§13.　クンマー拡大

以下において扱う体はすべて $\boldsymbol{C}$ の部分体とする．また，自然数 n に対して，$\zeta_n \in \boldsymbol{C}$ を 1 の原始 n 乗根とする．すなわち，$\zeta_n \in \boldsymbol{C}^{\times}$ であって，その位数が n であるとする（$\zeta_n = e^{2\pi i/n}$ であるとしてよい）．

定理 13.1　n を自然数とし，K が 1 の原始 n 乗根 ζ_n 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，$\sigma(\alpha) = \zeta_n\alpha$ をみたす K 上の自己同型 σ によって $\mathrm{Gal}(L/K)$ が生成される;

$$\mathrm{Gal}(L/K) = \langle\sigma\rangle = \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}.$$

(3) $\alpha^l \in K$ である最小の自然数 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，L/K は l 次巡回拡大である．

証明　(1) は例 9.11 ですでに示した．以下，$\zeta = \zeta_n$ と略記する．
(2) 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．$X^n - a$ が α の K 上の最小多項だから，G の位数は $[L : K] = n$ である．さらに，$X^n - a$ の根 $\zeta^i\alpha$ $(i = 0, 1, \ldots, n-1)$ に対して，$\sigma_i(\alpha) = \zeta^i\alpha$ をみたす $\sigma_i \in G$ が存在し，これらによって G が尽くされる; $G = \{\sigma_0, \sigma_1, \ldots, \sigma_{n-1}\}$．ここで，$\sigma = \sigma_1$ とおけば，

$$\sigma^2(\alpha) = \sigma(\zeta\alpha) = \zeta\sigma(\alpha) = \zeta \cdot \zeta\alpha = \zeta^2\alpha = \sigma_2(\alpha).$$

一般に $\sigma^i(\alpha) = \zeta^i\alpha = \sigma_i(\alpha)$ が順次確かめられ，とくに $\sigma^n(\alpha) = \alpha$ より $\sigma_n = \mathrm{id}_L(= 1)$．さらに $\sigma^i = \sigma_i$ $(i = 0, 1, \ldots, n-1)$ であることから，$G = \{1, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$，よって L/K は n 次巡回拡大である．
(3) 最小の l が存在することはあきらかであり，さらに l が n の約数であることを示すのも難しくない．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 $g(X) \in K[X]$ は，$1 \leq d < l$ と $0 \leq i_1 < \cdots < i_d \leq l-1$ を用いて

$$g(X) = (X - \xi^{i_1}\alpha) \cdots (X - \xi^{i_d}\alpha)$$

と表され，とくに，その定数項は $g(0) = \pm\xi^{i_1+\cdots+i_d}\alpha^d \in K$ となる．一方，$\xi = \zeta^{n/l} \in K$ より $\alpha^d \in K$ でなければならないが，これは l の最小性に矛盾する．　□

定義 13.2　前定理のようにして与えられる拡大 L/K を自然数 n に関する**クンマー拡大**という．すなわち，体の拡大 L/K が n に関する**クンマー拡大**であるとは，K が 1 の原始 n 乗根 ζ_n 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．クンマー拡大は，しばしば $L = K(\sqrt[n]{a})$ とも表される．

定義 13.3　L/K を体の拡大とする．

(1) $X^n - a$ $(a \in K^\times)$ の形の K 上の既約多項式の根 α によって $L = K(\alpha)$ と表すことができるとき，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 13.4　L/K を代数拡大とする．中間体の列 $K_0, K_1, \cdots, K_m$ で，

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_{m-1} \subset K_m = L$$
$$K_i/K_{i-1} \text{ はアーベル拡大 } \ (i = 1, 2, \cdots, m)$$

をみたすものがとれるとき，L/K を**塁アーベル拡大**という．

この節と次の節で，**ベキ根拡大と有限次塁アーベル拡大との密接な関係**，すなわち，これらの拡大が “本質的” に同等であることを述べる（定理 13.6 および定理 14.2 を参照）．

注意　定理 13.1 において，$X^n - a$ が K 上既約ならば L/K はあきらかに 2 項拡大であるが，たとえ既約でなくても，(3) より，やはり 2 項拡大になる．すなわち，一般にクンマー拡大は 2 項拡大，したがってベキ根拡大である．

補題 13.5　n を 1 より大きい自然数とする．体 K に対して $K(\zeta_n)/K$ は n より低い次数のアーベル拡大である．

証明　$\zeta = \zeta_n$ と略す．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．$\sigma(\zeta) \in K(\zeta)$ だから $K(\zeta)/K$ はガロア拡大である．そのガロア群を G とおき，あらためて $\sigma \in G$ に対して $\sigma(\zeta) = \zeta^j$ をみたす j を j_σ とおく．ここで σ は同型写像だから，ζ^{j_σ} も 1 の原始 n 乗根であり，したがって

$\gcd(j_\sigma, n) = 1$ が成り立つ．よって，$j_\sigma \in (\boldsymbol{Z}/n\boldsymbol{Z})^\times$（法 n に関する既約剰余類群）であるとしてよく，写像

$$G \longrightarrow (\boldsymbol{Z}/n\boldsymbol{Z})^\times, \qquad \sigma \mapsto j_\sigma$$

が定義できることがわかる．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，とくにアーベル群であり，

$$[K(\zeta) : K] = |G| \leq \left|(\boldsymbol{Z}/n\boldsymbol{Z})^\times\right| = \varphi(n) < n.$$

ここで，φ はオイラー関数である． □

定理 13.6　ベキ根拡大 L/K に対して，有限次塁アーベル拡大 L'/K で $L \subset L'$ をみたすものが存在する．

証明　L/K の中間体の列

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

が存在する．ここで，

$$K_i = K_{i-1}(\alpha_i), \qquad \alpha_i \text{ は } K_{i-1} \text{ 上の既約多項式 } X^{n_i} - a_i \text{ の根}$$

と表すことができる．そこで，n を $n_1, \ldots, n_m$ の公倍数とし，ζ を 1 の原始 n 乗根として，$M_i = K_i(\zeta)$ $(i = 0, 1, \ldots, m)$ とおく．$i = 1, \ldots, m$ に対して，M_{i-1} は 1 の原始 n_i 乗根をもっているから，$M_i = M_{i-1}(\alpha_i)$ は M_{i-1} 上のクンマー拡大，したがって巡回拡大である．一方，補題 13.5 より，$M_0 = K(\zeta)$ は K 上のアーベル拡大なので，$M_m = L(\zeta)$ は K 上有限次塁アーベル拡大である． □

補題 13.7　(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． $n=1$ のときはあきらかである． そこで，$n>1$ 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

$$(\spadesuit) \qquad c_1\sigma_1(\gamma)+c_2\sigma_2(\gamma)+\cdots+c_n\sigma_n(\gamma)=0$$

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． 等式 ($\spadesuit$) の γ の代わりに $\beta\gamma$ を用いれば，

$$c_1\sigma_1(\beta)\sigma_1(\gamma)+c_2\sigma_2(\beta)\sigma_2(\gamma)+\cdots+c_n\sigma_n(\beta)\sigma_n(\gamma)=0.$$

これと，($\spadesuit$) に $\sigma_n(\beta)$ をかけたもの

$$c_1\sigma_n(\beta)\sigma_1(\gamma)+c_2\sigma_n(\beta)\sigma_2(\gamma)+\cdots+c_n\sigma_n(\beta)\sigma_n(\gamma)=0$$

の差を取れば，最後の項 $c_n\sigma_n(\beta)\sigma_n(\gamma)$ 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，帰納法の仮定と β の取り方から $c_1=0$ を得る． したがって ($\spadesuit$) は

$$c_2\sigma_2(\gamma)+\cdots+c_n\sigma_n(\gamma)=0$$

と書き換えられ，再び帰納法の仮定より $c_2=\cdots=c_n=0$ を得る． □

定理 13.8 n を自然数とし，体 K は 1 の原始 n 乗根 ζ_n を含むとする． もし L/K が n 次巡回拡大ならば，ある $a \in K^\times$ が存在して，$L=K(\sqrt[n]{a})$ と表される． すなわち，$\zeta_n \in K$ ならば K 上の n 次巡回拡大はクンマー拡大である．

証明 $\zeta=\zeta_n$ と略記する． σ を $\mathrm{Gal}(L/K)$ の生成元とする;

$$\mathrm{Gal}(L/K)=\langle\sigma\rangle=\left\{1,\sigma,\sigma^2,\ldots,\sigma^{n-1}\right\}, \qquad \sigma^n=1.$$

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，$0 \neq \alpha \in L$ であって

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

両辺を n 乗して $\sigma(\alpha^n)=\alpha^n$ を得る． σ は $\mathrm{Gal}(L/K)$ の生成元だから，α は $\mathrm{Gal}(L/K)$ の不変体 K に属する． すなわち $\alpha^n \in K$ であり，$X^n-\alpha^n \in K[X]$ となる． さらに，$\sigma(\alpha)=\zeta\alpha$ より，$\mathrm{Conj}(\alpha,K)=\left\{\alpha,\zeta\alpha,\zeta^2\alpha,\ldots,\zeta^{n-1}\alpha\right\}$ 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． □