群論 (第4回)

4. 位数

今回は位数の定義や性質について解説します.

定義 4-1 (元の位数)
群 G の元 $x \in G$ に対して, $x^n = 1_G$ を満たす最小の自然数 n を x の**位数**と呼び, $|x|$ または $\mathrm{ord}(x)$ で表す. そのような自然数が存在しないとき, x の位数は無限であると言い, $|x| = \infty$ で表す.

※ 定義から次が成り立つ.

(i) $|x| = 1 \iff x = 1_G$.

(ii) $|x| = \infty \iff x^n \neq 1_G \ (\forall n \geq 1)$.

例えば, S_3 の元 $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ をとると,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq \mathrm{Id}, \quad \sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \neq \mathrm{Id}, \quad \sigma^3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \mathrm{Id}.$$

従って $|\sigma| = 3$ となる.

問題 4-1 2次正則行列全体 $\mathrm{GL}_2(\mathbb{C})$ において考える. 行列

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & k \\ i & 0 \end{pmatrix}$$

を考える. ただし, $i = \sqrt{-1}, \quad k \in \mathbb{C}^\times$ とする.

(1) A, B の位数を求めよ.

(2) C の位数が 4 のとき, k の値を求めよ.

(3) $M \in \mathrm{GL}_2(\mathbb{C})$ に対し, MBM^{-1} の位数を求めよ.

定理 4-1

群 G の元 $x \in G$ を考える．$|x| = n$ のとき，

$$x^m = 1_G \iff n \mid m.$$

[証明]

$\Longleftarrow$ について．$m = nk$ $(k \in \mathbb{Z})$ と表せるので，

$$x^m = (x^n)^k = 1_G^k = 1_G.$$

$\Longrightarrow$ について．$m = qn + r$ ($0 \le r \le n-1$) を満たす $q, r \in \mathbb{Z}$ をとる．このとき，

$$1_G = x^m = x^{qn+r} = (x^n)^q x^r = x^r.$$

x の位数は n だから，$r = 0$ でなければならない．よって $n \mid m$.

$\square$

定理 4-1 の使い方を紹介します．

例題 4-1

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 \end{pmatrix} \in S_7$ の位数を求めよ．

[解答]

$\sigma = (1\ 2\ 3\ 4\ 5)(6\ 7)$ と表せるので，

$$\sigma^{10} = (1\ 2\ 3\ 4\ 5)^{10}(6\ 7)^{10} = \mathrm{Id}.$$

定理 4-1 より $|\sigma| \mid 10$ であるから，$|\sigma| = 1, 2, 5, 10$ のいずれかとなる．

$$\begin{aligned} \sigma^1 &\neq \mathrm{Id}, \\ \sigma^2 &= (1\ 2\ 3\ 4\ 5)^2(6\ 7)^2 = (1\ 3\ 5\ 2\ 4) \neq \mathrm{Id}, \\ \sigma^5 &= (1\ 2\ 3\ 4\ 5)^5(6\ 7)^5 = (6\ 7) \neq \mathrm{Id}. \end{aligned}$$

従って $|\sigma| = 10$.

$\square$

問題 4-2 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 2 & 1 & 7 & 4 & 6 \end{pmatrix} \in S_7$ の位数を求めよ．

群 G の元 $x \in G$ を考える．位数の定義は次のように言い換えられる．

$$|a| = n \Longleftrightarrow \begin{cases} (1)\ a^n = 1_G, \\ \\ (2)\ a^l = 1_G\ (l \in \mathbb{N}) \implies l \geq n. \end{cases}$$

証明では上記の (1), (2) を示す場合が多い．

例題 4-2

群 G と $x \in G$ に対して次を示せ．

$$|x| = 2n \implies |x^2| = n.$$

[証明]

(1) $|x| = 2n$ より $(x^2)^n = x^{2n} = 1_G$.

(2) $(x^2)^l = 1_G$ $(l \in \mathbb{N})$ とする．$x^{2l} = 1_G$ で $|x| = 2n$ より, $2l \geq 2n$. 従って $l \geq n$.

以上から $|x^2| = n$ である．

$\square$

問 4-3 群 G と $x, y \in G$ を考える．

(1) $|xy| = n$ ならば, $|yx| = n$ を示せ．

(2) G はアーベル群, $m = |x|$, $n = |y|$ とする．$\gcd(m, n) = 1$ のとき, $|xy| = mn$ を示せ．

定理 4-2

有限群 G と $x \in G$ を考える．このとき, $|x| < \infty$ である．

[証明]

$n = |G|$ とすると, $x^1, x^2, \cdots, x^n, x^{n+1}$ の中で等しいものがある．$x^j = x^i$ $(1 \leq i < j \leq n+1)$ とすると, $x^{j-i} = 1_G$. 従って $|x| \leq j - i \leq n < \infty$.

$\square$

[コメント]

後の授業で紹介するラグランジュの定理を用いると, $|x|$ は $|G|$ の約数であることが分かる．