群論入門

大学院副コース　情報の取得と解析

蒲谷　祐一

第 1 回（11 月 2 日）

0. 群とは

群（ぐん）とは，集合に掛け算の仕方を定めたもの

掛け算の構造を用いて，

- 物の対称性や動きを記述
  - 空間の中の物体の動きを記述
- 物事の中の代数的構造を取り出し，利用する
  - ルービックキューブの組み合わせの個数や最小手数を調べる

    https://en.wikipedia.org/wiki/Optimal_solutions_for_Rubik%27s_Cube

1. 集合論の復習（集合）

集合とは，もの（要素，あるいは，元と呼ばれる）の集まり.

$X = \{a, b, c\}$　X は 3 つの要素 a, b, c からなる集合

x が X の元であるとき $x \in X$ と表し,
x が X の元でないとき $x \notin X$ と表す.

有限個の元からなる時有限集合，そうでない時無限集合という.

$\mathbb{N}$: 自然数全体の集合，つまり $\mathbb{N} = \{1, 2, 3, 4, \cdots\}$
$1 \in \mathbb{N}$ だが，$-1 \notin \mathbb{N}$ である.

$$\{x \in X \mid x \text{ に関する条件 }\}$$

で条件を満たす元のみを集めた集合を表す.

$\mathbb{Z}$: 整数全体の集合，つまり $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \cdots\}$

$$\{n \in \mathbb{Z} \mid n > 0\} = \{1, 2, 3, 4, \cdots\} = \mathbb{N}$$

1. 集合論の復習（部分集合）

A, B を集合とする.

全ての A の要素が B の要素でもある時，$A \subset B$ または $B \supset A$ で表す.

$A = \{1, 3, 5\}$, $B = \{1, 2, 4\}$, $C = \{1, 2, 3, 4, 5\}$ のとき，
$A \subset C$, $B \subset C$ である. しかし $A \subset B$ でも $A \supset B$ でもない.

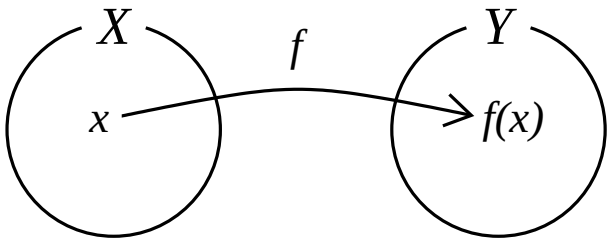
$\mathbb{N}$: 自然数全体の集合, $\mathbb{Z}$: 整数全体の集合
$\mathbb{R}$: 実数全体の集合, $\mathbb{C}$: 複素数全体の集合
のとき

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{R} \subset \mathbb{C}$$

要素を全く持たない集合を空集合といい $\emptyset$ で表す.
全ての集合は $\emptyset$ を部分集合に持つことに注意.

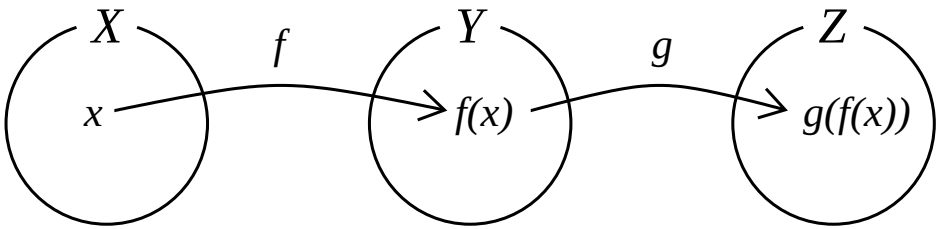
1. 集合論の復習（写像）

X, Y を集合とする．X の元 x に，Y の元 $y = f(x)$ を対応させる物を写像または関数という．これを $f : X \to Y$ のように表す．



$f : X \to Y$ と $g : Y \to Z$ を写像とする．$x \in X$ に $g(f(x))$ を対応させることで X から Z への写像が得られる．これを $g \circ f$ で表し，写像の合成と言う．すなわち

$$(g \circ f)(x) = g(f(x))$$



1. 集合論の復習（直積集合）

集合 X, Y に対して直積集合を

$$X \times Y = \{(x, y) \mid x \in X,\ y \in Y\}$$

で定義する.

$X = \{a, b, c\}$, $Y = \{1, 2\}$ のとき

$$X \times Y = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$$

同様に X が m 個，Y が n 個の有限集合とすると，$X \times Y$ は mn 個の有限集合となる.

$X \times X$ を X^2, $X \times X \times X$ を X^3, ... のように表す.

$\mathbb{R}$ を実数全体の集合とする.
$\mathbb{R}^2 = \{(x, y) \mid x, y \in \mathbb{R}\}$ は x を x-座標，y を y-座標と思うことで「平面」とみなせる．同様に $\mathbb{R}^3$ を「空間」とみなせる.

2. 群の定義

定義

集合 G と写像 $\mathrm{m} : G \times G \to G$ が次の性質を満たす時，G は群 (group) であるという．

(G1) $\mathrm{m}(\mathrm{m}(a,b),c) = \mathrm{m}(a,\mathrm{m}(b,c))$ （結合法則）

(G2) G の元 e で，全ての $a \in G$ に対して

$$\mathrm{m}(a,e) = \mathrm{m}(e,a) = a$$

となるものが存在（単位元の存在）

(G3) 全ての $a \in G$ に対して G の元 a^{-1} で

$$\mathrm{m}(a,a^{-1}) = \mathrm{m}(a^{-1},a) = e$$

を満たすものが存在（逆元の存在）

m は multiplication （掛け算）の m．乗法ともいう．
普通は $\mathrm{m}(a,b)$ を単に ab と省略し次の様に表される：

2. 群の定義

定義

集合 G が次の性質を満たす時,

(G1) $(ab)c = a(bc)$ （結合法則）

(G2) G の元 e で，全ての $a \in G$ に対して

$$ae = ea = a$$

となるものが存在（単位元の存在）

(G3) 全ての $a \in G$ に対して G の元 a^{-1} で

$$aa^{-1} = a^{-1}a = e$$

を満たすものが存在（逆元の存在）

(G1) の性質を結合法則とよぶ．(G2) を満たす e を単位元という．単位元は 1 と書かれる事も多い．(G3) を満たす a^{-1} を a の逆元という．

2. 群の定義（例）

整数全体の集合を $\mathbb{Z}$ とする．$\mathbb{Z}$ の元 a, b に対して

$$\mathrm{m}(a, b) := a + b$$

と定義する．

$$\mathrm{m}(\mathrm{m}(a, b), c) = (a + b) + c = a + (b + c) = \mathrm{m}(a, \mathrm{m}(b, c))$$

より (G1) が成り立つ．e として 0 を取れば

$$\mathrm{m}(a, 0) = a + 0 = a = 0 + a = \mathrm{m}(0, a)$$

なので (G2) をみたす．$a \in \mathbb{Z}$ に対して a^{-1} として $-a$ を取れば

$$\mathrm{m}(a, a^{-1}) = a + (-a) = 0 = (-a) + a = m(a^{-1}, a)$$

で (G3) をみたす．

全ての $a, b \in G$ に対し $ab = ba$ が成り立つ時，群 G を可換群，またはアーベル群という．可換群では乗法 ab を $a + b$，単位元 e を 0，逆元 a^{-1} を $-a$ と書くことがある．(上の例は可換群である．)

2. 群の定義（例）

$$\mathrm{SL}(2,\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a,b,c,d \in \mathbb{Z}, \quad ad-bc=1 \right\}$$

とすると $\mathrm{SL}(2,\mathbb{Z})$ は行列の積を乗法として群になる．単位元は単位行列 $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ で，逆元は逆行列

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

で与えられる．実際 $A,B,C \in \mathrm{SL}(2,\mathbb{Z})$ とすると，これらは 2×2 正則行列であるから，

$$\text{(G1) } (AB)C = A(BC) \quad \text{(G2) } AI = IA = A \quad \text{(G3) } AA^{-1} = A^{-1}A = I$$

が成立する．一般には $AB \neq BA$ であるから $\mathrm{SL}(2,\mathbb{Z})$ は可換ではない（非可換群という）．

$*$ この例で $\mathbb{Z}$ を $\mathbb{R}$ や $\mathbb{C}$ としても群になる．

2. 群の定義

定理

(G2) を満たす e は唯一つに定まる．G の元 a に対して (G3) を満たす a^{-1} は唯一つに定まる．

(G1) $(ab)c = a(bc)$
(G2) $e \in G$ で，全ての $a \in G$ に対して $ae = ea = a$ となるものが存在
(G3) 全ての $a \in G$ に対して $aa^{-1} = a^{-1}a = e$ となる a^{-1} が存在

Proof.

e と e' を単位元とすると $e = e'$ となることを示す．e が単位元であることから $e' = ee'$．e' が単位元であることから $ee' = e$ である．合わせて $e = e'$.
x と y を a の逆元とする．同様に $x = y$ が示せれば良い．

$$x = xe = x(ay) = (xa)y = ey = y$$

よって $x = y$. □

2. 群の定義（部分群）

定義

群 G の空でない部分集合 H が

(1) $a, b \in H \Longrightarrow ab \in H$

(2) $a \in H \Longrightarrow a^{-1} \in H$

を満たす時，H は G の部分群 (subgroup) であるという．

定理

群 G の部分群 H は G の乗法に関して群になる．

(G1) $(ab)c = a(bc)$　(G2) 単位元 $e \in G$ が存在
(G3) 全ての $a \in G$ に対して逆元 a^{-1} が存在

Proof.

(G1) G で (G1) が成り立つのでその部分集合 H でも成り立つ．
(G2) H は空ではないので $a \in H$ が存在．(2) より $a^{-1} \in H$．(1) より $e = aa^{-1} \in H$．e は G で単位元なので，その部分集合 H でも単位元．
(G3) 全ての $a \in H$ に対し (2) より $a^{-1} \in H$． □

2. 群の定義（部分群）

群 G の空でない部分集合 H が

$$(1)\ a, b \in H \Longrightarrow ab \in H, \quad (2)\ a \in H \Longrightarrow a^{-1} \in H$$

を満たす時 G の部分群 (subgroup) であるという.

$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \cdots\}$, $H = \{0, \pm 2, \pm 4, \pm 6, \cdots\}$ （偶数全体の集合）とすると， H は $\mathbb{Z}$ の部分群. (1) は「偶数 + 偶数 = 偶数」より. (2) も明らか.

$$\mathrm{SL}(2, \mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; \begin{array}{c} a, b, c, d \in \mathbb{Z}, \\ ad - bc = 1 \end{array} \right\}, \quad P = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \;\middle|\; n \in \mathbb{Z} \right\}$$

とすると，$P \subset \mathrm{SL}(2, \mathbb{Z})$ は部分群. 実際,

$$(1) \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & m+n \\ 0 & 1 \end{pmatrix} \in P, \quad (2) \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \in P$$

2. 群の定義（部分群）

定理

群 G の部分集合 X に対し，

$$\langle X \rangle = \{x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} \mid x_1, \ldots, x_n \in X, \quad \varepsilon_1, \ldots, \varepsilon_n = \pm 1\}$$

（つまり $\langle X \rangle$ は X の元と X の逆元の積で書ける G の元全体）

とすると $\langle X \rangle$ は G の部分群である．

(G1) 結合法則，と (G2) 単位元の存在，は明らか．(G3) 逆元の存在は次から直ちに従う．

群 G の元 $a_1, \ldots, a_n$ に対し，

$$(a_1 a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} a_1^{-1}.$$

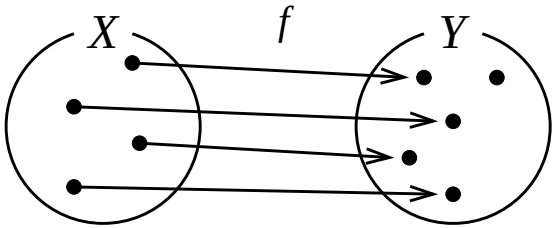
$\langle X \rangle$ は X を含む最小の G の部分群になる．$\langle X \rangle$ を X で生成される部分群という．

$\mathbb{Z} \supset X = \{2\}$ のとき $\langle X \rangle = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$
$\mathbb{Z} \supset X = \{2, 3\}$ のとき $\langle X \rangle = \{0, \pm 1, \pm 2, \pm 3, \ldots\} = \mathbb{Z}$ （$3 - 2 = 1$ より）

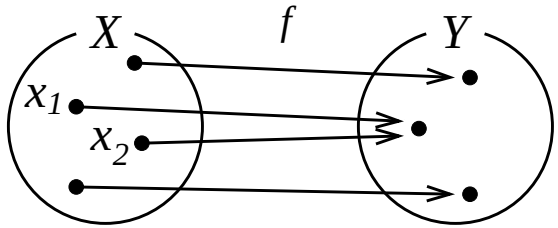
3. 置換群

X, Y を集合とする．写像 $f : X \to Y$ が

- 全ての $y \in Y$ に対して $f(x) = y$ となる $x \in X$ が存在する時，f は全射であるという．
- 全ての $x_1, x_2 \in X$ に対して $f(x_1) = f(x_2)$ ならば $x_1 = x_2$ である時，f は単射であるという．

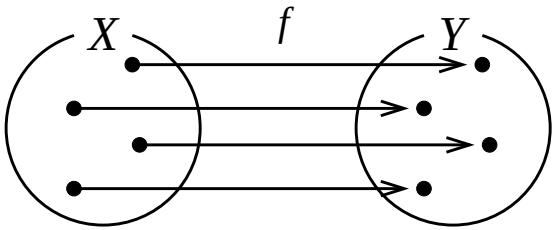


全射でない

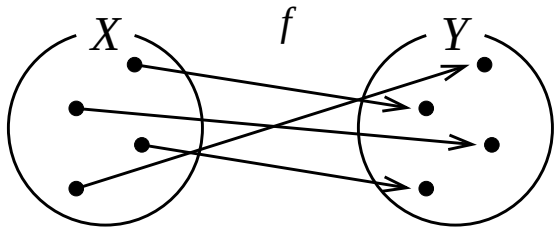


単射でない

- 全射かつ単射の写像を全単射という．



全単射

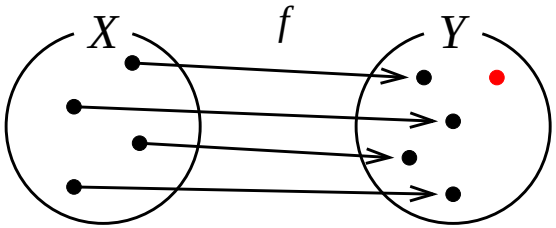


これも全単射

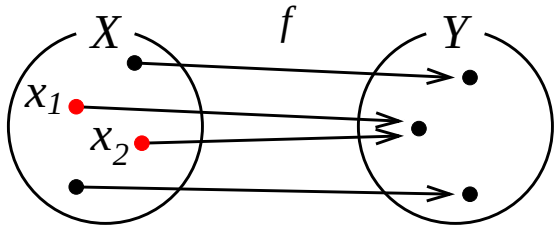
3. 置換群

X, Y を集合とする．写像 $f : X \to Y$ が

- 全ての $y \in Y$ に対して $f(x) = y$ となる $x \in X$ が存在する時，f は全射であるという．
- 全ての $x_1, x_2 \in X$ に対して $f(x_1) = f(x_2)$ ならば $x_1 = x_2$ である時，f は単射であるという．

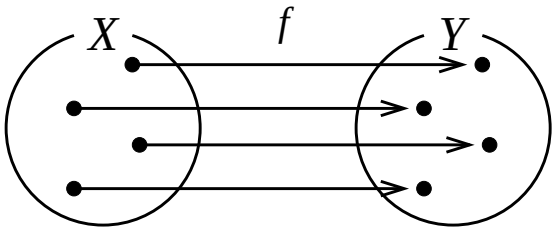


全射でない

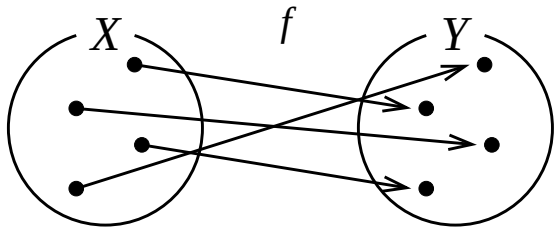


単射でない

- 全射かつ単射の写像を全単射という．



全単射

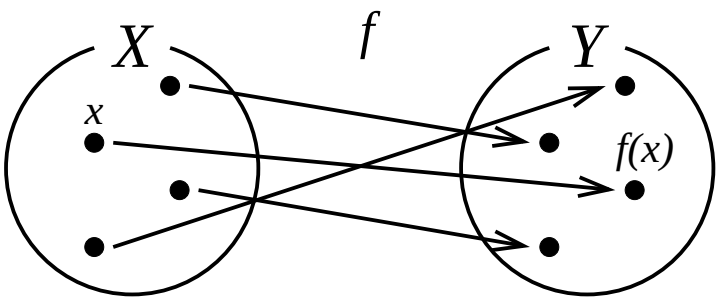


これも全単射

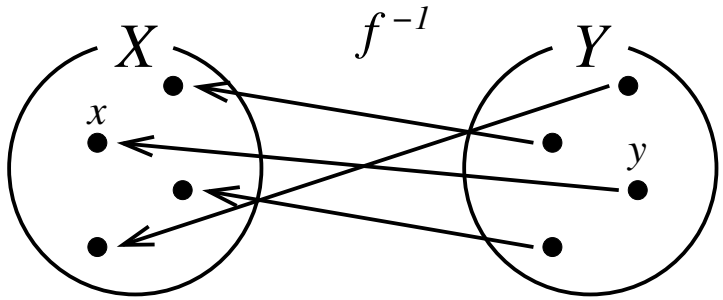
3. 置換群

$f : X \to Y$ を全単射とする.

$y \in Y$ に $f(x) = y$ となる $x \in X$ を対応させることで Y から X への写像を定義することができる. これを f の逆写像といい, $f^{-1} : Y \to X$ で表す. (逆写像は全単射になることがわかる.)



全単射 f



f の逆写像

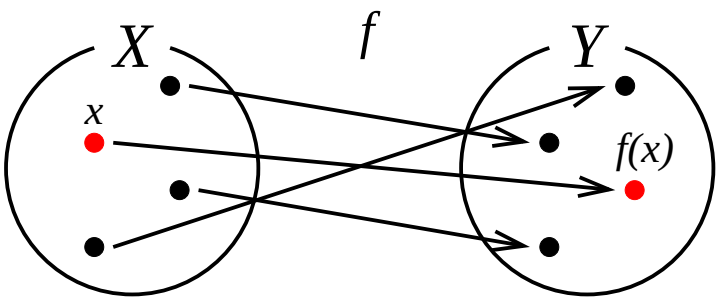
X の元の個数が n である時, X から X への全単射は $n!$ 個ある.
($n!$ は n の階乗を表す. すなわち $n! = n(n-1)\cdots 2 \cdot 1$.)

これは $X = \{x_1, \ldots, x_n\}$ のとき $f(x_1)$ の決め方が n 通り, $f(x_2)$ の決め方が $n-1$ 通り, $\cdots$, と考えれば分かる.

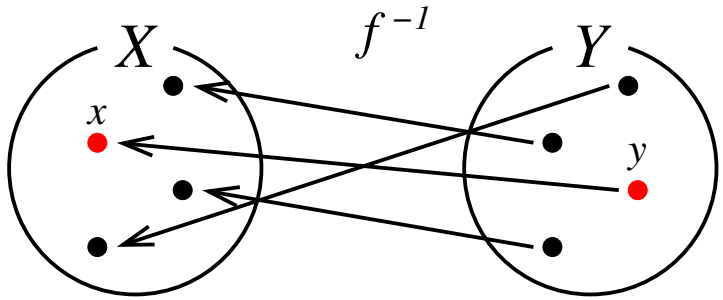
3. 置換群

$f : X \to Y$ を全単射とする.

$y \in Y$ に $f(x) = y$ となる $x \in X$ を対応させることで Y から X への写像を定義することができる. これを f の逆写像といい, $f^{-1} : Y \to X$ で表す. (逆写像は全単射になることがわかる.)



全単射 f



f の逆写像

X の元の個数が n である時, X から X への全単射は $n!$ 個ある.
($n!$ は n の階乗を表す. すなわち $n! = n(n-1)\cdots 2 \cdot 1$.)

これは $X = \{x_1, \ldots, x_n\}$ のとき $f(x_1)$ の決め方が n 通り, $f(x_2)$ の決め方が $n-1$ 通り, $\cdots$, と考えれば分かる.

3. 置換群

有限集合 $\{1, 2, \ldots, n\}$ からそれ自身への全単射 σ は $\sigma(1), \ldots, \sigma(n)$ で完全に決定される．そこで σ を

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

のように表す事とする．

$$S_n = \{\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} \mid \ \sigma \text{ は全単射 }\}$$

と置く．S_n の個数は $\{1, 2, \ldots, n\}$ の並べ方の総数に等しいから $n!$ である．

S_n の元 σ と τ に対して乗法を合成写像 $\sigma\tau = \sigma \circ \tau$ で定義する．

3. 置換群

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

とすると σ と τ の積 $\sigma\tau$ は

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

となる．これは次のように図示できる：

$$\begin{array}{ccccc} 1 & 2 & 3 & & 1 \ 2 \ 3 \\ & \downarrow & \tau & & \\ 2 & 1 & 3 & & \downarrow \ \sigma\tau \\ & \downarrow & \sigma & & \\ 2 & 3 & 1 & & 2 \ 1 \ 3 \end{array}$$

3. 置換群

$$S_n = \{\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} \mid \ \sigma \text{ は全単射 } \}$$

S_n の元 σ と τ に対して乗法を合成写像 $\sigma\tau = \sigma \circ \tau$ で定義した.

このとき，恒等写像（全ての k に対して $\sigma(k) = k$ となる S_n の元）を単位元，逆写像を逆元として S_n は群になる.

この群 S_n を置換群 (permutation group)，または対称群 (symmetric group) という.

3. 置換群

定理

全ての有限群 G はある置換群 S_n の部分群として表される.

ここで「表される」を数学的な言葉で表現すると，次のようになる.

定理

全ての有限群 G はある置換群 S_n の部分群に同型である.

次回は同型などの用語の説明をしていく.