群論 (第 2 回)

2. 対称群

今回は対称群について解説します.

定義 2-1(対称群)

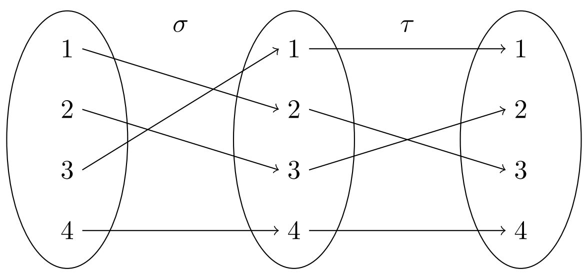
(1) S_n を $\{1, 2, \ldots, n\}$ から $\{1, 2, \ldots, n\}$ への全単射全体とし, その演算を写像の合成 $\circ$ で定める. このとき, $(S_n, \circ)$ は群になり, これを n **次対称群**と言う. S_n の単位元は恒等写像であり, $\sigma \in S_n$ の逆元は逆写像 σ^{-1} である.

(2) $\sigma \in S_n$ は $a_i = \sigma(i)$ $(i = 1, \ldots, n)$ を満たすとき,

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} \qquad \text{(eq1)}$$

で表す.

S_4 の元として下図の σ, τ を考えます.



このとき, σ, σ^{-1}, $\tau \circ \sigma$ はそれぞれ次のように表せます.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \quad \sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \quad \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

例題 2-1
S_3 の元を (eq1) の形で表せ．また S_3 がアーベル群でないことを示せ．

[解答]
S_3 の元を (eq1) の形で表すと次のようになる．

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

また

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

従って S_3 はアーベル群でない．

□

[コメント] n 次対称群 S_n は $n!$ 個の要素を持つ群であり，また $n \geq 3$ のときは常にアーベル群にはならない．

問題 2-1 S_7 の元

$$
\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 7 & 4 & 6 & 5 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 7 & 3 & 1 & 6 & 2 \end{pmatrix}
$$

に対して，$\sigma\tau$, σ^2, σ^{-1} をそれぞれ (eq1) の形で表せ．

定義 2-2 (巡回置換)

相異なる $a_1, a_2, \ldots, a_s \in \{1, 2, \ldots, n\}$ を取る. $\sigma \in S_n$ が

$$\sigma(x) = \begin{cases} a_{i+1} & x = a_i \ (i = 1, 2, \ldots, s-1), \\ a_1 & x = a_s, \\ x & \text{それ以外} \end{cases}$$

を満たすとき, σ は長さ s の**巡回置換**といい, $(a_1 \ a_2 \cdots a_s)$ で表す. 特に, $s = 2$ のとき $\sigma = (a_1 \ a_2)$ を**互換**と言う. また $\sigma = (a_1 \cdots a_s)$, $\tau = (b_1 \cdots b_t)$ に対して,

$$\{a_1, \ldots, a_s\} \cap \{b_1, \ldots, b_t\} = \emptyset$$

であるとき, σ と τ は**共通部分がない**と言う.

S_5 の元

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}$$

はそれぞれ $\sigma = (1 \ 2 \ 5)$, $\tau = (3 \ 4)$ と表せます. 次に巡回置換に関してよく使う性質をまとめておきます.

定理 2-1

(1) 長さ s の巡回置換 σ に対して $\sigma^s = 1$ が成り立つ.

(2) 巡回置換 σ_1,σ_2 に共通部分がないならば, $\sigma_1\sigma_2 = \sigma_2\sigma_1$ が成り立つ.

(3) S_n の元は巡回置換の積で書ける.

(4) $(a_1 \ a_2 \ \cdots \ a_s) = (a_1 \ a_2)(a_2 \ a_3)\cdots(a_{s-1} \ a_s)$. これと (3) より, S_n の各元は互換の積で表せる.

(5) $\sigma \in S_n$ を互換の積 $\sigma = \sigma_1\sigma_2\cdots\sigma_s$ (σ_i : 互換) で表すとき, s の偶奇は表し方に依存しない.

定理 2-1 (5) の記号のもと, 次の写像を考えます.

$$\mathrm{sgn} : S_n \to \{\pm 1\} \quad (\sigma \mapsto (-1)^s).$$

s の偶奇は互換の積の表し方に依存しないので, 上の写像は well-defined となります. $\mathrm{sgn}(\sigma) = 1$ のとき, σ を**偶置換**, $\mathrm{sgn}(\sigma) = -1$ のとき, σ を**奇置換**と言います. また sgn の定義から次が成り立

ちます.

$$\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau) \qquad (\sigma, \tau \in S_n).$$

次に定理 2-1 の使い方を確認しておきます.

例題 2-2

$\sigma \in S_7$ の元

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 4 & 5 & 3 & 7 & 6 \end{pmatrix}$$

を考える.

(1) σ を巡回置換の積で表せ.

(2) $\mathrm{sgn}(\sigma)$ を求めよ.

(3) σ^4 を求めよ.

(解答)

(1) $1, 2, ..., 7$ の各元は

$$1 \to 2 \to 1, \quad 3 \to 4 \to 5 \to 3, \quad 6 \to 7 \to 6$$

と循環するので, σ は次のように巡回置換で分解できる.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 4 & 5 & 3 & 7 & 6 \end{pmatrix} = (1\ 2)(3\ 4\ 5)(6\ 7).$$

(2) 定理 2-1 (4) から,

$$\sigma = (1\ 2)(3\ 4\ 5)(6\ 7) = (1\ 2)(3\ 4)(4\ 5)(6\ 7)$$

と分解できる. 従って $\mathrm{sgn}(\sigma) = (-1)^4 = 1$.

(3) (1 2), (3 4 5), (6 7) は互いに共通部分を持たないので定理 2-1 (2) からそれぞれの積は可換である. 従って

$$\sigma^4 = ((1\ 2)(3\ 4\ 5)(6\ 7))^4 = (1\ 2)^4(3\ 4\ 5)^4(6\ 7)^4.$$

定理 2-1 (1) より $(1\ 2)^2 = (3\ 4\ 5)^3 = (6\ 7)^2 = \mathrm{Id}$. よって

$$\sigma^4 = (3\ 4\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 5 & 3 & 6 & 7 \end{pmatrix}.$$

□

問題 2-2 S_7 の元

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 2 & 6 & 3 & 4 & 1 \end{pmatrix}, \ \ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 4 & 5 & 2 & 6 & 3 & 7 \end{pmatrix}$$

を考える.

(1) $\mathrm{sgn}(\sigma)$, $\mathrm{sgn}(\tau)$ を計算せよ.

(2) σ^{15}, $(\tau\sigma\tau^{-1})^{15}$ をそれぞれ (eq1) の形で表せ.

(3) $\eta^2 = \sigma$ を満たす $\eta \in S_7$ が存在しないことを示せ.

問題 2-3

(1) $\sigma \in S_n$ に対し, $\sigma(a_1\ a_2\ \cdots a_s)\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2)\ \cdots \sigma(a_s))$ を示せ.

(2) S_4 の部分集合 $C = \{\sigma \in S_4 \mid \sigma(1\ 2)\sigma^{-1} = (3\ 4)\}$ とするとき, C を具体的に求めよ.