応用代数学

2022 年 12 月 5 日現在

目次

0　準備

集合 X, Y, Z に対して

- $Y\backslash X$:$X, Y \subset Z$ に対して，X に属さない Y の元のなす集合

$$Y\backslash X = \{y \mid y \in Y \text{ かつ } y \notin X\}$$

- $X \sqcup Y$: 集合 X と Y の直和 (direct sum) あるいは分割和 (disjoint sum) を表し，互いに交わらない二つの集合 X と Y の和集合

$$A \sqcup B \Leftrightarrow A \cup B \quad \text{for} \quad A \cap B = \emptyset$$

- (有限) 集合 X の元の個数を $\sharp X$

$$\sharp\{a, b, c\} = 3$$

写像 集合 X から集合 Y への写像 f とは，X の各元 x に対して Y の元 $y = f(x)$ を対応させる規則

$$f : X \to Y; x \mapsto y = f(x)$$

- f による $A \subset X$ の像 (image)

$$f(A) = \{f(a) \mid a \in A\} \subset Y$$

- f による $B \subset Y$ の逆像あるいは f による引き渡し

$$f^{-1}(B) = \{a \in X \mid f(a) \in B\}$$

- $f : X \to Y, g : Y \to Z$ において，合成 $g \circ f$

$$\begin{array}{rccc} g \circ f : & X & \longrightarrow & Z \\ & \cup & & \cup \\ & x & \longmapsto & z \quad = g \circ f(x) = g(f(x)) \end{array}$$

0.1　集合の分割と同値関係

一般に集合 S を交わりのない (空でない) 集合の和で表すことを類別 (classification)という

$$S = A_1 \sqcup A_2 \sqcup \cdots$$

各部分集合 A_j をこの類別における類という

全ての類から一つずつ元を選んできて得られる集合 R を完全代表系という．集合 R の元を代表元という．このとき，任意の $x \in S$ に対して，集合 S から集合族 $\{A_1, A_2, \cdots\}$ への自然な全射写像$x \mapsto A_j (\ni x)$ が得られる．

定義 0.1 (同値関係)

集合 S 上の同値関係 $\sim \Leftrightarrow$ 集合 S 上の二項関係 $\sim$ が任意の $a, b, c \in S$ に対し，

反射則 $a \sim a$

対称則 $a \sim b \Rightarrow b \sim a$

推移則 $a \sim b$かつ$b \sim c \Rightarrow a \sim c$

定義 0.2 (同値類)
集合 S に同値関係 $\sim$ が存在するとき，S の各元 a に対して定まる空でない部分集合

$$C_a = \{x \mid x \in S, x \sim a\}$$

を a の同値類 (equivalence class) という．

定義 0.3 (商集合)
同値関係 $\sim$ による同値類の集合を S の $\sim$ による商集合 (quotient set) といい $S/\sim$ で表す

$$S/\sim = \{C_a \mid a \in S\}$$

定義 0.4 (同値類別)
同値関係による集合の分割．同値関係 $\sim$ による同値類別

$$S = \bigsqcup_{a \in R \subset S} C_a$$

ここで S の部分集合 R は全ての同値類の代表元の集合であり，完全代表系である．このとき，自然な全射 $\pi : S \to S/\sim; x \mapsto C_x$ が存在する．さらに全単射写像 $R \to S/\sim$ も存在する．

$$C_a \cap C_b \neq \emptyset \Rightarrow C_a = C_b$$

が成立する (同値関係の性質から直ちに示される)

例 S: ある学校の学生全体の集合．$a, b \in S$ の間の関係「クラスメートである」は同値関係．この関係を $\sim'$ で表すと，$a \sim' b$ は「a は b とクラスメートである」の意．このとき $C_a = \{x \in S \mid x \sim a\}$ は「a さんのクラスメート (a さんを含む) の全体」$\leftrightarrow$ a さんの属するクラス

1 群

定義 1.1 (二項演算)
一般に，集合 M の 2 つの元 x, y に対してただ一つの元 $\mu(x, y) \in M$ が対応しているとき，μ を M 上の二項演算という．すなわち，

$$\mu : M \times M \to M$$

ここで記号 μ は省略して，$\mu(x, y)$ を $x \cdot y, x \circ y$, あるいは xy などと書く (誤解のない限り).

定義 1.2 (群)
群 (group)G とは，以下の規則を満たす二項演算 μ をもつ集合のこと．

$$\mu : G \times G \to G$$

厳密には (G, μ) のことを群と呼ぶが群 G などと省略することが多い．任意の $x, y, z \in G$ に対して成立:

1. 結合法則
$$\mu(\mu(x,y),z) = \mu(x,\mu(y,z))$$

2. 単位元 $e \in G$ の存在.
$$\mu(e,x) = \mu(x,e) = x$$

3. 逆元の存在.
$$\mu(x,x') = \mu(x',x) = e$$

なる $x' \in G$[*1]

定義 1.3 群 G の位数 (order):G に含まれる元の個数を表し，$|G|$ と書く．位数が有限のとき，有限群という．有限群でないとき，無限群という．

一般に群では $(\mu(x,y) \neq \mu(y,x))$

$$x \circ y \neq y \circ x \quad \text{(交換関係が必ずしも成立しない)}$$

定義 1.4 G の任意の元について，$xy = yx$ が成り立つとき可換群 (Abel 群) という．可換群の演算記号を加法的に $x + y$ と書くとき，加法群と呼び，このとき加法に関する単位元を 0 と表し，零元と呼ぶことが多い (x の逆元は $-x$).

1.1 群の基本的な性質

命題 1.5 単位元 e は存在すればただ 1 つ．逆元 $x' \neq x$ に対してただ 1 つに定まる (通常，x' を x^{-1} と書く．)

単位元の一意性.
$$e = e \circ e' = e'$$

□

逆元の一意性.
$$x' = x' \circ e = x' \circ (x \circ x'') = (x' \circ x) \circ x'' = e \circ x'' = x''$$

□

命題 1.6 (簡約律)
$(G, \circ)$ が群のとき，$x, y, z \in G$ に対して，
$$x \neq y \Rightarrow z \circ x \neq z \circ y, \quad x \circ z \neq y \circ z$$

Proof. $z \circ x = z \circ y$ とすると
$$\begin{aligned} x = e \circ x &= (z' \circ z) \circ x = z' \circ (z \circ x) \\ &= z' \circ (z \circ y) = (z' \circ z) \circ y \\ &= e \circ y = y \end{aligned}$$

これは $x \neq y$ に矛盾．$x \circ z \neq y \circ z$ も同様に示される． □

[*1] あとで x の逆元 x' は唯一に定まることを示す．x' を x^{-1} と書くことが多い

系 1.7 (組み替え定理)
位数 n の群 G に任意の元 $x \in G$ をかけて得られる集合を $G' = xG$ とする．$G = \{y_k \mid k = 1, 2, \cdots, n\}$ と $G' = \{xy_k \mid k = 1, 2, \cdots, n\}$ の間には全単射の写像が存在し，G と G' は対等である．

例 $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$: 通常の足し算を群演算として加法群．単位元 0，x の逆元は $-x$．$K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ に対して，$K^\times = K \backslash \{0\}$: 通常の掛け算を群演算とした乗法群．単位元 1，x の逆元は $\frac{1}{x} = x^{-1}$.

まず, 位数の小さな群について考える.「有限集合 G に対して, $(G, \circ)$ が群となるよう二項演算 $\circ : G \times G \to G$ を与える」

- 位数 1 の群 $G_1 = \{e\}$ の群積表

表 1　自明な群 (trivial group)

G_1	e
e	$e \circ e = e$

- 位数 2 の群 $G_2 = \{e, a\}$

表 2

G_2	e	a
e	$e \circ e = e$	$e \circ a = a$
a	$a \circ e = a$	$a \circ a = e$[*2]

- 位数 3 の群 $G_3 = \{e, a, b\}$

表 3

G_3	e	a	b
e	e	a	b
a	a	b[*3]	e
b	b	e	a

- 位数 4 の群 $G_4^{(1)} = \{e, a, b, c\}, \circ_1$，$G_4^{(2)} = \{e, a, b, c\}, \circ_2$

群積表では

元は各行，各列においてそれぞれ 1 回のみ現れる．(全単射)

について確かめることができる．特に，対角線に対して対称な場合，可換群，非対称な場合，非可換群.

1.2　群の例

- 巡回群 C_n

[*2] a でないことは簡約律から従う.
[*3] $a \circ b$ が b だと簡約律を満たさない

定義 1.8 一つの元のべきで群の全ての元が表示できるとき，この群を巡回群 (cyclic group)という．位数 n の巡回群を C_n と書く．

$C_1 = \{e\}, C_2 = \{e, c\} = \langle c | c^2 = e \rangle, C_3 = \{e, c, c^2\} = \langle c | c^3 = e \rangle, C_4, \cdots, C_n = \{e, c, \cdots, c^{n-1}\} = \langle c | c^n = e \rangle, \cdots, C_\infty$ において指数法則 $c^m c^n = c^{m+n}$ が成り立ち，加法群 $\mathbb{Z}$ と同一視することができる．$C_\infty = \{e, c, c^{-1}, c^2, c^{-2}, \cdots\}$

- 二面体群 D_n

定義 1.9 位数 $2n$ の二面体群 (dihedral group)D_n

$$\begin{aligned} D_n &= \{e, a, a^2, \cdots, a^{n-1}, b, ab, a^2b, \cdots, a^{n-1}b\} \\ &= \langle a, b | e = a^n = b^2 = abab \rangle \\ |D_n| &= 2n. \end{aligned}$$

二面体群の表記の 1 つに，任意の元が 2 つの元 a, b のいくつかの積で表示するものがある．このとき，D_n は集合 $\{a, b\} \subset D_n$ によって生成されるといい，$\{a, b\}$ を生成系，生成系の元を生成元という．
また，生成元の間の任意の関係式が還元される関係式のことを基本関係式という．[*4]

  - 群積表で構成した群において，
$$G_1 = C_1, G_2 = C_2, G_3 = C_3, G_4^{(1)} = C_4$$
  - 巡回群でない最小位数の群 $D_2 = \left(G_4^{(2)}\right)$
  - 位数最小の非可換な群 D_3

定義 1.10 一般の群 G において，元 $x \in G$ が生成する巡回群の位数を元 x の位数という[*5]．$x^n = e$ となる最小の $n > 0$ が x の位数 (ない場合は，元 x の位数は ∞ として扱う).

例
$$C_4 = \{e, c, c^2, c^3\} = \langle c | c^4 = e \rangle$$
c の位数は 4，c^2 の位数は 2，$\cdots$

- (行列群) n 次正則行列の全体は，行列積について群をなす．単位元: n 次単位行列，x の逆元は x の逆行列.

  - 一般線形群
$$GL_n(\mathbb{C}) = \{g \in \mathrm{Mat}(n \times n; \mathbb{C}) \mid \det g \neq 0\}$$
  - 特殊線形群
$$SL_n(\mathbb{C}) = \{g \in GL_n(\mathbb{C}) \mid \det g = 1\}$$
  - 直交群
$$O_n = \left\{g \in GL_n(\mathbb{R}) \mid {}^t g \cdot g = 1\right\}$$
  - ユニタリー群
$$U_n = \left\{g \in GL_n(\mathbb{C}) \mid \overline{{}^t g} \cdot g = 1\right\}$$

[*4] D_n では，$e = a^n = b^2 = abab$
[*5] cf. 群の位数

1.3 いろいろな代数系

群以外にさまざまな” 代数” が考えられる.

定義 1.11 集合 M 上に二項演算 $\mu : M \times M \to M$ が定義されているとする.

- 結合法則を満たすとき，M は半群 (semi group)であるという.

$$\mu(\mu(x,y),z) = \mu(x,\mu(y,z))$$

- 単位元 (identity)$e \in M$ を持つ半群を単位的半群あるいは，モノイド (monoid)という．e を $1_M, I_d$ と表すこともある.

$$\mu(e,x) = \mu(x,e) = x$$

- 任意の $x \in M$ に対して

$$\mu(x,x') = \mu(x',x) = e$$

を満たす $x' \in M$ が存在するモノイドを群という.

さらに，環，体などの複雑な” 代数系” もある.

例: (半群の例)
$(\mathbb{R}, \max)$: $x, y \in \mathbb{R}$ に対して

$$x \circ y = \max(x,y)$$

このとき，$(\mathbb{R}, \max)$ は半群.

$$\max(\max(x,y),z) = \max(x,\max(y,z))$$

さらに形式的な単位元となる $-\infty$ を考慮に入れる場合，$(\mathbb{R} \cup \{-\infty\}, \max)$ はモノイドとなる．逆元は存在しない $(\cdots \max(x,x') = -\infty$ となる x' が存在しない)

定義 1.12 モノイド M の元で逆元 x' が存在するものを単元 (unit)といい $M^\times$ を M の単元のなす部分集合とする．このとき，M' は群をなし，単元群 (unit group)と呼ばれる.

例 $K \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ に対して，$K^\times = K \backslash \{0\}$ は積に関して単元群.

1.4 写像の合成と群

集合 X から X 自身への写像全体のなす集合を $M(X)$ とかく．$x \in X$ および $f, g \in M(X)$ に対し，写像の合成 $f \cdot g(x) = f(g(x))$ を $f \cdot g \in M(X)$ とかく．このとき

1. $f, g, h \in M(X)$ に対し，$(f \cdot g) \cdot h = f \cdot (g \cdot h)$
2. $e = Id_X$ を X の恒等写像とすると $f \cdot e = e \cdot f = f$
3. $S(X) = \{f \in M(X) \mid f$は全単射$\}$ とおくと，$e \in S(X)$ で，$f, g \in S(X)$ ならば，$f \cdot g \in S(X)$．また f^{-1} を $f \in S(X)$ の逆写像とすると

$$f \cdot f^{-1} = f^{-1} \cdot f = e$$

以上より，次の命題を得る．

命題 1.13 任意の集合 X に対し，X から X への写像の集合 $M(X)$ はモノイドをなす．全単射のなす部分集合 $S(X) = M(X)^\times$ が単位元となる．$S(X)$ を X の対称群 (symmetric group)

特に X が有限集合のとき ($\sharp X = n < \infty$)，$S(X)$ を n 次対称群といい，$S(X) = S_n$ あるいは $\mathcal{S}_n$ とかく．S_n を n 次置換群 (permutation group) と呼ぶ場合もある．S_n の位数は $|S_n| = n!$

Remark 特に $X = \{1, 2, \cdots, n\}$ のとき，$S_n = S(X)$ の元 σ を 1 つ選べば，重複なしに n 個の数字を並べたもの，つまり，$1, 2, \cdots, n$ の順列の 1 つが定まる．

$$\sigma : X \overset{1\text{to}1}{\to} X; \quad j \mapsto \sigma(j) \in X$$

置換の記法 $X = \{1, 2, \cdots, n\} = \{i_1, i_2, \cdots, i_n\} = \{j_1, j_2, \cdots, j_n\}$ に対して，$\sigma = \begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ j_1 & j_2 & \cdots & j_n \end{pmatrix}$ は $\sigma(i_k) = j_k \quad (k = 1, 2, \cdots, n)$ を定める．例えば，$X = \{1, 2, 3\}$ において，$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in S_3$ とすると，

$$\sigma(1) = 3, \quad \sigma(2) = 1, \quad \sigma(3) = 2$$

ここで，

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

定義 1.14 (交代群)

S_n の元の中で偶数個の互換の積で表すことができる元の全体を A_n で表す．[*6]この S_n の部分集合 A_n は，S_n の演算で群となり，n 次交代群 (alternating group) と呼ばれる．

命題 1.15 $S_n = A_n \cup (1, 2)A_n$ である $(n \geq 2)$.

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$$

Remark 表示方法によって偶奇性が変わらないことを証明する必要

巡回置換の記号

$$(j_1, j_2, \cdots, j_l) \coloneqq \begin{pmatrix} j_1 & j_2 & \cdots & j_{l-1} & j_l \\ j_2 & j_3 & \cdots & j_l & j_1 \end{pmatrix}$$

$$\begin{aligned} S_3 &= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\} \\ &= \{e, (2, 3), (1, 3), (1, 2), (1, 3, 2) = (2, 3)(1, 2), (1, 2, 3) = (1, 2)(2, 3)\} \\ A_3 &= \{e, (2, 3)(1, 2), (1, 2)(2, 3)\} \end{aligned}$$

[*6] ここで互換とは，2 つの数字 (文字) の入れ替え $i \leftrightarrow j$ を表し，(i, j) と表記する．

1.5 部分群

定義 1.16 群 G の空でない部分集合 H が群 G の演算で群となるとき，H を G の部分群 (subgroup)と呼び，$H \leqq G$ と書くことがある．

Remark 群 G の自明な部分群に，G の単位元のみからなる群と，G 自身の 2 つある．

命題 1.17 群 G の空でない部分集合 H が

$$x, y \in H \Rightarrow x \cdot y^{-1} \in H$$

をみたすとき，H は G の部分群となる．H は単位元を含み，G の演算で群をなす．

Proof. $x \in H$ とすると，$e = x \cdot x^{-1} \in H$.

$$x \in H \Rightarrow x^{-1} = x^{-1} \cdot e \in H$$

$$x, y \in H \Rightarrow x, y^{-1} \in H \Rightarrow xy \in H$$

H は空でない部分群. □

2 準同型写像

準同形写像: 群の二項演算の代数的構造を保つ写像

群の例

(1) $G = \mathbb{Z}, \quad a \circ b = a + b + 1, \quad (G, \circ)$ は群をなす．この群の単位元および a の逆元を求めよ

$$a \circ e = e \circ a = a \Leftrightarrow a + e + 1 = e + a + 1 = a \Leftrightarrow e = -1$$

$$a \circ a^{-1} = a^{-1} \circ a = e \Leftrightarrow a + a^{-1} + 1 = a^{-1} + a + 1 = -1 \Leftrightarrow a^{-1} = -a - 2$$

(2) $G = \mathbb{R}\backslash\{-1\}, \quad a \circ b = a + b + ab, \quad (G, \circ)$ は群をなす．この群の単位元および a の逆元を求めよ

$$e = 0, \quad a^{-1} = -\frac{a}{a+1}$$

(3) $G = \mathbb{R}\backslash\{0\}, \quad a \circ b = 2ab, \quad (G, \circ)$ は群をなす．この群の単位元および a の逆元を求めよ

$$e = \frac{1}{2}, \quad a^{-1} = \frac{1}{4a}$$

これらの例では，より簡単な群と関係づけることができる．以下，準同型，同型を導入する．

定義 2.1 2 つの群 G, G' に対して，写像 $f : G \to G'$ が

$$f(x \circ y) = f(x) \cdot f(y) \quad (x, y \in G)$$

を満たすとき，f を準同型写像または準同型 (homomorphism)という．また，G から G' への準同型写像全体を $\mathrm{Hom}\,(G, G')$ とかく．

Remark G, G' として，$(G, \circ), (G', \cdot)$ を意味している．

- G 上の二項演算 $\circ$ を G' 上の二項演算 $\cdot$ へ移す．

$$f(x \circ y) = f(x) \cdot f(y) = x' \cdot y' \quad \text{ここで} x', y' \in G'$$

- 群 G の単位元 e は，群 G' の単位元 e' に移される．

$$\begin{aligned} & f(e) \cdot f(e) = f(e \circ e) = f(e) \\ \Leftrightarrow & f(e)^{-1} \cdot f(e) \cdot f(e) = f(e)^{-1} f(e) \\ \Leftrightarrow & e' \cdot f(e) = f(e) = e' \end{aligned}$$

- 群 G の逆元は，群 G' の逆元に移される．

$$\begin{aligned} & f(a) \cdot f\left(a^{-1}\right) = \left(a \circ a^{-1}\right) = f(e) = e' \\ \Leftrightarrow & f\left(a^{-1}\right) = f(a)^{-1} \end{aligned}$$

$$\begin{array}{ccc} (x, y) \in G^2 & \overset{\circ}{\longmapsto} & x \circ y \in G \\ \downarrow f & & \downarrow f \\ (f(x), f(y)) \in G'^2 & \longmapsto & f(x) \cdot f(y) \in G' \end{array}$$

定義 2.2 準同型 f が全単射のとき，f を同型写像または同型 (isomorphism)という．同型写像 $f : G \to G'$ が存在すればG と G' は同型であるといい．$G \simeq G'$ または $G \xrightarrow{\sim} G'$ などとかく．

例 同型を用いると，先の例 (1),(2),(3) は...

(1) の群は，通常の加法に関する $\mathbb{Z}$ のなす群と同型．$f(a) = a + 1$ とする．

$$f(a \circ b) = f(a + b + 1) = a + b + 2 = (a + 1) + (b + 1) = f(a) + f(b)$$

(2) と (3) の群は，通常の乗法群としての $\mathbb{R}^\times = \mathbb{R} \backslash \{0\}$ と同型

(2) $f'(a) = a + 1$
(3) $f'(a) = 2a$

準同型，全単射であることは容易に確かめられる．

準同型の例

1 次分数変換

$$G = \left\{ f(x) = \frac{ax + b}{cx + d} \mid a, b, c, d \in \mathbb{C}, ad = bc \neq 0 \right\}$$

$GL(2, \mathbb{C})$[*7]の元 $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ に対して，G の元 $f_A(x)$ を $f_A(x) = \frac{ax+b}{cx+d}$ によって定める．$GL(2, \mathbb{C})$ の元と G の元を対応[*8]付けている．

$$f_{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}}(x) = \frac{x + 0}{0 + 1} = x, \quad f_A^{-1}(f_A(x)) = x$$

[*7] $|A| = ad - bc \neq 0$
[*8] $F : GL(2, \mathbb{C}) \to G$

$$f_A^{-1}(x) = \frac{1}{ad-bc}\frac{dx-b}{-cx+a} = f_{A^{-1}}(x)$$

ここで $A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ であることに注意.

このとき，任意の $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $P = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in GL(2,\mathbb{C})$ に対して,

$$\begin{array}{ccc} (A,P) & \longmapsto & A\cdot P \in GL(2,\mathbb{C}) \\ F\downarrow & & F\downarrow \\ (f_A, f_P) & \longmapsto & f_A \circ f_P = f_{AP} \end{array}$$

対応 F は $GL(2,\mathbb{C}) \to G$ の準同型を与えている.

Remark G は写像の合成に関して群.

$GL(2,\mathbb{C})$ は行列の積に関して群，単位元は $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$，$A$ の逆行列 A^{-1} が A の逆元．ただし，この対応 F は，全単射となっておらず同型ではない．$\Rightarrow$ 準同型と同型のズレを測るのが「核」である.

定義 2.3 準同型 $f : G \to G'$ に対して,

$$\mathrm{Ker}\, f = \{x \in G \mid f(x) = e'\}$$

を準同型写像 f の核 (kernel)という.

定義 2.4 準同型 $f : G \to G'$ に対して,

$$\mathrm{Im}\, f = \{f(x) \mid x \in G\}$$

を準同型写像の像 (image)という.

例

$$\begin{array}{ccccc} f : GL(2,\mathbb{C}) & \longrightarrow & G = \left\{\phi(z) = \frac{az+b}{cz+d} \mid a,b,c,d \in \mathbb{C}, ad = bc \neq 0\right\} \\ \cup & & \cup \\ \begin{bmatrix} a & b \\ c & d \end{bmatrix} & \longmapsto & \phi_A(z) = \frac{az+b}{cz+d} \end{array}$$

は準同型．核

$$\begin{aligned} \mathrm{Ker}\, f &= \{A \in GL(2,\mathbb{C}) \mid \phi_A(z)\} \\ &= \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \mid a \in \mathbb{C}\backslash\{0\} \right\} \end{aligned}$$

つまり，分子と分母に定数倍の不定性が存在することを示している.

命題 2.5 核が単位元のみからなることが，群の準同型が 1 対 1 となるための必要十分条件.

Proof. (必要条件は明らか)

十分性を準同型 $f : G \to G'$ の場合に示す.

$f(x) = f(y)$ とすると，準同型性から

$$f\left(x \circ y^{-1}\right) = f(x) \cdot f(y)^{-1} = e$$

よって核が単位元のみとすると

$$x \circ y^{-1} = e \Leftrightarrow x = y$$

□

命題 2.6 $f \in \mathrm{Hom}\,(G, G'), H \leqq G, H' \leqq G'$ とする．

- $f(H) \leqq G'$
- $f^{-1}(H') \leqq G$

Proof. (レポート) □

系 2.7 自明な群 $\{e'\} \subset G'$ の逆像である準同期写像 f の核 $\mathrm{Ker}\, f$ は G の部分群となる．

Note ベクトル空間の間の準同型のことを，通常，線形写像と呼ぶ．
線形写像 $\varphi : V \to W$ に対して，$\mathrm{Ker}\,\varphi$ は，V の部分ベクトル空間．$\mathrm{Im}\,\varphi$ は，W の部分ベクトル空間．

一般の準同型 $f : G \to G'$ は，G の元をいくつかずつまとめて，より” 粗い” 群を作って G' に埋め込む．準同型 f が元の群をどれだけ” 粗く” するかは，f の像の 1 点，特に単位元の逆像のみで決まる．

定義 2.8 G を群とする．G から G への準同型写像を G 上の自己準同型 (endomorphism)という．G 上の自己準同型写像の全体 $\mathrm{End}\,(G)$ はモノイドをなす．さらに同型写像である時は，G 上の自己同型 (automorphism)という．G 上の自己同型全体からなる集合 $\mathrm{Aut}\,(G)$ を自己同型群という．

例: (全単射だが同型でない例)

$$G : \text{位数}n\text{の有限群}$$
$$\phi_a : G \to G;\ g \mapsto ag$$

ここで $a \in G$ とする．[*9]

自己同型の重要な例

命題 2.9 群 G の元 $a \in G$ を選ぶ．$a \in G$ による共役変換と呼ばれる写像

$$A_a : G \to G;\ g \mapsto aga^{-1}$$

で定義する．これは G 上の自己同型を与える．

略証 準同型性:

$$A_a(g)A_a(h) = aga^{-1}aha^{-1} = agha^{-1} = A_a(gh)$$

全単射:(略)

[*9] 準同型でないことがわかる

3　群作用と軌道分解

3.1　作用について

群 G の集合 X への作用について，G 自身への作用を含めて議論する．群の作用には，左作用と右作用がある．

定義 3.1 群 G の集合 X への左作用 (left action)とは，次の条件を満たす写像 $\lambda : G \times X \to X$ のこと．

- $\forall x \in X$ に対し，
$$\lambda(e_G, x) = x$$
- $\forall g, h \in G$, $\forall x \in X$ に対し，
$$\lambda(gh, x) = \lambda(g, \lambda(h, x))$$

このとき，G は λ によって X に左から作用 (act from left) するという．このような写像 λ が与えられた集合 X を左 G 集合 (left G-set)という．

定義 3.2 群 G の集合 X への右作用 (right action)とは，次の条件を満たす写像 $\rho : X \times G \to X$ のこと．

- $\forall x \in X$ に対し，
$$\rho(x, e_G) = x$$
- $\forall g, h \in G$, $\forall x \in X$ に対し，
$$\rho(x, gh) = \rho(\rho(x, g), h)$$

このとき，G は ρ によって X に右から作用 (act from right) するという．このような写像 ρ が与えられた集合 X を右 G 集合 (right G-set)という．

Remark 明示する必要がない場合，$\lambda(g, x)$ を $g \cdot x$ や gx などと省略することが多い．

Note 自明な作用: 全ての $g \in G$, $x \in X$ に対し，$\lambda(g, x) = x$ とする作用

Note 対称群 $\mathcal{G}_n$ はその定義から，$X = \{1, 2, \cdots, n\}$ 上に自然に置換として作用している．本講義では通常は左作用としている．

Remark $\rho(x, g)$ を $(x)\rho_g$, x^g あるいは $x \cdot g$, xg などと省略する．

命題 3.3 群 G が集合 X に $(g, x) \mapsto g \cdot s$ によって左から作用しているとき，$\rho(x, g) = x^g = g^{-1} \cdot x$ とおくと，これは G の右作用となる．逆も同様，G の X への左作用と G の X への右作用は 1 対 1 となる．

Proof. $(G, \circ)$ に対し，
$$(g \circ h, h) \mapsto (g \circ h) \cdot x = g \cdot (h \cdot x)$$
このとき
$$\begin{aligned} \rho(x, g \circ h) &= (g \circ h)^{-1} \cdot x = \left(h^{-1} \circ g^{-1}\right) \cdot x = h^{-1} \cdot \left(g^{-1} \cdot x\right) \\ &= \rho(\rho(x, g), h) \end{aligned}$$

□

例 正三角形への作用について，

変換 1 ρ_a: 反時計周りに $\frac{2}{3}\pi$ 回転

ρ_h: 重心を通る垂直軸で折り返し変換

変換 2 $\sigma_{132} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$: 頂点番号集合 $\{1,2,3\}$ への置換

$\sigma_{23} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$: 頂点番号集合 $\{1,2,3\}$ への置換

$$
\begin{aligned}
\rho_a(\triangle(123)) &\mapsto \triangle(312) \\
\rho_b(\triangle(123)) &\mapsto \triangle(132) \\
\sigma_{132}(\triangle(123)) &\mapsto \triangle(312) \\
\sigma_{23}(\triangle(123)) &\mapsto \triangle(132) \\
(\rho_a \circ \rho_b)(\triangle(123)) &\mapsto \rho_a(\rho_b \triangle(123)) \\
&= \triangle(213) \\
(\sigma_{132} \circ \sigma_{23})(\triangle(123)) &= \sigma_{132}(\sigma_{23}\triangle(123)) \\
&= \sigma_{132}(\triangle(132)) \\
&= \triangle(321) \\
(\triangle(123))(\rho_a \circ \rho_b) &= ((\triangle(123))\rho_a)\rho_b \\
&= (\triangle(312))\rho_b = \triangle 321 \\
(\triangle(123))(\sigma_{132} \circ \sigma_{23}) &= ((\triangle(123))\sigma_{132})\sigma_{23} \\
&= \triangle(213)
\end{aligned}
$$

ここで $x \mapsto f\left(g^{-1} \circ x\right)$ とすると左作用となる．

命題 3.4 (G 集合 X 上の関数への作用)

群 G が集合 X に左から作用しているとき，X 上の複素数値関数全体を $F(X)$ と置き，$g \in G$ の $F(X)$ への作用を，関数 $f \in F(X)$ を関数 $x \mapsto f(g \cdot x) \quad (\forall x \in X)$ に写す写像を定める．これは右作用になる．これを G の X への作用から引き起こされる X 上の関数への作用という．

例 $\mathcal{H} = \{z \in \mathbb{C} \mid \mathrm{Im}\, z > 0\}$，左作用 $\mu : SL_2(\mathbb{R}) \times \mathcal{H} \to \mathcal{H}$

$$
\left(g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, z\right) \mapsto \mu(g,z) = \frac{az+b}{cz+d} \quad (ad - bc = 1)
$$

複素上半平面 $\mathcal{H}$ の上の正則関数 $f(z)$ 全体の集合 $H(\mathcal{H})$ への作用 $f(g \cdot z)$ は右作用となる．

このとき，

$$
\begin{aligned}
\mu(hg, z) &= \mu(h, \mu(g,z)) \\
&= \mu\left(\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}, \frac{az+b}{cz+d}\right) \\
&= \frac{a'(az+b)/(cz+d) + b'}{c'(az+b)/(cz+d) + d'}
\end{aligned}
$$

例えば，$g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, h = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in SL_2(\mathbb{R})$

$$gh = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad hg = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

$$\begin{aligned} f(z) &\xrightarrow{g} F(z) = f(g \cdot z) = f(z+1) \\ &\xrightarrow{h} F(h \cdot z) = F\left(\frac{z}{z+1}\right) = f\left(\frac{z}{z+1} + 1\right) = f\left(\frac{2z+1}{z+1}\right) = f((gh) \cdot z) = f(h \cdot (g \cdot z)) \end{aligned}$$

3.2 集合 X の軌道分解

定義 3.5 (二項演算が定義されている) 集合 S の集合 X への左からの作用とは，次の条件より写像

$$\lambda : S \times X \to X$$

のこと．

- 任意の $g, h \in S$, $x \in X$ に対し，
$$\lambda(gh, x) = \lambda(g, \lambda(h, x))$$

定義 3.6 $\cdot : S \times X \to X$ を集合 S の集合 X への左からの作用とする．$x \in X$ に対し，x の S-軌道 (S-orbit) を，

$$S(x) \coloneqq S \cdot x = \{s \cdot x \mid s \in S\} \subset X$$

で定義する．

命題 3.7 $(G, \circ)$ を群とし，$\cdot : G \times X \to X$ を G の群としての X への左からの作用とする．このとき，二項関係 $x \overset{G}{\sim} y$ を $x \in G \cdot y$で定義すると，同値関係[*10]になる．

$$\begin{aligned} x \overset{G}{\sim} y &\Leftrightarrow \exists g \in G \quad \text{s.t.} \quad x = g \cdot y \\ &\Leftrightarrow G(x) = G(y) \end{aligned}$$

ここで $x \overset{G}{\sim} y$ は同値関係なので同値類に関する類別を考えることができる．これを軌道分解という．

定義 3.8 $s \overset{G}{\sim} y$ に関して X を同値類に分割したものを，X の G による軌道分解といい $X/\sim G$ で表す．

$$X/\sim G = \{G(t) \mid t \in \Lambda\}, \quad \text{s.t.} \quad X = \bigsqcup_{t \in \Lambda} G(t)$$

ここで Λ は完全代表系，集合 X の群 G による軌道分解を $G\backslash X$ で表すことも多い．また，軌道が唯一つになるとき，作用が推移的(transitive) であるという．

[*10] cf. 同値関係: 集合 X 上の同値関係 $\sim \Leftrightarrow \forall a, b, c \in X$ に対し，
- $a \sim a$
- $a \sim b \Rightarrow b \sim a$
- $a \sim b$ かつ $b \sim c \Rightarrow a \sim c$

Note G の X への作用が推移的

$\Leftrightarrow \forall x, y \in X$ に対し，$\exists g \in G \quad \text{s.t.} \quad x = g \cdot y$

$\Leftrightarrow \forall x_0 \in X$ に対し，$G \cdot x_0 = G(x_0) = X$

例: (軌道分解の例)

4 次の巡回群 C_4 の正六面体に作用

$$C_4 \cdot 1 = \{1, 2, 3, 4\}$$
$$C_4 \cdot 5 = \{5, 6, 7, 8\}$$

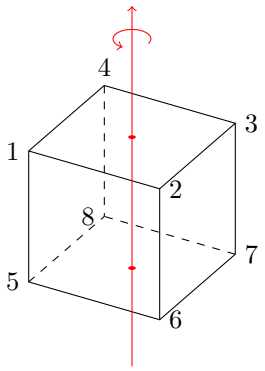

図 1　正六面体

定義 3.9 (固定部分群)

群 G が集合 X に作用しているとき，X の 1 点 x を動かさない $g \in G$ の全体は，G の部分群となる．これを x の固定部分群(stabilizer of x) といい，G_x とかく．

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

例 正六面体群 $P(6)$ において頂点 A_1 を固定する部分群は位数 3 の巡回部分群.

$$P(6)_{A_1} = \left\{ \text{恒等変換}, \text{立方体の重心と頂点} A_1 \text{を通る対角線周りの} \frac{2}{3}\pi \text{回転}, \frac{4}{3}\pi \text{回転} \right\}$$

- 集合 X への群 G の作用が推移的である時，集合 X と集合 G は以下の意味で” ほぼ同じ” とみなすことができる．

命題 3.10 G を群，X を G-集合．$x_0 \in X$ に対し，

$$f : G \to X;\ g \mapsto g \cdot x_0$$

を定める．このとき，

$$G\text{の } X \text{ への作用が推移的} \Leftrightarrow f\text{が全射}, f(G) = X$$

Remark このとき，f は単射であるとは限らない．しかし，群 G を固定部分群で” 割る” ことで全単射を作ることができる．(cf. 準同型定理など...)

「群 G を部分群で割る」$\to G$ の同値類のひとつである剰余類の導入

3.3 群 G の剰余類分解

特に，部分群の G 自身への作用による軌道分解

- 部分群 H の群 G への右作用乗法移動

$$\rho : G \times H \to G;\ (g, h) \mapsto gh$$

- 部分群 H の群 G への左作用乗法移動

$$\lambda : H \times G \to G;\ (h, g) \mapsto hg$$

$\Rightarrow$ 対応する軌道分解によって，群 G は部分群による同値類に分解 (類別) できる．

以下 $H \leqq G$ とする．

■部分群 H の群 G への右からの乗法移動による $g \in G$ の軌道

$$H(g) = \{\rho(g, h) \mid h \in H\} = \{g \cdot h \mid h \in H\} = gH$$

による軌道分解 $G = \bigsqcup_{a \in \Lambda} aH$ から誘導される同値関係，同値類，剰余 (商) 集合が得られる．

命題 3.11 (H 軌道から誘導される G 上の同値関係)
$H \leqq G$ とする．$a, b \in G$ に対する関係 $a \sim b$

$$a \sim b \Leftrightarrow a^{-1}b \in H$$

は同値関係．$\overset{\mathrm{L}}{\sim}$ と表すこともある．

Proof. $a \sim a$: $a^{-1}a = e \in H$.
$a \sim b \Leftrightarrow b \sim a$: $a^{-1}b \in H \Leftrightarrow \left(a^{-1}b\right)^{-1} = b^{-1}a \in H$
$a \sim b$ かつ $b \sim c \Rightarrow a \sim c$: $a^{-1}b, b^{-1}c \in H$ とすると，

$$a^{-1}c = \left(a^{-1}b\right) \cdot \left(b^{-1}c\right) \in H$$

□

Note 同値関係 $\overset{\mathrm{L}}{\sim}$ による a の同値類 aH

$$C_H(a) = \left\{b \in G \mid a \overset{\mathrm{L}}{\sim} b\right\} = \left\{b \in G \mid a^{-1}b \in H\right\}$$

と表すこともある．

このとき，$a \sim b$ ならば，$\exists h \in H \quad \text{s.t.} \quad a^{-1}b = h \Leftrightarrow b = ah$

定義 3.12 $H \leqq G$．G の部分集合 $gH = \{gh \mid h \in H\}$ を g の左剰余類(left coset) とよび，同値関係 $\overset{\mathrm{L}}{\sim}$ による g の同値類を表す．

定義 3.13 (剰余集合・商集合)
(左) 剰余類 aH 全体のなす集合(左) 剰余集合または商集合と呼ぶ．群 G の部分群 H による左剰余集合を G/H で表す．

また，各類から 1 つずつ代表元を取ってきた代表元全体の集合 Λ を G の H に関する左完全代表系という．

このとき，相異なる左剰余類の個数を H の G による指数(index) といい，$(G:H)$ で表す．指数が ∞ となる場合もある．定義より

$$(G:H) = |G/H|$$

である．

部分群 H による群 G の左剰余類への分解 (coset decomposition)(左類別ともいう)．

$$G = \bigsqcup_{a\in\Lambda} aH$$

このとき，左完全代表形 $\Lambda = \{a', b', \cdots\}$ とすると

$$\begin{aligned} G/H &= \{a'H, b'H, \cdots\} \\ |\Lambda| &= |G/H| = (G:H) \end{aligned}$$

■部分群の群 G への左からの乗法移動による $g \in G$ の H 軌道

$$H(g) = \{\lambda(h,g) \mid h \in H\} = \{h\cdot g \mid h \in H\} = Hg$$

による軌道分解 (右類別ともいう)

$$G = \bigsqcup_{a\in\Lambda'} Ha$$

から誘導される同値関係・同値類・剰余 (商) 集合が得られる．

命題 3.14 (左乗法移動から得られる H 軌道が誘導する G 上の同値関係)
$H \leqq G$ とする．$a, b \in G$ に対する関係 $a \sim b$

$$a \sim b \Leftrightarrow ba^{-1} \in H$$

は同値関係となる．以降 $\overset{\mathrm{R}}{\sim}$ と表す．

この同値関係 $\overset{\mathrm{R}}{\sim}$ による剰余類

$$C'_H(a) = \left\{x \in G \mid x \overset{\mathrm{R}}{\sim} a\right\}$$

を G の H による右剰余類という．Ha と表すことも多い

例 3 次対称群 $\mathcal{G}_3$ に対して，部分群 $H_1(\simeq C_2), H_2(\simeq C_3)$ を次で定める．

$$\begin{aligned} H_1 &= \{e, (1\ 2)\}, \\ H_2 &= \{e, (1\ 2\ 3), (1\ 3\ 2)\}, \\ \mathcal{G}_3 &= \{e, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\} \end{aligned}$$

において，

$$\begin{aligned} eH_1 &= \{e, (1\ 2)\}, \\ (1\ 2)H_1 &= \{(1\ 2)e = (1\ 2), (1\ 2)(1\ 2) = e\} \end{aligned}$$

よって

$$eH_1 = (1\ 2)H_1$$

左剰余集合 $\mathcal{G}_3/H_1 = \{eH_1, (1\ 3)H_1\}$

$$
\begin{aligned}
(1\ 3)H_1 &= \{(1\ 3)e = (1\ 3), (1\ 3)(1\ 2) = (1\ 2\ 3)\} = (1\ 2\ 3)H_1 \\
(2\ 3)H_1 &= \{(2\ 3)e = (2\ 3), (2\ 3)(1\ 2) = (1\ 3\ 2)\} = (1\ 3\ 2)H_1 \\
\mathcal{G}_3/H_1 &= \{e, (1\ 2)\} \sqcup \{(1\ 3), (1\ 2\ 3)\} \sqcup \{(2\ 3), (1\ 3\ 2)\} \\
H_1\backslash\mathcal{G}_3 &= \{H_1e = H_1(1\ 2), H_1(1\ 3) = H_1(1\ 3\ 2), H_1(2\ 3) = H_1(1\ 2\ 3)\} \\
H_1(1\ 3) &= \{e(1\ 3) = (1\ 3), (1\ 2)(1\ 3)\} = (1\ 3\ 2) = H_1(1\ 3\ 2) \\
&= \{e, (1\ 2)\} \sqcup \{(1\ 3), (1\ 3\ 2)\} \sqcup \{(2\ 3), (1\ 2\ 3)\}
\end{aligned}
$$

ここで

$$\mathcal{G}_3/H_1 \neq H_1\backslash\mathcal{G}_3$$

である．

H_2 による左剰余類の集合

$$
\begin{aligned}
\mathcal{G}_3/H_2 &= \{eH_2, (1\ 2)H_2\}, \\
eH_2 &= \{e, (1\ 2\ 3), (1\ 3\ 2)\}, \\
(1\ 2)H_2 &= \{(1\ 2), (1\ 2)(1\ 2\ 3) = (2\ 3), (1\ 2)(1\ 3\ 2) = (1\ 3)\} \\
H_2\backslash\mathcal{G}_3 &= \{H_2e, H_2(1\ 2)\} \\
H_2e &= H_2, \\
H_2(1\ 2) &= \{e(1\ 2), (1\ 2\ 3)(1\ 2) = (1\ 3), (1\ 3\ 2)(1\ 2) = (2\ 3)\}, \\
\mathcal{G}_3/H_2 &= \{e, (1\ 2\ 3), (1\ 3\ 2)\} \sqcup \{(1\ 2), (1\ 3), (2\ 3)\} = H_2\backslash\mathcal{G}_3
\end{aligned}
$$

ここで

$$\mathcal{G}_3/H_2 = H_2\backslash\mathcal{G}_3$$

である．

4　正規部分群と剰余群

命題 4.1 H を G の部分群とする．G の H による左類別と右類別が類別として一致するための必要十分条件は任意の $a \in G$ に対して

$$aHa^{-1} = H$$

が成立すること．

定義 4.2 (正規部分群)
$N \leqq G, G$ の任意の元 g に対して，$gNg^{-1} = N$ とする．このとき，N を G の正規部分群(normal subgroup)という．記号として，$N \triangleleft G$ または $G \triangleright N$ と書くことにする．

命題 4.3 $H \leqq G$，任意の $g \in G$ に対して $gHg^{-1} \subset H$ ならば，$H \triangleleft G$.

Proof. $\forall g \in G$ に対し，$gHg^{-1} \subset H$ ならば，

$$H \subset g^{-1}Hg = g^{-1}H\left(g^{-1}\right)^{-1}$$

であり，g^{-1} も G の任意の元を表すので，

$$gHg^{-1} \subset H \Rightarrow H \subset gHg^{-1}$$

である．よって

$$gHg^{-1} = H$$

□

N を群 G の正規部分群とすると，N による剰余 (商) 集合に群構造を導入することができる．

命題 4.4 $N \triangleleft G$．このとき，剰余集合 G/N は自然に群をなす．すなわち，G/N 上の群演算を

$$xN \cdot yN = (xy)N$$

によって定義することができる．

Proof. well-defined であることを確かめる (演算の定義が剰余類の代表元の選び方によらないことを示す必要がある)．つまり，

$$xN = x'N, yN = y'N \Rightarrow xyN = x'y'N$$

を示す必要がある．このとき，$x = x'h, y = y'h'$ を満たす $h, h' \in N$ が存在する．よって

$$xy = x'hy'h' = x'y'\left(y'^{-1}hy'\right)h' \in x'y'N$$

ここで ${y'}^{-1}hy' \in {y'}^{-1}Ny' = N$.
(その他の群としての性質についても省略) □

定義 4.5 $N \triangleleft G$．このとき，剰余集合 G/N を剰余群 (residue class group) または商群 (quotient group) という．

Remark $N \triangleleft G$ とする．剰余群 G/N の単位元は $C_N(e) = eN$．剰余群 G/N の元 $C_N(a) = aN$ の逆元は $C_N\left(a^{-1}\right) = a^{-1}N$

定義 4.6 (単純群)
正規部分群が (単位群と自分自身以外に)1 つもない群を単純群という．
cf. 有限単純群の分類 (巡回，交代，リー型，散在) モンスター群の位数 $\approx 8 \times 10^{53} \gg 6 \times 10^{23}$(アボガドロ数).