

§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。

まず、体から体への準同型写像は単射であることに注意する。

【理由】 体 K から体 M への準同型写像 $\sigma: K \rightarrow M$ 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。

…ということは、体から環への零でない準同型写像でも単射だなあ…

定義 5.1 L/K を体の拡大とする。

$$\sigma: L \rightarrow M, \quad \tau: K \rightarrow M$$

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 $\sigma(a) = a$ ($\forall a \in K$) のとき、 σ を K 上の**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

$$L \cong M$$

と表すことがある。

定義 5.4 可換環 R から可換環 S への準同型写像

$$\sigma: R \rightarrow S$$

が与えられたとき、 $f(X) \in R[X]$ 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。

定理 5.5 $f(X)$ を体 K 上の既約多項式とすると、剰余環 $K[X]/(f(X))$ は体である。さらに、

包含写像 $\iota: K \rightarrow K[X]$ および、自然な全射 $\nu: K[X] \rightarrow K[X]/(f(X))$

の合成写像として

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

を定めると、 σ は体の準同型写像であり、 $x = X + (f(X)) \in K[X]/(f(X))$ (つまり $x = \nu(X)$) とおけば、 $f^\sigma(x) = 0$ 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

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

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

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

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 3.7 参照)。したがって、準同型定理より、 φ_α は同型写像

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

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

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

を計算し, $\mathbf{Q}[X]/(f(X))$ における類を考えればよいから, この 4 次式を $f(X)$ で割って余りを求める;

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

こうして, 積 $\beta\gamma = 7 - 12\alpha + 8\alpha^2$ が計算できる.

定理 5.9 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. □

例 5.10 $X^2 + 1$ 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

$$\mathbf{C} \longrightarrow \mathbf{C}, \quad a + bi \mapsto a - bi$$

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

例 5.11 $X^3 - 2$ は \mathbf{Q} 上既約であり, その実根を $\alpha = \sqrt[3]{2}$ とすると, $1, \alpha, \alpha^2$ は $\mathbf{Q}(\alpha)$ の \mathbf{Q} 上の基底である. 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, $\mathbf{Q}(\alpha)$ と $\mathbf{Q}(\alpha\omega)$ は同型であり, 写像

$$\sigma : \mathbf{Q}(\alpha) \longrightarrow \mathbf{Q}(\alpha\omega), \quad a + b\alpha + c\alpha^2 \mapsto a + b\alpha\omega + c\alpha^2\omega^2$$

が同型写像を与えている ($a, b, c \in \mathbf{Q}$). 同様にして, $\mathbf{Q}(\alpha)$ と $\mathbf{Q}(\alpha\omega^2)$ も同型であり, 同型写像は

$$\tau : \mathbf{Q}(\alpha) \longrightarrow \mathbf{Q}(\alpha\omega^2), \quad a + b\alpha + c\alpha^2 \mapsto a + b\alpha\omega^2 + c\alpha^2\omega$$

で与えられる.