

# 代数学 I Extra 講義資料

担当：大矢 浩徳 (OYA Hironori)\*

本資料では講義内では扱いきれなかった群論において重要な概念や話題についての解説を行う。本講義の範囲から先へ進んで勉強したい方向けの内容である。今回の内容が今後の皆様の進んだ学習の中でお役に立てば幸いである。

## 12.1 共役類・類等式

本節では共役類を解説する。共役類の重要性は例えば**表現論 (representation theory)** を学ぶと非常に良く分かる。興味のある方は是非勉強してみて欲しい (以下の注意 2 も参照)。

### 定義 12.1

$G$  を群とする。第 13 回講義資料例 7 で見たように、写像

$$\psi_{\text{ad}}: G \times G \rightarrow G, (g, h) \mapsto ghg^{-1}$$

は  $G$  上の群  $G$  の作用を与える (随伴作用)。このとき、各元  $h \in G$  の随伴作用に関する  $G$ -軌道

$$K(h) := \{\psi_{\text{ad}}(g, h) \mid g \in G\} = \{ghg^{-1} \mid g \in G\}$$

を  $h$  の**共役類 (conjugacy class)** という。

群  $G$  の作用があるとその集合は  $G$ -軌道によって軌道分解されることから、 $G$  は互いに交わりのない共役類へと分割されることがわかる。またこのとき、各  $h \in G$  における固定部分群  $G_h$  は

$$G_h = \{g \in G \mid ghg^{-1} = h\} = \{g \in G \mid gh = hg\} =: Z(h)$$

となる。(この群  $Z(h)$  は  $h$  の**中心化群**と呼ばれる。) よって、軌道・固定群定理 (第 13 回講義資料定理 11.5) より、

$$|K(h)| = (G : Z(h)) \tag{12.1}$$

となる。特に  $G$  を有限群としたとき、共役類の元の個数は必ず  $|G|$  の約数である。

$G$  を有限群とし、 $G$  の共役類への分割

$$G = K(h_1) \cup K(h_2) \cup \cdots \cup K(h_m) \tag{12.2}$$

を考える。ここで、 $h_1 = e$  とする。このとき、

$$K(h_1) = K(e) = \{geg^{-1} \mid g \in G\} = \{e\}. \tag{12.3}$$

よって、(12.1), (12.2), (12.3) より、

$$|G| = |K(h_1)| + |K(h_2)| + \cdots + |K(h_m)| = 1 + \sum_{k=2}^m |K(h_k)| = 1 + \sum_{k=2}^m (G : Z(h_k)) \tag{12.4}$$

となることがわかる。この等式を**類等式 (class formula)** という。

\* e-mail: hoyo@shibaura-it.ac.jp

例 1. 3次二面体群  $D_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$  の共役類を全て求めてみよう. 最初に単位元  $e$  の共役類を考えると, (12.3) より,

$$K(e) = \{e\}$$

次に ( $K(e)$  に含まれない元であれば何でも良いが),  $\sigma \in D_3$  の共役類を考えると,

$$\begin{aligned} K(\sigma) &= \{\sigma^k \sigma (\sigma^k)^{-1}, (\sigma^k \tau) \sigma (\sigma^k \tau)^{-1} \mid k = 0, 1, 2\} \\ &= \{\sigma, \sigma^{-1}\} = \{\sigma, \sigma^2\}. \end{aligned}$$

次に ( $K(e)$ ,  $K(\sigma)$  のいずれにも含まれない元であれば何でも良いが),  $\tau \in D_3$  の共役類を考えると,

$$\begin{aligned} K(\tau) &= \{\sigma^k \tau (\sigma^k)^{-1}, (\sigma^k \tau) \tau (\sigma^k \tau)^{-1} \mid k = 0, 1, 2\} \\ &= \{\tau, \sigma^2 \tau, \sigma^4 \tau\} = \{\tau, \sigma\tau, \sigma^2\tau\}. \end{aligned}$$

以上で  $D_3$  の全ての元がここまで求めた共役類のいずれかの中に現れたので,  $D_3$  の共役類への分割が

$$D_3 = K(e) \cup K(\sigma) \cup K(\tau)$$

となることがわかる. よって,  $D_3$  の共役類は  $K(e)$ ,  $K(\sigma)$ ,  $K(\tau)$  で全てである.\*1類等式は,

$$6 = |D_3| = |K(e)| + |K(\sigma)| + |K(\tau)| = 1 + 2 + 3$$

となる.

例 2. 対称群の共役類を計算しよう. 第5回復習レポート課題解答例問題1 補足解説において証明した以下の定理を頭においておくと便利である.

**定理 12.2**

任意の  $n$  次対称群の元  $\sigma \in \mathfrak{S}_n$  に対し, 以下が成立する.

$$\begin{aligned} (1) \quad & \sigma \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n) \end{pmatrix}. \\ (2) \quad & \sigma \begin{pmatrix} i_1 & i_2 & \cdots & i_n \end{pmatrix} \sigma^{-1} = \begin{pmatrix} \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_n) \end{pmatrix}. \end{aligned}$$

ではまず  $\mathfrak{S}_3$  の共役類を計算してみよう. 最初に単位元  $e$  の共役類を考えると, (12.3) より,

$$K(e) = \{e\}$$

次に ( $K(e)$  に含まれない元であれば何でも良いが),  $(1\ 2) \in \mathfrak{S}_3$  の共役類を考えると, 定理 12.2 (2) より,

$$\begin{aligned} K((1\ 2)) &= \{\sigma(1\ 2)\sigma^{-1} \mid \sigma \in \mathfrak{S}_3\} \\ &= \{(\sigma(1)\ \sigma(2)) \mid \sigma \in \mathfrak{S}_3\} = \{(1\ 2), (1\ 3), (2\ 3)\}. \end{aligned}$$

なお, 最後の等式においては,  $(i\ j) = (j\ i)$  であったことに注意しよう. 次に ( $K(e)$ ,  $K((1\ 2))$ ) のいずれにも含まれない元であれば何でも良いが,  $(1\ 2\ 3) \in \mathfrak{S}_3$  の共役類を考えると, 定理 12.2 (2) より,

$$\begin{aligned} K((1\ 2\ 3)) &= \{\sigma(1\ 2\ 3)\sigma^{-1} \mid \sigma \in \mathfrak{S}_3\} \\ &= \{(\sigma(1)\ \sigma(2)\ \sigma(3)) \mid \sigma \in \mathfrak{S}_3\} = \{(1\ 2\ 3), (1\ 3\ 2)\}. \end{aligned}$$

なお, 最後の等式においては,  $(i\ j\ k) = (j\ k\ i) = (k\ i\ j)$  であったことに注意しよう.

以上で  $\mathfrak{S}_3$  の全ての元がここまで求めた共役類のいずれかの中に現れたので,  $\mathfrak{S}_3$  の共役類への分割が

$$\mathfrak{S}_3 = K(e) \cup K((1\ 2)) \cup K((1\ 2\ 3))$$

\*1 共役類は随伴作用の定める同値関係に関する同値類なので,  $\sigma^2 \in K(\sigma)$  であることから,  $K(\sigma) = K(\sigma^2)$  などが成立していることに注意する.

となることがわかる. よって,  $\mathfrak{S}_3$  の共役類は  $K(e)$ ,  $K((1\ 2))$ ,  $K((1\ 2\ 3))$  で全てである.

次に一般の  $\mathfrak{S}_n$  の場合を考えてみよう. 第 4 回講義資料定理 3.7 (2) より, 任意の  $\mathfrak{S}_n$  の単位元でない元はどの 2 つも互いに素な巡回置換の合成として (順序の違いを除いて) 一意に書かれるのであった.  $\sigma \in \mathfrak{S}_n$  がどの 2 つも互いに素な巡回置換の合成として,

$$\sigma = (i_{1,1} i_{1,2} \cdots i_{1,\ell_1})(i_{2,1} i_{2,2} \cdots i_{2,\ell_2}) \cdots (i_{t,1} i_{t,2} \cdots i_{t,\ell_t}), \ell_1 \geq \ell_2 \geq \cdots \geq \ell_t$$

と書かれるとき, この巡回置換の長さを並べた  $(\ell_1, \ell_2, \dots, \ell_t)$  を  $\sigma$  の **サイクルタイプ** と呼ぶ (第 13 回復習レポート課題問題 4 補足解説参照). ここで, 後の便利さのために, 上の表示においては,  $\sigma$  で動かされない数字  $k$  があつた時にも  $(k)$  という自明な (=単位元に等しい) 巡回置換が合成されていると考えて, 常に

$$\ell_1 + \ell_2 + \cdots + \ell_t = n$$

となるようにすることにする. 例えば,  $\mathfrak{S}_3$  においては,

$$e = (1)(2)(3) \quad (1\ 2) = (1\ 2)(3) \quad (2\ 3) = (2\ 3)(1) \quad (3\ 1) = (3\ 1)(2)$$

というようにする. こうすると,  $\mathfrak{S}_3$  の元

$$e, (1\ 2), (2\ 3), (3\ 1), (1\ 2\ 3), (1\ 3\ 2)$$

のサイクルタイプはこの順に,

$$(1, 1, 1), (2, 1), (2, 1), (2, 1), (3), (3)$$

である. こう見ると, サイクルタイプが同じものをまとめたものが  $\mathfrak{S}_3$  の共役類であることに気付けるだろう. 実はこの考察は一般の  $\mathfrak{S}_n$  で正しい! 定理 12.2 を考えれば, サイクルタイプが同じ 2 つの元は適切な  $\sigma \in \mathfrak{S}_n$  をとって, 左から  $\sigma$ , 右から  $\sigma^{-1}$  を掛けることで移りあえることがわかる. (厳密に考えてみよ. 上に書いた  $\mathfrak{S}_3$  の場合の計算が参考になると思われる.) 逆に左から  $\sigma$ , 右から  $\sigma^{-1}$  を掛けるという操作は元のサイクルタイプを変えないこともわかる. これより, 以下の定理がわかる.

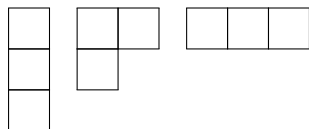
**定理 12.3**

$n$  を 2 以上の整数とする. このとき, 任意の  $\sigma \in \mathfrak{S}_n$  に対し,

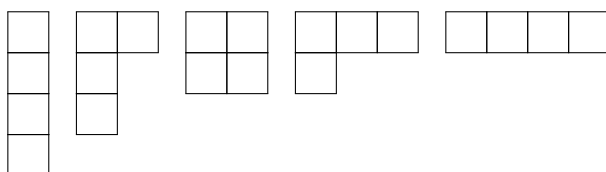
$$K(\sigma) = \{ \sigma' \in \mathfrak{S}_n \mid \sigma \text{ と } \sigma' \text{ のサイクルタイプは等しい} \}$$

となる. 特に,  $\mathfrak{S}_n$  の共役類と「 $\ell_1 + \ell_2 + \cdots + \ell_t = n$  かつ  $\ell_1 \geq \ell_2 \geq \cdots \geq \ell_t$  を満たす正の整数の組  $(\ell_1, \ell_2, \dots, \ell_t)$ 」は 1 対 1 に対応する.

$\ell_1 + \ell_2 + \cdots + \ell_t = n$  かつ  $\ell_1 \geq \ell_2 \geq \cdots \geq \ell_t$  を満たす正の整数の組  $(\ell_1, \ell_2, \dots, \ell_t)$  は  $n$  の **分割** と呼ばれる.  $n$  の分割  $(\ell_1, \ell_2, \dots, \ell_t)$  は, 同じ大きさの  $n$  個の正方形 (箱) を各行の正方形の数が上から順に  $\ell_1, \ell_2, \dots, \ell_t$  となるように左上詰めに配置して得られる図を用いて表されることもある. このようにして得られる図を **ヤング図形 (Young diagram)** と呼ぶ. 例えば, 箱の数が 3 つのヤング図形は



の 3 つあり, 順に 3 の分割  $(1, 1, 1), (2, 1), (3)$  に対応する. 定理を踏まえると, それぞれに対応して  $\mathfrak{S}_3$  の共役類が作れて,  $\mathfrak{S}_3$  の共役類は 3 つである. 同様に考えると, 箱の数が 4 つのヤング図形は



の5つあるので、定理 12.3 から  $\mathfrak{S}_4$  の共役類は全部で5つである\*2.

群構造を調べる上での類等式の応用例を1つ挙げておこう. 一般に群  $G$  に対し,

$$Z(G) := \{z \in G \mid gz = zg, \forall g \in G\}$$

とし,  $Z(G)$  を  $G$  の中心 (center) と呼ぶのであった (代数学 I 中間試験解答例問題 6 補足解説参照). この  $Z(G)$  は  $G$  の正規部分群であったことも合わせて思い出そう\*3.

**定理 12.4**

$p$  を素数とする. このとき, 位数  $p^k$  ( $k$  は 1 以上の整数) の群  $G$  の中心  $Z(G)$  は  $Z(G) \neq \{e\}$  となる. つまり, このような群においては必ず単位元以外に全ての元と可換性を持つ元が存在する.

注意 1. 位数が素数  $p$  の自然数べきであるような群を  $p$  群 ( $p$ -group) という. 例えば, 4 次二面体群  $D_4$  は位数  $8 = 2^3$  なので, 2-群である.

例 3. 4 次二面体群  $D_4$  においては  $Z(D_4) = \{e, \sigma^2\} \neq \{e\}$  となる.

定理 12.4 の証明. 背理法で証明する. もし,  $Z(G) = \{e\}$  となるとすると, 全ての単位元でない  $h \in G$  に対し,

$$K(h) \neq \{h\}$$

となる. なぜなら,  $K(h) = \{h\}$  は, 共役類の定義から任意の  $g \in G$  に対して,  $ghg^{-1} = h$  となることを意味するので, このとき, 任意の  $g \in G$  に対して  $gh = hg$  で,  $h \in Z(G)$  となるためである. よって,  $Z(G) = \{e\}$  のとき全ての単位元でない  $h \in G$  に対し,  $|K(h)| > 1$  である. 一方, (12.1) 直後の考察より, 全ての  $h \in G$  に対し,  $|K(h)|$  は  $|G| = p^k$  の約数である. よって, 全ての単位元でない  $h \in G$  に対し,  $|K(h)|$  は

$$p, p^2, \dots, p^k$$

のいずれかとなる. 特に  $|K(h)|$  の値は  $p$  の倍数となる. よって, ある単位元でない  $h_2, \dots, h_m \in G$  が存在して, 類等式 (12.4) から

$$p^k = |G| = 1 + \sum_{\ell=2}^m |K(h_\ell)| \equiv 1 \pmod{p}$$

となるが, これは矛盾である. 以上より,  $Z(G) \neq \{e\}$  となる. □



## 12.2 ケイリーの定理 (やや発展, 進んで勉強したい方向け)

本節では, 「任意の有限群が実は対称群の部分群として実現できる」というケイリーの定理 (Cayley's theorem) を証明する. まず, 準備として, 群作用の準同型を用いた言い換えについて説明する.

$G$  を群,  $X$  を集合としたとき, 以下の命題 12.5 は,

- $X$  上の  $G$  の作用  $G \times X \rightarrow X$
- 準同型  $G \rightarrow B(X) := \{f: X \rightarrow X \mid f \text{ は全単射}\}$  (群  $B(X)$  については第 4 回講義資料例 1 参照)

の間に一对一の対応が作れるということを述べている.  $X$  上の  $G$  の作用を定めるということは, 準同型  $G \rightarrow B(X)$  を与えることと等価なのである.

\*2 テトリスのブロックのようだが  や  はヤング図形ではない.

\*3 代数学 I 中間試験解答例問題 6 補足解説では  $Z(G)$  が  $G$  の部分群であることのみ証明している. 正規性については, 各自考えよ (証明を見たい方は 2021 年度第 10 回講義資料 p.5 例 7 参照).

**命題 12.5**

$G$  を群,  $X$  を集合とする.

(1)  $G \times X \rightarrow X, (g, x) \mapsto g \cdot x$  を集合  $X$  上の群  $G$  の作用とすると, 各  $g \in G$  に対し, 写像

$$\phi_g: X \rightarrow X, x \mapsto g \cdot x$$

は全単射である. つまり,  $\phi_g \in B(X)$  である. さらに, 写像

$$\phi: G \rightarrow B(X), g \mapsto \phi_g$$

は準同型である.

(2) 逆に, 準同型  $\phi: G \rightarrow B(X)$  が存在するとき, 写像

$$G \times X \rightarrow X, (g, x) \mapsto g \cdot x := \phi(g)(x)$$

は  $X$  上の  $G$  の作用を定める.

**証明.**

(1)  $\phi_g$  の全単射性: 各  $g \in G$  に対し,  $\phi_g$  の逆写像が構成できることを示せばよい. 各  $x \in X$  に対し,

$$(\phi_{g^{-1}} \circ \phi_g)(x) = \phi_{g^{-1}}(\phi_g(x)) = g^{-1} \cdot (g \cdot x) = (g^{-1} \cdot g) \cdot x = e \cdot x = x$$

となる. 全く同様に  $(\phi_g \circ \phi_{g^{-1}})(x) = x$ . よって,

$$\phi_{g^{-1}} \circ \phi_g = \phi_g \circ \phi_{g^{-1}} = \text{id}_X.$$

これより,  $\phi_{g^{-1}}$  が  $\phi_g$  の逆写像であり, 特に  $\phi_g$  は全単射である.

$\phi$  が準同型であること: 任意の  $g_1, g_2 \in G, x \in X$  に対し,

$$\phi(g_1 g_2)(x) = \phi_{g_1 g_2}(x) = (g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x) = \phi_{g_1}(\phi_{g_2}(x)) = (\phi(g_1) \circ \phi(g_2))(x)$$

となるので,  $B(X)$  の元として,  $\phi(g_1 g_2) = \phi(g_1) \circ \phi(g_2)$ . よって,  $\phi$  は準同型である.

(2) 作用の定義条件 (1) を満たすこと:  $e$  を  $G$  の単位元とすると, 任意の  $x \in X$  に対し,

$$e \cdot x = \phi(e)(x) = \text{id}_X(x) = x.$$

ここで,  $\phi(e) = \text{id}_X$  は第 10 回講義資料命題 8.2 (1) と群  $B(X)$  の単位元が  $\text{id}_X$  であることからわかる.

作用の定義条件 (2) を満たすこと: 任意の  $g, h \in G, x \in X$  に対し,

$$\begin{aligned} gh \cdot x &= \phi(gh)(x) = (\phi(g) \circ \phi(h))(x) \quad (\phi \text{ が準同型であることより}) \\ &= \phi(g)(\phi(h)(x)) = g \cdot (h \cdot x). \end{aligned}$$

以上より, (2) の主張で与えられた写像は  $X$  上の  $G$  の作用を定める. □

以下が本節の主題であるケイリーの定理 (Cayley's theorem) である.

**定理 12.6 (ケイリーの定理)**

$G$  が位数  $n$  の有限群であるとき, 単射準同型  $\phi: G \rightarrow \mathfrak{S}_n$  が存在する. つまり, 任意の位数  $n$  の有限群は  $n$  次対称群のある部分群と同型になる.

**証明.** 第 13 回講義資料例 7 で考えた集合  $G$  上の群  $G$  の作用

$$\psi_\ell: G \times G \rightarrow G, (g, h) \mapsto gh$$

を考える. ここで,  $G$  の元に適当に 1 から順に番号を割り振ることで, 集合として  $G$  と  $\{1, 2, \dots, n\}$  を同一視すると, この作用は

$$\psi_\ell: G \times \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$$

と見ることができる。命題 12.5 (1) より、これに対して準同型

$$\phi: G \rightarrow B(\{1, 2, \dots, n\}) = \mathfrak{S}_n$$

が構成できる。これが単射であることを示せばよい。  $g \in \text{Ker } \phi$  とする。このとき、

$$\phi(g) = \text{id}_{\{1, 2, \dots, n\}} = \text{id}_G$$

だが、命題 12.5 (1) における  $\phi$  の構成から、これは任意の  $h \in G$  に対し、

$$h = \phi(g)(h) = \psi_\ell(g, h) = gh$$

となることを主張している。ここで、  $h = e$  ととると ( $e$  は  $G$  の単位元)、

$$e = ge = g$$

となるので、結局  $g = e$  である。よって、  $\text{Ker } \phi = \{e\}$  となり、  $\phi$  は単射である。 □

注意 2 (表現. 進んで勉強したい方向け).  $\mathbb{K}$  を  $\mathbb{Q}, \mathbb{R}$  または  $\mathbb{C}$  とする。  $V$  を  $\mathbb{K}$  上のベクトル空間とし、

$$GL(V) := \{f: V \rightarrow V \mid f \text{ は全単射線形写像}\}$$

とする ( $V$  上の一般線型群と呼ばれる)。このとき、  $GL(V)$  は  $B(V)$  の部分群である (チェックせよ)。また、  $V$  が  $n$  次元ベクトル空間のとき、  $V$  の基底を 1 つ固定すると、  $GL(V)$  は  $GL_n(\mathbb{K})$  と同一視できるのであった (線形代数 II の内容. 線形写像とその表現行列を同一視する)。

このとき、群  $G$  に対し、準同型

$$\rho: G \rightarrow GL(V)$$

を群  $G$  の  $V$  における線形表現 (linear representation) という。これは命題 12.5 で見た群準同型と群作用の対応を頭において見ると、  $G$  の  $V$  上の“線形な”作用  $G \times V \rightarrow V$  を与えているとも言える。

群  $G$  を 1 つ与えたときに、『どのような線形表現が存在するか・どうすれば線形表現を構成できるか』ということを調べる数学の分野を (群の) 表現論 (representation theory) という。表現論は様々な数学的手法 (代数・幾何・解析全て!) を用いて研究されており、数学の枠を超えて物理・化学への応用も持つ非常に大きな分野である。興味を持った方は是非進んで勉強してもらいたい。

1 つ例を挙げておこう。  $n$  次二面体群  $D_n = \{\sigma^k \tau^\ell \mid k = 0, \dots, n-1, \ell = 0, 1\}$  を考える。このとき、準同型

$$\rho: D_n \rightarrow GL_2(\mathbb{R})$$

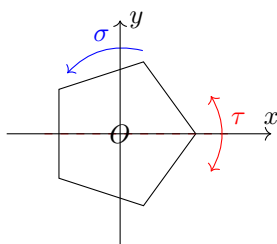
であって、

$$\rho(\sigma) = \begin{pmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{pmatrix} \quad \rho(\tau) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

を満たすものが存在する。これが定める  $\mathbb{R}^2$  上の  $D_n$  の作用は

$$D_n \times \mathbb{R}^2 \rightarrow \mathbb{R}^2, \left( \sigma^k \tau^\ell, \begin{pmatrix} x \\ y \end{pmatrix} \right) \mapsto \rho(\sigma^k \tau^\ell) \begin{pmatrix} x \\ y \end{pmatrix}$$

となる。このとき、  $\sigma$  は  $\mathbb{R}^2$  の原点を中心とする  $2\pi/n$  回転に対応し、  $\tau$  は  $x$  軸に関する線対称変換に対応する。  $n$  次二面体群が正  $n$  角形の対称性であったことを思い出すと、これは自然な作用である。



### 12.3 シローの定理 (発展, 進んで勉強したい方向け)

最後に紹介する定理はシローの定理 (Sylow's theorem) と呼ばれる定理で, 群の分類問題を扱う際に非常に便利になる定理である. この定理も群作用を用いて示される.

#### 定理 12.7 (シローの定理)

$p$  を素数,  $G$  を有限群とし,  $G$  の位数  $|G|$  は  $p^\ell$  では割り切れるが,  $p^{\ell+1}$  では割り切れないとする. (ただし  $\ell$  は正の整数.) このとき, 任意の  $1 \leq k \leq \ell$  に対し,  $G$  は位数  $p^k$  の部分群を持つ.

注意 3. 実はこの定理には続きがあり, 群の分類問題を扱う上ではそこまで知っているより良い. 興味のある方は是非調べてみてほしい. (例えば, 雪江明彦 著 「代数学 1 群論入門」 (日本評論社) の定理 4.5.7 参照.)

注意 4. シローの定理より, 特に  $G$  は位数  $p^\ell$  の部分群をもつことがわかる. これを  $p$ -シロー部分群 ( $p$ -Sylow subgroup) という.

例 4. 6 次二面体群  $D_6 = \{\sigma^k \tau^\ell \mid k = 0, \dots, 5, \ell = 0, 1\}$  は位数  $12 = 2^2 \cdot 3$  の群なので, シローの定理より, 必ず位数  $2, 2^2 = 4, 3$  の部分群をそれぞれ 1 つ以上持つということが言える. 実際, それぞれ

$$\langle \tau \rangle = \{e, \tau\}, \quad \langle \sigma^3, \tau, \sigma^3 \tau \rangle, \quad \langle \sigma^2 \rangle = \{e, \sigma^2, \sigma^4\}$$

が例を与えている.  $\{e, \sigma^3, \tau, \sigma^3 \tau\}$  は  $D_6$  の 2-シロー部分群の例であり,  $\{e, \sigma^2, \sigma^4\}$  は  $D_6$  の 3-シロー部分群の例である (実は 3-シロー部分群はこれしかない).

定理 12.7 の証明. 仮定より,  $G$  の位数は  $p^\ell n$  (ただし,  $p$  と  $n$  は互いに素) という形で書かれる. ここで,  $1 \leq k \leq \ell$  なる  $k$  に対し,

$$X := \{\{g_1, \dots, g_{p^k}\} \subset G \mid g_1, \dots, g_{p^k} \text{ は相異なる } G \text{ の } p^k \text{ 個の元}\}$$

としたとき,

$$G \times X \rightarrow X, \quad (g, \{g_1, \dots, g_{p^k}\}) \mapsto g \cdot \{g_1, \dots, g_{p^k}\} := \{gg_1, \dots, gg_{p^k}\}$$

は  $X$  上の  $G$  の作用を定める (チェックせよ). 各  $\{g_1, \dots, g_{p^k}\} \in X$  の固定部分群は定義より,

$$G_{\{g_1, \dots, g_{p^k}\}} = \{g \in G \mid \{gg_1, \dots, gg_{p^k}\} = \{g_1, \dots, g_{p^k}\}\}$$

である. よって各  $g \in G_{\{g_1, \dots, g_{p^k}\}}$  に対してある  $i \in \{1, \dots, p^k\}$  が定まり,

$$gg_1 = g_i$$

となる. このとき,  $g = g_i g_1^{-1}$  となるので, 結局

$$G_{\{g_1, \dots, g_{p^k}\}} \subset \{g_i g_1^{-1} \mid i = 1, \dots, p^k\}.$$

特に,

$$|G_{\{g_1, \dots, g_{p^k}\}}| \leq p^k$$

である. ここで,  $|G_{\{g_1, \dots, g_{p^k}\}}| = p^k$  となるものが存在することを示せば, 固定部分群  $G_{\{g_1, \dots, g_{p^k}\}}$  が  $G$  の位数  $p^k$  の部分群となり, 示すべきことが示される.

ラグランジュの定理より  $|G_{\{g_1, \dots, g_{p^k}\}}|$  の値は  $|G| = p^\ell n$  の約数なので,  $|G_{\{g_1, \dots, g_{p^k}\}}| < p^k$  とすると特にこれは  $p^{k-1} n$  の約数である. いま各  $\{g_1, \dots, g_{p^k}\} \in X$  に対し, 軌道・固定群定理 (第 13 回講義資料系 11.6) から,

$$|G \cdot \{g_1, \dots, g_{p^k}\}| = \frac{|G|}{|G_{\{g_1, \dots, g_{p^k}\}}|} = \frac{p^\ell n}{|G_{\{g_1, \dots, g_{p^k}\}}|}$$

が成立するので、以上の考察から、 $|G \cdot \{g_1, \dots, g_p\}|$  は

$$\begin{cases} p^{\ell-k+1} \text{の倍数} & (|G_{\{g_1, \dots, g_{p^k}\}}| < p^k \text{のとき}) \\ p^{\ell-k} n & (|G_{\{g_1, \dots, g_{p^k}\}}| = p^k \text{のとき}) \end{cases}$$

となる。これより、もし  $|G_{\{g_1, \dots, g_{p^k}\}}| = p^k$  となる  $\{g_1, \dots, g_{p^k}\} \in X$  が存在しないと仮定すると、 $X$  を軌道分解したときに元の個数が  $p^{\ell-k+1}$  の倍数の軌道で軌道分解されるので、特に  $|X|$  は  $p^{\ell-k+1}$  の倍数となる。今示したかったことは、 $|G_{\{g_1, \dots, g_{p^k}\}}| = p^k$  となるものの存在なので、あとは  $|X|$  が  $p^{\ell-k+1}$  の倍数でないことを示せば良い。

いま、

$$|X| = p^{\ell} n C_{p^k} = \frac{p^{\ell} n (p^{\ell} n - 1) \cdots (p^{\ell} n - p^k + 1)}{p^k (p^k - 1) \cdots 1} = p^{\ell-k} n \cdot \frac{(p^{\ell} n - 1) \cdots (p^{\ell} n - p^k + 1)}{(p^k - 1) \cdots 1} \quad (12.5)$$

である。ここで、 $m \in \mathbb{Z}_{>0}$  に対し、 $\ell(m)$  を

$$m \text{ は } p^{\ell(m)} \text{ で割り切れるが } p^{\ell(m)+1} \text{ では割り切れない}$$

という条件で定まる 0 以上の整数とすると、定義より  $p^{-\ell(m)} m$  は  $p$  で割り切れない整数であり、 $m = 1, 2, \dots, p^k - 1$  のとき  $\ell(m) < k$  である。よって、

$$\begin{aligned} & \frac{(p^{\ell} n - 1) \cdots (p^{\ell} n - p^k + 1)}{(p^k - 1) \cdots 1} \\ &= \frac{(p^{\ell-\ell(1)} n - p^{-\ell(1)} 1) \cdots (p^{\ell-\ell(m)} n - p^{-\ell(m)} m) \cdots (p^{\ell-\ell(p^k-1)} n - p^{-\ell(p^k-1)} (p^k - 1))}{(p^{k-\ell(1)} - p^{-\ell(1)} 1) \cdots (p^{k-\ell(m)} - p^{-\ell(m)} m) \cdots (p^{k-\ell(p^k-1)} - p^{-\ell(p^k-1)} (p^k - 1))}. \end{aligned}$$

ここで、右辺の分子分母の積の各項は整数であることに注意する。このとき、右辺の分子に現れる  $(p^{\ell-\ell(m)} n - p^{-\ell(m)} m)$ 、 $m = 1, \dots, p^k - 1$  という形の整数は  $p^{\ell-\ell(m)} n$  が  $p$  の倍数、 $-p^{-\ell(m)} m$  が  $p$  で割り切れない整数であることより、 $p$  で割り切れない整数である。よって、それらの積である右辺の分子は  $p$  で割り切れず、それをさらに整数で割って得られる数である右辺の値は  $p$  の倍数ではない。

以上より、 $\frac{(p^{\ell} n - 1) \cdots (p^{\ell} n - p^k + 1)}{(p^k - 1) \cdots 1}$  は  $p$  の倍数ではないことが示された。さらに  $p$  と  $n$  は互いに素であることより、(12.5) から、結局  $|X|$  は  $p^{\ell-k+1}$  の倍数ではないことがわかる。よって、示すべきことは全て示された。  $\square$