代数学 I 第 9 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

今回は前回少し予告をしたラグランジュの定理 (Lagrange's theorem) の証明を行う．これは一般の群において成り立つ定理で，群論における基本定理の 1 つである．証明に必要なことは前回考えた左・右剰余類の考え方のみで，証明自体は込み入っていないのであるが，そこから導かれる帰結は強力である．今回の講義資料でも応用の一部を紹介した．この定理は今後群の構造を調べる際に常に頭に入れておいてほしい定理であり，今回の講義でしっかり学んでほしい．

8.1 ラグランジュの定理

本節では G を群，$e \in G$ をその単位元とする．また，G の部分群 H に対し，以下 $H\backslash G$ と書くと常に「H に関する右合同の同値関係による G の商集合」を表すことにする．差集合でよく使われる記号と同じ記号になってしまうが，意味は異なるので注意してほしい．以下は今回重要になる G の部分群による左・右剰余類の基本性質である．

命題 8.1

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，$|H\backslash G| = |G/H| (= (G : H))$.*1

(2) 任意の $g \in G$ に対し，$|gH| = |Hg| = |H|$.

証明.

(1) 写像 $i\colon G/H \to H\backslash G$ を

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

と定義する．これは well-defined であることが次のようにわかる*2(well-defined については第 3 回講義資料を参照)．$gH = g'H \in G/H$ とする．これは第 8 回講義資料命題 7.3 より $g \overset{H}{\sim}_L g'$ と同値で，ある $h \in H$ が存在して，$g = g'h$．このとき，

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

なお，最後の等式は，$h^{-1}(g')^{-1} \overset{H}{\sim}_R (g')^{-1}$ 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.

---

* *e-mail* : hoya@shibaura-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る．$\#S$ 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 8 回講義資料命題 7.3 (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 8 回講義資料例 8) わかりやすいであろう．ちなみに，写像 $i'\colon G/H \to H\backslash G$ を $gH \mapsto Hg$ と定義しようとするとこれは well-definedではない．例えば，第 8 回講義資料例 9 の $G = D_3, H = \{e, \tau\}$ の場合，

$$\begin{array}{ccc} \sigma H & \mapsto & H\sigma = \{\sigma, \sigma^2\tau\} \\ \| & \not\mapsto & \\ \sigma\tau H & \mapsto & H\sigma\tau = \{\sigma\tau, \sigma^2\} \end{array}$$

となる．

全く同様に，$i' \colon H\backslash G \to G/H$ を

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

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．このとき，以下の同値関係が成立する．ここで，2 つめの同値関係の $\Rightarrow$ 方向は全単射写像 i を用いることでわかり，$\Leftarrow$ 方向は全単射写像 i' を用いることでわかる[*3]．

$$\begin{aligned}
&R \text{ は } G \text{ の } H \text{ に関する左完全代表系} \\
&\Leftrightarrow G/H = \{gH \mid g \in R\} \text{ かつ『} g, g' \in R, g \neq g' \text{のとき } gH \neq g'H \text{』} \\
&\Leftrightarrow H\backslash G = \{Hg^{-1} \mid g \in R\} \text{ かつ『} g, g' \in R, g \neq g' \text{のとき } Hg^{-1} \neq H(g')^{-1} \text{』} \\
&\Leftrightarrow \{g^{-1} \mid g \in R\} \text{ は } G \text{ の } H \text{ に関する右完全代表系}
\end{aligned} \tag{8.1}$$

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 (8.1) から，

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

なお，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わかる．以上より示すべきことは示された．

(2) 写像 $j \colon H \to gH$ を

$$h \mapsto gh$$

と定義し，写像 $j' \colon gH \to H$ を

$$k \mapsto g^{-1}k$$

と定義する．(写像 j, j' による元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． □

注意 1. 命題 8.1 の主張の中に元の個数に関する等式があるが，証明からもわかるようにこれらは有限の値である必要はない．例えば，$(G : H) = \infty$ のとき，$|H\backslash G| = |G/H| = \infty$ となり，$|H| = \infty$ のとき，任意の $g \in G$ に対し，$|gH| = |Hg| = |H| = \infty$ となる．

例 1. $D_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ を 3 次二面体群とする $(\sigma^3 = e, \tau^2 = e, \sigma^k\tau = \tau\sigma^{-k}\ (k \in \mathbb{Z}))$.

$$H \coloneqq \langle \tau \rangle = \{e, \tau\} \subset D_3$$

とし，第 8 回講義資料例 9 で行った計算を思い出すと，

$$\begin{aligned}
D_3/H &= \{gH \mid g \in D_3\} = \{H, \sigma H, \sigma^2 H\} = \{\{e, \tau\}, \{\sigma, \sigma\tau\}, \{\sigma^2, \sigma^2\tau\}\} \\
H\backslash D_3 &= \{Hg \mid g \in D_3\} = \{H, H\sigma, H\sigma^2\} = \{\{e, \tau\}, \{\sigma, \sigma^2\tau\}, \{\sigma^2, \sigma\tau\}\}
\end{aligned}$$

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

$$|H| = 2$$

[*3] この部分は難しいかもしれないので補足で解説しておこう．$G/H = \{gH \mid g \in R\}$ が成り立っているとき，i の全射性より，

$$H\backslash G = i(G/H) = \{i(gH) \mid g \in R\} = \{Hg^{-1} \mid g \in R\}$$

となる．さらに i の単射性より，$gH \neq g'H$ のとき，

$$Hg^{-1} = i(gH) \neq i(g'H) = H(g')^{-1}$$

となるため，『$g, g' \in R, g \neq g'$ のとき $gH \neq g'H$』が成り立っているならば，『$g, g' \in R, g \neq g'$ のとき $Hg^{-1} \neq H(g')^{-1}$』も成り立つ．これらより，$\Rightarrow$ 方向がわかる．逆に $\Leftarrow$ 方向は i' を用いることで同様の議論から示すことができる．

であることがわかる (命題 8.1 (2))．さらに，確かに

$$|D_3/H| = 3 = |H\backslash D_3|$$

である (命題 8.1 (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 8.1 (1))．

次が今回のメインであるラグランジュの定理である[*4]．

定理 8.2

G を群，H を G の部分群とすると，

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

注意 2. ラグランジュの定理は $|G|, |H|, (G : H)$ の中に ∞ のものがあっても成立する．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，

$$(G : H) = |G|/|H| = \infty$$

となる．

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 8.1 (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，

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

である (つまり集合 G が gH という形の部分集合で “クラス分け” されており，“クラス名の集合” が R であるという状況)．さらに命題 8.1 (2) より，任意の $g \in R$ に対して $|gH| = |H|$ となる (つまり全ての “クラス” の要素の数が等しい) 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 R は G/H の元の個数に等しいので，ここから

$$|G| = |G/H| \cdot |H|$$

を得る． □

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．

[*4] Joseph-Louis Lagrange (1736–1813) が定理 8.2 に対応する定理を述べた時代 (1770 年頃) は，まだこの講義で勉強しているような群の一般的な概念は整備されていなかった．このため，Lagrange が実際に述べたのは多項式とその変数の入れ替えで得られる新たな多項式の数に関する定理である (Lagrange は多項式の根の代数的な公式を求める研究を行っていた)．これは今の見方では n 次対称群 $\mathfrak{S}_n$ に関する上の定理に対応していると考えられる．英語の文献であるが，このあたりの歴史については，例えば R.Roth, “A History of Lagrange’s Theorem on Groups”, Mathematics Magazine, **74** no.2 (2001): 99–108 に詳しい．

8.2 ラグランジュの定理の応用

以下にラグランジュの定理の応用をいくつか述べる．まずは部分群の位数，群の元の位数に関する有用な性質をラグランジュの定理から導く．

系 8.3

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 の位数 $|G|$ 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 $\operatorname{ord} g$ は $|G|$ の約数である．
(3) 任意の $g \in G$ に対し，$g^{|G|} = e$.

証明.
(1) ラグランジュの定理より，$|G| = (G:H) \cdot |H|$．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 $\operatorname{ord} g$ 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，$|G| = k \cdot \operatorname{ord} g$．ここで，第 7 回講義資料命題 6.8 より，$\operatorname{ord} g$ は $g^m = e$ を満たす最小の正の整数 m だったので，

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

□

例 3. 第 5 回本レポート課題問題 1 で 3 次対称群 $\mathfrak{S}_3$ の部分群を全て列挙すると，

$$\{e\},\ \{e, (1\ 2)\},\ \{e, (2\ 3)\},\ \{e, (1\ 3)\},\ \{e, (1\ 2\ 3), (1\ 3\ 2)\},\ \mathfrak{S}_3$$

であることを計算してもらった (巡回置換を用いて各元を書き直した)．これを見ると，位数は順に $1, 2, 2, 2, 3, 6$ であり，どれも $|\mathfrak{S}_3| = 6$ の約数である．また，$\mathfrak{S}_3$ の各元の位数を計算してみると，

$$\operatorname{ord} e = 1, \qquad \operatorname{ord}(1\ 2) = \operatorname{ord}(1\ 3) = \operatorname{ord}(2\ 3) = 2, \qquad \operatorname{ord}(1\ 2\ 3) = \operatorname{ord}(1\ 3\ 2) = 3$$

となり，確かにどれも $|\mathfrak{S}_3| = 6$ の約数となっている．

上で示した系 8.3 (3) を用いると第 4 回講義資料定理 3.9 で紹介し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を再現するような，フェルマーの小定理の一般化であったことも思い出そう．

定理 3.9：オイラーの定理 (再掲)

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

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

ただし，φ はオイラーの φ 関数 (第 4 回講義資料定義 3.5).

証明. $\gcd(a, n) = 1$ のとき，第 4 回講義資料命題 3.4 より，$[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$．$(\mathbb{Z}/n\mathbb{Z})^\times$ は $\times$ を二項演算とする群 (単位元は $[1]_n$) であり，第 4 回講義資料命題 3.6 よりその位数は $\varphi(n)$ であったので，系 8.3 (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，

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

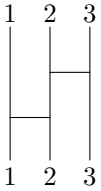
次に，あみだくじと対称群の関係を思い出すとあみだくじに関係する次のような面白い性質もわかる．

系 8.4

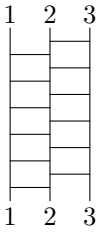
n 本の縦棒があるあみだくじは $n!$ 回同じものをつなげると，どの縦棒を選んでも必ず初めに選んだ縦棒に帰ってくるあみだくじとなる．

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 4.2 節)．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 $n!$ 回つなげて得られるあみだくじは $\sigma^{n!}$ に対応するあみだくじとなる．$|\mathfrak{S}_n| = n!$ であったので，系 8.3 (3) より，$\sigma^{n!} = e$．e に対応するあみだくじとはどの縦棒を選んでも必ず初めに選んだ縦棒に帰ってくるあみだくじに他ならないので，系 8.4 は示された． □

例 5.



というあみだくじは $3! = 6$ 回つなげると



となり，これは確かに 1 は 1 に，2 は 2 に，3 は 3 に行くあみだくじである．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，$\mathrm{ord}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = 3$ という事実に対応している．

次は位数が素数の群の構造についてである．今後の講義で “群の同型” という概念を学ぶが，以下の系は位数が素数の群は同型の差を除いて一通りしかないということを主張している (詳しくは先の講義で！)．

系 8.5

位数が素数 p の群 G は非自明な部分群を持たない．さらに，G は必ず巡回群となる．

証明. H を G の部分群とすると，系 8.3 (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 $|H| = p$ である．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 は巡回群である． □

以上の結果を用いると，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 回本レポート課題問題 1

3 次対称群 $\mathfrak{S}_3$ の部分群を全て求めよ．

解答例. $|\mathfrak{S}_3| = 6$ なので，系 8.3 (1) より，$\mathfrak{S}_3$ 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 $\mathfrak{S}_3$ 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 8.5 よりこれらは巡回群である．よって，非自明な部分群は $\mathfrak{S}_3$ 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，

$$\langle(1\ 2)\rangle = \{e, (1\ 2)\},\ \langle(2\ 3)\rangle = \{e, (2\ 3)\},\ \langle(1\ 3)\rangle = \{e, (1\ 3)\},\ \langle(1\ 2\ 3)\rangle = \langle(1\ 3\ 2)\rangle = \{e, (1\ 2\ 3), (1\ 3\ 2)\}.$$

以上より，$\mathfrak{S}_3$ の部分群は，

$$\{e\},\ \{e, (1\ 2)\},\ \{e, (2\ 3)\},\ \{e, (1\ 3)\},\ \{e, (1\ 2\ 3), (1\ 3\ 2)\},\ \mathfrak{S}_3$$

で全てである． □

例題：第 6 回本レポート課題問題 1

4 次二面体群

$$D_4 = \{e, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$$

の部分群を全て求めよ．ここで，σ, τ は第 6 回講義資料 5.2 節のものを指すこととする．

解答例. $|D_4| = 8$ なので，系 8.3 (1) より，D_4 の部分群の位数は $1, 2, 4, 8$ のいずれかである．さらに，位数 1 の部分群は $\{e\}$，位数 8 の部分群は D_4 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 4 である．2 は素数なので，系 8.5 より位数 2 の部分群は巡回群である．単位元以外の元の位数を計算してみると，

$$\operatorname{ord}\sigma = 4,\ \operatorname{ord}\sigma^2 = 2,\ \operatorname{ord}\sigma^3 = 4,\ \operatorname{ord}\tau = 2,\ \operatorname{ord}\sigma\tau = 2,\ \operatorname{ord}\sigma^2\tau = 2,\ \operatorname{ord}\sigma^3\tau = 2$$

となるので，位数 2 の部分群は

$$\{e, \sigma^2\},\ \{e, \tau\},\ \{e, \sigma\tau\},\ \{e, \sigma^2\tau\},\ \{e, \sigma^3\tau\}$$

で全てである．

次に，位数 4 の部分群 H を考える．

(i) $\sigma^2 \in H$ のとき．$Z := \{e, \sigma^2\} = \langle\sigma^2\rangle$ は H の部分群である．ここでラグランジュの定理より，

$$4 = |H| = (H : Z) \cdot |Z| = 2(H : Z)$$

となるので，$(H : Z) = 2$ である．よって，命題 8.1 より，ある $h \in H$ が存在して H は

$$H = Z \cup Zh$$

と 2 つの右剰余類に分解される．ここで，D_4 を Z による右剰余類に分解すると，

$$D_4 = Z \cup Z\sigma \cup Z\tau \cup Z\sigma\tau = \{e, \sigma^2\} \cup \{\sigma, \sigma^3\} \cup \{\tau, \sigma^2\tau\} \cup \{\sigma\tau, \sigma^3\tau\}$$

となるので，Zh は $Z\sigma, Z\tau, Z\sigma\tau$ のいずれかである．ここで，

$$Z \cup Z\sigma = \{e, \sigma, \sigma^2, \sigma^3\}$$
$$Z \cup Z\tau = \{e, \sigma^2, \tau, \sigma^2\tau\}$$
$$Z \cup Z\sigma\tau = \{e, \sigma^2, \sigma\tau, \sigma^3\tau\}$$

のいずれも二項演算と逆元を取る操作で閉じることが直接計算で確かめられるので，これらは全て H の候補である．

(ii) $\sigma^2 \notin H$ のとき．$\sigma \in H$ または $\sigma^3 \in H$ であれば，それぞれ $\sigma^2 \in H$ または $(\sigma^3)^2 = \sigma^6 = \sigma^2 \in H$ となるので，$\sigma^2 \notin H$ に矛盾する．よって，このとき $\sigma, \sigma^2, \sigma^3 \notin H$ である．これより，H の位数を 4 とするためには H の中に $0 \leq \ell < k \leq 3$ となる $\sigma^k\tau, \sigma^\ell\tau$ が含まれることとなる．このとき，

$$\sigma^k\tau\sigma^\ell\tau = \sigma^k\sigma^{-\ell}\tau\tau = \sigma^{k-\ell} \in H$$

となるが，$\sigma^{k-\ell}$ は $\sigma, \sigma^2, \sigma^3$ のいずれかなので，$\sigma, \sigma^2, \sigma^3 \notin H$ に矛盾する．よって，$\sigma^2 \notin H$ を満たす位数 4 の部分群 H は存在しない．

以上より，D_4 の部分群は，

$$\{e\},\ \{e,\sigma^2\},\ \{e,\tau\},\ \{e,\sigma\tau\},\ \{e,\sigma^2\tau\},\ \{e,\sigma^3\tau\},\ \{e,\sigma,\sigma^2,\sigma^3\},\ \{e,\sigma^2,\tau,\sigma^2\tau\},\ \{e,\sigma^2,\sigma\tau,\sigma^3\tau\},\ D_4$$

で全てである．□