群論 (第7回)

7. ラグランジュの定理

今回は部分群から作られる同値類について考察し, さらに有限群の重要な性質であるラグランジュの定理についてみます.

群 G とその部分群 H に対して, G 上の 2 項関係 $\underset{H}{\sim}$ を

$$x \underset{H}{\sim} y \overset{\text{def}}{\iff} x^{-1}y \in H$$

により定めます.

定理 7-1

2 項関係 $\underset{H}{\sim}$ は G の同値関係である.

[証明]

(1) $x \in G$ に対して, $x^{-1}x = 1_G \in H$ より $x \underset{H}{\sim} x$. 従って反射律を満たす.

(2) $x, y \in G$ に対して, H は G の部分群より

$$x \underset{H}{\sim} y \implies x^{-1}y \in H \implies (x^{-1}y)^{-1} \in H \implies y^{-1}x \in H \implies y \underset{H}{\sim} x.$$

よって対称律を満たす.

(3) $x, y, z \in G$ に対して,

$$x \underset{H}{\sim} y,\ y \underset{H}{\sim} z \implies x^{-1}y \in H,\ y^{-1}z \in H \implies x^{-1}z = (x^{-1}y)(y^{-1}z) \in H \implies x \underset{H}{\sim} z.$$

よって推移律も満たす .

□

$x \in G$ に対して, x の $\underset{H}{\sim}$ による同値類 $C(x)$ を考えます. つまり,

$$C(x) = \{y \in G \mid x \underset{H}{\sim} y\}.$$

これを x の**剰余類**と言います.

定理 7-2

$x \in G$ に対して,

$$xH = \{xy \mid y \in H\}$$

と置く. このとき, $C(x) = xH$ が成り立つ.

※ G の演算が加法 $+$ の場合は xH は $x + H$ で表す.

[証明]

$y \in G$ に対して,

$$y \in C(x) \iff x \underset{H}{\sim} y \iff x^{-1}y \in H \iff x^{-1}y = h \ \ (\exists h \in H) \iff y \in xH.$$

よって $C(x) = xH$ が成り立つ.

□

定理 7-3

群 G とその部分群 H を考える. また, $x, y \in G$ とする.

(1) $y \in xH \iff xH = yH.$

(2) $y \notin xH \iff xH \neq yH \iff xH \cap yH = \phi.$

[証明]

定理 7-3 は同値類の一般論から従う (文献 [1] 定理 7-1 を参照).

□

同値関係 $\underset{H}{\sim}$ のよる商集合を

$$G/H = \{C(x) \mid x \in G\} = \{xH \mid x \in G\}$$

で表します. G/H の要素の個数を H の G における**群指数**と言い, $(G : H)$ で表します.

例題 7-1

3 次対称群 S_3 の元

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

を取り, $H =< \tau >$ と置く. 各 $\rho \in H$ に対して, ρH を求めよ. また $(S_3 : H)$ を求めよ.

[**解答**]
I を S_3 の単位元とすると,

$$IH \quad = \quad H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

また H に含まれない S_3 の元として,

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

を選ぶと,

$$\sigma H \quad = \quad \{\sigma\mu \mid \mu \in H\} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}.$$

$\rho \in H$ のとき, 定理 7-3 (1) より $\rho H = H$ であり, $\rho \in \sigma H$ のとき, $\rho H = \sigma H$. 従って,

$$S_3/H = \{\rho H \mid \rho \in S_3\} = \{H, \sigma H\}.$$

特に $(S_3 : H) = 2$ である.

□

問題 7-1 3 次対称群 S_3 の元 $\sigma = (1, 2)$ を考える. $H =< \sigma >$ に対して, $(S_3 : H)$ を求めよ.

定義 7-1 (完全代表系)
群 G とその部分群 H に対して, G の部分集合 R が次の (1), (2) を満たすとき, G/H の**完全代表系**と言う.

(1) $G/H = \{xH \mid x \in R\}$.

(2) $x, y \in R \quad (x \neq y) \implies xH \neq yH$.

※ 完全代表系は各剰余類から一つずつ元をとってできる G の部分集合である.

例題 7-1 では, S_3/H の完全代表系として $R = \{I, \sigma\}$ をとることができます. 次の例題では, 「完全代表系の証明の仕方」についてみます.

例題 7-2
自然数 n に対して, $\mathbb{Z}$ の部分群 $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$ を考える. このとき, $\mathbb{Z}/n\mathbb{Z}$ の完全代表系は $R = \{0, 1, \ldots, n-1\}$ であることを示せ. 特に $(\mathbb{Z} : n\mathbb{Z}) = n$ が成り立つ.

[証明]

R が完全代表系の条件 (1), (2) を満たすことを示せばよい.

(i) $x+n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ とする. $x = an+b$ $(0 \leq b < n)$ となる $a, b \in \mathbb{Z}$ を取る. このとき, $x \in b+n\mathbb{Z}$. 定理 7-3 から $x+n\mathbb{Z} = b+n\mathbb{Z}$. また $0 \leq b < n$ より, $b \in R$. 従って, R は定義 7-1 の条件 (1) を満たす.

(ii) 次に定義 7-1 の条件 (2) を示す代わりに対偶をとって次を示す.

$$r_1, r_2 \in R\ (r_1 + n\mathbb{Z} = r_2 + n\mathbb{Z},\ r_1 \leq r_2) \Rightarrow r_1 = r_2.$$

$r_1 \in r_1 + n\mathbb{Z} = r_2 + n\mathbb{Z}$ より, $r_1 = r_2 + nk$ $(k \in \mathbb{Z})$ とかける. このとき,

$$0 \leq r_2 - r_1 \leq r_2 \leq n-1, \quad r_2 - r_1 = -nk$$

より $r_2 - r_1 = 0$ が従う. よって $r_1 = r_2$.

□

問題 7-2 $\mathbb{R}^2$ の部分群 $V = \{(t,t) \mid t \in \mathbb{R}\}$ を考える. このとき,

$$R = \{(a,0) \mid a \in \mathbb{R}\}$$

は $\mathbb{R}^2/V$ の完全代表系であることを示せ.

定理 7-4 (ラグランジュの定理)

有限群 G とその部分群 H に対して,

$$|G| = (G:H)|H|$$

が成り立つ.

例えば, 例題 7-1 の状況を考えると,

$$(S_3 : H) \times |H| = 2 \times 3 = |S_3|$$

となり, ラグランジュの定理を満たすことが分かる.

[**定理 7-4 の証明**]

$\{x_1, \ldots, x_n\}$ を G/H の完全代表系とすると, $(G:H) = n$ であり,

$$G = x_1H \cup x_2H \cup \cdots \cup x_nH, \quad x_iH \cap x_jH = \phi\ (i \neq j)$$

が成り立つ. $f_i : H \longrightarrow x_iH$ $(y \longmapsto x_iy)$ は全単射より $|H| = |x_iH|$. 従って

$$|G| = |x_1H| + \cdots + |x_nH| = n|H| = (G:H)|H|.$$

□

次に, ラグランジュの定理から導ける群の性質について考えます.

定理 7-5

有限群 G とその部分群 H, K を考える. また $x \in G$ とする.

(1) $|H| \mid |G|$.

(2) $|x| \mid |G|$.

(3) $x^{|G|} = 1_G$.

(4) $K \subseteq H$ のとき, $(G : K) = (G : H)(H : K)$.

[証明]

(1) 定理 7-4 より成り立つ.

(2) 定理 5-2 より $|x| = |\langle x \rangle|$ である. これと (1) より従う.

(3) (2) より, $|G| = n|x|$ (n : 自然数) と表せる. よって

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

(4) 定理 7-4 より,

$$|G| = (G : H)|H| = (G : K)|K|.$$

一方, K は H の部分群でもあるので $|H| = (H : K)|K|$. 従って

$$(G : K)|K| = (G : H)|H| = (G : H)(H : K)|K|.$$

よって $(G : K) = (G : H)(H : K)$.

□

例題 7-3

有限群 G と $x \in G$ を考える. $|G| = 10$ かつ $x^3 = 1_G$ ならば $x = 1_G$ を示せ.

[解答]

定理 7-5 (3) より $x^{10} = 1_G$. よって,

$$x = x^{10+3(-3)} = x^{10} \cdot (x^3)^{-3} = 1_G.$$

□

定理 7-6

素数 p と群 G を考える．$|G| = p$ ならば, G は巡回群である．

[**証明**]

$p \geq 2$ より, $x \in G \setminus \{1_G\}$ が取れる．このとき, 定理 7-5 (2) より $|x| \mid p$ を得る．p は素数より, $|x| = 1$ または p となる．$x \neq 1_G$ より $|x| = p$. 定理 5-2 より, $|\langle x \rangle| = |x| = p = |G|$ であるから, $G = \langle x \rangle$ が従う．よって G は巡回群である．

□

問題 7-3 奇数の位数を持つ群 G と $x \in G$ について考える．$x^2 = 1_G$ ならば $x = 1_G$ を示せ．

問題 7-4 群 G とその部分群 H, K について考える．異なる素数 p, q に対して, $|G| = pq$, $|H| = p$, $|K| = q$ のとき, $H \cap K = \{1_G\}$ を示せ．

最後にラグランジュの定理の応用として, 3 次対称群 S_3 の部分群について考察する．

例題 7-4

3 次対称群 S_3 の部分群を全て求めよ．

[**解答**]

まず,

$$\sigma_1 = I_{S_3} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

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

と置く．また H を G の部分群とする．ラグランジュの定理より, $|H| \mid |S_3| = 6$. よって, $|H|$ は $1, 2, 3, 6$ のいずれか. それぞれ場合分けをして考える．

(i) $|H| = 1$ のとき, $H = \{\sigma_1\}$.

(ii) $|H| = 6$ のとき, $H = S_3$.

(iii) $|H| = 2$ のとき, 定理 7-6 から $H =< \sigma >$ $(\sigma \in S_3)$ と表せる．ここで $|\sigma| = 2$ より, $\sigma = \sigma_2, \sigma_3, \sigma_6$ のいずれかとなる．従って

$$< \sigma_2 >= \{1, \sigma_2\}, \ < \sigma_3 >= \{1, \sigma_3\}, \ < \sigma_6 >= \{1, \sigma_6\}.$$

(iv) $|H| = 3$ のとき, $H =< \sigma >$ $(\sigma \in S_3)$ と表せる. $|\sigma| = 3$ より $\sigma = \sigma_4, \sigma_5$ のいずれか. 従って

$$H =< \sigma_4 >=< \sigma_5 >= \{\sigma_1, \sigma_4, \sigma_5\}.$$

□

参考文献

[1] 集合論 (第 7 回): 同値関係と同値類, 大学数学授業ノート.