大学院副コース　情報の取得と解析「群論入門」資料

情報システム工学科　蒲谷　祐一（かばや　ゆういち）

∗ レポート問題を除いた web 公開用

1. 集合論から

X を集合とする．x が X の元であるとき $x \in X$ と表し，x が X の元でないときは $x \notin X$ と表す．例えば $\mathbb{N}$ を自然数全体の集合とすると，$1 \in \mathbb{N}$ だが，$-1 \notin \mathbb{N}$ である．X と 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**という．このとき X から Y への写像を

$$f : X \to Y$$

のように表す．

写像 $f : X \to Y$ と $g : Y \to Z$ が与えられたとき，$x \in X$ 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 $g \circ f$ と書き，写像の**合成**と言う．すなわち

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

となる．

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．
- 全射かつ単射の写像を**全単射**という．

$f : X \to Y$ が全単射の時，$y \in Y$ に対して $f(x) = y$ 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．

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．例えば 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．

2. 群

2.1. 群の定義.

定義 1. 集合 G と写像 $\mathrm{m} : G \times G \to G$ が次の性質を満たす時，**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**）

普通は $\mathrm{m}(a, b)$ を単に ab と省略し次の様に表される：

(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**）

命題 2.1. (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) 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．

例 1. 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

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

で (G3) をみたす．

例 2.

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

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 $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ で，逆元は逆行列 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ で与えられる．

定義 2. 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．

例えば，例 1 の $\mathbb{Z}$ は可換群であるが，例 2 の $\mathrm{SL}(2, \mathbb{Z})$ は可換群ではない．

2.2. 部分群.

定義 3. 群 G の空でない部分集合 H が

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

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

を満たす時 G の**部分群** (subgroup) であるという．

命題 2.2. 群 G の部分群 H は G の乗法に関して群になる．

例 3. $\mathbb{Z}$ の部分集合として偶数全体の集合 $\{0, \pm 2, \pm 4, \dots\}$ をとると，これは $\mathbb{Z}$ の部分群である．

例 4. $P = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \;\middle|\; b \in \mathbb{Z} \right\}$ と置くと P は例 2 の $\mathrm{SL}(2, \mathbb{Z})$ の部分群である．

命題 2.3. 群 G の部分集合 X に対し，

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

（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．

$\langle X \rangle$ は X を含む最小の G の部分群である．命題 2.3 の証明で，逆元の存在は次の補題から直ちに従う．

補題 2.4. 群 G の元 $a_1, \dots, a_n$ に対し，

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

例 5. $X_1 = \{2\} \subset \mathbb{Z}$ とすると，$\langle X_1 \rangle = \{0, \pm 2, \pm 4, \dots\}$ である．$X_2 = \{2, 3\} \subset \mathbb{Z}$ とすると，$\langle X_2 \rangle = \mathbb{Z}$ である．

2.3. **置換群.** 有限集合 $\{1, 2, \dots, n\}$ からそれ自身への全単射 σ は $\sigma(1), \dots, \sigma(n)$ 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．

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

と置く．S_n の個数は $\{1, 2, \dots, n\}$ 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 $\sigma\tau = \sigma \circ \tau$ で定義すると，恒等写像（全ての $k = 1, \dots, n$ 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[1]．S_n の元は**置換**とよばれる[2].

例 6.

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

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：

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

定義 4. 群 G から群 H への写像 $f : G \to H$ が

$$f(ab) = f(a)f(b) \quad (a, b \in G)$$

を満たす時，**準同型（写像）** (homomorphism) であるという．全単射である準同型を**同型（写像）** (isomorphism) という．

問題 1. 同型写像の逆写像は同型写像であることを示せ．

定義 5. 群 G から群 H へ同型写像が存在する時，G と H は**同型** (isomorphic) であるという．G と H が同型であることを $G \cong H$ で表す．

同型な群は同じ群であるとみなせる．次の定理から全ての有限群はある置換群の部分群として実現できることがわかる．

定理 2.5. 有限群 G はある置換群 S_n の部分群に同型である．

証明. 概略を述べる．G の元 a に対して $\varphi(a) : G \to G$ を

$$\varphi(a)(g) := ag$$

で定める．$\varphi(a^{-1})$ は $\varphi(a)$ の逆写像であることが示せるので，$\varphi(a)$ は全単射であることがわかる．G は有限集合なので $G = \{g_1, \dots g_n\}$ と表せば，$\varphi(a) : G \to G$ は $\{1, 2, \dots, n\}$ から $\{1, 2, \dots, n\}$ への全単射と思える．すなわち $\varphi(a)$ を置換群 S_n の元と同一視できる．これにより $\varphi : G \to S_n$ を定めると，φ は準同型かつ単射であることが示せる．よって φ は G から φ の像 $\varphi(G)(\subset S_n)$ への同型を与える． □

[1] S_n は $\mathfrak{S}$ (ドイツ文字の S) を使って $\mathfrak{S}_n$ とも書かれる．

[2] 置換はギリシャ文字の σ, τ を使って表されることが多い．

2.4. **巡回群.** 自然数 n に対して

$C_n = \{x^0 = 1, x^1 = x, x^2, \dots, x^{n-1}\}$ （n 個からなる集合）

を考える．乗法を $x^k \cdot x^l = x^{k+l}$ で定める．ただし $x^n = 1$ とする．この時 C_n は 1 を単位元とする群になる．この群を**巡回群** (cyclic group) という．巡回群 C_n は 1 つの元 x で生成される．

問題 2. 逆に 1 つの元で生成される有限群は巡回群と同型であることを示せ．また 1 つの元で生成される無限群は $\mathbb{Z}$ と同型であることを示せ．（よって $\mathbb{Z}$ は**無限巡回群** (infinite cyclic group) ともよばれる．）

例 7 (定理 2.5 の簡単な例).

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix} \in S_n$$

とおくと，

$$\sigma^2 = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 3 & 4 & \dots & 1 & 2 \end{pmatrix}$$

$$\vdots$$

$$\sigma^{n-1} = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ n & 1 & \dots & n-2 & n-1 \end{pmatrix}$$

$$\sigma^n = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 1 & 2 & \dots & n-1 & n \end{pmatrix} = 1$$

となる．よって $\varphi : C_n \to S_n$ を $\varphi(x^k) = \sigma^k$ で定めると φ は C_n から $\langle \sigma \rangle \subset S_n$ への同型を与える．

例 7 の σ は**巡回置換**とよばれ $(1\,2 \cdots n)$ と書かれる．次のように一般化される．例えば S_4 の中で考える時，

$$(2\,3\,4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \quad (1\,4\,2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

のように定めることにする．

例 8. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} = (1\,3)(2\,4\,5)$. （これは $(2\,4\,5)(1\,3)$ とも書ける．）

問題 3. 全ての置換群の元は巡回置換の積で書ける事を示せ．

2.5. **剰余類分解.** G を群，H をその部分群とする．元 $a \in G$ に対して

$$aH = \{ah \mid h \in H\}, \quad Ha = \{ha \mid h \in H\}$$

と書くことにする．

例 9. $G = \mathbb{Z}$ と $H = \langle 3 \rangle = \{0, \pm 3, \pm 6, \pm 9, \dots\}$ に対して，

$$0 + H = \{\dots, -6, -3, 0, 3, 6, \dots\},$$
$$1 + H = \{\dots, -5, -2, 1, 4, 7, \dots\},$$
$$2 + H = \{\dots, -4, -1, 2, 5, 8, \dots\},$$

である．よって

$$\mathbb{Z} = (0 + H) \sqcup (1 + H) \sqcup (2 + H)$$

である．ここで $A \sqcup B$ は $A \cap B = \emptyset$ である場合の和集合 $A \cup B$ で**非交和** (disjoint union) とよばれる．

一般に，群 G と部分群 H に対して

$$G = \bigsqcup_{i \in I} a_i H$$

と G を $a_i H$ の非交和に分割することができる．各 $a_i H$ を**剰余類** (coset) といい，この分割を **剰余類分解** (coset decomposition) という．

群 G の個数を $|G|$ で表すことにする．（G が無限なら $|G| = \infty$ と表す．）$|G|$ を G の**位数** (order) という．

定理 2.6. 有限群 G とその部分群 H に対して，$|H|$ は $|G|$ の約数である．（これを $|G| = [G : H]\,|H|$ と表す．$[G : H]$ を（G における） H の**指数** (index) という．）

3. 準同型定理

定義 6. 群 G の部分群 N が全ての $g \in G$ に対して $gN = Ng$ をみたす時，N を**正規部分群** (normal subgroup) であるという．

群 G と正規部分群 N に対し，集合

$$G/N := \{gN \mid g \in G\}$$

を考える．G/N の 2 つの元 g_1N と g_2N に対し乗法を

$$(g_1N)(g_2N) = g_1Ng_2N = g_1g_2NN = g_1g_2N$$

で定めることができる．この時 G/N は $N = eN$ を単位元とする群になる．G/N を**剰余群** (quotient group) という．定義から剰余類分解 $G = \bigsqcup_{i\in I} a_iN$ の I と G/N は 1 対 1 に対応することがわかる．特に $|G/N| = [G : N]$ が成り立つ．

群 G から群 H への準同型 $f : G \to H$ に対して

$$\operatorname{Im} f = \{f(g) \mid g \in G\}, \quad \operatorname{Ker} f = \{g \in G \mid f(g) = e_H\}$$

とおく．ただし e_H は H の単位元を表す．$\operatorname{Im} f$ は f の**像** (image)，$\operatorname{Ker} f$ は f の**核** (kernel) と呼ばれる．

問題 4. $\operatorname{Im} f$ は H の部分群，$\operatorname{Ker} f$ は G の正規部分群になることを示せ．

定理 3.1 (準同型定理)**.** f を群 G から群 H への準同型とする．$\operatorname{Im} f$ は $G/\operatorname{Ker} f$ と同型（$G/\operatorname{Ker} f \cong \operatorname{Im} f$）．

例 10. $\mathbb{Z}$ を整数全体のなす群，$C_3 = \{1, x, x^2\}$ を位数 3 の巡回群とする．写像 $f : \mathbb{Z} \to C_3$ を $f(k) = x^k$ で定義すると f は準同型になる．$\operatorname{Im} f = C_3$ は明らかである．また

$$\operatorname{Ker} f = \{0, \pm 3, \pm 6, \pm 9, \dots\} = 3\mathbb{Z}$$

である．よって $C_3 \cong \mathbb{Z}/3\mathbb{Z}$.

一般に $C_n \cong \mathbb{Z}/n\mathbb{Z}$ であることから，位数 n の巡回群 C_n は $\mathbb{Z}/n\mathbb{Z}$，あるいは省略して $\mathbb{Z}/n$，$\mathbb{Z}_n$ と書かれる．

4. 計算機による有限群の計算例

4.1. **Sage.** 群の計算を行うプログラムはいろいろあると思うが，ここでは Sage (`http://www.sagemath.org`) を使った計算例を紹介する．置換群 S_5 の 2 つの元

$$(1\,2\,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}, (2\,4)(3\,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 2 & 3 \end{pmatrix}$$

で生成される群について調べてみよう．

```
sage: G = PermutationGroup([[(1,2,5)], [(2,4),(3,5)]])
sage: G.order()
60
```

よって位数 60 の S_5 の部分群であることがわかる．（S_5 の位数は $5! = 120$ であった．定理 2.6 と比べよ．）例えば群の乗法は次のようにして求められる：

```
sage: G.gens()
[(2,4)(3,5), (1,2,5)]
sage: b, a = G.gens()
sage: print a, b, b*a*(b.inverse())
(1,2,5) (2,4)(3,5) (1,4,3)
```

例えば部分群を何個持つか調べるには次のようにすればよい：

```
sage: len(G.subgroups())
59
```

4.2. **ルービックキューブの群.** ルービックキューブは立方体の各面に 9 つずつ四角があるので，合計で $6 \times 9 = 54$ の四角からなる．各面を回転させるとき中心は動かないので，$54 - 6 = 48$ 個の四角のみ考えればよい．それぞれの四角に次のように番号を付ける．

```
                +--------------+
                |  1    2    3 |
                |  4   up    5 |
                |  6    7    8 |
+---------------+--------------+--------------+---------------+
|  9  10  11 | 17   18   19 | 25   26   27 | 33  34  35 |
| 12 left 13 | 20  front 21 | 28 right 29 | 36 back 37 |
| 14  15  16 | 22   23   24 | 30   31   32 | 38  39  40 |
+---------------+--------------+--------------+---------------+
                | 41   42   43 |
                | 44  down  45 |
                | 46   47   48 |
                +--------------+
```

各面での回転はこの 1 から 48 の数字の入れ替えで表されるので，置換を用いて表すことができる．例えば前面 front での 90° 回転を巡回置換の積で表すと

$$(17, 19, 24, 22)(18, 21, 23, 20)(6, 25, 43, 16)(7, 28, 42, 13)(8, 30, 41, 11)$$

となる．すべてのルービックキューブの組み合わせは各面での 90° 回転を有限回繰り返すことで得られるのでこれらの置換で生成される S_{48} の部分群と 1 対 1 に対応する．

```
sage: f=[(17,19,24,22),(18,21,23,20),\
         ( 6,25,43,16),( 7,28,42,13),( 8,30,41,11)]
sage: b=[(33,35,40,38),(34,37,39,36),\
         ( 3, 9,46,32),( 2,12,47,29),( 1,14,48,27)]
sage: l=[( 9,11,16,14),(10,13,15,12),\
         ( 1,17,41,40),( 4,20,44,37),( 6,22,46,35)]
sage: r=[(25,27,32,30),(26,29,31,28),\
         ( 3,38,43,19),( 5,36,45,21),( 8,33,48,24)]
sage: u=[( 1, 3, 8, 6),( 2, 5, 7, 4),\
         ( 9,33,25,17),(10,34,26,18),(11,35,27,19)]
sage: d=[(41,43,48,46),(42,45,47,44),(14,22,30,38),\
         (15,23,31,39),(16,24,32,40)]
sage: rubik = PermutationGroup([f,b,l,r,u,d],canonicalize=False)
     # canonicalize=False は生成元の順序を保つため指定
sage: rubik.order()
43252003274489856000
```

よってルービックキューブの組み合わせの数は

$$43,252,003,274,489,856,000$$

となる．次の様にしてルービックキューブを解くことができる：

```
sage: a = rubik.random_element()
sage: F,B,L,R,U,D = rubik.gens()
sage: a.word_problem([F,B,L,R,U,D])
...
```

どんな置換群にでも適用できる手法のためか，出力される結果は一般には非常に長くなる．余談だが別の機能で最小手数の解（90° 回転を 1 回と数えて）も計算してくれる．

```
sage: C = RubiksCube()
sage: C = C.scramble(); C
                +--------------+
                | 48   34   40 |
                |  7   top   4 |
                | 17   37   22 |
+---------------+--------------+--------------+---------------+
| 32  18   6 | 11   12   16 | 41   10  46 | 14   2  38 |
| 15 left 21 | 28  front 42 | 23 right 47 | 39 rear 44 |
| 43  45  19 |  8   36    3 | 33   20  35 |  1  26  30 |
+---------------+--------------+--------------+---------------+
                | 25   29   27 |
                | 31 bottom 13 |
                | 24    5    9 |
                +--------------+

sage: C.solve("optimal") # 最小手数の解法．非常に時間がかかる．
Initializing tables...
Done.
"F  R  F  D  R  L  B' D' F' R' B' U  F' U' R  L2 F' U  R  B' R"
```

どの様なアルゴリズムを使っているか私は理解していないが，ルービックキューブの群や最小手数のアルゴリズムは Wikipedia でも簡単に紹介されている：

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