環論 (第 7 回)

7. 環準同型

環の代数構造を保つような写像を環準同型と言う. 今回は環準同型の基本事項と具体例について解説する.

定義 7-1 (環準同型)
可換環 A, B を考える. 写像 $f : A \to B$ が次の (1) ∼ (3) を満たすとき**環準同型**という.

(1) $f(x + y) = f(x) + f(y) \quad (x, y \in A)$.

(2) $f(xy) = f(x)f(y) \quad (x, y \in A)$.

(3) $f(1_A) = 1_B$.

可換環 A 上の恒等写像

$$\mathrm{Id}_A : A \to A \ \ (x \mapsto x)$$

は定義 7-1 の条件を満たすので環準同型である.

例題 7-1
平方数でない整数 n に対して, 可換環 $R = \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$ を考える. このとき,

$$f : R \to R \ (a + b\sqrt{n} \mapsto a - b\sqrt{n}\ )$$

は環準同型であることを示せ.

[証明]
$x = a + b\sqrt{n},\ y = c + d\sqrt{n} \in R\ (a, b, c, d \in \mathbb{Z})$ をとる.

(1) $f(x + y) = f(x) + f(y)$ であること.

$$\begin{aligned} f(x+y) &= f((a+c) + (b+d)\sqrt{n}) \\ &= (a+c) - (b+d)\sqrt{n} \\ &= (a - b\sqrt{n}) + (c - d\sqrt{n}) \\ &= f(x) + f(y). \end{aligned}$$

(2) $f(xy) = f(x)f(y)$ であること.

$$\begin{aligned} f(xy) &= f((ac+nbd)+(ad+bc)\sqrt{n}) \\ &= (ac+nbd)-(ad+bc)\sqrt{n} \\ &= (a-b\sqrt{n})(c-d\sqrt{n}) \\ &= f(x)f(y). \end{aligned}$$

(3) $f(1) = f(1+0\cdot\sqrt{n}) = 1-0\cdot\sqrt{n} = 1$.

以上 (1)~(3) より f は環準同型である.

□

問題 7-1 写像 $f : \mathbb{C} \to \mathbb{C}$ $(z \mapsto \bar{z})$ は環準同型であることを示せ.

問題 7-2 自然数 n に対して, 整数 p_n, q_n を

$$p_n + q_n\sqrt{-2} = (1+\sqrt{-2})^n$$

により定める. このとき,

$$p_n = \frac{1}{2}\left\{(1+\sqrt{-2})^n + (1-\sqrt{-2})^n\right\}, \quad q_n = \frac{1}{2}\left\{(1+\sqrt{-2})^n - (1-\sqrt{-2})^n\right\}$$

を示せ.

定理 7-1

可換環の環準同型 $f : A \to B$ に対して次が成り立つ.

(1) $f(0_A) = 0_B$.

(2) $x \in A$ に対して $f(-x) = -f(x)$.

(3) $x \in A^\times \Rightarrow f(x) \in B^\times$.

[証明]

(1) について.

$$f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A).$$

よって $f(0_A) = 0_B$.

(2) について.

$$f(x) + f(-x) = f(x+(-x)) = f(0_A) = 0_B.$$

よって $f(-x) = -f(x)$.

(3) $x \in A^\times$ より, $xy = 1_A$ となる $y \in A$ がある. よって

$$1_B = f(1_A) = f(xy) = f(x)f(y).$$

よって $f(x) \in B^{\times}$.

$\square$

次に代入写像が環準同型になることを示す.

定理 7-2

可換環 B とその部分環 A を考える. $\alpha \in B$ に対して

$$\varphi : A[x] \to B \quad \left(f(x) = \sum_i a_i x^i \mapsto f(\alpha) = \sum_i a_i \alpha^i \right)$$

は環準同型である.

[証明]

$f(x), g(x) \in A[x]$ とし,

$$f(x) = \sum_i a_i x^i, \qquad g(x) = \sum_i b_i x^i \qquad (a_i,\ b_i \in A)$$

と表す.

(1) について.

$$\begin{aligned} \varphi(f(x)+g(x)) &= \varphi\left(\sum_i (a_i+b_i)x^i\right) \\ &= \sum_i (a_i+b_i)\alpha^i \\ &= \sum_i a_i\alpha^i + \sum_i b_i\alpha^i \\ &= \varphi(f(x)) + \varphi(g(x)). \end{aligned}$$

(2) について.

$$\begin{aligned} \varphi(f(x)g(x)) &= \varphi\left(\sum_k \left(\sum_{i+j=k} a_i b_j\right) x^k\right) \\ &= \sum_k \left(\sum_{i+j=k} a_i b_j\right) \alpha^k \\ &= \left(\sum_i a_i\alpha^i\right)\left(\sum_i b_i\alpha^i\right) \\ &= \varphi(f(x))\varphi(g(x)). \end{aligned}$$

(3) $\varphi(1_{A[x]}) = \varphi(1_A) = 1_A = 1_B$.

以上より φ は環準同型である.

$\square$

定義 7-2
可換環の環準同型 $f: A \to B$ に対して

$$\ker(f) = \{x \in A \mid f(x) = 0_B\},$$
$$\mathrm{Im}(f) = \{f(x) \mid x \in A\}$$

とおく. $\ker(f)$ を f の**核**, $\mathrm{Im}(f)$ を f の**像**と呼ぶ.

[補足]

(1) 定理 7-1 より $0_A \in \ker(f)$, $1_B = f(1_A) \in \mathrm{Im}(f)$. 特に $\ker(f) \neq \phi$ と $\mathrm{Im}(f) \neq \phi$ が従う.

(2) 定理 7-2 の環準同型 $\varphi: A[x] \to B$ $(f(x) \mapsto f(\alpha))$ に対して $A[\alpha] := \mathrm{Im}(\varphi)$ とおく. このとき, $A[\alpha]$ は A と α を含む最小の B の部分環である.

定理 7-3
可換環の環準同型 $f: A \to B$ に対して次が成り立つ.

(1) $\ker(f)$ は A のイデアルである.

(2) $\mathrm{Im}(f)$ は B の部分環である.

[証明]
(1) 問題 7-3.
(2) $\mathrm{Im}(f)$ が定理 3-1 の部分環になるための条件を確認する. $y_1, y_2 \in \mathrm{Im}(f)$ とすると,

$$y_1 = f(x_1), \quad y_2 = f(x_2) \quad (x_1, x_2 \in A)$$

と表せる.

(i) $y_1 - y_2 = f(x_1) - f(x_2) = f(x_1) + f(-x_2) = f(x_1 - x_2) \in \mathrm{Im}(f)$.

(ii) $y_1 y_2 = f(x_1) f(x_2) = f(x_1 x_2) \in \mathrm{Im}(f)$.

(iii) $1_B = f(1_A) \in \mathrm{Im}(f)$.

以上 (i) ~(iii) より $\mathrm{Im}(f)$ は B の部分環である.

□

問題 7-3　定理 7-3 (1) を確認せよ.

例題 7-2

平方数でない整数 n に対して, 環準同型 $\varphi : \mathbb{Z}[x] \to \mathbb{C}$ $(f(x) \mapsto f(\sqrt{n}))$ を考える. また $R = \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$ とする.

(1) $\ker(\varphi) = (x^2 - n)$ を示せ. (注: $(x^2 - n)$ は $x^2 - n$ で生成される $\mathbb{Z}[x]$ のイデアル)

(2) $\mathrm{Im}(\varphi) = R$ を示せ.

[証明]

(1) $\varphi(x^2 - n) = (\sqrt{n})^2 - n = 0$ より $x^2 - n \in \ker\varphi$. よって

$$(x^2 - n) \subseteq \ker(\varphi).$$

逆に $f(x) \in \ker(\varphi)$ とする. 割り算の原理より,

$$f(x) = (x^2 - n)q(x) + ax + b \quad (q(x) \in \mathbb{Z}[x],\ a, b \in \mathbb{Z})$$

と表せる. よって $0 = f(\sqrt{n}) = a\sqrt{n} + b$. ここで $\sqrt{n}$ は無理数より $a = b = 0$.

$$f(x) = (x^2 - n)q(x) \in (x^2 - n).$$

これで $\ker(\varphi) \subseteq (x^2 - n)$ も示せた.

(2) $z \in R$ をとり,

$$z = a + b\sqrt{n} \quad (a, b \in \mathbb{Z})$$

と表す. $f(x) = a + bx$ とおくと, $f(x) \in \mathbb{Z}[x]$ であり,

$$z = a + b\sqrt{n} = \varphi(f(x)) \in \mathrm{Im}(\varphi).$$

従って $R \subseteq \mathrm{Im}(\varphi)$. 逆に $z \in \mathrm{Im}(\varphi)$ とすると, $z = f(\sqrt{n}\,)$ $(f(x) \in \mathbb{Z}[x])$ とかける. 割り算の原理より

$$f(x) = (x^2 - n)q(x) + a + bx \quad (q(x) \in \mathbb{Z}[x],\ a, b \in \mathbb{Z})$$

と表せる. このとき,

$$z = f(\sqrt{n}) = a + b\sqrt{n} \in R.$$

よって $\mathrm{Im}(\varphi) \subseteq R$ も示せた.

□

問題 7-4 整数 $a \in \mathbb{Z}$ と環準同型 $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$ $(f(x) \mapsto f(a))$ に対して次を示せ.

$$\ker(\varphi) = (x - a), \qquad \mathrm{Im}(\varphi) = \mathbb{Z}.$$