

離散数学と計算の理論

第1, 3回目講義の課題解説

大阪大学 大学院工学研究科
電気電子情報通信工学専攻
情報通信工学部門
奥村 伸也

目次

- 事前課題解説
- 課題解説
- 付録1（集合論と対称群（置換群）の補足）
- 付録2（講義アンケートの質問への回答）

(1) 演算で閉じる 1

次の集合が、加法に関して閉じているかを考える。それぞれの演算結果を答えよ。

- (1) {整数の集合} $\ni 8, 4$
- (2) {有理数の集合} = $\{a/b \mid a, b \text{ともに整数. 但し, } b \neq 0.\}$ $\ni 1/3, 2/5$
- (3) {1から5までの数の集合} = $\{1, 2, 3, 4, 5\}$ $\ni 3, 4$
- (4) $\{1, 0\} \ni 1, 1$
- (5) {無理数} = {有理数ではない実数} $\ni \sqrt{3}, -\sqrt{3}+1$
- (6) 上記(1)-(5)のうち加法について閉じている集合を選べ。

[解答]

(1) 12 (2) $\frac{11}{15}$ (3) 7 (4) 2 (5) 1 (6) (1), (2)の集合

(2) 演算で閉じる 2

次の集合が、乗法に関して閉じているかを考える．それぞれの演算結果を答えよ．

- (1) {整数の集合} $\ni 8, 4$
- (2) {有理数の集合} = $\{a/b \mid a, b \text{ともに整数.但し, } b \neq 0.\}$ $\ni 1/3, 2/5$
- (3) {1から5までの数の集合} = $\{1, 2, 3, 4, 5\}$ $\ni 3, 4$
- (4) $\{1, 0\} \ni 1, 1$
- (5) {無理数} = {有理数ではない実数} $\ni \sqrt{3}, -\sqrt{3}+1$
- (6) 上記(1)-(5)のうち乗法について閉じている集合を選べ．

[解答]

(1) 32 (2) $\frac{2}{15}$ (3) 12 (4) 1 (5) $-3 + \sqrt{3}$ (1), (2), (4)の集合

(3) 単位元とは

次の集合の各演算に対する単位元を考える．それぞれの演算結果を答えよ．

(1) ($Z = \{\text{整数の集合}\}$, 加算), $Z \ni 0$, 4の加算

(2) ($Z = \{\text{整数の集合}\}$, 乗算), $Z \ni 1$, 4の乗算

(3) ($Q = \{\text{有理数の集合}\} = \{a/b \mid a, b \text{ともに整数.但し, } b \neq 0.\}$, 乗算), $Q \ni 1/3$, 1の乗算

(4) $\{1, 0\} \ni 1$, 1の乗算

(5) 上記(1)-(4)の各演算に対する単位元を答えよ．

[解答]

(1) 4 (2) 4 (3) $1/3$ (4) 1 (5) (1): 0, (2): 1, (3): 1, (4): 1

(4) 逆元とは

次のモノイドの各演算に対する逆元を考える．それぞれの演算結果を答えよ．

(1) ($Z = \{\text{整数の集合}\}$, 加算), $Z \ni 4$ の逆元.

(2) ($Z = \{\text{整数の集合}\}$, 乗算), $Z \ni 4$ の逆元

(3) ($Q = \{\text{有理数の集合}\} = \{a/b \mid a, b \text{ともに整数.但し, } b \neq 0.\}$, 乗算), $Q \ni 1/3$ の逆元

(4) 上記(1)-(3)の各モノイド S で, S の全て元の逆元が S に含まれるモノイドを答えよ.

[解答]

(1) -4 (2) $\frac{1}{4}$ (3) 3 (4) (1), (3) のモノイド

(5)数の世界以外の演算

次の写像の集合と写像の演算に対して、逆元を考える。それぞれの演算結果を答えよ。ない時はないと答えよ。

(1) $S = \{h; \mathbb{Q} \rightarrow \mathbb{Q} \mid S \ni f: \mathbb{Q} \rightarrow \mathbb{Q} (Q \ni a \rightarrow Q \ni 2a) \text{ の逆元.}$

(2) $S = \{h; \mathbb{Z} \rightarrow \mathbb{Z} \mid S \ni g: \mathbb{Z} \rightarrow \mathbb{Z} (Z \ni a \rightarrow Z \ni a+1) \text{ の逆元.}$

(3) $S = \{\{1,2,3\} \text{ の置換} \}, S \ni \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ の逆元}$

(4) 上記(1)-(3)のSで、Sの全て元の逆元がSに含まれるモノイドを答えよ。

[解答]

$$(1) f^{-1}: \mathbb{Q} \rightarrow \mathbb{Q}; a \mapsto \frac{a}{2}$$

$$(2) g^{-1}: \mathbb{Q} \rightarrow \mathbb{Q}; a \mapsto a - 1$$

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

(4) (3) のモノイド

2回目-(1) 群の位数と元の位数

次の群あるいは群の元の位数を求めよ.

- (1) 置換群 S_3 の位数.
- (2) $S_3 \ni g = \begin{pmatrix} 123 \\ 231 \end{pmatrix}$ の位数.
- (3) $\Phi_6 = \langle \zeta_6 \rangle$ の位数
- (4) $\Phi_6 \ni \zeta_6^2$ の位数

[解答]

- (1) $3! = 6$ (2) 3 (3) 6 (4) 3

2回目-(2) 同値関係

次の集合と関係を考える．それぞれ同値関係になるか答えよ．同値関係にならない場合， (1) , (2),(3)の順で最初に成立しない性質を答えよ．

注：本講義の受講者には大阪大学学生でないも含みます．

(i) $S = \{\text{離散数学と計算の理論の講義の受講者}\}$ ， 関係 $a \sim b$: a と b は同じプロ野球チームのファンである．

(ii) $S = \{\text{離散数学と計算の理論の講義の受講者}\}$ ， 関係 $a \sim b$: a と b は血液型が同じ

(iii) $S = \{\text{離散数学と計算の理論の講義の受講者}\}$ ， 関係 $a \sim b$: a と b は誕生日が同じ

(iv) $Z = \{\text{整数の集合}\}$ ， 関係 $a \sim b$: $a - b$ は3の倍数

(v) $Z = \{\text{整数の集合}\}$ ， 関係 $a \sim b$: $a - b$ は0以上の整数

[解答]

(i) 同値関係 (ii) 同値関係 (iii) 同値関係

(iv) 同値関係

(v) 同値関係でない: (2) 対称律が成り立たない

2回目-(3) 同値類

次の集合と同値関係を考える．それぞれの直和分割の個数と代表元を求めよ．
なお，(1), (3)は直和分割の個数のみ．(2)の代表元は非負整数で最小の整数を求めよ．

- (1) $S = \{\text{日本在住者}\}$, 関係 $a \sim b$: a と b は血液型が同じ (ABO血液型で考える)
- (2) $Z = \{\text{整数の集合}\}$, 関係 $a \sim b$: $a - b$ は3の倍数
- (3) 置換群 S_3 , 関係 $a \sim b$: a と b は位数が同じ

[解答]

(1) 4 (2) 3, 代表元: 0, 1, 2 (3) 3

2回目 (4) \mathbb{Z} 上の加法の同値類

$\text{Mod } 5$ の加算を求めてみよう. 整数を5で割った余りは $[0, \dots, 4]$ なので, 加算を5個の非負整数で表します. 以下の表の穴を埋めましょう.

+	0	1	2	3	4
0					
1					
2				(1)	
3					
4		(2)			

整数

-1 -2 -3 -4
0 1 2 3 4
5 6 7 ...

無限個の元

整数

余り 0	余り 1	余り 2	余り 3	余り 4
0	1	2	3	4
...

5個の元

[解答]

(1)0 (2) 0

復習と補足 (群の生成元)

G を群, $S \subset G$ とする.

$$\langle S \rangle = \left\{ s_1^{k_1} s_2^{k_2} \cdots s_n^{k_n} \mid n \in \mathbb{N}, k_1, \dots, k_n \in \mathbb{Z}, s_1, \dots, s_n \in S \right\}$$

は G の部分群になる.

$\langle S \rangle$ を S で生成される G の部分群という.

S の元を $\langle S \rangle$ の生成元という.

$\langle S \rangle$ は S を含む最小の部分群.

(G の部分群 H について, $S \subset H \Rightarrow \langle S \rangle \subset H$)

$S = \{g_1, \dots, g_n\} \Rightarrow \langle S \rangle = \langle g_1, \dots, g_n \rangle$ と書く.

$|S| < \infty \Rightarrow \langle S \rangle$ は有限生成であるという.

$S' \subset G, |S'| < |S|$ でも $\langle S \rangle = \langle S' \rangle$ となることはある.

例

1. 加法群 \mathbb{Z} について考える.

$$S = \{2, 4, 8\} \Rightarrow \langle S \rangle = \langle 2, 4, 8 \rangle$$

$$= \{2x + 4y + 8z \mid x, y, z \in \mathbb{Z}\} = 2\mathbb{Z} + 4\mathbb{Z} + 8\mathbb{Z}.$$

$$\langle 2 \rangle \subset \langle 2, 4, 8 \rangle \text{ かつ } 2, 4, 8 \in 2\mathbb{Z} \text{ より}$$

$$\langle 2, 4, 8 \rangle \subset \langle 2 \rangle \Rightarrow \langle 2 \rangle = \langle 2, 4, 8 \rangle. \quad \langle 1 \rangle = \mathbb{Z}.$$

$$3 \cdot 7 - 5 \cdot 4 = 1 \Rightarrow \langle 3, 5 \rangle = \langle 1 \rangle = \mathbb{Z}.$$

2. ζ_8 : 1 の原始 8 乗根, $G = \langle \zeta_8 \rangle$ を考える.

$$\zeta_8^{-5} = \zeta_8^8 \cdot \zeta_8^{-5} = \zeta_8^{8-5} = \zeta_8^3. \quad \zeta_8^{12} = \zeta_8^8 \cdot \zeta_8^4 = \zeta_8^4.$$

一般に, ζ_8^k について, $k = 8q + r$ ($q, r \in \mathbb{Z}$, $0 \leq r < 8$)

$$\Rightarrow \zeta_8^k = (\zeta_8^8)^q \cdot \zeta_8^r = \zeta_8^r.$$

$$\text{よって, } G = \{1 (= \zeta_8^0), \zeta_8, \zeta_8^2, \zeta_8^3, \zeta_8^4, \zeta_8^5, \zeta_8^6, \zeta_8^7\}.$$

$$H = \langle \zeta_8^4, \zeta_8^5 \rangle \subset G \text{ について, } \zeta_8^5 \cdot (\zeta_8^4)^{-1} = \zeta_8^{5-4} = \zeta_8 \\ \Rightarrow G = \langle \zeta_8 \rangle = H.$$

$$H_1 = \langle \zeta_8^4, \zeta_8^6 \rangle, H_2 = \langle \zeta_8^2 \rangle \text{ を考える.}$$

$$\zeta_8^6 \cdot (\zeta_8^4)^{-1} = \zeta_8^2 \Rightarrow H_2 \subset H_1.$$

$$\zeta_8^4 = (\zeta_8^2)^2 \in H_2, \zeta_8^6 = (\zeta_8^2)^3 \in H_2 \Rightarrow H_1 \subset H_2.$$

$$\text{よって, } H_1 = H_2.$$

問1.1. 4次の置換 σ とは $\{1, 2, 3, 4\}$ から $\{1, 2, 3, 4\}$ への全単射写像である. $S_4 \ni \sigma, \tau$ に対して, $\sigma\tau$ を自然な写像の合成で定義する. 例えば,

$$S_4 \ni \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

に対して,

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

となる. このとき, 4次の置換からなる集合 S_4 は群となり, 4次対称群 (置換群) と呼ぶ. 特に2つの元入れ替える置換 (i, j) を互換と呼ぶ. S_4 の部分集合で, 偶数個の互換の積からなる集合を A_4 と表す. この時, 以下の問に答えよ.

(1) S_4 の元の個数を求めよ.

[解答例]

S_4 の元は $\{1, 2, 3, 4\}$ の元の並び替え方と $1:1$ に対応しているため、 $|S_4| = 4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$. \square

(2) S_4 から位数 4 の部分群を全て構成してみよう.

[解答例] 後で見るように、位数 4 の群は 1 つまたは 2 つの元で生成されるからそれぞれの場合で生成元の条件を考える.

(i) 1つの元で生成される位数4の部分群

位数が 4 の S_4 の元は以下の通り：

$$\begin{aligned}\sigma_1 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \\ \sigma_4 &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \sigma_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}, \sigma_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}.\end{aligned}$$

補題1 $\sigma \in S_4$ について次の(i)~(iii)は互いに同値である.

(i) σ の位数が 4

(ii) ある $i \in \{1, 2, 3, 4\}$ について $\sigma^k(i) \neq i$ ($1 \leq k \leq 3$), $\sigma^4(i) = i$

(iii) 任意の $i \in \{1, 2, 3, 4\}$ について $\sigma^k(i) \neq i$ ($1 \leq k \leq 3$), $\sigma^4(i) = i$

※位数の定義に従うなら $\sigma \in S_4$ の位数が 4 であることを

確かめるには

$$\sigma^k \neq e_{S_4} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad (1 \leq k \leq 3), \sigma^4 = e_{S_4}$$

が成り立つかを確かめる必要がある. しかし, 実は
どれか1つの $i \in \{1, 2, 3, 4\}$ について確かめればよい.

例 $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ について,

$$\sigma_1(1) = 2, \sigma_1^2(1) = 3, \sigma_1^3(1) = 4, \sigma_1^4(1) = 1$$

より σ_1 の位数は 4.

[証明]

(ii) \Rightarrow (iii) を示す.

(ii) の条件を満たす i とは異なる $j \in \{1,2,3,4\} \setminus \{i\}$ を任意にとる. $\sigma^k(i) \neq i$ ($1 \leq k \leq 3$) より $\sigma^m(i) \neq \sigma^n(i)$ ($1 \leq m \neq n \leq 3$).

※ 例えば, $\sigma^2(i) = \sigma^3(i) \Rightarrow \sigma(i) = e_{S_4}$.

よって, $\{1,2,3,4\} \setminus \{i\} = \{\sigma(i), \sigma^2(i), \sigma^3(i)\} \ni j$.

$j = \sigma(i) \Rightarrow \sigma^k(j) = \sigma^{k+1}(i) \neq j$ ($1 \leq k \leq 3$),

$$\sigma^4(j) = \sigma^5(i) = \sigma(\sigma^4(i)) = \sigma(i) = j.$$

同様に, $j = \sigma^2(i), \sigma^3(i)$ の場合も

$\sigma^k(j) \neq j$ ($1 \leq k \leq 3$), $\sigma^4(j) = j$ が示せる.

[証明]

(iii) \Rightarrow (i) は明らか. 最後に (i) \Rightarrow (ii) を示す.

$\sigma \in S_4$ の位数を 4 とする.

$$k_{\sigma,j} = \min\{i \geq 1 \mid \sigma^i(j) = j\},$$

$$d_\sigma = \max\{k_{\sigma,j} \mid 1 \leq j \leq 4\} \text{ とおく.}$$

$\sigma(j)$ の取り得る値は 4 通りしかないから $1 \leq d_\sigma \leq 4$.

また, $\sigma \neq e_{S_4}$ より $d_\sigma > 1$. $d_\sigma = 4$ を示せばよい.

(i) $d_\sigma = 2$ のとき

任意の $1 \leq j \leq 4$ について $\sigma^2(j) = j$ より σ の位数は 2.

(ii) $d_\sigma = 3$ のとき

ある $1 \leq j_1 \leq 4$ について $k_{\sigma,j_1} = 3$. このとき,

$$\{\sigma(j_1), \sigma^2(j_1), \sigma^3(j_1) = j_1, j'_1\} = \{1, 2, 3, 4\},$$

$$\sigma^3(\sigma^k(j_1)) = \sigma^{k+3}(j_1) = \sigma^k(\sigma^3(j_1)) = \sigma^k(j_1) \quad (1 \leq k \leq 3)$$

かつ $\sigma^3 \in S_4$ は全単射より $\sigma^3(j'_1) = j'_1$.

よって, σ の位数は 3.

よって, $d_\sigma = 4$. 以上より (i) \Leftrightarrow (ii) \Leftrightarrow (iii) が示せた.

□

次に、 $\langle \sigma_i \rangle = \langle \sigma_j \rangle$ となる $1 \leq i \neq j \leq 6$ を見つける.

補題2

σ_i の位数が 4 $\Rightarrow \sigma_i^3$ の位数も 4 .

言い換えると、 $\langle \sigma_i \rangle = \langle \sigma_i^3 \rangle$.

[証明]

$$\sigma_i^3 \neq e_{S_4}, (\sigma_i^3)^2 = \sigma_i^6 = \sigma_i^4 \sigma_i^2 = \sigma_i^2 \neq e_{S_4},$$

$$(\sigma_i^3)^3 = \sigma_i^9 = (\sigma_i^4)^2 \sigma_i = \sigma_i \neq e_{S_4},$$

$$(\sigma_i^3)^4 = (\sigma_i^4)^3 = e_{S_4} \text{ より } \sigma_i^3 \text{ の位数も 4.}$$

□

$$\sigma_1^3 = \sigma_3, \sigma_2^3 = \sigma_4, \sigma_5^3 = \sigma_6 \text{ より}$$

$$\langle \sigma_1 \rangle = \langle \sigma_3 \rangle, \langle \sigma_2 \rangle = \langle \sigma_4 \rangle, \langle \sigma_5 \rangle = \langle \sigma_6 \rangle.$$

σ_i^2 の位数は 2 より $\langle \sigma_i \rangle$ の元で位数が 4なのは σ_i^3 のみ.

$\Rightarrow \langle \sigma_1 \rangle = \langle \sigma_3 \rangle, \langle \sigma_2 \rangle = \langle \sigma_4 \rangle, \langle \sigma_5 \rangle = \langle \sigma_6 \rangle$ 以外に

$\langle \sigma_i \rangle = \langle \sigma_j \rangle$ となる組は存在しない.

以上より，1つの元で生成される位数4の部分群は以下の通り3つ：

$$\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \right\rangle \left(= \left\langle \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \right\rangle \right),$$

$$\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \right\rangle \left(= \left\langle \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \right\rangle \right),$$

$$\left\langle \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \right\rangle \left(= \left\langle \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \right\rangle \right).$$

(ii) 2つの元で生成される位数4の部分群

まず， $\sigma, \tau \in S_4$ が生成する部分群

$$\langle \sigma, \tau \rangle = \left\{ \sigma_1^{i_1} \sigma_2^{i_2} \cdots \sigma_k^{i_k} \mid \sigma_1, \dots, \sigma_k \in \{\sigma, \tau\}, i_1, \dots, i_k \in \mathbb{Z} \right\}$$

の位数が4になるための条件を考える.

補題3

$\sigma, \tau \in S_4 \setminus \{e_{S_4}\}$ ($\sigma \notin \langle \tau \rangle, \tau \notin \langle \sigma \rangle$) について,
 $\langle \sigma, \tau \rangle$ の位数が4 $\Leftrightarrow \sigma, \tau$ の位数が2であり $\sigma\tau = \tau\sigma$.

[証明]

(\Leftarrow) σ, τ の位数が2 より

$$k = 2k': \text{偶数} \Rightarrow \sigma^k = (\sigma^2)^{k'} = e_{S_4}, \tau^k = (\tau^2)^{k'} = e_{S_4}, \\ (\sigma\tau)^k = \sigma^k \tau^k = e_{S_4}.$$

$$k = 2k' + 1: \text{偶数} \Rightarrow \sigma^k = (\sigma^2)^{k'} \sigma = \sigma, \tau^k = (\tau^2)^{k'} \tau = \tau. \\ (\sigma\tau)^k = \sigma^k \tau^k = \sigma\tau.$$

$$\sigma^{i_1} \tau^{i_2} \sigma^{i_3} \tau^{i_4} \dots \sigma^{i_n} \tau^{i_n} \in \{e_{S_4}, \sigma, \tau, \sigma\tau\}.$$

以上より, $\langle \sigma, \tau \rangle = \{e_{S_4}, \sigma, \tau, \sigma\tau\}$ なので $\langle \sigma, \tau \rangle$ の位数は4.

(\Rightarrow)

$\langle \sigma, \tau \rangle$ の位数が4 とする.

$\sigma \notin \langle \tau \rangle, \tau \notin \langle \sigma \rangle \Rightarrow \sigma\tau, \tau\sigma \neq e_{S_4}, \sigma, \tau$ かつ $\sigma^2, \tau^2 \neq \sigma, \tau, \sigma\tau, \tau^2$.

実際, $\sigma\tau = e_{S_4} \Rightarrow \sigma = \tau^{-1} \in \langle \tau \rangle, \sigma\tau = \sigma \Rightarrow \tau = e_{S_4},$

$\sigma\tau = \tau \Rightarrow \sigma = e_{S_4}$ となる ($\tau\sigma, \sigma^2, \tau^2$ についても同様) .

$e_{S_4}, \sigma, \tau, \sigma^2, \tau^2, \sigma\tau, \tau\sigma \in \langle \sigma, \tau \rangle$ より $\langle \sigma, \tau \rangle$ の位数が4なら

$$\sigma\tau = \tau\sigma, \sigma^2 = \tau^2 = e_{S_4}$$

でなければならない.



補題4

$\sigma, \tau \in S_4 \setminus \{e_{S_4}\}$ ($\sigma \notin \langle \tau \rangle, \tau \notin \langle \sigma \rangle$) について,
 σ, τ の位数が2であり $\sigma\tau = \tau\sigma$ が成り立つとき,
 σ, τ は次の (i) または (ii) のように取れる:

(i) $\sigma = (i, j), \tau = (k, \ell)$ かつ $i, j \notin \{k, \ell\}$

例: $\sigma = (1, 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \tau = (2, 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$

(ii) $\sigma = (i_\sigma, j_\sigma)(k_\sigma, \ell_\sigma), \tau = (i_\tau, j_\tau)(k_\tau, \ell_\tau)$ かつ

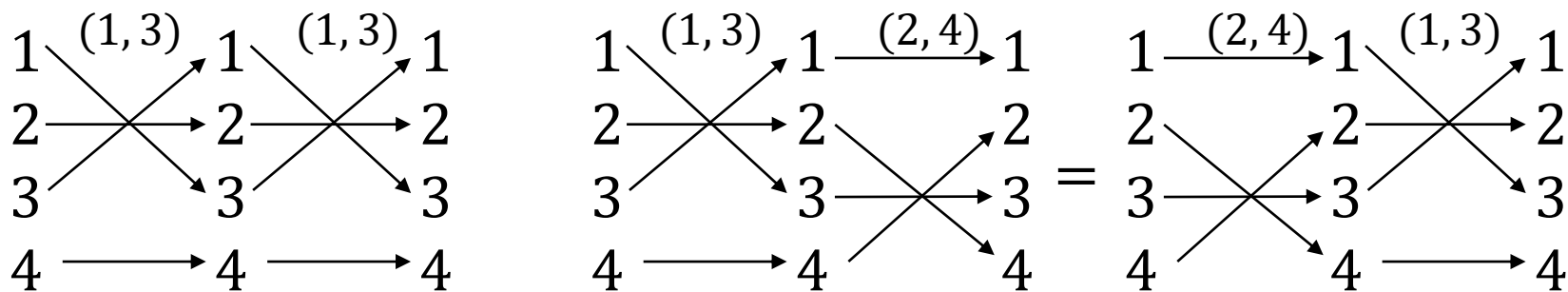
$i_\sigma, j_\sigma \notin \{k_\sigma, \ell_\sigma\}, i_\tau, j_\tau \notin \{k_\tau, \ell_\tau\}, \sigma \neq \tau.$

例: $\sigma = (1, 2)(3, 4), \tau = (1, 4)(2, 3)$

[証明]

まず, (i), (ii)の形の σ, τ は位数が2で $\sigma\tau = \tau\sigma$ であることを示す.

(i): 任意の互換 (i, j) は i, j の二つを入れ替えるのみなので位数は 2 になる.



$\sigma = (i, j), \tau = (k, \ell)$ かつ $i, j \notin \{k, \ell\}$ であれば,

$$\sigma\tau(i) = \sigma(\tau(i)) = \sigma(i) = j, \sigma\tau(j) = \sigma(j) = i,$$

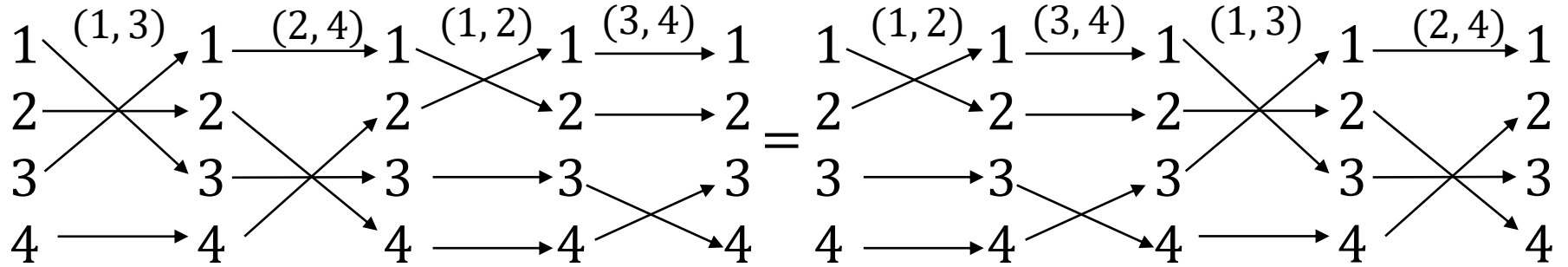
$$\sigma\tau(k) = \sigma(\ell) = \ell, \sigma\tau(\ell) = \sigma(k) = k.$$

$$\tau\sigma(i) = \tau(j) = j, \tau\sigma(j) = \tau(i) = i,$$

$$\tau\sigma(k) = \tau(k) = \ell, \tau\sigma(\ell) = \tau(\ell) = k. \Rightarrow \sigma\tau = \tau\sigma.$$

(ii): (i) より $\sigma = (i_\sigma, j_\sigma)(k_\sigma, \ell_\sigma) = (k_\sigma, \ell_\sigma)(i_\sigma, j_\sigma)$
 $\Rightarrow \sigma^2 = (i_\sigma, j_\sigma)^2(k_\sigma, \ell_\sigma)^2 = e_{S_4}$.

同様に $\tau^2 = (i_\tau, j_\tau)^2(k_\tau, \ell_\tau)^2 = e_{S_4}$ より σ, τ の位数は 2.



一般性を失うことなく, $i_\sigma = i_\tau = 1, k_\sigma < \ell_\sigma, k_\tau < \ell_\tau$

としてよい. このとき, $j_\sigma = j_\tau \Rightarrow \sigma = \tau$ より $j_\sigma \neq j_\tau$.

$\rightarrow j_\sigma = k_\tau$ または $j_\sigma = \ell_\tau$ かつ $j_\tau = k_\sigma$ または $j_\tau = \ell_\sigma$.

(a) $j_\sigma = k_\tau, j_\tau = k_\sigma$ のとき

$$\sigma\tau(1) = (1, j_\sigma)(k_\sigma, \ell_\sigma)(1, j_\tau)(k_\tau, \ell_\tau)(1) = \sigma(j_\tau) = \ell_\sigma,$$

$$\sigma\tau(j_\sigma) = \sigma(\ell_\tau) = k_\sigma \ (\ell_\tau \neq 1, j_\tau, k_\tau \Rightarrow \ell_\tau \neq j_\sigma, k_\sigma \Rightarrow \ell_\tau = \ell_\sigma),$$

$$\sigma\tau(k_\sigma) = \sigma(1) = j_\sigma, \sigma\tau(\ell_\sigma) = \sigma(j_\sigma) = 1 \text{ より } \sigma\tau = (1, \ell_\sigma)(j_\sigma, k_\sigma).$$

$\tau\sigma(1) = \tau(k_\tau) = \ell_\tau (= \ell_\sigma), \tau\sigma(j_\sigma) = \tau(1) = j_\tau (= k_\sigma),$
 $\tau\sigma(k_\sigma) = \tau(\ell_\tau) = k_\tau (= j_\sigma), \tau\sigma(\ell_\sigma) = \tau(j_\tau) = 1$ より
 $\tau\sigma = (1, \ell_\sigma)(j_\sigma, k_\sigma) = \sigma\tau.$

(b) $j_\sigma = k_\tau, j_\tau = \ell_\sigma$ のとき ($k_\sigma = \ell_\tau$ に注意)

$\sigma\tau(1) = \sigma(\ell_\sigma) = k_\sigma, \sigma\tau(j_\sigma) = \sigma(\ell_\tau) = \sigma(k_\sigma) = \ell_\sigma,$
 $\sigma\tau(k_\sigma) = \sigma(j_\sigma) = 1, \sigma\tau(\ell_\sigma) = \sigma(1) = j_\sigma$ より $\sigma\tau = (1, k_\sigma)(j_\sigma, \ell_\sigma).$

$\tau\sigma(1) = \tau(k_\tau) = \ell_\tau (= k_\sigma), \tau\sigma(j_\sigma) = \tau(1) = j_\tau (= \ell_\sigma),$
 $\tau\sigma(k_\sigma) = \tau(j_\tau) = 1, \tau\sigma(\ell_\sigma) = \tau(\ell_\tau) = k_\tau (= j_\sigma)$ より
 $\tau\sigma = (1, k_\sigma)(j_\sigma, \ell_\sigma) = \sigma\tau.$

σ, τ の役割を入れ替えれば

(c) $j_\sigma = \ell_\tau, j_\tau = k_\sigma$ のとき

(d) $j_\sigma = \ell_\tau, j_\tau = \ell_\sigma$ のとき

も $\sigma\tau = \tau\sigma$ が分かる.

次に,

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

の位数が2 になる条件を考える. σ の位数が 2 なら

$\sigma(i) = i$ または $\sigma(i) \neq i, \sigma(\sigma(i)) = i$ のいずれかが各 $i \in \{1, 2, 3, 4\}$ について成り立つから次の (i), (ii) のいずれかの場合に限る.

(i) 互換 $\sigma = (i, j)$ のように 1, 2, 3, 4 のうち, 1 つの組 $[i, j]$ ($i \neq j$) のみを入れ替える.

(ii) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ のように 1, 2, 3, 4 のうち, 2 つの組 $[i, j]$, $[k, \ell]$ ($i \neq j, k \neq \ell, \{i, j\} \cap \{k, \ell\} = \emptyset$) を入れ替える.

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ の場合 $[1, 3], [2, 4]$ の組を入れ替えており,

$\sigma = (1, 3)(2, 4) = (2, 4)(1, 3).$

□

以上より, 2つの元で生成される位数4の部分群は

$\langle (1, 2), (3, 4) \rangle, \langle (1, 3), (2, 4) \rangle, \langle (1, 4), (2, 3) \rangle, \langle (1, 2)(3, 4), (1, 3)(2, 4) \rangle.$

(iii) 3つの元で生成される位数4の部分群

3つの元 $\sigma_1, \sigma_2, \sigma_3 \in S_4$ ($\sigma_i \notin \langle \sigma_j, \sigma_k \rangle$ ($i \neq j, k$)) で生成される S_4 の部分群 $\langle \sigma_1, \sigma_2, \sigma_3 \rangle$ を考える.

$\sigma_i \notin \langle \sigma_j, \sigma_k \rangle$ ($i \neq j, k$) $\Rightarrow \langle \sigma_1, \sigma_2, \sigma_3 \rangle$ は1つや2つの元で生成できない.

$\langle \sigma_1, \sigma_2, \sigma_3 \rangle$ の位数が4 $\Rightarrow \langle \sigma_1, \sigma_2, \sigma_3 \rangle = \{e_{S_4}, \sigma_1, \sigma_2, \sigma_3\}$.

しかしこのような S_4 の部分群は存在しない.

実際, $\sigma_1\sigma_2 \in \langle \sigma_1, \sigma_2, \sigma_3 \rangle$ だが

(a) $\sigma_1\sigma_2 = e_{S_4} \Rightarrow \sigma_1 = \sigma_2^{-1} \in \langle \sigma_2 \rangle$ より矛盾.

(b) $\sigma_1\sigma_2 = \sigma_1 \Rightarrow \sigma_2 = e_{S_4}$ より矛盾.

(c) $\sigma_1\sigma_2 = \sigma_2 \Rightarrow \sigma_1 = e_{S_4}$ より矛盾.

(d) $\sigma_1\sigma_2 = \sigma_3 \Rightarrow \sigma_1 = \sigma_3\sigma_2^{-1} \in \langle \sigma_2, \sigma_3 \rangle$ より矛盾.

つまり, 3つの元でないと生成できない S_4 の位数4の部分群は存在しない. よって, 先に挙げた7つの部分群が S_4 の位数4のすべての部分群となる.

(3) S_4 の部分集合で $\{1,2,3\}$ の置換の集合 H を考える.

つまり, $S_4 \supset H = \left\{ f \mid \begin{pmatrix} 1 & 2 & 3 & 4 \\ f(1) & f(2) & f(3) & 4 \end{pmatrix} \right\}$ は S_4 の部分群である.

[解答例]

任意の $\sigma, \tau \in H$ に対して,

$$\tau(4) = 4 \Rightarrow \tau^{-1}(4) = 4$$

より

$$\begin{aligned} \sigma\tau^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(1) & \sigma(2) & \sigma(3) & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ \tau^{-1}(1) & \tau^{-1}(2) & \tau^{-1}(3) & 4 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma\tau^{-1}(1) & \sigma\tau^{-1}(2) & \sigma\tau^{-1}(3) & 4 \end{pmatrix} \in H \quad (\sigma\tau^{-1} \in S_4). \end{aligned}$$

よって, H は S_4 の部分群である.

//

(4) S_4 の元の最大位数を求めて、その位数を持つ元を1つ求めよ.

[解答例]

まず、 S_4 の元の位数は最大でも 4 であることを示す.

(2)の解答から位数 4 の元は存在する.

任意の $\sigma \in S_4$ に対して

$$k_{\sigma,j} = \min\{i \geq 1 \mid \sigma^i(j) = j\},$$

$$d_\sigma = \max\{k_{\sigma,j} \mid 1 \leq j \leq 4\} \text{ とおく.}$$

補題1 から d_σ と σ の位数は等しく、 $1 \leq d_\sigma \leq 4$ より

S_4 の元の位数は最大でも 4.

S_4 の位数 4 の元の例として

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

が挙げられる.

問1.2. $\zeta_6 : 1$ の原始6乗根とし, $G = \langle \zeta_6 \rangle$ とする.

G の全ての部分群は1つの生成元で表されることを以下のステップで証明しましょう.

(1) G の元を全て求めよ. (集合として元を記載する.)

[解答例]

$$G = \{1(=\zeta_6^0), \zeta_6, \zeta_6^2, \zeta_6^3, \zeta_6^4, \zeta_6^5\}.$$

□

(2) 異なる部分群 $H = \langle \zeta_6^i \rangle$ のみを列挙せよ.

[解答例]

$$H_0 = \langle \zeta_6^0 \rangle = \langle 1 \rangle = \{1\}$$

$$H_1 = \langle \zeta_6 \rangle (= \langle \zeta_6^5 \rangle = H_5) = G$$

$$H_2 = \langle \zeta_6^2 \rangle (= \langle \zeta_6^4 \rangle = H_4) = \{1, \zeta_6^2, \zeta_6^4\}$$

$$H_3 = \langle \zeta_6^3 \rangle = \{1, \zeta_6^3\}$$

□

(3) $G \ni \zeta_6^i, \zeta_6^j$ で生成される部分群 $H_{i,j} = \langle \zeta_6^i, \zeta_6^j \rangle$ を考える. このとき, $\langle \zeta_6^i, \zeta_6^j \rangle = \langle \zeta_6^k \rangle$ となる k を求めよ.
(任意の部分群が一つの元で生成できることを証明する)

[解答例]

$0 \leq i, j \leq 5$ について

$$\langle \zeta_6^i, \zeta_6^j \rangle = \left\{ (\zeta_6^i)^{k_1} \cdot (\zeta_6^j)^{k_2} \mid k_1, k_2 \in \mathbb{Z} \right\} = \langle \zeta_6^k \rangle$$

となる k を求める.

$$\cdot i = 0 \Rightarrow k = j, j = 0 \Rightarrow k = i$$

$$\cdot i = 1, 5 \text{ または } j = 1, 5 \Rightarrow k = 1$$

(ζ_6^5 も 1 の原始 6 乗根になることに注意)

- $i = kj$ (k は正の整数) $\Rightarrow \zeta_6^i = (\zeta_6^j)^k \in \langle \zeta_6^j \rangle \Rightarrow k = j$
- $j = ki$ (k は正の整数) $\Rightarrow k = i$
- $i = j \Rightarrow k = i$
- $i = 2, j = 2, 4$ または $j = 2, i = 2, 4 \Rightarrow k = 2$
- $i = 2, j = 3$ または $j = 2, i = 3 \Rightarrow k = 1$
- ※ $\zeta_6^3 \cdot (\zeta_6^2)^{-1} = \zeta_6 \Rightarrow k = 1$
- $i = 3, j = 4$ または $j = 3, i = 4 \Rightarrow k = 1$
- ※ $\zeta_6^4 \cdot (\zeta_6^3)^{-1} = \zeta_6 \Rightarrow k = 1$

まとめると，次の表のようになる．

$i \backslash j$	0	1	2	3	4	5
0	0	1	2	3	2	1
1	1	1	1	1	1	1
2	2	1	2	1	2	1
3	3	1	1	3	1	1
4	2	1	2	1	4	1
5	1	1	1	1	1	1

(4) (1)-(3)を用いて「 G の全ての部分群 H を1つの生成元で表せ. また, それら以外に部分群がないこと」を証明しましょう.

[解答例]

(3)より生成元が3つ以上の G の部分群についても, 一つの元で生成できることが分かる. 実際, 生成元が

3つの $H = \langle \zeta_6^h, \zeta_6^i, \zeta_6^j \rangle$ 場合, $\langle \zeta_6^i, \zeta_6^j \rangle = \langle \zeta_6^k \rangle, \langle \zeta_6^h, \zeta_6^k \rangle = \langle \zeta_6^\ell \rangle$ とすると, $H = \langle \zeta_6^h, \zeta_6^k \rangle = \langle \zeta_6^\ell \rangle$.

(2)より, 以下が G の全ての部分群とその生成元:

$$H_0 = \langle \zeta_6^0 \rangle = \langle 1 \rangle = \{1\}, H_1 = \langle \zeta_6 \rangle = G,$$

$$H_2 = \langle \zeta_6^2 \rangle = \{1, \zeta_6^2, \zeta_6^4\}, H_3 = \langle \zeta_6^3 \rangle = \{1, \zeta_6^3\}.$$

□

[補足1]

巡回群の任意の部分群は巡回群.

有限巡回群 $G = \langle g \rangle$ ($|G| = n$) について示す.

事実

整数 a, b に対して, 次式を満たす整数 x, y が存在する.

$$ax + by = \gcd(a, b) \cdots (*).$$

$$d = \gcd(a, b)$$

$$\Rightarrow a\mathbb{Z} + b\mathbb{Z} = \{ax + by \mid x, y \in \mathbb{Z}\} = d\mathbb{Z} = \{dz \mid z \in \mathbb{Z}\}$$

を示す.

$a, b \in d\mathbb{Z}$ より $a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}$.

式(*) から $d \in a\mathbb{Z} + b\mathbb{Z}$ より $d\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$.

よって, $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

以上の準備の下, G の部分群 H が巡回群となることを示す.

(i) $H = \langle g^i, g^j \rangle$ ($0 \leq i, j \leq n-1$) のとき

$i = 0 \Rightarrow H = \langle g^j \rangle, j = 0 \Rightarrow H = \langle g^i \rangle$.

$1 \leq i, j \leq n-1, d = \gcd(i, j)$ とする.

$$\begin{aligned} H &= \left\{ (g^i)^{k_1} \cdot (g^j)^{k_2} \mid k_1, k_2 \in \mathbb{Z} \right\} = \left\{ g^{ik_1+jk_2} \mid k_1, k_2 \in \mathbb{Z} \right\} \\ &= \left\{ g^{dk} \mid k \in \mathbb{Z} \right\} = \langle g^d \rangle. \end{aligned}$$

(ii) 一般の H のとき

$H = \langle g^{a_1}, g^{a_2}, \dots, g^{a_k} \rangle$ と書ける. (i) より $d_1 = \gcd(a_1, a_2)$,

$$d_2 = \gcd(d_1, a_3), \dots, d_{k-1} = \gcd(d_{k-2}, a_k)$$

$$\Rightarrow \langle g^{a_1}, g^{a_2} \rangle = \langle g^{d_1} \rangle, \langle g^{d_1}, g^{a_3} \rangle = \langle g^{d_2} \rangle, \dots,$$

$$\langle g^{d_{k-2}}, g^{a_k} \rangle = \langle g^{d_{k-1}} \rangle$$

$$\Rightarrow \langle g^{a_1}, g^{a_2}, \dots, g^{a_k} \rangle = \langle g^{d_1}, g^{a_3}, \dots, g^{a_k} \rangle$$

$$= \langle g^{d_2}, g^{a_4}, \dots, g^{a_k} \rangle = \dots = \langle g^{d_{k-2}}, g^{a_k} \rangle = \langle g^{d_{k-1}} \rangle.$$

※なお, 上の証明で $d_{k-1} = \gcd(a_1, \dots, a_k)$ が成り立つ.

※ 無限巡回群の部分群も巡回群になる.

(証明は次回)

[補足2]

$G = \langle g \rangle$ を位数 n の有限巡回群.

H が位数 k の G の部分群 $\Rightarrow H = \langle g^{\frac{n}{k}} \rangle$.

特に,

- ・ G の部分群の個数は n の約数の個数だけ存在.
- ・ G の部分群はその位数により一意的に決まる.

※ラグランジュの定理より $k \mid n$ に注意.

事実 (除法の原理)

整数 a, b ($b \neq 0$) に対して, 次を満たす整数 q, r が一意的に存在する:

$$a = qb + r \quad (0 \leq r < |b|).$$

g^h の位数が $k \Rightarrow \langle g^h \rangle = \left\langle g^{\frac{n}{k}} \right\rangle$ を示す.

$$hk = qn + r \quad (\exists q, r \in \mathbb{Z}, \quad 0 \leq r < n)$$

$$\Rightarrow 1 = g^{hk} = g^{qn} \cdot g^r = g^r \quad \text{より} \quad r = 0.$$

$$\text{よって, } h = q \frac{n}{k} \Rightarrow \langle g^h \rangle \subset \left\langle g^{\frac{n}{k}} \right\rangle \Rightarrow \langle g^h \rangle = \left\langle g^{\frac{n}{k}} \right\rangle.$$

$$\left(|\langle g^h \rangle| = \left| \left\langle g^{\frac{n}{k}} \right\rangle \right| \text{ に注意} \right)$$

[補足3]

$G = \langle g \rangle$: 補足2の通り.

$\gcd(k, n) = 1 \Rightarrow G = \langle g^k \rangle$ を示す.

(つまり, g^k の位数も n .)

$\langle g^k \rangle \subset G$ は明らか. $g \in \langle g^k \rangle$ を示せばよい.

$xk + ny = 1$ ($\exists x, y \in \mathbb{Z}$)

$\Rightarrow g = g^{xk+ny} = g^{xk} \cdot g^{ny} = g^{xk} \in \langle g^k \rangle$.

同様の議論で $\gcd(k, n) = k' \Rightarrow \langle g^{k'} \rangle = \langle g^k \rangle$ が分かる.

[補足4]

G : 位数が素数 p の群 $\Rightarrow G$ は巡回群であることを示す.

$e_G \neq \forall g \in G$ (e_G は G の単位元) をとる.

ラグランジュの定理より, g の位数は p の約数.

$g \neq e_G$ より g の位数は $p \Rightarrow G = \langle g \rangle$.

問1.3. 3 次の置換 σ とは $\{1, 2, 3\}$ から $\{1, 2, 3\}$ への全単射写像である. S_3 は問1.1 のように群となる. このとき, 以下の問に答えよ.

(1) S_3 の元の個数を求めよ.

(2) S_3 の位数 6 の元が存在しないことを示せ.

(存在すると矛盾することを示すと良い.)

[解答例]

(1) $|S_3| = 3! = 6.$

(2) S_3 に位数 6 の元が存在すると仮定すると,

(1) より S_3 は位数 6 の巡回群となる.

$S_3 = \langle \sigma \rangle$ とすると, 任意の $\sigma^k, \sigma^h \in S_3$ について
 $\sigma^k \sigma^h = \sigma^{k+h} = \sigma^h \sigma^k$ より S_3 は可換群となる.

ところが, $\tau_1 = (1, 2), \tau_2 = (2, 3) \in S_3$ について

$$\tau_1 \tau_2(1) = \tau_1(\tau_2(1)) = \tau_1(2) = 1,$$

$$\tau_2 \tau_1(1) = \tau_2(\tau_1(1)) = \tau_2(1) = 2$$

より $\tau_1 \tau_2 \neq \tau_2 \tau_1$ なので S_3 は非可換群.

よって, S_3 に位数 6 の元は存在しない.



問2.1. 正の整数 m に対して, $\zeta_m : 1$ の原始 m 乗根とし, $G = \langle \zeta_m \rangle$ とする. このとき, 以下の問いに答えよ.

(1) $m = 2, \dots, 20$ とする. G の全ての部分群の個数が最大となる m を求め, その理由を述べよ.

[解答例]

(1) $m = 12, 18, 20$ が答えであることを示す.

$G = \langle \zeta_m \rangle$ は位数 m の巡回群なので, [補足2]より G の部分群の個数と m の約数の個数は一致する.

※[補足2]を利用しない場合は, 問1.2を参考にして G の部分群の個数を数える.

$m = 2 \sim 20$ では, $m = 12, 18, 20$ のとき m の約数の個数は 6 個となり最大となる.

参考：各 m とその約数, $\langle \zeta_m \rangle$ の部分群を以下にまとめる.

m	m の約数	$\langle \zeta_m \rangle$ の部分群
2	1, 2	$\langle \zeta_2 \rangle, \{1\}$
3	1, 3	$\langle \zeta_3 \rangle, \{1\}$
4	1, 2, 4	$\langle \zeta_4 \rangle, \langle \zeta_4^2 \rangle, \{1\}$
5	1, 5	$\langle \zeta_5 \rangle, \{1\}$
6	1, 2, 3, 6	$\langle \zeta_6 \rangle, \langle \zeta_6^2 \rangle, \langle \zeta_6^3 \rangle, \{1\}$
7	1, 7	$\langle \zeta_7 \rangle, \{1\}$
8	1, 2, 4, 8	$\langle \zeta_8 \rangle, \langle \zeta_8^2 \rangle, \langle \zeta_8^4 \rangle, \{1\}$
9	1, 3, 9	$\langle \zeta_9 \rangle, \langle \zeta_9^3 \rangle, \{1\}$
10	1, 2, 5, 10	$\langle \zeta_{10} \rangle, \langle \zeta_{10}^2 \rangle, \langle \zeta_{10}^5 \rangle, \{1\}$
11	1, 11	$\langle \zeta_{11} \rangle, \{1\}$

m	m の約数	$\langle \zeta_m \rangle$ の部分群
12	1, 2, 3, 4, 6, 12	$\langle \zeta_{12} \rangle, \langle \zeta_{12}^2 \rangle, \langle \zeta_{12}^3 \rangle, \langle \zeta_{12}^4 \rangle, \langle \zeta_{12}^6 \rangle, \{1\}$
13	1, 13	$\langle \zeta_{13} \rangle, \{1\}$
14	1, 2, 7, 14	$\langle \zeta_{14} \rangle, \langle \zeta_{14}^2 \rangle, \langle \zeta_{14}^7 \rangle, \{1\}$
15	1, 3, 5, 15	$\langle \zeta_{15} \rangle, \langle \zeta_{15}^3 \rangle, \langle \zeta_{15}^5 \rangle, \{1\}$
16	1, 2, 4, 8, 16	$\langle \zeta_{16} \rangle, \langle \zeta_{16}^2 \rangle, \langle \zeta_{16}^4 \rangle, \langle \zeta_{16}^8 \rangle, \{1\}$
17	1, 17	$\langle \zeta_{17} \rangle, \{1\}$
18	1, 2, 3, 6, 9, 18	$\langle \zeta_{18} \rangle, \langle \zeta_{18}^2 \rangle, \langle \zeta_{18}^3 \rangle, \langle \zeta_{18}^6 \rangle, \langle \zeta_{18}^9 \rangle, \{1\}$
19	1, 19	$\langle \zeta_{19} \rangle, \{1\}$
20	1, 2, 4, 5, 10, 20	$\langle \zeta_{20} \rangle, \langle \zeta_{20}^2 \rangle, \langle \zeta_{20}^4 \rangle, \langle \zeta_{20}^5 \rangle, \langle \zeta_{20}^{10} \rangle, \{1\}$

(2) m は任意の正整数とする. G の全ての部分群の個数が 3 となる最小の m を求めよ. また, その m が最小となる理由を述べよ. さらに, その G の各部分群の生成元を ζ_m を用いて記述せよ.

[解答例]

m の約数の個数が 3 個となる最小の m は 4 なので $m = 4$ が答え.

(前ページの表も参照.)

$m = 4$ の時の $G = \langle \zeta_m \rangle$ の部分群とその生成元は以下の通り :

$G = \langle \zeta_4 \rangle \Rightarrow$ 生成元: ζ_4

$\langle \zeta_4^2 \rangle \Rightarrow$ 生成元: ζ_4^2

$\langle \zeta_4^4 \rangle = \{1\} \Rightarrow$ 生成元: 1

□

[補足5]

ラグランジュの定理を用いて, [補足1, 2]の結果を示す.

$G = \langle g \rangle$: 位数 n の巡回群.

$H \subset G$: G の任意の部分群, $|H| = m, n = n'm$.

G は可換群より $G \triangleright H$.

g は G を生成するので, gH は G/H を生成.

$|G/H| = n' \Rightarrow g^{n'} \in H$ より $\langle g^{n'} \rangle \subset H$.

$g^{n'}$ の位数は m , つまり $|\langle g^{n'} \rangle| = m$ より $\langle g^{n'} \rangle = H$.

逆に, n の任意の約数 m について,

$\langle g^{\frac{n}{m}} \rangle$ は位数 m の部分群.

ラグランジュの定理の逆は一般には不成立.

(群の位数の任意の約数について, その約数を位数にもつ部分群が存在するとは限らない.)

しかし, 巡回群については成立する.

問2.2. $1 \leq n$ を正整数とし, ζ_n を 1 の原始 n 乗根とする. $\mathbb{Z}/8\mathbb{Z}$ 上の演算は乗算とし,

$$H_8 = U(\mathbb{Z}/8\mathbb{Z}) = \{a \in \mathbb{Z}/8\mathbb{Z} \mid a^{-1} \in \mathbb{Z}/8\mathbb{Z}\}$$

及び $G_2 = \langle \zeta_2 \rangle$, $G = G_2 \times G_2$ を考える. ここで, G は G_2 の直積群と呼ばれ, 直積群の演算はそれぞれの群の演算で

定義する. つまり, $G \ni (x_1, y_1), (x_2, y_2)$ に対して,

$G \ni (x_1 x_2, y_1 y_2) = (x_1, y_1)(x_2, y_2)$ で定義する.

この時, 以下の問に答えよ.

1. H_8 の位数を求めて, 生成元の集合を1組求めよ.

なお, 生成元の集合は最小数の元で生成できる集合をさす.

[解答例]

整数 a で代表される剰余類 $a + 8\mathbb{Z}$ を \bar{a} で表す.

$H_8 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ より H_8 の位数は 4.

$\bar{3}^2 = \bar{9} = \bar{1}, \bar{5}^2 = \bar{1}, \bar{7}^2 = \bar{1} \Rightarrow H_8$ は巡回群でない.

$\bar{3} \cdot \bar{5} = \bar{7} \Rightarrow H_8$ の生成元の集合として $\{\bar{3}, \bar{5}\}$ が挙げられる.

($\{\bar{3}, \bar{7}\}, \{\bar{5}, \bar{7}\}$ も H_8 の生成元)

[補足6]

位数2の元 $\alpha \in H_8$, 別の位数2の元 $\beta \in H_8 \Rightarrow H_8 = \langle \alpha, \beta \rangle$.

実際, $\alpha^i \beta^j = \alpha^k \beta^h$ ($0 \leq i, k \leq 1, 0 \leq j, h \leq 1$)

$\Rightarrow \alpha^{i-k} = \beta^{h-j} \Rightarrow i = k, h = j$ ($\because \alpha \notin \langle \beta \rangle$).

$\Rightarrow \#\{\alpha^i \beta^j \mid 0 \leq i \leq 1, 0 \leq j \leq 1\} = 4 \Rightarrow H_8 = \langle \alpha, \beta \rangle$.

[補足7]

$\gcd(a, 8) = 1 \Leftrightarrow \bar{a} \in H_8$ を示す.

(\Rightarrow)

$\gcd(a, 8) = 1 \Rightarrow ax + 8y = 1 \ (\exists x, y \in \mathbb{Z})$ より

$ax \equiv 1 \pmod{8} \Rightarrow \bar{a}^{-1} = \bar{x} \in H_8.$

(\Leftarrow)

$\bar{a}^{-1} = \bar{x} \in H_8 \Rightarrow \exists x \in \mathbb{Z}, ax \equiv 1 \pmod{8}$

$\Rightarrow \exists y \in \mathbb{Z}, ax + 8y = 1 \Rightarrow \gcd(a, 8) = 1.$

2. H_8 の部分群を全て求めて、その生成元を挙げよ.

また、それが全てであることを示せ.

[解答例] H_8 の全ての部分群とその生成元は次の通り:

H_8 生成元: $\bar{3}, \bar{5}$

$\langle \bar{1} \rangle$ 生成元: $\bar{1}$

$\langle \bar{3} \rangle$ 生成元: $\bar{3}$

$\langle \bar{5} \rangle$ 生成元: $\bar{5}$

$\langle \bar{7} \rangle$ 生成元: $\bar{7}$

上記の部分群が全てであることを示す.

$H_8 = \langle \bar{3}, \bar{7} \rangle = \langle \bar{5}, \bar{7} \rangle = \langle \bar{3}, \bar{5}, \bar{7} \rangle$ かつ H_8 は巡回群でない.

($\bar{3}, \bar{5}, \bar{7}$ の位数は $2 \Rightarrow \langle \bar{3} \rangle, \langle \bar{5} \rangle, \langle \bar{7} \rangle \neq H_8$.)

よって、 H_8 以外の部分群は全て1つの元で生成されるから上記のものですべてである. □

3. G の位数を求めて, 生成元を求めよ.

[解答例]

$|G| = |G_2 \times G_2| = |G_2|^2 = 2^2 = 4$ より G の位数は 4.

$$\begin{aligned} G &= \left\{ \left(\zeta_2^i, \zeta_2^j \right) = (\zeta_2, 1)^i \cdot (1, \zeta_2)^j \mid 0 \leq i, j \leq 1 \right\} \\ &= \{(1, 1), (\zeta_2, 1), (1, \zeta_2), (\zeta_2, \zeta_2)\} \end{aligned}$$

より G の生成元の集合として $\{(\zeta_2, 1), (1, \zeta_2)\}$ が挙げられる.

[補足 8]

H_8 と G はともに位数が 4 の群であり, さらに, ともに 位数 2 の 2 つの元により生成され, 群構造が同じものになっている. のちに群の同型という概念を学ぶが, H_8 と G は群として同型であり, 群として考える限り同一視してよい.



4. G の部分群を全て求めて、その生成元を挙げよ.
また、それが全てであることを示せ.

[解答例]

G の全ての部分群とその生成元は以下の通り:

G 生成元: $(\zeta_2, 1), (1, \zeta_2)$ $\langle(\zeta_2, 1)\rangle$ 生成元: $(\zeta_2, 1)$

$\langle(1, \zeta_2)\rangle$ 生成元: $(1, \zeta_2)$ $\langle(1, 1)\rangle$ 生成元: $(1, 1)$

H_8 の場合と同様に、 G の G 以外の部分群は全て
1 つの元で生成される. よって、上記の部分群が G の
すべての部分群になる. □

問2.3. 3次の置換 σ とは $\{1,2,3\}$ から $\{1,2,3\}$ への全単射写像である. $S_3 \ni \sigma, \tau$ に対して, $\sigma\tau$ を自然な写像の合成で定義する. 順序は τ を行ってから σ を

実施する. 例えば, $S_3 \ni \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$,

$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ に対して, $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ となる.

このとき, 3次の置換からなる集合 S_3 は群となり, 3次対称群(置換群)と呼ぶ. 特に, 2つの元を入れ替える置換 (i, j) を互換と呼ぶ. 例えば, τ は互換となり $\tau = (2, 3)$ で表される.

(1) $H = \langle \sigma \rangle$ とするとき, H の元をすべて列挙し, 元の個数を求めよ.

[解答例]

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \right\} \text{ より } |H| = 3. \quad \square$$

(2) $K = \langle \sigma \rangle$ が S_3 の正規部分群になることを証明せよ.

[証明]

任意の $\kappa \in S_3$ について,

$$\kappa K \kappa^{-1} = \{ \kappa g \kappa^{-1} \mid g \in K \} = K$$

を示す. ($\kappa^{-1} K \kappa = K$ を示してもよい)

まず, $\kappa K \kappa^{-1} \subset K$ を示す. $\kappa \notin K$ について示せば十分.

$$\kappa = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \text{ のとき } \kappa^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \text{ より}$$

$$\kappa\sigma\kappa^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma^2 \in K.$$

$$\kappa = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ のとき } \kappa^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ より}$$

$$\kappa\sigma\kappa^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma^2 \in K.$$

$$\kappa = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ のとき } \kappa^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ より}$$

$$\kappa\sigma\kappa^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma^2 \in K.$$

よって、任意の $\kappa \in S_3$ について $\kappa\sigma\kappa^{-1} \in K$ が成り立つから
 任意の $\kappa\sigma^i\kappa^{-1} \in \kappa K \kappa^{-1}$ について $\kappa\sigma^i\kappa^{-1} = (\kappa\sigma\kappa^{-1})^i \in K$
 より $\kappa K \kappa^{-1} \subset K$. κ は S_3 の任意の元よりこれは
 $\kappa^{-1} K \kappa \subset K$ であることも意味する.

$$K = \kappa^{-1}(\kappa K \kappa^{-1})\kappa \subset \kappa^{-1} K \kappa \subset K \text{ より } \kappa K \kappa^{-1} = K.$$

以上より, K は S_3 の正規部分群であることが示せた. \square

(3) $L = \langle \tau \rangle$ が S_3 の正規部分群にならないことを証明せよ.

[証明]

$L = \{e_{S_3}, \tau\}$ より

$$\sigma\tau\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \notin L.$$

よって, L は S_3 の正規部分群ではない. \square

問2.4. $H = U(\mathbb{Z}/16\mathbb{Z}) = \{a \in \mathbb{Z}/16\mathbb{Z} \mid a^{-1} \in \mathbb{Z}/16\mathbb{Z}\}$ 及び H の部分群 $K = \langle \bar{5} \rangle$ について, 以下の問に答えよ.

(1) H/K の完全代表系を示せ.

[解答例]

$$H = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}, \bar{9}, \bar{11}, \bar{13}, \bar{15}\}, K = \{\bar{1}, \bar{5}, \bar{9}, \bar{13}\}$$

$$\Rightarrow \#H/K = 2 \Rightarrow a \in H \setminus K = \{\bar{5}, \bar{7}, \bar{13}, \bar{15}\} \text{なら}$$

$\{\bar{1}, a\}$ が H/K の完全代表系. 例えば, $\{\bar{1}, \bar{3}\}$.

注意

$\mathbb{Z}/16\mathbb{Z}$ は加法群だが, H は乗法群.

$\rightarrow H \subset \mathbb{Z}/16\mathbb{Z}$ だが H は $\mathbb{Z}/16\mathbb{Z}$ の部分群ではない.

(2) H/K は剰余群になる. このとき, $H/K \ni a, b$ に対して, $H/K \ni a, b$ を完全代表元で求めた乗算表を作成せよ.

[解答例]

完全代表系を $\{\bar{1}, \bar{3}\}$ とした場合の乗算表は以下の通り.

	$\bar{1}K$	$\bar{3}K$
$\bar{1}K$	$\bar{1}K$	$\bar{3}K$
$\bar{3}K$	$\bar{3}K$	$\bar{1}K$

付録1

(集合論と対称群(置換群)の補足)

集合論

整数全体の集合を \mathbb{Z} , 自然数全体の集合を \mathbb{N} とする.
すなわち

$$\mathbb{Z} := \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}, \quad \mathbb{N} := \{1, 2, 3, \dots\}.$$

n が自然数なら $n \in \mathbb{N}$, a が整数なら $a \in \mathbb{Z}$ と表す.

一般に, ある x が集合 A の要素 (元) であることを
 $x \in A$ または $A \ni x$ と表す. 逆に, x が集合 A の要素
でないことを $x \notin A$ または $A \not\ni x$ と表す.

A または $|A|$: A の要素数

事象 A, B について, A が成り立つなら B が成り立つ
ことを $A \Rightarrow B$ と表す. $A \Rightarrow B$ かつ $B \Rightarrow A$ のとき
 $A \Leftrightarrow B$ と表す.

集合 A, B について, $x \in A \Rightarrow x \in B$ のとき,
 A を B の部分集合といい, $A \subset B$ と表し,
そうでないとき, $A \not\subset B$ と表す.

要素が a, b, c, \dots である集合を $\{a, b, c, \dots\}$ と書く.

集合 X の要素で, 特定の条件 P を満たす要素の集合を
$$\{x \in X \mid x \text{ は } P \text{ を満たす}\}$$

と書く. この集合は明らかに X の部分集合.

集合 Ω の部分集合 A, B の和集合を次のように定義する:

$$A \cup B := \{x \in \Omega \mid x \in A \text{ または } x \in B\}.$$

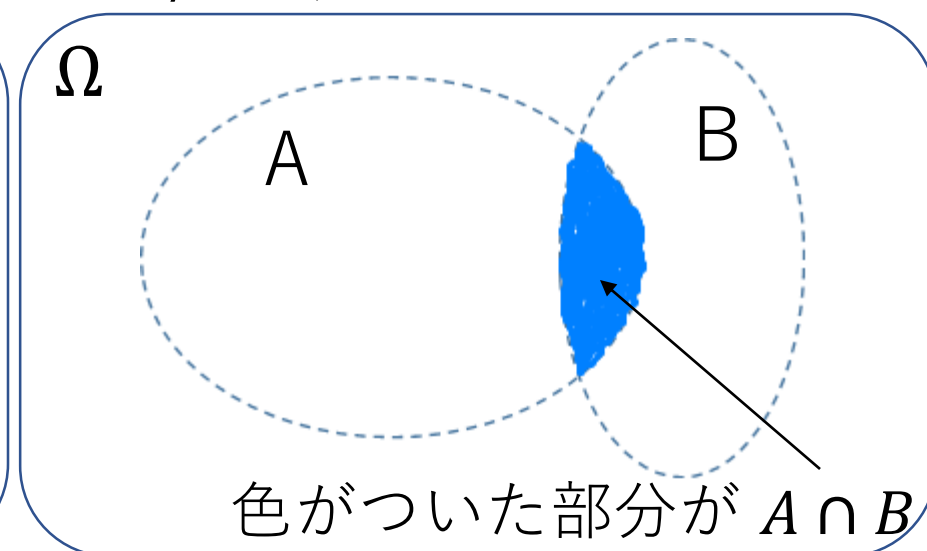
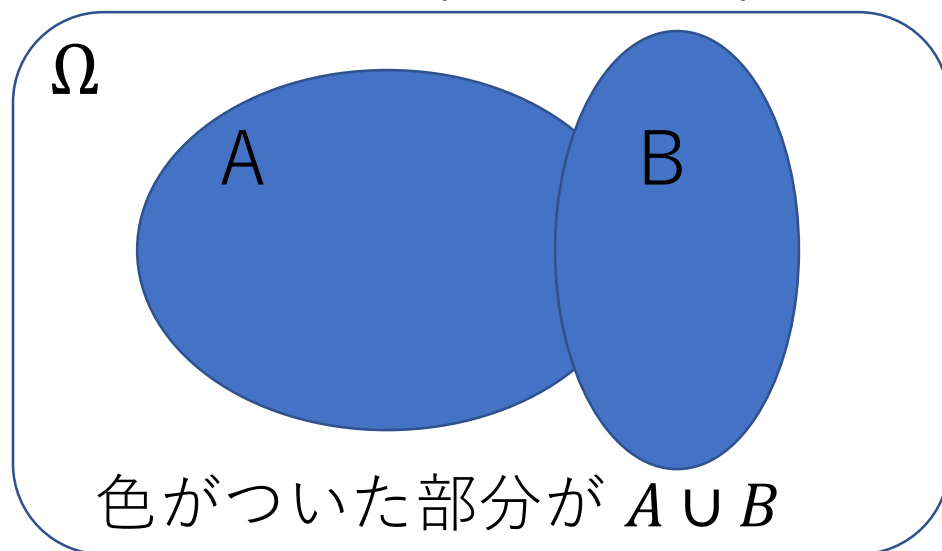
A, B の積集合 (共通部分) を次のように定義する:

$$A \cap B := \{x \in \Omega \mid x \in A \text{ かつ } x \in B\}.$$

定義より, $A \subset A \cup B, B \subset A \cup B, A \cap B \subset A, A \cap B \subset B$.

A から $a \in A$ を取り除いた集合を $A \setminus \{x\}$ または $A - \{x\}$ と書く.

便宜上, 要素を持たない集合を考えるとときがある.
そのような集合を空集合といい \emptyset で表す.



集合 A, B について,

$$A \times B := \{(a, b) | a \in A, b \in B\}$$

を A, B の直積集合という.

$$\#A, \#B < \infty \Rightarrow \#(A \times B) = \#A \#B.$$

3つ以上の集合の直積集合も同様に定義する.

各 $a \in A$ に対してただ1つの $b_a \in B$ を対応させる規則を A から B への写像という.

f が A から B への写像であることを,
$$f : A \rightarrow B$$

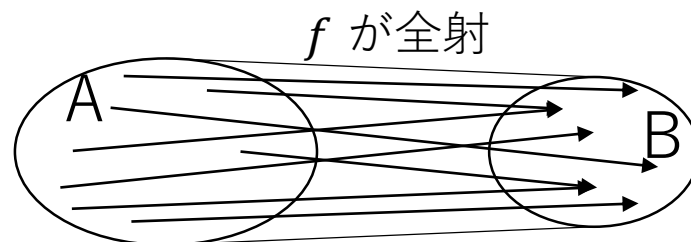
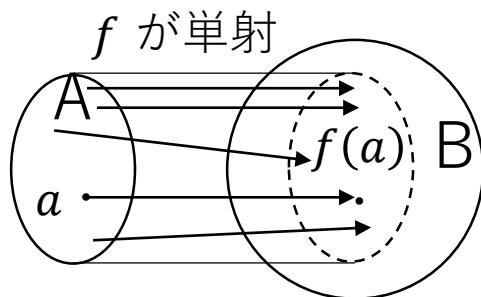
と表す. 要素同士の対応も明示するには $a \mapsto b_a$ と書く.

写像 f について $a \mapsto b_a$ は $f(a) = b_a$ であることを表す.

写像 $f : A \rightarrow B$ が, $a \neq b \Rightarrow f(a) \neq f(b)$ のとき f を単射,

任意の $b \in B$ に対して $f(a) = b$ を満たす $a \in A$ が存在

するなら f を全射という. 全射かつ単射の写像を全単射という.



[写像の合成]

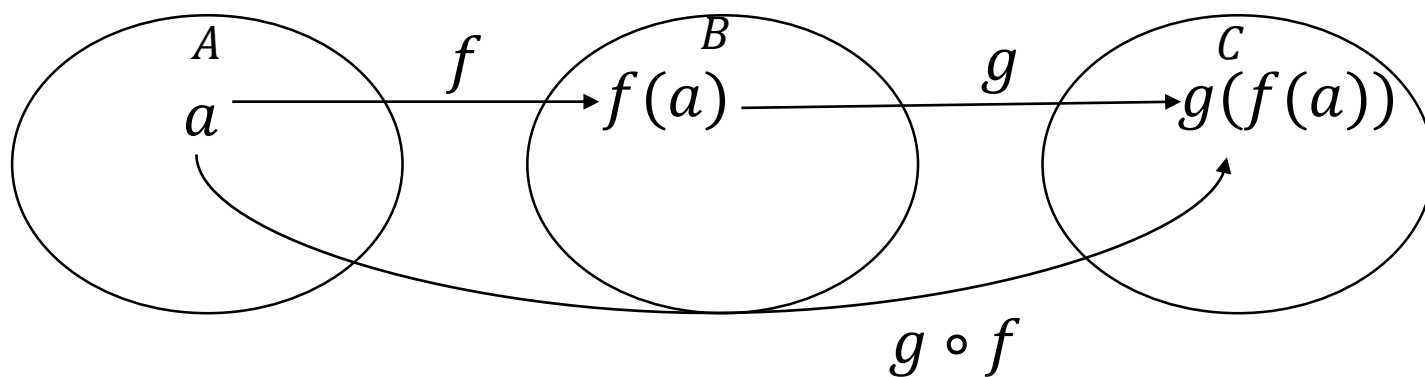
集合 A, B, C と 写像

$$f : A \rightarrow B,$$

$$g : B \rightarrow C$$

に対して, f と g の合成写像を次のように定義する:

$$g \circ f : A \rightarrow C; a \mapsto g(f(a)).$$



命題

集合 A, B, C と 写像

$$\begin{aligned} f &: A \rightarrow B, \\ g &: B \rightarrow C \end{aligned}$$

に対して, 次の(i), (ii), (iii)が成り立つ:

(i) f, g が単射なら $g \circ f$ も単射

(ii) f, g が全射なら $g \circ f$ も全射

(iii) f, g が全単射なら $g \circ f$ も全単射

[証明]

(i)を示す.

$x, y \in A$ が $(g \circ f)(x) = (g \circ f)(y)$ を満たすとき,

$g(f(x)) = g(f(y))$. g は単射であるから $f(x) = f(y)$ が成り立ち, f が単射であるから $x = y$ が成り立つ.

以上より, $g \circ f$ が単射であることが示せた.

(ii) 任意の $c \in C$ に対して, g は全射より $g(b) = c$ を満たす $b \in B$ が存在する. さらに, f が全射より $f(a) = b$ を満たす $a \in A$ が存在するから $g(f(a)) = g(b) = c$. 以上より, $g \circ f$ が全射であることが示せた.

(iii) は (i), (ii) から明らか. □

練習問題 (次のページに解答あり)

次の (i), (ii) を示してください.

(i) $g \circ f$ が単射のとき, f は単射であるが g は単射とは限らない.

(ii) $g \circ f$ が全射のとき, g は全射であるが f は全射とは限らない.

[解答例]

(i) f が単射になることを示す.

$x, y \in A$ が $f(x) = f(y)$ を満たすとき,

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

$g \circ f$ は単射であるから $x = y$. よって, f は単射.

g が単射とは限らないことを凡例を挙げることで示す.

$A = \{1, 2, 3\}, B = \{1, 2, 3, 4, 5, 6\}, C = \{4, 5, 6\}$ とし,

$$f : A \rightarrow B; i \mapsto i$$
$$g : B \rightarrow C; \begin{cases} i \mapsto i + 3 & (1 \leq i \leq 3) \\ i \mapsto i & (4 \leq i \leq 6) \end{cases}$$

と定義する. $(g \circ f)(i) = i + 3$ ($1 \leq i \leq 3$) より $g \circ f$ が単射なのは容易に確かめられる.

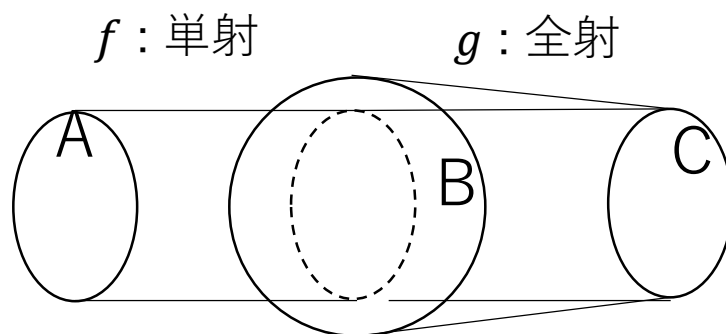
一方, $g(1) = 4 = g(4)$ より g は単射ではない.

[解答例]

(ii) g が全射になることを示す.

任意に $c \in C$ を取る. $g \circ f$ は全射であるから
ある $a \in A$ が存在して $g(f(a)) = c$ が成り立つが,
 $f(a) \in B$ より g は全射となる. f が全射とは限らない
ことは (i) の凡例からわかる. \square

凡例のイメージ



※ $g \circ f$ が全単射なら f は単射で g は全射になるが,
 g, f が全単射になるとは限らない.

注意 集合 A, B について

1. $B \subset A$ かつ $A \subset B \Leftrightarrow A = B$
2. A から B への単射が存在 $\Leftrightarrow |A| \leq |B|$
3. A から B への全射が存在 $\Leftrightarrow |A| \geq |B|$
4. A から B への全単射が存在 $\Leftrightarrow |A| = |B|$

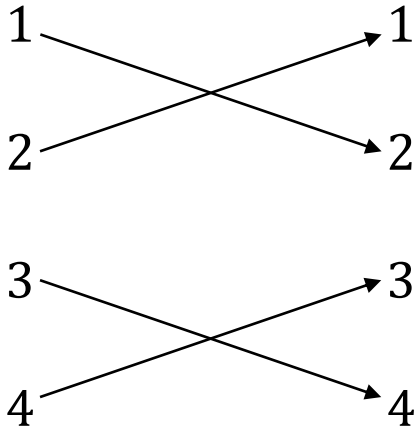
例

$$A = \{1, 4, 5, 9, 12\}, B = \{a_1, a_4, a_5, a_9, a_{12}\}, C = \{4, 12\}$$

- (1) $4 \in A, 6 \notin A, a_4 \notin A, a_4 \in B$
- (2) $C \subset A, |A| = |B|, B \not\subset A$
- (3) 写像 $f : A \rightarrow B$ を $i \mapsto a_i$ ($i \in A$) とする $\rightarrow f$ は全単射.
- (4) $C = \{i \in A \mid i \text{ は偶数}\}, \{a \in \mathbb{Z} \mid a \geq 3\} = \{3, 4, 5, \dots\}$
- (5) $A \cap C = C, A \cap B = \emptyset,$
 $B \cup C = \{a_1, a_4, a_5, a_9, a_{12}, 4, 12\}$

対称群（置換群）の補足

$$S_4 = \{\sigma : \{1,2,3,4\} \rightarrow \{1,2,3,4\} \mid \sigma : \text{全単射}\}$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \leftrightarrow$$


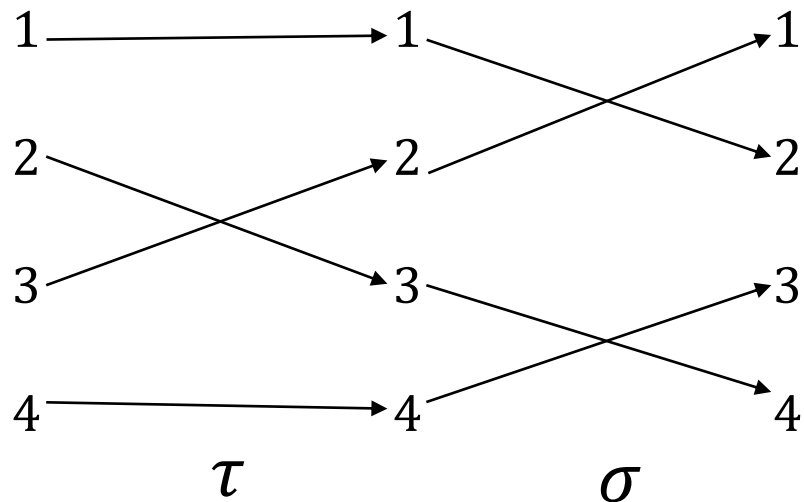
The diagram illustrates the permutation σ as a mapping from the set $\{1, 2, 3, 4\}$ to itself. It consists of two columns of numbers. The left column contains 1, 2, 3, 4 and the right column contains 1, 2, 3, 4. Arrows indicate the mapping: an arrow from 1 to 2, an arrow from 2 to 1, an arrow from 3 to 4, and an arrow from 4 to 3. This represents a permutation that swaps 1 and 2, and swaps 3 and 4.

数式で書くと

$$\sigma(1) = 2, \sigma(2) = 1, \\ \sigma(3) = 4, \sigma(4) = 3.$$

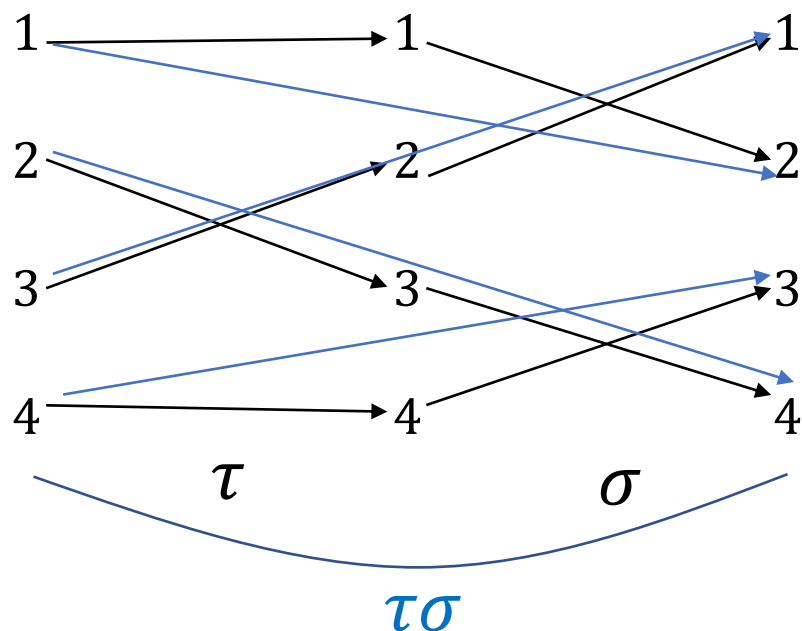
S_4 における演算：写像の合成

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$ の合成写像 $\sigma\tau := \sigma \circ \tau$



S_4 における演算：写像の合成

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$ の合成写像 $\sigma\tau := \sigma \circ \tau$



数式で書くと

$$\sigma\tau(1) = \sigma(\tau(1)) = \sigma(1) = 2,$$

$$\sigma\tau(2) = \sigma(\tau(2)) = \sigma(3) = 4,$$

$$\sigma\tau(3) = \sigma(\tau(3)) = \sigma(2) = 1,$$

$$\sigma\tau(4) = \sigma(\tau(4)) = \sigma(4) = 3,$$

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}.$$

[偶置換と奇置換]

任意の置換 $\sigma \in S_n$ は互換 (i, j) ($i < j$) の積で書ける.
証明は省略する.

例

$$(i) S_3 \ni \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1, 2)(1, 3)(2, 3)(1, 3) = (1, 3)(1, 3).$$

$$(ii) S_3 \ni \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2, 3).$$

$$(iii) S_4 \ni \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1, 2)(3, 4).$$

上の例(i)からわかるように、置換を互換の積での表し方は一意的ではないが、積に現れる互換の数の偶奇は積の表し方によらないことが知られている.

定義

- (i) $\sigma \in S_n$ が偶数個の互換の積で書けるとき,
 σ は偶置換といい, そうでない (つまり奇数個の互換の積で書ける) とき奇置換という. σ は偶置換
- (ii) $\sigma \in S_n$ の符号 $\text{sign}(\sigma)$ を次のように定義する:
- $$\text{sign}(\sigma) = \begin{cases} 1 & (\sigma \text{ は偶置換}), \\ -1 & (\sigma \text{ は奇置換}). \end{cases}$$
- (iii) S_n の偶置換全体の集合を A_n と書き, n 次交代群という.

A_n は S_n の正規部分群になること,
 $|A_n| = \frac{1}{2} |S_n|$ となることを示すことができる.

例

$$(i) S_3 \ni \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1, 2)(1, 3)(2, 3)(1, 3) = (1, 3)(1, 3),$$

$$S_4 \ni \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1, 2)(3, 4) \text{ は偶置換.}$$

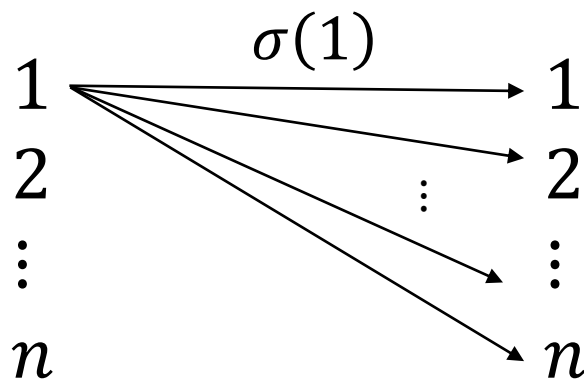
$$(ii) S_3 \ni \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2, 3) \text{ は奇置換.}$$

$$(iii) A_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

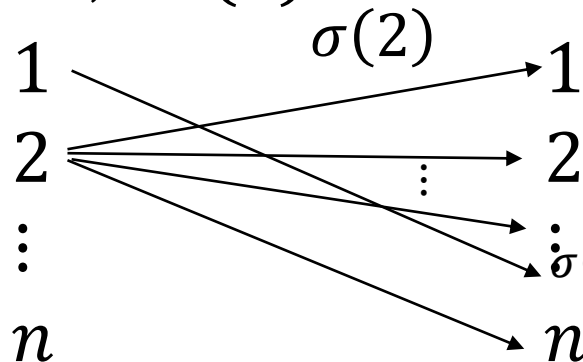
$|S_n|$ の求め方

S_n の位数は $n! = n(n-1)(n-2) \cdots 3 \cdot 2 \cdot 1$ であることを説明する.

$\sigma \in S_n$ について, $\sigma(1)$ が取り得る値は $1, \dots, n$ の n 通り存在する.



$\sigma(1)$ が決まったあとは, $\sigma(2)$ は $1, \dots, n$ から $\sigma(1)$ を除いた値になるので, $\sigma(2)$ が取り得る値は $n-1$ 通り存在する.



$\sigma(1)$ は $\sigma(2)$ の候補から外れる

$\sigma(1)$ は n 通りの値を取り，そのそれぞれについて $\sigma(2)$ は $n - 1$ 通りの値をとるので， $\sigma(1), \sigma(2)$ の組が取り得る値は $n(n - 1)$ 通り存在する．

同様に考えると， $\sigma(1), \sigma(2), \dots, \sigma(m)$ が決まったあと $\sigma(m + 1)$ が取り得る値は $n - m$ 通りある．

$m + 1$ 個の自然数 $\sigma(1), \sigma(2), \dots, \sigma(m), \sigma(m + 1)$ が取り得る値の組み合わせは $n(n - 1) \cdots (n - m)$ 通り存在する．よって，上の式で $m = n - 1$ とすれば $\sigma(1), \sigma(2), \dots, \sigma(n)$ が取り得る値の組み合わせは $n!$ 通り存在し，各組合せは $\sigma \in S_n$ の元を定めるから $|S_n| = n!$ ．

付録2

(講義アンケートの質問への回答)

講義アンケートの質問への回答

Q1. 細かい話ですが、集合 A と演算 \cdot があった際に「 A を群と呼ぶ」のか「 A と \cdot のセット」を群と呼ぶのかについて気になりました。講義では前者で説明されておりましたが、以前学習した際は後者であり、どちらも呼び方としてあり得るのかどうかについて教えていただければと思います。

A1. 丁寧な定義は「 (A, \cdot) を群と呼ぶ」です。ただし、誤解の恐れがない場合は演算は省略して書くことが多いです。元同士の演算でも $a \cdot b$ ではなく ab ($a, b \in A$) と演算を省略することが多いです。

Q2. 講義の後半で説明いただいた「証明」について、考え方（アプローチ）や記述方法などを理解したい。参考となるテキスト等を教えていただきたい。証明が極端に難しく感じるためです。

A2. 講義の参考書としては

- ・宮地 充子(著),「代数学から学ぶ暗号理論」,
日本評論社

が挙げられます。個人的にお勧めの代数学の入門書は次の二冊の本です。

- ・松坂 和夫(著),「代数系入門」, 岩波書店
- ・新妻 弘(著), 木村 哲三 (著),「群・環・体入門」,
共立出版（この本の問に解答を与えた
「演習 群・環・体入門」という本もある）

個人差があるので試し読みすることをお勧めします。

Q3. 置換の積の計算方法を補足で教えていただけたら
ありがたかったです。

A3. 補足1に説明を追加したのでご確認ください.

Q4. 全単射、行列計算

A4. 全単射については、補足1をご覧ください。
行列の計算について説明します。

$$m \times n \text{ 行列 } A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}, B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \cdots & b_{mn} \end{pmatrix}$$

(行の数が m 個で列の数が n この行列)について,
 A と B の和 (足し算) を

$$A + B = \begin{pmatrix} a_{11} + b_{11} & \cdots & a_{1n} + b_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & \cdots & a_{mn} + b_{mn} \end{pmatrix}$$

と定義する。

また, $n \times \ell$ 行列 $C = \begin{pmatrix} c_{11} & \cdots & c_{1\ell} \\ \vdots & \ddots & \vdots \\ c_{n1} & \cdots & c_{n\ell} \end{pmatrix}$ について,

A と C の積 (乗算, 掛け算) を

$$\begin{aligned} AC &= \begin{pmatrix} a_{11}c_{11} + a_{12}c_{21} + \cdots + a_{1n}c_{n1} & \cdots & a_{11}c_{1\ell} + \cdots + a_{1n}c_{n\ell} \\ \vdots & \ddots & \vdots \\ a_{m1}c_{11} + \cdots + a_{mn}c_{n1} & \cdots & a_{m1}c_{1\ell} + \cdots + a_{mn}c_{n\ell} \end{pmatrix} \\ &= \begin{pmatrix} \sum_{1 \leq i \leq n} a_{1i}c_{i1} & \cdots & \sum_{1 \leq i \leq n} a_{1i}c_{i\ell} \\ \vdots & \ddots & \vdots \\ \sum_{1 \leq i \leq n} a_{mi}c_{i1} & \cdots & \sum_{1 \leq i \leq n} a_{mi}c_{i\ell} \end{pmatrix} \end{aligned}$$

と定義する. ここで, 行列の成分 a_{ij}, b_{ij}, c_{ij} は, 和や積といった2つの演算が可能で, ある種の条件を満たす環とよばれる集合の元である. 後の講義で環を学習する.

行列の和は同じ行数と列数を持つ行列同士でのみ定義でき、
行列の積 AC は、左側の行列 (A) の列数と右側の行列 (C) の
行数が同じ行列同士でのみ定義できる。

$n \times n$ 行列 $\begin{pmatrix} d_{11} & \cdots & d_{1n} \\ \vdots & \ddots & \vdots \\ d_{n1} & \cdots & d_{nn} \end{pmatrix}$ について、

対角成分 d_{ii} ($1 \leq i \leq n$) が全て 1 でそれ以外の
 d_{ij} ($i \neq j$) は全て 0 であるとき n 次単位行列と呼び、
 I_n または E_n と書く (n を省略する場合もある)。

$n \times n$ 行列のように行数と列数が等しい行列を正方行列
という。 D を $n \times n$ 正方行列 (n 次正方行列) とする。
 $DD' = D'D = I_n$ を満たす n 次正方行列 D' が存在する
とき D を正則行列といい、 D' を D の逆行列といい、
 D^{-1} と書く。

例

$$A = \begin{pmatrix} 3 & 1 \\ 2 & 4 \end{pmatrix}, B = \begin{pmatrix} 1 & -1 \\ 5 & 2 \end{pmatrix}, C = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ とする.}$$

$$A + B = \begin{pmatrix} 3 + 1 & 1 - 1 \\ 2 + 5 & 4 + 2 \end{pmatrix} = \begin{pmatrix} 4 & 0 \\ 7 & 6 \end{pmatrix},$$

$$AB = \begin{pmatrix} 3 \cdot 1 + 1 \cdot 5 & 3 \cdot (-1) + 1 \cdot 2 \\ 2 \cdot 1 + 4 \cdot 5 & 2 \cdot (-1) + 4 \cdot 2 \end{pmatrix} = \begin{pmatrix} 8 & -1 \\ 22 & 6 \end{pmatrix}.$$

$$C^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = C.$$

Q5. 正規部分群の説明で $\text{INV}(a) \cdot N \cdot a = N$ と黒板に書いていましたが、他の解説書では $a \cdot N \cdot \text{INV}(a) = N$ と書いているものもありました。どちらも任意の $a \in G$ に足して $\text{inv}(a)$ を乗算して $a \cdot N = N \cdot a$ を変形しただけなのでどちらでもOKなののでしょうか？

A5. はい、どちらでもよいです.

Q6. 剰余類について ラグランジュの定理に関する証明
において、 $|H_a i| = |H|$ となることの証明について

A6. 一つの証明方法としては、写像

$$f : H \rightarrow Ha_i; h \mapsto ha_i$$

が全単射であることを示す方法があります.

f が全単射であれば $|H| = |Ha_i|$ です (補足1参照).

f の単射性 : $h, h' \in H$ について,

$$f(h) = f(h') \Rightarrow ha_i = h'a_i \Rightarrow h = h' \quad (\text{両辺に } a_i^{-1} \text{ をかける})$$

より f は単射.

f の全射性 : 任意の $ha_i \in Ha_i$ について, $h \in H$ は

$f(h) = ha_i$ を満たすから f は全射.

以上より, f は全単射となるから $|H| = |Ha_i|$ です.

Q7. 課題のテーマであった「 $U(\mathbb{Z}/n\mathbb{Z})$ との群としての違い」を正しく理解できていないです。説明をお願いしたいです。

A7. $U(\mathbb{Z}/n\mathbb{Z})$ と $\langle \zeta_n \rangle$ の群として違いですね.

例えば, 課題の解説でも見たように $U(\mathbb{Z}/8\mathbb{Z})$ は一つ元で生成できない, つまり, $U(\mathbb{Z}/8\mathbb{Z})$ は巡回群ではありません. 一方, $\langle \zeta_8 \rangle$ は ζ_8 で生成される巡回群です. また, $U(\mathbb{Z}/8\mathbb{Z})$ と $\langle \zeta_4 \rangle$ の位数はそれぞれ 4 となりますが, $\langle \zeta_4 \rangle$ は巡回群なので 2 つの群の構造は異なり, 位数によって群の構造が決まらないことも分かります. 一方, $U(\mathbb{Z}/7\mathbb{Z})$ など $U(\mathbb{Z}/n\mathbb{Z})$ が巡回群になる場合もあります. $U(\mathbb{Z}/n\mathbb{Z})$ が巡回群でありその位数を m とすると $U(\mathbb{Z}/n\mathbb{Z})$ と $\langle \zeta_m \rangle$ は群として同型になります⁹².