代数系入門

第 2 章 群

今村勇輝

November 25, 2021

Def. 2.1

G : 集合, $G \neq \emptyset$, $* : G \times G \to G$: 二項演算

G が算法 $*$ について次の 3 条件を満たす $\overset{\text{def}}{\Leftrightarrow}$ G : **群**

- G1 $(a * b) * c = a * (b * c)$: 結合律
- G2 $\exists e \in G, \forall a \in G (e * a = a * e = a) \overset{\text{def}}{\Leftrightarrow} e$: **単位元**
- G3 $\forall a \in G, \exists b \in G (b * a = a * b = e) \overset{\text{def}}{\Leftrightarrow} a^{-1} := b$: a の**逆元**

乗法記号によって $a * b$ を ab と書く場合, 群 G は **乗法群**
加法記号によって $a + b$ と書く場合, 群 G は **加法群**

Thm. 2.1

- 単位元はただ一つである
- a の逆元は一意的に定まる
- $(a^{-1})^{-1} = a$

Def. 2.2

G : 群, $\forall a, \forall b \in G, ab = ba \overset{\text{def}}{\Leftrightarrow} G$: 可換群 または Abel 群

Exm. 1

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ は加法について群をなす.

Exm. 2

$\mathbb{Q}^* := \mathbb{Q} - \{0\}, \mathbb{R}^* := \mathbb{R} - \{0\}, \mathbb{C}^* := \mathbb{C} - \{0\}$
$\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ は乗法について群をなす ($\mathbb{Q}, \mathbb{R}, \mathbb{C}$ では成り立たない).

Thm. 1

$\forall a, b \in G, \exists! u, v \in G$ s.t. $au = b, va = b$

Def. 3.1

G : 群, $H \subset G$, $\cdot$: G の演算
H : $\cdot$ に関して群 $\overset{\text{def}}{\Leftrightarrow}$ $H \leq G$, H : **部分群**

Lem. D

$H \subset G$
$H \leq G \Leftrightarrow$

1. $e \in H$
2. $a, b \in H \Rightarrow ab \in H$
3. $a \in H \Rightarrow a^{-1} \in H$

Rem. 条件 1 は「$H \neq \emptyset$」に置き換えてもよい
H が有限の場合は条件 3 を取り除ける

Lem. E

$H \subset G, H \neq \emptyset, |H| < \infty$, H : $\cdot$ 関して閉じている $\Rightarrow H \leq G$

Thm. 3.1

$G \leq G, \{e\} \leq G$

Def. 3.2

$H \leq G, H \neq G, H \neq \{e\} \overset{\text{def}}{\Leftrightarrow} H : G$ の **真部分群**

Thm. 3.2

$H_1 \leq G, H_2 \leq G \Rightarrow H_1 \cap H_2 \leq G$

Exm. 1

$\mathbb{Z}, \mathbb{Q}$: 加法群, $\mathbb{Z} \leq \mathbb{Q}$

Exm. 2

0 でない有理数の乗法群 $\mathbb{Q}^*$ は 0 でない実数の乗法群 $\mathbb{R}^*$ の部分群である
絶対値が 1 である複素数全体のなす乗法群は乗法群 $\mathbb{C}^*$ の部分群である

Exm. 3

Thm. 3.3

$S \subset G, S \neq \emptyset, S^{-1} := \{x^{-1} \mid x \in S\}$
$H := \{x_1 x_2 \dots x_m \mid x_i \in S \cup S^{-1}\} \Rightarrow H \leq G$

Thm. 3.4

$S \subset H$
$\forall K \leq G, S \subset K \Rightarrow H \subset K$

H は S を含む「最小」の部分群.

Proof.

$\forall a \in H \Rightarrow a \in K$ を示す.
$a \in H$ なので $\exists x_i \in S \cup S^{-1}, \exists m \in \mathbb{N}$ s.t $a = x_1 \cdots x_m$.
$x_i \in S$ のとき $S \subset K$ なので $x_i \in K$.
$x_i \in S^{-1}$ のとき $x_i^{-1} \in S, S \subset K$ なので $x_i^{-1} \in K$.
$x_i^{-1} \in K$ と 補題 D(3) より $x_i \in K$.
$x_i \in K$ と 補題 D(2) より $a = x_1 \cdots x_m \in K$. よって成立. □

Def. 3.3

$H := \langle S \rangle$: S によって**生成**される G の部分群
S : H の **生成元の集合** または H の **生成系**

$S = \{a\}$ のとき 乗法 $\langle S \rangle = \{a^n \mid n \in \mathbb{Z}\}$, 加法 $\langle S \rangle = \{na \mid n \in \mathbb{Z}\}$

Exm. 4

$H = \langle -1 \rangle, H \leq \mathbb{R}^*$ のとき $H = \{1, -1\}$
$H = \langle i \rangle, H \leq \mathbb{C}^*$ のとき $H = \{1, -1, i, -i\}$

Exm. 5

$\mathbb{Z}$: 加法群
$m \in \mathbb{Z}, m\mathbb{Z} = \langle m \rangle, m\mathbb{Z} \leq \mathbb{Z}$ のとき $m\mathbb{Z} = \{0, \pm m, \pm 2m, \cdots\}$

Exm. 6

π : 平面, $d(P,Q)$: π の 2 点 P,Q の距離, 写像 $\phi\colon \pi \to \pi$ が全単射で

$$d(\phi(P),\phi(Q)) = d(P,Q)$$

が成り立つとき, ϕ : π の **運動**
運動の全体は対称群 $S(\pi)$ の 1 つの部分群をつくる : π の **運動群**

Exm. 7

シンメトリー : 図形をそれ自身に重ねるような平面の運動
正方形のシンメトリーの全体は, 運動群の 1 つの部分群をつくる.

Exm. 8

X : 集合, $\langle X\rangle \le S(X) \overset{\text{def}}{\Leftrightarrow} \langle X\rangle$: **置換群**

Def. 4.1

$H \leq G$

$a, b \in G$ が H を**法**として**左合同**, $a \equiv b \pmod{H} \overset{\text{def}}{\Leftrightarrow} a^{-1}b \in H$

Thm. 4.1

G における同値関係

1. $\forall a \in G, a \equiv a \pmod{H}$
2. $a \equiv b \pmod{H} \Rightarrow b \equiv a \pmod{H}$
3. $a \equiv b \pmod{H}, b \equiv c \pmod{H} \Rightarrow a \equiv c \pmod{H}$

Thm. 4.2

$C_a := \{x \mid a \equiv x \pmod{H}\} \Rightarrow C_a = \{ah \mid h \in H\}$

Def. 4.2

$aH := \{ah \mid h \in H\}$: a の**左剰余類**

Thm. 4.3

$a, b \in G, H \leq G$
$a^{-1}b \in H \Leftrightarrow aH = bH$
$ab^{-1} \in H \Leftrightarrow Ha = Hb$
$a \not\equiv b \pmod{H} \Rightarrow aH \cap bH = \emptyset$

Rem. H : 左剰余類 ($\because H = eH$)

Thm. 4.4

$\exists a_1, a_2, \cdots \in G$ s.t $G = a_1H \cup a_2H \cup \cdots, a_iH \cap a_jH = \emptyset, i \neq j$

$H \leq G$ のとき, G は H を法とする互いに交わらない (有限個または無限個) の左剰余類に分割される.

Def. 4.3

右合同 $\overset{\text{def}}{\Leftrightarrow} ab^{-1} \in H$
$Ha := \{ha \mid h \in H\}$: a の右剰余類

Thm. 4.5

$a, b \in G, \forall c \in G, cH = Hc$
$a^{-1}b \in H \Leftrightarrow ab^{-1} \in H$

Def. $a^{-1}b, ab^{-1} \in H \overset{\text{def}}{\Leftrightarrow} aH = Ha$: 剰余類

Thm. 4.6

G : 可換群, $\forall H \leq G \Rightarrow a^{-1}b, ab^{-1} \in H$

Rem. G : 加法群 のとき, $a + H = \{a + h \mid h \in H\}$

Exm. 1

$m \in \mathbb{Z}, m > 0, m\mathbb{Z} \leq \mathbb{Z}$: 加法群
$a, b \in \mathbb{Z}, a \equiv b \pmod{m\mathbb{Z}} \Rightarrow \exists n \in \mathbb{Z}$ s.t. $a - b = nm$

Def. 4.4

$(G : H) := |\{aH \mid a \in G\}|$: H の**指数**

Rem. 指数の定義を Ha の個数としても同じ. $(G : H) = |\{Ha \mid a \in G\}|$
Rem. $|G| < \infty \Rightarrow \forall H \leq G, (G : H) < \infty$
Exm. Exm.1 の $\mathbb{Z}$ について, $(\mathbb{Z} : m\mathbb{Z}) = m$

Def. 4.5

$o(G) := |G|$: G の**位数**

<u>Rem.</u> o は order の頭文字.

Lem. F

$H \leq G, |H| < \infty$
$\forall aH \subset G \Rightarrow |aH| = o(H)$

Thm. 2

$|G| < \infty$
$H \leq G \Rightarrow o(G) = (G : H) \cdot o(H)$

Cor. 2.1 (Lagrange)

$|G| < \infty$
$\forall H \leq G \Rightarrow o(H) | o(G)$

<u>Thm.</u> $(G : G) = 1, (G : e) = o(G)$ ($\because$ Thm.2)

Exm. 2

Thm. 4.7

$J_n = \{1, 2, \cdots, n\}$: 集合
$S_n = \{f \mid f : J_n \to J_n$: bijection$\}$: n 次対称群

$$o(S_n) = n!$$

剰余類分解と Thm.2 を使って証明する.
$n \geq 2, H \subset S_n, H = \{\sigma \mid \sigma(n) = n\}$
明らかに $H \leq S_n$
このとき, H を S_{n-1} とみなせる
$\sigma, \rho \in S_n, \sigma^{-1} \circ \rho \in H \Leftrightarrow \sigma(n) = \rho(n)$
$\tau_i : J_n$ の置換 s.t $\tau_i(n) = i, \tau_i(i) = n, 1 \leq i \leq n, i, n$ 以外は固定
$\tau_1, \cdots \tau_n$ について $\tau_i^{-1} \circ \tau_j \notin H, i \neq j$
一方, $\forall \sigma \in S_n, \sigma(n) = i$ ならば $\sigma^{-1} \circ \tau_i \in H$
ゆえに $S_n = \tau_1 H \sqcup \cdots \sqcup \tau_n H$
$o(S_n) = (S : S_{n-1}) \cdot o(S_{n-1})$

Def. 5.1

$H \lhd G$ の**正規部分群** $\overset{\text{def}}{\Leftrightarrow} \forall a \in G, aH = Ha$

Thm. 5.1

G : 可換群 $\Rightarrow \forall H \leq G, H \lhd G$

Thm. 5.2

$\forall G, G \lhd G, \{e\} \lhd G$

Exm. 1

$\forall G, Z = \{x \in G \mid \forall a \in G, ax = xa\} \Rightarrow Z \lhd G$

Def. 5.2

$Z(G) := Z : G$ の **中心**

Rem. G : 可換群 $\Rightarrow Z(G) = G$

Exm. 2

$S_n : J_n$ 上の対称群, $H = \{\sigma \in S \mid \sigma(n) = n\}, H \leq S_n$
$n \geq 3 \Rightarrow H \ntriangleleft S_n$

交換子群

Lem. G

$H \triangleleft G \Leftrightarrow \forall a \in G, \forall x \in H, axa^{-1} \in H$

Exm. 3

$a, b \in G$
$aba^{-1}b^{-1} \in G$: **交換子**
$D(G) := \langle \{aba^{-1}b^{-1} \mid a, b \in G\} \rangle$: **交換子群**

Thm. 5.3

$\forall H, D(G) \subset H \Rightarrow H \triangleleft G$

Rem. G : **可換群** $\Rightarrow D(G) = \{e\}$

Def. 5.3

$S, S' \subset G, S \neq \emptyset, S' \neq \emptyset$
$SS' := \{xx' \mid x \in S, x' \in S'\}$: S, S' の**積**

Rem.

- 加法記号の場合, $S + S'$
- $S = \{x\}$ の場合, xS'
- $S' = \{x'\}$ の場合, Sx'

Thm. 5.4

$S_1, S_2, S_3 \subset G, S_1 \neq \emptyset, S_2 \neq \emptyset, S_3 \neq \emptyset$
$S_1(S_2S_3) = (S_1S_2)S_3 = \{x_1x_2x_3 \mid x_1 \in S_1, x_2 \in S_2, x_3 \in S_3\}$

Exm. 4

$H \leq G \Rightarrow HH = H$

Thm. 3

$a, b \in G$
$N \triangleleft G \Rightarrow (aN)(bN) = abN$ かつ $\{aN \mid a \in G\}$: 群

Def. 5.4

$G/N := \{aN \mid a \in G\}$: G の N による **剰余群** (または **商群**)

Rem. N : 単位元, $a^{-1}N$: aN の逆元
Rem. G : 可換群 $\Rightarrow \forall N, G/N$: 可換群

Thm. 5.5

$N \triangleleft G$
$(G : N) < \infty \Rightarrow o(G/N) = (G : N)$

Thm. 5.6

$$|G| < \infty \Rightarrow o(G/N) = \frac{o(G)}{o(N)}$$

Def. 5.5

$n > 0, n \in \mathbb{Z}, \mathbb{Z}$: 加法群, $n\mathbb{Z} \leq \mathbb{Z}$
$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$

Exm. 5

$o(\mathbb{Z}_n) = n$
$N = n\mathbb{Z}, k \in \mathbb{Z}$
$\overline{k} := k + N$
$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \cdots \overline{n-1}\}$
$\mathbb{Z}_4$ の場合,

$$\overline{0} + \overline{1} = \overline{1}, \overline{1} + \overline{1} = \overline{2}, \overline{2} + \overline{1} = \overline{3}, \overline{3} + \overline{1} = \overline{0}$$

Thm. 4

$N \lhd G$
G/N : 可換群 $\Leftrightarrow D(G) \subset N$

Def. 6.1

$f: G \to G'$: **準同型写像** (hom.) $\overset{\text{def}}{\Leftrightarrow} \forall x, y \in G, f(xy) = f(x)f(y)$

Rem. 群の算法の種類には関係ない.
Exm. G : 加法群, G' : 乗法群, $f(x+y) = f(x)f(y)$

Exm. 1

$\forall G, G', e' \in G'$
$f(x) = e' \Rightarrow f$: hom.
Rem. f : trivial な準同型写像

Exm. 2

Rem. $\mathbb{R}^+ := \{x \in \mathbb{R} \mid x > 0\}, \mathbb{R}^*$: 乗法群 $\Rightarrow \mathbb{R}^+ \leq \mathbb{R}^*$
$\mathbb{R}$: 加法群

- $f: \mathbb{R} \to \mathbb{R}^+, x \mapsto 2^x \Rightarrow f$: hom. ($\because 2^{x+y} = 2^x 2^y$)
- $f: \mathbb{R}^+ \to \mathbb{R}, x \mapsto \log_2 x \Rightarrow f$: hom. ($\because \log_2 xy = \log_2 x + \log_2 y$)

Exm. 3

$a \in G, n \in \mathbb{Z}, \mathbb{Z}$: **加法群**
$f : n \mapsto a^n \Rightarrow f$: hom.($\because a^{m+n} = a^m a^n$)

Exm. 4

$z \in \mathbb{C}, z \neq 0$
$f : \mathbb{C}^* \longrightarrow \mathbb{R}^+, z \mapsto |z| \Rightarrow f$: hom.

Exm. 5

$N \lhd G, a \in G$
$\varphi : G \longrightarrow G/N, a \mapsto aN \Rightarrow \varphi$: hom.
$\because \varphi(ab) = abN = (aN)(bN) = \varphi(a)\varphi(b)$
<u>Def.</u> φ : **標準的準同型写像** または **自然な準同型写像**

Thm. 6.1

$f: G \to G', g: G' \to G''$: hom.

- $e \in G, e' \in G', f(e) = e'$
- $\forall x \in G, f(x^{-1}) = f(x)^{-1}$
- $g \circ f : G \to G''$: hom.

Rem. 準同型写像を省略して準同型と呼ぶときもある

Def. 6.2

$f: G \to G' : hom.$

- f : 単射 : **単射準同型** (injective hom.)
- f : 全射 : **全射準同型** (surjective hom.)
- f : 全単射 : **同型写像** または **同型** (iso.)

Thm. 6.2

$f: G \to G'$: iso. $\Rightarrow f^{-1} : G' \to G$: iso.

Def. 6.3

$G \cong G'$: **同型** $\overset{\text{def}}{\Leftrightarrow} \exists f : G \to G'$: iso.

Thm. 6.3

- $G \cong G$
- $G \cong G' \Rightarrow G' \cong G$
- $G \cong G', G' \cong G'' \Rightarrow G \cong G''$

Exm. 6

$\mathbb{R} \cong \mathbb{R}^{+}$ ($\because$ Exm.2)

Thm. 6.4

$f : G \to G'$: hom. $\Rightarrow f(G) \leq G'$

Rem. 単射準同型は, G から G' の **中への同型写像** とも呼ばれる

Def. 6.4

f : hom.
$\ker f := \{x \in G \mid f(x) = e'\}$: f の **核** (kernel)

Thm. 6.5

$\ker f \lhd G$

Exm. 7

$N \lhd G, \varphi : G \to G/N \Rightarrow \ker \varphi = N$

Thm. 5

$f\colon G \to G'$: hom., $\ker f = N, a, b \in G$
$f(a) = f(b) \Leftrightarrow a \equiv b \pmod N$

Cor. 5.1

$f\colon G \to G'$: hom.
f : *injective* $\Leftrightarrow \ker f = \{e\}$

Thm. 6.6

$f\colon G \to G'$: hom., $\ker f = N, f(G) = G'_0, g\colon G/N \to G'_0, aN \mapsto f(a)$
$\Rightarrow g$: bijective(∵ Thm.5)

<u>Def.</u> g : f から誘導される全単射

Thm. 6 (準同型定理)

$f\colon G \to G'$: hom., $\ker f = N \Rightarrow g\colon G/N \to f(G)$: iso.$(G/N \cong f(G))$

Exm. 8

$f\colon \mathbb{C}^* \to \mathbb{R}^+, z \mapsto |z|$: hom.,$f(\mathbb{C}^*) = \mathbb{R}^+, \mathbb{T} := \ker f = \{z \in \mathbb{C}^* \mid |z| = 1\}$
$\mathbb{C}^*/\mathbb{T} \cong \mathbb{R}^+ (\because$ Thm.6)

Def. $z(\theta) := e^{i\theta} = \cos\theta + i\sin\theta$
Rem. $z(\theta_1)z(\theta_2) = z(\theta_1 + \theta_2)$

Exm. 9

$\mathbb{R}, \mathbb{Z}$: 加法群,$f\colon \mathbb{R} \to \mathbb{T}, \theta \mapsto z(2\pi\theta)$: hom.
$\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$
$\because f(\mathbb{R}) = \mathbb{T}, \ker f = \mathbb{Z}, (\because \theta \in \mathbb{Z} \Rightarrow z(2\pi\theta) = 0)$

Rem. $\mathbb{R}/\mathbb{Z}, \mathbb{T}$: 1 次元の トーラス群

Exm. 10

$I\colon G \to G, I(G) = G, \ker I = \{e\}, f$: Exm.1,$f(G) = \{e\}, \ker f = G$
$G/\{e\} \cong G, G/G \cong \{e\}$

Def. 6.5

G' : G の **準同型像** $\overset{\text{def}}{\Leftrightarrow} \exists f : G \to G'$: surjective hom.

Cor. 6.1

G' : G の準同型像 $\Leftrightarrow \exists N \lhd G$ s.t. $G' \cong G/N$

Def. 6.6

G : **単純群** $\overset{\text{def}}{\Leftrightarrow} \forall N \lhd G, N = \{e\}$ or G

Lem. H

$f : G \to G'$: surjective hom.
$H \leq G$ $(H \lhd G) \Rightarrow f(H) \leq G'$ $(f(H) \lhd G')$
$H' \leq G'$ $(H' \lhd G') \Rightarrow f^{-1}(H') \leq G$ $(f^{-1}(H') \lhd G)$

Thm. 7 (第 1 同型定理, 第 3 同型定理)

$f\colon G \to G'$: surjective hom., $\ker f = N$
$\Omega = \{H \mid H \leq G, N \subset H\}, \Omega' = \{H' \mid H' \leq G'\}$
$\varphi\colon \Omega \to \Omega'(H \mapsto f(H)), \varphi'\colon \Omega' \to \Omega(H' \mapsto f^{-1}(H'))$
(a1) φ, φ': bijection, $\varphi^{-1} = \varphi'$
(a2) (a1) の対応において, $H/N \cong H'$
(b1) $f(H) = H', f^{-1}(H') = H, H \lhd G \Leftrightarrow H' \lhd G'$
(b2) $G/H \cong G'/H' \cong (G/N)/(H/N)$

Exm. 6.1

$G = \mathbb{Z}, H = 3\mathbb{Z}, N = 12\mathbb{Z} \Rightarrow (\mathbb{Z}/12\mathbb{Z})/(3\mathbb{Z}/12\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z}$
$a, b \in \mathbb{N}, a|b \Rightarrow (\mathbb{Z}/b\mathbb{Z})/(a\mathbb{Z}/b\mathbb{Z}) \cong \mathbb{Z}/a\mathbb{Z}$

Thm. 8 (第 2 同型定理)

$\forall H \leq G, N \lhd G \Rightarrow$

- $HN \leq G, H \cap N \lhd H$
- $H/(H \cap N) \cong HN/N$

Exm. 6.2

$G = \mathbb{Z}, H = 6\mathbb{Z}, N = 10\mathbb{Z} \Rightarrow 6\mathbb{Z}/30\mathbb{Z} \cong 2\mathbb{Z}/10\mathbb{Z}$
$a, b \in \mathbb{Z}, lcm(a, b) = l, gcd(a, b) = m \Rightarrow a\mathbb{Z}/l\mathbb{Z} \cong m\mathbb{Z}/b\mathbb{Z}$

Def. 7.1

$f : G \to G$: iso. $\overset{\text{def}}{\Leftrightarrow}$ $f : G$ の**自己同型写像**または**自己同型** (automorphism)

Exm. 7.1

$I_G : G \to G$: aut.

Thm. 7.1

f, g : aut. $\Rightarrow f \circ g, f^{-1}$: aut.

Thm. 7.2

$Aut(G) := \{f \in S(G) \mid f : \text{aut.}\} \leq S(G)$

Def. 7.2

$Aut(G)$: G の**自己同型群**

Exm. 1

G:可換群, $f : G \to G (x \mapsto x^{-1}) \Rightarrow f$: aut.
$\because f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = f(x)f(y)$

Lem. I

$a \in G, \sigma_a : G \to G, x \mapsto axa^{-1} \Rightarrow \sigma_a \in Aut(G)$

Rem. σ_a が I_G と一致するのは, $a \in Z(G)$ のとき ($\because axa^{-1} = x, ax = xa$)

Def. 7.3

$\sigma_a : G$ の**内部自己同型**

Def. 7.4

$a, b \in G, \exists s \in G$ s.t. $\sigma_s(a) = sas^{-1} = b \overset{\text{def}}{\Leftrightarrow} a \sim b : a$ は b に**共役**

Thm. 7.3

$a, b, c \in G$

1. $a \sim a$
2. $a \sim b \Rightarrow b \sim a$
3. $a \sim b, b \sim c \Rightarrow a \sim c$

Def. 7.5

$a \in G, C_a := \left\{xax^{-1} \mid x \in G\right\}$: a の**共役類**

Def. 7.6

$a \in G, N(a) := \{x \in G \mid ax = xa\}$: G の a による**正規化群**

Thm. 7.4

$N(a) \leq G$

Lem. J

$|G| < \infty, |C_a| = (G : N(a))$

Thm. 9

$|G| < \infty, Z = Z(G), C := \{a \in C_a \mid a \in G \setminus Z\}$
$o(G) = o(Z) + \Sigma_{a \in C}(G : N(a))$: **類等式**

Def. 7.7

p : 素数, $n \geq 1, o(G) = p^n \overset{\text{def}}{\Leftrightarrow} G : p$ 群

Exm. 2

$G : p$ 群 $\Rightarrow \exists a \in Z(G)$ s.t. $a \neq e$

Exm. 3

$o(G) = p^2 \Rightarrow G$: 可換群

Def. 7.8

$S, S' \leq G, \exists a \in G$ s.t. $\sigma_a(S) = aSa^{-1} = S' \overset{\text{def}}{\Leftrightarrow} S$ は S' に共役

Thm. 7.5

$S, T, U \leq G$

1. $S \sim S$
2. $S \sim T \Rightarrow T \sim S$
3. $S \sim T, T \sim U \Rightarrow S \sim U$

Thm. 7.6

$H \leq G, a \in G \Rightarrow \sigma_a(H) = aHa^{-1} \leq G$

Def. 7.9

$\sigma_a(H)$: **共役部分群**

Thm. 7.7

$H \lhd G \Leftrightarrow H \leq G, a \in G, H = \bigcup C_a$

Thm. 7.8

$H \lhd G \Leftrightarrow \forall a \in G, \sigma_a(H) = H$

Rem. $n \in \mathbb{Z}, n \geq 0, n\mathbb{Z} \leq \mathbb{Z}$ ($\because$ §3 Exm.5)

Lem. K

$\forall A \leq \mathbb{Z} \Rightarrow \exists n \in \mathbb{Z}$ s.t. $n \geq 0, A = n\mathbb{Z}$

Def. 8.1

$a \in G, G = \left\{a^k \mid k \in \mathbb{Z}\right\} \overset{\text{def}}{\Leftrightarrow} G := \langle a \rangle$: **巡回群**
$a : G$ の**生成元**

Rem. 加法群の場合, $\langle a \rangle = \{ka \mid k \in \mathbb{Z}\}$

Exm. 8.1

$\mathbb{Z} = \langle 1 \rangle, n\mathbb{Z} = \langle n \rangle$
$\mathbb{Z}_n = \langle 1 + n\mathbb{Z} \rangle, o(\mathbb{Z}_n) = n$: 有限巡回群

Thm. 10

G, H : 巡回群

- $o(G) = \infty \Rightarrow G \cong \mathbb{Z}$
- $o(H) = n \Rightarrow H \cong \mathbb{Z}_n$

Exm. 1

$G = \langle i \rangle = \langle -i \rangle = \{1, i, -1, -i\}$

Thm. 8.1

$a \in G \Rightarrow \langle a \rangle \leq G$

Def. 8.2

$a \in G, \langle a \rangle \leq G$

$n > 0, \langle a \rangle \cong \mathbb{Z}_n \overset{\text{def}}{\Leftrightarrow} o(a) = n$: a の**位数**または**周期**

$\langle a \rangle \cong \mathbb{Z} \overset{\text{def}}{\Leftrightarrow} a$: **無限位数**の元

Rem. 位数が 1 の元は単位元

Exm. 2

Exm.1 において $o(-1) = 2, o(i) = o(-i) = 4$

Thm. 11

$o(G) < \infty, \forall a \in G \Rightarrow o(a) | o(G)$

Cor. 11.1

$o(G) = n \Rightarrow \forall a \in G, a^n = e$

Thm. 12

G : 巡回群, $\forall H \leq G \Rightarrow H$: 巡回群

Def. 9.1

$J_n = \{1, 2, \cdots, n\}$, $S_n : J_n$ 上の n 次対称群

$$\tau \in S_n, \tau : \begin{cases} i \mapsto j & \\ j \mapsto i & (j \neq i) \\ k \mapsto k & (k \neq i, k \neq j) \end{cases} \overset{\text{def}}{\Leftrightarrow} \tau = (i\ j) : J_n \text{ 上の互換}$$

Rem. τ : 互換 $\Rightarrow \tau = \tau^{-1}$

Lem. L

$\forall \sigma \in S_n, n \geq 2 \Rightarrow \exists \tau_1, \cdots, \tau_s \in S_n$: 互換 s.t. $\sigma = \tau_1 \cdots \tau_s$

Exm. 1

次の置換を互換の積で表す.

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

Def. 9.2

$n \geq 2, \Omega := \{\{i,j\} \mid i,j \in J_n, i \neq j\}, \sigma \in S_n$

$$\varepsilon(\sigma) := \prod_{\{i,j\} \in \Omega} \frac{\sigma(i) - \sigma(j)}{i - j} : \sigma \text{ の符号}$$

Rem. $\varepsilon(\sigma)$ は $\mathrm{sgn}(\sigma)$ とも書かれる.

Thm. 13

$n \geq 2$

- $\forall \sigma \in S_n \Rightarrow \varepsilon(\sigma) = 1$ または $\varepsilon(\sigma) = -1, \varepsilon : S_n \to \{1, -1\}$: hom.
- $\forall \tau \in S_n$: 互換 $\Rightarrow \varepsilon(\tau) = -1$

Def. 9.3

$n \geq 2, \sigma \in S_n$

$\varepsilon(\sigma) = 1 \overset{\text{def}}{\Leftrightarrow} \sigma$: **偶置換**, $\varepsilon(\sigma) = -1 \overset{\text{def}}{\Leftrightarrow} \sigma$: **奇置換**

Rem. $\forall \tau \in S_n$: 互換 $\Rightarrow \tau$: 奇置換 ($\because$ Thm. 13)

Cor. 13.1

$\sigma \in S_n, \exists \tau_1, \cdots, \tau_s \in S_n$: 互換 s.t. $\sigma = \tau_1 \cdots \tau_s$
σ : 偶置換（奇置換）$\Rightarrow s$: 偶数（奇数）

Cor. 13.2

$n \geq 2, \Omega_e = \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\}, \Omega_o = \{\sigma \in S_n \mid \varepsilon(\sigma) = -1\}$

- $A_n := \Omega_e, A_n \lhd S_n$: n 次の交代群
- $o(\Omega_e) = o(\Omega_o) = n!/2$

Exm. 9.1

$A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\}$

Def. 9.4

$i_1, \cdots, i_r \in J_n (r \geq 2, i_i \neq i_j)$
$\sigma \in S_n, \sigma(i_1) = i_2, \sigma(i_2) = i_3, \cdots, \sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1, \sigma(i_k) = i_k (r < k \leq n)$
$\overset{\text{def}}{\Leftrightarrow} \sigma = (i_1\ i_2\ \cdots\ i_r)$: **長さ r の巡回置換 (サイクル)**, r-巡回置換
$J_n(\sigma) := \{i_1, i_2, \cdots, i_r\}$: σ の**巡回域**

Rem. 互換: 2-巡回置換, e: 1-巡回置換

Thm. 9.1

$\sigma \in S_n$: r-巡回置換, $\forall i \in J_n(\sigma) \Rightarrow \sigma = (i\ \sigma(i)\ \sigma^2(i)\ \cdots\ \sigma^{r-1}(i))$

Def. 9.5

$\sigma, \sigma' \in S_n$: 巡回置換, $J_n(\sigma) \cap J_n(\sigma') = \emptyset \overset{\text{def}}{\Leftrightarrow} \sigma, \sigma'$ は**互いに素**

Thm. 9.2

$\sigma, \sigma' \in S_n$: 互いに素 $\Rightarrow \sigma\sigma' = \sigma'\sigma$

Def. 9.6

$\forall \sigma \in S_n, i, j \in J_n, \exists \alpha \in \mathbb{Z}$ s.t. $\sigma^{\alpha}(i) = j \overset{\text{def}}{\Leftrightarrow} i \underset{\sigma}{\equiv} j$

$T_i := \{i \in J_n \mid i \underset{\sigma}{\equiv} j\}$: σ に関する**推移類**

Lem. M

$\forall \sigma \in S_n \Rightarrow \exists! \sigma_1, \cdots, \sigma_k \in S_n$: 巡回置換 s.t. $\sigma = \sigma_1 \cdots \sigma_k \quad (\sigma_i, \sigma_j$: 互いに素)

$\sigma = \sigma_1 \cdots \sigma_k$: σ の**標準分解**

Exm. 2

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 3 & 9 & 4 & 7 & 2 & 1 & 8 & 6 \end{pmatrix} = (1\ 5\ 7)(2\ 3\ 9\ 6)(4)(8)$$

Def. 9.7

$\sigma \in S_n, \sigma = \sigma_1 \cdots \sigma_k$: σ の標準分解
$r_1, \cdots, r_k$: σ_i の長さ, $r_1 \geq \cdots \geq r_k, r_1 + \cdots + r_k = n$
$\overset{\text{def}}{\Leftrightarrow} [r_1, \cdots, r_k]$: σ の**分解型**

Thm. 14

$\sigma, \sigma' \in S_n, [r_1, \cdots, r_k]$: σ の分解型, $[r'_1, \cdots, r'_k]$: σ' の分解型
$\sigma \sim \sigma' \Leftrightarrow [r_1, \cdots, r_k] = [r'_1, \cdots, r'_k]$

Def. 9.8

$n \in \mathbb{Z}, n > 0, \exists r_1, \cdots, r_k \in \mathbb{Z}$ s.t. $r_1 \geq \cdots \geq r_k > 0, n = r_1 + \cdots + r_k$
$\overset{\text{def}}{\Leftrightarrow} [r_1, \cdots, r_k]$: n の**分割**
$p(n)$: n の分割の数

Cor. 14.1

S_n の共役類の個数 $= p(n)$

Def. 10.1

$a \in G, T_a\colon G \to G, T_a(x) = ax \overset{\text{def}}{\Leftrightarrow} T_a : a$ による G の左移動

Thm. 10.1

$T_a \in S(G)$

Thm. 15 (Cayley)

X : 集合, $\forall G$: 群 $\Rightarrow \exists S' \leq S(X)$ s.t. $G \cong S'$

Def. 10.2

X : 集合, $\rho\colon G \to S(X)$: hom. $\overset{\text{def}}{\Leftrightarrow} \rho : G$ の X における置換表現

ρ : injective hom. $\overset{\text{def}}{\Leftrightarrow} \rho$: 忠実な置換表現

Thm. 10.2

$a \in G, x \in X, \rho : G$ の X における置換表現, $a \cdot x := (\rho(a))(x) \Rightarrow$

1. $e \in G, \forall x \in X \Rightarrow e \cdot x = x$
2. $\forall a, b \in G, \forall x \in X \Rightarrow ab \cdot x = a \cdot (b \cdot x)$

Thm. 10.3

写像 $G \times X \to X, (a, x) \mapsto a \cdot x$ は Thm. 10.2 (1)(2) を満たす. $\Rightarrow$
$\forall a \in G, \rho(a) : X \to X, \rho(a) \in S(X), \rho : G \to S(X)$: hom.

Def. 10.3

Thm. 10.2 (1)(2) を満足する写像 $G \times X \to X, (a, x) \mapsto a \cdot x : G$ の X への**作用**
G の 1 つの作用が与えられた X : **G-集合**

Exm. 1

$T\colon G \to S(G)$: 群 G の集合 G における忠実な置換表現
作用の意味の $a \cdot x$ は G における積としての ax

Rem. T : G の左正則表現

Exm. 2

σ_a : G の内部自己同型, $\sigma\colon G \to S(G), a \mapsto \sigma_a$: G の G における置換表現
作用の意味の $a \cdot x$ は G における積としての axa^{-1}

Exm. 3

$\forall H \leq G, G/H := \{aH \mid a \in G\}$ ($H \ntrianglelefteq G$ のときこれは群ではない)
$a \in G, xH \in G/H, a \cdot xH = axH$: G の G/H への作用
この作用により, G の G/H における 1 つの置換表現, G/H に G-集合としての 1 つの構造が与えられる.

Rem. $H = \{e\}$ のとき, G の G/H における置換表現は G の左正則表現.

Rem. 今後, 混乱する恐れがなければ, $ax := a \cdot x$

Thm. 10.4

X : G-集合, $x, y \in X, \exists a \in G$ s.t. $ax = y \overset{\text{def}}{\Leftrightarrow} x \sim y \Rightarrow \sim$: X における同値関係

Def. 10.4

$C_x := \{y \in X \mid x \sim y\}$: G-集合 X の**推移類**または**軌道** **(orbit)**

Thm. 10.5

$Gx := \{ax \mid a \in G\} \Rightarrow C_x = Gx$

Def. 10.5

$\forall x, y \in X, \exists a \in G$ s.t. $ax = y$: G の X への作用 (とそれに対応する G の置換表現) は**推移的** **(transitive)**
上記を満たす X : **推移的** G-集合 または **等質** G-集合

Exm. 4

Exm. 2 の意味で群 G を G-集合と考えるとき, その推移類は G の共役類

Exm. 5

Exm. 3 で述べた G の G/H への作用は推移的
$\because\ \forall xH, yH \in G/H, yx^{-1} \cdot xH = yH$

Def. 10.6

X, X' : G-集合, ρ, ρ' : X, X' の置換表現

1. $\varphi : X \to X'$: bij., $\forall a \in G, \forall x \in X \Rightarrow \varphi(ax) = a\varphi(x) \overset{\text{def}}{\Leftrightarrow} \varphi$: **G-同型写像**
2. φ : G-同型写像のとき, ρ, ρ' は**同値**

$$\begin{array}{ccc} X \ni x & \xmapsto{\rho(a)} & ax \in X \\ \varphi \downarrow & & \downarrow \varphi \\ X' \ni \varphi(x) & \xmapsto{\rho'(a)} & a\varphi(x) = \varphi(ax) \in X' \end{array}$$

Thm. 16

X : 推移的な G-集合, $x_0 \in X, H = \{a \in G \mid ax_0 = x_0\}$

1. $H \leq G$: x_0 の**安定部分群** (stabilizer) または**固定群**
2. G の X における表現は G の G/H における表現と同値

Cor. 16.1

X : 推移的な G-集合, $|X| < \infty, H \leq G$: $x_0 \in X$ の安定部分群
$(G : H) = |X|$

Rem. X : G-集合 $\Rightarrow \forall C_x$: 推移的な G-集合

Thm. 10.6

X : G-集合, $|X| = n, X_1, \cdots, X_k$: X の推移類,
$x_i \in X_i (1 \leq i \leq k)$: X_i の代表元, H_i : x_i の安定部分群

$$\Rightarrow n = \sum_{i=1}^{k} (G : H_i)$$: X の**推移類分解等式**または**軌跡分解等式**

Rem. Exm. 2 の軌跡分解等式は有限群の類等式 (§7 Thm. 9)

Thm. 17

$H \leq G, \rho\colon G \to S(G/H)$: 置換表現, $N = \ker\rho$

1. $N \subset H$
2. $\forall N_1 \lhd G, N_1 \subset H \Rightarrow N_1 \subset N$

Cor. 17.1

$\rho\colon G \to S(G/H)$: 忠実 $\Leftrightarrow \forall N \lhd G, N \subset H \Rightarrow N = \{e\}$

Lem. N

$H \leq G, o(G) = n, (G : H) = i$

$n \nmid i! \Rightarrow \exists N \lhd G$ s.t. $N \neq \{e\}, N \subset H$

Thm. 11.1

G_1, G_2 : 群, $a_1, b_1 \in G_1, a_2, b_2 \in G_2, G' := G_1 \times G_2$
$(a_1, a_2), (b_1, b_2) \in G', (a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2) \Rightarrow G'$: 群

Def. 11.1

$G_1 \times G_2 : G_1, G_2$ の**直積**

Rem. G' : 可換群 $\Leftrightarrow G_1, G_2$: 可換群

Thm. 11.2

G_1, G_2 : 群, $G' = G_1 \times G_2$

1. $f_1 : G_1 \to G', a_1 \mapsto a_1' = (a_1, e_2) \Rightarrow G_1 \cong f_1(G_1), f_1(G_1) \leq G'$
2. $f_2 : G_2 \to G', a_2 \mapsto a_2' = (e_1, a_2) \Rightarrow G_2 \cong f_2(G_2), f_2(G_2) \leq G'$
3. $G_1' := f_1(G_1), G_2' := f_2(G_2), \forall a_1' \in G_1', \forall a_2' \in G_2' \Rightarrow a_1' a_2' = a_2' a_1'$
4. $\forall a' \in G' \Rightarrow \exists! a_1' \in G_1', a_2' \in G_2'$ s.t. $a' = a_1' a_2'$

Def. 11.2

$N_1, N_2 \le G$
$\forall x_1 \in N_1, \forall x_2 \in N_2, x_1x_2 = x_2x_1, \forall x \in G, \exists! x_1 \in N_1, x_2 \in N_2$ s.t. $x = x_1x_2$
$\overset{\text{def}}{\Leftrightarrow}$ G は N_1, N_2 の**直積に分解される**

Thm. 11.3

G が N_1, N_2 の直積に分解される $\Rightarrow G \cong N_1 \times N_2$

<u>Rem.</u> G が N_1, N_2 の直積に分解されるとき, $G = N_1 \times N_2$ とかく

Lem. O

$N_1, N_2 \le G$
G が N_1, N_2 の直積に分解される $\Leftrightarrow$

1. $N_1, N_2 \lhd G$
2. $G = N_1N_2$
3. $N_1 \cap N_2 = \{e\}$

Exm. 1

$\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$

§8 Exc. 5

$a, b \in G, ab = ba, o(a) = m, o(b) = n, (m, n) = 1 \Rightarrow o(ab) = mn$

Exm. 2

G_1, G_2 : 巡回群, $o(G_1) = n_1, o(G_2) = n_2$
$G_1 \times G_2$: 巡回群 $\Leftrightarrow (n_1, n_2) = 1$

Exm. 3

p : 素数, G : 群, $o(G) = p^2 \Rightarrow G$: 可換群 ($\because$§7 Exm. 3) で次のいずれか

1. G : 巡回群
2. $\exists N_1, N_2$: 巡回群 s.t. $o(N_1) = o(N_2) = p, G = N_1 \times N_2$

Thm. 11.4

$G_1, \cdots, G_n$: 群, $e_i \in G_i \ (i = 1, \cdots, n)$

$$G' := \prod_{i=1}^{n} G_i = G_1 \times \cdots \times G_n = \{(a_1, \cdots, a_n) \mid a_i \in G_i \ (i = 1, \cdots, n)\}$$

$a', b' \in G', a'b' = (a_1, \cdots, a_n)(b_1, \cdots, b_n) = (a_1 b_1, \cdots, a_n b_n) \Rightarrow G'$: 群

Def. 11.3

$\prod_{i=1}^{n} G_i : G_1, \cdots, G_n$ の**直積**

Thm. 11.5

$G_1, \cdots, G_n$: 群, $G' = G_1 \times \cdots \times G_n, 1 \leq i \leq n, 1 \leq j \leq n, i \neq j$

1. $f_i \colon G_i \to G', a_i \mapsto a'_i = (e_1, \cdots, a_i, \cdots, e_n) \Rightarrow G_i \cong f_i(G_i), f_i(G_i) \leq G'$
2. $G'_i := f_i(G_i), G'_j := f_j(G_j), \forall a'_i \in G'_i, \forall a'_j \in G'_j \Rightarrow a'_i a'_j = a'_j a'_i$
3. $\forall a' \in G' \Rightarrow \exists! a'_1 \in G'_1, \cdots, a'_n \in G'_n$ s.t. $a' = a'_1 \cdots a'_n$

Def. 11.4

$N_1, \cdots, N_n \leq G, 1 \leq i \leq n, 1 \leq j \leq n, i \neq j$
$\forall i, j, \forall x_i \in N_i, \forall x_j \in N_j, x_i x_j = x_i x_j, \forall x \in G, \exists! x_1 \in N_1, \cdots, x_n \in N_n$ s.t. $x = x_1 \cdots x_n$
$\overset{\text{def}}{\Leftrightarrow}$ G は $N_1, \cdots, N_n$ の**直積に分解される**

Thm. 11.6

G が $N_1, \cdots, N_n$ の直積に分解される $\Rightarrow G \cong \prod_{i=1}^{n} N_i$

Lem. O (n)

$N_1, \cdots, N_n \leq G$
G が $N_1, \cdots, N_n$ の直積に分解される $\Leftrightarrow$

1. $N_1, \cdots, N_n \lhd G$
2. $G = N_1 \cdots N_2$
3. $(N_1 \cdots N_{i-1} N_{i+1} \cdots N_n) \cap N_i = \{e\} \quad (i = 1, \cdots, n)$

Lem. 12.1

p : 素数, $\alpha, m \in \mathbb{Z}, (p, m) = 1 \Rightarrow p \nmid \binom{p^\alpha m}{p^\alpha}$

Thm. 18 (Sylow の第 1 定理)

p : 素数, $\exists \alpha \in \mathbb{Z}$ s.t. $p^\alpha \mid o(G) \Rightarrow \exists H \leq G$ s.t. $o(H) = p^\alpha$

Cor. 18.1

p : 素数, $p \mid o(G) \Rightarrow \exists x \in G$ s.t. $o(x) = p$

Cor. 18.2

p : 素数, $p \mid o(G), \exists e, s \in \mathbb{Z}$ s.t. $o(G) = p^e s, (p, s) = 1 \Rightarrow \exists H \leq G$ s.t. $o(H) = p^e$

Def. 12.1

Cor. 18.2 を満たす $H \leq G$: G の p Sylow 部分群

Thm. 12.1

$H \le G, A, B \subset G, \exists x \in H$ s.t. $xAx^{-1} = B \overset{\text{def}}{\Leftrightarrow} A \sim_H B$: A, B は H に関して共役
$\Rightarrow \sim_H$: G の部分集合間の同値関係

§5 Exc. 12

$S \neq \emptyset, S \subset G, N(S) := \{x \in G \mid xS = Sx\} \Rightarrow N(S) \le G$
$N(S)$: G における S の正規化群

§7 Exc. 6

$S \subset G, (G : N(S)) < \infty \Rightarrow |\{S' \subset G \mid S \sim S'\}| = (G : N(S))$

Lem. P

$o(G) < \infty, H \le G, A \subset G \Rightarrow |\{A' \subset G \mid A \sim_H A'\}| = (H : H \cap N(A))$

Def. 12.2

$H \leq G, \exists x \in \mathbb{Z}$ s.t. $o(H) = p^x \overset{\text{def}}{\Leftrightarrow} H : p$ **部分群**

Thm. 19

$o(G) < \infty, p$: **素数**, $o(G) = p^e s, (p, s) = 1$

- a $\forall H \leq G : p$ **部分群** $\Rightarrow \exists P \leq G : p$ Sylow **部分群** s.t. $H \subset P$
- b (Sylow **の第 2 定理**) $\forall P, P' \leq G : p$ Sylow **部分群** $\Rightarrow P \sim P'$
- c (Sylow **の第 3 定理**)
  $s' := |\{P \mid P \leq G : p$ Sylow **部分群** $\}| \Rightarrow s' = 1 + kp, s' \mid o(G)$

Exm. 1

位数 15 のすべての群を決定せよ.

Exm. 2

位数 10 のすべての群を決定せよ.