

§14. 可解性

この節でも、前節同様、扱う体はすべて C の部分体とする。

補題 14.1 有限次アーベル拡大 L/K に対して、中間体の列 K_1, \dots, K_r で、

$$K = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_{r-1} \subset K_r = L$$

$$K_i/K_{i-1} \text{ は巡回拡大 } (i = 1, 2, \dots, r)$$

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。 $[L:K] = 1$ すなわち $L = K$ のときは自明だから、 $[L:K] > 1$ として $G = \text{Gal}(L/K)$ 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、 $\text{Gal}(L/M) = H$ は巡回群だから L/M は巡回拡大である。一方、系 11.4 (2) より M/K はアーベル拡大である。しかも、 $H \neq \{1\}$ より $[M:K] < [L:K]$ 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 $K = K_0 \subset K_1 \subset \dots \subset K_s = M$ がとれる。これと $M \subset L$ を合わせれば証明が完了する。 \square

定理 14.2 有限次冪アーベル拡大 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。 $[L:K] = 1$ のときはあきらかだから、 $n = [L:K] > 1$ とする。いま、 L/K は冪アーベル拡大だから、前補題を何度か適用することにより、中間体の列 K_1, \dots, K_r で、

$$K = K_0 \subset K_1 \subset K_2 \subset \dots \subset K_{r-1} \subset K_r = L$$

$$K_i/K_{i-1} \text{ は巡回拡大 } (i = 1, 2, \dots, r)$$

をみたすものが存在する。各 $i = 1, 2, \dots, r$ について $n_i = [K_i:K_{i-1}]$ とすると、それらの最小公倍数 m は n の約数である。 ζ を 1 の原始 m 乗根とすれば、補題 13.8 より、 $K(\zeta)/K$ はアーベル拡大で次数は m 未満、したがって n 未満である。よって、帰納法の仮定が適用でき、ベキ根拡大 M/K で $K(\zeta) \subset M$ をみたすものがとれる。 $M_i = K_i M$ とおけば、 $M_i = K_i M_{i-1}$ だから、定理 11.6 より M_i/M_{i-1} はガロア拡大でそのガロア群 $\text{Gal}(M_i/M_{i-1})$ は $\text{Gal}(K_i/K_{i-1})$ の部分群と同型である。よって M_i/M_{i-1} は巡回拡大でその次数 m_i は n_i の約数であり m の約数でもある。したがって M_{i-1} は 1 の原始 m_i 乗根を含み、定理 13.4 が適用できて、 M_i/M_{i-1} は巡回クンマー拡大、よって 2 項拡大となる。このことから M_r/M_0 すなわち LM/M はベキ根拡大であることがわかり、 M/K がベキ根拡大であることと合わせて定理が証明された。 \square

定義 14.3 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 14.4 $f(X) \in K[X]$ 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 14.5 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

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

と変形できるからである.

例 14.6 体 K に対して, 1 のベキ根は K 上ベキ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, 定義から直接には導けない. 証明は, 補題 13.8 および定理 14.2 を用いて与えられる (定理 14.7). なお, $n = 3, 5$ の場合は以下を参照せよ.

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

(2) 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, $\eta = \zeta + \frac{1}{\zeta}$ とおけば, $\eta^2 = \zeta^2 + \frac{1}{\zeta^2} + 2$ だから

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

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

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

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

定理 14.7 (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 13.8 から $K(\zeta)/K$ はアーベル拡大であり, 定理 14.2 より, ベキ根拡大 L/K で $K(\zeta) \subset L$ をみたすものがとれる. とくに ζ は K 上ベキ根で表される. \square

いま, L/K を有限次ガロア拡大としそのガロア群を G とする. さらに L/K が冪アーベル拡大でもあるとすると, 中間体の列

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

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

に G の部分群の列

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{m-1} \supset G_m = \{1\}$$

$$G_i \text{ は } G_{i-1} \text{ の正規部分群で } G_{i-1}/G_i \text{ はアーベル群 } (i = 1, 2, \dots, m)$$

が対応する. 群論で学んだように, このような部分群列が存在する群は**可解群**とよばれる. すなわち, 冪アーベルであるガロア拡大とは可解拡大のことに他ならない. よって, 定理 14.2 から次の定理を得る.

定理 14.8 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.

一方で, 与えられた有限次冪アーベル拡大 L/K に対して, 原始元定理により $L = K(\alpha)$ と表したとき, L/K の正規閉包 (いまの場合, L を含む K 上の最小のガロア拡大体) L' は, 命題 9.17 より

$$L' = K(\text{Conj}(\alpha, K)) = \prod_{\beta \in \text{Conj}(\alpha, K)} K(\beta)$$

で与えられる. K 上の有限個の冪アーベル拡大体の合成体が冪アーベル拡大体となることは, 定理 11.5 (2) を使って (厳密には数学的帰納法により) 示すことができるので, L'/K は可解拡大であることわかる. したがって, 定理 13.9 から次の定理が帰結される.

定理 14.9 ベキ根拡大 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.

以上で, この講義の最終目標である定理の証明の準備がすべて整った.

定理 14.10 (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 上ベキ根によって解けるための必要十分条件は L/K が可解拡大であることである.

証明 L/K が可解拡大ならば, 定理 14.8 から, $f(X)$ が K 上ベキ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 上ベキ根によって解けるとする. すなわち $f(X)$ の任意の根 α に対して, ベキ根拡大 L_α/K が存在して $\alpha \in L_\alpha$ をみたすとする. 定理 14.9 を用いれば, $L_\alpha \subset L'_\alpha$ をみたす有限次可解拡大 L'_α/K がとれる. よって, $f(X)$ のすべての根 α にわたる合成体

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

は, 定理 11.5 (2) より K 上ガロアで, そのガロア群 $\text{Gal}(\tilde{L}/K)$ は可解群の直積の部分群に同型, したがって可解群となる. 最後に, \tilde{L}/K の中間体である L は K 上ガロアだから, 系 11.4 (3) より, L/K は可解拡大であることがわかる. \square

定理 14.11 $f(X)$ を \mathbb{Q} 上の 5 次既約多項式とする. $f(X)$ が実根をちょうど 3 個もつならば, $f(X)$ は \mathbb{Q} 上ベキ根によって解けない.

証明 $f(X)$ の \mathbb{Q} 上の最小分解体を L とし, L/\mathbb{Q} のガロア群を G とする. G は $f(X)$ の 5 つの根の置換群と考えられるので, 5 次対称群 S_5 の部分群とみなすことができる. ここで, $f(X)$ のひとつの根 α に対して $\mathbb{Q}(\alpha)$ は L/\mathbb{Q} の中間体だから, G の位数は $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$ で割り切れる. したがって G は位数 5 の元をもつ. このことから, 置換群としての G は長さ 5 の巡回置換をもつことが示せる. 一方, 複素共役を対応させる写像 $C \rightarrow C, z \mapsto \bar{z}$ を L に制限したものを $\tau \in G$ とおけば, L がちょうど 2 個の虚根をもつことから, τ は互換とみなすことができる. 互換および長さ 5 の巡回置換をもつ S_5 の部分群は S_5 と一致することは, 群論の一般論から証明できる. したがって $G = S_5$ であるが, S_5 は可解群ではないので L/\mathbb{Q} は可解拡大ではない. よって, 定理 14.10 より $f(X)$ は \mathbb{Q} 上ベキ根によって解けない. \square

上の定理の条件をみたす 5 次既約多項式として, たとえば $f(X) = X^5 - 5X - 1$ があげられる. 実際, 既約であることは $f(X+1)$ にアイゼンシュタインの定理を素数 5 に関して適用すればよい. また, 実根が 3 つであることは微積分学の簡単な計算で確かめられる. よって, $f(X)$ は \mathbb{Q} 上ベキ根によって解けない.

定理 14.12 (アーベル) \mathbb{Q} 上の 5 次方程式には, 四則とベキ根によって表される「解の公式」は存在しない.

証明 もし存在すれば, 有理数係数のどんな 5 次方程式の解も \mathbb{Q} 上ベキ根で表されることになる. しかし, 上に述べたように \mathbb{Q} 上ベキ根によって解けない 5 次既約多項式が存在するから矛盾である. \square