群論 (第5回)

5. 生成系

今回は群の生成系について説明します.

定義 5-1

群 G の空でない部分集合 S に対して,

$$< S >= \{x_1^{n_1} x_2^{n_2} \cdots x_t^{x_t} \mid t \in \mathbb{N},\ n_i \in \mathbb{Z},\ x_i \in S\}$$

を S **で生成された** G **の部分群**と言う. $S = \{x_1, \ldots, x_m\}$ のときは, $< S >$ を単に $\langle x_1, \ldots, x_m \rangle$ で表す.

例えば, 3 次対称群 S_3 において $\sigma = (1\ 2),\ \tau = (1\ 3) \in S_3$ を考えます. このとき,

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \mathrm{Id} = \sigma^0, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \sigma\tau\sigma, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \sigma,$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \tau\sigma, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma\tau, \quad \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \tau.$$

従って, S_3 の各元は σ, τ の積で表せており, $S_3 =< \sigma, \tau >$ が成り立ちます.

定理 5-1

群 G の空でない部分集合 S に対して, $< S >$ は S を含む最小の G の部分群である.

[証明]

(I) $x \in S$ とすると, $x = x^1 \in < S >$. よって $S \subseteq < S >$.

(II) 次に $< S >$ が G の部分群であること示す.

(1) $S \neq \emptyset$ より, $x \in S$ がとれる. よって, $1_G = x^0 \in < S >$.

(2) $z_1, z_2 \in < S >$ を取り,

$$z_1 = x_1^{m_1} \cdots x_s^{m_s}, \quad z_2 = y_1^{n_1} \cdots y_t^{n_t} \quad (m_i, n_i \in \mathbb{Z},\ x_i, y_i \in S)$$

で表す. このとき, $z_1 z_2 = x_1^{m_1} \cdots x_s^{m_s} y_1^{n_1} \cdots y_t^{n_t} \in < S >$.

(3) $z \in < S >$ を取り,

$$z = x_1^{m_1} \cdots x_{t-1}^{m_{t-1}} x_t^{m_t} \quad (m_i \in \mathbb{Z},\ x_i \in S)$$

で表す. このとき, $z^{-1} = x_t^{-m_t} x_{t-1}^{-m_{t-1}} \cdots x_1^{-m_1} \in < S >$.

よって, $< S >$ は G の部分群である.

(III) 最小性を証明する. これを示すには, H が S を含む G の部分群なら, $< S > \subseteq H$ が成り立つことを言えばよい. $z \in < S >$ を取り,

$$z = x_1^{n_1} \cdots x_t^{n_t} \quad (n_i \in \mathbb{Z},\ x_i \in S)$$

で表す. $x_i \in S \subseteq H$ $(i = 1, \ldots, t)$ であり, H は部分群だから, $z = x_1^{n_1} \cdots x_t^{n_t} \in H$. 従って, $\langle S \rangle \subseteq H$ である.

□

問 5-1 4 次対称群 S_4 の部分集合 $S = \{(1\ 2),\ (1\ 3),\ (1\ 4)\}$ に対して, $S_4 =< S >$ を示せ.

例題 5-1
G をアーベル群とし, $x, y \in G$ とする. $|x| = 2,\ |y| = 3$ のとき, $< x, y > = < xy >$ を示せ.

[解答]

$x, y \in < x, y >$ より $xy \in < x, y >$. 定理 5-1 から $< xy >$ は xy を含む最小の部分群なので $< xy > \subseteq < x, y >$ が成り立つ. 同様に $x = (xy)^3 \in < xy >,\ y = (xy)^4 \in < xy >$ であるから, $< x, y >$ の最小性より $< x, y > \subseteq < xy >$ も従う.

□

問 5-2 群 G と $x \in G$ を考える. x の位数が奇数のとき, $< x > = < x^2 >$ を示せ.

定理 5-2

G を群とし, $x \in G$ は位数 d の元とする. このとき, 次が成り立つ.

(1) $< x >= \{1_G,\ x, \ldots,\ x^{d-1}\}$.

(2) $1_G,\ x, \ldots,\ x^{d-1}$ は相異なる.

特に, $| < x > | = d$ が成り立つ.

[証明]

(1) $y \in \langle x \rangle$ を取り, $y = x^n$ $(n \in \mathbb{Z})$ と表す. $n = qd + r$ $(0 \leq r < d)$ を満たす $q, r \in \mathbb{Z}$ を取れば,

$$x^n = (x^d)^q \cdot x^r = x^r \in \{1_G, \ldots, x^{d-1}\}.$$

従って, $< x > \subseteq \{1_G, \ldots, x^{d-1}\}$. 逆の包含は明らか.

(2) $x^i = x^j$ $(0 \leq i < j \leq d-1)$ と仮定する. このとき,

$$x^{j-i} = 1_G, \qquad 1 \leq j - i \leq j < d$$

となるが, これは $|x| = d$ に反する. 従って $1_G,\ x, \ldots,\ x^{d-1}$ は相異なる.

□

定義 5-2 (巡回群)

群 G が**巡回群**であるとは $G = \langle a \rangle$ となる $a \in G$ が存在することである. また, 部分群が巡回群であるとき, **巡回部分群**と言う.

自然数 n に対して, $\mathbb{C}^\times$ の部分集合 H を

$$H = \{z \in \mathbb{C}^\times \mid z^n = 1\}$$

で定めます. $\alpha = e^{\frac{2\pi i}{n}}$ と置くと, $\alpha^n = 1$ より

$$H = \left\{ \alpha^k \,\middle|\, k = 0, 1, ..., n-1 \right\} = < \alpha > .$$

従って, H は $\mathbb{C}^\times$ の巡回部分群です.

問題 5-3 巡回群はアーベル群であることを示せ.

問題 5-4 巡回群の部分群は巡回部分群であることを示せ.