと, $\sigma H \sigma^{-1} = H$ が成り立つ. よって, H が $\mathfrak{A}_n$ の正規部分群である. したがって, $H = \mathfrak{A}_n$ が成り立つ.

系 7.17　$n \geq 5$ とし, $3 \leq k \leq n$ を奇数とする. このとき, 長さ k の巡回置換全体の集合は $\mathfrak{A}_n$ の生成系をなす.

命題 7.18　$n \geq 5$ のとき, $\mathfrak{S}_n$ の正規部分群は $\{1\}$, $\mathfrak{A}_n$, $\mathfrak{S}_n$ の 3 つに限る.

証明

$H \triangleleft \mathfrak{S}_n$ とする. このとき, $H \cap \mathfrak{A}_n \triangleleft \mathfrak{A}_n$ である. よって, $H \cap \mathfrak{A}_n = \{\mathrm{id}\}$ または $H \cap \mathfrak{A}_n = \mathfrak{A}_n$ である. $H \cap \mathfrak{A}_n = \{\mathrm{id}\}$ の場合は, $\mathrm{sgn}\colon H \to \{\pm 1\}$ は単射になる. ゆえに $|H| \leq 2$ となる. $|H| = 2$ ならば, 位数 2 の置換 τ が存在し, $H = \{\mathrm{id}, \tau\}$ である. よって, 任意の $\tau \in \mathfrak{S}_n$ に対し $\tau\sigma\tau^{-1} = \sigma$ となり, $\sigma \in Z(\mathfrak{S}_n)$ が成り立つ. $\mathfrak{S}_n$ の中心が自明であることに矛盾する. ゆえに, $H = \{1\}$ である. 最後に, $H \cap \mathfrak{A}_n = \mathfrak{A}_n$ のとき $\mathfrak{A}_n \subset H$ となるので, $H = \mathfrak{A}_n$ または $H = \mathfrak{S}_n$ である.

7.7　$\mathfrak{S}_n$ の自己同型群

命題 7.19　$\varphi\colon \mathfrak{S}_n \to \mathfrak{S}_n$ を自己同型とする. 以下が同値である.

(i) φ が内部自己同型である.

(ii) 全ての互換 t に対し $\varphi(t)$ が互換である.

(iii) 互換 t が存在し, $\varphi(t)$ が互換である.

証明

- 「(ii) $\Longrightarrow$ (iii)」は明らかである. また, 互換の共役元が互換であるので, 「(i) $\Longrightarrow$ (ii)」が成り立つ.
- 「(iii) $\Longrightarrow$ (ii)」を示す. t' を他の互換とする. 全ての互換が互いに共役であるので, $t' = \sigma t \sigma^{-1}$ となる $\sigma \in \mathfrak{S}_n$ が存在する. よって, $\varphi(t') = \varphi(\sigma)\varphi(t)\varphi(\sigma)^{-1}$ となる. $\varphi(t)$ が互換であるので, $\varphi(t')$ も互換である.
- 「(ii) $\Longrightarrow$ (i)」を示す. $\tau_i := (1\ i)$ とおく $(2 \leq i \leq n)$. $i \neq j$ のとき, $\tau_i\tau_j \neq \tau_j\tau_i$ であるので, $\varphi(\tau_i)\varphi(\tau_j) \neq \varphi(\tau_j)\varphi(\tau_i)$ である. ゆえに, $\varphi(\tau_i)$ と $\varphi(\tau_j)$ は互いに素な互換でない. よって, $\varphi(\tau_2) = (a_1\ a_2)$ かつ $\varphi(\tau_3) = (a_1\ a_3)$ と書ける (但し a_1, a_2, a_3 は相異なる元である). 全ての $i = 2, \ldots, n$ に対し, $\varphi(\tau_i) = (a_1\ a_i)$ であることを示す. $i > 3$ の場合を考えれば十分である. $\gamma = (a_2\ a_3)$ とおくと,

$$\gamma = (a_1\ a_2)(a_1\ a_3)(a_1\ a_2) = \varphi(\tau_2)\varphi(\tau_3)\varphi(\tau_2)^{-1} = \varphi(\tau_2\tau_3\tau_2^{-1}) = \varphi((2\ 3)) \tag{7.2}$$

と表せる. $\varphi(\tau_i)$ は $\varphi(\tau_2) = (a_1\ a_2)$ 及び $\varphi(\tau_3) = (a_1\ a_3)$ の両方とは素でなく, かつ (7.2) より $\varphi(\tau_i) \neq (a_2\ a_3)$ であるので, $\varphi(\tau_i) = (a_1\ a_i)$ となる a_i が存在する. 但し, $\{a_1, \ldots, a_n\} = \{1, \ldots, n\}$

であるので, $i \mapsto a_i$ は $\{1, \dots, n\}$ の置換である. この置換を α とおくと,

$$\varphi(\tau_i) = (a_1 \ a_i) = (\alpha(1) \ \alpha(i)) = \alpha\tau_i\alpha^{-1}$$

となる. $\{\tau_2, \dots \tau_n\}$ が $\mathfrak{S}_n$ を生成するので, 全ての $\sigma \in \mathfrak{S}_n$ に対し $\varphi(\sigma) = \alpha\sigma\alpha^{-1}$ となる. 以上より, φ が内部自己同型である.

$k_1, \dots, k_n \in \mathbb{Z}_{\geq 0}$ で $n = \sum_{i=1}^{n} ik_i$ が成り立つとする ($k_i = 0$ も可). 全ての $i = 2, \dots, n$ に対し,

$$c_1^{(i)}, c_2^{(i)}, \dots, c_{k_i}^{(i)}$$

を k_i 個の長さ i の巡回置換とし, $c_j^{(i)}$ $(1 \leq i \leq n,\ 1 \leq j \leq k_i)$ のどの 2 つも互いに素であるとする. さらに, $i = 1$ のとき $c_j^{(1)} = \mathrm{id}$ $(1 \leq j \leq k_1)$ とする. また,

$$\sigma = \prod_{i,j} c_j^{(i)}$$

とおく. ただし, $c_j^{(i)}$ は互いに素であるので, 上の積は置換の順序によらず一意的に定まることに注意する. 以下, σ の中心化群 $\mathrm{Cent}_{\mathfrak{S}_n}(\sigma)$ について考える.

定理 7.20　このとき, $\mathrm{Cent}_{\mathfrak{S}_n}(\sigma)$ の位数は $\prod_{i=1}^{n} k_i!\, i^{k_i}$ である.

証明

$\tau \in \mathfrak{S}_n$ とする. 全ての i, j に対し, $\tau c_j^{(i)} \tau^{-1}$ は長さ i の巡回置換である. $2 \leq i \leq n$ に対し, $c_j^{(i)}$ によって動かされるもの全体の集合を $X_j^{(i)}$ とおく. また,

$$c_j^{(i)} = (x_{j,1}^{(i)} \ \dots \ x_{j,i}^{(i)})$$

とおく (つまり, $X_j^{(i)} = \{x_{j,1}^{(i)}, \dots, x_{j,i}^{(i)}\}$ である).

$$\tau\sigma\tau^{-1} = \prod_{i,j} \tau c_j^{(i)} \tau^{-1}$$

また,

$$\tau c_j^{(i)} \tau^{-1} = (\tau(x_{j,1}^{(i)}) \ \dots \ \tau(x_{j,i}^{(i)}))$$

である. 互いに素な巡回置換への分解の一意性より, $\tau\sigma\tau^{-1} = \tau$ が成り立つためには, 以下の条件がが必要十分である.

(1) 置換 $\gamma_i \in \mathfrak{S}_{k_i}$ $(i = 1, \dots, n)$ が存在し, $\tau(X_j^{(i)}) = X_{\gamma_i(j)}^{(i)}$ $(j = 1, \dots, k_i)$ である.

(2) $(\tau(x_{j,1}^{(i)}) \dots \tau(x_{j,i}^{(i)})) = (x_{\gamma_i(j),1}^{(i)} \dots x_{\gamma_i(j),i}^{(i)})$ である.

よって, 全射群準同型

$$\zeta\colon \mathrm{Cent}_{\mathfrak{S}_n}(\sigma) \to \prod_{i=1}^{n} \mathfrak{S}_{k_i}, \quad \tau \mapsto (\gamma_1, \dots, \gamma_n)$$

が定まる. 但し, $k_i = 0$ のとき, $\mathfrak{S}_{k_i} = \{1\}$ とする. ζ の核について考える. $\tau \in \mathrm{Ker}(\zeta)$ のとき, 全ての i, j に対し, $\tau(X_j^{(i)}) = X_j^{(i)}$ である. とくに, $\tau(x_{j,1}^{(i)}) \in X_j^{(i)}$ である. さらに, 上の条件 (2) より, τ は $\tau(x_{j,1}^{(i)})$ で一意に定まる. ゆえに, 写像

$$\mathrm{Ker}(\zeta) \to \prod_{i=1}^{n} \prod_{j=1}^{k_i} X_j^{(i)}, \quad \tau \mapsto (\tau(x_{j,1}^{(i)}))_{i,j}$$

は全単射である．したがって，$|X_j^{(i)}| = i$ より

$$|\operatorname{Ker}(\zeta)| = \prod_{i=1}^{n}\prod_{j=1}^{k_i} i = \prod_{i=1}^{n} i^{k_i}$$

である．以上より，

$$|\operatorname{Cent}_{\mathfrak{S}_n}(\sigma)| = |\operatorname{Im}(\zeta)||\operatorname{Ker}(\zeta)| = \prod_{i=1}^{n} k_i! i^{k_i}$$

が成り立つ．

定理 7.21　$n \neq 6$ のとき，$\mathfrak{S}_n$ の全ての自己同型が内部自己同型である．すなわち，$\operatorname{Aut}(\mathfrak{S}_n) = \operatorname{Int}(\mathfrak{S}_n)$ が成り立つ．

証明

$\varphi \in \operatorname{Aut}(\mathfrak{S}_n)$ とする．命題 7.19 より，任意の互換 τ に対し，$\varphi(\tau)$ が互換であることを示せば良い．$\varphi(\tau)$ は位数 2 の元であるので，m 個の互いに素な互換 $\tau_1, \ldots, \tau_m$ が存在し，

$$\varphi(\tau) = \tau_1 \ldots \tau_m$$

が成り立つ（ただし，$m \geq 1$ である）．また，$\operatorname{Cent}_{\mathfrak{S}_n}(\varphi(\tau)) = \varphi(\operatorname{Cent}_{\mathfrak{S}_n}(\tau))$ が成り立つので，$|\operatorname{Cent}_{\mathfrak{S}_n}(\tau)| = |\operatorname{Cent}_{\mathfrak{S}_n}(\varphi(\tau))|$ である．τ の場合は $k_1 = n-2$, $k_2 = 1$ で，$\varphi(\tau)$ の場合は $k_1 = n-2m$, $k_2 = m$ で定理 7.20 を使えば

$$|\operatorname{Cent}_{\mathfrak{S}_n}(\tau)| = 2(n-2)!$$
$$|\operatorname{Cent}_{\mathfrak{S}_n}(\varphi(\tau))| = (n-2m)!\, m!\, 2^m$$

となる．ゆえに，

$$2(n-2)! = (n-2m)!\, m!\, 2^m$$

が成り立つ．$m \geq 2$ と仮定する．このとき，

$$(n-2) \times (n-3) \times \cdots \times (n-2m+1) = (2m) \times (2m-2) \times \cdots \times 4$$

となる．左辺の積は $(2m-2)$ 個の項を持ち，右辺の積は $m-1$ 個の項を持つ．このことから，$2m > n-2$ がいえる．また $2m \leq n$ より，$2m = n-1$ または $2m = n$ が成り立つ．$2m = n-1$ ならば，

$$(n-2) \times (n-3) \times \cdots \times 2 = (n-1) \times (n-3) \times \cdots \times 4$$
$$\text{ゆえに} \quad (n-2) \times (n-4) \times \cdots \times 3 \times 2 = n-1$$

であり，$n-2 \mid n-1$ となり矛盾する．よって，$2m = n$ である．$m = 2$, $n = 4$ のときに成立しない．$m > 2$ のとき，

$$(n-2) \times (n-3) \times \cdots \times 1 = n(n-2) \times \cdots \times 4$$
$$\text{ゆえに} \quad (n-3) \times (n-5) \times \cdots \times 3 = n/2$$

となる．よって，$n/2 \geq n-3$, すなわち $n \leq 6$ となる．したがって，$n = 6$, $m = 3$ の場合のみ成り立つ．以上より，$n \neq 6$ の場合に $m = 1$ である．命題 7.19 により，φ は内部自己同型である．

最後に，$\mathfrak{S}_6$ の自己同型について調べる．まず，$\mathfrak{S}_n$ の指数 n の部分群について考える．$i \in \{1, \ldots, n\}$ に対し，

$$H_i := \{\sigma \in \mathfrak{S}_n \mid \sigma(i) = i\}$$

とおくと, H_i は $\{1,\dots,n\}\setminus\{i\}$ の対称群と同一視できる. とくに, $H_i \simeq \mathfrak{S}_{n-1}$ であり, $[\mathfrak{S}_n : H_i] = n$ である. $\sigma \in \mathfrak{S}_n$ に対し, $\sigma H_i \sigma^{-1} = H_{\sigma(i)}$ が成り立つことに注意する. よって, $\{H_1,\dots,H_n\}$ の n 個の部分群は互いに共役である.

補題 7.22　以下が同値である.

(i) $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Inn}(\mathfrak{S}_n)$ である.

(ii) $\mathfrak{S}_n$ の指数 n の部分群は $\{H_1,\dots,H_n\}$ に限る.

証明

$n = 3, 4$ のとき, (i) 及び (ii) の両方が成り立つことは, 定理 7.21 と §7.4, §7.5 から分かる. ゆえに, $n \geq 5$ と仮定して良い.

- 「(i) $\Longrightarrow$ (ii)」を示す. $H \subset \mathfrak{S}_n$ を指数 n の部分群とする. $\mathfrak{S}_n$ は自然に $\mathfrak{S}_n/H$ に作用している (§4.2 参照). H の安定化部分群は $\{\sigma \in \mathfrak{S}_n \mid \sigma H = H\} = H$ である. この作用に対応する群準同型

$$\rho\colon \mathfrak{S}_n \to \mathfrak{S}(\mathfrak{S}_n/H)$$

を考える. ρ が群同型であることを示す. $\mathrm{Ker}(\rho)$ が $\mathfrak{S}_n$ の正規部分群である. また, H の安定化部分群が H と一致するので, $\mathrm{Ker}(\rho) \subset H$ である. とくに, $[\mathfrak{S}_n : H] \geq n$ である. 命題 7.18 により $H = \{\mathrm{id}\}$ となり, ゆえに ρ が単射である. ρ の定義域と終域の濃度が等しいより, ρ は群同型である. $f(1) = H$ を満たす全単射 $f\colon \{1,\dots,n\} \to \mathfrak{S}_n/H$ をとる. $\gamma \in \mathfrak{S}_n$ ならば, $f\circ\gamma\circ f^{-1} \in \mathfrak{S}(\mathfrak{S}_n/H)$ である. ゆえに, 群同型

$$\psi\colon \mathfrak{S}_n \to \mathfrak{S}(\mathfrak{S}_n/H), \quad \gamma \mapsto f\circ\gamma\circ f^{-1}$$

が得られる. よって, $\psi^{-1}\circ\rho$ が $\mathfrak{S}_n$ の自己同型である. 仮定より, $\psi^{-1}\circ\rho$ が内部自己同型である. つまり, 適当な $\theta \in \mathfrak{S}_n$ が存在し,

$$(\psi^{-1}\circ\rho)(\sigma) = \theta\sigma\theta^{-1}, \quad \sigma \in \mathfrak{S}_n$$

となる. ゆえに, $\rho(\theta^{-1}\sigma\theta) = \psi(\sigma) = f\circ\sigma\circ f^{-1}$ である. とくに,

$$\theta^{-1}\sigma\theta H = f(\sigma(1)), \quad \sigma \in \mathfrak{S}_n$$

が成り立つ. ゆえに, 任意の $\sigma \in \mathfrak{S}_n$ に対し,

$$\begin{aligned} \sigma(1) = 1 &\iff f(\sigma(1)) = f(1) = H \\ &\iff \theta^{-1}\sigma\theta H = H \\ &\iff \sigma \in \theta H \theta^{-1} \end{aligned}$$

よって, $\theta H\theta^{-1} = \{\sigma \in \mathfrak{S}_n \mid \sigma(1) = 1\} = H_1$ である. ゆえに, $H = \theta^{-1}H_1\theta = H_{\theta^{-1}(1)}$ である.

- 「(ii) $\Longrightarrow$ (i)」を示す. $\rho\colon \mathfrak{S}_n \to \mathfrak{S}_n$ を自己同型とする. $\rho(H_i)$ が指数 n の部分群であるので, 仮定より, $\rho(H_i) = H_{\sigma(i)}$ となる置換 $\sigma \in \mathfrak{S}_n$ が存在する. σ で定まる $\mathfrak{S}_n$ の内部自己同型 $\tau \mapsto \sigma\tau\sigma^{-1}$ を φ_σ とおく. 明らかに, $\varphi_\sigma(H_i) = H_{\sigma(i)}$ が成り立つ. よって, $\gamma = \rho^{-1}\circ\varphi_\sigma$ とおくと, γ は $\gamma(H_i) = H_i$ $(i = 1,\dots,n)$ を満たす. $\gamma = \mathrm{id}_{\mathfrak{S}_n}$ を示せば良い. $\tau = (ab)$ が互換ならば, 明らかに

$$\tau \in \cap_{i\neq a,b} H_i$$

である. $\gamma(H_i) = H_i$ より, $\gamma(\tau) \in \cap_{i\neq a,b} H_i = \{\mathrm{id}, \tau\}$ となる. $\gamma(\tau) \neq \mathrm{id}$ より $\gamma(\tau) = \tau$ となる. よって, γ が恒等写像である. 以上より, $\rho = \varphi_\sigma$ となり, 内部自己同型である.

系 7.23　$n \neq 6$ のとき, $\mathfrak{S}_n$ の指数 n の部分群は $\{H_1, \ldots, H_n\}$ に限る.

証明

定理 7.21 と補題 7.22 より従う.

以下, $n = 6$ の場合を考える.

命題 7.24　$\mathfrak{S}_6$ の外部自己同型が存在する. また, $[\mathrm{Aut}(\mathfrak{S}_6) : \mathrm{Inn}(\mathfrak{S}_6)] = 2$ である.

証明

まず, $\mathrm{Aut}(\mathfrak{S}_6) \neq \mathrm{Inn}(\mathfrak{S}_6)$ を示す. 補題 7.22 により, 指数 6 の部分群で, $H_1, \ldots, H_6$ とは異なるものが存在することを示せば良い. 以下の集合を考える.

$$X = \{\mathfrak{S}_5 \text{ の } 5 \text{ シロー部分群 }\}$$

$\mathfrak{S}_5$ の 5 シロー部分群の個数を n_5 とおくと, $n_5 \equiv 1 \pmod 5$ かつ $n_5 \mid 24$ である. ゆえに, $n_5 \in \{1, 6\}$ である. 命題 7.18 により 5 シロー部分群は正規部分群でないので, $n_5 = 6$ である. $\mathfrak{S}_5$ が共役により X に作用している. この作用で定まる準同型

$$\rho\colon \mathfrak{S}_5 \to \mathfrak{S}(X)$$

を考える. シローの定理より, $\mathfrak{S}_5$ の X への作用は推移的である. $H \in X$ ならば, $N_{\mathfrak{S}_5}(H)$ が指数 6 の部分群である. また,

$$\mathrm{Ker}(\rho) = \bigcap_{H \in X} N_{\mathfrak{S}_5}(H)$$

であるので, とくに $\mathrm{Ker}(\rho)$ の指数が ≥ 6 となる. $\mathrm{Ker}(\rho) \triangleleft \mathfrak{S}_5$ だから, 命題 7.18 により $\mathrm{Ker}(\rho) = \{\mathrm{id}\}$ である. よって, ρ は単単射であり, $\rho(\mathfrak{S}_5)$ は $\mathfrak{S}(X)$ の指数 6 の部分群である. $\mathfrak{S}_5$ が X に推移的に作用しているので, $X^{\mathfrak{S}_4} = \emptyset$ である. $\mathfrak{S}(X)$ と $\mathfrak{S}_6$ を同一視する. 部分群 $\rho(\mathfrak{S}_5)$ に対応しているものを K とおくと, K が $\{1, 2, 3, 4, 5, 6\}$ に推移的に作用している. とくに, $K = H_i$ を満たす i が存在しない. したがって, $\mathrm{Aut}(\mathfrak{S}_6) \neq \mathrm{Inn}(\mathfrak{S}_6)$ である.
最後に, $[\mathrm{Aut}(\mathfrak{S}_6) : \mathrm{Inn}(\mathfrak{S}_6)] = 2$ を示す. $\varphi\colon \mathfrak{S}_6 \to \mathfrak{S}_6$ を外部自己同型とする. 定理 7.21 の証明より, 任意の互換 $\tau \in \mathfrak{S}_6$ に対し, $\varphi(\tau)$ は互いに素な 3 つの互換の積である. 写像

$$\{\mathfrak{S}_6 \text{の互換 }\} \to \{(ab)(cd)(ef) \mid a, b, c, d, e, f \text{ は相異なる }\}, \qquad \tau \mapsto \varphi(\tau)$$

を考える. この写像は明らかに単射である. 終域と定義域は両方 15 個の元をもつので, 写像は全単射である. あるいは, φ^{-1} を考えることで全単射性が分かる. したがって, $\varphi_1, \varphi_2\colon \mathfrak{S}_6 \to \mathfrak{S}_6$ が外部自己同型ならば, 任意の互換 τ に対し, $(\varphi_1 \circ \varphi_2)(\tau)$ は互換になる. 命題 7.19 より, $\varphi_1 \circ \varphi_2$ は内部自己同型である. よって, 剰余群 $\mathrm{Aut}(\mathfrak{S}_6)/\mathrm{Inn}(\mathfrak{S}_6)$ においては, 単位元でない任意の x, y に対し xy が単位元である. ゆえに, $[\mathrm{Aut}(\mathfrak{S}_6) : \mathrm{Inn}(\mathfrak{S}_6)] = 2$ が成り立つ.