§10. 可解性

以下において扱う体はすべて $\boldsymbol{C}$ の部分体とする．
$X^n - a \quad (a \in \boldsymbol{C})$ 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 K 上**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 次多項式は K 上ベキ根によって解ける． なぜなら，すべての 2 次式 $f(X) = X^2 + bX + c$ は

$$f(X) = \left(X + \frac{b}{2}\right)^2 - \left(\frac{b^2}{4} - c\right)$$

と変形でき，2 項式に帰着できるからである．

例 10.5 体 K に対して，1 のべき根は K 上べき根によって表される． この事実は当たり前のように思えるが，$n > 1$ のとき 2 項式 $X^n - 1$ は K 上既約ではないので，現段階では簡単には確認することができない． 証明はこの節の終盤で行われる (定理 10.16)． なお，$n = 3, 5$ の場合は以下の例を参照せよ．

例 10.6　1 の原始 3 乗根 $\omega = e^{\frac{2\pi\sqrt{-1}}{3}}$ について，$L = \boldsymbol{Q}(\omega)$ 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，$L = \boldsymbol{Q}\big(\sqrt{-3}\big)$ であって $L/\boldsymbol{Q}$ は 2 項拡大，したがって，ω は $\boldsymbol{Q}$ 上ベキ根によって表される．

例 10.7　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

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

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

定理 10.8　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（すなわち α の K 上の最小多項式）ならば，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；　$\mathrm{Gal}(L/K) = \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$．

(3) $\alpha^l \in K$ であるような最小の自然数 l が存在し，この l に対して $X^l - \alpha^l$ は K 上既約である．この場合，とくに L/K は l 次巡回拡大である．

証明 (1) $X^n - a$ のすべての根は $\alpha, \zeta\alpha, \zeta^2\alpha, \ldots \zeta^{n-1}\alpha$ であるが，$\zeta \in K$ より最小分解体は $K(\alpha) = L$ と一致する．
(2) $X^n - a$ が K 上既約なので，$[L : K] = n$ がわかる． 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，$\sigma_i(\alpha) = \zeta^i\alpha$ をみたす $\sigma_i \in G$ が存在するが，$\zeta^i\alpha$ $(i = 0, \ldots, n-1)$ がすべての根であることより，$G = \{\sigma_0, \sigma_1, \ldots, \sigma_{n-1}\}$． 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 $\sigma^i = \sigma_i$ $(i = 0, \ldots, n-1)$ 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，$G = \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$ が得られた．
(3) $\alpha^n = a \in K$ だから，l の存在は明らかである． いま，$\xi = \zeta^{n/l}$ とおけば，ξ は 1 の原始 l 乗根であり，$X^l - \alpha^l$ のすべての根は $\xi^i\alpha$ $(i = 1, \ldots, l-1)$ である． よって，もし $X^l - \alpha^l$ が K 上可約ならば，その既約因子の定数項は $\xi^j\alpha^r$ $(1 \le r < l)$ の形をしていて，かつ K に属している． しかし，$\xi = \zeta^{n/l} \in K$ より $\alpha^r \in K$ となって l の最小性に矛盾する． □

定義 10.9 前定理のようにして与えられる拡大 L/K を**クンマー拡大**という． すなわち，L/K がクンマー拡大であるとは，K が 1 の原始 n 乗根 ζ を含み，ある $a \in K^\times$ について $\alpha^n = a$ をみたす α によって $L = K(\alpha)$ と表されることである．
前定理 (3) より，クンマー拡大は 2 項拡大であることに注意せよ．

補題 10.10 (デデキント) Γ を乗法群とし，$\sigma_1, \ldots, \sigma_n$ を Γ から $\boldsymbol{C}^\times$ 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 $c_1, \ldots, c_n \in \boldsymbol{C}$ 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，$c_1, \ldots, c_n \in \boldsymbol{C}$ 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 10.11　n を自然数とし，体 K は 1 の原始 n 乗根 ζ を含むとする． もし 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． すなわち，K 上の n 次巡回拡大はクンマー拡大，したがって 2 項拡大である．

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，

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

をみたす $\gamma \in L$ が存在する． この和を α とすると，$\alpha \in L$ であって

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

両辺を n 乗して $\sigma(\alpha^n) = \alpha^n$ を得る．したがって $\alpha^n \in K$ であり，$X^n - \alpha^n \in K[X]$ 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 $X^n - \alpha^n$ 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． □

補題 10.12　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．

証明 L/K の次数に関する数学的帰納法によって示す．1 次のときは自明だから，$[L:K]>1$ として $G=\mathrm{Gal}(L/K)$ とおく．$1\neq\sigma\in G$ をひとつとって $H=\langle\sigma\rangle$ とし，対応する L/K の中間体を M とすると，L/M は巡回拡大である．一方，L/K はアーベル拡大だから，系 9.10 (2) より M/K もアーベル拡大だが，$[M:K]<[L:K]$ だから，帰納法の仮定より各拡大が巡回拡大である中間体の列 $K=K_0\subset K_1\subset\cdots\subset K_s=M$ がとれる．これと $M\subset L$ を合わせれば証明が完了する．□

定理 10.13 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．

証明 前補題のように中間体の列 $K=K_0,K_1,\cdots,K_r=L$ をとる．各 $i=1,\ldots,r$ について K_i/K_{i-1} は巡回拡大でありその次数 n_i は n の約数となり，とくに K_{i-1} は 1 の原始 n_i 乗根を含むから，定理 10.11 より K_i/K_{i-1} は 2 項拡大である．よって L/K はベキ根拡大となる．□

補題 10.14 n を 1 より大きい自然数とし，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．

証明 任意の $\sigma\in\mathrm{Aut}(\overline{K}/K)$ に対して $\sigma(\zeta)^n=\sigma(\zeta^n)=\sigma(1)=1$ だから，$\sigma(\zeta)=\zeta^j$ をみたす j が存在する．とくに $\sigma(\zeta)\in K(\zeta)$ だから $K(\zeta)/K$ はガロア拡大である．一方，σ は同型写像だから ζ^j も 1 の原始 n 乗根であり，したがって $\gcd(j,n)=1$ が成り立つ．このことより $j\in(\boldsymbol{Z}/n\boldsymbol{Z})^\times$（法 n に関する既約剰余類群）であるとしてよいから，$K(\zeta)/K$ のガロア群 G から $(\boldsymbol{Z}/n\boldsymbol{Z})^\times$ への写像が定まることがわかる．この写像が単射準同型であることを確かめるのは難しくない．よって，G は $(\boldsymbol{Z}/n\boldsymbol{Z})^\times$ の部分群に同型であり証明が完了する．□

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．

証明 L/K の次数に関する数学的帰納法による．$n=[L:K]>1$ とする．ζ を 1 の原始 n 乗根とすれば，前補題より，$K(\zeta)/K$ に対して帰納法の仮定が適用でき，べき根拡大 M/K で $K(\zeta)\subset M$ をみたすものがとれる．ここで，定理 9.12 より LM/M はアーベル拡大でその次数 m は n の約数なので，M は 1 の原始 m 乗根を含む．よって，定理 10.13 から LM/M はべき根拡大，したがって LM/K はべき根拡大である．□

定理 10.16 (ガウス) 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．

証明 補題 10.14 から $K(\zeta)/K$ はアーベル拡大であり，定理 10.15 より $K(\zeta) \subset L$ をみたすべき根拡大 L/K がとれる． よって ζ は K 上べき根で表される． □

定理 10.17 有限次可解拡大 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．

証明 L/K の次数に関する数学的帰納法による． 次数 1 の場合は自明なので，以下，$[L : K] > 1$ とする． $G = \mathrm{Gal}(L/K)$ は可解群だから，正規部分群 $H \subsetneq G$ で G/H がアーベル群であるものがとれる． H に対応する L/K の中間体を M とすると，M/K はアーベル拡大だから，定理 10.15 より，べき根拡大 M'/K で $M \subset M'$ であるものがとれる． ここで，定理 9.12 より，拡大 LM'/M' はガロア拡大でそのガロア群は H の部分群と同型だから $[LM' : M'] \leq |H| < |G| = [L : K]$. 一方，$H$ が可解群であることから，LM'/M' は可解拡大である． したがって，LM'/M' に対して帰納法の仮定が適用でき，べき根拡大 L'/M' で $LM' \subset L'$ をみたすものがとれる． M'/K とあわせて，L' は L を含む K 上のべき根拡大となる． □

定理 10.18 べき根拡大 L/K に対して，有限次可解拡大 L'/K で $L \subset L'$ をみたすものが存在する．

証明 L/K の次数に関する数学的帰納法によって示す． 次数 1 のときは明らかだから，以下では $[L : K] > 1$ とする． L/K はべき根拡大だから，$K \subset M \subsetneq L$ で，L/M が 2 項拡大，M/K がべき根拡大であるような中間体 M がとれる． $M \subsetneq L$ より $[M : K] < [L : K]$ だから，帰納法の仮定より，有限次可解拡大 M'/K で $M \subset M'$ をみたすものが存在する． いま，$n = [L : M]$ とし，ζ を 1 の原始 n 乗根とする． 補題 10.14 から $K(\zeta)/K$ はアーベル拡大，したがって，定理 9.13 (2) より，$K(\zeta)$ と M' の合成である $M'(\zeta)$ は K 上の可解拡大体である． そこで，$M'(\zeta)$ をあらためて M' とおくことによって，$\zeta \in M'$ であるとしてよい．

一方，$\tilde{L}$ を拡大 L/K の正規閉包 (定義 8.12) とすると，$\tilde{L}$ は K 上ガロアであり，さらに M' との合成体を $L' = \tilde{L}M'$ とすれば，定理 9.13 (1) より L'/K はガロア拡大である． いま，L'/K のガロア群を G とし，中間体 M' に対応する部分群を H とする． M'/K が可解拡大ということは，H が G の正規部分群で，かつ G/H が可解群であることを示している． このことから，H が可解群であるこ

とを示せば，群論の一般論から，G が可解群，すなわち L'/K が可解拡大であることが導かれ証明が完了する． そのためには，$H = \mathrm{Gal}(L'/M')$ がアーベル群であることを確かめれば十分である． そこで，以下において，L'/M' がアーベル拡大となることを示す．

まず，M' が 1 の原始 n 乗根 ζ を含んでいることと，L/M が n 次の 2 項拡大であることから，LM'/M' はクンマー拡大，したがってアーベル拡大であることがわかる． 同様に，任意の $\sigma \in \mathrm{Aut}(\overline{K}/K)$ に対して，拡大 $\sigma(L)\sigma(M')/\sigma(M')$ もアーベル拡大であるが，M'/K がガロアなので $\sigma(M') = M'$，よって $\sigma(L)M'$ は M' 上アーベルである． 次に，定理 7.12 を用いて，$L = K(\alpha)$ となる $\alpha \in L$ をとる．$\mathrm{Conj}(\alpha, K) = \{\alpha_1, \ldots, \alpha_r\}$ とすると，$\sigma_i(\alpha) = \alpha_i$ をみたす $\sigma_i \in \mathrm{Aut}(\overline{K}/K)$ が存在する (定理 6.12)．このとき，定理 8.13 から，L/K の正規閉包 $\tilde{L}$ は $\sigma_1(L), \ldots, \sigma_r(L)$ の合成体として表せることがわかる;

$$\prod_i^r \sigma_i(L) = \prod_i^r K(\sigma_i(\alpha)) = K(\alpha_1, \ldots, \alpha_r) = \tilde{L}.$$

上で示したように，各 i について $\sigma_i(L)M'$ は M' 上アーベルなので，定理 9.13 (2) を使えば，これらの合成体 $\tilde{L}M' = L'$ も M' 上アーベルであることが導かれ証明が完了する． □

定理 10.19 (ガロア) $f(X) \in K[X]$ の K 上の最小分解体を L とする． $f(X)$ が K 上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．

証明 $\mathrm{Gal}(L/K)$ が可解群，すなわち L/K が可解拡大ならば，定理 10.17 から，$f(X)$ が K 上べき根によって解けることが直ちにわかる． 逆を示すために，$f(X)$ が K 上べき根によって可解であるとする． すなわち $f(X)$ の任意の根 α に対して，べき根拡大 L_α/K が存在して $\alpha \in L_\alpha$ をみたすが，ここで定理 10.18 を用いれば，$L_\alpha \subset L'_\alpha$ をみたす可解拡大 L'_α/K がとれる． そこで，$f(X)$ のすべての根 α にわたる合成体

$$\tilde{L} = \prod_\alpha L'_\alpha$$

を考えると，定理 9.13 (2) より，$\tilde{L}/K$ は可解拡大であり，さらに $f(X)$ の任意の根 α について $\alpha \in L_\alpha \subset L'_\alpha \subset \tilde{L}$ より $L \subset \tilde{L}$ が成り立つ． 最後に，L/K はガロア拡大だから $\mathrm{Gal}(\tilde{L}/L)$ は $\mathrm{Gal}(\tilde{L}/K)$ の正規部分群であり，したがって系 9.10 (3) より L/K が可解拡大であることがわかる． □