

# 代数学 I 第 8 回講義資料

担当：大矢 浩徳 (OYA Hironori)\*

## 7.1 剰余類, Lagrange の定理 (後半)

前回の 6.2 節に引き続き,  $G$  を群,  $e \in G$  をその単位元とする. 以下は,  $G$  の部分群による左・右剰余類の基本性質である.

### 命題 7.1

$H$  を  $G$  の部分群とする. このとき, 以下が成立する.

- (1)  $R \subset G$  が  $G$  の  $H$  に関する左完全代表系であることの必要十分条件は,  $\{g^{-1} \mid g \in R\} \subset G$  が  $H$  に関する右完全代表系であることである. 特に,  $|H \setminus G| = |G/H| (= (G:H))$ .<sup>\*1</sup>
- (2) 任意の  $g \in G$  に対し,  $|gH| = |Hg| = |H|$ .

証明.

(1) 写像  $i: G/H \rightarrow H \setminus G$  を

$$gH \mapsto Hg^{-1}$$

と定義する. これは, 実際に well-defined であることが次のようにわかる.<sup>\*2</sup>(well-defined については第 1, 2 回講義資料 p.3 を参照.) :

$gH = g'H \in G/H$  とする. これは  $g \stackrel{H}{\sim}_L g'$  と同値なので, ある  $h \in H$  が存在して,  $g = g'h$ . このとき,

$$Hg^{-1} = H(g'h)^{-1} = Hh^{-1}(g')^{-1} = H(g')^{-1}$$

(最後の等式は,  $h^{-1}(g')^{-1} \stackrel{H}{\sim}_R (g')^{-1}$  を用いて, 右剰余類を表す代表元を取り替えた.) よって,  $i$  は well-defined.

全く同様に,  $i': H \setminus G \rightarrow G/H$  を

$$Hg \mapsto g^{-1}H$$

\* e-mail: hoyashibaura-it.ac.jp

\*1 集合  $S$  に対し,  $|S|$  は  $S$  の元の個数を表す記号であったことを思い出すこと.  $\#S$  と同じ意味である.

\*2 これは well-defined 性をチェックする必要がある. なぜなら,  $g' \in gH$  となる  $g'$  に対して,  $gH = g'H$  が成り立つので (第 7 回講義資料命題 6.3(2)),  $G/H$  は 1 つの元の表し方が何通りもあるような集合の例であるからである. 例えば,  $G = \mathbb{Z}, H = n\mathbb{Z}$  のとき,  $G/H$  が  $\mathbb{Z}/n\mathbb{Z}$  に他ならなかったことを思い出すと (第 7 回講義資料例 8) わかりやすいであろう. ちなみに, 写像  $i': G/H \rightarrow H \setminus G$  を  $gH \mapsto Hg$  としようとするとは well-defined ではない. 例えば, 第 7 回講義資料例 9 の  $G = D_3, H = \{e, \tau\}$  の場合,

$$\begin{aligned} \sigma H &\mapsto H\sigma = \{\sigma, \sigma^2\tau\} \\ &\parallel \quad \neq \\ \sigma\tau H &\mapsto H\sigma\tau = \{\sigma\tau, \sigma^2\}. \end{aligned}$$

となる.

と定義すると、これは well-defined. このとき、 $i$  と  $i'$  は互いに逆写像であり、特に  $i, i'$  は全単射写像である.

$R$  は  $G$  の  $H$  に関する左完全代表系

$$\Leftrightarrow G/H = \{gH \mid g \in R\} \text{ かつ } \llbracket g, g' \in R, g \neq g' \text{ のとき } gH \neq g'H \rrbracket$$

$$\Leftrightarrow H \backslash G = \{Hg^{-1} \mid g \in R\} \text{ かつ } \llbracket g, g' \in R, g \neq g' \text{ のとき } Hg^{-1} \neq H(g')^{-1} \rrbracket \quad (i \text{ と } i' \text{ の全単射性より})$$

$$\Leftrightarrow \{g^{-1} \mid g \in R\} \text{ は } G \text{ の } H \text{ に関する右完全代表系} \quad (7.1)$$

となる. これで前半の主張は示された.

完全代表系の定義より、 $G$  の  $H$  に関する左完全代表系の元の個数は  $G/H$  の元の個数に等しく、 $G$  の  $H$  に関する右完全代表系の元の個数は  $H \backslash G$  の元の個数に等しい. よって、 $R$  を  $G$  の  $H$  に関する左完全代表系とすると、上で示した同値性 (7.1) から、

$$|G/H| = |R| = |\{g^{-1} \mid g \in R\}| = |H \backslash G|.$$

(2 つめの等式は逆元を取る操作が全単射であることから.) 以上より示すべきことは示された.  $\square$

(2) 写像  $j: H \rightarrow gH$  を  $h \mapsto gh$  と定義し、 $j': gH \rightarrow H$  を  $h' \mapsto g^{-1}h'$  と定義する. (写像  $j, j'$  による元への行き先は確かにそれぞれ  $gH, H$  に入っていることに注意.) このとき、 $j$  と  $j'$  は互いに逆写像であり、特に  $j, j'$  は全単射写像である. よって、 $|gH| = |H|$ .  $|Hg| = |H|$  の証明もこれと全く同様である.  $\square$

例 1.  $D_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$  を 3 次二面体群とする ( $\sigma^3 = e, \tau^2 = e, \sigma^k\tau = \tau\sigma^{-k}$  ( $k \in \mathbb{Z}$ )).  $H := \langle \tau \rangle = \{e, \tau\} \subset D_3$  とし、第 7 回講義資料例 9 で行った計算を思い出すと、

$$D_3/H = \{gH \mid g \in D_3\} = \{H, \sigma H, \sigma^2 H\} = \{\{e, \tau\}, \{\sigma, \sigma\tau\}, \{\sigma^2, \sigma^2\tau\}\}$$

$$H \backslash D_3 = \{Hg \mid g \in D_3\} = \{H, H\sigma, H\sigma^2\} = \{\{e, \tau\}, \{\sigma, \sigma^2\tau\}, \{\sigma^2, \sigma\tau\}\}$$

となる. これを見ると、確かに各剰余類の元の個数は全て等しく  $2 (= |H|)$  であることがわかる (命題 7.1(2)). さらに、確かに  $|D_3/H| = 3 = |H \backslash D_3|$  である (命題 7.1(1)).  $D_3$  の  $H$  に関する左完全代表系としては例えば、

$$\{e, \sigma, \sigma^2\} \text{ や } \{\tau, \sigma, \sigma^2\tau\}$$

が取れるが、このとき、

$$\{e^{-1}, \sigma^{-1}, (\sigma^2)^{-1}\} = \{e, \sigma^2, \sigma\} \text{ や } \{\tau^{-1}, \sigma^{-1}, (\sigma^2\tau)^{-1}\} = \{\tau, \sigma^2, \sigma^2\tau\}$$

は確かに、 $D_3$  の  $H$  に関する右完全代表系である (命題 7.1(1)).

次が群論において基本的だが非常に強力な Lagrange の定理である :

**定理 7.2 (Lagrange の定理)**

$G$  を群、 $H$  を  $G$  の部分群とすると、

$$|G| = |G/H| \cdot |H| = |H \backslash G| \cdot |H| = (G : H) \cdot |H|. *3$$

証明. まず  $(G : H) = |G/H|$  は定義そのものであり、 $|G/H| = |H \backslash G|$  は命題 7.1(1) からわかるので、 $|G| = |G/H| \cdot |H|$  のみ示せば十分である.  $R$  を  $G$  の  $H$  に関する左完全代表系とすると、

$$G = \bigcup_{g \in R} gH \text{ かつ } \llbracket g, g' \in R, g \neq g' \text{ のとき } gH \neq g'H \rrbracket$$

であり、さらに命題 7.1(2) より、任意の  $g \in R$  に対して  $|gH| = |H|$  となるので、 $|G| = |R| \cdot |H|$  となる. 完全代表系の定義より、 $G$  の  $H$  に関する左完全代表系の元の個数は  $G/H$  の元の個数に等しいので、結局  $|G| = |G/H| \cdot |H|$  を得る.  $\square$

\*3 この等式は  $|G|, |H|, (G : H)$  の中に  $\infty$  のものがあったとしても成立する. 例えば、 $G$  を無限群とし、 $H$  をその有限部分群とすると、指数  $(G : H)$  は  $\infty$  となる.

例 2. 例 1 の設定では  $|D_3| = 6, |H| = 2, (D_3 : H) = 3$  なので, 確かに

$$|D_3| = (D_3 : H) \cdot |H|$$

が成立している.

Lagrange の定理の応用 : 以下に Lagrange の定理の応用をいくつか述べる.

**系 7.3**

有限群  $G$  に対して, 以下が成立する :

- (1)  $H$  を  $G$  の部分群とすると,  $H$  の位数  $|H|$  は  $|G|$  の約数である. また,  $H$  の  $G$  における指数  $(G : H)$  も  $|G|$  の約数である.
- (2) 任意の  $g \in G$  に対し, その位数  $\text{ord } g$  は  $|G|$  の約数である.
- (3) 任意の  $g \in G$  に対し,  $g^{|G|} = e$ .

証明.

(1) Lagrange の定理より,  $|G| = (G : H) \cdot |H|$  であり, 定義より  $(G : H)$  も  $|H|$  も正の整数なので, (1) の主張が成立する. □

(2)  $g \in G$  の位数  $\text{ord } g$  は  $g$  が生成する  $G$  の部分群  $\langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$  の位数として定義されたので, (1) よりその値は  $|G|$  の約数である. □

(3) (2) より, ある  $k \in \mathbb{Z}_{>0}$  が存在して,  $|G| = k \cdot \text{ord } g$ . ここで, 第 6 回講義資料命題 5.9 より,  $\text{ord } g$  は  $g^{\text{ord } g} = e$  を満たす最小の正の整数だったので,

$$g^{|G|} = g^{k \cdot \text{ord } g} = (g^{\text{ord } g})^k = e^k = e.$$

□

例 3. 第 5 回レポート課題問題 2 で 3 次二面体群  $D_3$  の部分群を全て列挙すると,

$$\{e\}, \{e, \sigma, \sigma^2\}, \{e, \tau\}, \{e, \sigma\tau\}, \{e, \sigma^2\tau\}, D_3$$

であることを計算してもらった (系 7.6 の後の解説も参照のこと). これを見ると, 位数は順に 1, 3, 2, 2, 2, 6 であり, どれも  $|D_3| = 6$  の約数である. また,  $D_3$  の各元の位数を計算してみると,

$$\text{ord } e = 1 \quad \text{ord } \sigma = 3 \quad \text{ord } \sigma^2 = 3 \quad \text{ord } \tau = 2 \quad \text{ord } \sigma\tau = 2 \quad \text{ord } \sigma^2\tau = 2$$

となり, 確かにどれも  $|D_3| = 6$  の約数となっている.

ここで, 第 3 回講義資料で書いたオイラーの定理が (一瞬で!) 証明できる. これは  $n$  が素数  $p$  のときフェルマーの小定理であったことを思い出そう.

**系 7.4 (定理 2.9: オイラーの定理, Euler's theorem)**

$n$  が正の整数,  $a \in \mathbb{Z}, \text{gcd}(a, n) = 1$  のとき,  $\mathbb{Z}/n\mathbb{Z}$  において,

$$[a^{\varphi(n)}]_n = [1]_n.$$

ただし,  $\varphi$  はオイラーの  $\varphi$  関数 (第 3 回講義資料定義 2.6).

証明.  $\text{gcd}(a, n) = 1$  のとき, 第 3 回講義資料命題 2.5 より,  $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$  であった.  $(\mathbb{Z}/n\mathbb{Z})^\times$  は乗法を二項演算 (単位元は  $[1]_n$ ) とする位数  $\varphi(n)$  の群だったので, 系 7.3 (3) より,

$$[a^{\varphi(n)}]_n = [a]_n^{\varphi(n)} = [1]_n.$$

□

例 4.  $n = 8$  のとき,  $\varphi(8) = 4$ . (8 と互いに素な 1 以上 8 以下の数は 1, 3, 5, 7 の 4 つ.) このとき,

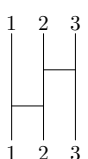
$$[1^4]_8 = [1]_8 \quad [3^4]_8 = [81]_8 = [1]_8 \quad [5^4]_8 = [625]_8 = [1]_8 \quad [7^4]_8 = [2401]_8 = [1]_8.$$

あみだくじと対称群の関係を思い出してもらおうとあみだくじに関する次のような性質もわかる:

**系 7.5**

$n$  本の縦棒があるあみだくじは  $n!$  回同じものをつなげると, どこを選んでも初めに選んだものと同じところに帰ってくるあみだくじとなる.

証明. 与えられたあみだくじは縦棒が  $n$  本なので,  $n$  次対称群のある元  $\sigma \in \mathfrak{S}_n$  に対応する (第 5 回講義資料 p.3 の注意参照). あみだくじの連結は  $\mathfrak{S}_n$  における二項演算に対応したので, 与えられたあみだくじを  $n!$  回つなげてできるあみだくじは  $\sigma^{n!}$  に対応するあみだくじとなる.  $|\mathfrak{S}_n| = n!$  であったので, 系 7.3 (3) より,  $\sigma^{n!} = e$ .  $e$  に対応するあみだくじとはどこを選んでも初めに選んだものと同じところに帰ってくるあみだくじに他ならないので, 系 7.5 は証明された.  $\square$

例 5. 例えば,  というあみだくじは  $3! = 6$  回つなげると 1 は 1 に, 2 は 2 に, 3 は 3 に行くあみだく

じとなる. なお, 実際には 3 回つなげた時点でそうなっている. これは,  $\text{ord} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = 3$  という事実に対応している.

**系 7.6**

位数が素数  $p$  の群  $G$  は必ず非自明な部分群を持たない巡回群となる.

証明.  $H$  を  $G$  の部分群とすると, 系 7.3 (1) より,  $|H|$  は  $|G| = p$  の約数であるが,  $p$  は素数なので,  $|H| = 1$  または  $|H| = p$ . ここで,  $|H| = 1$  のとき,  $H = \{e\}$  であり,  $|H| = p$  のとき,  $H = G$  となるので, どちらも自明である. よって,  $G$  は非自明な部分群をもたない. さらに,  $g \in G$  を  $G$  の単位元でない元とすると,  $g$  の生成する  $G$  の部分群  $\langle g \rangle$  は少なくとも単位元  $e$  と  $g$  を含むことから, 位数は 1 ではないので  $|\langle g \rangle| = p$  となる. これより,  $G = \langle g \rangle$  で  $G$  は巡回群.  $\square$

以上の知識を用いると例えば, 次のような問題は今までよりもかなり楽に解けるようになる.

**例題: 第 5 回レポート課題問題 2**

3 次二面体群  $D_3$  の部分群を全て列挙せよ.

解答例. まず,  $|D_3| = 6$  なので, 系 7.3 (1) より,  $D_3$  の部分群の位数は 1, 2, 3, 6 のいずれかである. さらに, 位数 1 の部分群は  $\{e\}$ , 位数 6 の部分群は  $D_3$  という自明なものに限られるので, 非自明な部分群の位数は 2 か 3 である. ここで, 2 と 3 は素数なので, 系 7.6 よりこれらは巡回群である. よって, 非自明な部分群は  $D_3$  の (単位元でない) 1 元で生成される部分群に限られる. これらを具体的に計算してみると,

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

以上より, 求める部分群は,

$$\{e\}, \{e, \sigma, \sigma^2\}, \{e, \tau\}, \{e, \sigma\tau\}, \{e, \sigma^2\tau\}, D_3$$

で全て.  $\square$