代数学 1 群論入門 演習問題解答

@GirlwithAHigoi, @mikecat1024

第 1 章　集合論

問題 1.1.1.

$f \longleftrightarrow g, A \longleftrightarrow X, B \longleftrightarrow X.$

問題 1.1.2.

(1) $f(S) = \{3, 4\}$.
(2) $f^{-1}(S_1) = \emptyset$, $f^{-1}(S_2) = \{1, 3, 4, 5\}$.
(3) $f^{-1}(2) = \emptyset$ なので全射ではない.
(4) $f(1) = 3 = f(4)$ なので単射ではない.

問題 1.1.3.

全射:　行き先のすべての元に対して, そこに行くもとの集合の元がある.
単射:　どの 2 つの元も同じ元に行かない.

問題 1.1.4.

全射:　$f(x) = x$, $g(x) = x^3$, $h(x) = x + \sin x$.
単射:　$f(x) = x$, $g(x) = e^x$, $h(x) = \arctan x$.

問題 1.1.5.

『f が全単射 $\iff$ f は逆写像をもつ』を示せばよい.

$\Longrightarrow$　f が全単射であることから, $\forall b \in B$ について, $f(a) = b$ となるような $a \in A$ がただ一つだけ存在する. このような a, b に対して, 写像 $g : B \to A$ を $g(b) = a$ となるように定義することができ, このとき $g \circ f = id_A, f \circ g = id_B$ なので, g は f の逆写像になる.

$\Longleftarrow$　$a_1, a_2 \in A$ について, $f(a_1) = f(a_2)$ ならば,

$$a_1 = f^{-1} \circ f(a_1) = f^{-1}(f(a_1)) = f^{-1}(f(a_2)) = f^{-1} \circ f(a_2) = a_2$$

なので, f は単射である. また, $f \circ f^{-1} = id_B$ より, $\forall b \in B$ について, $f^{-1}(b) \in A$ が存在して, $f(f^{-1}(b)) = b$ となるので, f は全射である.

問題 1.1.6.

(1) g が全射なので, $\forall c \in C$ について, $g(b) = c$ となるような $b \in B$ が存在し, f が全射なので, この b に対して $f(a) = b$ となるような $a \in A$ が存在する. したがって, $\forall c \in C$ について, $g \circ f(a) = g(f(a)) = c$ となるような $a \in A$ が存在するので, $g \circ f$ は全射である.

(2) f が単射なので, 相異なる $x, y \in A$ について, $f(x) \neq f(y)$ であり, g が単射なので, $g(f(x)) \neq g(f(y))$ が成立する. したがって, $g \circ f$ は単射である.

(3) $g \circ f$ が全射なので, $\forall c \in C$ について, $g \circ f(a) = c$ となるような $a \in A$ が存在する. このとき, $b = f(a)$ とすれば, $\forall c \in C$ について, $g(b) = c$ となるような $b \in B$ が存在することがいえるので, g は全射である.

(4) $g \circ f$ が単射なので, 相異なる $x, y \in A$ について $g \circ f(x) \neq g \circ f(y)$ である. ここで, $f(x) = f(y)$ と仮定すれば, $g(f(x)) = g(f(y))$ となって矛盾するので, $f(x) \neq f(y)$. したがって, f は単射である.

問題 1.1.7.

『f が全射 $\iff \forall S \subset B$ について, $f(f^{-1}(S)) = S$』を示せばよい.

$\Longrightarrow$ $f(f^{-1}(S)) = \{f(b) \in B \mid b \in \{a \in A \mid f(a) \in S\}\}$ であり, $\forall y \in S$ について, f の全射性から $f(x) = y$ となるような $x \in A$ が存在するので, $f(\{a \in A \mid f(a) \in S\}) = S$. したがって, $f(f^{-1}(S)) = S$.

$\Longleftarrow$ f が全射でないならば, ある $b \in B$ が存在して, $f(a) = b$ となるような $a \in A$ が存在しない. このとき $S = \{b\}$ とすれば, $\{a \in A \mid f(a) \in S\} = \emptyset$ なので, $f(f^{-1}(S)) = \emptyset \neq S$ となって矛盾.

問題 1.1.8.

$$\begin{aligned} f^{-1}(f(f^{-1}(S))) &= \{z \in A \mid f(z) \in f(f^{-1}(S))\} \\ &= \{z \in A \mid f(z) \in \{f(x) \in B \mid x \in \{y \in A \mid f(y) \in S\}\}\} \\ &= \{z \in A \mid f(z) \in S\} \\ &= f^{-1}(S). \end{aligned}$$

問題 1.1.9.

(1) $x = \frac{9}{2}$.

(2) $A = \mathbb{Z}, B = \{0\}$.

(3) $A = B = \mathbb{Z}$, $S_1 = \{0\}$, $S_2 = \{1\}$, $f(0) = f(1) = 0$.

問題 1.1.10.

(1) (d), (2) (a), (3) (b).

問題 1.1.11.

(1) (A が成り立たないまたは B が成り立たない) かつ C が成り立たない.

(2) A が成り立ち, かつ B と C の両方が成り立たない.

(3) (A が成り立ち, B が成り立たない) または (B が成り立ち, A が成り立たない).

(4) ある自然数 n が存在して, すべての実数 x に対して, $x \leq 0$ または $\frac{1}{n} \leq x$.

(5) ある $\epsilon > 0$ があり, すべての $\delta > 0$ に対し, ある $x, y \in [0, 1]$ が存在し, $|x - y| < \delta$ かつ $|f(x) - f(y)| \geq \epsilon$ が成り立つ.

問題 1.1.12.

(1) ある. (2) ない.

問題 1.1.13.

$\{(x,y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$, $\{(x,y) \in \mathbb{R} \times \mathbb{R} \mid x = y\}$, $\{(x,y) \in \mathbb{Z} \times \mathbb{Z} \mid x \equiv y \pmod 2\}$.

問題 1.2.1.

$f : \mathbb{C} \to \mathbb{R}$ を極座標を用いて, $z = r(\cos\theta + i\sin\theta) \mapsto \cos\theta$ で定める.

$$z = r(\cos\theta + i\sin\theta) = r(\cos(\theta + 2\pi) + i\sin(\theta + 2\pi))$$

なので z の表示は一意ではないが, f は表示の仕方によらずに well-defined になる.

問題 1.2.2.

べき集合 2^V, 恒等写像 id_V, 直積集合 $V \times V$, $\{f : V \to V \mid f$ は線形写像 $\}$, V の加法単位元 0_V.

問題 1.3.1.

(1) X の全順序部分集合 A の添え字集合を Λ とし, $T = \bigcup_{(S,f)\in A} S$ とする. $x \in T$ に対して, ある $\lambda \in \Lambda$ が存在して $x \in S_\lambda$ となるので, $g(x) = f_\lambda(x)$ と定めれば, これは A が全順序であることから well-defined であり, (T, g) は A の上界になる. したがって, Zorn の補題により, X は極大元をもつ.

(2) (a) が成立しないならば (b) が成立することを示せばよい. (a) が成立しない時には $x \in A \setminus S_0$ をとることができ, $B \setminus f(S_0) \neq \emptyset$ ならば, $y \in B \setminus f(S_0)$ として, F を $F(x) = y$ となるような f_0 の拡張とすれば, F は単射であり, これは $(S_0, f_0) \leq (S_0 \cup \{x\}, F)$ かつ $(S_0, f_0) \neq (S_0 \cup \{x\}, F)$ となるので, (S_0, f_0) が極大元であることに反する. したがって, (b) が成立する.

第 2 章　群の基本

問題 2.1.1.

1 が G の単位元であることに注意すれば, これに対する 0 の逆元が存在しないので, G は群ではない.

問題 2.1.2.

$0 \in \mathbb{R}$ が G の単位元であることに注意すれば, $a = -1$ のとき $-1 \circ b = -1$ となるので, -1 の逆元は存在しない. ゆえに, G は群ではない.

問題 2.1.3.

$\rho_1 = (1\ 2\ 3)$, $\rho_2 = (1\ 3\ 2)$, $\tau_1 = (1\ 2)$, $\tau_2 = (1\ 3)$, $\tau_3 = (2\ 3)$, e を単位元とする.

$\mathfrak{S}_3$	e	τ_1	τ_2	τ_3	ρ_1	ρ_2
e	e	τ_1	τ_2	τ_3	ρ_1	ρ_2
τ_1	τ_1	e	ρ_2	ρ_1	τ_2	τ_3
τ_2	τ_2	ρ_1	e	ρ_2	τ_3	τ_1
τ_3	τ_3	ρ_2	ρ_1	e	τ_1	τ_2
ρ_1	ρ_1	τ_3	τ_1	τ_2	ρ_2	e
ρ_2	ρ_2	τ_2	τ_3	τ_1	e	ρ_1

問題 2.1.4.

$((ab)c)d = (a(bc))d = a((bc)d)$.

問題 2.1.5.

$c = ((ba)^{-1}abdd^{-1})^{-1} = ((ba)^{-1}ab)^{-1} = (ab)^{-1}ba = b^{-1}a^{-1}ba$.

問題 2.1.6.

(1) $\sigma_1^{-1} = (2\ 3\ 4\ 1) = (1\ 2\ 3\ 4)$.

(2) $\sigma_2^{-1} = (1\ 3)(2\ 4)$.

(3) $\sigma_1\sigma_3 = (4\ 2\ 3\ 1) = (1\ 4)$.

(4) $\sigma_2^{-1}\sigma_4 = (2\ 4)$.

(5) $\sigma_3^{-1} = (4\ 2\ 3)$ より, $\sigma_3\sigma_1\sigma_3^{-1} = (1\ 2\ 4\ 3)$.

(6) $\sigma_2^{-1}\sigma_4\sigma_2 = (1\ 3)$.

問題 2.2.1.

(1) $\overline{2}$. (2) $\overline{4}$. (3) $\overline{6}$. (4) $\overline{6}$. (5) $\overline{4}^{32} = \overline{2}^{16} = \overline{1}^{5} \times \overline{2} = \overline{2}$.

問題 2.2.2.

(1) $\overline{34} \times \overline{21} \times \overline{33} = \overline{17} \times \overline{3} \times \overline{33} = \overline{12} \times \overline{33} = \overline{6}$.

(2) $\overline{25} \times \overline{18} \times \overline{13} = \overline{0}$.

(3) $\overline{16}^{8} = \overline{22}^{4} = \overline{16}^{2} = \overline{22}$.

(4) $\overline{16}^{34} = \overline{16}^{8}\overline{22} = \overline{484} = \overline{16}$.

問題 2.3.1.

『H が G の部分群 $\iff \forall x, y \in H \neq \emptyset$ に対して, $x^{-1}y \in H$』を示せばよい.

$\Longrightarrow$ H が部分群なので, $\forall x, y \in H$ について, $x^{-1} \in H$ より, $x^{-1}y \in H$.

$\Longleftarrow$ $H \neq \emptyset$ より, $x = y$ とすれば, $1_G \in H$ がいえ, $y = 1_G$ とすれば, $\forall x \in H$ について $x^{-1} \in H$ がわかる. これを使えば, $\forall x, y \in H$ について, $x^{-1} \in H$ より, $xy = (x^{-1})^{-1}y \in H$ となるので, 命題 2.3.2 より, H は部分群になる.

問題 2.3.2.

$1_{GL_{2n}(\mathbb{R})} \in H$ より, H は空でなく, $x, y \in H$ について,

$$ {}^t(x^{-1}y)J_n(x^{-1}y) = {}^ty({}^tx^{-1}J_nx^{-1})y = {}^ty({}^tx^{-1}({}^txJ_nx)x^{-1})y = {}^tyJ_ny = J_n $$

となるので, 演習問題 2.3.1 より H は部分群になる.

問題 2.3.3.

$1_{GL_n(\mathbb{C})} \in H$ より, H は空でなく, $x, y \in H$ について,

$$ {}^t\overline{(x^{-1}y)}(x^{-1}y) = {}^t\overline{y}{}^t\overline{x}^{-1}x^{-1}y = {}^t\overline{y}{}^t\overline{x}^{-1}({}^t\overline{x}x)x^{-1}y = I_n $$

となるので, 演習問題 2.3.1 より H は部分群になる.

問題 2.3.4.

(1) $1_G \in B$ で, $x \in B$ について, x の余因子行列を $\tilde{x}$ とする. これの (i, j) 小行列を $M_{i,j}$ とすれば, $(\tilde{x}_{i,j}) = (-1)^{i+j} \det M_{i,j}$ であり, $i < j$ のときには $\det M_{i,j} = 0$ なので, $x^{-1} = \frac{\tilde{x}}{\det x} \in B$ がわかる. また, $x, y \in B$ について, $xy \in B$ となるので, B は部分群である.

(2) $n = 1$ の場合には明らかに可換群なので, $n \geq 2$ の場合を考える. $E_{i,j}$ を (i, j) 成分のみが 1 で, それ以外の成分が 0 となるような行列として定めれば, $E_{1,1}, E_{n,1} \in B$ であり,

$$ E_{1,1}E_{n,1} = O \neq E_{n,1} = E_{n,1}E_{1,1} $$

となるので, B は可換群ではない.

問題 2.3.5.

$\mathbb{R}_>$ は空ではなく, $x, y \in \mathbb{R}_>$ について, $x^{-1}y = \frac{y}{x} \in \mathbb{R}_>$ となるので, 演習問題 2.3.1 より $\mathbb{R}_>$ は部分群になる.

問題 2.3.6.

$0_{\mathbb{R}} = 0 \notin \mathbb{R}_>$ より, $\mathbb{R}_>$ は部分群ではない.

問題 2.3.7.

$w = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$ とすれば, $w^n = 1$ である. また, 逆に $z^n = 1$ のとき, $z = \cos\theta + i\sin\theta$ とすれば, $\theta = \frac{2\pi}{n}k$ $(k \in \mathbb{Z})$ がわかるので, H の元は w^m という形で表すことができる. このとき, $1 \leq m < n$ ならば $w^m \neq 1$ であり, $1 \leq i, j < n$ について, $i \neq j$ ならば $w^i \neq w^j$ なので, H は w を生成元とする位数 n の巡回部分群である.

問題 2.3.8.

(1) $\mathfrak{S}_3$ は可換群ではないので, 巡回群ではない.

(2) $\mathbb{Q}$ のすべての元がゼロでないある $g \in \mathbb{Q}$ を用いて, ng の形で表すことができると仮定すると, $\frac{g}{2} \notin \mathbb{Q}$ となって矛盾する. また, $g = 0$ の場合にも, $\{0\} \neq \mathbb{Q}$ なので, $\mathbb{Q}$ は加法について巡回群ではない.

(3) $\mathbb{R}$ のすべての元がゼロでないある $g \in \mathbb{R}$ を用いて, ng の形で表すことができると仮定すると, $\frac{g}{2} \notin \mathbb{R}$ となって矛盾する. また, $g = 0$ の場合にも, $\{0\} \neq \mathbb{R}$ なので, $\mathbb{R}$ は加法について巡回群ではない.

(4) $g \in \mathbb{Q}^\times$ は $g = \frac{n}{m}$ $(m > 0)$ と既約分数で表すことができる. $p > \max\{|m|, |n|\}$ なる素数 p を取れば, $\frac{1}{p} \in \mathbb{Q}^\times$ であり, ある k を用いて $g^k = \frac{1}{p}$ と仮定すれば, $n^k p = m^k$ となるが, これは n, m が互いに素なことと p の選び方から矛盾が生じる. したがって, $\mathbb{Q}^\times$ は巡回群ではない.

(5) x, y 平面上において, (a, b) と原点を通る直線を考えると,

$$\{n(a,b) \mid n \in \mathbb{Z}\} \subset \begin{cases} (\mathbb{Z}_\geq \times \mathbb{Z}_\geq) \cup (\mathbb{Z}_\leq \times \mathbb{Z}_\leq) & ((a,b) \in (\mathbb{Z}_\geq \times \mathbb{Z}_\geq) \cup (\mathbb{Z}_\leq \times \mathbb{Z}_\leq)) \\ (\mathbb{Z}_\geq \times \mathbb{Z}_\leq) \cup (\mathbb{Z}_\leq \times \mathbb{Z}_\geq) & ((a,b) \in (\mathbb{Z}_\geq \times \mathbb{Z}_\leq) \cup (\mathbb{Z}_\leq \times \mathbb{Z}_\geq)) \end{cases}$$

なので, $\mathbb{Z} \times \mathbb{Z}$ は成分同士の加法について巡回群ではない.

問題 2.3.9.

(1) $S = \langle \sigma_1, \sigma_2, \cdots, \sigma_{n-1} \rangle$ とすれば, $(i\ i+2) = \sigma_i \sigma_{i+1} \sigma_i \in S$ であり, 同様にして互換はすべて S に属することがわかる. 次に, $(i_1\ i_2\ \cdots\ i_r) \in S$ を示す. $\sigma = (i_1\ i_r)$, $\tau = (i_1\ i_2\ \cdots\ i_{r-1})$ とすれば,

$$\sigma\tau(i_k) = \begin{cases} \sigma(i_{k+1}) = i_{k+1} & (1 \leq k \leq r-2) \\ \sigma(i_1) = i_r & (k = r-1) \\ \sigma(i_r) = i_1 & (k = r) \end{cases}$$

となるので, $\sigma\tau = (i_1\ i_2\ \cdots\ i_r)$. これを繰り返すことにより, $(i_1\ i_2\ \cdots\ i_r)$ は互換の積で表すことができる, つまり, S に属するということが分かるので, $\mathfrak{S}_n$ は $\sigma_1, \sigma_2, \cdots, \sigma_{n-1}$ で生成されることが示された.

(2) $1 \leq i < n$ について, $\sigma^{i-1}\tau\sigma^{-(i-1)} = (i\ i+1)$ となることを示す. k を n で割った余りを $\overline{k}$ とすれ

ば, n と $\overline{0}$ を同一視することにより,

$$\sigma^{i-1}\tau\sigma^{-(i-1)}(\overline{k}) = \sigma^{i-1}\tau(\overline{k-(i-1)}) = \begin{cases} \sigma^{i-1}(2) = \overline{i+1} & (\overline{k} = \overline{i}) \\ \sigma^{i-1}(1) = \overline{i} & (\overline{k} = \overline{i+1}) \\ \sigma^{i-1}(\overline{k-(i-1)}) = \overline{k} & (\overline{k} \neq \overline{i}, \overline{i+1}) \end{cases}$$

となるので, $\sigma^{i-1}\tau\sigma^{-(i-1)} = (i\ i+1) = \sigma_i$ であり, (1) より, $\mathfrak{S}_n$ は $\sigma_1, \sigma_2, \cdots, \sigma_{n-1}$ で生成されるので, $\mathfrak{S}_n$ は σ, τ で生成されることが示された.

問題 2.4.1.

(1) GCD(36, −48) = 12, LCM(36, −48) = |36||−48|/GCD(36, -48) = 144.

(2) 互いに素.

問題 2.4.2.

(1) ユークリッドの互除法を用いれば, $395 = 1 \cdot 265 + 130$, $265 = 2 \cdot 130 + 5$, $130 = 26 \cdot 5$ より, $d = 5$.

(2) $(x, y) = (-2, 3)$.

問題 2.4.3.

(1) $\overline{2}^{-1} = \overline{4}$, $\overline{3}^{-1} = \overline{5}$, $\overline{4}^{-1} = \overline{2}$, $\overline{5}^{-1} = \overline{3}$, $\overline{6}^{-1} = \overline{6}$.

(2) $284x + 3y = 1$ となるような (x, y) を求めればよい. ユークリッドの互除法を用いて, $284 = 94 \cdot 3 + 2$, $3 = 1 \cdot 2 + 1$ より, $(x, y) = (-1, 95)$ が解の一つなので, $\overline{3}^{-1} = \overline{95}$.

問題 2.4.4.

系 2.4.13 より, q が p^n と互いに素なことと, $qx + p^n y = 1$ となるような整数の組 (x, y) が存在することは同値である. このような (x, y) が存在するとき, $\overline{q}^{-1} = \overline{x}$ となるので, $q \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ がわかる. これより, p^n より小さい自然数で, p^n とは互いに素であるものの個数が $(p-1)p^{n-1}$ であることをいえればよく, p は素数なので, 互いに素でないものの個数は $\frac{p^n}{p} = p^{n-1} = p^n - (p-1)p^{n-1}$ とわかり, 主張が示された.

問題 2.4.5.

$(x^{35})^k = 1_G$ となるような k が求めるものである, つまり, $35k = 60m$ を満たす整数 m が存在する最小の自然数 k を求めればよい. これは両辺を 5 で割れば, $k = 12$ であることがわかる.

問題 2.4.6.

$nk = dm$ を満たす整数 m が存在するような最小の自然数 k を求めれば十分であり, これは $k = d/\mathrm{GCD}(n, d) = \mathrm{LCM}(n, d)$ とすればよい.

問題 2.4.7.

命題 2.4.19 より位数 n の元が生成する群の位数は n であり, $\mathbb{Z}/d\mathbb{Z}$ について, 元の位数が d となるには演習問題 2.4.6 から d と互いに素であることが必要十分である. したがって, 以下のようになる.

(1) $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$.

(2) $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$, $\overline{6}$.

(3) $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$.
(4) $\overline{1}$, $\overline{2}$, $\overline{4}$, $\overline{5}$, $\overline{7}$, $\overline{8}$.
(5) $\overline{1}$, $\overline{2}$, $\overline{4}$, $\overline{7}$, $\overline{8}$, $\overline{11}$, $\overline{13}$, $\overline{14}$.

問題 2.4.8.
$g \in G$ に対し $g^{-1} = g$ より, $a, b \in G$ について, $(ab)(ba)^{-1} = (ab)(ba) = abba = aa = 1_G$

問題 2.4.9.
(1)
$$g^4 = g^2 g^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = 1_G$$
と命題 2.4.18 より, g の位数は 4 となる.
$$h^6 = h^3 h^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = 1_G$$
であって, これより $h^3 \neq h$ なので $h^2 \neq I_2$ がわかる. これらと命題 2.4.18 より, h の位数は 6 となる.
(2)
$$gh = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$
であり,
$$\begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ n+1 & 1 \end{pmatrix}$$
なので,
$$(gh)^n = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \neq 1_G$$
となって, gh の位数は無限である.

問題 2.4.10.
(1) a, b の位数をそれぞれ n, m とすれば可換性より, $(ab)^{nm} = 1_G$ なので, ab の位数は有限.
(2) $1_g \in H$ であり, a と a^{-1} の位数は一致するので, これらと (1) より H は部分群である.

問題 2.5.1.
(1) $x^{m+k} = x^k$ のとき, $y^{m+k} = y^k$ となるので, m は n の倍数であることがわかる. 逆に, m が n の倍数ならば, この性質は成立する. したがって, 求めるべき必要十分条件は m が n の倍数であることとなる.
(2) $\phi(x) = y$ で定めれば, $\phi(x^i) = \phi(x) \cdots \phi(x) = y^i$ が成立し, G, H はそれぞれ x, y で生成されるので, (1) よりこれは well-defined な準同型になる.

問題 2.5.2.
G の可換性より, $g, h \in G$ について, $\phi_n(gh) = (gh)^n = g^n h^n = \phi_n(g)\phi_n(h)$ なので, これは準同型.

問題 2.5.3.

(1) ϕ が準同型なので, g の位数を n とすれば, $\phi(g)^n = \phi(g^n) = \phi(1_G) = 1_H$ となり, これより, $\phi(g)$ の位数は n の約数であることが分かる.

(2) $\phi(g)$ の位数を m とする. このとき, $\phi(g^m) = \phi(g)^m = 1_H$ となるが, ϕ が準同型なことより $\phi(1_G) = 1_H$ であり, 仮定よりこれが単射なので, $g^m = 1_G$ になる. 今, これより n は m の約数であることがわかり, これと (1) より, $n = m$ がいえる.

問題 2.5.4.

同型 $\phi : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ が存在すると仮定する. $\mathbb{Z}/4\mathbb{Z}$ の元 $\overline{0}, \overline{1}, \overline{2}, \overline{3}$ の位数はそれぞれ $1, 4, 2, 4$ であり, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ には位数が 4 の元は存在しない. しかし, これは演習問題 2.5.3(2) に反する. したがって, $\mathbb{Z}/4\mathbb{Z}$ と $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ は同型ではない.

問題 2.5.5.

$(xyx^{-1})^n = (xyx^{-1}) \cdots (xyx^{-1}) = xy^n x^{-1}$.

問題 2.5.6.

(1)

$$G = \begin{pmatrix} g_{1,1} & g_{1,2} \\ g_{2,1} & g_{2,2} \end{pmatrix}$$

として, $GA = BG$ を解けば, $g_{1,1} = 0$, $g_{1,2} = g_{2,1}$ がわかる. 逆にこのとき, $GA = BG$ が成立する. 例えば, $g_{1,2} = g_{2,1} = g_{2,2} = 1$ とすれば,

$$G = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$$

なので, A と B は $GL_2(\mathbb{R})$ において, 共役であることがわかる.

(2) (1) の条件を満たす G について, $\det G = -g_{1,2}^2 \neq 1$ より, A と B は $\mathrm{SL}_2(\mathbb{R})$ において共役ではない.

(3) (1) の条件を満たす G について, $\det G = -g_{1,2}^2$ より, $g_{1,2} = i$ とすれば, $G \in \mathrm{SL}_n(\mathbb{C})$ となるので, A と B は $SL_n(\mathbb{C})$ においては共役である.

問題 2.5.7.

G を位数 n の有限巡回群とすれば, $\mathrm{Aut}G \cong (\mathbb{Z}/n\mathbb{Z})^\times$ であることを示す. G から G への恒等写像は自己同型なので, $\mathrm{Aut}G \neq \emptyset$ であり, また, G の生成元を g とし, 以下のように ψ を定める

$$\psi : (\mathbb{Z}/n\mathbb{Z})^\times \ni \overline{m} \mapsto \phi_m \in \mathrm{Aut}G \quad (\phi_m(g) = g^m)$$

このとき, g の位数は n なので, ψ は well-defined であり, $x, y \in (\mathbb{Z}/n\mathbb{Z})^\times$ について, $\psi(x) = \psi(y)$ とすれば, 特に生成元 g について $\psi(x)(g) = \psi(y)(g)$ となるので, $x = y$. ゆえに, ψ は単射である. また, $\phi \in \mathrm{Aut}G$ について, $\phi(g) = g^k$ $(0 \leq k < n)$ と表すことができ, このとき, $\phi = \phi_k$ となる. ここで, 演習問題 2.5.3(2) より, $\phi(g)$ の位数は n なので, k は n と互いに素であることがわかり, 系 2.4.14 より, $|\mathrm{Aut}G| = |(\mathbb{Z}/n\mathbb{Z})^\times|$ がいえる. これらはともに有限なので, ψ は全射である. 次に, $x, y \in (\mathbb{Z}/n\mathbb{Z})^\times$ について,

$$\psi(xy)(g) = \phi_{xy}(g) = g^{xy} = \phi_x(\phi_y(g)) = (\phi_x \circ \phi_y)(g) = (\psi(x) \circ \psi(y))(g)$$

より, ψ が準同型であることもわかる. 以上より, $\mathrm{Aut}G \cong (\mathbb{Z}/n\mathbb{Z})^\times$ が示された.

(1) $\mathbb{Z}/5\mathbb{Z}$ は $\overline{1}$ を生成元とする巡回群なので, 上に述べたことにより, $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z}) \cong (\mathbb{Z}/5\mathbb{Z})^\times$. 次に, $\mathbb{Z}/4\mathbb{Z} \cong (\mathbb{Z}/5\mathbb{Z})^\times$ を示す. 例 2.4.15(1) より, $(\mathbb{Z}/5\mathbb{Z})^\times$ は位数 4 の群であり, $\overline{2} \in (\mathbb{Z}/5\mathbb{Z})^\times$ は位数 4 の元なので, $(\mathbb{Z}/5\mathbb{Z})^\times$ は位数 4 の巡回群になる. これと例 2.10.6 より, $\mathbb{Z}/4\mathbb{Z} \cong (\mathbb{Z}/5\mathbb{Z})^\times$ がわかる. したがって, $\mathrm{Aut}(\mathbb{Z}/5\mathbb{Z}) \cong \mathbb{Z}/4\mathbb{Z}$ が示された.

(2) (1) と同様に $\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) \cong (\mathbb{Z}/7\mathbb{Z})^\times$ であり, 例 2.4.15(1) より, これは位数 6 の群で, $\overline{5} \in (\mathbb{Z}/7\mathbb{Z})^\times$ は位数 6 の元なので, $(\mathbb{Z}/7\mathbb{Z})^\times$ は位数 6 の巡回群になる. これと例 2.10.6 より, $(\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$ がわかる. したがって, $\mathrm{Aut}(\mathbb{Z}/7\mathbb{Z}) \cong \mathbb{Z}/6\mathbb{Z}$ が示された.

(3) (1) と同様に $\mathrm{Aut}(\mathbb{Z}/8\mathbb{Z}) \cong (\mathbb{Z}/8\mathbb{Z})^\times$ である. 次に $(\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ を示す. $\overline{-1}, \overline{5} \in (\mathbb{Z}/8\mathbb{Z})^\times$ が生成する部分群 $\langle\overline{-1}\rangle$, $\langle\overline{5}\rangle$ について, $(\mathbb{Z}/8\mathbb{Z})^\times$ は可換なので, これらは正規部分群となる. また, 4 を法として考えれば, $\langle\overline{-1}\rangle \cap \langle\overline{5}\rangle = \{1_{(\mathbb{Z}/8\mathbb{Z})^\times}\}$ がわかる. $\overline{-1}$, $\overline{5}$ の位数はそれぞれ 2 であって, 命題 2.9.2 と演習問題 2.4.7(3) より, $|\langle\overline{-1}\rangle\langle\overline{5}\rangle| = 4 = |(\mathbb{Z}/8\mathbb{Z})^\times|$ となるので, 有限性から $\langle\overline{-1}\rangle\langle\overline{5}\rangle = (\mathbb{Z}/8\mathbb{Z})^\times$ がいえる. ここで, 命題 2.9.2 を使えば, $(\mathbb{Z}/8\mathbb{Z})^\times \cong \langle\overline{-1}\rangle \times \langle\overline{5}\rangle$ となるが, $\langle\overline{-1}\rangle$, $\langle\overline{5}\rangle$ は位数が 2 の巡回群であることと, 例 2.10.6 より, $\langle\overline{-1}\rangle \cong \langle\overline{5}\rangle \cong \mathbb{Z}/2\mathbb{Z}$ なので, $(\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ となる. したがって, $\mathrm{Aut}(\mathbb{Z}/8\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ が示された.

(4) (1) と同様に $\mathrm{Aut}(\mathbb{Z}/9\mathbb{Z}) \cong (\mathbb{Z}/9\mathbb{Z})^\times$ であり, $(\mathbb{Z}/9\mathbb{Z})^\times$ には位数 $3, 2$ の元がそれぞれ存在する $(\overline{4}, \overline{8})$ ので, 可換性から $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ は $(\mathbb{Z}/9\mathbb{Z})^\times$ の正規部分群である. ここで, 元の位数を比較すれば, $\mathbb{Z}/3\mathbb{Z} \cap \mathbb{Z}/2\mathbb{Z} = \{1_{(\mathbb{Z}/9\mathbb{Z})^\times}\}$ であって, 命題 2.10.3 と演習問題 2.4.4 より, $|(\mathbb{Z}/3\mathbb{Z})(\mathbb{Z}/2\mathbb{Z})| = |(\mathbb{Z}/9\mathbb{Z})^\times|$ となる. ゆえに, 有限性から, $(\mathbb{Z}/3\mathbb{Z})(\mathbb{Z}/2\mathbb{Z}) = (\mathbb{Z}/9\mathbb{Z})^\times$ がいえる. これらと, 命題 2.9.2 より, $(\mathbb{Z}/9\mathbb{Z})^\times \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ となるので, $\mathrm{Aut}(\mathbb{Z}/9\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ が示された.

(5) (1) と同様に $\mathrm{Aut}(\mathbb{Z}/15\mathbb{Z}) \cong (\mathbb{Z}/15\mathbb{Z})^\times$ であり, 定理 2.9.3(中国式剰余定理) から $\mathbb{Z}/15\mathbb{Z} \cong (\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z})^\times \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ なので, 単元の準同型写像による像が単元であることを考えれば, $(\mathbb{Z}/15\mathbb{Z})^\times \cong (\mathbb{Z}/5\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times$ がいえる. (1) より, $(\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z}$ であり, 同様にして $(\mathbb{Z}/3\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}$ がわかるので, これらより, $(\mathbb{Z}/15\mathbb{Z})^\times \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ となる. したがって, $\mathrm{Aut}(\mathbb{Z}/15\mathbb{Z}) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ が示された.

問題 2.5.8.

(1) $g = b \in G$ とすれば, $gab = bag$ なので ab, ba は G で共役.

(2) ab の位数が有限な場合　ab の位数を n とすれば, $(ba)^{n+1} = b(ab)\cdots(ab)a = ba$ であり, 両辺に ba の逆元をかければ, $(ba)^n = 1_G$ がわかる. これより, ba の位数は有限であり, それを m とすれば, n は m の倍数である. 同様に m が n の倍数であることもわかるので, $n = m$ が示される.

ab の位数が無限な場合　ba が有限の位数をもつと仮定すれば, 上記より ab も有限の位数をもつことになって矛盾. したがって, ba の位数も無限である.

問題 2.5.9.

ϕ が全単射であることを示せばよい. $x \in G$ に対し, $\phi(x) = id_G$ ならば, 任意の $g \in G$ について, $xgx^{-1} = g$ となる. これは x と任意の g が可換であることを示しているが, 演習問題 2.1.3 より, $x = 1_G$ となることがわかる. ゆえに, 命題 2.5.13 より, ϕ は単射である. $\sigma = (1\ 2\ 3)$, $\tau = (1\ 2)$ とすれば, 例 2.3.20 より, $\langle\sigma, \tau\rangle = G$ となるので, $\mathrm{Aut}G$ の元を区別するには σ と τ の像をみればよいが, 演習問題 2.5.3(2) と G の各元の位数を考えれば, σ, τ の像として取り得るのはそれぞれ 3 通りと 2 通りあるので, $|G| = 6 \geq |\mathrm{Aut}G|$ がわかる. これより ϕ は全単射であることが示された.

問題 2.6.1.

R により定まる二項関係を $\sim$ とすれば, $(1,2),(2,4) \in R$ なので, $1 \sim 2$ かつ $2 \sim 4$. しかし, $(1,4) \notin R$ なので, これは推移律を満たさず, 同値関係にはならない.

問題 2.6.2.

$a,b,c \in G$ について, $1_G a = a1_G$ より, $a \sim a$ であり, $a \sim b$ ならば, ある $g \in G$ が存在して $ga = bg$ となるが, このとき $g^{-1}b = ag^{-1}$ なので, $b \sim a$. また, $a \sim b$ かつ $b \sim c$ ならば, ある $g,h \in G$ を用いて $ga = bg$ かつ $hb = ch$ と表すことができるが, このとき $(hg)a = c(hg)$ なので, $a \sim c$ となる. したがって, $\sim$ は G 上の同値関係である.

問題 2.6.3.

位数 5 の群の部分群として位数 3 の群が存在するならば, 系 2.6.21(1) より 3 は 5 の約数となるが, これは明らかに不合理なので, そのような部分群は存在しない.

問題 2.6.4.

命題 2.3.3 より, $H \cap K$ は群になるので, $H \cap K$ は H, K それぞれの部分群である. ここで, 系 2.6.21(1) より, $|H \cap K|$ は $|H|$ と $|K|$ の約数であるが, $|H|$, $|K|$ は互いに素なので, $|H \cap K| = 1$. したがって, $|H \cap K| = \{1_G\}$ がわかる.

問題 2.7.1.

$\sigma \in G$ について, $\sigma \notin H = H1_G H$ のとき, $\sigma(4) \neq 4$ であり, $\sigma(4) = 1$ の場合には $(1\ 1)\sigma(4) = \sigma(4)$ と定めることにより, $(1\ 4)(1\ \sigma(4))\sigma(4) = 4$ となるので, $(1\ 4)(1\ \sigma(4))\sigma \in H$ となることがわかる. このとき, $\sigma \in H(1\ 4)H$ なので, 完全代表系として $\{1_G, (1\ 4)\}$ がとれる.

問題 2.7.2.

(1) $i_n < i$ について, $\alpha_i = -g_{i,n}/g_{i_n,n}$ とし, b_1 を対角成分が 1 で, (i, i_n) 成分が a_i であるような行列, つまり, 以下のようなものとする.

$$b_1 = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & \alpha_{i_n+1} & \ddots & & \\ & & \vdots & & \ddots & \\ & & \alpha_n & & & 1 \end{pmatrix}$$

このとき, b_1 は正則な下三角行列であり,

$$(b_1 g)_{i,n} = \begin{cases} 0 & (i \neq i_n) \\ g_{i_n,n} & (i = i_n) \end{cases}$$

が満たされる. 次に, $0 \leq j < n$ について, $\beta_j = -(b_1 g)_{i_n,j}/(b_1 g)_{i_n,n}$ とし, b_2 を対角成分が 1 で, (n, j)

成分が β_j となるような行列, つまり, 以下のようなものとする.

$$b_2 = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & \ddots & & & \\ & & & \ddots & & \\ & & & & \ddots & \\ \beta_1 & \cdots & \cdots & \cdots & \beta_{n-1} & 1 \end{pmatrix}$$

このとき, b_2 は正則な下三角行列であり,

$$(b_1 g b_2)_{i,n} = \begin{cases} 0 & (i \neq i_n) \\ g_{i_n,n} & (i = i_n) \end{cases}, \qquad (b_1 g b_2)_{i_n,j} = \begin{cases} 0 & (j \neq n) \\ g_{i_n,n} & (j = n) \end{cases}$$

が満たされる. したがって, 条件を満たすような正則な下三角行列 b_1, b_2 は存在する.

(2) $g_n = g$ とし, $g_{k-1} = b_{1,k} g_k b_{2,k}$ と定める. また, $(g_k)_{i,k} \neq 0$ となるような最小の i を i_k とする. $g_k \in GL_n(\mathbb{R})$ なので, このような i_k $(1 \leq k \leq n)$ は存在する. ここで,

$$\alpha_{k,l} = -(g_k)_{l,k}/(g_k)_{i_k,k}, \qquad \beta_{k,l} = -(b_{1,k} g_k)_{i_k,l}$$

$$b_{1,k} = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & \frac{1}{(g_k)_{i_k,k}} & & & \\ & & \alpha_{k,i_k+1} & \ddots & & \\ & & \vdots & & \ddots & \\ & & \alpha_{k,n} & & & 1 \end{pmatrix}, \quad b_{2,k} = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & \ddots & & & \\ \beta_{k,1} & \cdots & \beta_{k,k-1} & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{pmatrix}$$

と定めれば, g_0 は置換行列になる. 正則な下三角行列の積は正則な下三角行列になるので,

$$b_1 = b_{1,1} \cdots b_{1,n}, \qquad b_2 = b_{2,1} \cdots b_{2,n}$$

とすることにより, $b_1 g b_2$ は置換行列になる.

(3) $\sigma(n) = k$ のとき,

$$(P_\sigma)_{n,j} = \begin{cases} 0 & (j \neq k) \\ 1 & (j = k) \end{cases}, \qquad (P_\sigma)_{i,k} = \begin{cases} 0 & (i \neq n) \\ 1 & (i = n) \end{cases}$$

となる. このとき

$$(P_\tau)_{n,k} = (b_1 P_\sigma b_2)_{n,k} = \sum_{l=1}^{n} (b_1)_{n,l} (P_\sigma b_2)_{l,k} = (b_1)_{n,n} (P_\tau b_2)_{n,k} = (b_1)_{n,n}$$

であって, b_1 が正則な下三角行列であることから $(b_1)_{n,n} \neq 0$ となるので, P_τ が置換行列であることから $(P_\tau)_{n,k} = 1$. したがって, $\tau(n) = k = \sigma(n)$ である.

(4) $b_1 P_\sigma b_2 = P_\tau$ と b_2 が下三角行列であることから,

$$\begin{aligned}(b_1)_{i,\sigma(n)} &= \sum_{l=1}^{n}\sum_{k=1}^{n}(P_\tau)_{i,k}(b_2^{-1})_{k,l}(P_\sigma^{-1})_{l,\sigma(n)} \\ &= \sum_{l=1}^{n}\sum_{k\geq l}^{n}(P_\tau)_{i,k}(b_2^{-1})_{k,l}(P_\sigma^{-1})_{l,\sigma(n)}\end{aligned}$$

が成り立つ. また, P_σ, P_τ は置換行列なので,

$$(b_1)_{i,\sigma(n)} = (b_2^{-1})_{\tau^{-1}(i),n}$$

となる. ここで, $(b_2^{-1})_{\tau^{-1}(i),n} \neq 0$ とすれば, $\tau^{-1}(i) \geq n$ が成り立つ. これより, $\tau(n) = i$ であり, (3) より $i = \sigma(n)$ が従う.

行列の成分を計算することにより,

$$(P_\nu b_1 P_{\nu^{-1}})_{i,j} = (P_\nu)_{i,\nu^{-1}(i)}(b_1)_{\nu^{-1}(i),\nu^{-1}(j)}(P_{\nu^{-1}})_{\nu^{-1}(j),j}$$

が従う. 以下, $i < j$ の場合に $(b_1)_{\nu^{-1}(i),\nu^{-1}(j)} = 0$ であることを示す.

$\underline{i < \sigma(n) \text{ のとき}}$ $\nu^{-1}(i) = i$ であり, $j \geq \sigma(n)$ ならば $\nu^{-1}(j) \geq \sigma(n)$ であり, $j < \sigma(n)$ ならば $\nu^{-1}(j) = j$ となるので, それぞれの場合について $\nu^{-1}(i) < \nu^{-1}(j)$ が成り立つ. b_1 は下三角行列なので, これより, $(b_1)_{\nu^{-1}(i),\nu^{-1}(j)} = 0$ となる.

$\underline{\sigma(n) \leq i \text{ のとき}}$ $i < j$ より, $i \neq n$ であり, このとき ν の定義から $\nu^{-1}(i) < \nu^{-1}(j)$ が成り立つので, $(b_1)_{\nu^{-1}(i),\nu^{-1}(j)} = 0$ となる.

以上より, $P_\nu b_1 P_{\nu^{-1}} \in b$ である.

(5) $P_\nu b_1 {P_\nu}^{-1} = b_3$ とおくと, (4) より $b_3 \in B$ であり, $b_3 P_{\nu\sigma} b_2 = P_{\nu\tau}$ となる. b_2, b_3 を以下のようにおく.

$$b_2 = \left(\begin{array}{c|c} \alpha_2 & \mathbf{0} \\ \hline \gamma_2 & \delta_2 \end{array}\right), \qquad b_3 = \left(\begin{array}{c|c} \alpha_3 & \mathbf{0} \\ \hline \gamma_3 & \delta_3 \end{array}\right).$$

ここで, α_2, α_3 は $n-1$ 次の正則な下三角行列である. また,

$$P_\sigma = \left(\begin{array}{c|c} A_\sigma & \mathbf{0} \\ \hline {}^t\mathbf{0} & 1 \\ \hline B_\sigma & \mathbf{0} \end{array}\right)$$

とおくと,

$$P_{\nu\sigma} = \left(\begin{array}{c|c} A_\sigma & \mathbf{0} \\ \hline B_\sigma & \mathbf{0} \\ \hline {}^t\mathbf{0} & 1 \end{array}\right)$$

となるので, $\nu\sigma$ の $\{1, \ldots, n-1\}$ への制限を σ' とすると,

$$P_{\nu\sigma} = \left(\begin{array}{c|c} P_{\sigma'} & \mathbf{0} \\ \hline {}^t\mathbf{0} & 1 \end{array}\right).$$

同様に $\nu\tau$ の $\{1, \ldots, n-1\}$ への制限を τ' とし, (3) より $\sigma(n) = \tau(n)$ が成り立つことに注意すれば,

$$P_{\nu\tau} = \left(\begin{array}{c|c} P_{\tau'} & \mathbf{0} \\ \hline {}^t\mathbf{0} & 1 \end{array}\right)$$

となる．ゆえに, $b_3P_{\nu\sigma}b_2 = P_{\nu\tau}$ より,

$$\left(\begin{array}{c|c} \alpha_3P_{\sigma'}\alpha_2 & \mathbf{0} \\ \hline \gamma_3P_{\sigma'}\alpha_2 + \delta_3\gamma_2 & \delta_3\delta_2 \end{array}\right) = \left(\begin{array}{c|c} P_{\tau'} & \mathbf{0} \\ \hline {}^t\mathbf{0} & 1 \end{array}\right).$$

であるから, $\alpha_3P_{\sigma'}\alpha_2 = P_{\tau'}$ が成り立つ．このとき, (3) と同様にして $\sigma'(n-1) = \tau'(n-1)$ となり, $\sigma(n-1) = \tau(n-1)$ が従う．以上を繰り返せば, $\sigma(n) = \tau(n), \sigma(n-1) = \tau(n-1), \ldots, \sigma(1) = \tau(1)$ となり，$\sigma = \tau$ が示された．

問題 2.8.1.

(1) $(1\ 2\ 3) \in \mathfrak{S}_3$ と $(1\ 4) \in \mathfrak{S}_4$ について, それぞれを σ, τ で表すことにすれば,

$$\tau\sigma\tau^{-1}(4) = \tau\sigma\tau(4) = 2$$

となるので, $\tau\sigma\tau^{-1} \notin \mathfrak{S}_3$．したがって, $\mathfrak{S}_3$ は $\mathfrak{S}_4$ の正規部分群ではない．

(2)
$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \in \mathrm{SO}(2), \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$$

について,

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

となるので, $\theta = \pi/2$ などとすれば, $\mathrm{SO}(2)$ は $\mathrm{GL}_2(\mathbb{R})$ の正規部分群ではないことがわかる．

(3)
$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \qquad \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$$

について,

$$\begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -i & 0 \end{pmatrix} = \begin{pmatrix} \cos\theta & i\sin\theta \\ -i\sin\theta & \cos\theta \end{pmatrix}$$

となるので, $\theta = \pi/2$ などとすれば, $\mathrm{GL}_2(\mathbb{R})$ は $\mathrm{GL}_2(\mathbb{C})$ の正規部分群ではないことがわかる．

(4) 演習問題 2.3.9 に注意すれば, $\mathfrak{S}_4$ の任意の元は互換の積として表すことができる．また, 互いに素な互換の積は可換であり, 互いに素ではない互換の積は一つの互換として表すことができるので, $g \in \mathfrak{S}_4, h \in H$ について, ghg^{-1} は互いに素な互換の積, または単位元になるよう整理することができる．したがって, H は $\mathfrak{S}_4$ の正規部分群である．

(5)
$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \in G \qquad \begin{pmatrix} x & 0 \\ y & x \end{pmatrix} \in H$$

とすれば, 正則性から $a, c \neq 0$ であり,

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}\begin{pmatrix} x & 0 \\ y & x \end{pmatrix}\begin{pmatrix} \frac{1}{a} & 0 \\ -\frac{b}{ac} & \frac{1}{c} \end{pmatrix} = \begin{pmatrix} x & 0 \\ \frac{c}{a}y & x \end{pmatrix} \in G$$

となるので, H は G の正規部分群.

問題 2.8.2.

$a \in H$ ならば, $aH = H = Ha$ であり, 仮定より $|G/H| = |H\backslash G| = 2$ なので, $a \in G - H$ のときも $aH = Ha$ が満たされる．したがって, H は正規部分群である．

問題 2.8.3.

N_1N_2 の元は $n_1 \in N_1, n_2 \in N_2$ を用いて n_1n_2 と表すことができ, 仮定より $g \in G$ について, $gn_1n_2g^{-1} = gn_1g^{-1}gn_2g^{-1} \in N_1N_2$ となるので, N_1N_2 は正規部分群である.

問題 2.8.4.

$G = \mathfrak{S}_3$ とすれば, $|G| = 6$ なので, 部分群の位数としてありうるのは $1, 2, 3, 6$ のいずれか. また, 位数が $1, 6$ の場合はそれぞれ $1_G, G$ とわかるので位数 $2, 3$ のものについて考えればよい. 位数 2 のものは単位元以外の元について, それ自身が逆元である必要があるので, 単位元と互換一つからなる部分群であることがわかる. 位数 3 のものは単位元以外の二つの元がそれ自身を逆元としてもつか, 互いに逆元になる. 前者の場合では単位元と互換二つの集合が考えられるが, 相異なる互換の積はかけあわせた二つの互換には一致しないので, この場合の部分群は存在しない. また, 後者の場合では位数が 3 であることから巡回群であり, すべての単位元以外の元の位数は 3 であることが必要になる. これを満たすのは $(1\ 2\ 3), (1\ 3\ 2)$ のみであり, これらはたがいに逆元なので, 位数 3 の部分群は $\{1_G, (1\ 2\ 3), (1\ 3\ 2)\}$ となる. 位数 $1, 6$ の部分群は明らかに正規部分群であり, 位数 3 の部分群は命題 2.6.20 と演習問題 2.8.2 より正規部分群であることがわかる. 位数 2 の部分群は $1_G, (a\ b)$ $(a \neq b)$ という形をしたものだが, $(a\ c)(a\ b)(a\ c) = (b\ c)$ となるので, これは正規部分群ではない.

問題 2.8.5.

四元数群の位数は 8 なので, 位数が $1, 2, 4, 8$ の部分群が存在するかを確認すれば十分である. 演習問題 2.8.4 と同様に位数 $1, 8$ については自明なので, それ以外について考える. 四元数群の元で, 元の位数が 2 であるものは p32 の乗法表から -1 のみであることがわかるので, 位数 2 の部分群は $\{\pm 1\}$ のみである. 位数 4 のものについて, これが巡回群として存在するならば位数 4 の元が生成元となるが, 乗法表から ± 1 以外の元はすべて位数が 4 であることがわかるので, 四元数群の元 $g \neq \pm 1$ を用いて, $\langle g \rangle$ と表すことができる. 次に, これが巡回群でないならば, 位数 2 の元が二つ存在することが必要だが, 四元数群の元で位数が 2 のものは -1 のみなので, このようなものは存在しない. また, 位数 $1, 8$ の部分群は明らかに正規であり, 位数 4 の部分群も命題 2.6.20 と演習問題 2.8.2 より正規部分群である. 位数 2 の部分群についても, ± 1 は任意の元と可換なので, 正規である.

問題 2.9.1.

(1) 定理 2.9.3 より $\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.
(2) 定理 2.9.3 より $\mathbb{Z}/28\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.
(3) 定理 2.9.3 より $\mathbb{Z}/60\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.
(4) 定理 2.9.3 より $\mathbb{Z}/1400\mathbb{Z} \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/25\mathbb{Z}$.

問題 2.9.2.

準同型の制限と射影はともに準同型であり, 準同型の合成は準同型なので ϕ_1, ϕ_2 は存在する.[*1]

問題 2.9.3.

[*1] $\phi_1(g_1)\phi_2(g_2)$ は $(\phi_1(g_1), \phi_2(g_2))$ の意味である. 定義 2.3.22 参照.

(1) $8a+15b=1$ となるような (a,b) をユークリッドの互除法を使って求めれば, $(a,b)=(2,-1)$ などが条件を満たす. 系 2.9.4 より,

(2) $35a+24b=1$ となるような (a,b) をユークリッドの互除法を使って求めれば, $(a,b)=(11,-16)$ などが条件を満たす. 系 2.9.4 より, $35\cdot 11\cdot 5+24\cdot(-16)\cdot 4=389$ が条件を満たすことがわかる.

問題 2.10.1.

$\phi_1 : G \ni g \mapsto |g| \in H_2$ は全射な準同型であり, 明らかに $\mathrm{Ker}(\phi_1)=H_1$ となるので, 定理 2.10.1 から $G/H_1 \cong H_2$ となる.

$\phi_2 : G \ni g \mapsto g/|g| \in H_1$ とすれば, ϕ_2 は全射準同型であり, $\mathrm{Ker}(\phi_2)=H_2$ となるので, これと定理 2.10.1 より $G/H_2 \cong H_1$ となる.

問題 2.10.2.

$\phi : \mathbb{R} \ni x \mapsto ax+a\mathbb{Z} \in \mathbb{R}/a\mathbb{Z}$ とすれば, これは全射な準同型である. ここで, $\mathrm{Ker}(\phi)=\mathbb{Z}$ なので, 準同型定理を適用すれば, $\mathbb{R}/\mathbb{Z} \cong \mathbb{R}/a\mathbb{Z}$ が示される.

問題 2.10.3.

$$\phi : G \ni \begin{pmatrix} x & 0 \\ y & z \end{pmatrix} \longmapsto \frac{x}{z} \in \mathbb{R}^\times$$

と定めれば, ϕ は全射な準同型になる. また, $\mathrm{Ker}(\phi)=H$ なので, 準同型定理より $G/H \cong \mathbb{R}^\times$ が従う.

問題 2.10.4.

G は可換群なので, H は正規部分群である. 仮定より $|G/H|=n$ であり, G/H の元は $g\in G$ を使って $g+H$ と表せる. 系 2.6.21 より, $ng+H=n(g+H)=H$ となるので, $ng\in H$ であることがわかる.

問題 2.10.5.

一般に指数が素数 p の場合について解く. 指数 p の部分群を H とすれば, 演習問題 2.10.4 より $pG\subset H$ となり, 定理 2.10.2 より G の pG を含む部分群は G/pG の部分群と一対一に対応する. この対応は $H \leftrightarrow H/pG$ である. ここで, $|G/H|=p$, $|G/pG|=p^2$ であり, 定理 2.10.4 に注意すれば, $|G/H|=|(G/pG)/(H/pG)|$ なので, G の pG を含む指数 p の部分群は G/pG の指数 p の部分群と一対一に対応する. また, $G/pG \cong \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ となるので, $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ の指数 p の部分群 H' の数を求めればよい. 定理 2.6.20 より $|H'|=p$ であり, $x,y\in\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ について,

$$\langle x\rangle=\langle y\rangle \Longleftrightarrow \exists n\in\mathbb{N} \text{ s.t. } nx=y$$

となるが, x は $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ の元なので,

$$\langle x\rangle=\langle y\rangle \Longleftrightarrow 1\le \exists n\le p-1 \text{ s.t. } nx=y$$

が成り立つ. これと, $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ の単位元以外の元の位数が p であることから, $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ の位数 p の部分群の個数は $(p^2-1)/(p-1)=p+1$ である. したがって, G の指数 p の部分群の個数は $p+1$ となる. 以上より, (1) 3, (2) 14.

問題 2.10.6.

例題 2.10.12 と同様に $G/2G$ の指数 2 の部分群の個数を求めればよいが, 定理 2.9.3 より

$$G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$$

であるので, 剰余群の直積と直積の剰余群は等しいことから

$$\begin{aligned} G/2G \cong (\mathbb{Z}/2\mathbb{Z})/2(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})/2(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})/2(\mathbb{Z}/5\mathbb{Z}) \\ \times (\mathbb{Z}/7\mathbb{Z})/2(\mathbb{Z}/7\mathbb{Z}) \times (\mathbb{Z}/8\mathbb{Z})/2(\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/9\mathbb{Z})/2(\mathbb{Z}/9\mathbb{Z}). \end{aligned}$$

また, $2(\mathbb{Z}/(2n+1)\mathbb{Z}) = \mathbb{Z}/(2n+1)\mathbb{Z}$ より, $G/2G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ となる. ここからは例題 2.10.12 の後半と全く同様なので, 求める部分群の個数は 3 である.

問題 2.10.7.

(1) 巡回群の部分群は巡回群であり, $\mathbb{Z}/12\mathbb{Z}$ の部分群の位数としては $1, 2, 3, 4, 6, 12$ がありえ, 位数 k の生成元として $\overline{12/k}$ がとれるので, 部分群は $n\mathbb{Z}/12\mathbb{Z}$ $(n = 1, 2, 3, 4, 6, 12)$ となる.

(2) (1) と同様に $n\mathbb{Z}/18\mathbb{Z}$ $(n = 1, 2, 3, 6, 9, 18)$ が部分群になる.

問題 2.10.8.

(1) 位数 3 の元が存在しないと仮定する. このとき, 系 2.6.21 より, G の単位元以外の元の位数としては $2, 6$ のみが考えられるが, $g \in G$ の位数が 6 ならば $(g^2)^3 = g^6 = 1_G$ となるので, 位数 3 の元が存在しないことに反する. ゆえに, $g \in G$ ならば $g^2 = 1_G$ なので, 演習問題 2.4.8 より G は可換群である. したがって, ある位数 2 の元から生成される部分群 H は正規部分群であり, G/H は位数 3 の群になる. これより, ある $x \in G - H$ が存在して $x^3 \in H$ となるが, $x = x^3$ なので, $x \notin H$ に反する. したがって, 位数 3 の元は存在する.

(2) G に位数 6 の元が存在するならば, 明らかに位数 2 の元は存在するので, 位数 6 の元が存在しない場合について示す. まず, H は指数 2 の部分群なので, 演習問題 2.8.2 より H は正規部分群であり, G/H は群になる. したがって, $G/H \cong \mathbb{Z}/2\mathbb{Z}$ なので, G/H には位数 2 の元 gH が存在する. このとき, $g^2 \in H$ となるが, 位数 6 の元は存在しないので, $g^2 = 1_H = 1_G$. 以上より, 位数 2 の元は存在する.

(3) 位数 $2, 3$ の元をそれぞれ x, y とすれば, G の可換性から xy は位数 6 の元である. したがって, $G \cong \mathbb{Z}/6\mathbb{Z}$ となる.

(4) 位数 $2, 3$ の元をそれぞれ y, x とすれば, これらは非可換である. 実際, これが可換ならば xy は位数 6 の元となるので不適になる. このとき, xyx^{-1} は位数 2 であり, $xyx^{-1} = y$ ならば, これは非可換であることに反するので, $xyx^{-1} \neq y$. また, x^2yx^{-2} も同様に位数 2 かつ $x^2yx^{-2} \neq xyx^{-1}$ であり, x の位数が 3 であることから $y = x^3yx^{-3} \neq x^2yx^{-2}$ となる. 今, x^2 も位数 3 の元であるから, 位数 2 の元は 4 つ以上存在しないので, 主張が示された.

(5) $\rho(g) : \{1, 2, 3\} \to \{1, 2, 3\}$ であり, $gag^{-1} = gbg^{-1}$ ならば $a = b$ なので, $\rho(g)$ は単射である. したがって, $\rho(g)$ は全単射なので, $\rho(g) \in \mathfrak{S}_3$. また,

$$\rho(gh)(x) = (gh)x(gh)^{-1} = (\rho(g) \circ \rho(h))(x)$$

なので, ρ は準同型である. $\rho(g) = id_G$ ならば, 任意の位数 2 の元 $x \in G$ について, $gx = xg$ となる. これは $g = 1_G$ となるので,

第 4 章　群の作用とシローの定理

問題 4.1.1.

$$\begin{array}{llll} x_2 \cdot x_1 = x_2 & x_2 \cdot x_2 = x_1 & x_2 \cdot x_3 = x_4 & x_2 \cdot x_4 = x_3 \\ x_3 \cdot x_1 = x_3 & x_3 \cdot x_2 = x_4 & x_3 \cdot x_3 = x_1 & x_3 \cdot x_4 = x_2 \\ x_4 \cdot x_1 = x_4 & x_4 \cdot x_2 = x_3 & x_4 \cdot x_3 = x_2 & x_4 \cdot x_4 = x_1 \end{array}$$

となるので, $\rho(x_2) = (1\ 2)(3\ 4)$, $\rho(x_3) = (1\ 3)(2\ 4)$, $\rho(x_4) = (1\ 4)(2\ 3)$.

問題 4.1.2.

$$x_4 \cdot x_1 = x_4 \quad x_4 \cdot x_2 = x_6 \quad x_4 \cdot x_3 = x_5 \quad x_4 \cdot x_4 = x_1 \quad x_4 \cdot x_5 = x_3 \quad x_4 \cdot x_6 = x_2$$

となるので, $\rho((2\ 3)) = (1\ 4)(2\ 6)(3\ 5)$.

問題 4.1.3.

$$x_3 \cdot x_1 = x_3 \in x_3H \qquad x_3 \cdot x_2 = x_1 \in x_1H \qquad x_3 \cdot x_3 = x_2 \in x_2H$$

となるので, $\rho((1\ 3\ 2)) = (1\ 3\ 2)$.

問題 4.1.4.

$\tau = (1\ 2\ 3)$ とすれば,

$$\begin{array}{lll} \mathrm{Ad}(\tau)(1) = 1 & \mathrm{Ad}(\tau)((1\ 2)) = (2\ 3) & \mathrm{Ad}(\tau)((1\ 3)) = (1\ 2) \\ \mathrm{Ad}(\tau)((2\ 3)) = (1\ 3) & \mathrm{Ad}(\tau)((1\ 2\ 3)) = (1\ 2\ 3) & \mathrm{Ad}(\tau)((1\ 3\ 2)) = (1\ 3\ 2) \end{array}$$

となるので, $\rho(\tau) = (2\ 4\ 3)$.

問題 4.1.5.

$$\begin{array}{llll} x_3 \cdot x_1 = x_3 & x_3 \cdot x_2 = x_4 & x_3 \cdot x_3 = x_2 & x_3 \cdot x_4 = x_1 \\ x_3 \cdot x_5 = x_7 & x_3 \cdot x_6 = x_8 & x_3 \cdot x_7 = x_6 & x_3 \cdot x_8 = x_5 \end{array}$$

となるので, $\rho(i) = (1\ 3\ 2\ 4)(5\ 7\ 6\ 8)$ であり,

$$\begin{array}{llll} x_7 \cdot x_1 = x_7 & x_7 \cdot x_2 = x_8 & x_7 \cdot x_3 = x_6 & x_7 \cdot x_4 = x_5 \\ x_7 \cdot x_5 = x_4 & x_3 \cdot x_6 = x_3 & x_3 \cdot x_7 = x_2 & x_3 \cdot x_8 = x_1 \end{array}$$

となるので, $\rho(k) = (1\ 7\ 2\ 8)(3\ 6\ 4\ 5)$.

問題 4.1.6.

(1) $y^{100}xy^{-100} = y^{99}x^3y^{-99} = \cdots = x^{3^{100}} = x^4$.

(2) $y^{1000}xy^{-1000} = y^{999}x^5y^{-999} = \cdots = x^{5^{1000}} = x^2$.

問題 4.1.7.

$\|\boldsymbol{x}\| = \|\boldsymbol{y}\| = 0$ ならば, $\boldsymbol{x} = \boldsymbol{y} = \boldsymbol{0}$ となるので, $G\boldsymbol{x} = G\boldsymbol{y}$. 以下, $\|\boldsymbol{x}\| = \|\boldsymbol{y}\| \neq 0$ と仮定する. $\{\boldsymbol{x}/\|\boldsymbol{x}\|\}$ を延長して $\mathbb{R}^n$ の正規直交基底をとれるので, $\boldsymbol{x}/\|\boldsymbol{x}\|$ を第一列にもつ行列, つまり, $\boldsymbol{x}/\|\boldsymbol{x}\| = A[1, 0, \cdots, 0]$ を満たす行列 $A \in \mathrm{SO}(n)$ が存在する. 同様に $\boldsymbol{y}/\|\boldsymbol{y}\| = B[1, 0, \cdots, 0]$ となるような $B \in \mathrm{SO}(n)$ が存在するので,

$$\|\boldsymbol{x}\|BA^{-1}\frac{\boldsymbol{x}}{\|\boldsymbol{x}\|} = \|\boldsymbol{y}\|\frac{\boldsymbol{y}}{\|\boldsymbol{y}\|}$$

より, $BA^{-1}\boldsymbol{x} = \boldsymbol{y}$ となる. ここで, $BA^{-1} \in \mathrm{SO}(n)$ である. これより, $G\boldsymbol{x} \cap G\boldsymbol{y} \neq \emptyset$ なので, $G\boldsymbol{x} = G\boldsymbol{y}$ となる.

問題 4.1.8.

(1) $\sigma((2, 4)) = (\sigma(2), \sigma(4)) = (1, 4)$.

(2) $\mathfrak{S}_n$ の元は写像として全単射なので, Y における G の軌道としてありえるのは

$$A := \{(x, y) \in X \mid x \neq y\}, \qquad B := \{(x, y) \in X \mid x = y\}$$

の二つである. ここで, 単射性から $A \cap B = \emptyset$ となり, 全射性から $A \cup B = \bigcup_{y \in Y} Gy$ が従う. その代表元はそれぞれ $(1, 1), (1, 2)$ である.

(3) $(1, 1)$ の安定化群は 1 を不変にする n 次置換の群であり, これは $\mathfrak{S}_{n-1}$ と同型. また, $(1, 2)$ の安定化群も同様に $\mathfrak{S}_{n-2}$ と同型になる. ($n = 2$ のときには $\mathfrak{S}_1$ と同型である.)

問題 4.1.9.

(1)

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix}$$

となるので, 安定化群は $\{g \in \mathrm{GL}_2(\mathbb{R}) \mid (g)_{1,1} = 1, (g)_{2,1} = 0\}$ である.

(2) 一般線形群の元の正則性から $\mathbb{R}^2 \setminus \{[0, 0]\}$.

問題 4.1.10.

(1) $g \in G$ について, $g1g^{-1} = 1$ なので, 1 の共役類は $\{1\}$. また,

$$gig^{-1} = h \Longrightarrow \begin{cases} h = i & (g = \pm 1, \pm i) \\ h = -i & (otherwise) \end{cases}$$

$$gjg^{-1} = h \Longrightarrow \begin{cases} h = j & (g = \pm 1, \pm j) \\ h = -j & (otherwise) \end{cases}$$

$$gkg^{-1} = h \Longrightarrow \begin{cases} h = k & (g = \pm 1, \pm k) \\ h = -k & (otherwise) \end{cases}$$

より, 共役類は $\{1\}, \{-1\}, \{\pm i\}, \{\pm j\}, \{\pm k\}$ となる.

(1') 四元数群の真なる部分群は巡回群であり, また, 正規部分群でもあるので, 同値類は $\{1\}, \{-1\}, \{\pm i\}, \{\pm j\}, \{\pm k\}$ となる.

(2) 1 の中心化群は G 自身であり, $i(\pm j) \neq (\pm j)i$, $i(\pm k) \neq (\pm k)i$ なので, i の中心化群は $\{\pm 1, \pm i\}$.

問題 4.1.11.

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

(2) 命題 4.1.10 より, σ, τ の位数はそれぞれ 8, 2 である. l_1 は τ の作用に対して不変であり, また, 逆に τ が不変にするならば l_1 となる. また, σ^k の l_1 への作用は l_1 を $k\pi/4$ 回転を表すので, $k = 0, 4$ のときのみ σ^k は l_1 を不変にする. したがって安定化群は $\langle \tau, \sigma^4 \rangle$.

問題 4.1.12.

(a) (1) 命題 4.1.10 より $rtr^{-1} = t^{-1}$ であり, $r(rt)r = rt^3, (rt)r(rt)^{-1} = rt^2$ などとなるので, 共役類は $\{1\}, \{t, t^3\}, \{t^2\}, \{r, rt^2\}, \{rt, rt^3\}$ であり, 代表元は $1, t, t^2, r, rt$.

(2) $rt^k = t^{4-k}r$ に注意すれば, $Z_G(1) = G$, $Z_G(t) = \langle t \rangle$, $Z_G(t^2) = G$, $Z_G(r) = \langle t^2, r \rangle$, $Z_G(rt) = \langle t^2, rt \rangle$.

(a) (1) (a) に加えて, $(rt^2)r(rt^2)^{-1} = rt^4, (rt^3)r(rt^3)^{-1} = rt, (rt^4)r(rt^4)^{-1} = rt^3$ などより, 共役類は $\{1\}, \{t, t^4\}, \{t^2, t^3\}, \{r, rt, rt^2, rt^3rt^4\}$ であり, 代表元は $1, t, t^2, r$.

(2) $rt^k = t^{5-k}r$ に注意すれば, $Z_G(1) = 1$, $Z_G(t) = \langle t \rangle$, $Z_G(t^2) = \langle t \rangle$, $Z_G(r) = \langle r \rangle$.

問題 4.1.13.

(1)

$$AB := \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} =: BA$$

ならば,

$$\begin{pmatrix} 2a & 2b \\ c & d \end{pmatrix} = \begin{pmatrix} 2a & b \\ 2c & d \end{pmatrix}$$

となるので, $AB = BA$ となる必要十分条件は $b = c = 0$ である. したがって, 中心化群は

$$\{g \in \mathrm{GL}_2(\mathbb{C}) \mid (g)_{1,2} = (g)_{2,1} = 0\}$$

となる.

(2)

$$AB := \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} =: BA$$

ならば,

$$\begin{pmatrix} 2a + c & 2b + d \\ 2c & 2d \end{pmatrix} = \begin{pmatrix} 2a & a + 2b \\ 2c & c + 2d \end{pmatrix}$$

となるので, $AB = BA$ となる必要十分条件は $a = d, c = 0$ である. したがって, 中心化群は

$$\{g \in \mathrm{GL}_2(\mathbb{C}) \mid (g)_{1,1} = (g)_{2,2}, (g)_{1,2} = 0\}$$

となる.

問題 4.1.14.

問題文の g について, $g \in \mathrm{SL}_2(\mathbb{R})$ と解釈する.

(1) $cz+d=0$ とすれば, $c,d \neq 0$ と $\mathrm{Im}(z)>0$ に矛盾するので, $cz+d \neq 0$. また,

$$\begin{aligned}\mathrm{Im}\, gz &= \frac{gz-\overline{gz}}{2i} \\ &= \frac{1}{2i}\left(\frac{az+b}{cz+d}-\frac{a\overline{z}+b}{c\overline{z}+d}\right) \\ &= \frac{1}{2i}\frac{(ad+bc)\overline{z}+(ad-bc)z}{|cz+d|^2} \\ &= \frac{ad-bc}{|cz+d|^2}\frac{z-\overline{z}}{2i} > 0\end{aligned}$$

となるので, $gz \in \mathbb{H}$.

(2) $I_2 z = z$ であり,

$$\begin{aligned}g(hz) &= g\frac{(h)_{1,1}z+(h)_{1,2}}{(h)_{2,1}z+(h)_{2,2}} \\ &= \left((g)_{1,1}\frac{(h)_{1,1}z+(h)_{1,2}}{(h)_{2,1}z+(h)_{2,2}}+(g)_{1,2}\right)\Big/\left((g)_{2,1}\frac{(h)_{1,1}z+(h)_{1,2}}{(h)_{2,1}z+(h)_{2,2}}+(g)_{2,2}\right) \\ &= \frac{((g)_{1,1}(h)_{1,1}+(g)_{1,2}(h)_{2,1})z+(g)_{1,1}(h)_{1,2}+(g)_{1,2}(h)_{2,2}}{((g)_{2,1}(h)_{1,1}+(g)_{2,2}(h)_{2,1})z+(g)_{2,1}(h)_{1,2}+(g)_{2,2}(h)_{2,2}} \\ &= (gh)z\end{aligned}$$

なので, $\mathrm{SL}_2(\mathbb{R})$ は $\mathbb{H}$ に左から作用する.

(3) (1) の計算から

$$gz = \frac{ac|z|^2+adz+bc\overline{z}+bd}{|cz+d|^2}$$

であり, $\mathrm{Im}(gz)=\mathrm{Im}(z)/|cz+d|^2$ となる. また,

$$\mathrm{Re}(gz) = \frac{ac|z|^2+2(ad+bc)\mathrm{Re}(z)+bd}{|cz+d|^2}$$

となる. ここで, a,b,c,d が満たすべき条件は $ad-bc=1$ のみなので, gz は g を適当にとることにより $\mathbb{H}$ の任意の元に等しくすることができる. (例えば, $w \in \mathbb{H}$ に対し, d を適当に取ることにより $\mathrm{Im}(gz)=\mathrm{Im}(w)$ とし, b,c を $\mathrm{Re}(gz)=\mathrm{Re}(w)$ となるように選び, $ad-bc=1$ を満たすように a を定めることができる.) したがって (2) の作用は推移的である.

(4) $gi=i$ より, $a=d, b=-c$ かつ $1=ad-bc=d^2+c^2$ という条件がえられるが, 逆にこのとき $gi=i$ を満たす. したがって, 求めるべき安定化群は $\mathrm{SO}(2)$ となる.

問題 4.1.15.

ρ を作用, つまり $\rho(g)f=\rho(g,f)$ と解釈する.

問題 4.1.16.

$|G| \leq |\mathfrak{S}_n| < \infty$ なので, $x \in X$ について, 命題 4.1.23 より $|Gx|=|G|/|G_x|$ となる. また, 推移的なことから $Gx=X$ なので, $|G|=|G_x||X|=|G_x|n$ となって, $|G|$ は n で割り切れる.

問題 4.1.17.

(1) 素数位数の群は巡回群なので, 位数 17 の群は $\mathbb{Z}/17\mathbb{Z}$ と同型であり, 問題 2.5.7 より $\mathrm{Aut}(\mathbb{Z}/17\mathbb{Z}) \cong (\mathbb{Z}/17\mathbb{Z})^\times \cong \mathbb{Z}/16\mathbb{Z}$ なので, $|\mathrm{Aut}(N)| = 16$.

(2) 一般に奇数位数の群に対して, $p = 2^n + 1$ の形をした素数 p を位数にもつ正規部分群 N は G の中心に含まれることを示す. $\phi : G \ni g \mapsto \mathrm{Ad}(g) \in \mathrm{Aut}(N)$ とすれば, これは準同型である. また, (1) と同様に $|\mathrm{Aut}(N)| = 2^n$ であり, 系 2.6.21 と問題 2.5.3 より $\mathrm{Im}(\phi)$ に含まれる元の位数はすべて奇数となる. $\mathrm{Im}(\phi)$ が $\mathrm{Aut}(N)$ の部分群なので, これらと再び系 2.6.21 より, $\mathrm{Im}(\phi) = \{1\}$. ゆえに, 共役による作用が常に恒等写像になる. したがって, N は G の中心に含まれる.

問題 4.1.18.

右辺に含まれる数は 8 の約数であることが必要なので, (1) は類等式ではなく, 右辺に現れる 1 の個数は 8 の約数になる必要があるので, (4) も類等式ではない.

問題 4.2.1.

(1) (1 5)(3 8 4 6 10)(7 9)

(2) (1 6)(2 10 9 3 4)(5 8 7)

問題 4.2.2.

(1) 定理 4.2.3 より, $\mathfrak{S}_5$ において共役であることと型が等しいことは同値なので, 代表元は $1, (1\ 2), (1\ 2\ 3), (1\ 2\ 3\ 4), (1\ 2)(3\ 4), (1\ 2\ 3\ 4\ 5), (1\ 2\ 3)(4\ 5)$ となる.

(2) 例題 4.2.7 と全く同様に代表元は $1, (1\ 2), (1\ 2\ 3), (1\ 2)(3\ 4), (1\ 2\ 3\ 4\ 5), (1\ 3\ 4\ 5\ 2)$ であり, (1) と異なる共役類は $(1\ 2\ 3\ 4\ 5), (1\ 3\ 4\ 5\ 2)$.

問題 4.2.3.

(1) 補題 4.2.2 より, $\tau = (\nu(1)\ \nu(2)\ \nu(3))(\nu(4)\ \nu(5)\ \nu(6))$ となるので, 例えば $\nu = (1\ 4\ 2)(5\ 6)$ が条件を満たす.

(2) (1) より,

$$\{(\nu(1)\ \nu(2)\ \nu(3)), (\nu(4)\ \nu(5)\ \nu(6))\} = \{(4\ 1\ 3), (2\ 6\ 5)\}$$

ただし、ここでの $=$ は対称群の元の集合として等しいという意味である. これより, $2 \times 3 \times 3 = 18$ が求めるべき個数である.

問題 4.2.4.

(1) $\tau \in Z_G(\sigma)$ ならば $\tau\sigma = \sigma\tau$ なので, $\tau\sigma\tau^{-1} = \sigma$ を満たす. ゆえに, 補題 4.2.2 より $(1\ 2) = (\tau(1)\ \tau(2))$ となるが, このとき $(\tau(1), \tau(2)) = (1, 2), (2, 1)$ であり, 逆も成り立つ. これより, $Z_G(\sigma) = \langle (1\ 2), (3\ 4) \rangle$ となる.

(2) (1) と同様に, $\nu \in Z_G(\sigma)$ ならば,

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

なので, $Z_G(\sigma) = \langle (1\ 2), (3\ 4), (1\ 3)(2\ 4) \rangle$.

(3) (1) と同様に, $Z_G(\sigma) = \langle\sigma\rangle$.
(4) (1) と同様に, $Z_G(\sigma) = \langle(1\ 2\ 3), (4\ 5)\rangle$.
(5) (1) と同様に, $Z_G(\sigma) = \langle(1\ 2\ 3), (4\ 5\ 6), (1\ 4)(2\ 5)(3\ 6)\rangle$.
(6) (1) と同様に, $Z_G(\sigma) = \langle(1\ 2), (3\ 4), (5\ 6), (1\ 3)(2\ 4), (1\ 5)(2\ 6)\rangle$

問題 4.2.5.

(1) 問題 4.2.4 と同様に $\tau \in Z_G(\sigma)$ とすれば, $(\tau(1)\ \tau(2)\ \cdots\ \tau(n)) = \sigma$ となる. ここで, $=$ は $\mathfrak{S}_n$ の元として等しいという意味である. $\tau(1) = k$ ならば, $\tau = \sigma^{k-1}$ となるので, $\tau \in \langle\sigma\rangle$. 逆は明らかである. よって, $Z_G(\sigma) = \langle\sigma\rangle$ となる.
(2) $Z(G) \subset Z_G(\sigma)$ であることと $\sigma^k(1\ 2) \neq (1\ 2)\sigma^k$ $(k = 1, \cdots, n-1)$ であることから, $Z(G) = \{1\}$.

問題 4.2.6.

σ を型の通りに表し,

$$\sigma = \sigma_{j_1,1}\sigma_{j_1,2}\cdots\sigma_{j_1,a_1}\sigma_{j_2,1}\cdots\sigma_{j_2,a_2}\cdots\sigma_{j_m,a_m}$$

とおく. ただし, 任意の a について, $\sigma_{j,a}$ は長さ j の巡回置換であり, どの 2 つも互いに素である. ここで,

$$N = \langle\sigma_{j_k,i}\rangle_{1\leq k\leq m, 1\leq i\leq a_k}$$

と定めれば, $N \subset Z_G(\sigma)$ であり, 自然に

$$N \cong (\mathbb{Z}/j_1\mathbb{Z})^{a_1} \times \cdots \times (\mathbb{Z}/j_m\mathbb{Z})^{a_m}$$

が成り立つ. また, $\tau \in Z_G(\sigma)$ であることは任意の k について,

$$\{\tau\sigma_{j_k,1}\tau^{-1}, \cdots, \tau\sigma_{j_k,a_k}\tau^{-1}\} = \{\sigma_{j_k,1}, \cdots, \sigma_{j_k,a_k}\}$$

であることと同値なので, 置換表現 $\phi_k : Z_G(\sigma) \to \mathfrak{S}_{a_k}$ が定まる. さらに, ϕ_k は全射である. ここで, $\phi = (\phi_1, \ldots, \phi_m)$ とすれば, $\phi : Z_G(\sigma) \to \mathfrak{S}_{a_1} \times \cdots \times \mathfrak{S}_{a_m}$ は全射であり, $N \subset \operatorname{Ker}\phi$ は明らかであり, 逆を示すために $\nu \in \operatorname{Ker}\phi$ とする. このとき, 任意の j, a について, $\nu\sigma_{j,a}\nu^{-1} = \sigma_{j,a}$ が成り立つ. ここで,

$$\sigma_{j,a} = (s_1\ s_2\ \cdots\ s_j)$$

とすれば, 問題 4.2.5 と同様に, ある n が存在して, 任意の $1 \leq k \leq i$ について $\nu(s_k) = \sigma_{j,a}^n(s_k)$ となる. さらに, $\sigma_{j,a}$ が互いに素であることから $\nu \in N$ が成り立つ. これより $N = \operatorname{Ker}\phi$ であり, 定理 2.10.1 から $Z_G(\sigma)/N \cong \mathfrak{S}_{a_1} \times \cdots \times \mathfrak{S}_{a_m}$ が従う.

問題 4.2.7.

(1) $i_1, \cdots, i_l$ がすべて異なる奇数であることから, 問題 4.2.4 と同様に, $Z_{\mathfrak{S}_n}(\sigma)$ は σ を巡回置換の積として表したときの巡回置換で生成されており, この巡回置換は長さの異なる偶置換なので, $Z_{\mathfrak{S}_n}(\sigma)$ は偶置換しか含まない. したがって, $Z_{\mathfrak{S}_n}(\sigma) = Z_{A_n}(\sigma)$ となる.
(2) まず, $i_1, \cdots, i_l$ において, $i_j = i_k = n$ (n は奇数) なる j, k が存在すると仮定する. このような巡回置換をそれぞれ $(a_1\ \cdots\ a_n), (b_1\ \cdots\ b_n)$ と表すことにすれば, 問題 4.2.4 と同様に $(a_1\ b_1)\cdots(a_n\ b_n) \in Z_{\mathfrak{S}_n}(\sigma)$ となり, これは n が奇数であることから $[Z_{\mathfrak{S}_n}(\sigma) : Z_{A_n}(\sigma)] \geq 2$ になる.[*1] また, $[Z_{\mathfrak{S}_n}(\sigma) :$

[*1] $[Z_{\mathfrak{S}_n}(\sigma) : Z_{A_n}(\sigma)]$ は指数である.

$Z_{A_n}(\sigma)] \leq 2$ は明らかなので, $[Z_{\mathfrak{S}_n}(\sigma) : Z_{A_n}(\sigma)] = 2$ が満たされる. 次に, ある j が存在して i_j が偶数のとき, それに対応する巡回置換は $Z_{\mathfrak{S}_n}(\sigma)$ に含まれるので, 同様に $[Z_{\mathfrak{S}_n}(\sigma) : Z_{A_n}(\sigma)] = 2$ が満たされる.

問題 4.2.8.

$|G| = |\mathfrak{S}_3|$ であり, $\mathfrak{S}_3 = \langle (1\ 2), (2\ 3) \rangle$ なので, $Z(\mathfrak{S}_3) = Z_{\mathfrak{S}_3}(X)$ が成り立つ. これより, $\tau \in \mathrm{Ker}(\rho)$ ならば $\rho = id_{\mathfrak{S}_3}$ である. したがって, ρ. ゆえに, 同型である.

問題 4.2.9.

(1) $\rho((1\ 2)) = (2\ 3)$, $\rho((1\ 2\ 3)) = (1\ 3\ 2)$, $\rho((2\ 3)) = (1\ 2)$.

(2) $\mathfrak{S}_3 = \langle (1\ 2), (2\ 3) \rangle$ であり, (1) より, $\rho((1\ 2)) = (2\ 3)$, $\rho((2\ 3)) = (1\ 2)$ なので, ρ が準同型であることより全射である.

(3) $\mathrm{Ker}(\rho) = Z_G(x_1) \cap Z_G(x_2) \cap Z_G(x_3) = \{1, x_1, x_2, x_3\}$.

問題 4.2.10.

$\mathfrak{S}_4$ の部分群の位数は $1, 2, 3, 4, 6, 8, 12, 24$ のいずれかであり, $1, 24$ を位数にもつ部分群は $\{1\}, \mathfrak{S}_4$ のみである. 以下, 位数で場合分けをするが, 各場合について H はその位数の部分群とする. また, 同じ共役類に属する部分群は同型であることに注意しておく.

位数 2 の部分群について, H は位数 2 の元によって生成されている. $\mathfrak{S}_4$ の位数 2 の元は互換または互換の積で表され, 定理 4.2.3 より, 互換で生成される部分群と互換の積で生成される部分群はそれぞれ部分群の共役類をなす.

位数 3 の部分群について, H は位数 3 の元によって生成されている. $\mathfrak{S}_4$ の位数 3 の元はすべて長さが 3 の巡回置換で表されるので, 定理 4.2.3 より, 位数 3 の部分群全体で一つの共役類をなす.

位数 4 の部分群について, 命題 4.4.4 より H は Abel 群であり, 定理 4.8.2 から $H \cong \mathbb{Z}/4\mathbb{Z}$ または $H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ が従う. $H \cong \mathbb{Z}/4\mathbb{Z}$ のとき, H は位数 4 の元によって生成されるが, $\mathfrak{S}_4$ の位数 4 の元はすべて長さが 4 の巡回置換で表されるので, 定理 4.2.3 より, このような部分群全体で一つの共役類をなす. また, $H \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ のとき, H は積の位数が 2 となるような二つの位数 2 の元で生成される. このような部分群は $\langle (a\ b), (c\ d) \rangle$ または $\langle (a\ b)(c\ d), (a\ c)(b\ d) \rangle$ という形で表されるが, $H = \langle (a\ b), (c\ d) \rangle$ のときには $g = (b\ c)$ について,

$$g(a\ b)g^{-1} = (a\ c), \qquad g(c\ d)g^{-1} = (b\ d)$$

となるので, そのような形の部分群はすべて共役である. また, $H = \langle (a\ b)(c\ d), (a\ c)(b\ d) \rangle$ のときには正規部分群となるので, それぞれ別の共役類をなす.

位数 6 の部分群について, 問題 2.10.8 より, $H \cong \mathbb{Z}/6\mathbb{Z}$ または $H \cong \mathfrak{S}_3$ が成り立つ. しかし, $\mathfrak{S}_4$ には位数 6 の元は含まれないので, $H \cong \mathfrak{S}_3$ が従う. このとき, 問題 2.3.9 より, H は相違なる二つの位数 2 の元であって, その積が位数 3 となるようなもので生成される. ゆえに, $H = \langle (a\ b), (a\ c) \rangle$ と表すことができ, $g = (b\ d)$ に対して,

$$g(a\ b)g^{-1} = (a\ d), \qquad g(a\ c)g^{-1} = (a\ c)$$

であって, $h=(a\ d)$ に対して,

$$h(a\ b)h^{-1}=(b\ d),\qquad\qquad h(a\ c)h^{-1}=(c\ d)$$

も成り立つので, 位数 6 の部分群全体で一つの共役類をなす.

位数 8 の部分群について, これは 2-Sylow 部分群なので, 定理 4.5.7(3) より, 位数 8 の部分群全体で一つの共役類をなす. ただし, 位数 8 の部分群は正規部分群ではない. 実際, $\langle(1\ 2),(1\ 3\ 2\ 4)\rangle$ は位数 8 の部分群であるが,

$$(1\ 3)\notin N_{\mathfrak{S}_4}(\langle(1\ 2),(1\ 3\ 2\ 4)\rangle)$$

なので, 命題 4.5.6 と定理 4.5.7(3)(4) より, 位数 8 の部分群は正規部分群ではない.

位数 12 の部分群について, $|\mathfrak{S}_4/H|=2$ なので, $\mathfrak{S}_4/H\cong\mathbb{Z}/2\mathbb{Z}$ となるが, $\mathbb{Z}/2\mathbb{Z}$ はアーベル群なので, 問題 2.8.2 と命題 4.3.2(2) より $D(\mathfrak{S}_4)\subset H$ となる. 一般に $D(\mathfrak{S}_n)=A_n$ なので, $A_4\subset H$ であり, $|A_4|=|H|=12$ なので, $A_4=H$ が成り立つ. 特に, A_4 は正規部分群である.

問題 4.3.1.

(1) $[\sigma,\tau]=\sigma\tau\sigma^{-1}\tau=(1\ 2\ 3)(2\ 3)(1\ 3\ 2)(2\ 3)=(1\ 3\ 2)$.

(2) $[i,j]=iji^{-1}j^{-1}=-1$

問題 4.3.2.

問題文の定義によって $\mathrm{GL}_n(\mathbb{C})$ に定められた N_i を N_i^n と表し, $\mathbb{C}^n$ の標準的な基底 $e_1,\dots,e_n$ について, $e_1,\dots,e_k$ で張られた $\mathbb{C}$-部分空間を V_k とする.

(1) n に関する帰納法で示す. まず, $N_1^1=\mathrm{GL}_1(\mathbb{C})$ より, N_1^1 は $\mathrm{GL}_1(\mathbb{C})$ の部分群である. $n\in\mathbb{N}$ について, N_i^n $(i=1,\dots,n)$ は $\mathrm{GL}_n(\mathbb{C})$ の部分群であると仮定し, N_i^{n+1} $(i=1,\dots,n+1)$ について考える. $X,Y\in N_i^{n+1}$ を

$$X=\left(\begin{array}{c|c}A & \boldsymbol{b}\\ \hline {}^t\mathbf{0} & 1\end{array}\right),\qquad\qquad Y=\left(\begin{array}{c|c}C & \boldsymbol{d}\\ \hline {}^t\mathbf{0} & 1\end{array}\right)$$

とおけば, $A,C\in N_i^n$ かつ $\boldsymbol{b},\boldsymbol{d}\in V_{n-i+1}$ である. 仮定より, $A^{-1}\in N_i^n$ が存在し,

$$\left(\begin{array}{c|c}A & \boldsymbol{b}\\ \hline {}^t\mathbf{0} & 1\end{array}\right)\left(\begin{array}{c|c}A^{-1} & -A^{-1}\boldsymbol{b}\\ \hline {}^t\mathbf{0} & 1\end{array}\right)=E_{n+1}$$

であり, A^{-1} は上三角行列なので $A^{-1}\boldsymbol{b}\in V_{n-i+1}$ となる. よって

$$X^{-1}=\left(\begin{array}{c|c}A^{-1} & -A^{-1}\boldsymbol{b}\\ \hline {}^t\mathbf{0} & 1\end{array}\right)\in N_i^{n+1}$$

である. また

$$XY=\left(\begin{array}{c|c}AC & A\boldsymbol{d}+\boldsymbol{b}\\ \hline {}^t\mathbf{0} & 1\end{array}\right)$$

であり, 仮定より $AC\in N_i^n$ かつ $A\boldsymbol{d}+\boldsymbol{b}\in V_{n-i+1}$ である. したがって, $XY\in N_i^{n+1}$ である. これより, N_i^{n+1} は $\mathrm{GL}_{n+1}(\mathbb{C})$ の部分群となり, 以上より任意の n に対して N_i^n $(i=1,\dots,n)$ は $\mathrm{GL}_n(\mathbb{C})$ の部分群である.

(2) n に関する帰納法で示す．まず，

$$\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix} \in N_1^2 \subset \mathrm{GL}_2(\mathbb{C})$$

について，

$$\begin{aligned}\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}^{-1}\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}^{-1} &= \begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & -a\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & -b\\ 0 & 1\end{pmatrix}\\ &= \begin{pmatrix}1 & a+b-a-b\\ 0 & 1\end{pmatrix}\\ &= E_2 \in N_2^2\end{aligned}$$

が成り立つ．これより，$[N_1^2, N_1^2] \subset N_2^2$ である．次に，$n \in \mathbb{N}$ について，$[N_1^n, N_i^n] \subset N_{i+1}^n$ $(i = 1, \ldots, n-1)$ であると仮定する．$X \in N_1^{n+1}, Y \in N_i^{n+1}$ $(i = 1, \ldots, n)$ を

$$X = \left(\begin{array}{c|c} A & \boldsymbol{b} \\ \hline {}^t\mathbf{0} & 1 \end{array}\right), \qquad Y = \left(\begin{array}{c|c} C & \boldsymbol{d} \\ \hline {}^t\mathbf{0} & 1 \end{array}\right)$$

とおく．ただし，$A \in N_1^n, C \in N_i^n$ かつ $\boldsymbol{d} \in V_{n-i+1}$ である．また，(1) より，

$$X^{-1} = \left(\begin{array}{c|c} A^{-1} & -A^{-1}\boldsymbol{b} \\ \hline {}^t\mathbf{0} & 1 \end{array}\right), \qquad Y^{-1} = \left(\begin{array}{c|c} C^{-1} & -C^{-1}\boldsymbol{d} \\ \hline {}^t\mathbf{0} & 1 \end{array}\right)$$

である．ここで，

$$\begin{aligned}XYX^{-1}Y^{-1} &= \left(\begin{array}{c|c} AC & A\boldsymbol{d}+\boldsymbol{b} \\ \hline {}^t\mathbf{0} & 1 \end{array}\right)\left(\begin{array}{c|c} A^{-1}C^{-1} & -A^{-1}C^{-1}\boldsymbol{d}-A^{-1}\boldsymbol{b} \\ \hline {}^t\mathbf{0} & 1 \end{array}\right)\\ &= \left(\begin{array}{c|c} ACA^{-1}C^{-1} & -(ACA^{-1}C^{-1}-A)\boldsymbol{d}-(ACA^{-1}-E_n)\boldsymbol{b} \\ \hline {}^t\mathbf{0} & 1 \end{array}\right).\end{aligned}$$

であり，仮定より $ACA^{-1}C^{-1} \in N_{i+1}^n$ が成り立つ．

$$\begin{aligned}\boldsymbol{d}' &= -A(CA^{-1}C^{-1}-E_n)\boldsymbol{d},\\ \boldsymbol{b}' &= -(ACA^{-1}-E_n)\boldsymbol{b}\end{aligned}$$

とおけば，

$$CA^{-1}C^{-1} = A^{-1}(ACA^{-1}C^{-1}) \in N_1^n$$

と $\boldsymbol{d} \in V_{n-i+1}$ より，$\boldsymbol{d}' \in V_{n-i}$ である．また，

$$ACA^{-1} = (ACA^{-1}C^{-1})C \in N_i^n$$

より，$\boldsymbol{b}' \in V_{n-i}$ も従う．したがって，$\boldsymbol{d}' + \boldsymbol{b}' \in V_{n-i}$ となり，$XYX^{-1}Y^{-1} \in N_{i+1}^{n+1}$ が成り立つ．

(3) 部分群の列

$$N_1^n \supset N_2^n \supset \cdots \supset N_{n-1}^n \supset N_n^n = \{E_n\}$$

を考える．(2) より，任意の $g \in N_1^n, h \in N_i^n$ $(i = 1, \ldots, n-1)$ に対して

$$ghg^{-1}h^{-1} \in N_{i+1}^n \subset N_i^n$$

となるので，$ghg^{-1} \in N_i^n$ である．ゆえに，$N_1^n \rhd N_i^n$ が成り立つ．また，N_1^n/N_{i+1}^n において

$$(gN_{i+1}^n)(hN_{i+1}^n)(g^{-1}N_{i+1}^n)(h^{-1}N_{i+1}^n) = ghg^{-1}h^{-1}N_{i+1}^n = N_{i+1}^n$$

より,

$$(gN_{i+1}^n)(hN_{i+1}^n) = (hN_{i+1}^n)(gN_{i+1}^n)$$

したがって, $N_i^n/N_{i+1}^n \subset Z(N_1^n/N_{i+1}^n)$ となる. 以上より N_1^n はべき零である.

問題 4.4.1.

G を群で, $|G| = p^n$ となるものとする. $n = 1$ のとき, G はアーベル群なので特にべき零である. $n-1$ 以下で主張が成立すると仮定する. 命題 4.4.3 より, $G/Z(G)$ は G より小さい p 群となるので, 帰納法の仮定より, 部分群の列

$$G/Z(G) = L_0 \supset L_1 \supset \cdots \supset L_r = \{e\}$$

であって, $L_{i+1} \triangleleft G/Z(G)$ かつ L_i/L_{i+1} が $(G/Z(G))/L_{i+1}$ の中心に含まれるようなものが存在する. これと定理 2.10.2 より, $L_i = A_i/Z(G)$ となるような部分群 $A_i \subset G$ が存在する. このような A_i を並べれば, 部分群の列

$$G = A_0 \supset A_1 \supset \cdots \supset A_r = Z(G)$$

が得られ, 命題 2.10.4(2) より, $A_{i+1} \triangleleft G$ かつ A_i/A_{i+1} が G/A_{i+1} の中心に含まれる. ここで, $A_{r+1} = \{e\}$ と定めれば, $A_{r+1} \triangleleft G$ であって, 定義より,

$$A_r/A_{r+1} = Z(G) \subset Z(G/A_{r+1})$$

が成り立つ. したがって, 帰納的に p 群はべき零群である.

問題 4.5.1.

(1) $\sigma y = \{(1\ 3\ 2), (2\ 3\ 4)\}$.

(2) $N_{\mathfrak{S}_4}(y) = \{1, (1\ 2)(3\ 4)\}$.

問題 4.5.2.

(1) 命題 4.1.10(1)(3) より, 位数 2 の部分群は $\langle \tau\sigma^i \rangle$ $(i = 0, 1, 2, 3), \langle \sigma^2 \rangle$ である.

(2) $\tau(\tau\sigma^i) = (\tau\sigma^{-i})\tau, \sigma(\tau\sigma^i) = (\tau\sigma^{i-2})\sigma$ より, $g = \tau^j\sigma^k$ とおけば,

$$g(\tau\sigma^i)g^{-1} = \tau^j(\tau\sigma^{i-2k})\tau^{-j} = \tau\sigma^{(-1)^j(i-2k)}$$

となので, 軌道は $\{\langle\sigma^2\rangle\}, \{\langle\tau\rangle, \langle\tau\sigma^2\rangle\}, \{\langle\tau\sigma\rangle, \langle\tau\sigma^3\rangle\}$ である.

(3) (2) より, $\mathrm{Stab}(\langle\sigma^2\rangle) = G, \mathrm{Stab}(\langle\tau\sigma\rangle) = \langle\sigma^2, \tau\sigma\rangle, \mathrm{Stab}(\langle\tau\rangle) = \langle\sigma^2, \tau\rangle$.

問題 4.5.3.

(1) $q < p$ としてよい. 定理 4.5.7 の (1) より, Sylow-p 部分群 H は存在し, (4) より, Sylow-p 部分群の数 s は $|G|$ の約数であり, $q < p$ なので, $s = 1$ となる. これより $|G| = |N_G(H)|$ となるので, H は正規部分群である. $1 < |H| < |G|$ なので, H は自明でない正規部分群となり, G は可解群である. 特に, 単純群ではない.

(2) 仮定より, Sylow-q 部分群 K も一意に存在するので, (1) と合わせて H, K が正規部分群であることが従う. H, K の元の位数はそれぞれ p, q なので, $H \cap K = \{1\}$. また, $H, K \subset HK$ なので $|HK| = pq$ となり, $HK = G$ が満たされる. 命題 2.9.2 と命題 2.9.3 より, $G \cong H \times K \cong \mathbb{Z}/pq\mathbb{Z}$ となるので, G は巡回群である.

(3) (1) $n = 6, 10, 14, 15, 21, 22, 26, 33, 34, 35, 38, 39, 46, 51, 55, 57, 58.$
(2) $n = 15, 33, 35, 51.$

問題 4.5.4.

(1) Sylow-5 部分群 H の数は 40 の約数であり, 5 で割って 1 あまる数なので, 1 となる. これより $|G| = |\mathrm{N}_G(H)|$ となり, H は正規部分群なので, G は単純群ではない.
(2) Sylow-7 部分群を考えれば, (1) と同様に証明できる.
(3) Sylow-3 部分群を考えれば, (1) と同様に証明できる.

問題 4.5.5.

K が正規部分群でないと仮定する. このとき, Sylow-7 部分群が 8 だけ存在する. Sylow-7 部分群は位数 7 の巡回群であるから, これらを構成する元の個数は $(7-1)\times 8+1 = 49$ である. 今, 56 の約数であって奇数であるものは $1, 7$ のみであり, Sylow-2 部分群が 7 だけ存在するならば, 元の位数を考えることで, G の元の数が 56 を超えてしまうことが示されるが, これは矛盾である. したがって, Sylow-2 部分群は 1 だけ存在し, ゆえに, Sylow-2 部分群は正規部分群である.

問題 4.5.6.

(1) Sylow-5 部分群が正規部分群ではないとき, 30 の約数を考えることにより, Sylow-5 部分群は 6 だけ存在する. また, Sylow-3 部分群の数としては $1, 10$ があり得るが, 3-Sylow 部分群が 10 だけ存在すれば, 問題 4.5.5 と同様に G の位数を超えてしまうことが従うが, これは矛盾である. したがって, Sylow-3 部分群の数は 1 であり, 正規部分群である. また, 問題 4.5.3(2) より, $HK \cong \mathbb{Z}/15\mathbb{Z}$ が成り立つ.
(2) HK は指数 2 の部分群なので, 正規部分群である. ここで, 位数 2 の元 $g \in G$ に対して, $\phi = \mathrm{Ad}(g)$ とする. HK の生成元を y とすれば, $\phi(y)$ は共役の単射性から位数 15 の元であり, HK が正規部分群であることから $\langle \phi(y) \rangle = HK$ が従う. これより, $\phi \in \mathrm{Aut}(HK) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$（問題 2.5.7 参照）であり, $\phi^2 = 1$ なので, ϕ は

$$(0,0), (0,2), (1,0), (1,2) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

のいずれかに対応している. $\langle g \rangle \langle y \rangle = G$ であることに注意して, 場合分けを行う.

(0,0) のとき　ϕ は恒等写像なので, 任意の $x \in HK$ に対して $xg = gx$ が成り立つ. ゆえに, $G \cong \mathbb{Z}/30\mathbb{Z}$ となる.

(0,2) のとき　$\phi(y^5) = y^5$ であり, $\phi^2 = 1$ より, $\phi(y) = y^4$ が従う. これより, $z = y^3$ とおけば, $gzg^{-1} = z^{-1}$ が成り立つ. ここで, $F = \langle g, z \rangle$ とおけば, これは G の正規部分群であり, 定理 4.6.5 と $|F| = |D_5|$ から, $F \cong D_5$ となる. また, $\phi(y^5) = y^5$ であることから, $\langle y^5 \rangle$ は G の正規部分群である. さらに, $F \cap \langle y^5 \rangle = \{1\}$ も成り立つので, 命題 2.9.2 より $G \cong \mathbb{Z}/3\mathbb{Z} \times D_5$ となる.

(1,0) のとき　$\phi(y^3) = y^3$ であり, $\phi^2 = 1$ より, $\phi(y) = y^{11}$ が従う. これより, $z = y^5$ とおけば, $gzg^{-1} = z^{-1}$ が成り立つ. ここで, $F = \langle g, z \rangle$ とおけば, これは G の正規部分群であり, 定理 4.6.5 と $|F| = |D_3|$ から, $F \cong D_3$ となる. これらより, $(0,2)$ の場合と同様にして $G \cong \mathbb{Z}/5\mathbb{Z} \times D_3$ が成り立つ.

(1,2) のとき　$\phi(y^3) \neq y^3$, $\phi(y^5) \neq y^5$ と $\phi^2 = 1$ より, $\phi(y) = y^{14}$ が従う. これより, $gyg^{-1} = y^{-1}$ であり, $F = \langle g, y \rangle$ とおけば, これは G の部分群であり, 定理 4.5.6 と $|F| = |D_{15}|$ より, $F \cong D_{15}$ が

成り立つ. さらに, 定理 4.5.6 と $|F| = |G|$ より, $F \cong G$ も成り立つので, $G \cong D_{15}$ が従う.

問題 4.5.7.

(1) H が正規部分群でないと仮定すれば, 定理 4.5.7(4) と $|G| = p^2q$ より, $q \equiv 1 \pmod{p}$ が成り立が, これは $p > q$ であることに反する. ゆえに, H は正規部分群である.

(2) 定理 4.5.7(4) より, K の共役の数としてありえるのは $1, p, p^2$ のうち, q で割って 1 だけ余るものである. このうち, 1 は K が正規部分群でないことに反し, p は $p < q$ に矛盾するので, K の共役の数は p^2 である.

(3) H, K がともに正規部分群ではないと仮定する. (1)(2) より, $p < q$ かつ $p^2 \equiv 1 \pmod{q}$ であり, ゆえに $p + 1$ は q の倍数である. さらに, $p < q$ より, $p + 1 = q$ であることが従うので $p = 2, q = 3$ となる. したがって, $|G| = 12$ となるが, このとき H, K がともに正規部分群でないことは定理 4.7.1 の証明に矛盾するので, H, K のどちらかは正規部分群である.

問題 4.5.8.

(1) 定理 4.5.7 より, H の共役な部分群の数は 1 または 3 であるが, H が正規部分群ならば G は単純ではない. また, 共役な部分群の数が 3 の場合には H の共役な部分群の集合への G の共役作用による置換表現を考えれば, $\varphi : G \to \mathfrak{S}_3$ という群準同型が導かれる. このとき, $\operatorname{Ker}\varphi$ は正規部分群であるが, $\operatorname{Ker}\varphi = G$ とすれば, H は正規部分群となるので矛盾. さらに, $\operatorname{Ker}\varphi = \{1\}$ とすれば, φ は単射であるが, $|\mathfrak{S}_3| < |G|$ より, これも不合理である. したがって, G は単純群ではない.

(2) Sylow-3 部分群について考えれば, (1) と同様に証明できる.

(3) Sylow-2 部分群について考えれば, (1) と同様に証明できる.

問題 4.5.9.

単純群の定義と命題 4.4.3 より, p 群は単純群ではない. また, それ以外の位数の群については問題 4.5.3 から問題 4.5.8 より, 単純群ではないことが従う.

問題 4.6.1.

$H := \langle x^2, y \rangle$ の元は $y^i x^{2j}$ という形で表すことができるので, $|H| \leq 6$ である. $y^{i_1}x^{2j_1} = y^{i_2}x^{2j_2}$ $(0 \leq i_1, i_2 \leq 2, 0 \leq j_1, j_2 \leq 1)$ とすれば, $y^{i_1 - i_2} = x^{2(j_2 - j_1)}$ が成り立つが, y, x^2 の位数はそれぞれ $3, 2$ なので, $i_1 = i_2, j_1 = j_2$ となる. したがって, $|H| = 6$ であり, G の関係式から x^2 と y は可換なので, 問題 2.10.8 より, $H \cong \mathbb{Z}/6\mathbb{Z}$ である.

問題 4.6.2.

$$F = \langle x, y \mid x^n = y^2 = 1, yxy = x^{-1} \rangle$$

とする. 定理 4.6.5 より, 全射準同型 $\varphi : F \to D_n$ が存在する. また, F の元は $x^i y^j$ $(0 \leq i \leq n-1, 0 \leq j \leq 1)$ という形で表せるので, $|F| \leq |D_n|$ が成り立つ. したがって, $F \cong D_n$ である.

問題 4.6.3.

$xy^3x = (xyx)^3 = y$ より, $y^2 = (xy^3x)^2 = xyx = y^3$ なので, $y = 1$.

問題 4.6.4.

(1) $x_i^2 = 1$, $x_ix_j = x_jx_i$ $(|i-j| \geq 2)$ は明らか. また,

$$x_ix_{i+1}x_i = (i\ i+1)(i+1\ i+2)(i\ i+1) = (i\ i+2)$$

であり,

$$x_{i+1}x_ix_{i+1} = (i+1\ i+2)(i\ i+1)(i+1\ i+2) = (i\ i+2)$$

なので, これらも等しい.

(2) まず, H_n の任意の元は x_{n-1} が高々一回しか現れないように表せることを示す. $n = 3$ の場合には明らかであり, $n-1$ で主張が成立していると仮定する. このとき, H_n の任意の元は $y_\lambda \in H_{n-1}$ を x_{n-2} が高々一回現れるようなものとして, x_{n-1} と y_λ の語として表せる. このことと, $x_ix_j = x_jx_i$ $(|i-j| \geq 2)$, $x_ix_{i+1}x_i = x_{i+1}x_ix_{i+1}$ より, 主張は帰納的に従う. さらに, $x_ix_j = x_jx_i$ $(|i-j| \geq 2)$ より, $x \in H_n$ は x_{n-1} を含まない, または $\tau_i = x_ix_{i+1}\cdots x_{n-1}$, $y \in H_{n-1}$ として, $x = \tau_i y$ という形で表すことができる. $|H_3| = 3!$ であることは明らかなので, これらより, 帰納的に $|H_n| \leq n!$ であることが従う.

(3) 定理 4.6.5 と問題 2.3.9(1) より, 全射準同型 $H_n \to \mathfrak{S}_n$ が存在するので, $|H_n| \geq |\mathfrak{S}_n| = n!$. ゆえに, $H_n \cong \mathfrak{S}_n$ が成り立つ.

問題 4.6.5.

(1) $yxy^{-1} = x^2$ より, $yx = x^2y$ なので, これを繰り返し使えば, x, y の位数がそれぞれ $7, 3$ であることから, G の任意の元は x^iy^j $(i = 0, 1, \ldots, 6, j = 0, 1, 2)$ と表せる.

(2) $\sigma = (1\ 2\ 3\ 4\ 5\ 6\ 7)$ とすれば, $\tau^{-1}(j) = i$ のときに $\tau\sigma\tau^{-1}(i+1) = j+2$ となることが必要なので, $\tau = (1\ 2\ 4)(3\ 5\ 6)$ とすれば, それを満たす. 逆に, このように定めれば, $\tau\sigma\tau^{-1} = \sigma^2$ が成り立つ.

(3) $\langle \sigma, \tau \rangle$ に対して, 定理 4.6.5 を使えば, $|G| \geq |\langle \sigma, \tau \rangle| = 21$ となるので従う.

問題 4.6.6.

G の元は x^iy^j $(0 \leq i \leq 12, 0 \leq j \leq 2)$ という形で表すことができるので, $|G| \leq 39$ であり, $x^iy^j = x^ky^l$ とすれば, $x^{i-j} = y^{l-k}$ となる. x, y はそれぞれ位数 $13, 3$ なので, $i-j$, $k-l$ はそれぞれ $13, 3$ の倍数である. したがって, $i = j, k = l$ となり, $|G| = 39$ である.

問題 4.6.7.

Q を四元数群とし,

$$F = \langle x, y \mid x^4 = y^4, x^2 = y^2, yxy^{-1} = x^3 \rangle$$

とする. 定理 4.6.5 より, 全射準同型 $\varphi : F \to Q$ が存在する. ここで, $\varphi(x) = i$, $\varphi(y) = j$ である. F の元は x^ny^m $(0 \leq i, j \leq 3)$ という形で表すことができ, その φ による像は i^nj^m となるが, $i^nj^m = 1$ と仮定すれば, $m = n = 0$ または $m = n = 2$ である. また, $x^2y^2 = 1$ なので, $\operatorname{Ker}\varphi = \{1\}$ であり, したがって, $F \cong Q$ が成り立つ.

問題 4.6.8.

(1) $\tau\nu = \sigma$ なので, $\sigma\tau\nu = 1$ は成り立つ.

$$\tau\nu = (1\ 3\ 4), \qquad \tau\nu^2 = (1\ 2\ 4)$$

であるから, これらと τ, ν で長さ 3 の巡回置換はすべて生成される. 補題 4.9.1 より, $\langle \sigma, \tau, \nu \rangle = A_4$ となる.

(2) まず, $HSy \subset HS$ を示す. S から $1, y, y^2$ を選ぶ場合は明らかなので, y^2z を選ぶ場合について考える. つまり, $z^u y^2 z y \in HS$ を示せばよいが, $x^2 = 1$, $xyz = 1$ より, $yz = x$ であり, これより, $yzyz = 1$ も導かれるので,

$$z^i y^2 z y = z^i y (z^{-1}y^{-1}) y = z^i y z^2 = z^i (z^{-1}y^{-1}) z = z^{i-1} y^2 z \in HS$$

が従う. 同様に, $HSz \subset HS$ も成り立つ.

(3) (2) より, 例えば

$$HSy^2 = (HSy)y \subset HSy \subset HSy$$

などとなるので, HS は積について閉じている. これと $x = yz = z^2y^2 \in HS$ より, $G = HS$ は従う. また, $|G| = |HS| \leq |H||S| = 12$ より, $|G| \leq 12$ も成り立つ.

(4) 定理 4.6.5 より, 全射準同型 $G \to A_4$ が存在し, (3) より, $|G| \leq |A_4|$ なので, $G \cong A_4$ である.

問題 4.6.9.

(1) $\tau\nu = \sigma$ より, $\sigma\tau\nu = 1$ が従う. また, 数字を適当に入れ替えることにより, $\sigma = (1\ 2)$, $\tau = (1\ 2\ 3\ 4)$ とみなすことができるので, 問題 2.3.9(2) より, $\mathfrak{S}_4$ は σ, τ, ν で生成される.

(2) まず, $HSy \subset HS$ を示す. S の元として $1, y, y^2, y^2z^2$ をとる場合は明らかなので, y^2z, y^2z^2y をとる場合を考える. 問題 4.6.9 と同様に関係式より, $yzyz = 1$ となるので,

$$y^2zy = y(z^{-1}y^{-1})y = yz^3 = (yz)z^2 = z^3y^2z^2 \in HS$$

であり,

$$y^2z^2y^2 = (zyz^{-1})y^2 = zy(z^{-1}y^{-1}) = zy^2z \in HS$$

となるので, HS は積について閉じている. また, $x = yz = y^2(y^2z) \in HS$ なので, $G = HS$ が成り立つ.

(3) 問題 4.6.9(4) と全く同様に証明できる.

問題 4.6.10.

(1) $\tau\nu = (12)(34)$ なので, $\sigma\tau\nu = 1$ が従う. また, 型が等しいことと共役であることは同値であることに注目して, $\nu^i\tau\nu^{-i}$, $(\nu^3\tau)^i\tau(\nu^3\tau)^{-i}$ を計算すれば, 長さ 3 の巡回置換がすべて生成されるので, 補題 4.9.1 より, $\langle \sigma, \tau, \nu \rangle = A_5$ となる.

(2) $H = \langle z \rangle$ とし, S[*2]を次のように定める.

$$S = \{1, y^2, y^2z^2, y^2z^2, y^2z^3, yz^3y, y^2z^2y, y^2z^2y^2, y^2z^2y^2z, y^2z^2y^2z^2, y^2z^2y^2z^2y\}.$$

まず, $HSy \subset HS$ であることを示す. $y^2z, y^2z^3y, y^2z^2y^2z, y^2z^2y^2z^2y$ 以外は明らかなので, これらについて示す.

[*2] S の求め方は Todd–Coxeter algorithm による. [2] を参考にした.

$\underline{y^2z}$　$y^2zy = y^2y^2z^4 = yz^4 = z^4y^2z^3 \in HS$.
$\underline{y^2z^3y}$　$y^2z^3y^2 = y^2z^4z^4y^2 = zy^2z \in HS$.
$\underline{y^2z^2y^2z}$

$$\begin{aligned}(y^2z^2y^2zy)(y^2z^2y^2z^2)^{-1} &= y^2z^2y^2zyz^3yz^3y\\ &= y^2z^2yz^2yz^3y\\ &= y^2zy^2zyz^3y\\ &= y^2zyz^2y\\ &= yzy = z^2 \in H\end{aligned}$$

より, $y^2z^2y^2zy = z^2y^2z^2y^2z^2 \in HS$.
$\underline{y^2z^2y^2z^2y}$

$$\begin{aligned}(y^2z^2y^2z^2y^2)(y^2z^2y^2z)^{-1} &= y^2z^2y^2z^2y^2z^4yz^3y\\ &= y^2z^2y^2z^3y^2z^3y\\ &= y^2z^2y^2z^4z^4y^2z^3y\\ &= y^2z^3y^2z^4y\\ &= y^2z^4y^2 = z \in H\end{aligned}$$

より, $y^2z^2y^2z^2y^2 = zy^2z^2y^2z \in HS$.
これらより, $HSy \subset HS$ が示された. 同様に, $HSz \subset HS$ も従うので, HS は積について閉じており, $x = yz = z^4y^2 \in HS$ より, $G = HS$ が成り立つ. これより, $|G| = |HS| \leq |H||S| = 60$ が従い,

$$F = \langle x, y, z \mid x^2 = z^3 = z^5 = xyz = 1\rangle$$

とすれば, (1) と定理 4.6.5 より, 全射準同型 $F \to A_5$ が存在するので, $F \cong A_5$ が成り立つ.

問題 4.6.11.

(1) ϕ は自己同型なので, $\phi(\sigma)$ は $1 \leq m \leq n/2$ として, m 個の互いに素な互換の積で表せる. 問題 4.2.6 より, $Z_{\mathfrak{S}_n(\sigma)}$ は正規部分群 $N \cong \mathbb{Z}/2\mathbb{Z}$ を含み,

$$Z_{\mathfrak{S}_n}(\sigma)/N \cong \mathfrak{S}_1 \times \mathfrak{S}_{n-2} \cong \mathfrak{S}_{n-2}$$

が成り立つ. さらに, $Z_{\mathfrak{S}_n}(\phi(\sigma))$ は正規部分群 $N' \cong (\mathbb{Z}/2\mathbb{Z})^m$ を含み,

$$Z_{\mathfrak{S}_n}(\phi(\sigma))/N' \cong \mathfrak{S}_m \times \mathfrak{S}_{n-2m}$$

も従う. ここで, ϕ が自己同型であることから, $\phi(Z_{\mathfrak{S}_n}(\sigma)) = Z_{\mathfrak{S}_n}(\phi(\sigma))$ であり,

$$2(n-2)! = |N||\mathfrak{S}_n| = |Z_{\mathfrak{S}_n}(\sigma)| = |Z_{\mathfrak{S}_n}(\phi(\sigma))| = |N'||\mathfrak{S}_m \times \mathfrak{S}_{n-2m}| = 2^m m!(n-2m)!$$

より,

$$(n-2)(n-3)\cdots(n-2m+1) = 2^{m-1}m! \tag{4.6.1}$$

となる. このとき, 左辺を $f_m(n)$ とすれば, 各 m について $f_m(n)$ は単調増加であり, $m \geq 3$ の場合には

$$f_m(2m) = (2m-2)! = 2^{m-1}(m-1)!(2m-3)(2m-5)\cdots 1 \geq 2^{m-1}m!$$

なので, $n=6$ かつ $m=3$ となる. $m=2$ の場合には式 (4.6.1) が成り立たないことが計算によりすぐに従うので, $2 \leq m \leq n/2$ について, 式 (4.6.1) が成り立つならば, $n=6$ となる. 今, $n \neq 6$ を仮定しているので, $m=1$ となり, 実際にこの場合には式 (4.6.1) は常に成り立つ. これより, $\phi(\sigma)$ は互換である.

(2) (1) と同様にして

$$(n-3)(n-4)\cdots(n-3m+1) = 3^{m-1}m! \tag{4.6.2}$$

が成り立つ. 左辺を $g_m(n)$ とすれば, 各 m について単調増加であり, $m=1$ の場合には式 (4.6.2) は常に成立する. $m \geq 2$ とすれば,

$$g_m(3m) = (3m-3)! = 3^{m-1}(m-1)!(3m-4)(3m-5)\cdots 2\cdot 1 \geq 3^{m-1}(m-1)!$$

なので, $n=6$ かつ $m=2$ となる. 今, $n \neq 6$ を仮定しているので, $m=1$ となり, したがって $\phi(\sigma)$ は長さ 3 の巡回置換である.

(3) $i \neq j$ とし, $\phi((1\ i)) = (a_1\ a_i)$, $\phi((1\ j)) = (a'_1\ a_j)$ とおく. $\{a_1, a_i\} \cap \{a'_1, a_j\} = \emptyset$ とすれば,

$$\phi((1\ i\ j)) = \phi((1\ i))\phi((1\ j)) = (a_1\ a_i)(a'_1\ a_j)$$

であるから, $\phi((1\ i\ j))$ の位数が 3 であることに反する. また, $\{a_1, a_i\} = \{a'_1, a_j\}$ の場合にも単射性に矛盾が生じる. 適当に記号を書き換えることにより, $\phi((1\ i)) = (a_1\ a_i)$ かつ $\phi((1\ j)) = (a_1\ a_j)$ と表せる. ここで, $k \neq i, j$, $\phi((1\ k)) = (\alpha\ \beta)$ とし, $a_1 \notin \{\alpha, \beta\} \cap \{a_1, a_i\}$ を仮定する. このとき, $\alpha = a_i$ としてよく, $a_i \neq a_j$ なので $\alpha \neq a_j$ である. また, $\alpha \notin \{\alpha, \beta\} \cap \{a_1, a_j\}$ でもあるので, $\alpha \neq a_j$ より, $\beta = a_j$ である. しかし,

$$\phi((1\ k)) = (a_i\ a_j) = (1\ a_i)(1\ a_j)(1\ a_i) = \phi((i\ j))$$

より, $(1\ k) = (i\ j)$ となり, $k \neq i, j$ に矛盾する. したがって, 主張は成立する.

(4) (3) より,

$$\phi((i\ i+1)) = \phi((1\ i)(1\ i+1)(1\ i)) = (a_1\ a_i)(a_1\ a_{i+1})(a_1\ a_i) = (a_i\ a_{i+1})$$

であり, 問題 2.3.9 より, $(a_i\ a_{i+1})$ という元全体は $\mathfrak{S}_n$ を生成する. また, $\tau \in \mathfrak{S}_n$ を任意の $1 \leq i \leq n$ に対して $\tau(i) = a_i$ が成り立つようなものとしてとれば, 補題 4.2.2 より, $\phi(\sigma) = \tau\sigma\tau^{-1}$ となるので, ϕ は内部自己同型である.

問題 4.6.12.

ϕ が自己同型であるためには $\sigma = \sigma_1\sigma_2\cdots\sigma_m$ と隣接互換の積で表したときに

$$\phi(\sigma) = \phi(\sigma_1)\phi(\sigma_2)\cdots\phi(\sigma_m)$$

となることが必要である. したがって, これにより ϕ を定義する. まず, ϕ が写像として well-defined であることを示す. τ_i を隣接互換として, $\sigma = \tau_1\tau_2\cdots\tau_k$ とすれば

$$\phi(\sigma) = \phi(\tau_1)\phi(\tau_2)\cdots\phi(\tau_k)$$

であり, 問題 4.6.4(3) より, $\mathfrak{S}_n$ の関係式は本質的に問題 4.6.4(1) で示されているものしか存在しないので, その関係式を適当に使えば, $\tau_1\tau_2\cdots\tau_k$ を $\sigma_1\sigma_2\cdots\sigma_m$ に変形することができる. また, 問題 4.6.4(1) で示されている関係式は準同型で送られた先でも成り立つので, 原像と同様に関係式を使って変形することにより, well-defined であることは従う. 次に, well-defined であることの証明と同様に単射であることが従い, 有限群の全射自己準同型であることから ϕ は自己同型であることが示された.

問題 4.7.1.

定理 4.5.7 より, Sylow-p 部分群 H と Sylow-2 部分群が K が存在するので, 位数 $p, 2$ の元 h, k はそれぞれ存在する. H は指数 2 の部分群なので問題 2.8.2 より正規部分群である. ゆえに, HK は G の部分群であり, $H, K \subset HK$ より $HK = G$ が成り立つ. ここで, $hk = kh$ ならば G は可換群となり矛盾するので, $hk \neq kh$ である. kh の位数が 2 でないと仮定すれば, kh の位数は p である. また, H は正規部分群なので, 定理 4.5.7 より, 唯一の Sylow-p 部分群であり, したがって $kh \in H$ となる. これより, $kh = h^i$ と表すことができるが, これは不合理なので, kh は位数 2 の元である. ゆえに, $khk = h^{-1}$ が成り立つ.

$$F_p = \langle x, y \mid x^p = y^2 = 1, yxy = x^{-1} \rangle$$

とすれば, 定理 4.6.5 より, 全射準同型 $F_p \to G$ が存在する. さらに, 問題 4.6.2 より, $F_p \cong D_p$ となるので, 特に $|F_p| = |D_p| = 2p$ である. したがって, $|G| = 2p = |F_p|$ となり, $F_p \cong G$ が従う. 以上から, $G \cong D_p$ である.

問題 4.7.2.

問題 4.7.1 と同様に, Sylow-7 部分群 H と Sylow-3 部分群が K が存在するので, 位数 $7, 3$ の元 h, k はそれぞれ存在する. $|G| = 21$ であることと, 定理 4.5.7 より, Sylow-7 部分群は一つしか存在しない. ゆえに, 正規部分群である. これより, HK は G の部分群であり, $H, K \subset HK$ より, $G = HK$ が成り立つ. ゆえに, $kh \neq hk$ である. H が正規部分群であることから, $khk^{-1} \in H$ となるので, $0 \leq i \leq 6$ を使って, $khk^{-1} = h^i$ と表すことができる. したがって,

$$h = k^3hk^{-3} = h^{i^3}$$

より, $h^{i^3-1} = 1$ となるので, $i^3 - 1$ は 7 の倍数である. これより, $i = 1, 2, 4$ のいずれかとなるが, $kh \neq hk$ より, $i = 2$ または $i = 4$ である. $i = 4$ の場合には k^2 を k と置きなおすことで, $khk^{-1} = h^2$ という関係式が成り立つ.

$$F = \langle x, y \mid x^7 = y^3 = 1, yxy^{-1} = x^2 \rangle$$

とすれば, 定理 4.6.5 より, 全射準同型 $F \to G$ が存在する. また, 問題 4.6.5 より, $|F| = 21 = |G|$ も成り立つので, $F \cong G$ となる.

問題 4.7.3.

問題 4.7.1 と同様に, Sylow-13 部分群 H と Sylow-3 部分群が K が存在するので, 位数 $12, 3$ の元 h, k はそれぞれ存在する. また, 問題 4.7.2 と同様に Sylow-13 部分群は一つしか存在しないので, H は正規部分群となり, $HK = G$ が従う. これより, $khk^{-1} \in H$ なので, $khk^{-1} = h^i$ となるような $0 \leq i \leq 12$ が存在するが,

$$h = k^3hk^{-3} = h^{i^3}$$

より, $i^3 - 1$ は 13 の倍数であり, これを満たすのは $i = 1, 3, 9$ である. $i = 1$ と仮定すれば, $hk \neq kh$ となるので, $G = HK$ であり, G が非可換群であることに反する. $i = 9$ の場合には k^2 を k と置きなおすことで, $khk^{-1} = h^3$ という関係式が成り立つ. あとは問題 4.7.2 と同様に, 定理 4.6.5 と問題 4.6.6 より, 主張が従う.

問題 4.7.4.

(1) 位数 8 の元をもてば, $G \cong \mathbb{Z}/8\mathbb{Z}$ となって可換群になるので矛盾.

(2) $G \setminus \{1\}$ の元の位数は 2 または 4 であるが, 任意の $G \setminus \{1\}$ の元について位数が 2 ならば問題 2.4.8 より可換群となって矛盾.

(3) $H := \langle x \rangle$ は指数 2 の部分群なので正規部分群であり, $yxy^{-1} \in H$ となる. ゆえに, $yxy^{-1} = x^i$ と表せる. また, $K = \langle y \rangle$ とすれば, H が正規部分群であることから HK は G の部分群である. $K, H \subset HK$ であり, $y \notin H$ なので, $|HK| > 4$ となる. ゆえに $HK = G$ が従う. これと G が非可換であることから, $xy \neq yx$ なので, $i \neq 1$ である. $i = 2$ と仮定すれば, $yx^2y^{-1} = 1$ より, $x^2 = 1$ となるので矛盾. したがって, $yxy^{-1} = x^{-1}$ である.

四元数群を Q と表し, 位数 8 の非可換群を分類する. G のうち, 位数 n の元の集合を $G(n)$ とおく.

$|G(4)| = 2$ のとき　このとき, $G(4) \subset H$ なので, y は位数 2 の元である. ゆえに,

$$F = \langle x, y \mid x^4 = y^2 = 1, yxy^{-1} = x^{-1} \rangle$$

とすれば, 定理 4.6.5 より全射準同型 $F \to G$ が存在する. さらに, 問題 4.6.2 より特に $|F| = |D_4| = 8 = |G|$ となるので, $F \cong G$ が従う. これと, 再び問題 4.6.2 より, $G \cong D_4$ である.

$|G(4)| \neq 2$ のとき　$|G(4)| + |G(2)| = 7$ となるので, このとき, y を位数 4 の元をとしてよい. x, y を入れ替えれば, $xyx^{-1} = y^{-1}$ も成り立ち, これより $x^2 = y^2$ が従うので,

$$F = \langle x, y \mid x^4 = y^4 = 1, x^2 = y^2, yxy^{-1} = x^{-1} \rangle$$

とすれば, 定理 4.6.5 より全射準同型 $F \to G$ が存在する. さらに, 問題 4.6.7 より特に $|F| = |Q| = 8 = |G|$ となるので, $F \cong G$ が従う. これと, 再び問題 4.6.7 より, $G \cong Q$ である.

問題 4.7.5.

位数 18 の群を G とする. G が可換群の場合には定理 4.8.2 より, G は $\mathbb{Z}/18\mathbb{Z}$ または $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ に同型であることが従う. 次に, G が非可換群の場合を考える. 定理 4.5.7 より, Sylow-3 部分群 H が存在し, H は指数 2 の部分群なので正規部分群である. Sylow-2 部分群を K とし, $k \in K$ を位数 2 の元とする. H が正規部分群であることから HK は G の部分群であり, $H, K \subset HK$ より, $G = HK$ となる. H は位数が 3^2 なので可換群であり, 定理 4.8.2 より $H \cong \mathbb{Z}/9\mathbb{Z}$ または $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ が成り立つ.

$H \cong \mathbb{Z}/9\mathbb{Z}$ のとき　位数 9 の元 $h \in H$ が存在する. H が正規部分群なので, $khk^{-1} = h^i$ と表すことができ,

$$h = k^2hk^{-2} = h^{i^2}$$

より, $h^{i^2-1} = 1$ となる. ゆえに, $i^2 - 1$ は 9 の倍数であり, これを満たすのは $i = 1, 8$ のみである. $i = 1$ のときには $kh = hk$ となって, $G = HK$ より G が可換群となってしまうので矛盾. したがって, $khk^{-1} = h^{-1}$ である.

$$F = \langle x, y \mid x^9 = y^2 = 1, yxy^{-1} = x^{-1} \rangle$$

とすれば, 定理 4.6.5 より全射準同型 $F \to G$ が存在し, $|F| = |D_9| = 18 = |G|$ なので, $F \cong G$ が従う. さらに, 問題 4.6.2 より, $G \cong D_9$ が成り立つ.

$H \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ のとき　a, b を $H = \langle a, b \rangle$ となるものとする. このとき, $H = \langle a, b \rangle$ かつ $G = HK$ であって, G は非可換なので, a, b の少なくとも一方は k と非可換になる. それを a とする. また, $\phi = \mathrm{Ad}(k)$ と定める.

$\underline{\phi(b) = b \text{ のとき}}$　$\phi(a) = a^i b^j$ とすれば,

$$a = \phi^2(a) = a^{i^2} b^j$$

より, $a^{1-i^2} = b^j$ が成り立つが, a, b の定義より, $i = 2, j = 0$ が従う. ゆえに, $kak^{-1} = a^{-1}$ であり, 定理 4.6.5 と問題 4.6.2 より, $\langle k, a\rangle \cong D_3$ が成り立つ. また, $G = HK$ と $H = \langle a\rangle\langle b\rangle$ より, $\langle k, a\rangle\langle b\rangle = G$ であり, $\langle k, a\rangle \cap \langle b\rangle = \{1\}$ となる. b は a, k と可換なので, $\langle k, a\rangle$, $\langle b\rangle$ は G の正規部分群となる. これらと命題 2.9.2 より $G \cong D_3 \times \mathbb{Z}/3\mathbb{Z}$ が成り立つ.

$\underline{\phi(b) \neq b \text{ のとき}}$　まず, a, b を $H = \langle a, b\rangle$ かつ $\phi(a) = a^{-1}$, $\phi(b) = b^{-1}$ を満たすようにとれることを示す. $\phi \in \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \cong \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ であって, ϕ に対応する行列を P とすれば, a, b に関する条件はある線形独立な $\alpha, \beta \in (\mathbb{Z}/3\mathbb{Z})^2$ が存在して,

$$P\alpha = -\alpha, \qquad P\beta = -\beta$$

となることである. これは, P が重複度 2 の固有値 -1 をもち, 対角化可能であることと同値である. P の最小多項式を m_P とすれば, $P^2 = 1$ より, $m_P(\lambda)$ は $\lambda^2 - 1$ を割り切るので,

$$m_P(\lambda) = \lambda + 1 \text{ または } m_P(\lambda) = \lambda^2 - 1$$

であり, P の最小多項式は重根を持たない. したがって, 対角化可能である. これらより, 条件を満たすような a, b が存在することが示された. 次に,

$$F = \langle x, y, z \mid x^3 = y^3 = z^2 = 1, xy = yx, zxz^{-1} = x^{-1}, zyz^{-1} = y^{-1}\rangle$$

とする. 上で示したことと定理 4.6.5 より, 全射準同型 $F \to G$ が存在する. また, F の関係式より, F の任意の元は $x^s y^t z^u$ という形で表すことができるので, $|F| \leq 18$ である. これより, $F \cong G$ となる.

問題 4.8.1.

$G \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/150\mathbb{Z} \times \mathbb{Z}/9000\mathbb{Z} \times \mathbb{Z}/27000\mathbb{Z}$.

問題 4.9.1.

$(1\ 2\ 3\ 4\ 5) = (1\ 5)(1\ 4)(1\ 3)(1\ 2)$ なので, $(1\ 2\ 3\ 4\ 5) = (1\ 4\ 5)(1\ 2\ 3)$.

問題 4.9.2.

(1) $\mathfrak{S}_n$ $(n = 2, 3, 4)$ について, 自明でない置換表現 $\rho_n : A_5 \to \mathfrak{S}_n$ をもつならば, $\mathrm{Ker}\,\rho_n \subset A_5$ はそれぞれ正規部分群となる. A_5 は単純群なので, ρ_n が自明でないことから $\mathrm{Ker}\,\rho_n = \{1\}$ となるが, $|A_5| > n!$ より, これは矛盾である.

(2) 位数 n の真部分群 H が存在するならば, $|A_5/H| = 60/n$ であり, $X = A_5/H$ とすれば, X への $a \cdot xH = (ax)H$ で定まる置換表現 $\rho : A_5 \to \mathfrak{S}_{60/n}$ が導かれる. 任意の $a \in A_5$ について, $a \cdot H = aH$ となることと, $|X| > 1$ より, この置換表現は自明ではない. したがって, $60/n \neq 2, 3, 4$ であり, $n \neq 15, 20, 30$ となる.

問題 4.9.3.

(1) 指数 2 の部分群を $H \subset \mathfrak{S}_n$ とする．このとき, $\mathfrak{S}_n/H$ は位数 2 の群なので可換であり, 命題 4.3.2 より $D(\mathfrak{S}_n) \subset H$ が成り立つ．ここで, 問題 4.2.10 で示したように $D(\mathfrak{S}_n) = A_n$ であるから, $A_n \subset H$ である．さらに, $|A_n| = |H|$ も成り立つので, $H = A_n$ となる．

(2) 仮定より, 自明でない置換表現 $\rho : G \to \mathfrak{S}_5$ が存在し, $\mathrm{Ker}\,\rho$ は G の正規部分群である．G は単純群であり, ρ は自明でないので, $\mathrm{Ker}\,\rho = \{1\}$ が成り立つ．これより, 部分群 $\rho(G) \subset \mathfrak{S}_5$ の位数は 60 である．これは指数 2 の部分群であることを示すので, (1) より, $G \cong A_5$ が成立する．

(3) G の Sylow-p 部分群 H_p の数を $n(p)$ とする．定理 4.5.7 より, $n(3) = 1, 4, 10$ であり, $n(3) = 1$ のときには H_3 が G の正規部分群となるので, G が単純群であることに反する．さらに, $n(3) = 4$ のときには $|N_G(H_3)| = 15$ となるので, 問題 4.9.2 の証明に反する．したがって, $n(3) = 10$ である．同様に, $n(5) = 1, 6$ であり, $n(5) = 1$ のときには H_5 が正規部分群になるので, G が単純群であることに反する．これより, $n(5) = 6$ である．

(4) G の位数 n の元の集合を $G(n)$ で表す．(3) より, $|G(3)| = 20$, $|G(5)| = 24$ なので, 位数が $3, 5$ 出ないものの数は $60 - 20 - 24 = 16$ である．

(5) $g_0 \in G$ を位数 10 の元とする．$\langle g_0 \rangle$ は位数 10 の部分群であり, Sylow-5 部分群 H_0 を含む．定理 4.5.7 より, Sylow-5 部分群はすべて共役であり, Sylow-5 部分群全体の集合を X とすれば, 任意の $H_i \in X$ $(i = 1, 2, \ldots, 5)$ について, ある $a_i \in G$ が存在して, $a_i H_0 a_i^{-1} = H_i$ が成り立つ．このとき, $a_i H_0 a_i^{-1}$ で表される部分群は相違なる Sylow-5 部分群をちょうど一つ含む, 位数 10 の巡回群である．ゆえに, それぞれの生成元を g_i で表せば, これらは相異なる元である．ここで, $H_i \cap H_j$ が位数 10 の元 g を含んでいると仮定すれば, g は g_i, g_j も生成するので, $H_i = H_j$ が成り立つ．また, H_i は位数 10 の元を 4 つ含むので, 位数 10 の元が 24 個存在することになり, 不合理である．したがって, G は位数 10 の元を持たない．

(6) $\langle x \rangle$ の位数は 2 なので, 定理 4.5.7 より, $\langle x \rangle$ はある Sylow-2 部分群 H に含まれる．また, $|H| = 4$ なので可換群となる．これより, $H \subset Z_G(x)$ となり, $Z_G(x)$ は位数が 4 の倍数であるような G の部分群となる．このとき, (2) と問題 4.9.2 の証明より, $|Z_G(x)| = 4$ が従う．

(7) $x \in H_1 \cap H_2$ とする．x の位数が 4 のとき, x は H_1, H_2 をそれぞれ生成するので, $H_1 \neq H_2$ に反する．また, x の位数が 2 のとき, $H_1 \cap H_2$ は H_1, H_2 の指数 2 の部分群なので, H_1, H_2 の正規部分群である．これより, $N_G(H_1 \cap H_2)$ は H_1, H_2 を部分群にもつので, 位数が 4 の倍数となる．さらに, $H_1, H_2 \subset N_G(H_1 \cap H_2)$ より, $|N_G(H_1 \cap H_2)| \geq 6$ となるので, その位数は 12 以上となる．しかし, これは (2) と問題 4.9.2 の証明に反するので, $H_1 \cap H_2 = \{1\}$ となる．

(8) Sylow-2 部分群の数を n とすれば, 定理 4.5.7 より, n は 60 の約数かつ奇数となる．さらに, 問題 4.9.2 と定理 4.5.7 より, $n \neq 2, 3, 4$ であり, $n = 1$ は G が単純群であることに反する．また, (4) より, Sylow-2 部分群を構成する元の数は 16 以下であるから, (7) によって $n \leq 5$ となる．以上より, $n = 5$ が導かれるが, このときには Sylow-2 部分群を H として, $|N_G(H)| = 12$ となるので, (2) より, $G \cong A_5$ が示される．

問題 4.9.4.

(1) $(1\ i\ j)(1\ j\ k) = (i\ j\ k)$ となるので, 長さ 3 の巡回置換はすべて生成される．これと補題 4.9.2 より, 主張は成り立つ．

(2) $\phi(\sigma)$ の位数は 3 なので, $\phi(\sigma)$ は互いに素な長さ 3 の巡回置換の積で表せる．これより, $n \leq 5$ のときには $\phi(\sigma)$ は長さ 3 の巡回置換となる．以下, $n \geq 7$ について考える．$\tau \in A_n$ と部分群 $G \subset \mathfrak{S}_n$ において

共役な元の集合を $C_G(\tau)$ で表せば, 定理 4.1.28 より,

$$|C_{A_n}(\tau)| = \frac{|A_n|}{|Z_{A_n}(\tau)|}, \qquad |C_{\mathfrak{S}_n}(\tau)| = \frac{|\mathfrak{S}_n|}{|Z_{\mathfrak{S}_n}(\tau)|}$$

が成り立つ. また, τ が互いに素な長さ 3 の巡回置換の積で表される時, 問題 4.2.7 より, $[Z_{\mathfrak{S}_n}(\tau) : Z_{A_n}(\tau)] = 2$ であり, これより, $|C_{\mathfrak{S}_n}(\tau)| = |C_{A_n}(\tau)|$ となる. 一方, 補題 4.2.2 より, 共役な元の自己同型による像は型が等しいので, $\phi(\sigma)$ は長さ 3 の巡回置換であることが従う.

(3) $\phi((1\ 2\ i)) = (a\ b\ c_1)$ のとき, $S_i = \{a, b, c_1\}$ などと定める. $i \neq j$ について, $|S_i \cap S_j| = 1, 3$ の場合, $\phi((1\ 2\ i)(1\ 2\ j))$ の位数が 2 となることに反するので, 矛盾. ゆえに,

$$|S_i \cap S_j| = 2$$

である. $S_j = \{a, b, c_2\}$ とおく. $(1\ 2\ i)$ と $(1\ 2\ j)$ の積をとり, その像の位数を考えれば, $\phi((1\ 2\ j)) = (a\ b\ c_2)$ なので, 主張は従う.

(4) $n = 3, 4$ の場合には明らかである. $n \geq 5$ の場合, $3 \leq k \leq n$ を $k \neq i, j$ なるものとしてとり, $\phi((1\ 2\ k))$ について考える. $T_i = S_i \cap S_k$ とすれば, $T_i = \{a, b\}, \{a, c_1\}, \{b, c_2\}$ のいずれかであり, $T_i = \{a, c_1\}$ と仮定すれば, $S_k = \{a, c_1, c_2\}$ となる. しかし, 積をとり, 像の位数を考えれば, 矛盾が生じる. $T_i = \{b, c_1\}$ と仮定しても同様に矛盾が導かれる. したがって, $T_i = \{a, b\}$ である. 再び積をとり, 像の位数を考えれば, 主張が従う.

(5) $\sigma \in \mathfrak{S}_n$ を $\sigma(i) = a_i$ を満たすようなものとしてとる. ϕ の単射性と (1), (4) より, σ は写像として well-defined である. これより, ϕ は $\mathfrak{S}_n$ の内部自己同型の制限であることが示された.

問題 4.10.1.

ρ の像に $(1\ 2), (2\ 3)$ が存在することを示せば十分である. $X = \{F_1, F_2, F_3\}$ とすれば, $(1\ 2)$ の場合について, F_3 の二面の中心を軸にして $\pi/2$ 回転させるような作用をする元 $g \in G$ は明らかに存在し, $\rho(g) = (1\ 2)$ となる. 同様に, $\rho(h) = (2\ 3)$ となるような $h \in G$ も存在するので, $\operatorname{Im}\rho = G$ となり, ρ は全射である.

参考文献

[1] 雪江明彦：代数学 1 群論入門, 日本評論社, 2010

[2] Ken Brown：The Toddo-Coxecter procedure, 2011,
http://pi.math.cornell.edu/~kbrown/6310/toddcox.pdf