代数学 I 第 9 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

今回の資料の前半ではいよいよ群論における基本定理の 1 つであるラグランジュの定理 (Lagrange's theorem) の証明を行う．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．

また，後半では群 G が良い性質を持つ部分群 H を持つとき，そこから考えられる商集合 G/H が再び群の構造を自然に持つ (剰余群と呼ばれる) ということを解説する．例えば，加法群 $\mathbb{Z}$ とその部分群 $n\mathbb{Z}$ を考えると，商集合 $\mathbb{Z}/n\mathbb{Z}$ が再び $+$ という二項演算によって群になっていたということを思い出してほしい．この良い性質を持つ部分群 H は正規部分群と呼ばれるもので，群の構造を調べる上で大事である．これを用いれば，例えば G の正規部分群 H と剰余群 G/H の群構造をそれぞれ調べることで G の群構造を調べるといったようなことができるようになる．

7.1 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

$$H \text{ に関する右合同 } \overset{H}{\sim}_R \text{ の同値関係による } G \text{ の商集合}$$

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 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，$R^{-1} \coloneqq \{g^{-1} \mid g \in R\} \subset G$ 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) G において逆元を取る写像を $i\colon G \to G, g \mapsto g$ と書く．$i \circ i = \mathrm{id}_G$ なので，i は全単射写像であることに注意する．このとき，各 $g \in G$ に対し，

$$\begin{aligned} i(gH) &= \{i(gh) \mid h \in H\} \\ &= \{(gh)^{-1} \mid h \in H\} \\ &= \{h^{-1}g^{-1} \mid h \in H\} \\ &= \{hg^{-1} \mid h \in H\} \quad (h \text{ が } H \text{ の元全体をわたるとき，} h^{-1} \text{も } H \text{ の元全体をわたるので}) \\ &= Hg^{-1} \end{aligned}$$

* *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．

となる．ここで，$R \subset G$ を H に関する左完全代表系とすると，G は

$$G = \coprod_{g \in R} gH$$

というように分割されるが[*2]，ここに全単射写像 i を施すと，上で示した等式より，

$$G = \coprod_{g \in R} i(gH) = \coprod_{g \in R} Hg^{-1} = \coprod_{g' \in R^{-1}} Hg'$$

となる．右辺は G の H による右剰余類による分割を与えており，R^{-1} がそこに現れる全ての右剰余類からちょうど 1 つずつ元を取ってきたものになっているという状況を示している．これより，右完全代表系の定義から R^{-1} は G の H に関する右完全代表系となる．逆に R^{-1} が G の H に関する右完全代表系であるとき，R が G の H に関する左完全代表系となるということも上の議論を逆にたどることによりわかる．よって，前半の主張は示された．

さらに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，

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

なお，2 つめの等式は i 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 に入っているということに注意．) このとき，j と j' は互いに逆写像であるので，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 7.1 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．(n 次二面体群の元の記号は第 5 回講義資料と同じものを用いる．以下も同様．)

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

とし，第 8 回講義資料例 9 で行った計算を思い出すと，

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

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

$$|H| = 2$$

であることがわかる (命題 7.1 (2))．さらに，

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

[*2] $\coprod$ は非交和 (交わりを持たない和) を表す記号．すなわち，$G = \coprod_{g \in R} gH$ とは，$G = \bigcup_{g \in R} gH$ であって，かつ $g, g' \in R, g \neq g'$ であれば $gH \cap g'H = \varnothing$ となっているということ．これは G が「クラス分け」されている (各「クラス」が gH) という状態に他ならない．

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,

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

が取れるが, このとき,

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

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)).

次が今回前半のメインであるラグランジュの定理である[*3].

定理 7.2

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 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 は

$$G = \coprod_{g \in R} gH$$

というように分割されるので,

$$|G| = \sum_{g \in R} |gH|$$

であるが, 命題 7.1 (2) より, 任意の $g \in R$ に対して $|gH| = |H|$ となるので,

$$|G| = |R| \cdot |H|.$$

完全代表系の定義より, R の元の個数は G/H の元の個数に等しいので, 結局

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

□

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.

[*3] Joseph-Louis Lagrange (1736–1813) が定理 7.2 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.

7.2 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 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，主張は示された．
(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 6 回講義資料命題 5.5 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，

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

□

上で示した系 7.3 (3) を用いると補足資料「フェルマーの小定理について」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．

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，$\mathbb{Z}/n\mathbb{Z}$ において，

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

ただし，φ はオイラーの φ 関数 (第 3 回講義資料定義 2.10).

証明. $\gcd(a,n) = 1$ のとき，第 3 回講義資料命題 2.9 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 3 回講義資料命題 2.11 よりその位数は $\varphi(n)$ であったので，系 7.3 (3) より，

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

□

例 3. $n = 8$ 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，

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

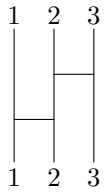
次に，あみだくじと対称群の関係を思い出すとあみだくじに関係する次のような面白い性質もわかる．

系 7.4

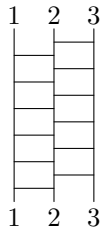
n 本の縦棒があるあみだくじは $n!$ 回同じものをつなげると，どの縦棒を選んでも必ず初めに選んだ縦棒に帰ってくるあみだくじとなる．

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 4 回講義資料 3.2 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 7.3 (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，主張は示された． □

例 4.



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 7.5

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 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 $|H| = p$ 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かなり楽に解けるようになる．

例題：代数学 I 中間試験 Extra 問題 (2)

3 次二面体群 D_3 の部分群を全て求めよ．

解答例. $|D_3| = 6$ 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 7.5 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，

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

以上より，D_3 の部分群は，

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

で全てである． □

7.3 正規部分群，剰余群

群 G とその部分群 H があったとき，そこから商集合 G/H を考えることができた．この G/H は左剰余類からなる単なる集合であって一般には何の構造も持っていないが，本節では G/H が再び自然に群構造を持つという状況を考える．このためには H が正規部分群という良い性質を持つ部分群であれば良い．例えば，加法群 $\mathbb{Z}$ とその部分群 $n\mathbb{Z}$ を考えると，商集合 $\mathbb{Z}/n\mathbb{Z}$ は再び $+$ という二項演算によって群になっていたということを思い出そう (第 8 回講義資料例 8)．本節で解説するのはこの状況の一般化である．

定義 7.6

H を G の部分群とする．任意の $g \in G$ に対して，

$$gHg^{-1} \coloneqq \{ghg^{-1} \mid h \in H\} \subset H$$

が成立するとき，H を G の**正規部分群 (normal subgroup)** という．

注意 3. H が正規部分群のとき，任意の $g \in G$ に対して，$g^{-1}Hg = g^{-1}H(g^{-1})^{-1} \subset H$ なので，任意の $g \in G$ に対し，

$$H = \{gg^{-1}hgg^{-1} \mid h \in H\} = \{gh'g^{-1} \mid h' \in g^{-1}Hg\} \subset \{ghg^{-1} \mid h \in H\} = gHg^{-1} \subset H.$$

よって，実はこのとき任意の $g \in G$ に対し，$gHg^{-1} = H$ である．

例 5. G を可換群，H をその部分群とすると，任意の $g \in G$ に対し，

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\} = \{hgg^{-1} \mid h \in H\} = \{h \mid h \in H\} = H$$

が成立するので，H は正規部分群である．つまり，可換群の任意の部分群は正規部分群である．

例 6. 3 次二面体群 D_3 とその部分群 $H \coloneqq \langle \tau \rangle = \{e, \tau\}$ を考える．このとき，$\sigma \in D_3, \tau \in H$ に対し，

$$\sigma H \sigma^{-1} \ni \sigma\tau\sigma^{-1} = \sigma^2\tau \notin H$$

となるので，$\sigma H \sigma^{-1} \not\subset H$ であるから，H は正規部分群ではない.

一方，

$$N \coloneqq \langle \sigma \rangle = \{e, \sigma, \sigma^2\}$$

とすると，任意の $\sigma^k, \sigma^k\tau \in D_3, \sigma^\ell \in N$ $(k, \ell \in \mathbb{Z})$ に対し，

$$\sigma^k\sigma^\ell(\sigma^k)^{-1} = \sigma^\ell \in N \qquad\qquad \sigma^k\tau\sigma^\ell(\sigma^k\tau)^{-1} = \sigma^{-\ell} \in N$$

となる．よって，任意の $g \in D_3$ に対して，

$$gNg^{-1} \subset N$$

なので，N は D_3 の正規部分群である．

例 7. n を正の整数とし，$\mathbb{K}$ を $\mathbb{Q}, \mathbb{R}$ または $\mathbb{C}$ とする．一般線型群

$$GL_n(\mathbb{K}) \coloneqq \{A \mid A \text{ は } \mathbb{K} \text{ の元を成分とする } n \times n \text{ 行列で, } \det A \neq 0\}$$

を考える．(第 1,2 回講義資料例 5 参照．二項演算は行列の積であった．) このとき，特殊線形群

$$SL_n(\mathbb{K}) = \{A \in GL_n(\mathbb{K}) | \det A = 1\}$$

は $GL_n(\mathbb{K})$ の正規部分群である．部分群であることの確認は第 1,2 回講義資料例 5 で既に行っているので，ここでは正規部分群であることを確認しよう．正規部分群の定義より，

$$\text{任意の } A \in GL_n(\mathbb{K}) \text{ と } X \in SL_n(\mathbb{K}) \text{ に対して, } AXA^{-1} \in SL_n(\mathbb{K})$$

となることを示せばよい．行列式が $A, B \in GL_n(\mathbb{K})$ に対して，

$$\det(AB) = \det(A)\det(B), \qquad \det(A^{-1}) = \frac{1}{\det(A)}$$

という性質を満たしたことを思い出すと，

$$\begin{aligned}\det(AXA^{-1}) &= \det(A)\det(X)\det(A^{-1}) = \det(A)\det(A^{-1}) \quad (X \in SL_n(\mathbb{K}) \text{ なので}) \\ &= \det(A) \cdot \frac{1}{\det(A)} = 1\end{aligned}$$

となる．よって，$AXA^{-1} \in SL_n(\mathbb{K})$ であり，$SL_n(\mathbb{K})$ は確かに $GL_n(\mathbb{K})$ の正規部分群であることがわかる．

それでは今回の講義資料の後半のメインの主張を示そう．

定理 7.7

G を群，N を G の正規部分群とすると，二項演算

$$\cdot : G/N \times G/N \to G/N,\ (gN, hN) \mapsto gN \cdot hN \coloneqq ghN$$

が well-defined であり，これによって G/N が再び群となる．

定義 7.8

定理 7.7 の方法で作られる群 G/N を G の N による**剰余群 (quotient group)** という．

定理 7.7 の証明. まず，二項演算の well-defined 性をチェックする．このためには，

$$gN = g'N,\ hN = h'N \text{ としたとき，} ghN = g'h'N$$

となることを示せばよい．$gN = g'N,\ hN = h'N$ のとき，ある $n_1, n_2 \in N$ が存在して，

$$g = g'n_1,\ h = h'n_2$$

となる．このとき，

$$gh = g'n_1h'n_2 = g'h'(h')^{-1}n_1h'n_2 \tag{7.1}$$

となるが，いま N は正規部分群なので $(h')^{-1}n_1h' \in N$ である[*4]．さらに N は二項演算で閉じていることより，

$$((h')^{-1}n_1h')n_2 \in N.$$

よって，(7.1) は $gh \overset{N}{\sim}_L g'h'$ であるということを示している (第 8 回講義資料定義 6.4 参照)．よって，$ghN = g'h'N$.

次に，この二項演算が群の二項演算の 3 性質を満たしていることを確かめる．

(I) (結合法則) 任意の $gN, hN, kN \in G/N$ に対し，

$$(gN \cdot hN) \cdot kN = ghN \cdot kN = (gh)kN = g(hk)N = gN \cdot hkN = gN \cdot (hN \cdot kN)$$

(群 G の二項演算が結合法則を満たしていることを用いた．)

(II) (単位元の存在) 単位元は $eN = N \in G/N$ である．実際，任意の $gN \in G/N$ に対し，

$$eN \cdot gN = egN = gN = geN = gN \cdot eN$$

が成立する．

[*4] 定義と -1 の付き方が逆だと思うかもしれないが，$(h')^{-1}n_1h' = (h')^{-1}n_1((h')^{-1})^{-1}$ と見れば良い．

(III) (逆元の存在) 各 $gN \in G/N$ に対し，$g^{-1}N$ を考えると，これは

$$gN \cdot g^{-1}N = gg^{-1}N = eN = g^{-1}gN = g^{-1}N \cdot gN$$

を満たしている．よって，$(gN)^{-1} = g^{-1}N$ である．

以上より，示すべきことは示された． □

例 8. n を正の整数とする．加法群 $\mathbb{Z}$ と n の倍数全体からなる部分群

$$n\mathbb{Z} \coloneqq \langle n \rangle = \{nk \mid k \in \mathbb{Z}\}$$

を考える．$\mathbb{Z}$ は可換群なので，その部分群 $n\mathbb{Z}$ は正規部分群である．これにより，定理 7.7 から剰余群 $\mathbb{Z}/n\mathbb{Z}$ が構成できる．これは集合としては，

$$\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$$

であったことを思い出そう (第 8 回講義資料例 8)．このとき，$\mathbb{Z}/n\mathbb{Z}$ の二項演算は定理 7.7 から，

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = a + b + n\mathbb{Z}$$

で定義される．剰余類 $a + n\mathbb{Z}$ を $[a]_n$ と書くと，これは今まで学んできた群 $(\mathbb{Z}/n\mathbb{Z}, +)$ に他ならない！ $\mathbb{Z}/n\mathbb{Z}$ という記号を使っていたのはこの考え方によるものだったのである．

なお，$n\mathbb{Z}$ は加法群 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ らの部分群でもあるので，剰余群 $(\mathbb{Q}/n\mathbb{Z}, +), (\mathbb{R}/n\mathbb{Z}, +), (\mathbb{C}/n\mathbb{Z}, +)$ も同様に定義することができる[*5]．

例 9. 例 6 の状況を考えよう．3 次二面体群 D_3 とその正規部分群 $N \coloneqq \langle \sigma \rangle = \{e, \sigma, \sigma^2\}$ に対し，

$$D_3 = N \cup \tau N$$

であったので，

$$D_3/N = \{gN \mid g \in D_3\} = \{N, \tau N\}$$

となる．このとき，剰余群 D_3/N の乗積表は定理 7.7 から，

	N	τN
N	N	τN
τN	τN	$\tau^2 N = N$

となる．

正規部分群の定義条件の剰余類の性質を用いた言い換え

群 G とその部分群 H に対し，$g \in G$ の H による左剰余類 gH と右剰余類 Hg は一般には異なっていた．実は H が正規部分群であるという条件はこれらが全て一致するような部分群であるということに他ならない．この同値性を示そう．

命題 7.9

H を G の部分群とする．このとき，以下の (1), (2), (3) は同値である．

(1) H は正規部分群である．

(2) 任意の $g \in G$ に対して，$gH = Hg$ である．

証明.

[*5] 第 3 回講義資料 p.2 の well-defined 性のところで，$(\mathbb{Z}/n\mathbb{Z}, +)$ は $(\mathbb{Q}/n\mathbb{Z}, +)$ に拡張できるという話題があったことも合わせて思い出そう．

(1) ⇒ (2) 正規部分群の定義より，任意の $g \in G$ と $h \in H$ に対して，$ghg^{-1}, g^{-1}hg \in H$ なので，

$$gh = (ghg^{-1})g \in Hg, \qquad hg = g(g^{-1}hg) \in gH.$$

よって，$gH \subset Hg$ かつ $Hg \subset gH$ である．よって，任意の $g \in G$ に対して，$gH = Hg$.

(2) ⇒ (1) 任意の $g \in G$ と $h \in H$ に対し，

$$gh \in gH = Hg$$

なので，ある $h' \in H$ が存在して，$gh = h'g$．よって，$ghg^{-1} = h'gg^{-1} = h' \in H$ である．よって，任意の $g \in G$ に対し，$gHg^{-1} \subset H$. □

この同値性をふまえれば，$H = \{e, \tau\}$ が D_3 において正規部分群でないという例 6 の結果は

$$\sigma H \neq H\sigma$$

であるという第 8 回講義資料例 9 の計算からも得られることがわかる．