群論入門

大学院副コース　情報の取得と解析

蒲谷　祐一

第２回（11 月 9 日）

前回

前回の内容：集合論の復習，群の定義，部分群の定義，置換群の紹介

群とは集合に掛け算（乗法）が定まっているもの.
掛け算は次の性質（公理）を満たすとする.

(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）

(G2) と (G3) では e や a^{-1} が「存在」すればいいが，これらの公理から「唯一つ」に決まってしまう.

復習（例：S_3）

置換群 $S_3 = \{\{1,2,3\}$ から $\{1,2,3\}$ への全単射全体 $\}$　で練習

有限集合 $\{1,2,3\}$ からそれ自身への全単射 σ を

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

で表すことにする．S_3 は $3! = 3 \cdot 2 \cdot 1 = 6$ 個の元からなる．

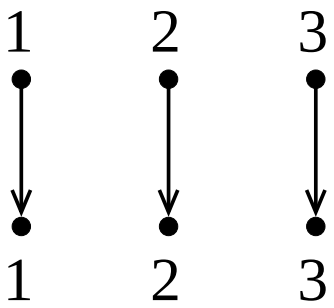
$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

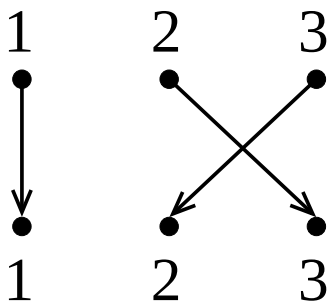
図示すると次のようになる：

復習（例：S_3）

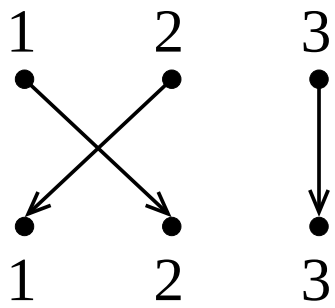
$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$



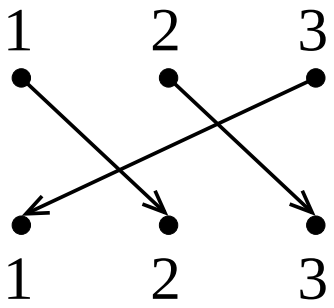
$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$



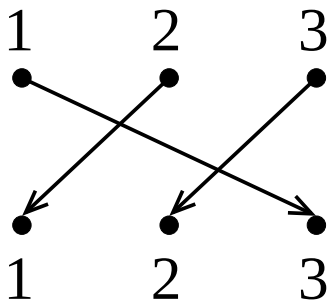
$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$



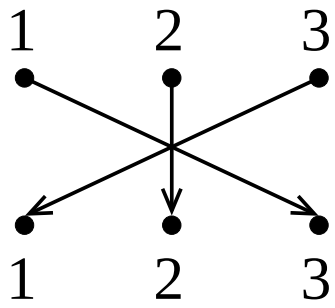
$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$



$$\sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

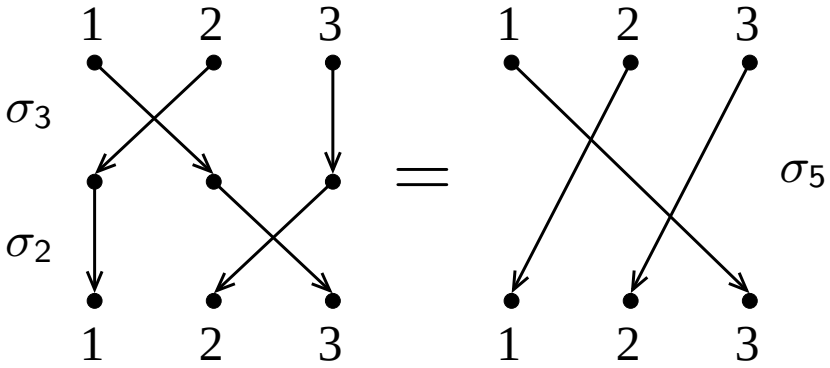


$$\sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

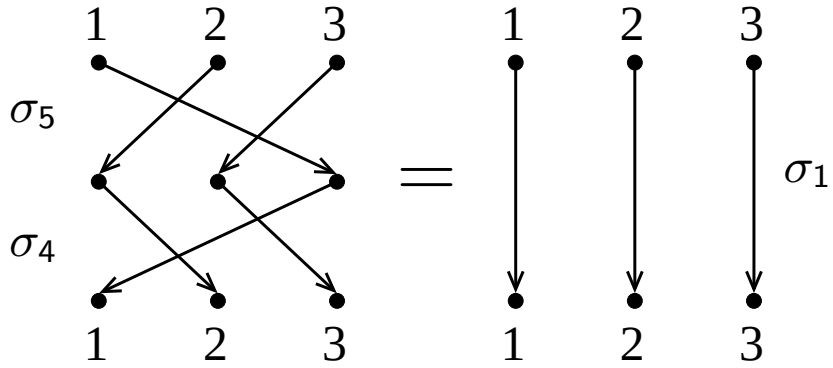


σ_i と σ_j に対して乗法を合成写像 $\sigma_i\sigma_j = \sigma_i \circ \sigma_j$ で定義する．これを図示すると次のようになる：

復習（例：S_3）



$\sigma_2\sigma_3 = \sigma_5$



$\sigma_4\sigma_5 = \sigma_1$

全部求めてみると

	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_5	σ_6	σ_3	σ_4
σ_3	σ_3	σ_4	σ_1	σ_2	σ_6	σ_5
σ_4	σ_4	σ_3	σ_6	σ_5	σ_1	σ_2
σ_5	σ_5	σ_6	σ_2	σ_1	σ_4	σ_3
σ_6	σ_6	σ_5	σ_4	σ_3	σ_2	σ_1

σ_1 が単位元. $\sigma_2\sigma_3 = \sigma_5 \neq \sigma_4 = \sigma_3\sigma_2$ だから S_3 は非可換群.

復習

S_n $(n \geq 4)$ も同様に図示して理解できる.

結合法則，恒等写像が単位元であること，逆写像が逆元になることもわかりやすい.

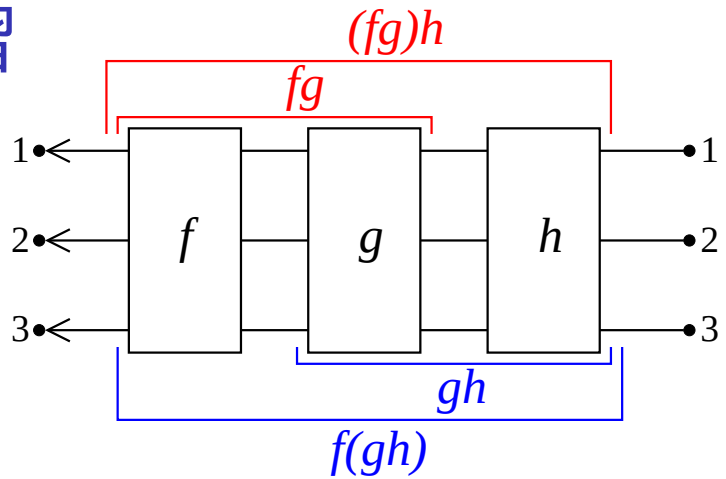
先週の補足

S_n の結合法則，恒等写像が単位元であること，逆写像が逆元になることは次から従う（全て簡単に示せる）:

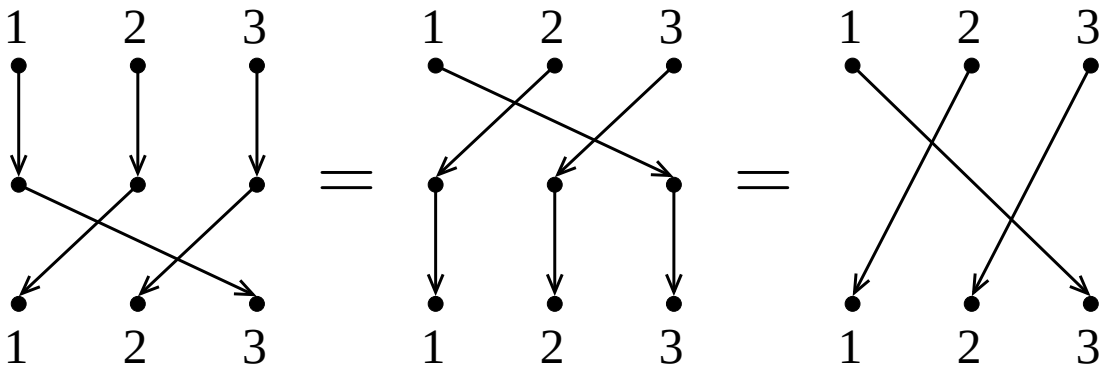
- 写像 $f, g, h : X \to X$ に対して
$$(f \circ g) \circ h = f \circ (g \circ h)$$
- 恒等写像 $\mathrm{id}_X : X \to X$ （$\forall x \in X,\ \mathrm{id}_X(x) = x$）に対して
$$f \circ \mathrm{id}_X = \mathrm{id}_X \circ f = f$$
- $f : X \to X$ が全単射であるとき，f^{-1} を f の逆写像とすると
$$f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_X$$

それぞれ S_3 の場合に図示すると次のようになる：

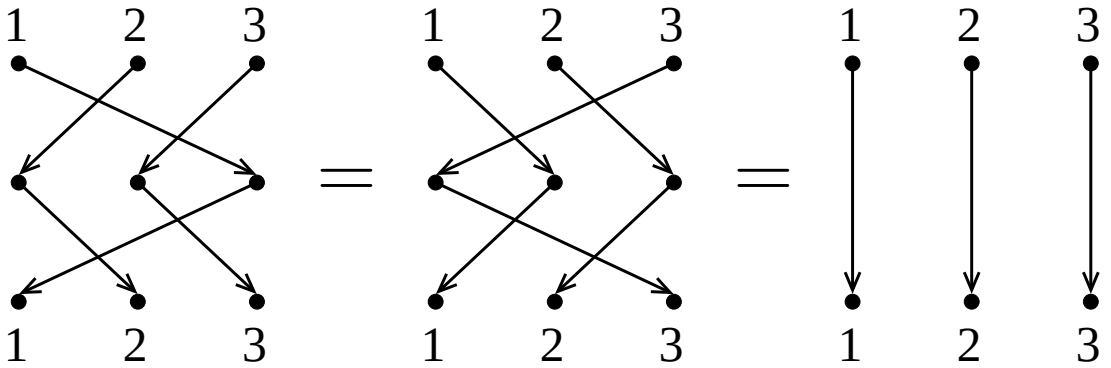
復習



結合法則



恒等写像が単位元



逆写像が逆元

今日の当面の目標

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.

今日は同型などの用語の説明をして，上の定理の証明をする.

4. 準同型と同型

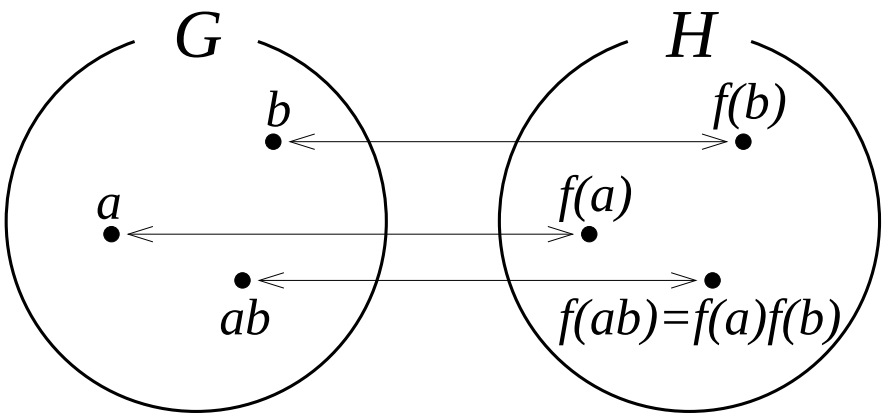
定義

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．

同型写像の逆写像は同型写像であることが示せる．f が同型である時，$f(ab) = f(a)f(b)$ は f を通して G と H の掛け算の仕方が同じであることを意味する．



説明

同型 $f : G \to H$ で G と H を同一視した時，a と b の積 ab は，$f(a)$ と $f(b)$ の積 $f(a)f(b)$ になっているべきである．

4. 準同型と同型

定義 (再掲)

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．

定義

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．

4. 準同型と同型

定理

$f : G \to H$ を準同型とする.

(1) e_G を G の単位元，e_H を H の単位元とすると $f(e_G) = e_H$.

(2) $g \in G$ に対して $f(g^{-1}) = f(g)^{-1}$.

Proof.

(1) $f(g) = f(g\,e_G) = f(g)f(e_G)$. 両辺に左から $f(g)^{-1}$ をかけて

$$e_H = f(g)^{-1}f(g) = f(g)^{-1}f(g)f(e_G) = f(e_G).$$

(2) (1) より

$$f(g)f(g^{-1}) = f(g\,g^{-1}) = f(e_G) = e_H,$$
$$f(g^{-1})f(g) = f(g^{-1}\,g) = f(e_G) = e_H.$$

よって $f(g^{-1})$ は $f(g)$ の逆元. つまり $f(g^{-1}) = f(g)^{-1}$. □

4. 準同型と同型

定理

$f : G \to H$ を準同型とする

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

は H の部分群である.

$\mathrm{Im}(f)$ を f の像 (image) という. $\mathrm{Im}(f)$ は $f(G)$ とも書かれる.

Proof.

群 G に対して, $H \subset G$ が部分群であるとは (1) $a, b \in H \Longrightarrow ab \in H$, (2) $a \in H \Longrightarrow a^{-1} \in H$ を満たすことであった.

(1) $f(a), f(b) \in \mathrm{Im}(f)$ のとき, $f(a)f(b) = f(ab) \in \mathrm{Im}(f)$.

(2) 前の定理より, $f(a)^{-1} = f(a^{-1}) \in \mathrm{Im}(f)$. □

4. 準同型と同型

定理

$f : G \to H$ を準同型とする

$$\mathrm{Ker}(f) = \{g \in G \mid f(g) = e_H\} \quad (e_H \text{ は } H \text{ の単位元})$$

は G の部分群である.

$\mathrm{Ker}(f)$ を f の核 (kernel) という.

Proof.

群 G に対して，$H \subset G$ が部分群であるとは (1) $a, b \in H \Longrightarrow ab \in H$, (2) $a \in H \Longrightarrow a^{-1} \in H$ を満たすことであった.

(1) $a, b \in \mathrm{Ker}(f)$ のとき $f(a) = e_H$, $f(b) = e_H$ より

$$f(ab) = f(a)f(b) = e_H e_H = e_H$$

だから $ab \in \mathrm{Ker}(f)$.

(2) $a \in \mathrm{Ker}(f)$ とする．2 つ前の定理より $f(a^{-1}) = f(a)^{-1} = e_H^{-1} = e_H$ だから $a^{-1} \in \mathrm{Ker}(f)$. □

5. Cayley の定理

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 (Cayley)

有限群 G はある置換群 S_n の部分群に同型である.

Proof.

G の元 a に対して $\varphi(a) : G \to G$ を

$$\varphi(a)(g) := ag \quad (g \in G)$$

で定める. $\varphi(a^{-1})$ は $\varphi(a)$ の逆写像である. 実際

$$\varphi(a^{-1})(\varphi(a)(g)) = \varphi(a^{-1})(ag) = a^{-1}(ag) = (a^{-1}a)g = g$$

より $\varphi(a^{-1}) \circ \varphi(a) = \mathrm{id}_G$. 同様に $\varphi(a) \circ \varphi(a^{-1}) = \mathrm{id}_G$. よって $\varphi(a)$ は全単射である. (次ページへ続く)

5. Cayley の定理

Proof 続き.

G は有限集合なので $G = \{g_1, \ldots, g_n\}$ と表せば，$\varphi(a) : G \to G$ は $\{1, 2, \ldots, n\}$ から $\{1, 2, \ldots, n\}$ 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（後で）．よって φ は G から φ の像 $\mathrm{Im}(\varphi)(\subset S_n)$ への同型を与える．

φ が準同型であること：
$\forall g \in G$ に対して

$$\varphi(ab)(g) = abg = \varphi(a)(bg) = \varphi(a)(\varphi(b)(g)) = (\varphi(a)\varphi(b))(g)$$

より $\varphi(ab) = \varphi(a)\varphi(b)$.

φ が単射であること：
$\varphi(a) = \varphi(b)$ ならば，単位元 e について $\varphi(a)(e) = \varphi(b)(e)$. よって $ae = be$ だから $a = b$. □

6. 巡回群

自然数 n に対して

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

を考える．ただし $x^0 = 1$, $x^1 = x$ とする．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．巡回群は可換群である．

巡回群 C_5 の乗法：

	1	x	x^2	x^3	x^4
1	1	x	x^2	x^3	x^4
x	x	x^2	x^3	x^4	1
x^2	x^2	x^3	x^4	1	x
x^3	x^3	x^4	1	x	x^2
x^4	x^4	1	x	x^2	x^3

例えば

$$x^3x^4 = x^7 = x^5x^2 = 1 \cdot x^2 = x^2$$

6. 巡回群

巡回群 C_n は 1 つの元で生成されるが逆も言える：

練習問題

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.

7. 剰余類

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．

$G = \mathbb{Z}$ 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．

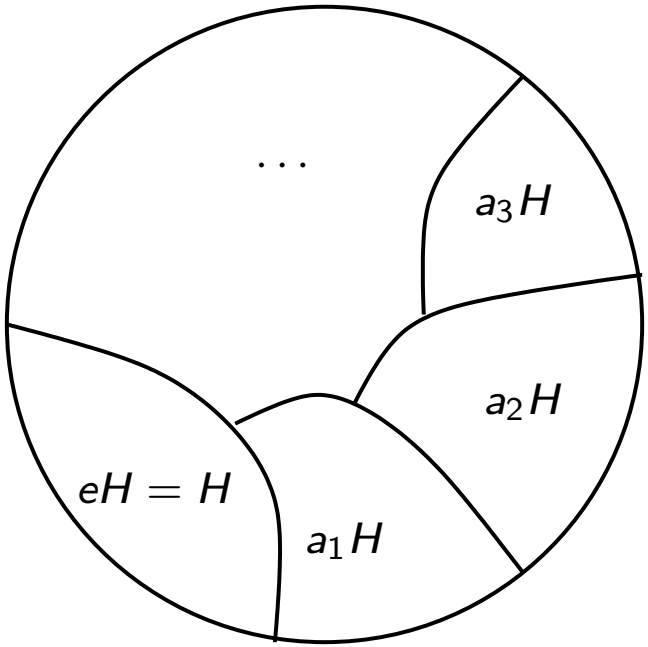
ここで $A \sqcup B$ は $A \cap B = \emptyset$ である場合の和集合 $A \cup B$ で非交和 (disjoint union) とよばれる．

7. 剰余類

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．



7. 剰余類

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 (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.

これを

$$|G| = [G : H]\,|H| \qquad （つまり\ [G : H] = \frac{|G|}{|H|}\ ）$$

と表す. $[G : H]$ を（G における） H の指数 (index) という.

Proof.

G は有限なので剰余類分解も有限個の剰余類からなる：

$$G = a_1 H \sqcup a_2 H \sqcup \cdots \sqcup a_N H$$

各 $a_i H = \{a_i h \mid h \in H\}$ は $|H|$ 個の要素からなるから，$|G| = N \cdot |H|$ である. □

7. 剰余類

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 $G \cong Cp$.）

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，Lagrange の定理からその位数 $|\langle x \rangle|$ は p の約数．つまり $|\langle x \rangle| = 1$ または p.

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

よって $|\langle x \rangle| = p$ だから $\langle x \rangle = G$. 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． □

次回の予定

- 群論の基本定理である「準同型定理」を紹介する.
- ルービックキューブを群で理解する.