応用代数学

2022 年 10 月 31 日現在

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

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

- (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,

$$x\neq y\Rightarrow z\circ x\neq z\circ y,\quad x\circ z\neq y\circ z$$

[*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

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． □

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

[*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

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.

1.1.1 群の例

- 巡回群 C_n

  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.

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

– 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
$$U_n = \left\{g \in GL_n(\mathbb{C}) \mid \overline{{}^t g} \cdot g = 1\right\}$$

1.2 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.

1.3 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. $S(X) = \{f \in M(X) \mid f\text{は全単射}\}$ 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

[*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．

巡回置換の記号

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

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

2 部分群

定義 2.1 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 2.2 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. □

2.1 準同型写像

準同形写像: 群の二項演算を保つ変換” 代数的構造を保つ写像”
cf. ベクトル空間における線形写像