最低限の群論

高瀬 幸一

ver.2023.3.1

目 次

1 群の定義と例 **3**

2 置換群 **4**

3 部分群 **7**

4 部分群を法とした剰余類 **9**

5 正規部分群 **11**

6 剰余類群 **13**

7 群の準同型写像と準同型定理 **14**

8 巡回群 **18**

9 群の自己同型群 **23**

10 群の直積 **25**

11 群の集合への作用 **27**

12 G-軌道と固定部分群 **29**

13 群の共役類と類公式 **32**

14 **Sylow** の定理 **34**

15 半直積 **38**

16 位数が二つの素数の積となる有限群の決定 **41**

17 4 次対称群の部分群 **44**

1　群の定義と例

定義 1.1 集合 G の任意の二つの元 $x, y \in G$ に対して，その**積** $x \cdot y \in G$ が定義されて，次の三条件を満たすとき，G は演算 $(x, y) \mapsto x \cdot y$ に関して**群**をなすという：

1) 任意の $x, y, z \in G$ に対して $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,

2) $e \in G$ が存在して，任意の $x \in G$ に対して $x \cdot e = e \cdot x = x$ となる,

3) 任意の $x \in G$ に対して，$x \cdot x' = x' \cdot x = e$ となる $x' \in G$ が存在する.

注意 1.2 群の定義にある条件 2) を満たす $e \in G$ は唯一存在する.
[**証明**] $e' \in G$ が同様の性質をもつとすると

$$e' = e' \cdot e = e$$

となるから. ■
そこで条件 2) を満たす $e \in G$ を群 G の**単位元** と呼び，1_G と表す. 記号を簡単にしたいときには単純に 1 と書く.

注意 1.3 群の定義にある条件 3) を満たす $x' \in G$ は $x \in G$ に対して唯一存在する.
[**証明**] $x'' \in G$ が同様の性質を持つとすると

$$x'' = x \cdot e = x'' \cdot (x \cdot x') = (x'' \cdot x) \cdot x' = e \cdot x' = x'$$

となるから. ■
そこで，$x' \in G$ を $x \in G$ の**逆元**と呼び，x^{-1} と書く.

定義 1.4 G が群であって，任意の $x, y \in G$ に対して $x \cdot y = y \cdot x$ が成り立つとき，G は**可換群**である，あるいは**アーベル群**であるという.

例 1.5 整数の全体

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \cdots\}$$

は整数の加法に関して可換群となる.

例 1.6 実数の全体を $\mathbb{R}$ とし，複素数の全体を $\mathbb{C}$ とする. 0 でない実数の全体，および 0 でない複素数の全体

$$\mathbb{R}^\times = \{0 \neq x \in \mathbb{R}\}, \qquad \mathbb{C}^\times = \{0 \neq z \in \mathbb{C}\}$$

は実数の乗法，あるいは複素数の乗法に関して可換群となる. 更に一般に体 F の 0 でない元の全体

$$F^\times = \{0 \neq x \in F\}$$

は F の乗法に関して群となる. これを体 F の乗法群と呼ぶ.

例 1.7 実数を成分とする n 次正方行列全体を $M_n(\mathbb{R})$ とする．n 次実正則行列の全体

$$GL_n(\mathbb{R}) = \{g \in M_n(\mathbb{R}) \mid \det g \neq 0\}$$

は行列の積に関して群となる．単位元は n 次単位行列

$$1_n = \begin{bmatrix} 1 & & \underline{0} \\ & \ddots & \\ \underline{0} & & 1 \end{bmatrix}$$

であり，$g \in GL_n(\mathbb{R})$ の逆元は正則行列 g の逆行列である．$n > 1$ ならば $GL_n(\mathbb{R})$ は非可換群である．$GL_n(\mathbb{R})$ を n **次実一般線形群** (real general linear group of degree n) と呼ぶ．

課題 1.1 例 1.5 を確かめよ．単位元は何か，$a \in \mathbb{Z}$ の逆元は何か．

課題 1.2 例 1.6 を確かめよ．単位元は何か，逆元は何か．

課題 1.3 例 1.7 を確かめよ．

課題 1.4

$$G = \{(x, y) \in \mathbb{R}^2 \mid (x, y) \neq (0, 0)\}$$

は演算

$$(x, y) \cdot (z, w) = (xz - yw, xw + yz)$$

に関して可換群となる．

課題 1.5 群 G において

1) 任意の $x \in G$ に対して $(x^{-1})^{-1} = x$ であることを示せ．

2) $(1_G)^{-1} = 1_G$ であることを示せ．

2 置換群

集合 X をとる．X から X への全単射の全体を $S(X)$ と書く．このとき

1) $\sigma, \tau \in S(X)$ に対して，その合成写像 $\sigma \circ \tau$ は再び X から X への全単射となる．即ち $\sigma \circ \tau \in S(X)$ である，

2) $\alpha, \beta, \gamma \in S(X)$ に対して $(\alpha \circ \beta) \circ \gamma = \alpha \circ (\beta \circ \gamma)$ である，

$$X \xrightarrow{\gamma} X \xrightarrow{\beta} X \xrightarrow{\alpha} X$$

3) X から X への恒等写像を $\mathrm{id}_X \in S(X)$ と書くと，任意の $\sigma \in S(X)$ に対して

$$\sigma \circ \mathrm{id}_X = \mathrm{id}_X \circ \alpha = \alpha$$

である，

4) $\sigma \in S(X)$ の逆写像 σ^{-1} は X から X への全単射だから $\sigma^{-1} \in S(X)$ で，

$$\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{id}_X$$

である．

以上により，$S(X)$ は写像の合成に関して群となることが判る．単位元は X の恒等写像 id_X であり，$\sigma \in S(X)$ の逆元は σ の逆写像である．こうしてできた群 $S(X)$ を集合 X 上の置換群と呼ぶ．

特に $X = \{1, 2, \cdots, n\}$ のとき，$S(X)$ を S_n と書いて，n **次対称群**と呼ぶ．$\sigma \in S_n$ に対して

$$\sigma(1) = i_1,\ \sigma(2) = i_2, \cdots, \sigma(n) = i_n \tag{2.1}$$

とおくと，$(i_1, i_2, \cdots, i_n)$ は $(1, 2, \cdots, n)$ を並べ替えたものである．逆に $(1, 2, \cdots, n)$ の並べ替え $(i_1, i_2, \cdots, i_n)$ に対して (2.1) により X から X への写像 σ を定めれば，$\sigma \in S_n$ である．そこで $\sigma \in S_n$ に対して，(2.1) であるとき

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \tag{2.2}$$

と書くことにする．従って

$$S_n = \left\{ \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \;\middle|\; \begin{array}{l} (i_1, i_2, \cdots, i_n) \text{ は} \\ (1, 2, \cdots, n) \text{ の並べ替え} \end{array} \right\}$$

と表すことが出来る．このとき

$$\mathrm{id}_X = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} \in S_n$$

であり，(2.2) に対して

$$\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ 1 & 2 & \cdots & N \end{pmatrix} \in S_n$$

である．$(1, 2, \cdots, n)$ の並べ替えは $n!$ 個あるから，$|S_n| = n!$ である．

注意 2.1 S_3 の二つの元

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

に対して

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

となる．即ち $\sigma\circ\tau\neq\tau\circ\sigma$ である．よって $n\geq 3$ ならば S_n は非可換群である．

n 次対称群の元の**符号**を定義しよう．n 個の変数 $X_1,X_2,\cdots,X_n$ の多項式

$$P(X_1,X_2,\cdots,X_n)=\prod_{1\leq i<j\leq n}(X_i-X_j)$$

を考える．例えば $n=2$ のときには

$$P(X_1,X_2)=X_1-X_2$$

であり，$n=3$ のときには

$$P(X_1,X_2,X_3)=(X_1-X_2)(X_1-X_3)(X_2-X_3)$$

である．$P(X_1,X_2,\cdots,X_n)$ の形から，$\sigma\in S_n$ に対して

$$P(X_{\sigma(1)},X_{\sigma(2)},\cdots,X_{\sigma(n)})=\mathrm{sign}(\sigma)\cdot P(X_1,X_2,\cdots,X_n)$$

なる $\mathrm{sign}(\sigma)=\pm1$ が定まる．これを $\sigma\in S_n$ の符号と呼ぶ．ここで次が成り立つ：

命題 2.2 $\sigma,\tau\in S_n$ に対して

$$\mathrm{sign}(\sigma\circ\tau)=\mathrm{sign}(\sigma)\cdot\mathrm{sign}(\tau)$$

である．

[**証明**] $\rho=\sigma\circ\tau$ とおくと，符号の定義から

$$P(X_{\rho(1)},X_{\rho(2)},\cdots,X_{\rho(n)})=\mathrm{sign}(\rho)\cdot P(X_1,X_2,\cdots,X_n)$$

である．一方

$$\begin{aligned}P(X_{\rho(1)},X_{\rho(2)},\cdots,X_{\rho(n)})&=P(X_{\sigma(\tau(1))},X_{\sigma(\tau(2))},\cdots,X_{\sigma(\tau(n))})\\&=\mathrm{sign}(\sigma)\cdot P(X_{\tau(1)},X_{\tau(2)},\cdots,X_{\tau(n)})\\&=\mathrm{sign}(\sigma)\cdot\mathrm{sign}(\tau)\cdot P(X_1,X_2,\cdots,X_n)\end{aligned}$$

となる．よって $\mathrm{sign}(\rho)=\mathrm{sign}(\sigma)\cdot\mathrm{sign}(\tau)$ となる．■

異なる二つの番号 i と j $(1\leq i<j\leq n)$ に対して，n 次対称群 S_n の元

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

を i,j の**互換**と呼ぶ．即ち，二つの番号 i,j を交換して，その他の番号は動かさないような S_n の元である．

課題 2.1 互換 $\sigma=(i,j)\in S_n$ $(1\leq i<j\leq n)$ に対して $\mathrm{sign}(\sigma)$ を求めよ．

3　部分群

定義 3.1 群 G の空でない部分集合 $H \subset G$ に対して，次の二条件が成り立つとき，H は G の**部分群**であるという：

1) 任意の $x, y \in H$ に対して $x \cdot y \in H$,

2) 任意の $x \in H$ に対して $x^{-1} \in H$.

注意 3.2 H が群 G の部分群ならば，$1_G \in H$ である．
[**証明**] $H \neq \emptyset$ だから $x \in H$ がとれる．条件 2) より $x^{-1} \in H$ である．よって条件 1) より $1_G = x \cdot x^{-1} \in H$ となる．■
よって群 G の部分群 H は G の演算に関して群となる．

例 3.3 群 G に対して G 自身および $\{1_G\}$ は G の部分群である．これらを G の**自明な部分群**と呼ぶ．

例 3.4 0 でない実数の全体 $\mathbb{R}^\times$ は実数の乗法に関して群である．

1) 正の実数全体
$$\mathbb{R}_{>0} = \{0 < x \in \mathbb{R}\}$$
は $\mathbb{R}^\times$ の部分群である．

2) $\{\pm 1\}$ は $\mathbb{R}^\times$ の部分群である．

例 3.5
$$SL_n(\mathbb{R}) = \{g \in M_n(\mathbb{R}) \mid \det g = 1\}$$
は $GL_n(\mathbb{R})$ の部分群である．$SL_n(\mathbb{R})$ を n **次実特殊線形群** (real special linear group of degree n) と呼ぶ．

例 3.6 $0 < d \in \mathbb{Z}$ に対して
$$d\mathbb{Z} = \{dx \mid x \in \mathbb{Z}\}$$
は $\mathbb{Z}$ の部分群である．

命題 3.7 群 G の空でない部分集合 $H \subset G$ に対して，次は同値である：

1) H は G の部分群である．

2) 任意の $x, y \in H$ に対して $x \cdot y^{-1} \in H$.

[**証明**] 1) $\Rightarrow$ 2) 部分群の条件 2) より $y^{-1} \in H$．よって部分群の条件 1) より $x \cdot y^{-1} \in H$ となる．
2) $\Rightarrow$ 1) H は空でないから $x \in H$ がとれる．よって $1_G = x \cdot x^{-1} \in H$ である．任意の $x \in H$ に対して $x^{-1} = 1_G \cdot x^{-1} \in H$ である．任意の $x, y \in H$ に対して，$y^{-1} \in H$ だから，$x \cdot y = x \cdot (y^{-1})^{-1} \in H$ となる．■

定理 3.8 部分群 $H \subset \mathbb{Z}$ は $H \neq \{0\}$ とする．このとき H に含まれる最小の正の整数を d とすると，$H = d\mathbb{Z}$ である．

[**証明**] まず H が正の整数を含むことを示す．$H \neq \{0\}$ だから $0 \neq x \in H$ がとれる．$x < 0$ ならば x の逆元 $-x \in H$ は正である．よって H は正の整数を含み，H に含まれる最小の正の整数 d が定まる．$H \subset \mathbb{Z}$ は部分群だから，$d \in H$ に対して

$$dn = \underbrace{d + \cdots + d}_{n\text{ 個}} \in H, \qquad d(-n) = \underbrace{(-d) + \cdots + (-d)}_{n\text{ 個}} \in H$$

$(n = 1, 2, 3, \cdots)$ かつ $d \cdot 0 = 0 \in H$ だから，$d\mathbb{Z} \subset H$ である．任意の $x \in H$ をとる．x を d で割って

$$x = qd + r \qquad 0 \leq r < d$$

なる整数 q, r がとれる（商と余り）．$r \neq 0$ と仮定すると

$$r = x - dq \in H \qquad 0 < r < d$$

となり，d の定義に反するから，$r = 0$ である．よって

$$x = qd \in d\mathbb{Z}$$

となる．よって $H \subset d\mathbb{Z}$. ∎

課題 3.1 例 3.4 にある二つの例が，実際に部分群であることを定義に基づいて確かめよ．

課題 3.2 群 G の元 $g \in G$ に対して

$$\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$$

は G の部分群となることを示せ．

課題 3.3 群 G の部分群 $H \subset G$ と $g \in G$ に対して

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

は再び G の部分群となることを示せ．

課題 3.4 2 次一般線形群 $GL_2(\mathbb{R})$ の部分集合

$$H = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in GL_2(\mathbb{R}) \right\}$$

は $GL_2(\mathbb{R})$ の部分群となることを示せ．

4　部分群を法とした剰余類

群 G の部分群 $H \subset G$ と $g \in G$ をとる．

$$gH = \{gh \mid h \in H\} \tag{4.3}$$

を H を法とした g の**右剰余類**と呼ぶ．次が成り立つ：

命題 4.1 群 G の部分群 $H \subset G$ に対して

1) 任意の $g \in G$ に対して $g \in gH$,

2) 任意の $g, g' \in G$ に対して，$gH \cap g'H \neq \emptyset$ ならば $gH = g'H$,

3) $g, g' \in G$ に対して

$$gH = g'H \iff g^{-1}g' \in H.$$

[**証明**] 1) $1_G \in H$ だから $g = g \cdot 1_G \in gH$ である．

2) $gH \cap g'H \neq \emptyset$ だから $gh = g'h'$ なる $h, h' \in H$ が存在する．このとき $g = g'h'h^{-1}$ だから

$$gH = \{g'h'h^{-1}h'' \mid h'' \in H\} \subset g'H$$

となる．同様にして $g'H \subset gH$ となるから，$gH = g'H$ である．

3) $gH = g'H$ とすると $g' \in g'H = gH$ だから $g' = gh$ なる $h \in H$ が存在する．よって $g^{-1}g' = h \in H$ となる．

逆に $g^{-1}g' = h \in H$ とすると，

$$g' = gh \in gH \cap g'H$$

となるから $gH \cap g'H \neq \emptyset$，よって $gH = g'H$ となる．■

同様に

$$Hg = \{hg \mid h \in H\}$$

を H を法とした g の**左剰余類**と呼ぶ．左剰余類と同様に次が成り立つ：

命題 4.2 群 G の部分群 $H \subset G$ に対して

1) 任意の $g \in G$ に対して $g \in Hg$,

2) 任意の $g, g' \in G$ に対して，$Hg \cap Hg' \neq \emptyset$ ならば $Hg = Hg'$,

3) $g, g' \in G$ に対して

$$Hg = Hg' \iff g'g^{-1} \in H.$$

よって群 G の部分群 $H \subset G$ に対して，部分集合 $S, T \subset G$ があって，G はそれぞれ $\{gH\}_{s\in S}$, $\{Hg\}_{g\in T}$ の重なりのない和集合となる：

$$G = \bigsqcup_{g\in S} gH = \bigsqcup_{g\in T} Hg. \tag{4.4}$$

S, T をそれぞれ**左剰余類の代表系**, **右剰余類の代表系**と呼ぶ．更に記号で

$$G/H = \{gH \mid g \in G\}, \qquad H\backslash G = \{Hg \mid g \in G\}$$

とおく．

命題 4.3 群 G の部分群 $H \subset G$ に対して，$gH \mapsto Hg^{-1}$ は全単射

$$G/H \to H\backslash G$$

を与える．特に $\sharp(G/H) = \sharp(H\backslash G)$ だから，これを H の G における**群指数** (group index) と呼び，$(G : H)$ と表す．

[**証明**] $gH = g' \in G/H$ ならば，$g^{-1}g' \in H$ だから $g'^{-1}g = (g^{-1}g')^{-1} \in H$ となる．よって $Hg'^{-1} = Hg^{-1}$ となる．よって写像

$$\varphi : G/H \to H\backslash G \qquad (gH \mapsto Hg^{-1})$$

が well-defined である．同様に写像

$$\psi : H\backslash G \to G/H \qquad (Hg \mapsto g^{-1}H)$$

が well-defined である．ここで

$$\psi \circ \varphi = \mathrm{id}_{G/H}, \qquad \varphi \circ \psi = \mathrm{id}_{H\backslash G}$$

となるから，φ は全単射となる．∎

群 G の部分群 $H \subset G$ をとる．任意の $g \in G$ に対して，全単射

$$H \to gH \qquad (h \mapsto gh)$$

が成り立つ．実際，

$$\varphi : H \ni x \mapsto gx \in gH, \quad \psi : gH \ni x \mapsto g^{-1}x \in H$$

とおくと，$\psi\circ\varphi = \mathrm{id}_H$, $\varphi\circ\psi = \mathrm{id}_{gH}$ となるからである．従って $\sharp(gH) = |H|$ である．よって (4.4) から

$$|G| = \sharp S \cdot |H|$$

となるが，群指数の定義から $\sharp S = \sharp(G/H) = (G : H)$ である．よって次の定理を得る：

定理 4.4 (Lagrange の定理) 群 G の部分群 $H \subset G$ に対して

$$|G| = (G : H) \cdot |H|$$

である．

課題 4.1 命題 4.2 を証明せよ．

課題 4.2 群 G の部分群 $K \subset L \subset G$ に対して

$$(G : K) = (G : L) \cdot (L : K)$$

であることを示せ．

課題 4.3 3 次対称群 S_3 の部分群 $H \subset S_3$ について，次の問いに答えよ：

1) H の位数 $|H|$ として可能な値をすべて求めよ．

2) 上で求めた可能な $|H|$ の値に対して，そのような部分群を一つ探せ．

課題 4.4 有限群 G の部分群 H, N に対して，$\mathrm{GCD}\{|H|, |N|\} = 1$ ならば $H \cap N = \{1_G\}$ であることを示せ．

5 正規部分群

一般に群 G の部分群 $H \subset G$ と $g \in G$ に対して

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

は G の部分群である（課題 3.3）が，一般には $gHg^{-1} \neq H$ である．例えば

例 5.1 3 次対称群 S_3 の部分群

$$H = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\rangle = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

と $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3$ に対して

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

だから

$$\sigma H \sigma^{-1} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$$

となる．よって $\sigma H \sigma^{-1} \neq H$ である．

そこで次のように定義する：

定義 5.2 群 G の部分群 $N \subset G$ であって，任意の $g \in G$ に対して $gNg^{-1} = N$ となるものを，G の**正規部分群**と呼び，記号で $N \triangleleft G$ と表す．

実際に正規部分群であることを示すときには，次の命題が便利である：

命題 5.3 群 G の部分群 $N \subset G$ に対して，次は同値である：

1) N は G の正規部分群である，

2) 任意の $g \in G$ に対して $gNg^{-1} \subset N$ である，

3) 任意の $g \in G$ に対して $gNg^{-1} \supset N$ である．

[**証明**] 1) $\Rightarrow$ 3) 正規部分群の定義から明らか．

3) $\Rightarrow$ 2) 任意の $g \in G$ に対して，$h = g^{-1} \in G$ とおくと $g^{-1}Ng = hNh^{-1} \supset N$ である．この両辺に，左から g 右から g^{-1} をかけると $N \supset gNg^{-1}$ となる．

2) $\Rightarrow$ 1) 任意の $g \in G$ をとる．仮定から $gNg^{-1} \subset N$ である．$h = g^{-1} \in G$ に対して仮定から $hNh^{-1} \subset N$ であるが，$hNh^{-1} = g^{-1}Ng$ だから $g^{-1}Ng \subset N$．この両辺に，左から g 右から g^{-1} をかけて $N \subset gNg^{-1}$ を得る．よって $gNg^{-1} = N$ となる．■

課題 5.1 $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3$ に対して

$$N = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\rangle$$

は S_3 の正規部分群となることを示せ．

課題 5.2 特殊線形群 $SL_n(\mathbb{R})$ は一般線形群 $GL_n(\mathbb{R})$ の正規部分群となることを示せ．

課題 5.3 群 G に対して

$$Z(G) = \{g \in G \mid \text{任意の } x \in G \text{ に対して } gx = xg\}$$

は G の正規部分群であることを示せ．$Z(G)$ を G の中心と呼ぶ．

6　剰余類群

群 G の正規部分群 $N \triangleleft G$ をとる．G の部分集合 $S, T \subset G$ に対して，G の部分集合 $S \cdot T$ を

$$S \cdot T = \{g \cdot t \mid s \in S, t \in T\}$$

により定義する．二つの剰余類 $xN, yN \in G/N$ に対して

$$(xN) \cdot (yN) = (xNy) \cdot N = xyN \cdot N = xyN$$

となる．ここで N は G の正規部分群だから $Ny = yN$ であり，また $N \cdot N = N$ であることに注意する．そこで N を法とした左剰余類の全体 G/N 上の演算を $(xN) \cdot (yN) = xyN$ により定義することができる．このとき次が成り立つ：

1) $\{(xN) \cdot (yN)\} \cdot (zN) = (xN) \cdot \{(yN) \cdot (xN)\}$,

2) $e = 1_G N = N \in G/N$ とおくと，任意の $xN \in G/N$ に対して

$$e \cdot (xN) = (xN) \cdot e = xN,$$

3) 任意の $xN \in G/N$ に対して $x^{-1}N \in G/N$ で

$$(xN) \cdot (x^{-1}N) = (x^{-1}N) \cdot (xN) = N.$$

即ち，G/N は演算 $(xN) \cdot (yN) = xyN$ により群となる．

$$\text{単位元} = N, \qquad xN \text{ の逆元} = x^{-1}N$$

である．

注意 6.1 群 G の正規部分群 $N \triangleleft G$ と $g \in G$ に対して，$\overline{g} = gN \in G/N$ と書くことにすると，記号が簡潔になる．即ち，左剰余類の全体 G/N は演算 $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$ により群となり

$$\text{単位元} = \overline{1_G}, \qquad \overline{x}^{-1} = \overline{x^{-1}}$$

である．このようにすると，演算を表すことは簡潔になるが，どのような正規部分群を法としているかは判らなくなるから，注意が必要である．

整数全体 $\mathbb{Z}$ は整数の加法に関して群である（例 1.5）．整数 $0 < d \in \mathbb{Z}$ をとると，$\mathbb{Z}$ は可換群だから

$$d\mathbb{Z} = \{dn \mid n \in \mathbb{Z}\}$$

は $\mathbb{Z}$ の正規部分群となる．整数 $x, y \in \mathbb{Z}$ に対して

$$\mathbb{Z}/d\mathbb{Z} \text{ で } \overline{x} = \overline{y} \Leftrightarrow x - y \in d\mathbb{Z} \text{ 即ち } x - y \text{ が } d \text{ の倍数}$$
$$\Leftrightarrow x \equiv y \pmod{d}$$

だから

$$\mathbb{Z}/d\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{d-1}\}$$

となる．即ち $(\mathbb{Z} : d\mathbb{Z}) = |\mathbb{Z}/d\mathbb{Z}| = d$ である．群 $\mathbb{Z}/d\mathbb{Z}$ の演算は $\overline{x}+\overline{y} = \overline{x+y}$ であり

$$\text{単位元} = \overline{0}, \qquad \overline{x} \text{ の逆元} = \overline{-x}$$

となる．

課題 6.1 特殊線形群 $SL_n(\mathbb{R})$ は一般線形群 $GL_n(\mathbb{R})$ の正規部分群である（課題 5.2）．

1) $x \in \mathbb{R}^\times$ に対して，n 次正方行列

$$[x] = \begin{bmatrix} x & & & \underline{0} \\ & 1 & & \\ & & \ddots & \\ \underline{0} & & & 1 \end{bmatrix}$$

は $GL_n(\mathbb{R})$ の元であることを示せ．

2) $x \mapsto \overline{[x]}$ は $\mathbb{R}^\times$ から剰余類群 $GL_n(\mathbb{R})/SL_n(\mathbb{R})$ への全単射であることを示せ．

3) $x, y \in \mathbb{R}^\times$ に対して $\overline{[x]} \cdot \overline{[y]} = \overline{[x \cdot y]}$ であることを示せ．

7　群の準同型写像と準同型定理

定義 7.1 群 G から群 H への写像 $f : G \to H$ を考える．任意の $x, y \in G$ に対して $f(x \cdot y) = f(x) \cdot f(y)$ となるとき，f を G から H への**群準同型写像**と呼ぶ．

例 7.2 $\alpha \in \mathbb{C}^\times$ をとると，写像

$$f_\alpha : \mathbb{Z} \to \mathbb{C}^\times \qquad (n \mapsto \alpha^n)$$

は加法群 $\mathbb{Z}$ から乗法群 $\mathbb{C}^\times$ への群準同型写像である．

例 7.3 $a \in \mathbb{R}$ に対して

$$f_a : \mathbb{R} \to \mathbb{C}^\times \quad (x \mapsto \cos(ax) + i\sin(ax))$$

は群準同型写像である．

命題 7.4 群 G から群 H への群準同型写像 $f : G \to H$ に対して

1) $f(1_G) = 1_H$,

2) 任意の $x \in G$ に対して $f(x^{-1}) = f(x)^{-1}$

である．

[証明] 1) $x \in G$ を一つとって

$$f(x) = f(x \cdot 1_G) = f(x) \cdot f(1_G)$$

だから，両辺に左から $f(x)^{-1}$ をかけて

$$\begin{aligned} 1_H = f(x)^{-1} \cdot f(x) &= f(x)^{-1} \cdot (f(x) \cdot f(1_G)) \\ &= (f(x)^{-1} \cdot f(x)) \cdot f(1_G) = 1_H \cdot f(1_G) = f(1_G). \end{aligned}$$

2) 任意の $x \in G$ に対して

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

両辺に左から $f(x)^{-1}$ をかけて

$$\begin{aligned} f(x)^{-1} = f(x)^{-1} \cdot 1_H &= f(x)^{-1} \cdot (f(x) \cdot f(x^{-1})) \\ &= (f(x)^{-1} \cdot f(x)) \cdot f(x^{-1}) = 1_H \cdot f(x^{-1}) = f(x^{-1}). \end{aligned}$$

■

命題 7.5 群 G から群 H への群準同型写像 $f : G \to H$ に対して

1) $\mathrm{Im}(f) = \{f(x) \mid x \in G\}$ は H の部分群である．これを群準同型写像 f の**像** (image) と呼ぶ．

2) $\mathrm{Ker}(f) = \{x \in G \mid f(x) = 1_H\}$ は G の正規部分群である．これを f の**核** (kernel) と呼ぶ．

[証明] 1) $\mathrm{Im}(f)$ が H の空でない部分集合であることは明らかである．任意の $z, w \in \mathrm{Im}(f)$ に対して，$z = f(x), w = f(y)$ なる $x, y \in G$ が存在する．このとき

$$z \cdot w^{-1} = f(x) \cdot f(y)^{-1} = f(x) \cdot f(y^{-1}) = f(x \cdot y^{-1}) \in \mathrm{IM}(f)$$

となるから，命題 3.7 より，$\mathrm{Im}(f)$ は H の部分群となる．

2) $f(1_G) = 1_H$ だから $1_G \in \mathrm{Ker}(f)$ となるから，$\mathrm{Ker}(f)$ は G の空でない部分集合である．任意の $x, y \in \mathrm{Ker}(f)$ に対して $f(x) = f(y) = 1_H$ だから

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

よって $xy^{-1} \in \mathrm{Ker}(f)$ となる．よって命題 3.7 より $\mathrm{Ker}(f)$ は H の部分群となる．任意の $g \in G$ をとる．任意の $x \in \mathrm{Ker}(f)$ に対して

$$f(gxg^{-1}) = f(g) \cdot f(x) \cdot f(g^{-1}) = f(g) \cdot 1_H f(g)^{-1} = f(g) \cdot f(g)^{-1} = 1_H$$

だから $gxg^{-1} \in \mathrm{Ker}(f)$ となる．よって $g \cdot \mathrm{Ker}(f) \cdot g^{-1} \subset \mathrm{Ker}(f)$ となる．よって命題 5.3 より $\mathrm{Ker}(f)$ は G の正規部分群である．∎

命題 7.6 群 G から群 H への群準同型写像 $f : G \to H$ に対して

1) f が全射である必要十分条件は $\mathrm{Im}(f) = H$ なることである．

2) f が単射である必要十分条件は $\mathrm{Ker}(f) = \{1_G\}$ なることである．

[**証明**] 1) $\mathrm{Im}(f)$ の定義から明らか．

2) f は単射とする．$\mathrm{Ker}(f)$ は G の部分群だから $1_G \in \mathrm{Ker}(f)$ である．逆に $x \in \mathrm{Ker}(f)$ ならば

$$f(x) = 1_H = f(1_G) \qquad \therefore x = 1_G$$

だから $\mathrm{Ker}(f) = \{1_G\}$ である．

$\mathrm{Ker}(f) = \{1_G\}$ とする．$x, y \in G$ に対して $f(x) = f(y)$ ならば

$$f(xy^{-1}) = f(x) \cdot f(y)^{-1} = 1_H \qquad \therefore xy^{-1} \in \mathrm{Ker}(f) = \{1_G\}$$

だから $xy^{-1} = 1_G$．よって $x = y$ となる．よって f は単射である．∎

例 7.7 命題 2.2 から，n 次対称群の元の符号

$$\mathrm{sign} : S_n \to \{\pm 1\}$$

は群準同型写像である．その核

$$\mathrm{Ker}(\mathrm{sign}) = \{\sigma \in S_n \mid \mathrm{sign}(\sigma) = 1\}$$

は S_n の正規部分群となる．これを n 次交代群と呼び A_n と表す：

$$A_n = \{\sigma \in S_n \mid \mathrm{sign}(\sigma) = 1\}.$$

例 7.8 行列式の性質から，n 次正方行列 A, B に対して $\det(AB) = \det A \cdot \det B$ である．よって

$$\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$$

は群準同型写像である．その核は

$$\mathrm{Ker}(\det) = \{g \in GL_n(\mathbb{R}) \mid \det g = 1\} = SL_n(\mathbb{R})$$

である．よって n 次特殊線形群 $SL_n(\mathbb{R})$ は n 次一般線形群 $GL_n(\mathbb{R})$ の正規部分群となる．

定義 7.9 群 G から群 H への群準同型写像 $f : G \to H$ が全単射のとき，f を群 G から群 H への**群同型写像**と呼び，記号で

$$f : G \xrightarrow{\sim} H$$

と書く．

例 7.10 課題 6.1 は $\mathbb{R}^\times$ から $GL_n(\mathbb{R})/SL_n(\mathbb{R})$ への写像 $x \mapsto \overline{[x]}$ が群同型写像となることを示している．

定理 7.11 (群の準同型定理) 群 G から群 H の準同型写像 $F : G \to H$ に対して，群同型写像

$$\overline{f} : G/\mathrm{Ker}(f) \xrightarrow{\sim} \mathrm{Im}(f) \quad (\overline{x} \mapsto f(x))$$

が成り立つ．

[**証明**] まず $x, x' \in G$ に対して，剰余類群 $G/\mathrm{Ker}(f)$ で $\overline{x} = \overline{x'}$ ならば $x^{-1}x' \in \mathrm{Ker}(f)$ となるから

$$1 = f(x^{-1}x') = f(x)^{-1}f(x') \quad \therefore f(x) = f(x').$$

よって $G/\mathrm{Ker}(f)$ から $\mathrm{Im}(f)$ への写像 $\overline{x} \mapsto f(x)$ が well-defined である．これを

$$\overline{f} : G/\mathrm{Ker}(f) \xrightarrow{\sim} \mathrm{Im}(f)$$

と書く．$\overline{f}$ が全射であることは明らかである．一方，$x, x' \in G$ に対して，$f(x) = f(x')$ ならば

$$f(x^{-1}x') = f(x)^{-1}f(x') = 1_H, \quad \therefore x^{-1}x' \in \mathrm{Ker}(f)$$

となるから $G/\mathrm{Ker}(f)$ で $\overline{x} = \overline{x'}$ となる．よって $\overline{f}$ は単射である．更に $x, x' \in G$ に対して

$$\begin{aligned}\overline{f}\left(\overline{x} \cdot \overline{x'}\right) &= \overline{f}\left(\overline{x \cdot x'}\right) \\ &= f(x \cdot x') = f(x) \cdot f(x') = \overline{f}\left(\overline{x}\right) \cdot \overline{f}\left(\overline{x'}\right)\end{aligned}$$

となるから，$\overline{f}$ は $G/\mathrm{Ker}(f)$ から $\mathrm{Im}(f)$ への群準同型写像である．■

例 7.12 群準同型写像

$$\det : GL_n(\mathbb{R}) \to \mathbb{R}^\times$$

に対して $\mathrm{Ker}(\det) = SL_n(\mathbb{R})$ である（例 7.8）．

$$\det \begin{bmatrix} x & & & \underline{0} \\ & 1 & & \\ & & \ddots & \\ \underline{0} & & & 1 \end{bmatrix} = x$$

だから $\mathrm{Im}(\det) = \mathbb{R}^\times$ である．よって群の準同型定理から．群の同型写像

$$\overline{\det} : GL_n(\mathbb{R})/SL_n(\mathbb{R}) \xrightarrow{\sim} \mathbb{R}^\times \quad (\overline{g} \mapsto \det g)$$

が得られる．

課題 7.1 例 7.3 を確かめよ．

課題 7.2 整数 $1 < d \in \mathbb{Z}$ に対して

$$\alpha = \cos\frac{2\pi}{d} + i\sin\frac{2\pi}{d} \in \mathbb{C}^\times$$

とおく．例 7.2 の群準同型写像

$$f_\alpha : \mathbb{Z} \to \mathbb{C}^\times \quad (n \mapsto \alpha^n)$$

に対して $\mathrm{Im}(f_\alpha)$ と $\mathrm{Ker}(f_\alpha)$ を求めよ．

課題 7.3 6 ページで定義した S_n の元の符号を考える．

1) $A_n = \{\sigma \in S_n \mid \mathrm{sign}(\sigma) = 1\}$ は n 次対称群の正規部分群であることを示せ．A_n を n **次交代群**と呼ぶ．

2) 群の準同型定理を用いて，群の同型

$$S_n/A_n \xrightarrow{\sim} \{\pm 1\}$$

が成り立つことを示せ．

8 巡回群

定義 8.1 群 G に対して $G = \langle g \rangle$ なる $g \in G$ が存在するとき，G を**巡回群**と呼ぶ．

注意 8.2 G が巡回群ならば G はアーベル群である．実際，$G = \langle g \rangle$ なる $g \in G$ がとれるから，任意の $x, y \in G$ に対して $x = g^m, y = g^n$ $(m, n \in \mathbb{Z}$ とおける．よって指数法則により

$$x \cdot y = g^m \cdot g^n = g^{m+n}, \quad y \cdot x = g^n \cdot g^m = g^{n+m}$$

となり，$x \cdot y = y \cdot x$ となる．

例 8.3 整数 $n > 1$ に対して，1 の n 乗根全体

$$\mu_n = \{z \in \mathbb{C} \mid z^n = 1\}$$

は乗法群 $\mathbb{C}^\times$ (例 1.6) の部分群である．

$$\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \in \mathbb{C}$$

とおくと

$$\mu_n = \left\{\omega^k \mid k = 0, 1, 2, \cdots, n-1\right\} = \langle\omega\rangle$$

だから，μ_n は巡回群である．

例 8.4　1) 整数全体 $\mathbb{Z}$ は $\mathbb{Z} = \langle 1\rangle$ となるから，巡回群である．

2) $0 < d \in \mathbb{Z}$ に対して，剰余類群 $\mathbb{Z}/d\mathbb{Z}$ は

$$\mathbb{Z}/d\mathbb{Z} = \left\{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{d-1}\right\} = \langle\overline{1}\rangle$$

だから，巡回群である．

一般に群 G の元 $g \in G$ をとると，群の準同型写像

$$f : \mathbb{Z} \to G \qquad (n \mapsto g^n)$$

ができる．ここで

$$\mathrm{Im}(f) = \{g^n \mid n \in \mathbb{Z}\} = \langle g\rangle$$

であり，

$$\mathrm{Ker}(f) = \{n \in \mathbb{Z} \mid g^n = 1\}$$

である．ここで二つの場合を分けて考える：

$\underline{\mathrm{Ker}(f) = \{0\} \text{ のとき}}$．$f$ は群の同型

$$\mathbb{Z} \xrightarrow{\sim} \langle g\rangle$$

を与える．このとき $|\langle g\rangle = \infty$ である．

$\underline{\mathrm{Ker}(f) \neq \{0\} \text{ のとき}}$.定理 3.8 より，$\mathrm{Ker}(f)$ に含まれる最小の正の整数を d とすると，$\mathrm{Ker}(f) = d\mathbb{Z}$ だから，群の準同型定理 7.11 から群の同型

$$\overline{f} : \mathbb{Z}/d\mathbb{Z} \xrightarrow{\sim} \langle g\rangle \qquad (\overline{n} \mapsto g^n)$$

が成り立つ．このとき

$$|\langle g\rangle| = |\mathbb{Z}/d\mathbb{Z}| = d$$

である．以上の事から次のように定義する：

定義 8.5 群 G の元 $g \in G$ に対して

$$\mathrm{ord}(g) = \mathrm{Min}\{0 < n \in \mathbb{Z} \mid g^n = 1\}$$

とおいて，これを g の**位数**と呼ぶ．

注意 8.6 上の定義で，任意の $0 < n \in \mathbb{Z}$ に対して $g^n \neq 1$ であるときには，$\mathrm{ord}(g) = \infty$ とする．

上に述べたことをまとめると，次の定理が得られる：

定理 8.7 群 G の元 $g \in G$ に対して

1) $|\langle g \rangle| = \mathrm{ord}(g)$,

2) $\mathrm{ord}(g) = \infty$ ならば $\mathbb{Z} \xrightarrow{\sim} \langle g \rangle$ $(n \mapsto g^n)$,

3) $\mathrm{ord}(g) = d < \infty$ ならば $\mathbb{Z}/d\mathbb{Z} \xrightarrow{\sim} \langle g \rangle$ $(\overline{n} \mapsto g^n)$

である．

群の元の位数についてもう少し性質をまとめると

定理 8.8 群 G の元 $g \in G$ について $\mathrm{ord}(g) < \infty$ とすると，任意の $n \in \mathbb{Z}$ に対して

$$g^n = 1_G \ \Leftrightarrow \ \mathrm{ord}(g) | n$$

である．特に $|G| < \infty$ のとき，$\mathrm{ord}(g) \,\big|\, |G|$ 従って $g^{|G|} = 1_G$ である．

[**証明**] $\mathrm{ord}(g) = d$ は $g^d = 1_G$ となる最小の正の整数である．$n \in \mathbb{Z}$ に対して，$d|n$ ならば $n = dm$ $(m \in \mathbb{Z})$ だから

$$g^n = g^{dm} = (g^d)^m = 1_G^m = 1_G$$

となる．逆に $g^n = 1_G$ とする．n を d で割って

$$n = qd = r, \qquad 0 \leq r < d \qquad (q, r \in \mathbb{Z})$$

とする．$r \neq 0$ と仮定すると，$r = n - dq$ だから

$$g^r = g^{n-dq} = g^n \cdot (g^d)^q = 1_G \ \text{ かつ } 0 < r < d$$

となり，$d = \mathrm{ord}(g)$ の仮定に反する．よって $r = 0$，即ち $d|n$ となる．
特に $|G| < \infty$ のとき

$$|G| = (G : \langle g \rangle)|\langle g \rangle|, \qquad |\langle g \rangle| = \mathrm{ord}(g)$$

だから，$\mathrm{ord}(g) \,\big|\, |G|$，よって $g^{|G|} = 1_G$ となる．■

上の定理 8.7 を巡回群について言い換えれば，次の系を得る：

系 8.9 巡回群 G について

1) $|G| = \infty$ ならば $\mathbb{Z} \xrightarrow{\sim} G$,

2) $|G| = d < \infty$ ならば $\mathbb{Z}/d\mathbb{Z} \xrightarrow{\sim} G$

である．

巡回群の部分群に関しては，次の定理が基本的である：

定理 8.10 巡回群 $G = \langle g \rangle$ の部分群 $H \subset G$ をとり，H は単位元以外の元も含むと仮定する．このとき $(G : H) = d$ は有限である．更に

$$d = \mathrm{Min}\{0 < n \in \mathbb{Z} \mid g^n \in H\}, \qquad H = \langle g^d \rangle$$

であり， $G/H = \langle \overline{g} \rangle$ は巡回群である．

[**証明**] 巡回群 G はアーベル群だから（注意 8.2），部分群 H は G の正規部分群となる．そこで剰余類群 G/H を考えると

$$\begin{aligned} G/H =& \{\overline{x} = xH \mid x \in G\} \\ =& \{\overline{g^n} = \overline{g}^n \mid n \in \mathbb{Z}\} \\ =& \langle \overline{g} \rangle \end{aligned}$$

となり，G/H は巡回群である．ここで群の準同型写像

$$f : \mathbb{Z} \to G/H \quad (n \mapsto \overline{g}^n = \overline{g^n})$$

に群の準同型定理を適用する．まず

$$\mathrm{Im}(f) = \{\overline{g}^n \mid n \in \mathbb{Z}\} = \langle \overline{g} \rangle = G/H$$

は明らか．一方

$$\begin{aligned} \mathrm{Ker}(f) =& \{n \in \mathbb{Z} \mid g^n H = H\} \\ =& \{n \in \mathbb{Z} \mid g^n \in H\} \end{aligned}$$

であるが，H が単位元以外の元も含むから，$\mathrm{Ker}(f)$ は 0 以外の元も含む．よって定理 3.8 より

$$\begin{aligned} d =& \mathrm{Min}\{0 < n \in \mathrm{Ker}(f)\} \\ =& \mathrm{Min}\{0 < n \in \mathbb{Z} \mid g^n \in H\} \end{aligned}$$

とおくと $\mathrm{Ker}(f) = d\mathbb{Z}$ となる．よって群の準同型定理より群の同型写像

$$\overline{f} : \mathbb{Z}/d\mathbb{Z} \xrightarrow{\sim} G/H \quad (\overline{n} \mapsto \overline{g}^n)$$

が得られる．これは全単射だから

$$|G/H| = |\mathbb{Z}/d\mathbb{Z}| = d \qquad \therefore (G : H) = d$$

となる．更に $g^d \in H$ だから

$$\langle g^d \rangle = \{(g^d)^m \mid m \in \mathbb{Z}\} \subset H$$

であるが，任意の $g^n \in G$ に対して

$$\begin{aligned} g^n \in H &\Rightarrow n \in \mathrm{Ker}(f) = d\mathbb{Z} \\ &\Rightarrow n = dm \quad (m \in \mathbb{Z}) \Rightarrow g^n = (g^d)^m \in \langle g^d \rangle \end{aligned}$$

となるから，$H = \langle g^d \rangle$ である．■

命題 8.11 巡回群 G の部分群 $K, L \subset G$ に対して

$$K \subset L \Leftrightarrow (G:L) \,\Big|\, (G:K)$$

である．

[**証明**] $\Rightarrow$) $K \subset L$ ならば

$$(G:K) = (G:L) \cdot (L:K)$$

だから $(G:L) \,\Big|\, (G:K)$ である．

$\Leftarrow$) $(G:K) = k, (G:L) = l$ として $k = lm$ $(m \in \mathbb{Z})$ とする．$G = \langle g \rangle$ とおくと

$$K = \langle g^k \rangle = \langle g^{lm} \rangle \subset \langle g^l \rangle = L$$

となる．■

定理 8.12 有限群 G に対して $|G| = p$ が素数ならば G は巡回群である．

[**証明**] $|G| = p \geq 2$ だから $1 \neq g \in G$ が存在する．部分群 $\langle g \rangle \subset G$ に対して，$|\langle g \rangle|$ は $|G| = p$ の約数となるが，p は素数だから $|\langle g \rangle| = 1$ または $|\langle g \rangle| = p$ である．一方

$$\{1, g\} \subset \langle g \rangle, \qquad 1 \neq g$$

だから $|\langle g \rangle| \geq 2$．よって $|\langle g \rangle| = p = |G|$ となり，$\langle g \rangle = G$ となるから G は巡回群である．■

定理 8.13 群 G に対して，剰余類群 $G/Z(G)$ が巡回群ならば G はアーベル群である．

[証明] $G/Z(G) = \langle \overline{g} \rangle$ なる $g \in G$ が存在する．任意の $x, y \in G$ をとる．$G/Z(G)$ で

$$\overline{x} = \overline{g}^m, \qquad \overline{y} = \overline{g}^n \qquad (m, n \in \mathbb{Z})$$

と書ける．即ち $xg^{-m} = h \in Z(G), yg^{-n} = k \in Z(G)$ だから $x = hg^m, y = kg^n$ である．$h, k \in Z(G)$ だから

$$xy = hg^m kg^n = hkg^m g^n = hkg^{m+n}, \qquad yx = kg^n hg^m = khg^n g^m = hkg^{n+m}$$

かつ $hk = kh$ となるから，$xy = yx$ となる．よって G はアーベル群である．
∎

課題 8.1 3 次対称群 S_3 の部分群を全て求めよ．

課題 8.2 G を有限巡回群として $|G| = n$ とする．n の約数 m に対して

$$H = \{x \in G \mid x^m = 1\}$$

は G の部分群（従って巡回群）で $|H| = m$ であることを示せ．

課題 8.3 群 G の元 $g \in G$ に対して $\mathrm{ord}(g) = d$ は有限であるとする．このとき整数 $e \in \mathbb{Z}$ に対して

$$\mathrm{ord}(g^e) = \frac{d}{\mathrm{GCD}\{e, d\}}$$

であることを示せ．

9 群の自己同型群

定義 9.1 群 G に対して，G から G への群の同型写像の全体を $\mathrm{Aut}(G)$ と書く．即ち $\mathrm{Aut}(G)$ は次の二条件を満たす写像 $\sigma : G \to G$ の全体である：

1) $\sigma : G \to G$ は群の準同型写像（即ち任意の $x, y \in G$ に対して $\sigma(x \cdot y) = \sigma(x) \cdot \sigma(y)$）,

2) $\sigma : G \to G$ は全単射．

$\mathrm{Aut}(G)$ は写像の合成に関して群となる．

$$\text{単位元} = \mathrm{id}_G, \qquad \sigma \text{ の逆元} = \sigma^{-1} : \sigma \text{ の逆写像}$$

である．

群 G に対して，G から G への全単射の全体 $S(G)$ は写像の合成に関して群となった（2 節参照）．$\mathrm{Aut}(G)$ は $S(G)$ の部分群である．

さて $g \in G$ に対して，G の自己同型写像

$$\sigma_g : G \xrightarrow{\sim} G \qquad (x \mapsto gxg^{-1})$$

が定義される．このとき

$$f : G \to \mathrm{Aut}(G) \quad (g \mapsto \sigma_g)$$

は群の準同型写像である．これに群の準同型定理を適用しよう．まず

$$\begin{aligned}
\mathrm{Ker}(f) =& \{g \in G \mid \sigma_g = \mathrm{id}_G\} \\
=& \{g \in G \mid \text{任意の } x \in G \text{ に対して } \sigma_g(x) = x\} \\
=& \{g \in G \mid \text{任意の } x \in G \text{ に対して } gxg^{-1} = x\} \\
=& \{g \in G \mid \text{任意の } x \in G \text{ に対して } gx = xg\} \\
=& Z(G)
\end{aligned}$$

は G の中心である（課題 5.3 参照）．一方

$$\mathrm{Im}(f) = \{\sigma_g \in \mathrm{Aut}(G) \mid g \in G\}$$

は $\mathrm{Aut}(G)$ の部分群である．これを G の内部自己同型群と呼び $\mathrm{Inn}(G)$ と書く．即ち

$$\mathrm{Inn}(G) = \{\sigma_g \in \mathrm{Aut}(G) \mid g \in G\}$$

である．よって群の準同型定理により，群の同型写像

$$\overline{f} : G/Z(G) \xrightarrow{\sim} \mathrm{Inn}(G) \qquad (\overline{g} \mapsto \sigma_g)$$

が得られる．

課題 9.1 群 G に対して次を示せ：

1) $g \in G$ と $\tau \in \mathrm{Aut}(G)$ に対して $\tau \circ \sigma_g \circ \tau^{-1} = \sigma_{\tau(g)}$ である．

2) G の内部自己同型群 $\mathrm{Inn}(G)$ は $\mathrm{Aut}(G)$ の正規部分群である．

課題 9.2 G を有限アーベル群とする．$a \in \mathbb{Z}$ に対して写像

$$f_a : G \ni x \mapsto x^a \in G$$

を考える．

1) $f_a : G \to G$ は群の準同型写像となることを示せ．

2) $a, b \in \mathbb{Z}$ に対して $f_a \circ f_b = f_{ab}$ となることを示せ．

3) G が巡回のとき，$f_a \in \mathrm{Aut}(G)$ となる必要十分条件は $\mathrm{GCD}\{a, |G|\} = 1$ なることを示せ.

課題 9.3 群 G の正規部分群 $N \subset G$ について，次の問いに答えよ：

1) $g \in G$ に対して N の自己同型写像 $\theta_g \in \mathrm{Aut}(N)$ が $\theta_g(x) = gxg^{-1}$ $(x \in N)$ により定義されることを示せ.

2) $g \mapsto \theta_g$ は群の準同型写像

$$\theta : G \to \mathrm{Aut}(N)$$

を定義することを示せ.

10 群の直積

定義 10.1 r 個の群 G_i $(i = 1, 2, \cdots, r)$ の直積集合

$$G = G_1 \times G_2 \times \cdots \times G_r = \{(x_1, x_2, \cdots, x_r) \mid x_i \in G_i\}$$

は演算

$$(x_1, x_2, \cdots, x_r) \cdot (y_1, y_2, \cdots, y_r) = (x_1 y_1, x_2 y_2, \cdots, x_r y_r)$$

により群となる.

$$1_G = (1_{G_1}, 1_{G_2}, \cdots, 1_{G_r}), \qquad (x_1, x_2, \cdots, x_r)^{-1} = (x_1^{-1}, x_2^{-1}, \cdots, x_r^{-1})$$

である．こうして出来た群 $G = G_1 \times G_2 \times \cdots \times G_r$ を G_i $(i = 1, 2, \cdots, r)$ の直積群と呼ぶ.

定理 10.2 群 G の二つの正規部分群 $K, L \subset G$ について

1) $K \cap L = \{1_G\}$ ならば，写像

$$f : K \times L \to G \qquad ((k, l) \mapsto kl)$$

は単射群準同型写像である.

2) $K \cap L = \{1_G\}$ かつ $G = \{k \cdot l \mid k \in K, l \in L\}$ ならば

$$f : K \times L \xrightarrow{\sim} G \quad ((k, l) \mapsto kl)$$

は群の同型写像である.

[**証明**] 1) まず $k \in K, l \in L$ に対して

$$(kl)(lk)^{-1} = klk^{-1}l^{-1} \in K \cap L = \{1_G\}$$

だから $kl = lk$ である．よって $(k,l), (k',l') \in K \times L$ に対して

$$\begin{aligned} f((k,l)\cdot(k',l')) =& f(kk', ll') = kk'll' \\ =& klk'l' = f(k,l)\cdot f(k',l') \end{aligned}$$

となるから，$f : K \times L \to G$ は群の準同型写像である．更に

$$\begin{aligned} (k,l) \in \mathrm{Ker}(f) \ &\Rightarrow\ f(k,l) = kl = 1_G \\ &\Rightarrow\ k = l^{-1} \in K \cap L = \{1_G\} \ \Rightarrow\ (k,l) = (1_G, 1_G) \end{aligned}$$

だから $\mathrm{Ker}(f) = \{1_{K\times L}\}$ となる．命題 7.6 の 2) から，これは f が単射であることを意味する．

2) 上で示したことから，f は単射群準同型写像であるが，仮定からよって f は全射である．よって f は群の同型写像である．■

証明は省略するが，有限アーベル群について次の定理を証明することが出来る：

定理 10.3 (有限アーベル群の構造定理) 有限アーベル群 G に対して，群の同型

$$G \xrightarrow{\sim} \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r$$

が成り立つような $1 < d_i \in \mathbb{Z}$ $(i = 1, 2, \cdots, r)$ で

$$d_1 | d_2,\ d_2 | d_3, \cdots, d_{r-1} | d_r$$

なるものが唯一存在する．

有限アーベル群の構造定理の応用として，次の定理を証明しておこう：

定理 10.4 体 F の乗法群 $F^\times$ (例 1.6 を参照) の有限部分群は巡回群である．

[**証明**] $G \subset F^\times$ を有限部分群とする．G はアーベル群だから，有限アーベル群の構造定理から

$$G \simeq \mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \times \mathbb{Z}/a_r\mathbb{Z}$$

なる $1 < a_i \in \mathbb{Z}$ で $a_i | a_{i+1}$ なるものが定まる．ここで左辺 G の演算は乗法であるが，右辺は加法が演算となっている事を注意しよう．従って右辺の a_r 倍は左辺で考えれば a_r 乗となる．ここで $a_i | a_r$ $(i = 1, 2, \cdots, r)$ だから，右

辺は a_r 倍すると全ての元が単位元 0 となる．よって左辺では a_r 乗すると全ての元が単位元 1 となる．即ち

$$G \subset \{x \in F \mid x^{a_r} = 1\}$$

である．ところで体 F の中には a_r 次方程式 $X^{a_r} = 1$ の根は高々a_r しかないから $|G| \leq a_r$ である．一方

$$|G| = \left|\mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z} \times \cdots \times \mathbb{Z}/a_r\mathbb{Z}\right| = a_1 a_2 \cdots a_r$$

である．$a_i > 1$ $(i = 1, 2, \cdots, r)$ だから，これは $r = 1$ のときのみ可能である．よって $G \simeq \mathbb{Z}/a_1\mathbb{Z}$ となり， G は巡回群である．∎

課題 10.1 $|G| = 26$ なるアーベル群 G を全て求めよ．

課題 10.2 有限アーベル群 G の位数 $|G|$ が平方因子を持たなければ（即ち，素数の二乗で割り切れなければ），G は巡回群であることを示せ．

11　群の集合への作用

定義 11.1 群 G と集合 X に対して，写像

$$G \times X \ni (g, x) \mapsto g * x \in X$$

が**作用**であるとは

1) 任意の $x \in X$ に対して $1_G * x = x$,

2) 任意の $g, h \in G$ と $x \in X$ に対して $(gh) * x = g * (h * x)$

なることをいう．

群 G の集合 X への作用

$$G \times X \ni (g, x) \mapsto g * x \in X$$

があるとき，$g \in G$ に対して

$$\theta_g : X \ni x \mapsto g * x \in X$$

とおくと

1) $\theta_g \circ \theta_h = \theta gh$,

2) θ_g は X から X への全単射

である．
[**証明**] 実際，まず任意の $x \in X$ に対して

$$\theta_g \circ \theta_h(x) = \theta_g(h * x) = g * (h * x) = (gh) * x = \theta_{gh}(x)$$

だから $\theta_g \circ \theta_h = \theta gh$ となる．特に

$$\theta_{1_G}(x) = 1_G * x = x \quad (x \in X), \qquad \therefore\ \theta_{1_G} = \mathrm{id}_X$$

だから，任意の $g \in G$ に対して

$$\theta_g \circ \theta_{g^{-1}} = \theta_{g^{-1}} \circ \theta_g = \theta_{1_G} = \mathrm{id}_X$$

である．よって $x, x' \in X$ に対して

$$\theta_g(x) = \theta_g(x')\ \Rightarrow\ \theta_{g^{-1}} \circ \theta_g(x) = \theta_{g^{-1}} \circ \theta_g(x')\ \Rightarrow\ x = x'$$

だから θ_g は単射である．また任意の $y \in X$ に対して $x = \theta_{g^{-1}}(y) \in X$ とおけば

$$\theta_g(x) = \theta_g \circ \theta_{g^{-1}}(y) = y$$

となるから，θ_g は全射である．∎
よって群準同型写像

$$\theta : G \ni g \mapsto \theta_g \in S(X)$$

ができる．逆に群準同型写像

$$\varphi : G \ni g \mapsto \varphi_g \in S(X)$$

があるときに，$g \in G$ と $x \in X$ に対して $g * x = \varphi_g(x) \in X$ とおくと

$$G \times X \ni (g, x) \mapsto g * x \in X$$

は作用である：実際，$\varphi_{1_G} = \mathrm{id}_X$ だから，任意の $x \in X$ に対して

$$1_G * x = \varphi_{1_G}(x) = x$$

である．また $g, h \in G$ に対して $\varphi_{gh} = \varphi_g \circ \varphi_h$ だから

$$(gh) * x = \varphi_{gh}(x) = \varphi_g \circ \varphi_h(x) = \varphi_g(h * x) = g * (h * x)$$

となる．

例 11.2 群 G に対して，G を単なる集合とみて $X = G$ とおく．このとき $g \in G$ と $x \in X$ に対して $g * x = g \cdot x \in X$ とすると

$$G \times X \ni (g, x) \mapsto g * x \in X$$

は作用となる．実際

$$1_G * x = 1_g \cdot x = x \qquad (\forall x \in X)$$

であり，$g, h \in G$ に対して

$$(gh) * x = (gh) \cdot x = g \cdot (h \cdot x) = g * (h * x) \quad (\forall x^i n X)$$

である．すると群の準同型写像

$$\theta : G \ni g \mapsto \theta_g \in S(X)$$

が $\theta_g(x) = g * x$ により定義される．このとき $\mathrm{Ker}(\theta) = \{1_G\}$ である：実際，

$$g \in \mathrm{Ker}(\theta) \ \Rightarrow \ \theta_g = \mathrm{id}_X \ \Rightarrow \ 1_G = \theta_g(1_G) = g * 1_G = g \cdot 1_G = g$$

だからである．即ち $\theta : G \to S(X)$ は単射群準同型写像となるから，群の同型

$$\theta : G \tilde{\to} \mathrm{Im}(\theta) \subset S(X)$$

が成り立つ．

上の例を G が有限群の場合に適用すると，$|G| = n$ ならば $S(G)$ は n 次対称群 S_n と同型だから，次の定理が得られる：

定理 11.3 G が有限群で $|G| = n$ ならば，G は n 次対称群 S_n の部分群と同型である．

課題 11.1 有限群 G の部分群 $N \subset G$ に対して，群指数 $(G : N) = p$ が $|G|$ の最小の素因数ならば，N は G の正規部分群である．この命題を次の手順で証明せよ：

1) 群 G の集合 $X = G/N$ への作用が $(g, xN) \mapsto *(xN) = gxN$ により定義されることを示せ．

2) 上で定義した作用に付随する群の準同型写像 $\theta : G \to S(X)$ の核 $\mathrm{Ker}(\theta)$ について，群指数 $(G : \mathrm{Ker}(\theta))$ は $p!$ の約数であることを示せ．

3) $\mathrm{Ker}(\theta) \subset N$ であることを示せ．

4) $N = \mathrm{Ker}(\theta)$ であることを示せ．

12 G-軌道と固定部分群

群 G が集合 X に

$$G \times X \ni (g, x) \mapsto g * x \in X$$

により作用しているとする．このとき $x \in X$ に対して

$$\Omega = \{g * x \mid g \in G\}$$

を x の G-軌道と呼ぶ．G-軌道は次のような性質がある：

命題 12.1　1) $x \in X$ の G-軌道 Ω に対して $x \in \Omega$ である．

2) $\Omega \subset X$ が G-軌道で $y \in \Omega$ ならば，Ω は y の G-軌道である．

3) 二つの G-軌道 $\Omega, \Omega' \subset X$ に対して，$\Omega \neq \Omega'$ ならば $\Omega \cap \Omega' = \emptyset$ である．

[**証明**] 1) $x = 1_G * x \in \Omega$ である．

2) Ω は $x \in X$ の G-軌道であるとすると，$y = g * x$ なる $g \in G$ が存在する．すると任意の $h \in G$ に対して

$$h * y = h * (g * x) = (hg) * x \in \Omega$$

だから

$$\{h * y \mid h \in G\} \subset \Omega$$

である．一方

$$g^{-1} * y = g^{-1} * (g * x) = (g^{-1}g) * x = 1_G * x = x$$

だから，任意の $h \in G$ に対して

$$h * x = h * (g^{-1} * y) = (hg^{-1}) * y$$

となる．即ち

$$\Omega = \{h * x \mid h \in G\} \subset \{h * y \mid h \in G\}$$

となる．よって $\Omega = \{h * y \mid h \in G\}$ は y の G-軌道となる．

3) $\Omega \cap \Omega' \neq \emptyset$ と仮定すると，$y \in \Omega \cap \Omega'$ が存在する．$y \in \Omega$ だから Ω は y の G-軌道である．$y \in \Omega'$ だから Ω' も y の G-軌道である．よって $\Omega = \Omega'$ となる．■

命題 12.2 群 G が集合 X に

$$G \times X \ni (g, x) \mapsto g * x \in X$$

により作用しているとき，$x \in X$ に対して

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

は G の部分群となる．これを G における x の固定部分群と呼ぶ．

[証明] まず $1_G * x = x$ だから $1_G \in G_x$ である．$g, h \in G_x$ とすると，$g*x = x, h*x = x$ だから

$$(gh) * x = g * (h * x) = g * x = x$$

となり，$gh \in G_x$ である．更に $g \in G_x$ とすると，$g*x = x$ の両辺に $g^{-1} \in G$ を作用させて

$$g^{-1} * x = g^{-1} * (g * x) = (g^{-1}g) * x = 1_G * x = x$$

だから $g^{-1} \in G_x$ である．■

群が集合に作用しているとき，軌道と固定部分群の間の次の関係が重要である：

定理 12.3 群 G が集合 X に

$$G \times X \ni (g, x) \mapsto g * x \in X$$

により作用しているとき，$x \in X$ の G-軌道を Ω とすると，全単射

$$G/G_x \ni gG_x \mapsto g * x \in \Omega$$

が成り立つ．

[証明] まず $gG_X = g'G_x$ とすると，$g^{-1}g' = h \in G_x$ だから $g' = gh$ である．よって

$$g'x = (gh) * x = g * (h * x) = g * x$$

となる．よって写像

$$(*) : G/G_x \ni gG_x \mapsto g * x \in \Omega$$

が定義される．このとき

$$\Omega = \{g * x \mid g \in G\}$$

だから $(*)$ が全射であることは明らかである．■

課題 12.1 $G = SL_2(\mathbb{R})$ は行列の積に関して群である（例 3.5 参照）．

$$X = \{z \in \mathbb{C} \mid \mathrm{Im}\, z > 0\}$$

とおいて，次の問いに答えよ：

1) $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$ と $z \in X$ に対して

$$g * z = \frac{az+b}{cz+d} \in X$$

であることを示せ.

2) $G \times X \to X$ $((g,z) \mapsto g*z)$ は作用であることを示せ.

3) $z \in X$ の固定部分群 G_z の位数 $|G_z|$ を求めよ.

13 群の共役類と類公式

群 G をとる. $X = G$ を集合とみて, $g \in G, x \in X$ に対して $g * x = gxg^{-1} \in X$ とおくと

$$G \times X \ni (g,x) \mapsto g * x = gxg^{-1} \in X$$

は作用となる. この作用に関して, $x \in X$ の G-軌道

$$\{x\}_G = \{g * x \mid g \in G\} = \{gxg^{-1} \mid g \in G\}$$

を $x \in G$ の G-共役類と呼ぶ. また $x \in X$ の固定部分群

$$Z_G(x) = \{g \in G \mid g * x = x\} = \{g \in G \mid gx = xg\}$$

を G における $x \in G$ の中心化群と呼ぶ. すると作用の一般論から, 全単射

$$G/Z_G(x) \to \{x\}_G \qquad \left(gZ_G(x) \mapsto gxg^{-1}\right) \tag{13.5}$$

が成り立つ. G-共役類の全体を $\mathrm{Conj}(G)$ と書く.

特に $|G| < \infty$ の場合を考えよう. $\{x\}_G \in \mathrm{Conj}(G)$ に対して

$$\begin{aligned} \sharp\{x\}_G(G : Z_G(x)) = 1 &\Leftrightarrow G = Z_G(x) \\ &\Leftrightarrow \text{任意の } g \in G \text{ に対して } gx = xg \\ &\Leftrightarrow x \in Z(G) \end{aligned}$$

である. 従って

$$\begin{aligned} |G| &= \sum_{\{x\} \in \mathrm{Conj}(G)} \sharp\{x\}_G = \sum_{\substack{\{x\} \in \mathrm{Conj}(G) \\ \sharp\{x\}_G = 1}} \sharp\{x\}_G + \sum_{\substack{\{x\} \in \mathrm{Conj}(G) \\ \sharp\{x\}_G > 1}} \sharp\{x\}_G \\ &= |Z(G)| + \sum_{\substack{\{x\} \in \mathrm{Conj}(G) \\ \sharp\{x\}_G > 1}} (G : Z_G(x)) \end{aligned}$$

となる. つまり次の定理が成り立つ:

定理 13.1 有限群 G に対して

$$|G| = |Z(G)| + \sum_{\substack{\{x\} \in \mathrm{Conj}(G) \\ \sharp\{x\}_G > 1}} (G : Z_G(x))$$

である．これを**類公式**と呼ぶ．

類公式の応用として，次の定理を示そう：

定理 13.2 有限群 G に対して，$|G| = p^e > 1$ (p : 素数) に対して $|Z(G)| > 1$ である．

[**証明**] $\sharp\{x\}_G > 1$ なる $\{x\}_G \in \mathrm{Conj}(G)$ に対して

$$\sharp\{x\}_G = (G : Z_G(x)) = \frac{|G|}{|Z_G(x)|}$$

は $|G| = p^e > 1$ の約数だから，$(G : Z_G(x))$ は p で割り切れる．一方，類公式

$$|G| = |Z(G)| + \sum_{\substack{\{x\} \in \mathrm{Conj}(G) \\ \sharp\{x\}_G > 1}} (G : Z_G(x))$$

で $|G| = p^e > 1$ だから，$|Z(G)| \geq 1$ は p で割り切れなくてはならない．よって $|Z(G)| > 1$ である．∎

この定理の系として，次が成り立つ：

系 13.3 有限群 G に対して $|G| = p^2$ (p : 素数) ならば G はアーベル群である．

[**証明**] $|Z(G)|$ は $|G| = p^2$ の約数だから $|Z(G)| = 1, p, p^2$ である．定理 13.2 から $|Z(G)| > 1$ だから $|Z(G)| = p$ または $|Z(G)| = p^2$ である．$|Z(G)| = p$ とすると，$Z(G) \neq G$ だから G はアーベル群ではない．ところが

$$|G/Z(G)| = (G : Z(G)) = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p$$

だから，定理 8.12 より $G/Z(G)$ は巡回群となる．よって定理 8.13 より G はアーベル群となり，矛盾する．よって $|Z(G)| = p^2$ のみが可能である．$|Z(G)| = p^2$ ならば $|Z(G)| = |G|$ だから $G = Z(G)$，よって G はアーベル群である．∎

課題 13.1 有限アーベル群の構造定理を用いて，有限群 G で $|G| = 4$ なるものを全て求めよ．

課題 13.2 p を素数とする．$|G| = P^3$ なる非アーベル群 G に対して，

$$G/Z(G) \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

であることを示せ．

14 Sylow の定理

命題 14.1 有限アーベル群 G の位数の素因子 p にたいして，G の位数 p の部分群が存在する．

[**証明**] $G = \{g_1 = 1, g_2, \cdots, g_n\}$ として

$$\langle g_2 \rangle \times \cdots \times \langle g_n \rangle \to G \quad ((x_2, \cdots, x_n) \mapsto x_2 \cdots x_n)$$

は全射だから $|\langle g_i \rangle|$ $(i = 2, \cdots, n)$ の少なくとも一つは p で割り切れる．■

定理 14.2 有限群 G の位数の約数なる p^e $(e > 0)$ に対して $|H| = p^e$ なる G の部分群 H が存在する．

[**証明**] $|G| = p$ ならば明らかだから，$|H| < |G|$ なる任意の群 H に対して定理が成り立つと仮定する．$p \not| (G : H)$ なる部分群 $H \lneqq G$ があれば，$|H| < |G|$ かつ p^e は $|H|$ の約数だから，帰納法の仮定から H の部分群で位数 p^e なるものが存在する．任意の部分群 $H \lneqq G$ に対して $p|(G : H)$ ならば，類公式から $p||Z(G)|$．よって命題 14.1 から $Z(G)$ は位数 p の部分群 N をもつ．$N \triangleleft G$ で $p^{e-1}||G/N|$ かつ $|G/N| < |G|$ だから，帰納法の仮定から G/N は位数 p^{e-1} の部分群 H/N $(N \subset H \subset G)$ をもつ．このとき $|H| = p^e$ である．■

命題 14.3 p-群 G が集合 X に $(g, x) \mapsto g \cdot x$ により作用していて $p \not| \sharp X$ ならば，$g \cdot x = x$ for $\forall g \in G$ なる $x \in X$ が存在する．

[**証明**] $X = \Omega_1 \cup \cdots \cup \Omega_r$ を G-軌道分解とし，$x_i \in \Omega_i$ の固定部分群を G_i とすると

$$\sharp X = \sum_{i=1}^{r} \sharp \Omega_i = \sum_{i=1}^{r} (G : G_i).$$

ここで $(G : G_i) > 1$ ならば $p|(G : G_i)$ で $p \not| \sharp X$ だから，$(G : G_i) = 1$ なる i がある．即ち $g \cdot x_i = x_i$ for $\forall g \in G$ となる．■

定義 14.4 有限群 G と素数 p に対して $|G| = p^e m$, $p \not| m$ $(e > 0)$ のとき，$|S| = p^e$ なる部分群 $S \subset G$ を G の **p-Sylow 部分群**と呼ぶ．

定理 14.5 有限群 G と $p||G|$ なる素数 p に対して

1) G の p-Sylow 部分群が存在する．
2) p-Sylow 部分群 $S \subset G$ と p-部分群 $T \subset G$ に対して $T \subset gSg^{-1}$ なる $g \in G$ が存在する．

3) p-Sylow 部分群 $S \subset G$ に対して

$$\sharp\{G \text{ の } p\text{-Sylow 部分群 }\} = (G : N_G(S)) \equiv 1 \pmod{p}.$$

[**証明**] 1) 定理 14.2 より良い．

2) p-群 T が $X = G/S$ に自然に作用していて $p \not| \sharp X$ だから，命題 14.3 より $t \cdot gS = gS$ for $\forall t \in T$ なる $gS \in X$ が存在する．即ち $g^{-1}Tg \subset S$ となる．■

系 14.6 有限群 G の位数 $|G|$ の素因数 p に対して，S, S' が G の p-Sylow 部分群ならば $S' = gSg^{-1}$ なる $g \in G$ が存在する．

[**証明**] 定理 14.5 の 2) より $S' \subset gSg^{-1}$ なる $g \in G$ が存在する．ここで

$$|gSg^{-1}| = |S| = |S'|$$

だから $S' = gSg^{-1}$ である．■

3 次対称群の場合を考えてみると

例 14.7 3 次対称群 S_3 の位数は $|S_3| = 3! = 6 = 2 \cdot 3$ だから，S_3 の 2-Sylow 部分群と 3-Sylow 部分群が考えられる．$S \subset S_3$ が 2-Sylow 部分群とすると，$|S| = 2$ は素数だから S は巡回群となる．従って S_3 の 2-Sylow 部分群は

$$S_1 = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\rangle, \quad S_2 = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\rangle, \quad S_3 = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\rangle$$

の 3 個である．$T \subset S_3$ が 3-Sylow 部分群とすると，$|T| = 3$ は素数だから T は巡回群となる．従って S_3 の 3-Sylow 部分群は

$$T = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\rangle$$

の 1 個である．

上の例からも判るとおり，有限群の p-Sylow 部分群の個数は様々である．ここで次の定理が成り立つ：

定理 14.8 有限群 G の位数 $|G|$ の素因数 p に対して，G の p-Sylow 部分群の個数を $n_p(G)$ と書くことにすると

1) $n_p(G)$ は $|G|$ の約数である．

2) $n_p(G) \equiv 1 \pmod{p}$ である．

[証明] 1) G の p-Sylow 部分群の全体を X とすると

$$G \times X \to X \qquad ((g, S) \mapsto gSg^{-1})$$

は群 G の X への作用である．$S \in X$ を一つ取ると，系 14.6 から，X 全体が S の G-軌道であることが判る．$S \in X$ の固定部分群は

$$\{g \in G \mid gSg^{-1} = S\} = N_G(S)$$

となり，G における $S \subset G$ の正規化群である．よって

$$n_p(G) = \sharp X = \sharp(G/N_G(S)) = (G : N_G(S))$$

となる．ところが $|G| = (G : N_G(S)) \cdot |N_G(S)|$ だから，$n_p(G)$ は $|G|$ の約数である．

2) p-Sylow 部分群 $S \subset G$ を一つとると，上で見た通り $n_p(G) = \sharp(G/N_G(S))$ である．ここで

$$S \times G/N_G(S) \to G/N_G(S) \qquad \big((s, gN_G(S)) \mapsto sgN_G(S)\big)$$

は群 S の集合 $G/N_G(S)$ への作用である．そこで $x = gN_G(S) \in G/N_G(S)$ の S-軌道を Ω とする．x の固定部分群は

$$\begin{aligned} S_x =& \{s \in S \mid sgN_G(S) = gN_G(S)\} \\ =& \{s \in S \mid g^{-1}sg \in N_G(S)\} \end{aligned}$$

で

$$\sharp\Omega = \sharp(S/S_x) = (S : S_x) = \frac{|S|}{|S_x|}$$

となる．ここで $|S|$ は p の冪だから，$\sharp\Omega$ は p の冪となる．よって $\sharp\Omega > 1$ ならば $\sharp\Omega$ は p で割り切れる．更に

$$\begin{aligned} \sharp\Omega = 1 \;&\Leftrightarrow\; |S| = |S_x| \qquad \therefore\;\; S = S_x \\ &\Leftrightarrow\; \text{任意の } s \in S \text{ に対して } g^{-1}sg \in N_G(S) \\ &\Leftrightarrow\; g^{-1}Sg \subset N_G(S) \end{aligned}$$

である．ところで $g^{-1}Sg \subset N_G(S)$ ならば $g^{-1}Sg$ は $N_G(S)$ の p-Sylow 部分群である．一方，常に $S \subset N_G(S)$ であって，S も $N_G(S)$ の p-Sylow 部分群である．よって系 14.6 より $g^{-1}Sg = hSh^{-1}$ なる $h \in N_G(S)$ が存在する．ところが $h \in N_G(S)$ ならば $hSh^{-1} = S$ だから $g^{-1}Sg = S$ となる．よって $g \in N_G(S)$ となるから $gN_G(S) = N_G(S)$ となる．つまり

$$\sharp\Omega = 1 \;\Leftrightarrow\; \Omega \text{ は } N_G(S) \in G/N_G(S) \text{ の } S\text{-軌道}$$

となる．言い換えれば $\sharp\Omega = 1$ となる S-軌道は一つだけある．そこで $G/N_G(S)$ の S-軌道への分解を

$$G/N_G(S) = \Omega_1 \cup \Omega_2 \cup \cdots \cup \Omega_r$$

として $\sharp\Omega_1 = 1$ とすると $\sharp\Omega_i$ $(i = 2, \cdots, r)$ は p で割り切れるから

$$n_p(G) = \sharp(G/N_G(S)) = \sum_{i=1}^{r} \sharp\Omega_i \equiv 1 \pmod{p}$$

となる．■

Sylow 部分群の応用として，次の定理を示そう：

定理 14.9 二つの異なる素数 $p < q$ に対して $|G| = pq$ なる有限群 G は

$$q \not\equiv 1 \pmod{p}$$

ならば巡回群 $\mathbb{Z}/pq\mathbb{Z}$ と同型である．

[**証明**] $S \subset G$ を p-Sylow 部分群，$T \subset G$ を q-Sylow 部分群とする．G の q-Sylow 部分群の個数 $n_q(G)$ は $|G| = pq$ の約数だから $n_q(G) = 1, p, q, pq$ のいずれかである．更に $n_q(G) \equiv 1 \pmod{q}$ だから，q, pq はあり得ない．$p < q$ だから p もあり得ない．よって $n_q(G) = 1$ である．ところが任意の $g \in G$ に対して，gTg^{-1} は G の q-Sylow 部分群だから $gTg^{-1} = T$ となる．よって T は G の正規部分群である．同様に G の p-Sylow 部分群の個数 $n_p(G)$ は $|G| = pq$ の約数だから $n_p(G) = 1, p, q, pq$ である．$n_p(G) \equiv 1 \pmod{p}$ だから，仮定 $q \not\equiv 1 \pmod{p}$ から，$np(G) = 1$ のみが可能である．よって T の場合と同様に S は G の正規部分群となる．ここで $S \cap T = \{1\}$ である．実際，$g \in S \cap T$ とすると

$$\langle g \rangle \subset S : \text{部分群} \quad \therefore \ |\langle g \rangle| \text{ は } |S| = p \text{ の約数} \quad \therefore \ |\langle g \rangle| = 1, p,$$

$$\langle g \rangle \subset T : \text{部分群} \quad \therefore \ |\langle g \rangle| \text{ は } |T| = q \text{ の約数} \quad \therefore \ |\langle g \rangle| = 1, q,$$

だから $|\langle g \rangle| = 1$，即ち $\langle g \rangle = \{1\}$ だから $g = 1$ である．よって定理 10.2 の 1) から

$$f : S \times T \to G \qquad ((x, y) \mapsto xy)$$

は単射群準同型写像である．よって

$$|\mathrm{Im}(f)| = |S \times T| = |S| \cdot |T| = pq = |G|$$

だから $\mathrm{Im}(f) = G$，即ち f は全射となる．よって f は群の同型写像である．よって G は二つの巡回群（従ってアーベル群）の直積だからアーベル群となる．よって有限アーベル群の構造定理から

$$G \simeq \mathbb{Z}/pq\mathbb{Z}$$

となり，G は巡回群である．■

課題 14.1　1) 5 次対称群 S_5 の 5-Sylow 部分群を一つ求めよ．

2) 5 次対称群 S_5 の 5-Sylow 部分群は 12 個あることを示せ．

課題 14.2 素数 p に対して p 次対称群 S_p を考える．

1) p 次対称群 S_p の p-Sylow 部分群を一つ求めよ．

2) p 次対称群 S_p の p-Sylow 部分群の個数は $(p-2)!$ 個であることを示せ．

15　半直積

二つの群 N, H を考える．10 節で群の直積 $N \times H$ を定義したが，ここではそれを少し一般化してみよう．

まず群 N の自己同型群 $\mathrm{Aut}(N)$ に対して，群の準同型写像

$$\theta : H \to \mathrm{Aut}(N) \qquad (s \mapsto \theta_s)$$

が与えられたとする．このとき

1) 任意の $s, t \in H$ に対して $\theta_s \circ \theta_t = \theta_{st}$,

2) 任意の $s \in H$ に対して $\theta_{s^{-1}} = \theta_s^{-1}$ は θ_s の逆写像である，

3) $\theta_{1_H} = \mathrm{id}_N$ は N の恒等写像である

が成り立つ．ここで N, H, θ を用いて新しい群を構成することが出来る：

命題 15.1 直積集合 $N \times H$ は演算

$$(x, s) \cdot (y, t) = (x \cdot \theta_s(y), s \cdot t)$$

により群となる．

$$\text{単位元} = (1_N, 1_H), \qquad (x, s) \text{ の逆元} = (\theta_{s^{-1}}(x)^{-1}, s^{-1})$$

である．このようにして出来る群を N と H の θ に関する**半直積**と呼び $N \times_\theta H$ と表す．

[**証明**] $(x, s), (y, t), (z, u) \in N \times H$ とする．

$$\begin{aligned} \big((x, s) \cdot (y, t)\big) \cdot (z, u) &= (x \cdot \theta_s(y), st) \cdot (z, u) \\ &= (x \cdot \theta_s(y) \cdot \theta_{st}(z), stu)\,, \end{aligned}$$

$$\begin{aligned}(x,s)\big((y,t)\cdot(z,u)\big) &= (x,s)\cdot(y\cdot\theta_t(z),tu)\\ &= (x\cdot\theta_s(y\cdot\theta_t(z)),stu)\end{aligned}$$

である．ここで $s\mapsto\theta_s$ は群の準同型写像だから $\theta_s\circ\theta_t=\theta_{st}$ である．従って

$$x\cdot\theta_s(y\cdot\theta_t(z))=x\cdot\theta_s(y)\cdot\theta_{st}(z)$$

となるから

$$\big((x,s)\cdot(y,t)\big)\cdot(z,u)=(x,s)\big((y,t)\cdot(z,u)\big)$$

となり，結合法則が成り立つ．また θ_{1_H} は N 上の恒等写像だから

$$\begin{aligned}(1_N,1_H)\cdot(x,s)&=(1_N\cdot\theta_{1_H}(x),1_H\cdot s)=(x,s),\\ (x,s)\cdot(1_N,1_H)&=(x\cdot\theta_s(1_N),s\cdot 1_H)=(x,s)\end{aligned}$$

となり，$(1_N,1_H)$ が単位元となることが判る．最後に

$$\begin{aligned}&\theta_s\circ\theta_{s^{-1}}=\theta_{ss^{-1}}=\theta_{1_H}=N\text{ 上の恒等写像},\\ &\theta_{s^{-1}}\circ\theta_s=\theta_{s^{-1}s}=\theta_{1_H}=N\text{ 上の恒等写像}\end{aligned}$$

だから

$$\begin{aligned}&(x,s)\cdot(\theta_{s^{-1}}(x)^{-1},s^{-1})=(x\cdot\theta_s(\theta_{s^{-1}}(x)^{-1}),ss^{-1})=(xx^{-1},1_H)=(1_N,1_H),\\ &(\theta_{s^{-1}}(x)^{-1},s^{-1})\cdot(x,s)=(\theta_{s^{-1}}(x)^{-1}\cdot\theta_{s^{-1}}(x),s^{-1}s)=(1_N,1_H)\end{aligned}$$

となり，$(\theta_{s^{-1}}(x)^{-1},s^{-1})$ が (x,s) の逆元であることが判る．■

半直積 $N\times_\theta H$ の特別な場合として，全ての $s\in H$ に対して $\theta_s=\mathrm{id}_N$ が N の恒等写像となる場合，$N\times_\theta H$ 上の演算は

$$(x,s)\cdot(y,t)=(x\cdot\theta_s(y),st)=(xy,st)$$

となり，N と H の直積群となる．

定理 15.2 群 G の部分群 $H\subset G$ と正規部分群 $N\subset G$ に対して，群準同型写像

$$\theta:H\to\mathrm{Aut}(N)\qquad(s\mapsto\theta_s)$$

を $\theta_s(x)=sxs^{-1}$ $(s\in H,x\in N)$ により定義する．このとき

$$f:N\times_\theta H\to G\qquad\big((x,s)\mapsto xs\big)$$

は群準同型写像である．更に

1) $N\cap H=\{1_G\}$ ならば f は単射である．

2) $G = \{xs \mid x \in N, s \in H\}$ ならば f は全射である．

よって

$$N \cap H = \{1_G\} \text{ かつ } G = \{xs \mid x \in N, s \in H\}$$

ならば G は半直積 $N \times_\theta H$ と同型である．

[**証明**] $x, y \in N, s, t \in H$ に対して，G であの演算で

$$(xs) \cdot (yt) = x \cdot (sys^{-1}) \cdot (st) = x \cdot \theta_s(y) \cdot (st)$$

となることに注意しよう．従って

$$\begin{aligned} f\big((x,s)\cdot(y,t)\big)\big) &= f\left(x \cdot \theta_s(y), st\right) = x \cdot \theta_s(y) \cdot st \\ &= (xs) \cdot (yt) = f(x,s) \cdot f(y,t) \end{aligned}$$

となり，f は群準同型写像である．

1) $(x, s) \in N \times_\theta H$ に対して

$$f(x,s) = 1_G \quad \Leftrightarrow \quad xs = 1_G \quad \Leftrightarrow \quad x = s^{-1} \in N \cap H$$

だから

$$\mathrm{Ker}(f) = \left\{(x, x^{-1}) \mid x \in N \cap H\right\}$$

となる．よって $N \cap H = \{1_G\}$ ならば $\mathrm{Ker}(f) = \{(1_G, 1_G)\}$ となり，群準同型写像 f は単射である．

2) 明らか．■

例 15.3 位数 n の巡回群 N と位数 2 の巡回群 $\{\pm 1\}$ を考えると，群準同型写像

$$\theta : \{\pm 1\} \to \mathrm{Aut}(N) \qquad \big(\theta_\varepsilon(x) = x^\varepsilon \ \ \varepsilon = \pm 1,\ x \in N\big)$$

があるから，半直積 $N \times_\theta \{\pm 1\}$ が定義される．これを位数 $2n$ の**二面体群**と呼び D_{2n} で表す．

二面体群 D_{2n} を幾何学的に考えると次のようになる：平面上の正 n 角形 P を考えよう．P に対する回転，裏返しで，もとの P に重なるもの全体を群と考えると，それが D_{2n} と同型である．N の元は P の中心の周りの回転に対応し，$\{\pm 1\}$ の元は P 中心と一つの頂点を通る直線に関する裏返しに対応する．

課題 15.1 $GL_2(\mathbb{R})$ の部分群

$$G = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in GL_2(\mathbb{R}) \right\}$$

について（課題 3.4 参照），次の問いに答えよ：

1) $N = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbb{R}) \right\}$ は G の正規部分群であることを示せ.

2) $H = \left\{ \begin{bmatrix} a & 0 \\ 0 & d \end{bmatrix} \in GL_2(\mathbb{R}) \right\}$ は G の部分群であることを示せ.

3) $N \cap H = \{1_G\}$ かつ

$$G = \{xs \mid x \in N, s \in H\}$$

であることを示せ.

4) 定理 15.2 にあるように G と半直積 $N \times_\theta H$ が同型となるような，群準同型写像

$$\theta : H \to \mathrm{Aut}(N) \qquad (s \mapsto \theta_s)$$

を具体的に書け.

課題 15.2 群 N, H と群準同型写像

$$\theta : H \to \mathrm{Aut}(N) \qquad (s \mapsto \theta_s)$$

に対して

$$N \times_\theta H : \text{アーベル群} \Leftrightarrow \begin{cases} N, H \text{ はアーベル群}, \\ \text{任意の } s \in H \text{ に対して } \theta_s = \mathrm{id}_N \end{cases}$$

であることを示せ.

16 位数が二つの素数の積となる有限群の決定

位数が二つの素数の積となる有限群 G がどのようなものか考えてみよう.

$$|G| = pq \qquad (p, q : \text{素数})$$

とする．$p = q$ ならば，系 13.3 より G はアーベル群となる．更に $p < q$ の場合に，$q \not\equiv 1 \pmod{p}$ の場合には，定理 14.9 より G は巡回群となる．従って残されているのは $p < q$ かつ $q \equiv 1 \pmod{p}$ の場合である．まず

定理 16.1 $|G| = 2q$ ($q > 2$ は素数) なる有限群 G は巡回群 $\mathbb{Z}/2q\mathbb{Z}$ か二面体群 D_{2q} と同型である.

[**証明**] $N \subset G$ を q-Sylow 部分群，$H \subset G$ を 2-Sylow 部分群とする．$|N| = q, |H| = 2$ だから N, H は共に巡回群である (定理 8.12)．また $N \cap H = \{1_G\}$ である (課題 4.4)．さて G の q-Sylow 部分群の個数を $N_G(q)$ とすると，定理 14.5 の 3) より，$N_G(q)$ は $|G| = 2q$ の約数であり，かつ $N_G(q) \equiv 1 \pmod{q}$

である．よって $N_G(q)=1$ 以外にはありえない．ところで任意の $g\in G$ に対して $gNg^{-1}\subset G$ は q-Sylow 部分群となるから，$gNg^{-1}=N$ でなくてはならない．即ち $N\subset G$ は正規部分群である．よって定理 15.2 より，群準同型写像

$$\theta : H\to \mathrm{Aut}(N)\qquad \big(s\in H, x\in N \text{ に対して } \theta_s(x)=sxs^{-1}\big)$$

に対して，G は半直積 $N\times_\theta H$ と同型である．ここで $N=\langle g\rangle, H=\langle s\rangle$ とおく．$\theta_s(g)=g^e$ とすると，$s^2=1$ だから

$$\theta_s\circ\theta_s=\theta_{s^2}=\mathrm{id}_N,$$

従って

$$g=\theta_s\circ\theta_s(g)=\theta_s(g^e)=\theta_s(g)^e=g^{e^2}$$

となる．これは $e^2\equiv 1\,(\mathrm{mod}\ q)$ を意味するが，q は奇数の素数だから $e\equiv\pm 1\ (\mathrm{mod}\ q)$ である．

$e\equiv 1\,(\mathrm{mod}\ q)$ ならば $\theta_s(g)=g$ だから，$N\times_\theta H$ は直積群 $N\times H$ となり，G はアーベル群となる．よって有限アーベル群の構造定理から G は巡回群 $\mathbb{Z}/2q\mathbb{Z}$ と同型である．

$e\equiv -1\,(\mathrm{mod}\ q)$ ならば $\theta_s(G)=g^{-1}$ だから，$N\times_\theta H$ は二面体群 D_{2q} と同型である．■

特に

系 16.2 $|G|=6$ なる有限群 G は，巡回群 $\mathbb{Z}/6\mathbb{Z}$ か 3 次対称群 S_3 と同型である．

[**証明**] $|G|=2\cdot 3$ だから，定理 16.1 より G は巡回群 $\mathbb{Z}/6\mathbb{Z}$ または二面体群 D_6 と同型である．ここで D_6 は非アーベル群である．一方 3 次対称群 S_3 は $|S_3|=6$ なる非アーベル群だから D_6 と同型である．■

更に一般的に

定理 16.3 二つの異なる素数 $p<q$ に対して $|G|=pq$ なる有限群 G は

$$q\equiv 1\ \ (\mathrm{mod}\ p)$$

ならば同型を除いて二つあって，巡回群または非アーベル群である．

[**証明**] p-Sylow 部分群 $H\subset G$ と q-Sylow 部分群 $N\subset G$ をとる．$|H|=p, |N|=q$ だから，H, N は共に巡回群である (定理 8.12)．また $N\cap H=\{1_G\}$ である (課題 4.4)．さて G の q-Sylow 部分群の個数を $n_q(G)$ とすると，$n_q(G)$

は $|G| = pq$ の約数かつ $n_q(G) \equiv 1 \pmod q$ だから，$n_q(G) = 1$ である．よって $N \subset G$ は正規部分群である．よって定理 15.2 より，群準同型写像

$$\theta : H \to \mathrm{Aut}(N) \qquad \left(s \in H, x \in N \text{ に対して } \theta_s(x) = sxs^{-1}\right)$$

に対して，G は半直積 $N \times_\theta H$ と同型である．ここで $N = \langle g \rangle, H = \langle h \rangle$ とおいて $\theta_h(g) = g^e$ とする．$h^p = 1$ だから

$$\underbrace{\theta_h \circ \cdots \circ \theta_h}_{p \text{ 個}} = \theta_{h^p} = \mathrm{id}_N$$

だから

$$g = \underbrace{\theta_h \circ \cdots \circ \theta_h}_{p \text{ 個}}(g) = g^{e^p}$$

となる．これは $e^p \equiv 1 \pmod q$ を意味する．

さて剰余類環 $\mathbb{Z}/q\mathbb{Z}$ は有限個の元からなる体で，その乗法群 $(\mathbb{Z}/(q))^\times$ は巡回群となり（定理 10.4），$|(\mathbb{Z}/(q))^\times| = q - 1$ である．ここで

$$M = \{x \in (\mathbb{Z}/(q))^\times \mid x^p = 1\}$$

は $(\mathbb{Z}/(q))^\times$ の部分群となるが，$p|(q-1)$ だから M は位数 p の巡回群となる（課題 8.2）．そこで

$$M = \langle \overline{r} \rangle = \{1, \overline{r}, \overline{r}^2, \cdots, \overline{r}^{p-1}\}$$

($1 < r < p$ とおく．$\overline{e} \in M$ だから $e \equiv r^k \pmod q$ $(0 \le k < p)$ である．

$k = 0$ のとき．$e \equiv 1 \pmod q$ だから $\theta_h(g) = g$．よって任意の $s \in H$ に対して $\theta_s = \mathrm{id}_N$ である．よって半直積 $N \times_\theta H$ は直積群 $N \times H$ となり，よって G はアーベル群となる．よって有限アーベル群の構造定理から G は巡回群 $\mathbb{Z}/pq\mathbb{Z}$ と同型である．

$k \neq 0$ のとき．$0 < k < p$ だから $kl \equiv 1 \pmod p$ なる整数 $0 < l < p$ がとれる．ここで

$$\theta_{h^l}(g) = \underbrace{\theta_h \circ \cdots \circ \theta_h}_{l \text{ 個}}(g) = g^{e^l}$$

であるが，$e^l \equiv r^{kl} \equiv r \pmod q$ となるから

$$\theta_{h^l}(g) = g^r$$

である．ここで $\langle h^l \rangle = \langle h \rangle = H$ だから，h を h^l で置き替えれば

$$H = \langle h \rangle, \qquad \theta_h(g) = g^r$$

として一般性を失わない．ここで $\theta_h(g) = hgh^{-1}$ だから $hgh^{-1} = \theta_h(g) = g^r$ となるが，$1 < r < p$ だから $g^r \neq g$，従って $hgh^{-1} \neq g$ 即ち $hg \neq gh$ となるから，G は非アーベル群である．■

注意 16.4 定理 16.3 の非アーベル群を具体的に書くと，次のようになる．

二つの素数 p, q について

$$2 < p < q, \qquad q \equiv 1 \pmod{p}$$

とする．

$$\left\{\overline{n} \in (\mathbb{Z}/(q))^{\times} \mid \overline{n}^p = \overline{1}\right\} = \left\{\overline{1}, \overline{r}, \overline{r}^2, \cdots, \overline{r}^{p-1}\right\}$$

なる $1 < r < p$ がとれる．このとき $|G| = pq$ なる有限群 G は

$$G = \left\{g^i h^j \mid 0 \leq i < q, 0 \leq j < p\right\}, \quad \begin{cases} \mathrm{ord}(g) = q, \mathrm{ord}8h) = p, \\ hgh^{-1} = g^r \end{cases}$$

である．

課題 16.1 1) $|G| = 29$ なる有限群 G を同型を除いて全て求めよ．

2) $|G| = 49$ なる有限群 G を同型を除いて全て求めよ．

3) $|G| = 34$ なる有限群 G を同型を除いて全て求めよ．

4) $|G| = 35$ なる有限群 G を同型を除いて全て求めよ．

5) $|G| = 39$ なる有限群 G を同型を除いて全て求めよ．

17 4 次対称群の部分群

正八面体の各面に，番号 $\{1, 2, 3, 4\}$ を，対面が同じ番号になるようにふったものを Ω としよう．この正八面体を空間で回転させて，もとの八面体に重なるような回転の全体を G としよう．G は二つの回転を続けて行うことを群演算として，群となるので，これを正八面体群と呼ぶ．

G の回転を Ω に施すと，各面が移動して $\{1, 2, 3, 4\}$ 上の置換，即ち 4 次対称群 S_4 の元が生じる．このようにして G から S_4 への群準同型写像 θ ができる．向い合う辺の中点を通る直線の周りの 180 度回転は任意の互換 (i, j) $(1 \leq i, j \leq 4)$ を生じるから，θ は全射である．Ω の各面が動かない G の元は単位元（Ω を回転しない）だから，θ は単射である．即ち 4 次対称群 S_4 は正八面体群 G と同型である．

以下，正八面体の回転を考えながら，4 次対称群 S_4 の全ての部分群を見つけてみよう．

向い合う頂点を通る 3 本の直線 l_1, l_2, l_3 に G が作用すると，G から 3 次対称群 S_3 への群準同型写像 η が出来る．l_1 の周りの 90 度回転は l_2, l_3 の互換を生じ，他も同様だから，η は全射である．その核を V とすると $|V| = 4$ である．l_i $(i = 1, 2, 3)$ の周りの 180 度回転が V の 3 個の自明でない元を与えて

$$V = \{\mathbf{1}, (12)(34), (13)(24), (14)(23)\}$$

となり，$\overline{\eta} : G/V \xrightarrow{\sim} S_3$ である．

$|G| = 2^3 . \cdot 3$ で，Ω の中心を通り l_i $(i = 1, 2, 3)$ に直交する平面が Ω から切り出す正方形 Q_i の固定部分群 $D_8^{(i)}$ が G の 3 個の 2-Sylow 部分群である．

$$V = D_8^{(1)} \cap D_8^{(2)} = D_8^{(2)} \cap D_8^{(3)} = D_8^{(2)} \cap D_8^{(1)}$$

である．

G の 3-Sylow 部分群は 4 個あって，夫々 Ω の対面 $1, 2, 3, 4$ の中心を通る直線 M_1, M_2, M_3, M_4 の周りの 60 度回転で生成される．これを $T^{(1)}, T^{(2)}, T^{(3)}, T^{(4)}$ とする．

$H \subset G$ を位数 6 の部分群とする．G の位数 6 の部分群は，系 16.2 から，巡回群 $\mathbb{Z}/6\mathbb{Z}$ か S_3 と同型であるが，$G \simeq S_4$ は位数 6 の元を含まないから，H は S_3 と同型である．H は $\{1, 2, 3, 4\}$ に作用するから，一つの軌道を ω とする．固定部分群の位数は $1, 2, 3,$ 又は 6 だから $\sharp\omega = 3, 2$ 又は 1 である．H が G の 3-Sylow 部分群 $\langle M_4 \rangle$ (M_4 の周りの 60 度回転で生成された）を含めば，H は巡回置換 $(1, 2, 3)$ を含むから，H 軌道は二つあって，一つは 3 個の点，他の一つは 1 個の点からなる．即ち S_4 の元で $1, 2, 3, 4$ の一つを固定する部分群が S_3 と同型な G の部分群となる．

G の位数 4 の部分群 H は $D_8^{(i)}$ $(i = 1, 2, 3)$ の部分群である．$H \subset D_8^{(1)}$ とする．H が巡回群ならば l_1 の周りの回転で生成された巡回群 $H_c^{(1)}$ である．H が $(2, 2)$-型アーベル群ならば，l_2, l_3 の周りの 180 度回転で生成された V か，又は Q_1 の対辺の中点を通る直線の周りの 180 度回転で生成された $H_{2,2}^{(1)}$ で，例えば

$$H_{(2,2)}^{(1)} = \{1, (1, 2), (3, 4), (1, 2)(3, 4)\}$$

である．

S_4 の共役類とそこに含まれる元の個数は

共役類	1^4	$1^2 2^1$	$1^1 3^1$	2^2	4^1
元の個数	1	6	8	3	6

である[1]．$|H| = 12$ なる部分群 $H \subset G$ は，$(G : H) = 2$ より，$G = S_4$ の正規部分群だから S_4 の共役類の和集合となるが，可能な組み合わせは

$$H = 1^4 \sqcup 1^1 3^1 \sqcup 2^2 = A_4$$

のみである．

課題 17.1 4 次交代群 A_4 の部分群を全て求めよ．

[1] $\sigma \in S_n$ の共役類は σ を巡回置換の積に書いた時に現れる巡回置換の長さにより決まる．長さ i の巡回置換が e_i 個現れるとき，その共役類を $1^{e_1} 2^{e_2} \cdots n^{e_n}$ $(1 \cdot e_1 + 2 \cdot e_2 + \cdots + n \cdot e_n = n)$ と書くと，そこに含まれる元の個数は $\dfrac{n!}{1^{e_1} 2^{e_2} \cdots n^{e_n} e_1! e_2! \cdots e_n!}$ 個．