第 2 章 2.8 節 正規部分群と剰余群

climax

2025 年 7 月 16 日

目次

1　正規部分群と剰余群

1.1　正規部分群の定義と例

定義 1.1 (教科書 p.61 定義 2.8.1 正規部分群)**.** H を群 G の部分群とする。すべての $g \in G, h \in H$ に対し、$ghg^{-1} \in H$ となるとき、H を G の**正規部分群**といい、$H \lhd G$ あるいは $G \rhd H$ と書く。

例 1.2 (教科書 p.61 例 2.8.2 正規部分群 1)**.** G がアーベル群で H が任意の部分群なら、H は正規部分群である。

証明. G がアーベル群（可換）なので、任意の $g \in G, h \in H$ に対し、

$$ghg^{-1} = gg^{-1}h = 1_G h = h \in H$$

となるので、H は正規部分群である。

命題 1.3 (教科書 p.61 命題 2.8.3)**.** G_1, G_2 が群で $\phi : G_1 \to G_2$ が準同型なら、$\ker(\phi)$ は G_1 の正規部分群である。

証明. $g \in G_1, h \in \ker(\phi)$ なら、$\phi(h) = 1_{G_2}$ である。

$$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1} = \phi(g)1_{G_2}\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = 1_{G_2}$$

となるので、$ghg^{-1} \in \ker(\phi)$ となる。よって、$\ker(\phi) \lhd G_1$ である。

例 1.4 (教科書 p.61 例 2.8.4 正規部分群 2)**.** $GL_n(\mathbb{R}) \ni g \mapsto \det g \in \mathbb{R}^\times$ は全射準同型で、$\ker(\det) = SL_n(\mathbb{R})$ であった。したがって、$SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$ である。同様に、$SL_n(\mathbb{C}) \lhd GL_n(\mathbb{C})$ である。

例 1.5 (教科書 p.61 例 2.8.5 正規部分群 3)**.** 置換 σ にその符号 $\mathrm{sgn}(\sigma)$ を対応させる写像は準同型であった。したがって、交代群 $A_n = \ker(\mathrm{sgn}) \lhd \mathfrak{S}_n$ である。$n = 3$ なら、$A_3 = \langle (123) \rangle$ である。したがって、$\langle (123) \rangle \lhd \mathfrak{S}_3$ である。

例 1.6 (教科書 p.61 例 2.8.6 正規部分群 4)**.** $G = GL_2(\mathbb{R})$ とし、部分群として $N = \{n(u) \mid u \in \mathbb{R}\}$, $B = \{a(t_1, t_2)n(u) \mid t_1, t_2 \in \mathbb{R}^\times, u \in \mathbb{R}\}$ を考える。ただし、

$$a(t_1, t_2) = \begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix}, \quad n(u) = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$$

である。このとき、B の元 $b = a(t_1, t_2)n(u)$ と N の元 $n(u')$ に対して共役を計算すると、

$$\begin{aligned} bn(u')b^{-1} &= (a(t_1, t_2)n(u))n(u')(a(t_1, t_2)n(u))^{-1} \\ &= a(t_1, t_2)n(u)n(u')n(-u)a(t_1, t_2)^{-1} \\ &= a(t_1, t_2)n(u + u' - u)a(t_1^{-1}, t_2^{-1}) \\ &= a(t_1, t_2)n(u')a(t_1^{-1}, t_2^{-1}) \\ &= \begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix} \begin{pmatrix} 1 & u' \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t_1^{-1} & 0 \\ 0 & t_2^{-1} \end{pmatrix} \\ &= \begin{pmatrix} 1 & t_1 t_2^{-1} u' \\ 0 & 1 \end{pmatrix} = n(t_1 t_2^{-1} u') \in N \end{aligned}$$

となる。したがって、$N \lhd B$ である。B は $GL_2(\mathbb{R})$ のボレル (Borel) 部分群とよばれるものの一つである。

命題 1.7 (教科書 p.61 命題 2.8.7)**.** N は群 G の部分群で、G, N はそれぞれ部分集合 S, T で生成されているとする。このとき、すべての $x \in S, y \in T$ に対し $xyx^{-1}, x^{-1}yx \in N$ なら、N は正規部分群である。もし G が有限群なら、条件 $xyx^{-1} \in N$ だけで十分である。

証明. [教科書 p.62] まず、S の任意の元 x に対し、$xNx^{-1} \subset N$ および $x^{-1}Nx \subset N$ であることを示す。N の任意の元は T の元による語なので、$y_1, \ldots, y_n \in T$ により $y_1^{\pm 1} \cdots y_n^{\pm 1}$ という形をしている。すると、

$$x(y_1^{\pm 1} \cdots y_n^{\pm 1})x^{-1} = (xy_1^{\pm 1}x^{-1})(xy_2^{\pm 1}x^{-1}) \cdots (xy_n^{\pm 1}x^{-1})$$

となる。仮定より、すべての i について $xy_ix^{-1} \in N$ であり、N は部分群なのでその逆元 $(xy_ix^{-1})^{-1} = xy_i^{-1}x^{-1}$ も N に含まれる。したがって、右辺の各項は N の元であり、その積も N の元となる。よって $xNx^{-1} \subset N$ が示された。$x^{-1}Nx \subset N$ も同様である。

次に、G の任意の元 g について $gNg^{-1} \subset N$ を示す。g は S の元による語なので、$g = x_1^{\pm 1} \cdots x_m^{\pm 1}$ $(x_i \in S)$ と書ける。m に関する帰納法で示す。$m = 1$ の場合は、上で示した通り成立する。$m > 1$ とし、$g' = x_1^{\pm 1} \cdots x_{m-1}^{\pm 1}$ とおくと、$g = g'x_m^{\pm 1}$ である。

$$gNg^{-1} = (g'x_m^{\pm 1})N(g'x_m^{\pm 1})^{-1} = g'(x_m^{\pm 1}N(x_m^{\pm 1})^{-1})g'^{-1}$$

ここで、$m = 1$ の場合の結果から $x_m^{\pm 1}N(x_m^{\pm 1})^{-1} \subset N$ である。したがって、

$$gNg^{-1} \subset g'Ng'^{-1}$$

帰納法の仮定より、$g'Ng'^{-1} \subset N$ なので、$gNg^{-1} \subset N$ が示された。よって、N は正規部分群である。

系 1.8 (教科書 p.62 系 2.8.8)**.** G を群、S を G の部分集合とする。このとき、

$$N = \langle \{gsg^{-1} \mid g \in G, s \in S\} \rangle$$

は、S を含む最小の G の正規部分群である。

証明. [ノートによる補足] この証明は 3 つのステップに分かれる。

1. **N が S を含むことの証明**: S の任意の元 s をとる。N の定義において g として単位元 e を選ぶと、$ese^{-1} = s$ となる。これは N の生成元の一つである。したがって、S の全ての元は N の生成元に含まれるため、$S \subset N$ である。
2. **N が正規部分群であることの証明**: G の任意の元 g と N の任意の元 n に対し、$gng^{-1} \in N$ を示したい。生成元について示せば十分である。N の生成元は $t = hsh^{-1}$ $(h \in G, s \in S)$ の形をしている。

   $$gtg^{-1} = g(hsh^{-1})g^{-1} = (gh)s(h^{-1}g^{-1}) = (gh)s(gh)^{-1}$$

   gh は G の元なので、$(gh)s(gh)^{-1}$ は再び N の生成元の形をしている。したがって $gtg^{-1} \in N$ である。よって N は正規部分群である。
3. **N が最小であることの証明**: S を含む他の任意の正規部分群を H とする $(S \subset H, H \triangleleft G)$。このとき $N \subset H$ を示せば良い。N の生成元 gsg^{-1} を考える。$s \in S$ であり、$S \subset H$ なので、$s \in H$ である。H は正規部分群なので、任意の $g \in G$ に対して $gsg^{-1} \in H$ でなければならない。これは、N のすべての生成元が H に含まれることを意味する。H は部分群なので、これらの生成元から作られる群 N も H に含まれる。よって $N \subset H$ である。

以上より、N は S を含む最小の G の正規部分群である。

例 1.9 (教科書 p.62 例 2.8.9 正規部分群 5)**.** $G = \mathfrak{S}_3$, $N = \langle (123) \rangle$ とする。命題 2.8.7 を適用して $N \triangleleft G$ を示す。G は有限群であり、$S = \{(123), (12)\}$ で生成される。N は $T = \{(123)\}$ で生成される。$x \in S, y \in T$ について $xyx^{-1} \in N$ を確認すればよい。

- $x = (123), y = (123)$ の場合: $(123)(123)(123)^{-1} = (123) \in N$.
- $x = (12), y = (123)$ の場合: $(12)(123)(12)^{-1} = (132) = (123)^2 \in N$.

よって、命題 2.8.7 より N は正規部分群である。

1.2 剰余群 (商群)

命題 1.10 (ノートによる補足：剰余類の同値な定義)**.** Hを Gの部分群、xを Gの元とする。以下の 2つの集合は等しい。

$$Hx = \{y \in G \mid yx^{-1} \in H\}$$

証明. $(\subset)$ $z \in Hx$ をとる。$z = hx$ $(h \in H)$ と書ける。両辺に右から x^{-1} を掛けると、$zx^{-1} = h \in H$ となる。よって $z \in \{y \in G \mid yx^{-1} \in H\}$。

$(\supset)$ $z \in \{y \in G \mid yx^{-1} \in H\}$ をとる。$zx^{-1} = h$ となる $h \in H$ が存在する。両辺に右から x を掛けると、$z = hx$ となる。これは $z \in Hx$ を意味する。

補題 1.11 (教科書 p.63 補題 2.8.10)**.** Nが群 Gの正規部分群で $g \in G$ なら、$gN = Ng$ である。

証明. gN の任意の元 gn $(n \in N)$ をとる。N は正規部分群なので、$gng^{-1} \in N$ である。これを $n' = gng^{-1}$ とおくと、$n' \in N$ である。この式の両辺に右から g を掛けると、$n'g = gn$ となる。$n'g$ は Ng の元なので、$gn \in Ng$ が示され、$gN \subset Ng$ である。同様の議論で $Ng \subset gN$ も示せるため、$gN = Ng$ となる。

■剰余群の演算の定義　N が G の正規部分群であるとき、剰余類の集合 G/N に演算を定義する。G/N の 2 つの元 gN, hN の積を

$$(gN)(hN) \stackrel{\text{def}}{=} (gh)N$$

と定義する。

証明. [well-defined であることの証明 (教科書 p.63)] この定義が代表元 g, h の取り方によらないことを示す。gN, hN の任意の元は、それぞれ gn, hn' $(n, n' \in N)$ と書ける。この新しい代表元による積 'gnhn'' が、元の代表元による積 'gh' と同じ剰余類に属することを示す。これは、$(gh)^{-1}(gnhn') \in N$ を示すことと同値である。

$$(gh)^{-1}(gnhn') = h^{-1}g^{-1}gnhn' = h^{-1}(e)nhn' = h^{-1}nhn'$$

ここで、N は正規部分群なので $h^{-1}nh \in N$ である。これを $n'' = h^{-1}nh$ とおくと、式全体は $n''n'$ となる。$n'', n' \in N$ なので、その積 $n''n'$ も N の元である。よって演算は well-defined である。

定理 1.12 (教科書 p.64 定理 2.8.11)**.** G/N は上の演算により群になる。

証明.
- **単位元**: $1_G N = N$ が単位元となることは明らかである。
- **結合法則**: $g, h, k \in G$ なら、G での結合法則 $(gh)k = g(hk)$ より、

$$((gN)(hN))(kN) = (ghN)(kN) = ((gh)k)N = (g(hk))N = (gN)((hk)N) = (gN)((hN)(kN))$$

  となり、結合法則が成り立つ。
- **逆元**: $gN \in G/N$ の逆元が $g^{-1}N$ であることを示す。演算の定義より、

$$(gN)(g^{-1}N) = (gg^{-1})N = eN = N$$
$$(g^{-1}N)(gN) = (g^{-1}g)N = eN = N$$

  よって、任意の元 gN に対し逆元 $g^{-1}N$ が存在する。

以上より、G/N は群となる。

定義 1.13 (教科書 p.64 定義 2.8.12)**.** G/N に上の演算を考えたものを、G の N による**商群 (quotient group)** または**剰余群 (residue group)** という。

証明. [ノートによる補足：用語の整理 (教科書 p.64, 65)]

■Coset と Residue Class

- **Coset**: 日本語では「剰余類」または「傍系」と訳される。群 G を部分群 H によって分割した各ブロックを指す、抽象群論で一般的に使われる用語。
- **Residue Class**: 日本語では同じく「剰余類」と訳されるが、特に整数論で「n で割った余り」によるクラス分けを指す文脈で使われることが多い。

両者は本質的に同じ概念だが、使われる文脈にニュアンスの違いがある。

■商構造の用語　群論以外でも、同様の「商」構造が現れる。

1. G/N: G は群で N はその正規部分群
2. A/I: A は環で I はその「イデアル」
3. M/N: M は環上の加群で N はその部分加群
4. $\{a/b \mid a \in A, b \in A \setminus \{0\}\}$: A は「整域」

記号	日本語	英語
G/N	剰余群 / 商群	quotient group
A/I	剰余環	quotient ring
M/N	剰余加群	quotient module
$\{a/b\}$	商体	fraction field

命題 1.14 (教科書 p.65 命題 2.8.14)**.** 自然な写像 $\pi : G \to G/N$（$g \mapsto gN$）は群の全射準同型である。また、$\ker(\pi) = N$ である。

証明. π が全射であることは G/N の定義より明らか。準同型であることは $\pi(gh) = (gh)N = (gN)(hN) = \pi(g)\pi(h)$ より従う。核 $\ker(\pi)$ は、$\pi(g)$ が G/N の単位元 N となるような $g \in G$ の集合である。$\pi(g) = N$ は $gN = N$ と同値であり、これは剰余類の性質から $g \in N$ と同値である。よって $\ker(\pi) = N$ が示された。

例 1.15 (教科書 p.65 例 2.8.15 剰余群 1)**.** $n \neq 0$ を整数とし、剰余群 $\mathbb{Z}/n\mathbb{Z}$ を考える。$x \in \mathbb{Z}$ の $n\mathbb{Z}$ に関する剰余類を $\bar{x}$ とする。剰余群 $\mathbb{Z}/n\mathbb{Z}$ の演算の定義は $x, y \in \mathbb{Z}$ に対して

$$(x + n\mathbb{Z}) + (y + n\mathbb{Z}) = (x + y) + n\mathbb{Z}$$

とするものである。もし $x + y = qn + r$ で $r \in \mathbb{Z}, 0 \leq r < |n|$ なら、$x + y + n\mathbb{Z} = r + n\mathbb{Z}$ である。

例 1.16 (教科書 p.65 例 2.8.16 剰余群 2)**.** $G = \mathfrak{S}_3$, $N = \langle (123) \rangle$ とおく。$|G| = 6, |N| = 3$ なので、剰余群の位数 (元の数) は $|G/N| = |G|/|N| = 6/3 = 2$ である。N の元は $N = \{e, (123), (132)\}$ である。剰余類は 2 つ存在する。

- 単位元: $N = \{e, (123), (132)\}$
- もう一つの元: $(12)N = \{(12)e, (12)(123), (12)(132)\} = \{(12), (13), (23)\}$

よって、$G/N = \{N, (12)N\}$ となる。位数が 2（素数）なので、これは $(12)N$ で生成される巡回群である。