

§5. 根の添加

以下で扱う準同型写像はどれも零写像ではないとする。このとき、

体から（単位元をもつ）環への準同型写像は単射

であることに注意する。【理由】 体 K から環 R への準同型写像 $\sigma : K \rightarrow R$ の核 $\text{Ker } \sigma$ は体 K のイデアルだから、 $\{0\}$ または K のどちらかであるが、いま、 σ は零写像ではないとしているので、 $\text{Ker } \sigma = \{0\}$ 。したがって σ は単射である。

とくに、以下において、体から体への準同型写像が頻繁に現れるが、これらはすべて単射準同型である。

定義 5.1 L/K を体の拡大とする。 $\sigma : L \rightarrow M$, $\tau : K \rightarrow M$ がそれぞれ L, K から体 M への準同型写像であって、

$$\forall a \in K \quad \text{に対して} \quad \sigma(a) = \tau(a)$$

をみたすとき、 σ は τ の L への**延長**、あるいは、 τ は σ の K への**制限**であるという。また、このとき $\tau = \sigma|_K$ と表す。

定義 5.2 L, M がともに体 K の拡大体で、準同型写像 $\sigma : L \rightarrow M$ が K の恒等写像 $\text{id}_K : K \rightarrow K$ の延長であるとき、つまり、すべての $a \in K$ について $\sigma(a) = a$ が成り立つとき、 σ を K 上の**準同型写像**という。

定義 5.3 体 L から体 M への準同型写像 $\sigma : L \rightarrow M$ が全射であるとき、 σ を**同型写像**といい、 L と M は**同型**であるという。このとき

$$L \cong M$$

と表すことが多い。

定義 5.4 可換環 R から可換環 S への準同型写像

$$\sigma : R \longrightarrow S$$

が与えられたとき、 R 上の多項式 $f(X) \in R[X]$ に対して、その係数に σ をほどこして得られる S 上の多項式を $f^\sigma(X)$ と表す。すなわち、 $f(X) = \sum c_i X^i$ のとき $f^\sigma(X) = \sum \sigma(c_i) X^i$ と定める。このようにして、多項式環の間の準同型写像

$$R[X] \longrightarrow S[X]. \quad f(X) \mapsto f^\sigma(X)$$

が自然に定義される。

定理 5.5 $f(X)$ が体 K 上の既約多項式ならば、剰余環 $K[X]/(f(X))$ は体である。ここで、

$$\text{包含写像 } \iota: K \longrightarrow K[X], \quad \text{自然な全射 } \nu: K[X] \longrightarrow K[X]/(f(X))$$

の合成写像として

$$\sigma = \nu \circ \iota: K \longrightarrow K[X]/(f(X))$$

を定めると、 σ は体の準同型写像である。さらに、 $\alpha \in K[X]/(f(X))$ を

$$\alpha = \nu(X) = X + (f(X))$$

と定めれば（すなわち、 X の属する $K[X]/(f(X))$ の類を α とすれば）、 $f^\sigma(\alpha) = 0$ が成り立つ。

証明 $K[X]$ は PID だから、既約元で生成されるイデアル $(f(X))$ は極大イデアルであり、したがって、それによる剰余環 $K[X]/(f(X))$ は体である。また、 ι, ν はどちらも準同型写像だから、 σ は準同型写像である。いま、

$$f(X) = c_0 + c_1X + \cdots + c_nX^n \quad (c_i \in K)$$

とすれば、 $\iota(c_i) = c_i \in K \subset K[X]$ だから、 $\sigma(c_i) = \nu(c_i)$ 、したがって

$$f^\sigma(\alpha) = \nu(c_0) + \nu(c_1)\nu(X) + \cdots + \nu(c_n)\nu(X)^n = \nu(f(X)) = 0$$

となる。 □

定理 5.6 (クロネッカー) 体 K 上の定数でない任意の多項式 $f(X)$ に対して、 K の拡大体 L とその元 α で $f(\alpha) = 0$ をみたすものが存在する。

証明 $f(X)$ の K 上の既約因子をあらためて $f(X)$ とおくことにより、初めから $f(X)$ は K 上の既約多項式であるとしてよい。このとき、 $L = K[X]/(f(X))$ 、 $\alpha = X + (f(X)) \in L$ とおけば、定理 5.5 より、 L は体であり、単射準同型写像 $\sigma: K \rightarrow L$ が定義できて、 $f^\sigma(\alpha) = 0$ をみたす。そこで、 σ の像 $\sigma(K)$ を K と同一視すればよい。 □

注意 定理 5.6 から、 K 上の既約多項式 $f(X)$ に対して、 K の拡大体 L と $f(X)$ の根 $\alpha \in L$ が存在する。この α を用いて、準同型写像

$$\varphi_\alpha: K[X] \longrightarrow L, \quad g(X) \mapsto g(\alpha)$$

が定義できて、 $\text{Im } \varphi_\alpha = K(\alpha) \subset L$ がわかる (§3 を参照)。一方、 $\text{Ker } \varphi_\alpha$ が $K[X]$ のイデアル $(f(X))$ に一致することが、 $f(X)$ の K 上の既約性から確認できる (定理 3.8 参照)。したがって、準同型定理より、 φ_α は同型写像

$$\tilde{\varphi}_\alpha: K[X]/(f(X)) \longrightarrow K(\alpha)$$

を引き起こす。なお、定理 5.5 の準同型写像 σ と $\tilde{\varphi}_\alpha$ との合成 $\tilde{\varphi}_\alpha \circ \sigma$ は、 K から $K(\alpha)$ への包含写像に他ならない。

例 5.7 $X^2 + 1$ は実数体 $\mathbf{R}$ 上の既約多項式であり, その根 i に対して, $\mathbf{R}(i)$ は剰余環 $\mathbf{R}[X]/(X^2 + 1)$ と同型である. $\mathbf{C} = \mathbf{R}(i)$ とかけば,

$$\mathbf{C} \cong \mathbf{R}[X]/(X^2 + 1).$$

$1, i$ は $\mathbf{C}$ の $\mathbf{R}$ 上の基底であって, $\mathbf{C}$ の任意の元は $a + bi$ ($a, b \in \mathbf{R}$) の形に一意的に表される. ここで, $\mathbf{C}$ の 2 元

$$a + bi, \quad c + di \quad (a, b, c, d \in \mathbf{R})$$

に “対応” する多項式 $a + bX, c + dX \in \mathbf{R}[X]$ の積

$$ac + (ad + bc)X + bdX^2 = (ac - bd) + (ad + bc)X + bd(X^2 + 1)$$

は, $\mathbf{R}[X]/(X^2 + 1)$ においては $(ac - bd) + (ad + bc)X$ と同じ類に属する. つまり

$$(a + bX)(c + dX) \equiv (ac - bd) + (ad + bc)X \pmod{(X^2 + 1)}$$

であり, これはよく知られた複素数における積の公式

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

に対応する. この例は, 虚数単位 i を導入しなくても複素数体が構成できることを示している.

例 5.8 $f(X) = X^3 - 4X + 2$ は $\mathbf{Q}$ 上既約であり, その任意の根 α に対して, $\mathbf{Q}(\alpha)$ は剰余環 $\mathbf{Q}[X]/(f(X))$ と同型である;

$$\mathbf{Q}(\alpha) \cong \mathbf{Q}[X]/(f(X)).$$

$1, \alpha, \alpha^2$ は $\mathbf{Q}(\alpha)$ の $\mathbf{Q}$ 上の基底であり, $\mathbf{Q}(\alpha)$ の任意の元は $1, \alpha, \alpha^2$ の $\mathbf{Q}$ 上の 1 次結合で表される. たとえば

$$\beta = 1 + \alpha^2, \quad \gamma = 3 - 2\alpha + \alpha^2$$

の積は, 次の様に計算される. まず, 多項式の積を計算して得られる 4 次式

$$(1 + X^2)(3 - 2X + X^2) = X^4 - 2X^3 + 4X^2 - 2X + 3$$

を $f(X)$ で割って

$$X^4 - 2X^3 + 4X^2 - 2X + 3 = (X - 2)f(X) + (8X^2 - 12X + 7).$$

このとき, 余り $8X^2 - 12X + 7$ に対応する $\mathbf{Q}(\alpha)$ の元が $\beta\gamma$ である. こうして, 積 $\beta\gamma = 7 - 12\alpha + 8\alpha^2$ が計算できた.

例 5.9 $g(X) = X^3 + X^2 + X + 1$ は $\mathbf{Q}$ 上既約ではなく, $g(X) = (X+1)(X^2+1)$ のように $\mathbf{Q}$ 上の既約因子に分解される. この分解に対応して, 剰余環 $\mathbf{Q}[X]/(g(X))$ は

$$\mathbf{Q}[X]/(g(X)) \cong (\mathbf{Q}[X]/(X+1)) \oplus (\mathbf{Q}[X]/(X^2+1)) \cong \mathbf{Q} \oplus \mathbf{Q}(i).$$

のように体の直和と同型になることが確かめられる. 一般に, 体 K 上の多項式 $g(X)$ が可約であってかつ重根をもたないならば, 剰余環 $K[X]/(g(X))$ は複数個の体の直和と同型である.

定理 5.10 体 K 上の既約多項式 $f(X)$ とその任意の 2 根 α, β に対して, K 上の同型写像

$$\sigma : K(\alpha) \longrightarrow K(\beta)$$

で, $\sigma(\alpha) = \beta$ をみたすものが存在する.

証明 定理 5.6 の後の注意より, $g(X) \in K[X]$ を $g(\alpha)$ または $g(\beta)$ に写すことで定まる準同型写像

$$K[X] \longrightarrow K(\alpha), \quad K[X] \longrightarrow K(\beta)$$

は, 同型写像

$$\tau : K[X]/(f(X)) \longrightarrow K(\alpha), \quad \rho : K[X]/(f(X)) \longrightarrow K(\beta)$$

をそれぞれ引き起こす. このとき, $\sigma = \rho \circ \tau^{-1}$ が求める同型写像となる. $\square$

例 5.11 $X^2 + 1$ のひとつの根を i とすれば, もうひとつの根は $-i$ である. このとき, $\mathbf{C} = \mathbf{R}(i)$ から自分自身への写像

$$\mathbf{C} \longrightarrow \mathbf{C}, \quad a + bi \mapsto a - bi \quad (\text{ただし } a, b \in \mathbf{R})$$

が $\mathbf{R}$ 上の同型写像になっている. この写像は, ふつう複素共役写像とよばれる.

例 5.12 $X^3 - 2$ は $\mathbf{Q}$ 上既約であり, その実根を $\alpha = \sqrt[3]{2}$ とすると, 他の根は $\alpha\omega, \alpha\omega^2$ ($\omega = e^{2\pi i/3}$ は 1 の原始 3 乗根) である. このとき, 3 つの体 $\mathbf{Q}(\alpha), \mathbf{Q}(\alpha\omega), \mathbf{Q}(\alpha\omega^2)$ は互いに同型である. より具体的には, 写像

$$\begin{aligned} \sigma : \mathbf{Q}(\alpha) &\longrightarrow \mathbf{Q}(\alpha\omega), & a + b\alpha + c\alpha^2 &\mapsto a + b\alpha\omega + c\alpha^2\omega^2 \\ \tau : \mathbf{Q}(\alpha) &\longrightarrow \mathbf{Q}(\alpha\omega^2), & a + b\alpha + c\alpha^2 &\mapsto a + b\alpha\omega^2 + c\alpha^2\omega \end{aligned}$$

が $\mathbf{Q}$ 上の同型写像となっている ($a, b, c \in \mathbf{Q}$). $\mathbf{Q}(\alpha)$ は実数体の部分体であり, $\mathbf{Q}(\alpha\omega)$ と $\mathbf{Q}(\alpha\omega^2)$ は実数体には含まれていないが, これら 3 つの体は代数的には同等の性質をもっている.