群論 (第10回)

10 群の準同型定理と使い方

準同型定理は現代数学の様々な場面で用いられる重要な道具です. 今回は準同型定理の主張とその使い方を紹介します.

定理 10-1 (準同型定理)

群の準同型 $f : G_1 \longrightarrow G_2$ を考える.

(1) $\ker f$ は G_1 の正規部分群であり, $\mathrm{Im} f$ は G_2 の部分群である.

(2) 写像

$$F : G_1/\ker f \longrightarrow \mathrm{Im} f \ (x \ker f \longmapsto f(x))$$

は同型写像である. 特に $G_1/\ker f \simeq \mathrm{Im} f$ が成り立つ.

(3) $|G_1| < \infty$ ならば,

$$|G_1| = |\mathrm{Im} f||\ker f|.$$

[証明]

(1) 定理 6-1 と定理 8-2 より成り立つ.

(2) F が同型写像であること.

(i) $x \ker f,\ y \ker f \in G_1/\ker f$ に対して,

$$\begin{aligned} x \ker f = y \ker f &\iff x^{-1}y \in \ker f \\ &\iff f(x^{-1}y) = 1_{G_2} \\ &\iff f(y) = f(x) \\ &\iff F(y \ker f) = F(x \ker f). \end{aligned}$$

よって, F は well-defined かつ単射である.

(ii) $z \in \mathrm{Im} f$ を取ると, $f(x) = z$ となる $x \in G_1$ が存在する. $F(x \ker f) = f(x) = z$ より F は全射である.

(iii) $x \ker f,\ y \ker f \in G_1/\ker f$ に対して,

$$\begin{aligned} F((x \ker f)(y \ker f)) &= F((xy) \ker f) \\ &= f(xy) \\ &= f(x)f(y) \\ &= F(x \ker f)F(y \ker f). \end{aligned}$$

よって F は準同型である.

以上 (i)–(iii) より F は同型写像である.

(3) ラグランジュの定理と (2) より

$$|G_1| = (G_1 : \ker f) \cdot |\ker f| = |G_1/\ker f| \cdot |\ker f| = |\mathrm{Im} f| \cdot |\ker f|.$$

□

例題で準同型定理の使い方を確認しておきます.

例題 10-1
群 $\mathbb{C}^\times$ とその部分群

$$S^1 = \{z \in \mathbb{C}^\times \mid |z| = 1\}$$

を考える. このとき, $\mathbb{C}^\times/S^1 \simeq \mathbb{R}_{>0}$ を示せ.

[解答]
写像 $f : \mathbb{C}^\times \to \mathbb{R}^\times$ $(z \mapsto |z|)$ を考える. ただし, $|z|$ は z の絶対値を表す. $z, w \in \mathbb{C}^\times$ に対して

$$f(zw) = |zw| = |z||w| = f(z)f(w).$$

よって f は準同型. また $\mathrm{Im} f = \mathbb{R}_{>0}$ であり,

$$\ker f = \{z \in \mathbb{C}^\times \mid f(z) = 1\} = S^1.$$

準同型定理より $\mathbb{C}^\times/S^1 \simeq \mathbb{R}_{>0}$ が従う.

□

問題 10-1 $f : \mathbb{R} \to \mathbb{C}^\times$ $(x \mapsto e^{2\pi ix})$ が準同型であることを示し, さらに $\mathbb{R}/\mathbb{Z} \simeq S^1$ を示せ. ただし, S^1 は例題 10-1 のものとする.

問題 10-2 アーベル群 G の部分群

$$A = \{x^2 \mid x \in G\}, \qquad B = \{x \mid x^2 = 1\}$$

を考える. このとき, $G/B \simeq A$ を示せ.

例題 10-2

群 $G = \mathrm{GL}_2(\mathbb{C})$ とその部分群 $N = \{\alpha \in G | \det \alpha = 1\}$ を考える.

(1) $G/N \simeq \mathbb{C}^\times$ を示せ.

(2) G/N はアーベル群であることを示せ.

(3) $g = \begin{pmatrix} i & 5 \\ 0 & 1 \end{pmatrix} \in G$ のとき, gN の位数を求めよ.

[解答]

(1) $f : G \longrightarrow \mathbb{C}^\times$ $(\alpha \longmapsto \det \alpha)$ と置くと,

$$f(\alpha\beta) = \det(\alpha\beta) = \det(\alpha)\det(\beta) = f(\alpha)f(\beta) \quad (\alpha, \beta \in G).$$

よって f は準同型である. また

$$\ker f = \{\alpha \in G \mid f(\alpha) = 1\} = N.$$

$a \in \mathbb{C}^\times$ に対して, $\alpha = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$ と置くと, $\alpha \in G$ であり $f(\alpha) = a$ を満たす. よって f は全射であり, $\mathrm{Im} f = \mathbb{C}^\times$ を得る. 以上より, 準同型定理から

$$F : G/N \longrightarrow \mathbb{C}^\times \ (\alpha N \longmapsto f(\alpha))$$

は同型写像である. 特に $G/N \simeq \mathbb{C}^\times$.

(2) $\mathbb{C}^\times$ がアーベル群より, 定理 9-2 (1) から G/N もアーベル群である.

(3) 定理 9-2 (3) より,

$$|gN| = |F(gN)| = |f(g)| = |i| = 4.$$

$\square$

問題 10-3 $\mathrm{GL}_2(\mathbb{C})$ の二つの部分群

$$G = \left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{C},\ ac \neq 0\right\}, \quad N = \left\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{C},\ a \neq 0\right\}$$

と写像

$$f : G \to \mathbb{C}^\times \left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto \frac{a}{c}\right)$$

を考える. さらに $g = \begin{pmatrix} 1+i & 3-i \\ 0 & 1-i \end{pmatrix}$ と置く.

(1) f が準同型であることを示せ.

(2) 準同型定理を用いて, $G/N \simeq \mathbb{C}^{\times}$ を示せ.

(3) gN の G/N における位数を求めよ.

(4) G/N の元で位数 6 のものをすべて求めよ.

最後に準同型定理の応用として, 中国剰余定理を証明します.

定理 10-2 (中国剰余定理)
互いに素な自然数 m, n に対して,

$$F : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \ (x + mn\mathbb{Z} \longmapsto (x + m\mathbb{Z}, x + n\mathbb{Z}))$$

は同型写像である.

$\star$ 上の同型写像から, 整数 a, b に対して,

$$x \equiv a \pmod{m}, \qquad x \equiv a \pmod{n}$$

を満たす整数 x が法 mn の差を除いて一意的に存在することが分かる. 中国剰余定理については資料「合同式の基礎 (2) 」(初等整数論, 第 5 回) も参照のこと.

[証明]
写像

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \ (x \longmapsto (x + m\mathbb{Z}, x + n\mathbb{Z}))$$

を考える. $x, y \in \mathbb{Z}$ に対して,

$$\begin{aligned} f(x+y) &= ((x+y) + m\mathbb{Z}, (x+y) + n\mathbb{Z}) \\ &= ((x + m\mathbb{Z}) + (y + m\mathbb{Z}), (x + n\mathbb{Z}) + (y + n\mathbb{Z})) \\ &= (x + m\mathbb{Z}, x + n\mathbb{Z}) + (y + m\mathbb{Z}, y + n\mathbb{Z}) \\ &= f(x) + f(y). \end{aligned}$$

よって, f は準同型である. $x \in \mathbb{Z}$ に対して,

$$\begin{aligned} x \in \ker f &\iff (x + m\mathbb{Z}, x + n\mathbb{Z}) = (0 + m\mathbb{Z}, 0 + n\mathbb{Z}) \\ &\iff x \in m\mathbb{Z} \cap n\mathbb{Z} \\ &\iff x \in mn\mathbb{Z} \qquad (\gcd(m,n) = 1 \text{ に注意}). \end{aligned}$$

従って $\ker f = mn\mathbb{Z}$. 準同型定理より,

$$F : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathrm{Im} f \ \ (x + mn\mathbb{Z} \longmapsto f(x))$$

は同型写像である．また

$$mn = |\mathbb{Z}/mn\mathbb{Z}| = |\mathrm{Im} f| \leq |\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}| = mn.$$

従って $|\mathrm{Im} f| = |\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}|$．よって $\mathrm{Im} f = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

□