§10. 可解性

以下において扱う体はすべて $\mathbb{C}$ の部分体とする．$X^n - a \quad (a \in \mathbb{C})$ の形の多項式を 2 項式という．

定義 10.1 L/K を体の拡大とする．

(1) K 上の既約 2 項式 $X^n - a$ $(a \in K)$ の根 α によって $L = K(\alpha)$ と表されるとき，L/K を 2 **項拡大**という．

(2) 体の列 $K_0, K_1, \cdots, K_m$ で，

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_{m-1} \subset K_m = L$$
$$K_i/K_{i-1} \text{ は 2 項拡大 } (i = 1, 2, \cdots, m)$$

をみたすものが存在するとき，L/K を**ベキ根拡大**という．

定義 10.2 α を K 上代数的な元とする．$\alpha \in L$ をみたすベキ根拡大 L/K が存在するとき，α は K 上**ベキ根によって表される**という．

定義 10.3 $f(X) \in K[X]$ とする．$f(X)$ の任意の根が K 上ベキ根によって表されるとき，$f(X)$ は K 上**ベキ根によって解ける**，または**ベキ根によって可解である**という．

例 10.4 体 K 上のすべての 2 次式は K 上ベキ根によって解ける．

例 10.5 1 の原始 3 乗根 $\omega = e^{\frac{2\pi\sqrt{-1}}{3}}$ について，$L = \mathbb{Q}(\omega)$ とおく．$\omega^3 = 1$ かつ $\omega \neq 1$ より $\omega^2 + \omega + 1 = 0$ だから，

$$\omega = \frac{-1 \pm \sqrt{-3}}{2},$$

よって，$L = \mathbb{Q}\big(\sqrt{-3}\big)$ であって $L/\mathbb{Q}$ は 2 項拡大，したがって，ω は $\mathbb{Q}$ 上ベキ根によって表される．

例 10.6　ζ を 1 の原始 5 乗根とすると，$\zeta^4+\zeta^3+\zeta^2+\zeta+1=0$．これを ζ^2 で割って

$$\zeta^2+\zeta+1+\frac{1}{\zeta}+\frac{1}{\zeta^2}=0.$$

そこで，$\eta=\zeta+\dfrac{1}{\zeta}$ とおけば，$\eta^2=\zeta^2+\dfrac{1}{\zeta^2}+2$ だから

$$\eta^2+\eta-1=0,\qquad \therefore \eta=\frac{-1\pm\sqrt{5}}{2}.$$

一方，$\zeta^2-\eta\zeta+1=0$ より

$$\zeta=\frac{\eta\pm\sqrt{\eta^2-4}}{2}$$

であるから，2 項拡大の列

$$\mathbb{Q}\subset\mathbb{Q}(\sqrt{5})\subset\mathbb{Q}(\sqrt{5},\sqrt{\eta^2-4})$$

が得られ，$\zeta\in\mathbb{Q}(\sqrt{5},\sqrt{\eta^2-4})$．このことから，$\zeta$ は $\mathbb{Q}$ 上ベキ根によって表されることがわかる．

定理 10.7　n を自然数とし，体 K は 1 の原始 n 乗根 ζ を含むとする．$a\in K^\times$ に対して，$\alpha^n=a$ をみたす α を任意にひとつとり $L=K(\alpha)$ とおく．

(1) L は X^n-a の K 上の最小分解体である．

(2) X^n-a が K 上既約ならば，α の K 上の最小多項式は X^n-a であり，L/K は n 次巡回拡大であり，$\sigma(\alpha)=\zeta\alpha$ であるような K 上の自己同型 σ によって $\mathrm{Gal}(L/K)$ が生成される；　$\mathrm{Gal}(L/K)=\{1,\sigma,\sigma^2,\dots,\sigma^{n-1}\}$．

証明　(1) X^n-a のすべての根は $\alpha,\zeta\alpha,\zeta^2\alpha,\dots\zeta^{n-1}\alpha$ だが，$\zeta\in K$ より最小分解体は $K(\alpha)=L$ と一致する．
(2) X^n-a が K 上の最小多項式であることと $[L:K]=n$ であることは，§3 からわかる．また，L/K がガロア拡大であることは (1) よりわかる．$G=\mathrm{Gal}(L/K)$ とおく．X^n-a の根 $\zeta^i\alpha$ に対して，§6 の結果より，$\sigma_i(\alpha)=\zeta^i\alpha$ をみたす $\sigma_i\in G$ が存在するが，$\zeta^i\alpha$ $(i=0,\dots,n-1)$ がすべての根であることより，$G=\{\sigma_0,\sigma_1,\dots,\sigma_{n-1}\}$．ここで，$\sigma=\sigma_1$ とおけば，$\sigma^2(\alpha)=\sigma(\zeta\alpha)=\zeta\sigma(\alpha)=\zeta\cdot\zeta\alpha=\zeta^2\alpha$ であり，一般に $\sigma^i(\alpha)=\zeta^i\alpha=\sigma_i(\alpha)$，したがって $\sigma^i=\sigma_i$ $(i=0,\dots,n-1)$ であることが順次確かめられる．とくに，$\sigma^n=\sigma^0=\sigma_0=\mathrm{id}_K(=1)$ であり，$G=\{1,\sigma,\sigma^2,\dots,\sigma^{n-1}\}$ が得られた．　□

補題 10.8 (デデキント) Γ を乗法群とし，$\sigma_1, \ldots, \sigma_n$ を Γ から $\mathbb{C}^\times$ への相異なる準同型写像とする．このとき，$(c_1, \ldots, c_n) \neq (0, \ldots, 0)$ をみたす任意の $c_1, \ldots, c_n \in \mathbb{C}$ に対して

$$\sum_{i=1}^{n} c_i \sigma_i(\gamma) = c_1\sigma_1(\gamma) + \cdots + c_n\sigma_n(\gamma) \neq 0$$

をみたす $\gamma \in \Gamma$ が存在する．

証明 対偶，すなわち，$c_1, \ldots, c_n \in \mathbb{C}$ とするとき，

$$\forall \gamma \in \Gamma \text{ に対して}, \sum_{i=1}^{n} c_i \sigma_i(\gamma) = 0 \quad \Longrightarrow \quad c_1 = \cdots = c_n = 0$$

を n に関する数学的帰納法によって示す．$n = 1$ のとき，$c_1\sigma_1(\gamma) = 0$ かつ $\sigma_1(\gamma) \neq 0$ より $c_1 = 0$．次に，$n > 1$ として，$n-1$ のときは成り立つと仮定し，任意の $\gamma \in \Gamma$ について

$$c_1\sigma_1(\gamma) + \cdots + c_n\sigma_n(\gamma) = 0$$

とする．いま，$\sigma_1 \neq \sigma_n$ だから，$\sigma_1(\beta) \neq \sigma_n(\beta)$ であるような $\beta \in \Gamma$ がとれる．上式の γ の代わりに $\beta\gamma$ を用いれば，

$$c_1\sigma_1(\beta)\sigma_1(\gamma) + \cdots + c_n\sigma_n(\beta)\sigma_n(\gamma) = 0.$$

これと，はじめの式に $\sigma_n(\beta)$ をかけたものの差を取れば，$\sigma_n(\gamma)$ が消去されて，

$$c_1(\sigma_1(\beta) - \sigma_n(\beta))\sigma_1(\gamma) + \cdots + c_n(\sigma_{n-1}(\beta) - \sigma_n(\beta))\sigma_{n-1}(\gamma) = 0$$

が任意の $\gamma \in \Gamma$ について成り立つ．よって，帰納法の仮定より，とくに

$$c_1(\sigma_1(\beta) - \sigma_n(\beta)) = 0$$

が得られるが，β の取り方から $c_1 = 0$ でなければならない．そこで，再び帰納法の仮定から $c_2 = \cdots = c_n = 0$ を得る． □

定理 10.9 n を自然数とし，体 K は 1 の原始 n 乗根 ζ を含むとする．このとき，K 上の n 次巡回拡大は 2 項拡大である．すなわち L/K が n 次巡回拡大ならば，ある $a \in K$ が存在して，$\alpha^n = a$ をみたす α によって $L = K(\alpha)$ と表される．

証明 $\mathrm{Gal}(L/K) = \langle\sigma\rangle = \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$ とする． いま，$\Gamma = L^\times$, $\sigma_i = \sigma^{i-1}$ および $c_i = \zeta^{-(i-1)}$ $(i = 1, \ldots, n)$ として前補題を適用すれば，

$$\sum_{i=0}^{n-1} \zeta^{-i}\sigma^i(\gamma) = \gamma + \zeta^{-1}\sigma(\gamma) + \cdots + \zeta^{-(n-1)}\sigma^{n-1}(\gamma) \neq 0.$$

これを α とすると，

$$\zeta^{-1}\sigma(\alpha) = \sum_{i=0}^{n-1} \zeta^{-i-1}\sigma^{i+1}(\gamma) = \alpha,$$

両辺を n 乗して $\sigma(\alpha^n) = \alpha^n$ を得る． したがって $a = \alpha^n$ とおけば $a \in K$ となる． さらに，$\sigma(\alpha) = \zeta\alpha$ より，$\mathrm{Conj}(\alpha, K) = \{\alpha, \zeta\alpha, \zeta^2\alpha, \ldots, \zeta^{n-1}\alpha\}$ であるが，$\alpha \neq 0$ なので $|\mathrm{Conj}(\alpha, K)| = n$，したがって $X^n - a$ が α の K 上の最小多項式でなければならず，$L = K(\alpha)$ が得られる． □

定理 10.10 有限次アーベル拡大 L/K に対して，中間体の列 $K_1, \cdots, K_r$ で，

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_{r-1} \subset K_r = L$$
$$K_i/K_{i-1} \text{ は巡回拡大 } (i = 1, 2, \cdots, r)$$

をみたすものが存在する．

定理 10.11 n を自然数とし，体 K は 1 の原始 n 乗根を含むとする． このとき任意の n 次アーベル拡大 L/K はベキ根拡大である．

補題 10.12 n を自然数とし，ζ を 1 の原始 n 乗根とすると，体 K に対して $K(\zeta)/K$ は n より低い次数のアーベル拡大である．

補題 10.13 L/K がガロア拡大ならば，任意の拡大 M/K に対して LM/M もガロア拡大であり，さらに $\mathrm{Gal}(LM/M)$ は $\mathrm{Gal}(L/K)$ の部分群と同型である． とくに，L/K がアーベル拡大ならば LM/M もアーベル拡大，L/K が巡回拡大ならば LM/M も巡回拡大である．

定理 10.14 n を自然数とし，ζ を 1 の原始 n 乗根とすると，任意の体 K に対して ζ は K 上ベキ根で表される．

定理 10.15 有限次アーベル拡大 L/K に対して，ベキ根拡大 L'/K で $L \subset L'$ をみたすものが存在する．

定理 10.16 $f(X) \in K[X]$ の K 上の最小分解体を L とする． $f(X)$ がベキ根によって可解であるための必要十分条件は $\mathrm{Gal}(L/K)$ が可解群となることである．