群論入門

大学院副コース　情報の取得と解析

蒲谷　祐一

第３回（11 月 16 日）

前回

前回の内容：

- 群の定義の復習（特に置換群の図を使った説明）
- 準同型と同型（同型である群は同じ群であるとみなす）
- Cayley の定理（全ての有限群はある置換群の部分群に同型）
- 巡回群（一元生成の群）
- 剰余類分解（すぐあとで復習）

今回の予定：

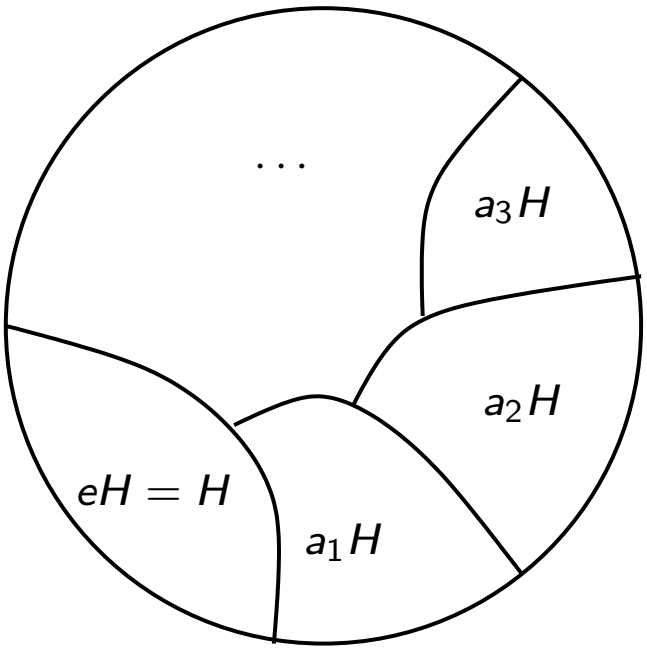
剰余類分解の復習，正規部分群，準同型定理，ルービックキューブの群

剰余類分解の復習

一般に，群 G と部分群 H に対して

$$G = \bigsqcup_{i \in I} a_i H, \qquad a_i H = \{a_i h \mid h \in H\}$$

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．



$|G| =$（群 G の個数），とする．
（$|G|$ を G の位数 (order) という）

定理 (Lagrange の定理)

有限群 G とその部分群 H に対して，$|H|$ は $|G|$ の約数である．

正の整数 $[G : H] = \dfrac{|G|}{|H|}$ を指数 (index) という．（補足 G や H が有限でない場合も $[G : H] = |I|$ で定義する．）

剰余類分解の復習

定理

群 G の位数が素数である時，G は巡回群である．
（つまり $|G| = p$ （p は素数）ならば $G \cong C_p$．（C_n : 位数 n の巡回群））

Proof.

$|G| = p$ とする（p は素数）．$x \in G$ を G の単位元ではない元とする．

x で生成される部分群 $\langle x \rangle$ を考えると，$\langle x \rangle$ は G の部分群であるので，Lagrange の定理から，位数 $|\langle x \rangle|$ は p の約数．つまり $|\langle x \rangle| = 1$ または p．

$|\langle x \rangle| = 1$ ならば $\langle x \rangle = \{e\}$ （e は単位元）より $x = e$ となり x が単位元ではないという仮定に反する．

よって $|\langle x \rangle| = p$．$\langle x \rangle \subset G$ と $|G| = p$ より $\langle x \rangle = G$．つまり G は 1 つの元 x で生成される．「6. 練習問題」より G は巡回群． □

群 G の位数が素数だったら，G の構造は簡単．

8. 正規部分群（準備）

群 G の部分集合 $A, B \subset G$ に対して

$$AB := \{ab \mid a \in A,\ b \in B\}$$

と定める. (定義から $AB \subset G$.)

定理

群 G と部分群 $H \subset G$ に対して

$$HH = H.$$

注意　集合 X の部分集合 A, B について

$$A = B \iff A \subset B \text{ and } A \supset B$$

Proof.

$e \in H$ であった. ($H \neq \emptyset$ より $\exists a \in H$. 部分群の定義 (2) から $a^{-1} \in H$. 部分群の定義 (1) から $aa^{-1} \in H$. よって $e = aa^{-1} \in H$.)
部分群の定義 (1) より $h_1 h_2 \in HH$ ならば $h_1 h_2 \in H$. つまり $HH \subset H$.
$h \in H$ ならば $h = he \in HH$. つまり $HH \supset H$. □

8. 正規部分群

定義

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

$Ng = gN$ は，左から g^{-1} を掛けることで $g^{-1}Ng = N$ とも書ける．

群 G と正規部分群 N に対し，集合

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

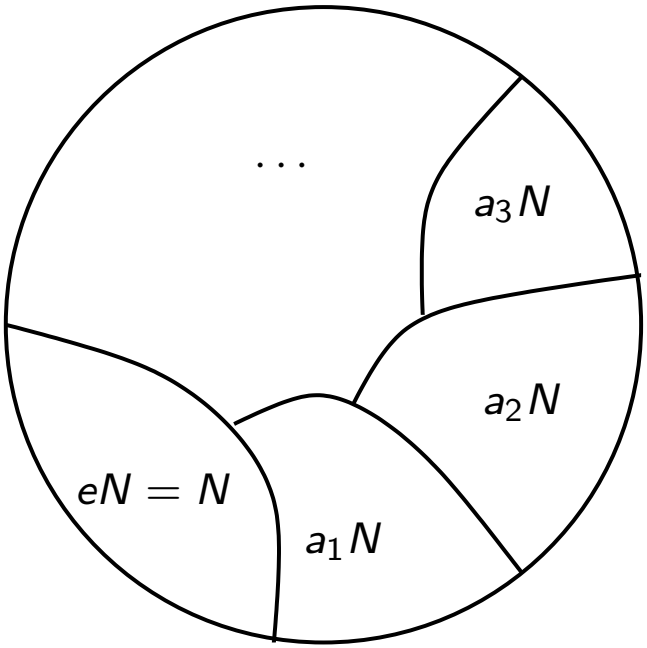
を考える．G/N は剰余類 gN を全部集めたものと思える．G/N の 2 つの元 g_1N と g_2N に対し乗法を

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

で定めると 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．

8. 正規部分群

定義から剰余類分解 $G = \bigsqcup_{i \in I} a_i N$ 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.



$a_i N$ たちに乗法を定めたものが G/N. 添字の集合 I に群の構造を入れたとも思える.

G と N が有限であれば

$$|G/N| = [G : N] = \frac{|G|}{|N|}$$

だから群の “割り算” と思える.

8. 正規部分群

定理 (前回示した)

G, H を群，$f : G \to H$ を準同型とする．e_H を H の単位元とする．

$$\mathrm{Im}(f) = \{f(g) \mid g \in G\} \quad \text{は } H \text{ の部分群.}$$

$$\mathrm{Ker}(f) = \{g \in G \mid f(g) = e_H\} \quad \text{は } G \text{ の部分群.}$$

さらに次が言える．

定理

G, H を群，$f : G \to H$ を準同型とする．$\mathrm{Ker}(f)$ は G の正規部分群.

Proof.

全ての $g \in G$ に対して $g^{-1}\mathrm{Ker}(f)g = \mathrm{Ker}(f)$ を示せばよい．つまり $g^{-1}\mathrm{Ker}(f)g \subset \mathrm{Ker}(f)$ と $g^{-1}\mathrm{Ker}(f)g \supset \mathrm{Ker}(f)$ を示せばよい．

(次ページへ続く)

8. 正規部分群

Proof 続き.

$g^{-1}\mathrm{Ker}(f)g \subset \mathrm{Ker}(f)$ の証明：
$g^{-1}\mathrm{Ker}(f)g$ の元を $a \in \mathrm{Ker}(f)$ を用いて $g^{-1}ag \in g^{-1}\mathrm{Ker}(f)g$ と表す.

$$f(g^{-1}ag) = f(g^{-1})f(a)f(g) = f(g^{-1})e_H f(g) = f(g)^{-1}f(g) = e_H$$

だから $g^{-1}ag \in \mathrm{Ker}(f)$.

$g^{-1}\mathrm{Ker}(f)g \supset \mathrm{Ker}(f)$ の証明：
前半の結果の g を g^{-1} にかえると，$g\mathrm{Ker}(f)g^{-1} \subset \mathrm{Ker}(f)$. 両辺に左から g^{-1}, 右から g を掛けると $\mathrm{Ker}(f) \subset g^{-1}\mathrm{Ker}(f)g$. □

9. 準同型定理

定理 (準同型定理)

f を群 G から群 H への準同型とする．$\mathrm{Im}\, f$ は $G/\mathrm{Ker}\, f$ と同型：

$$G/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$$

同型写像は $\varphi(g\mathrm{Ker}(f)) = f(g)$ で与えられる．

$\mathbb{Z}$ 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．$\mathrm{Im}(f) = C_3$ は明らかである．また

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

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 $\mathbb{Z}/n$，$\mathbb{Z}_n$ などと書かれる．

9. 準同型定理

定理 (準同型定理（再掲）)

f を群 G から群 H への準同型とする．$\mathrm{Im}\, f$ は $G/\mathrm{Ker}\, f$ と同型：

$$G/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$$

同型写像は $\varphi(g\mathrm{Ker}(f)) = f(g)$ で与えられる．

証明の概略.

まず $\varphi(g\mathrm{Ker}(f)) = f(g)$ が‘ちゃんと定まっている’(well-defined) ことを示す必要がある．($g \neq g'$ だけど $g\mathrm{Ker}(f) = g'\mathrm{Ker}(f)$ かもしれないので.)
well-defined が示せれば φ が準同型であることはすぐにわかる：

$$\varphi(a\mathrm{Ker}(f))\varphi(b\mathrm{Ker}(f)) = f(a)f(b) = f(ab) = \varphi(ab\mathrm{Ker}(f)).$$

φ が全射であることは明らか．単射であることは次のように示せる：
$\varphi(a\mathrm{Ker}(f)) = \varphi(b\mathrm{Ker}(f)) \Longleftrightarrow f(a) = f(b) \Longleftrightarrow f(a^{-1}b) = e$
$\Leftrightarrow a^{-1}b \in \mathrm{Ker}(f) \Longleftrightarrow a^{-1}b\mathrm{Ker}(f) = \mathrm{Ker}(f) \Longleftrightarrow b\mathrm{Ker}(f) = a\mathrm{Ker}(f)$ □

9. 準同型定理

定理 (準同型定理（再掲）)

f を群 G から群 H への準同型とする．$\mathrm{Im}\, f$ は $G/\mathrm{Ker}\, f$ と同型：

$$G/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$$

同型写像は $\varphi(g\mathrm{Ker}(f)) = f(g)$ で与えられる．

次は準同型定理から直ちに従う．（直接証明するのも難しくない．）

練習問題

G, H を群とする．準同型 $f : G \to H$ に対して

$$f \text{ が単射} \iff \mathrm{Ker}(f) = \{e\}$$

10. ルービックキューブの群（準備：巡回置換）

S_n の元

$$\begin{pmatrix} i_1 & i_2 & i_3 & \dots & i_{k-1} & i_k \\ i_2 & i_3 & i_4 & \dots & i_k & i_1 \end{pmatrix}$$

は巡回置換とよばれ $(i_1\, i_2 \cdots i_k)$ と書かれる．例えば S_4 のとき

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

のようになる．

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

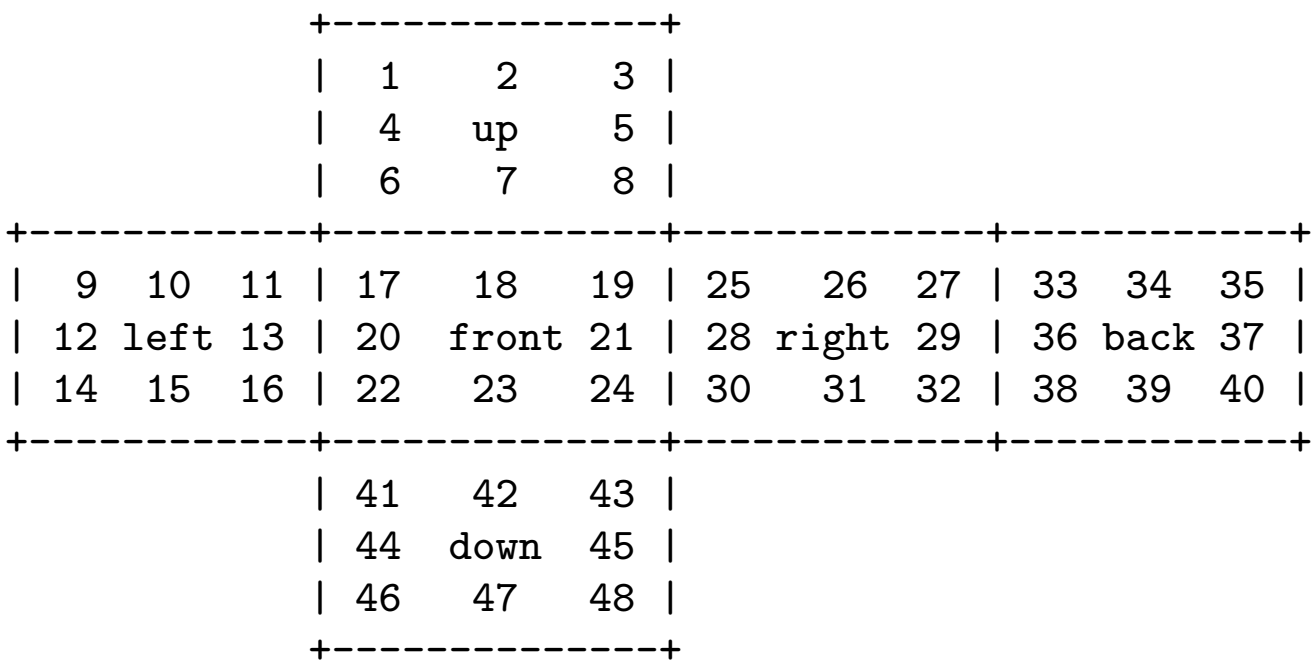
この例は次のように一般化される：

練習問題

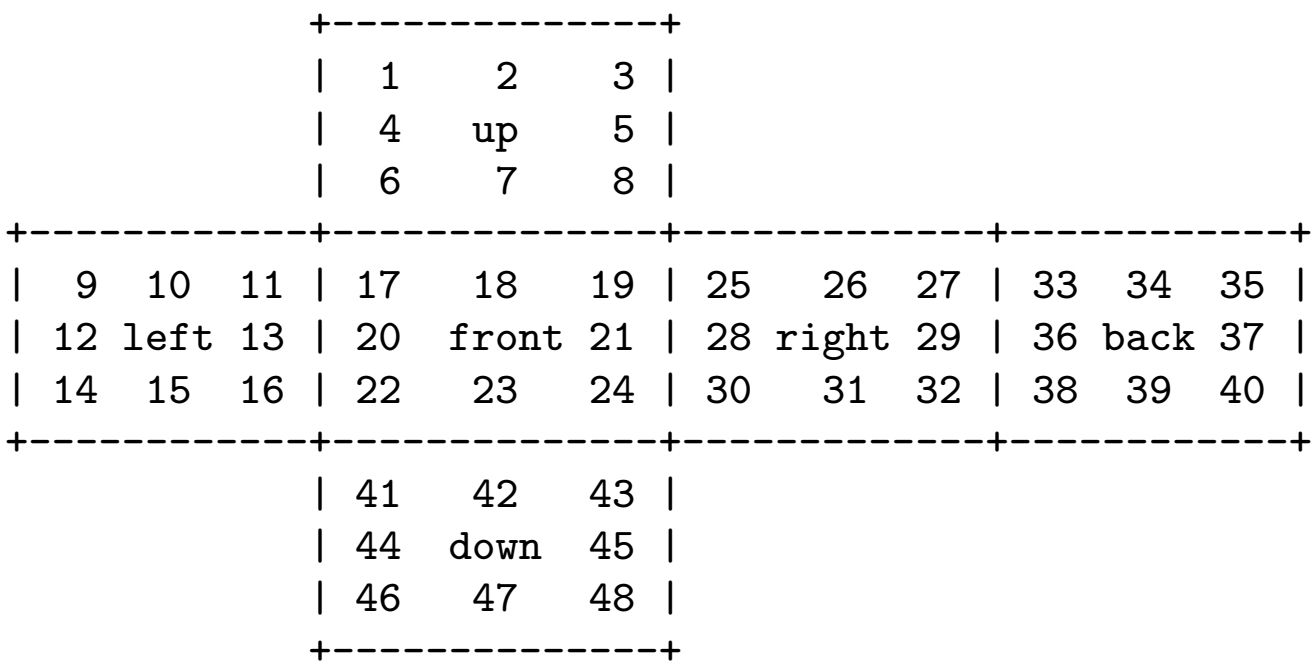
全ての置換群の元は巡回置換の積で書ける事を示せ．

10. 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と考えると，$54 - 6 = 48$ 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．



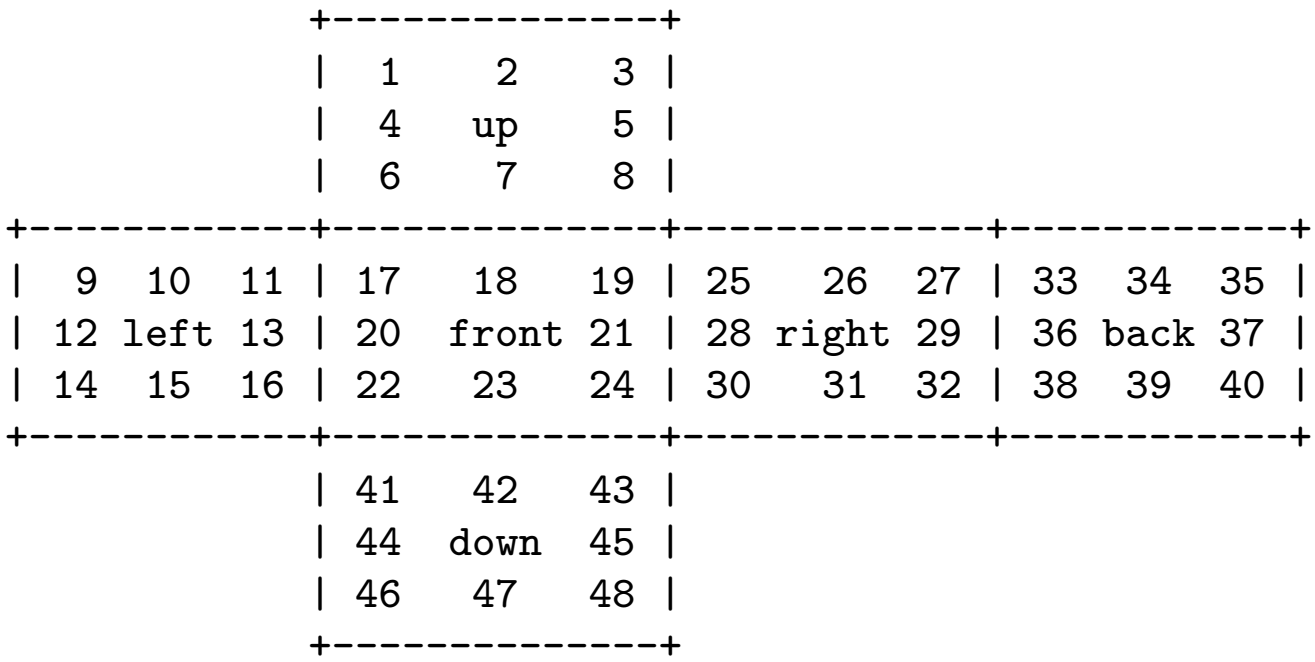
10. ルービックキューブの群



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，置換群の元を用いて表すことができる．例えば前面 front で（時計回りに）$+90^\circ$ 回転を巡回置換の積で表すと

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

10. ルービックキューブの群



同様に背面 (b)，左面 (l)，$\cdots$ での $+90^\circ$ 回転を巡回置換の積で表すと

```
f:(17,19,24,22)(18,21,23,20)( 6,25,43,16)( 7,28,42,13)( 8,30,41,11)
b:(33,35,40,38)(34,37,39,36)( 3, 9,46,32)( 2,12,47,29)( 1,14,48,27)
l:( 9,11,16,14)(10,13,15,12)( 1,17,41,40)( 4,20,44,37)( 6,22,46,35)
r:(25,27,32,30)(26,29,31,28)( 3,38,43,19)( 5,36,45,21)( 8,33,48,24)
u:( 1, 3, 8, 6)( 2, 5, 7, 4)( 9,33,25,17)(10,34,26,18)(11,35,27,19)
d:(41,43,48,46)(42,45,47,44)(14,22,30,38)(15,23,31,39)(16,24,32,40)
```

10. ルービックキューブの群

これら 6 つの元で生成される S_{48} の部分群でルービックキューブにあらわれる全ての組み合わせを表現することができる.

群論を扱うプログラム（GAP という群論のプログラムを Sage という数学の統合環境で使った）を使えば色々な計算ができる.

```
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
```

上の計算からルービックキューブの組み合わせの数は

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

であることがわかる.（ちなみに S_{48} の位数は $48! =$ 12413915592536072670862289047373375038521486354677760000000000）

11. 語距離 (word length)

群 G の部分集合 S に対し，S で生成される部分群 $\langle S \rangle$ を

$$\langle S \rangle = \{ s_1^{\varepsilon_1} s_2^{\varepsilon_2} \cdots s_n^{\varepsilon_n} \mid s_1, \ldots, s_n \in S, \quad \varepsilon_1, \ldots, \varepsilon_n = \pm 1 \}$$

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

で定義した．$G = \langle S \rangle$ のとき S を G の生成系という．

群 G の生成系 S に対し，関数 $\ell_S : G \to \mathbb{Z}$ を

$$\ell_S(g) := \min\{ n \mid g = s_1^{\pm 1} s_2^{\pm 1} \cdots s_n^{\pm 1} \quad (s_1, \ldots, s_n \in S) \}$$

つまり $\ell_S(g)$ は g を S の元と S の逆元の積で表すときの最小の個数．

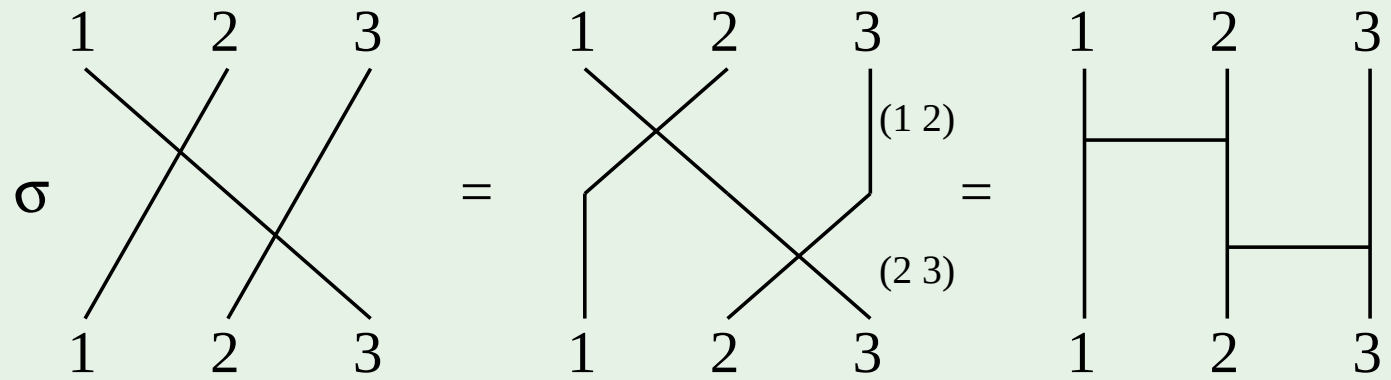
整数全体のなす群 $\mathbb{Z}$ で生成系 $S = \{1\}$ を考えると

$$n = \begin{cases} 1 + \cdots + 1 \quad (n \text{ 個の } 1 \text{ の和}) & (n \geq 0) \\ -1 - 1 \cdots - 1 \quad (n \text{ 個の } -1 \text{ の和}) & (n < 0) \end{cases}$$

だから $\ell_S(n) = |n|$.

11. 語距離 (word length)

あみだくじで，ある組み合わせを実現したい．必要な最小の横線の数は？



$\sigma = (2\,3)(1\,2)$　2 本の横線で実現できる

あみだくじで出来得る組み合わせは，置換群の元 $\sigma \in S_n$ で表される．

σ を表すのに必要な最小の横線の数は，σ を表すのに必要な互換

$$(1\ 2),\ (2\ 3),\ \cdots,\ (n-1\ n)$$

の最小個数（各互換は何度使ってもよい）．つまり
$S = \{(1\ 2),\ (2\ 3),\ \cdots,\ (n-1\ n)\}$ とすれば $\ell_S(\sigma)$ が最小の横線の本数．

11. 語距離 (word length)

ルービックキューブが何回の操作で，解けるか？という問題を考える．

生成系を $S = \{f, b, l, r, u, d\}$ ，ルービックキューブの群を $G = \langle S \rangle$ とおく．ルービックキューブの組み合わせは G の元 $g \in G$ で表される．g に到達するのに必要な最小の 90° 回転は $\ell_S(g)$ 回となる．
（$\ell_S(g)$ の最大値が 26 とわかったのは 2014 年のことらしい．）

生成元を増やして $S' = \{f, ff, b, bb, l, ll, r, rr, u, uu, d, dd\}$ とすれば $\ell_{S'}(g)$ は 180° 回転を（2 回ではなく）1 回の操作と考えて g に到達するのに必要な最小の操作の回数となる．
（$\ell_{S'}(g)$ の最大値が 20 とわかったのは 2010 年のことらしい．）

11. 語距離 (word length)

さらに $d_S : G \times G \to \mathbb{Z}$ を $d_S(a, b) := \ell_S(a^{-1}b)$ で定義する.

$a^{-1}b = g$ のとき $b = ag$ だから

$$b \text{ は } a \text{ から } \ell_S(g) = d_S(a, b) \text{ だけ離れている}$$

と考えられる.

$d_S : G \times G \to \mathbb{Z}$ は '距離' になっている :

正値性 $d(a, b) \geq 0$ で等号は $a = b$ のときのみ成り立つ.
対称性 $d(a, b) = d(b, a)$
三角不等式 $d(a, b) + d(b, c) \geq d(a, c)$

次回の予定

これまでは有限群を主に扱ってきたが，最終回では空間の回転を表す群を紹介する．