

§13. クンマー拡大

以下において扱う体はすべて C の部分体とする. また, 自然数 n に対して, $\zeta_n \in C$ を 1 の原始 n 乗根とする. すなわち, $\zeta_n \in C^\times$ 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 $\text{Gal}(L/K)$ が生成される;

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

- (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 は n の約数であり, L/K は l 次巡回拡大である.

証明 $\zeta = \zeta_n$ と略記する.

(1) $X^n - a$ のすべての根は $\alpha, \zeta\alpha, \zeta^2\alpha, \dots, \zeta^{n-1}\alpha$ であるが, $\zeta \in K$ より最小分解体は $K(\alpha) = L$ と一致する (例 9.12 参照).

(2) L/K がガロア拡大であることは (1) よりわかる. $G = \text{Gal}(L/K)$ とおく. $X^n - a$ は α の K 上の最小多項式なので, $|G| = [L : K] = n$ である. さらに, $\zeta\alpha$ は α と共役なので, 定理 6.11 より, $\sigma(\alpha) = \zeta\alpha$ をみたす $\sigma \in G$ が存在する. このとき,

$$\sigma^2(\alpha) = \sigma(\zeta\alpha) = \zeta\sigma(\alpha) = \zeta \cdot \zeta\alpha = \zeta^2\alpha,$$

同様にして, $\sigma^j(\alpha) = \zeta^j\alpha$ が任意の $j \in \mathbf{Z}$ について成り立ち, とくに $\sigma^n(\alpha) = \zeta^n\alpha = \alpha$ より $\sigma^n = \text{id}_L (= 1)$ となる. よって $|G| = n$ に注意すれば,

$$G = \{1, \sigma, \sigma^2, \dots, \sigma^{n-1}\} = \langle \sigma \rangle$$

を得る. とくに 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 $\xi^i\alpha$ ($i = 0, \dots, l-1$) 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 $0 \leq i_1 < \dots < i_d \leq l-1$ 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 $g(0) = \pm \xi^{i_1 + \dots + i_d} \alpha^d \in K$ となる. 一方, $\xi = \zeta^{n/l} \in K$ だから $\alpha^d \in K$ でなければならないが, これは l の最小性に矛盾する. L/K が l 次巡回拡大であることは (2) を援用すればわかる. $\square$

定義 13.2 前定理のようにして与えられる体の拡大 L/K を自然数 n に関する巡回クンマー拡大という. n に関する巡回クンマー拡大の合成を, n に関するクンマー拡大という. とくに, 有限次拡大 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, 有限個の $a_1, \dots, a_r \in K^\times$ について $\alpha_j^n = a_j$ をみたす α_j によって $L = K(\alpha_1, \dots, \alpha_r)$ と表されることである. n に関する有限次クンマー拡大は, しばしば $L = K(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_r})$ と表される.

補題 13.3 (デデキント) Γ を乗法群とし, $\sigma_1, \dots, \sigma_n$ を Γ から $C^\times$ への相異なる準同型写像とする. このとき, $(c_1, \dots, c_n) \neq (0, \dots, 0)$ をみたす任意の $c_1, \dots, c_n \in C$ に対して

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

をみたす $\gamma \in \Gamma$ が存在する.

証明 対偶, すなわち, $c_1, \dots, c_n \in C$ とするとき,

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

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

$$(\spadesuit) \quad c_1 \sigma_1(\gamma) + c_2 \sigma_2(\gamma) + \dots + c_n \sigma_n(\gamma) = 0$$

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,

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

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

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

の差を取れば, 最後の項 $c_n \sigma_n(\beta) \sigma_n(\gamma)$ が消去されて,

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

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

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

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

定理 13.4 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、 K 上の n 次巡回拡大は巡回クンマー拡大である。

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

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

いま、 $\Gamma = L^\times$ 、 $\sigma_i = \sigma^{i-1}$ および $c_i = \zeta^{-(i-1)}$ ($i = 1, \dots, n$) として前補題を適用すれば、

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

をみたす $\gamma \in L^\times$ が存在する。この和を α とすると、 $0 \neq \alpha \in L$ であって

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

が成り立ち、両辺を n 乗して $\sigma(\alpha^n) = \alpha^n$ を得る。 σ は $\text{Gal}(L/K)$ の生成元だから、 α^n は $\text{Gal}(L/K)$ の不変体 K に属する。すなわち $\alpha^n \in K$ である。ここで、系 6.12 より

$$\{\sigma^j(\alpha) \mid j = 0, 1, 2, \dots, n-1\} \subset \text{Conj}(\alpha, K)$$

だが、左辺は $\{\alpha, \zeta\alpha, \zeta^2\alpha, \dots, \zeta^{n-1}\alpha\}$ に等しく、 $\alpha \neq 0$ より n 個の元からなるので、

$$n \leq |\text{Conj}(\alpha, K)| \leq [K(\alpha) : K] \leq [L : K] = n,$$

よって、不等号はすべて等号であり、とくに $L = K(\alpha)$ が得られる。 $\square$

定理 13.5 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。このとき、 L/K が n に関する有限次クンマー拡大であるためには、 L/K が有限次アーベル拡大でガロア群のすべての元の位数が n の約数であることが必要十分である。

証明は、定理 13.1 と定理 13.4 を組み合わせればよい。後で引用されないので、ここでは証明を省略する。

定義 13.6 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) 体の有限列 $K_0, K_1, \dots, K_m$ で、

$$K = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_{m-1} \subset K_m = L$$

$$K_i/K_{i-1} \text{ は 2 項拡大 } (i = 1, 2, \dots, m)$$

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 13.7 L/K を代数拡大とする. 中間体の有限列 $K_0, K_1, \dots, K_m$ で,

$$K = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_{m-1} \subset K_m = L$$

$$K_i/K_{i-1} \text{ はアーベル拡大 } (i = 1, 2, \dots, m)$$

をみたすものがとれるとき, L/K を**冪アーベル拡大**という.

注意 定理 13.1 において, $X^n - a$ が K 上既約ならば L/K は 2 項拡大かつ巡回拡大であるが, たとえ既約でなくても, (3) より, やはり 2 項拡大かつ巡回拡大になる. したがって, 一般に有限次クンマー拡大はベキ根拡大でありかつアーベル (したがって冪アーベル) 拡大である.

補題 13.8 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 $\sigma \in \text{Aut}(\overline{K}/K)$ に対して $\sigma(\zeta)$ も 1 の原始 n 乗根だから, とくに $\sigma(\zeta) \in K(\zeta)$, よって $K(\zeta)/K$ はガロア拡大である. そのガロア群を G とおく. $\sigma \in G$ に対して, $\sigma(\zeta) = \zeta^j$ をみたす整数 j が n を法として一意的に定まる. また, 上述のように ζ^j は 1 の原始 n 乗根だから, j, n は互いに素である. よって, 写像

$$G \longrightarrow (\mathbf{Z}/n\mathbf{Z})^\times, \quad \sigma \mapsto \bar{j}$$

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 $(\mathbf{Z}/n\mathbf{Z})^\times$ の部分群に同型, とくにアーベル群であり,

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

ここで, φ はオイラー関数である. □

定理 13.9 ベキ根拡大 L/K に対して, 有限次冪アーベル拡大 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

$$K = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_{m-1} \subset K_m = L$$

$$K_i/K_{i-1} \text{ は 2 項拡大 } (i = 1, 2, \dots, m)$$

が存在する. ここで, K_{i-1} 上の既約多項式 $X^{n_i} - a_i$ の根 α_i によって $K_i = K_{i-1}(\alpha_i)$ と表すことができる. そこで, n を $n_1, \dots, n_m$ の公倍数とし, ζ を 1 の原始 n 乗根として, $M_i = K_i(\zeta)$ ($i = 0, 1, \dots, m$) とおく. $i = 1, \dots, m$ 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} 上の巡回クンマー拡大, したがって巡回拡大である. 一方, 補題 13.8 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 上有限次冪アーベル拡大である. □

上の定理において, ベキ根拡大と有限次冪アーベル拡大の役割を入れ替えても正しいことが次節で示される (定理 14.2). すなわち, これらの拡大は“本質的”に同等であると考えることができる.