準同型定理

定義 1 G, G' がそれぞれ演算 $\cdot, *$ について群をなし，写像 $f : G \longrightarrow G'$ が $\forall a, b \in G$ について

$$f(a \cdot b) = f(a) * f(b)$$

を満たすとき，f を G から G' への**準同型写像 (homomorphism)** という．

例 1 $\boldsymbol{C}^{\times}$=$\boldsymbol{C}$−$\{0\}$,$\boldsymbol{R}^{\times}$=$\boldsymbol{R}$−$\{0\}$ はともに乗法 $\cdot$ について群である．今，写像 f を

$$\begin{aligned} f : \boldsymbol{C}^{\times} &\longrightarrow \boldsymbol{R}^{\times} \\ z &\longmapsto f(z) = |z| \end{aligned}$$

とすると，f は準同型写像である．

例 2 $\boldsymbol{R}$ は加法 $+$ について群である．$\boldsymbol{R}^{+} = \{x | x > 0, x \in \boldsymbol{R}\}$ は乗法 $\cdot$ について群である．今，写像 f を

$$\begin{aligned} f : \boldsymbol{R} &\longrightarrow \boldsymbol{R}^{+} \\ x &\longmapsto f(x) = e^{x} \end{aligned}$$

とすると，f は準同型写像である．

定理 1 演算 $\cdot$ について e を単位元とする群 G から, 演算 $*$ について e' を単位元とする群 G' への準同型写像 $f : G \longrightarrow G'$ について次のことが成り立つ.

1. $f(e) = e'$
2. $f(a^{-1}) = f(a)^{-1}$

［証明］

1.

$$\begin{aligned} e \cdot e &= e \\ f(e \cdot e) &= f(e) \\ f(e) * f(e) &= f(e) \\ \{f(e) * f(e)\} * f(e)^{-1} &= f(e) * f(e)^{-1} \\ f(e) * \{f(e) * f(e)^{-1}\} &= f(e) * f(e)^{-1} \\ f(e) * e' &= e' \\ \therefore f(e) &= e' \end{aligned}$$

［証明おわり］

2.

$$\begin{aligned} a \cdot a^{-1} &= e \\ f(a \cdot a^{-1}) &= f(e) \\ f(a) * f(a^{-1}) &= e' \\ f(a)^{-1} * \{f(a) * f(a^{-1})\} &= f(a)^{-1} * e' \\ \{f(a)^{-1} * f(a)\} * f(a)^{-1} &= f(a)^{-1} * e' \\ e' * f(a)^{-1} &= f(a)^{-1} * e' \\ \therefore f(a^{-1}) &= f(a)^{-1} \end{aligned}$$

［証明おわり］

つまり単位元は単位元に写り，逆元は像の逆元に写るというわけである．

定理 2 f を群 G から群 G' への準同型写像とする．H が G の部分群ならば $H' = f(H)$[*1]も G' の部分群である．

［証明］

$$a, b \in H \Longrightarrow f(a), f(b) \in H'$$

$$f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$$

H が G の部分群なので，

$$ab^{-1} \in H$$

$$\therefore f(ab^{-1}) \in H'$$

よって H' は G' の部分群である．［証明おわり］

定理 3 演算 $\cdot$ についての群 G と，演算 $*$ についての群 G' がある．f は $G \longrightarrow G'$ の準同型写像で，全射であるとき，H が G の正規部分群ならば $f(H)$ も G' の正規部分群である．

［証明］$\forall g' \in G, \forall h' \in f(H) \Longrightarrow g'^{-1} * h' * g' \in f(H)$ であることをこれから証明する．

$\forall g' \in G, \forall h' \in f(H)$ について，f は全写なので

$$f(g) = g' \ (\exists g \in g), f(h) = h' \ (\exists h \in H)$$

と書くことができる．

$$\therefore g'^{-1} * h' * g' = f(g)^{-1} * f(h) * f(g)$$

f は準同型写像なので

$$f(g)^{-1} * f(h) * f(g) = f(g^{-1}hg)$$

h は正規部分群 H の元なので

$$g^{-1}hg \in H$$

$$\therefore f(g^{-1}hg) \in f(H)$$

[*1] $f(H) = \{f(h) \mid h \in H\}$ と定義する．

$$g'^{-1} * h' * g' \in f(H)$$

［証明おわり］

定理 4 f を群 G から群 G' への準同型写像とするとき，

$$\{k \mid f(k) = e', k \in G\}$$

を f の**核 (kernel)** といい，Ker.f と表す[*2]．ただし，e' は G の単位元である．

当然 G の単位元 e も Ker.f に含まれるがそれ以外にもある可能性がある．f が単射であれば Ker.$f = e$ である．

定理 5 準同型写像 $f : G \longrightarrow G'$ の Ker.f は G の正規部分群である．

［証明］部分群であることの証明．$K = \mathrm{Ker}.f$ とし，G' の単位元を e' とする．今 $\forall k_1, k_2 \in K$ とすると，

$$f(k_1 \cdot k_2^{-1}) = f(k_1) * f(k_2)^{-1} = e' * e'{-1} = e'$$

核の定義より

$$k_1 \cdot k_2^{-1} \in K$$

よって Ker.f は G の部分群である．

正規部分群であることの証明．$\forall g \in G$ について

$$f(g^{-1} \cdot k \cdot g) = f(g)^{-1} * f(k) * f(g) = f(g)^{-1} * e' * f(g) = f(g)^{-1} * f(g) = e'$$
$$\therefore g^{-1} \cdot k \cdot g \in K$$

よって K は G の正規部分群である．［証明おわり］

例 3 乗法群 $\boldsymbol{C}^\times$ から乗法群 $\boldsymbol{R}^\times$ への準同型写像

$$\begin{aligned} f : \boldsymbol{C}^\times &\longrightarrow \boldsymbol{R}^\times \\ z &\longmapsto f(z) = |z| \end{aligned}$$

について, $\boldsymbol{R}^\times$ の単位元は 1 であるから, Ker.$f = \{z \mid |z| = 1, z \in \boldsymbol{C}^\times\}$．あるいは Ker.$f = \{a+bi \mid a^2+b^2 = 1, a, b \in \boldsymbol{R}\}$ である．

例 4 加法群 $\boldsymbol{R}$ から乗法群 $\boldsymbol{R}^+$ への準同型写像

$$\begin{aligned} f : \boldsymbol{R} &\longrightarrow \boldsymbol{R}^+ \\ x &\longmapsto f(x) = e^x \end{aligned}$$

の場合，$\boldsymbol{R}^+$ の単位元は 1 であり，Ker.$f = 0$ である．

定義 2 準同型写像 $f : G \longrightarrow G'$ が全単射であるとき，f を**同型写像 (isomorphism)** という．また，G, G' について同型写像 $f : G \longrightarrow G'$ が存在するとき，G と G' は**同型 (isomorphic)** であるといい，$G \cong G'$ と表す[*3]．

[*2] ほかに kernel(f) などと表す場合もある．
[*3] $G \sim G'$ あるいは $G \approx G'$ などと表す場合もある

例 5 例 4 の準同型写像

$$\begin{aligned} f : \boldsymbol{R} &\longrightarrow \boldsymbol{R}^{+} \\ x &\longmapsto f(x) = e^{x} \end{aligned}$$

は全単射であるので f は同型写像である．つまり $\boldsymbol{R} \cong \boldsymbol{R}^{+}$ である．

例 6 加法についての群 $\boldsymbol{Z}$ からその部分群 $2\boldsymbol{Z}$ への写像

$$\begin{aligned} f : \boldsymbol{Z} &\longrightarrow 2\boldsymbol{Z} \\ n &\longmapsto f(n) = 2n \end{aligned}$$

を考えた場合，$f(n+m) = f(n) + f(m)$ が成り立つので，f は準同型写像である．また f は全単射であるので同型写像である．よって $\boldsymbol{Z} \cong 2\boldsymbol{Z}$ である．

問題 1 複素数全体の集合 $\boldsymbol{C}$ は加法について群である．また $M = \left\{ A \,\middle|\, A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, a, b \in \boldsymbol{R} \right\}$ も加法について群である．このとき写像

$$\begin{aligned} f : \boldsymbol{C} &\longrightarrow M \\ a + bi &\longmapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \end{aligned}$$

が同型写像であることを示し，$\boldsymbol{C} \cong M$ を示せ．

［証明］$f(a+bi+c+di) = f\left(a+c+(b+d)i\right) = \begin{pmatrix} a+c & -(b+d) \\ b+d & a+c \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix}$ であるから f は準同型写像である．また $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} c & -d \\ d & c \end{pmatrix}$ であれば $a + bi = c + di$ となるので単射である．また $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ $(\forall a, b \in \boldsymbol{R})$ に対して $z = a + bi$ とおけば $f(z) = A$ が成り立つので全射である．よって f は同型写像であり，$\boldsymbol{C} \cong M$ である． ［証明おわり］

定理 6 準同型定理 f を群 G から群 G' への全射準同型写像とする．$K = \mathrm{Ker}.f$ とし，G/K を G の K による剰余群とするとき，

$$G/K \cong G'$$

が成り立つ．

［証明］

$$\begin{aligned} f : G &\longrightarrow G' \\ a &\longmapsto f(a) \end{aligned}$$

をもとに，写像

$$\begin{aligned} \tilde{f} : G/K &\longrightarrow G' \\ Ka &\longmapsto \tilde{f}(Ka) = f(a) \end{aligned}$$

を考える．剰余類の演算の定義より，

$$\tilde{f}(Ka \cdot Kb) = \tilde{f}(Ka \cdot b)$$

$\tilde{f}(Ka) = f(a)$ より，

$$\tilde{f}(Ka \cdot b)$$

f は準同型写像なので

$$f(a \cdot b) = f(a) * f(b)$$

$\tilde{f}(Ka) = f(a)$ より，

$$f(a) * f(b) = \tilde{f}(Ka) * \tilde{f}(Kb)$$

よって $\tilde{f}$ は準同型写像である．

$\forall a, b \in G$ について

$$\tilde{f}(Ka) = \tilde{f}(Kb)$$

とすると，$\tilde{f}(Ka) = f(a)$ より，

$$f(a) = f(b)$$

右側より $f(b)^1$ を演算させると，

$$f(a) * f(b)^{-1} = e'$$

ただし，e' は G' の単位元．準同型写像の性質を用いて

$$f(a) * f(b^{-1}) = e'$$

$$\therefore f(a \cdot b^{-1}) = e'$$

$$\therefore a \cdot b^{-1} \in K$$

$$a \equiv b \pmod{K}$$

$$\therefore Ka = Kb$$

つまり $\forall a, b \in G$ について

$$\tilde{f}(Ka) = \tilde{f}(Kb) \Longrightarrow Ka = Kb$$

が示せたので $\tilde{f}$ は全射である．よって $\tilde{f}$ は同型写像で

$$G/K \cong G'$$

が成り立つ． ［証明おわり］

問題 2 $T = \{z \mid |z| = 1, z \in \boldsymbol{C}\}$ とするとき次の問いに答えよ．

1. 乗法に関して T は $\boldsymbol{C}$ の部分群であることを示せ．
2. $\boldsymbol{R}$ は加法 $+$ について群をなし，T は乗法 $\cdot$ について群をなす．今，

$$\begin{aligned} f : \boldsymbol{R} &\longrightarrow T \\ \theta &\longmapsto f(\theta) = \cos 2\theta\pi + i \sin 2\theta\pi \end{aligned}$$

と定義するとき，f は全射準同型写像であることを証明せよ．

3. Ker.f を求めよ．
4. $\boldsymbol{R}/\boldsymbol{Z} \cong T$ を証明せよ．

［解］

1. $|z| = |w| = 1$ とするとき $|zw^{-1}| = |z||w|^{-1} = 1$ であるから $zw^{-1} \in T$．よって T は $\boldsymbol{C}$ の部分群である．
2.
$$\begin{aligned} f(\theta_1 + \theta_2) &= \cos 2(\theta_1 + \theta_2)\pi + i \sin 2(\theta_1 + \theta_2)\pi \\ &= (\cos 2\theta_1\pi + i \sin 2\theta_1\pi)(\cos 2\theta_2\pi + i \sin 2\theta_2\pi) \\ &= f(\theta_1) \cdot f(\theta_2) \end{aligned}$$

   よって f は準同型写像である．また $\forall z \in T$ について $z = f(\theta)$ $(\exists\theta \in \boldsymbol{R})$ と表せるので全射である．よって f は全射準同型写像である．
3. T の単位元は 1 である．よって Ker.$f = \{n \mid n \in \boldsymbol{Z}\} = \boldsymbol{Z}$ である．
4. 準同型定理より明らか．

例 7 剰余類群（整数全体の加法群 $\boldsymbol{Z}$ から作られる剰余類の作る群，residual class group of the additive group) は，次のように定義される．

m を与えられた整数（普通は $m \geq 2$）とするとき，m で割って k 余る整数全体の集合を $\overline{k}$ と表し，

$$f : \boldsymbol{Z} \longrightarrow M = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m}\}$$

を考える（言い換えると，全ての整数に m についての剰余類を対応させる）と

$$\mathrm{Ker.}(f) = \{x \mid f(x) = \overline{0}\} = \{km \mid k \in \boldsymbol{Z}\} = m\boldsymbol{Z}(= \overline{0})$$

よって準同型定理より

$$\boldsymbol{Z}/m\boldsymbol{Z} \cong M$$

これは一般の剰余類群の起源である．剰余類 $\boldsymbol{Z}/m\boldsymbol{Z}$ は $\boldsymbol{Z}/m$ と表すことも多い．

参考文献

[1] 石村園子『すぐわかる代数』（東京図書，2003 年）

[2] 長岡亮介『線形代数学』（放送大学教育振興会，2004 年）

[3] 「ウィキペディア」<http://ja.wikipedia.org/wiki/>

[4] 「Wikipedia」<http://en.wikipedia.org/wiki/>