表現論による Kummer 理論の解釈

@Metachick_2021

2026 年 5 月 11 日

一般に Galois 群の構造が分かっても、その拡大体を $K(\alpha_1, \cdots, \alpha_r)$ と具体的に記述することは容易でない。しかし、Abel 拡大（Galois 群が Abel 群となる拡大）の場合には適切な仮定のもとで拡大体を比較的明示的に記述することができる。その際に重要となるのが Kummer 理論である。

1　表現論からの準備

まずは、基本的な表現論の命題を確認しておく。Maschke の定理の証明に関しては参考文献 [1] や [2] を参照されたい。なお、補題 1.2 は有限群に限らなくても成立するが、証明の簡単のため、有限群を仮定した。

【定理 1.1】Maschke の定理

基礎体の標数が群の位数を割らないとする。このとき、有限群の任意の表現は完全可約。すなわち、既約表現の直和に分解可能である。

【補題 1.2】

有限 Abel 群 G の既約表現は一次元の表現である。

証明　$|G| = k$ とおく。G は Abel 群であるから、任意の共役類は 1 元集合となり、G の共役類の個数は k 個となる。また、G の既約表現の個数は G の共役類の個数に等しいから、G の既約表現の個数は k 個である。すなわち、G の既約表現の同値類の代表系を $V_1, \cdots, V_k$ とおける。いま、

$$|G| = \sum_{i=1}^{k} (\dim V_i)^2$$

が成り立つ。各 i について、$\dim V_i$ は正の整数であるから、$\dim V_i = 1$ となるほかない。これより、G の既約表現は一次元である。 □

【定義 1.3】指標

G を群、K を体とし、(V, ρ) を G の K 上の有限次元表現とする。このとき、各 $\sigma \in G$ に対して表現行列 $\rho(\sigma)$ のトレースを対応させる関数 $\chi_\rho : G \to K$ を表現 ρ の指標という。すなわち、$\chi_\rho(\sigma) = \mathrm{Tr}(\rho(\sigma))$ と定める。

【定理 1.4】Schur の補題

K を十分に 1 の根を持つ体とする。K 上のベクトル空間 V_1, V_2 が群 G の既約表現であるとき、以下が成り立つ。

$$\mathrm{Hom}_G(V_1, V_2) \cong \begin{cases} K & (V_1 \cong_G V_2) \\ 0 & (V_1 \ncong_G V_2) \end{cases}$$

証明は参考文献 [1] や [2] を参照せよ。

【定理 1.5】射影公式

G を有限群、K を $\mathrm{ch}K \nmid |G|$ かつ十分に 1 の根を持つ体、V を K 上の G の表現空間とする。G の既約表現 W（その次元を d、指標を χ とする）に対し、V における χ-等型成分を $V_\chi = \sum_{U \subseteq V,\ U \cong W} U$ と定義する。このとき、線形写像

$$P_\chi = \frac{d}{|G|} \sum_{\sigma \in G} \chi(\sigma^{-1})\sigma$$

は、V から V_χ への射影作用素となる。すなわち、$x \in V_\chi$ ならば $P_\chi(x) = x$ であり、他の既約成分に属する x ならば $P_\chi(x) = 0$ を満たす。

証明　Maschke の定理より V を既約表現の直和に分解し、その 1 つの成分を U 、指標を ψ とする。U は部分表現であり、P_χ は $\sigma \in G$ の線形結合として定義されているため、任意の $x \in U$ に対して $P_\chi(x) \in U$ となる。すなわち $P_\chi(U) \subseteq U$ が成り立つ。さらに P_χ は和の順序の入れ替えにより G の作用と Abel（$P_\chi \tau = \tau P_\chi$）であるため、その制限は $P_\chi|_U \in \mathrm{Hom}_G(U, U)$ となる。Schur の補題より $\mathrm{Hom}_G(U, U) \cong K$ であるから、$P_\chi|_U$ はスカラー倍作用素となる。すなわち、ある定数 λ が存在して $P_\chi|_U = \lambda \mathrm{id}_U$ と表せる。

この両辺のトレースをとる。左辺は P_χ の定義と指標の直交関係式により、

$$\mathrm{Tr}(P_\chi|_U) = \frac{\chi(1)}{|G|} \sum_{\sigma \in G} \chi(\sigma^{-1})\psi(\sigma) = \chi(1)\delta_{\chi,\psi}$$

となる。一方、右辺は $\mathrm{Tr}(\lambda \mathrm{id}_U) = \lambda \psi(1)$ である。これらを比較すると $\lambda\psi(1) = \chi(1)\delta_{\chi,\psi}$ となる。$\chi = \psi$（すなわち $U \cong W$）のときは $\chi(1) = \psi(1)$ より $\lambda = 1$、$\chi \neq \psi$（すなわち $U \ncong W$）のときは $\lambda = 0$ と定まる。したがって、P_χ は、W と同型な既約成分には恒等写像としてはたらき、それ以外の成分は 0 に潰す。以上より、P_χ は等型成分 V_χ への射影作用素である。 □

2　Kummer 理論

【定義 2.1】Kummer 拡大

n は 2 以上の正整数、ζ_n は 1 の原始 n 乗根とし、K を ζ_n を含む体、L をその有限次元 Abel 拡大とする。任意の $\sigma \in \mathrm{Gal}(L/K)$ に対して $\sigma^n = \mathrm{id}_L$ が成り立つとき、L を K の Kummer 拡大という。

ここで、K は ζ_n を含むから標数が n を割り切らないことがわかる。実際、$chK = p > 0$ が n を割り切ると仮定すると、方程式 $x^n - 1 = 0$ は $(x^{\frac{n}{p}} - 1)^p = 0$ と書けるから原始 n 乗根であることに矛盾する。

【定理 2.2】

K を ζ_n を含む体、L をその拡大体とする。このとき、以下は同値である。

(1) L/K は Kummer 拡大

(2) $a_i \in K^\times$ を用いて $L = K(\sqrt[n]{\alpha_1}, \cdots, \sqrt[n]{\alpha_r})$ と書ける

ここで、$\sqrt[n]{a_i}$ は $\alpha_i^n = a_i \in K^\times$ となるような数のうちのひとつを指すものとする。今回の状況設定においては、$\sqrt[n]{a_i}$ としてどの元を選んでも $\zeta_n \in K$ であるから問題は生じない。

証明

(1) $\Rightarrow$ (2)：

$G = \mathrm{Gal}(L/K)$ とおく。仮定より G は有限 Abel 群であり、任意の元 $\sigma \in G$ の位数は n を割り切る。したがって G の位数の素因数はすべて n の素因数に含まれる。K は原始 n 乗根 ζ_n を含むため $\mathrm{ch}K \nmid n$ であり、ゆえに $\mathrm{ch}K \nmid |G|$ となる。

いま、L は K 上のベクトル空間であり、G の各元は K 上の線形変換として作用する、すなわち $G = \mathrm{Gal}(L/K) \subseteq \mathrm{GL}_K(L)$ である。したがって、$\rho : G \to \mathrm{GL}_K(L)$ を包含写像とすれば、(L, ρ) は G の表現である。$\mathrm{ch}K \nmid |G|$ より Maschke の定理が適用でき、表現空間 L は完全可約となる。さらに補題 1.2 より有限 Abel 群の既約表現はすべて 1 次元であるため、L は 1 次元表現の直和に分解される。すなわち、ある 1 次元の部分空間 $V_1, \ldots, V_m$ が存在して、以下のように直和分解できる。ただし、$m = [L : K]$ である。

$$L = \bigoplus_{i=1}^{m} V_i \quad (\dim_K V_i = 1)$$

各 V_i は 1 次元表現であるため、その作用を与える準同型 $\rho_i : G \to \mathrm{GL}_K(V_i) \cong K^\times$ は、それ自体が群の指標 $\chi_i : G \to K^\times$ と同一視できる。いま、任意の $\sigma \in G$ と $\alpha \in L$ に対して、$\alpha \in V_i$ とすれば、$\sigma(\alpha) = \sigma|_{V_i}(\alpha) = \rho_i(\sigma)(\alpha) = \chi_i(\sigma) \cdot \alpha$ となるから、α は全ての σ に対しての同時固有ベクトルである。また、各 σ に対して、その固有値は $\chi_i(\sigma)$ である。ここで、仮定より群 G の任意の元 σ は $\sigma^n = \mathrm{id}_L$ を満たすため固有値についても $\chi_i(\sigma)^n = \chi_i(\sigma^n) = 1$ が成り立つから、$\chi_i(\sigma) \in \langle \zeta_n \rangle \subseteq K$ である。

次に、各 V_i からゼロでない元 α_i を一つずつ選ぶ。$\alpha_i^n \in L$ への σ の作用を考えると、σ は体 L の自己同型であるから積の構造を保ち、

$$\sigma(\alpha_i^n) = (\sigma(\alpha_i))^n = (\chi_i(\sigma)\alpha_i)^n = \chi_i(\sigma)^n \alpha_i^n = 1 \cdot \alpha_i^n = \alpha_i^n$$

となる。すなわち、α_i^n は Galois 群 G のすべての元 σ の作用によって固定されるから、$\alpha_i^n \in L^G$ である。L/K は Kummer 拡大、特に有限次 Galois 拡大だから $\alpha_i^n \in L^G = K$ である。

したがって、$\alpha_i^n = a_i \in K$ とおけば、$\alpha_i = \sqrt[n]{a_i}$ と書ける。ベクトル空間 L はこれら 1 次元の空間の直和 $L = \bigoplus_{i=1}^m V_i$ であったから、L のすべての元は基底 $\alpha_1, \ldots, \alpha_m$ の線形結合で表される。これは体の拡大として見れば、基礎体 K にこれら α_i たちをすべて添加した体に他ならない。ゆえに、適当な $a_i \in K^\times$ を用いて $L = K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_m})$ と表すことができる。

(2) ⇒ (1)：

仮定より、K は 1 の原始 n 乗根 ζ_n を含み、$L = K(\alpha_1, \ldots, \alpha_m)$（ただし $\alpha_i^n = a_i \in K^\times$）と表されている。まず、$L/K$ が Galois 拡大であることを示す。各 α_i は K 上の多項式 $f_i(x) = x^n - a_i$ の根である。K は ζ_n を含むため、$f_i(x)$ の n 個の根は $\alpha_i, \zeta_n\alpha_i, \zeta_n^2\alpha_i, \ldots, \zeta_n^{n-1}\alpha_i$ となり、すべて L に含まれる。また、$\mathrm{ch}K \nmid n$ であるから、$f_i'(x) = nx^{n-1} \neq 0$ となり、$f_i(x)$ は重根を持たない（分離的である）。したがって、L は分離多項式 $f_1(x) \cdots f_m(x)$ の K 上の最小分解体となるため、L/K は有限次 Galois 拡大である。よって、$G = \mathrm{Gal}(L/K)$ とおくことができる。

次に、G が Abel 群であることを示す。任意の $\sigma \in G$ に対して、σ は $f_i(x)$ の根を同じ $f_i(x)$ の根に移すため、$\sigma(\alpha_i) = \zeta_{\sigma,i}\alpha_i$ を満たす 1 の n 乗根 $\zeta_{\sigma,i} \in \langle \zeta_n \rangle$ がただ一つ定まる。ここで、$\zeta_{\sigma,i}$ は K の元であるため、Galois 群 G の作用で固定されることに注意する。任意

の $\sigma, \tau \in G$ をとり、α_i への合成作用を計算すると、

$$\sigma(\tau(\alpha_i)) = \sigma(\zeta_{\tau,i}\alpha_i) = \zeta_{\tau,i}\sigma(\alpha_i) = \zeta_{\tau,i}\zeta_{\sigma,i}\alpha_i$$

$$\tau(\sigma(\alpha_i)) = \tau(\zeta_{\sigma,i}\alpha_i) = \zeta_{\sigma,i}\tau(\alpha_i) = \zeta_{\sigma,i}\zeta_{\tau,i}\alpha_i$$

となる。これより、$\sigma(\tau(\alpha_i)) = \tau(\sigma(\alpha_i))$ が成り立つ。任意の生成元で $\sigma\tau = \tau\sigma$ となるから L 全体で $\sigma\tau = \tau\sigma$ である。ゆえに G は Abel 群である。

最後に、任意の $\sigma \in G$ について $\sigma^n = \mathrm{id}_L$ であることを確認する。先ほどの式を用いると、σ を n 回作用させたとき、$\sigma^n(\alpha_i) = (\zeta_{\sigma,i})^n\alpha_i = 1 \cdot \alpha_i = \alpha_i$ となる。これもすべての生成元 α_i で成り立つため、L 全体で $\sigma^n = \mathrm{id}_L$ が結論づけられる。

□

以上の考察により、Kummer 拡大 L/K においてガロア拡大の生成元 $\sqrt[n]{a}$ を探すという操作は、可換な線形変換の族に対する同時固有ベクトルを探すことにほかならないとわかる。また、右のような対応も見えてくる。

体論・Galois 理論	線形代数（表現論）
拡大体 L	K 上のベクトル空間
G の元 σ	可逆変換 σ
$\sigma \in G$ で不変	σ の固有値 1 の固有ベクトル
生成元 $\sqrt[n]{a}$	同時対角化の基底

このような生成元（同時固有ベクトル）を具体的に構成するには、射影公式と次に述べる定理を組み合わせれば良い。証明は参考文献 [5] の Theorem8 を参照されたい。

【定理 2.3】正規基底定理

L/K を有限次 Galois 拡大とし、その Galois 群を $G = \mathrm{Gal}(L/K)$ とする。このとき、ある元 $\alpha \in L$ が存在して、集合

$$\{\sigma(\alpha) \mid \sigma \in G\}$$

は、K 上のベクトル空間 L の基底となる。

正規基底定理によれば、L には G の作用で移り合う基底が存在し、K 上の G の表現空間として正則表現と同型になる。正則表現にはすべての既約表現がその次元に等しい重複度で現れるため、L は各指標 χ_k に対応する 1 次元固有空間 V_k の直和に分解される。これにより、V_{χ_i} は V_i であるから、射影公式を用いて各 V_i の基底を次のように構成できる。

$$(\chi_i, \alpha) = \sum_{\sigma \in G} \chi_i(\sigma)^{-1}\sigma(\alpha)$$

この (χ_i, α) を指標 χ_i に関する Lagrange resolvent という。

いま、再び正規基底定理により集合 $\{\sigma(\alpha) \mid \sigma \in G\}$ は K 上の基底であるため、互いに線形独立である。また、任意の $\sigma \in G$ に対して $\chi_i(\sigma)^{-1} \neq 0$ であるから、それらの非自明な線形結合である (χ_i, α) は決して 0 にならない。すなわち、(χ_i, α) は指標 χ_i の等型成分 V_i に属する非零のベクトルとなる。ゆえに、拡大体 L はこれら m 個の resolvent を K に添加した体として、

$$L = K((\chi_1, \alpha), \cdots, (\chi_m, \alpha))$$

と完全に明示化されることがわかる。（これを用いて、構成的な証明を行うこともできる。）

3　応用：代数方程式の解

Kummer 拡大の自然な応用として、代数方程式の冪根による可解性、すなわち解の公式の構成が挙げられる。K を 1 の原始 n 乗根 ζ_n を含む体として、K 上の n 次方程式 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$ を考える。これらの根を $\alpha_1, \cdots, \alpha_n$ とし、最小分解体を $L = K(\alpha_1, \cdots, \alpha_n)$ とおく。

もし仮に、L/K が Kummer 拡大となるような都合の良い状況であれば、前述の議論から適当な $a_1 \cdots, a_m \in K^\times$ を用いて $L = K(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_m})$ と書ける。方程式の根 α_i は L の元であるから、これら $\sqrt[n]{a_j}$ の線形結合で表される。さらに、Lagrange resolvent を用いればこれらの累乗根を具体的に構成できるため、これは方程式が代数的に解けることにほかならない。

3.1　三次方程式の解の公式

【命題 3.1】

$p, q \in \mathbb{Q}$ が $\sqrt{-4p^3 - 27q^2} \in \mathbb{Q}$ を満たし、$x^3 + px + q$ が既約であるとする。このとき、三次方程式 $x^3 + px + q = 0$ の根は以下のようになる。

$$\frac{\sqrt[3]{A} + \sqrt[3]{B}}{3}, \quad \frac{\omega\sqrt[3]{A} + \omega^2\sqrt[3]{B}}{3}, \quad \frac{\omega^2\sqrt[3]{A} + \omega\sqrt[3]{B}}{3}$$

ただし、A, B は以下の二次方程式 $t^2 + 27qt - 27p^3 = 0$ の解であり、立方根の選び方は $\sqrt[3]{A}\sqrt[3]{B} = -3p$ を満たすようにとる。

既約な三次方程式の最小分解体の Galois 群は S_3 か A_3 に同型なことが知られている。特に、A_3 と同型となるための必要十分条件は、判別式 $D = (\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2$ が $\sqrt{D} \in K$ を満たすことである。なお、上の場合には判別式は $-4p^3 - 27q^2$ となる。実際、根と係数の関係によって

$$D = f'(\alpha)f'(\beta)f'(\gamma) = -27(\alpha\beta\gamma)^2 - 4(\alpha\beta + \beta\gamma + \gamma\alpha)^3 = -4p^3 - 27q^2$$

とわかる。これにより、$\mathbb{Q}(\omega)$ 上の最小分解体 L が $\mathbb{Q}(\omega)$ の Kummer 拡大体であることがわかる。

証明　$K = \mathbb{Q}(\omega)$ とし、L を $\mathbb{Q}(\omega)$ 上の最小分解体とする。$\sqrt{-4p^3-27q^2} \in \mathbb{Q}$ ゆえ $\mathrm{Gal}(L/K) \cong A_3$ となる。A_3 は位数 3 の巡回群であるから、$G = \langle\sigma\rangle$ とおき、方程式の 3 つの根を σ が $\alpha \mapsto \beta \mapsto \gamma \mapsto \alpha$ と巡回させるものとしてよい。ここで、根 α, β, γ と 1 の原始 3 乗根 ω を用いて、次の 3 つの元（resolvent）を定義する。

$$R_0 = \alpha+\beta+\gamma, \quad R_1 = \alpha+\omega^2\beta+\omega\gamma, \quad R_2 = \alpha+\omega\beta+\omega^2\gamma$$

三次方程式 $x^3+px+q=0$ において、解と係数の関係より $\alpha+\beta+\gamma=0$ であるから、$R_0 = 0$ である。また、R_1 と R_2 の積および 3 乗の和を計算すると係数を用いて次のように書ける。

$$\begin{aligned} R_1R_2 &= (\alpha+\omega^2\beta+\omega\gamma)(\alpha+\omega\beta+\omega^2\gamma) = \alpha^2+\beta^2+\gamma^2-(\alpha\beta+\beta\gamma+\gamma\alpha) \\ &= (\alpha+\beta+\gamma)^2 - 3(\alpha\beta+\beta\gamma+\gamma\alpha) = 0^2 - 3p = -3p \end{aligned}$$

$$\begin{aligned} R_1^3+R_2^3 &= (\alpha+\omega^2\beta+\omega\gamma)^3 + (\alpha+\omega\beta+\omega^2\gamma)^3 \\ &= 2(\alpha^3+\beta^3+\gamma^3) - 3(\alpha^2\beta+\alpha\beta^2+\beta^2\gamma+\beta\gamma^2+\gamma^2\alpha+\gamma\alpha^2) + 12\alpha\beta\gamma = -27q \end{aligned}$$

これより、R_1^3 と R_2^3 は、和が $-27q$、積が $(-3p)^3 = -27p^3$ となる 2 つの数である。したがって、これらは二次方程式 $t^2+27qt-27p^3=0$ の解となる。この方程式の解を A, B とおくと、根号のとり方を適切に選べば $R_1 = \sqrt[3]{A}, R_2 = \sqrt[3]{B}$ と表せる。このとき、$R_1R_2 = -3p$ であるため、立方根の選び方は $\sqrt[3]{A}\sqrt[3]{B} = -3p$ を満たすように選ばなければならない。

最後に、これらを用いて元の根を復元する。$R_0+R_1+R_2 = 3\alpha+(1+\omega+\omega^2)\beta+(1+\omega+\omega^2)\gamma$ であり、$1+\omega+\omega^2=0$ であるから、

$$3\alpha = R_0+R_1+R_2 = \sqrt[3]{A}+\sqrt[3]{B} \implies \alpha = \frac{\sqrt[3]{A}+\sqrt[3]{B}}{3}$$

を得る。さらに、β, γ についても、R_1, R_2 の定義式に ω や ω^2 を乗じて足し合わせることで抽出できる。

$$R_0+\omega R_1+\omega^2 R_2 = 3\beta \implies \beta = \frac{\omega\sqrt[3]{A}+\omega^2\sqrt[3]{B}}{3}$$

$$R_0+\omega^2 R_1+\omega R_2 = 3\gamma \implies \gamma = \frac{\omega^2\sqrt[3]{A}+\omega\sqrt[3]{B}}{3}$$

以上により、所望の公式が得られた。　□

今までの議論を踏まえれば、証明中で用いた resolvent R_0, R_1, R_2 は偶然の産物ではなく、論理的に導出できることは明白であろう。

resolvent の導出 Note

$K = \mathbb{Q}(\omega)$ の標数は 0 であり、群 $G = \mathrm{Gal}(L/K) \cong A_3$ の位数 3 を割り切らないため、Maschke の定理が適用でき、K-ベクトル空間 L は完全可約となる。さらに G は位数 3 の Abel 群であり、K は 1 の原始 3 乗根 ω を含むため、既約表現はすべて 1 次元である。その指標は $\chi_k(\sigma) = \omega^k$ $(k = 0, 1, 2)$ で与えられる。

正規基底定理によれば、L には G の作用で移り合う基底が存在し、K 上の G の表現空間として正則表現と同型になる。正則表現にはすべての既約表現がその次元に等しい重複度で（今回はそれぞれ 1 回ずつ）現れるため、L は各指標 χ_k に対応する 1 次元固有空間 V_k の直和に過不足なく分解される。

$$L = V_0 \oplus V_1 \oplus V_2$$

これより、resolvent が具体的に書き下せるので、例えば、α を代入して計算すれば、R_0, R_1, R_2 を得る。$x^3 + px + q$ は既約だから $p \neq 0$ であるので、R_1, R_2 も 0 でないから、V_1, V_2 の基底が得られる。また、V_0 は指標が自明だから K に他ならず、基底として 1 を取れば良い。以上により、$1, R_1, R_2$ は L の基底だから、三次方程式 $x^3 + px + q = 0$ の解はそれらの線型結合として書き表せる。また、resolvent を計算する際に、α を代入したので、復元することも容易であるから、解の公式が導ける。

3.2　方程式の可解性

【定義 3.2】代数的に解ける

一般 n 次方程式 $f(x) = 0$ が K 上代数的に解けるとは、以下の体 $L_1, \cdots, L_r$ が存在することを言う。ただし、L は $f(x)$ の K 上最小分解体である。

$$\begin{cases} K = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_r, \quad L_{i+1} = L_i(\sqrt[n_i]{\alpha_i})(\alpha_i \in L_i) \\ L \subseteq L_r \end{cases}$$

一般に、方程式の最小分解体は Kummer 拡大体であるとは限らない。しかし、適切に中間体を挟めば Kummer 拡大の連鎖として記述できる。Galois 群が可解群の場合にはまさに Kummer 拡大の連鎖で表せる。

【定理 3.3】方程式の可解性

一般方程式 $f(x)=0$ が代数的に解けるための必要十分条件は、L/K が可解拡大をなすことである。

証明

$\Rightarrow$ の証明：

方程式 $f(x)=0$ が代数的に解けると仮定する。定義より、体の塔 $K=L_0\subseteq L_1\subseteq\cdots\subseteq L_r$ が存在し、各 i について、$L_{i+1}=L_i(\sqrt[n_i]{\alpha_i})$ と表され、最小分解体 L は L_r に含まれる。ここで、これらすべての冪指数 n_i の最小公倍数を N とし、基礎体 K に 1 の原始 N 乗根 ζ_N を添加した体 $K'=K(\zeta_N)$ を考える。方程式 $x^N-1=0$ の解である ζ_N もまた冪根 $\sqrt[N]{1}$ とみなせるため、この添加も許される操作である。

この K' 上に先ほどの塔を持ち上げた $L_i'=L_i(\zeta_N)$ の列を考える。

$$K\subseteq K'=L_0'\subseteq L_1'\subseteq\cdots\subseteq L_r'$$

すると、$L_{i+1}'=L_i'(\sqrt[n_i]{\alpha_i})$ であり、基礎体 L_i' は常に十分な 1 の冪根 ζ_{n_i} を含むため、前節で見た通り各拡大 L_{i+1}'/L_i' は Kummer 拡大となる。すなわち、各段階は Galois 拡大であり、その Galois 群は Abel 群である。

ただし、L_r' は K 上の Galois 拡大（正規拡大）とは限らないため、$\sqrt[n_i]{\alpha_i}$ たちの共役をすべて添加した L_r' の K 上の正規閉包 M をとる。共役元の添加もまた同種の冪根の添加であるため、M も K から Abel 群を Galois 群に持つ拡大の繰り返しで到達できる。Galois 理論の基本定理より、この体の塔に対応して $\mathrm{Gal}(M/K)$ には正規部分群の列が存在し、各剰余群が Abel 群となる。すなわち $\mathrm{Gal}(M/K)$ は可解群である。L は $f(x)$ の最小分解体であるから L/K は Galois 拡大であり、$L\subseteq M$ より $\mathrm{Gal}(L/K)$ は $\mathrm{Gal}(M/K)$ の剰余群に同型となる。可解群の剰余群もまた可解群であるため、$\mathrm{Gal}(L/K)$ は可解群となり、L/K は可解拡大であることが示された。

$\Leftarrow$ の証明：

L/K が可解拡大であると仮定する。すなわち、$G=\mathrm{Gal}(L/K)$ は可解群である。可解群の性質より、G には剰余群が素数位数の巡回群となるような組成列が存在する。

$$G=G_0\rhd G_1\rhd\cdots\rhd G_m=\{\mathrm{id}\}\quad(G_i/G_{i+1}\text{ は巡回群})$$

各剰余群の位数の最小公倍数を N とし、先ほどと同様に K に ζ_N を添加した体 $K' = K(\zeta_N)$ と、合成体 $L' = L(\zeta_N)$ を考える。ζ_N の添加は $x^N - 1 = 0$ の解（冪根）の添加である。

いま、L'/K' は Galois 拡大であり、$\mathrm{Gal}(L'/K')$ は $G = \mathrm{Gal}(L/K)$ の部分群に同型となるため、これも可解群である。したがって $\mathrm{Gal}(L'/K')$ にも剰余群が巡回群となる正規列が存在し、Galois 理論の基本定理によりこれに対応する中間体の列が得られる。

$$K' = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_s = L'$$

ここで各拡大 F_{i+1}/F_i は Galois 拡大であり、$\mathrm{Gal}(F_{i+1}/F_i)$ は位数が N を割る巡回群である。基礎体 F_i はすでに K' を含んでいるため、十分な 1 の冪根を備えている。ゆえに、Kummer 理論が完全に適用でき、各ステップはある要素 $\beta_i \in F_i$ を用いて $F_{i+1} = F_i(\sqrt[n_i]{\beta_i})$ と冪根の添加で書き表される。結果として L' は K から冪根の添加を繰り返して得られる体の塔の頂点であり、最小分解体 L は $L \subseteq L'$ を満たす。以上より、方程式 $f(x) = 0$ は代数的に解ける。 □

例えば、$K = \mathbb{Q}(\omega)$ 上の一般三次方程式 $x^3 + ax^2 + bx + c = 0$ の場合には、$K \subseteq K(\sqrt{D}) \subseteq L$ と中間体を挟むことで、各段階の拡大は Kummer 拡大となる。これによれば、L の元は $K(\sqrt{D})$ の元の冪根で記述でき、また $K(\sqrt{D})$ の元は K の元の冪根を用いて記述できる。したがって、これらをつなぎ合わせれば、L の元（すなわち方程式の解）は、基礎体 K の元に冪根や四則演算を繰り返し適用して得られることがわかる。これこそが、方程式が「代数的に解ける（可解である）」という事実に他ならない。また、resolvent によって、ある程度具体的な解の公式を与えるアルゴリズムが得られた。

参考文献

[1] 桂利行,『環上の加群』, 東京大学出版会,「大学数学の入門 2」, 2007.

[2] 池田岳,『テンソル代数と表現論』, 東京大学出版会, 2022.

[3] 本間泰史,「有限群の表現，対称群の表現の基礎」, 早稲田大学, https://yhomma.w.waseda.jp/homma2/download/representation.pdf

[4] 森下昌紀,『ガロア圏と基本群』, 森北出版, 2024.

[5] Arthur Ogus, “Galois Theory and the Normal Basis Theorem,” 2010, https://math.berkeley.edu/~ogus/Math_250A/Notes/galoisnormal.pdf