

§3. 代数的元

定義 3.1 L/K を体の拡大とし $\alpha \in L$ とする. α を根とする K 上の零でない多項式が存在するとき, すなわち,

$$\exists f(X) \in K[X] - \{0\} \quad \text{s.t.} \quad f(\alpha) = 0$$

であるとき, α は K 上**代数的**であるという. K 上代数的でない元は, K 上**超越的**であるといわれる.

次の補題は上の定義から直ちに導かれる.

補題 3.2 L/K を体の拡大とし $\alpha \in L$ とする. α が K 上代数的ならば, L/K の任意の中間体 M について, α は M 上代数的である.

例 3.3 (1) 体 K のすべての元は K 上代数的である.

(2) $\sqrt{3}, \frac{1+\sqrt{2}}{\sqrt[3]{5}}$ は, どちらも $\mathbf{Q}$ 上代数的である.

(3) 円周率 π は $\mathbf{Q}$ 上超越的である (Lindemann の定理 (1882)).

(4) 自然対数の底 e は $\mathbf{Q}$ 上超越的である (Hermite の定理 (1873)).

以下, L/K を体の拡大とし $\alpha \in L$ とする. いま, α が K 上代数的であるかはいかにかわらず, 写像

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

を考えることができる. φ_α は可換環の準同型写像であり, その像は $K[\alpha]$ だから, 準同型定理によって $K[X]/\text{Ker } \varphi_\alpha$ は $K[\alpha]$ と同型;

$$K[X]/\text{Ker } \varphi_\alpha \cong K[\alpha].$$

ここで, 核は α を根とする K 上の多項式全体

$$\text{Ker } \varphi_\alpha = \{f(X) \in K[X] \mid f(\alpha) = 0\}$$

であり, $K[X]$ のイデアルである.

補題 3.4 α が K 上代数的であれば, $K[\alpha]$ は体である. よって, $K[\alpha] = K(\alpha)$ であり, 変数 X の属する類を α に対応させることによって, 体の同型

$$K[X]/\text{Ker } \varphi_\alpha \cong K(\alpha)$$

が得られる.

証明 可換環の同型 $K[X]/\text{Ker } \varphi_\alpha \cong K[\alpha]$ において, $K[\alpha]$ は体 L の部分環だから整域, したがって $\text{Ker } \varphi_\alpha$ は $K[X]$ の素イデアルである. ここで, α が K 上代数的だから, $\text{Ker } \varphi_\alpha \neq (0)$ である. よって, $K[X]$ が PID であることを考慮すると, $\text{Ker } \varphi_\alpha$ は $K[X]$ の極大イデアル, したがって $K[\alpha]$ は体である. $\square$

注意 α が K 上超越的ならば, $\text{Ker } \varphi_\alpha = (0)$, すなわち $K[X] \cong K[\alpha]$ である. とくに, $K[\alpha]$ は体ではない.

補題 3.5 α が K 上代数的で, $f(X)$ が α を根にもつ K 上の m 次多項式 ($m > 0$) ならば, $K(\alpha)$ は K 上のベクトル空間として $1, \alpha, \alpha^2, \dots, \alpha^{m-1}$ によって生成される. とくに

$$[K(\alpha) : K] \leq m = \deg f.$$

証明 前補題から $K[\alpha] = K(\alpha)$ であることに注意すれば, 任意の $\beta \in K(\alpha)$ に対して, $\beta = g(\alpha)$ をみたす $g(X) \in K[X]$ が存在する. このとき,

$$g(X) = q(X)f(X) + r(X), \quad r(X) = 0 \text{ または } \deg r < m = \deg f$$

をみたす $q(X), r(X) \in K[X]$ がとれるが, $f(\alpha) = 0$ より

$$\beta = g(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha).$$

そこで, $r(X) = a_0 + a_1X + a_2X^2 + \dots + a_{m-1}X^{m-1} \in K[X]$ と表しておけば

$$\beta = a_0 + a_1\alpha + a_2\alpha^2 + \dots + a_{m-1}\alpha^{m-1} \quad (a_i \in K)$$

と書けるから, $K(\alpha)$ は K 上 $1, \alpha, \alpha^2, \dots, \alpha^{m-1}$ によって生成される. $\square$

補題 3.6 $K(\alpha)/K$ が有限次拡大ならば, α を根にもつ多項式 $f(X) \in K[X]$ で

$$[K(\alpha) : K] = \deg f$$

をみたすものが存在する. とくに, α は K 上代数的である.

証明 $n = [K(\alpha) : K]$ とすると, $n+1$ 個の元 $1, \alpha, \alpha^2, \dots, \alpha^n$ は K 上 1 次従属, よって (どれかは 0 ではない) $c_i \in K$ が存在して

$$c_0 + c_1\alpha + c_2\alpha^2 + \dots + c_n\alpha^n = 0$$

が成り立つ. そこで, $f(X) \in K[X]$ を

$$f(X) = c_0 + c_1X + c_2X^2 + \dots + c_nX^n$$

と定めれば, $f(X)$ は α を根とする零でない K 上の多項式であり, 補題 3.5 より

$$[K(\alpha) : K] \leq \deg f \leq n.$$

さらに, n の定義より, 不等号は等号に置き換わり $[K(\alpha) : K] = \deg f$ を得る. $\square$

定理 3.7 α に対して次は同値である.

- (i) α は K 上代数的である.
- (ii) $K(\alpha)/K$ は有限次拡大である.

証明 補題 3.5 と補題 3.6 からわかる. □

定理 3.8 α が K 上代数的であるとき, α を根にもつ $f(X) \in K[X]$ に対して次は同値である.

- (i) $f(X)$ は K 上既約である.
- (ii) $\text{Ker } \varphi_\alpha = (f(X))$.
- (iii) $[K(\alpha) : K] = \deg f$.
- (iv) $f(X)$ の次数は最小である. すなわち, $g(X) (\neq 0) \in K[X]$ が α を根にもつならば, $\deg f \leq \deg g$.

証明 まず, $f(\alpha) = 0$ より $f(X) \in \text{Ker } \varphi_\alpha$, 言い換えれば $(f(X)) \subset \text{Ker } \varphi_\alpha$ が成り立つことに注意する.

(i) $\Rightarrow$ (ii): (i) を仮定すれば, 単項イデアル $(f(X))$ は極大イデアルなので, (ii) を得る.
(ii) $\Rightarrow$ (iii): 補題 3.5 から $[K(\alpha) : K] \leq \deg f$ が成り立つ. とくに $K(\alpha)/K$ は有限次だから, 補題 3.6 を用いれば, $[K(\alpha) : K] = \deg g$ をみたす $g(X) \in \text{Ker } \varphi_\alpha$ がとれ, さらに仮定 (ii) より $g(X) = f(X)h(X)$ ($h(X) \in K[X]$) と表される. よって

$$[K(\alpha) : K] \leq \deg f \leq \deg f + \deg h = \deg g = [K(\alpha) : K],$$

したがって $[K(\alpha) : K] = \deg f$ を得る.

(iii) $\Rightarrow$ (iv): 補題 3.5 からすぐにわかる.

(iv) $\Rightarrow$ (i): $f(X)$ が K 上可約だとすると,

$$f(X) = g(X)h(X), \quad 1 \leq \deg g, \deg h < \deg f$$

をみたす $g(X), h(X) \in K[X]$ が存在する. ここで $g(\alpha)h(\alpha) = f(\alpha) = 0$ だから, $g(\alpha) = 0$ または $h(\alpha) = 0$ である. $g(\alpha) = 0$ のとき, 仮定 (iv) より $\deg f \leq \deg g$ となって $g(X)$ の取り方に矛盾する. $h(\alpha) = 0$ の場合も同様に矛盾する. よって $f(X)$ は K 上既約でなければならない. □

定義 3.9 前定理の (i)-(iv) のどれか (したがってすべて) をみたす多項式 $f(X) \in K[X]$ のうちモニックなものは一意的に定まる. これを α の K 上の**最小多項式**という. ここで, モニックな多項式とは, 最高次の係数が 1, すなわち

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$$

の形をした多項式のことである.

定理 3.10 α が K 上代数的ならば, α の K 上の最小多項式が存在する.

証明 定理 3.7, 補題 3.6 および最小多項式の定義から直ちに導かれる. $\square$

定理 3.11 $K(\alpha)/K$ が有限次拡大で $[K(\alpha) : K] = n$ ならば,

$$1, \alpha, \alpha^2, \dots, \alpha^{n-1}$$

は K 上ベクトル空間としての $K(\alpha)$ の基底である.

証明 $f(X)$ を α の K 上の最小多項式とすると, $n = \deg f$ である. さらに $f(\alpha) = 0$ であるから, 補題 3.5 から, n 個の元 $1, \alpha, \dots, \alpha^{n-1}$ は K 上 $K(\alpha)$ を生成している. 一方, $K(\alpha)$ は K 上 n 次元のベクトル空間だから, これらは基底となる. $\square$

例 3.12 (1) $\sqrt{3}$ の $\mathbf{Q}$ 上の最小多項式は $X^2 - 3$.

(2) $1 - \sqrt{5}$ の $\mathbf{Q}$ 上の最小多項式は $X^2 - 2X - 4$.

(3) $\frac{1}{\sqrt[3]{7}}$ の $\mathbf{Q}$ 上の最小多項式は $X^3 - \frac{1}{7}$.

(4) $\sqrt{2} + \sqrt[3]{3}$ の $\mathbf{Q}$ 上の最小多項式は $X^6 - 6X^4 - 6X^3 + 12X^2 - 36X + 1$.

最後の例は, たとえば, 以下を順に示すことで得られる; ただし,

$$\alpha = \sqrt{2} + \sqrt[3]{3}, \quad f(X) = X^6 - 6X^4 - 6X^3 + 12X^2 - 36X + 1$$

とする.

(a) $f(\alpha) = 0$ より $[\mathbf{Q}(\alpha) : \mathbf{Q}] \leq \deg f = 6$ (補題 3.5)

(b) $\sqrt[3]{3} = \alpha - \sqrt{2}$ の両辺を 3 乗することにより, $\sqrt{2} \in \mathbf{Q}(\alpha)$

(c) $\mathbf{Q}(\alpha) = \mathbf{Q}(\sqrt{2}, \sqrt[3]{3})$

(d) $[\mathbf{Q}(\alpha) : \mathbf{Q}]$ は 2 でも 3 でも割り切れる (定理 2.9) から, $[\mathbf{Q}(\alpha) : \mathbf{Q}] \geq 6$

(e) (a), (d) をあわせて, $[\mathbf{Q}(\alpha) : \mathbf{Q}] = 6 = \deg f$

(f) $f(X)$ は α の最小多項式であり, さらに $\mathbf{Q}$ 上既約である (定理 3.8).