

# テンソル積と自己準同型環による有限次Galois拡大の近代的・構造論的考察

## 概要と解説の目的：

本稿では、方程式の根の可換性や置換を主体とする古典的なGalois理論の記述スタイルから離れ、多項式環のイデアル論、テンソル積の完全分解（分裂）、および自己準同型環の構造定理（Jacobson-Bourbakiの定理）を用いた、現代的な抽象代数学におけるGalois理論の再構築を行います。

数式や証明のステップを極めて丁寧に記述し、基本概念の定義からGaloisの基本定理（Galois対応の一对一性）の完成までを自己完結的 (self-contained) に解説します。

## 1. 基本概念の定義と準備

本稿において、集合の包含関係は $\subset$ を用い、真の包含関係である必要はないものとする。空集合は $\emptyset$ で表し、集合 $A$ から集合 $B$ を除く差集合は $A \setminus B$ と表記する。まず、議論の土台となる代数的構造を定義する。

### 定義 1.1 (有限次Galois拡大とGalois群)

体 $K$ の有限次代数拡大 $L$ が正規拡大かつ分離拡大であるとき、 $L/K$ を有限次Galois拡大 (finite Galois extension) と呼ぶ。また、 $K$ の各元を固定する $L$ の自己同型全体のなす群をGalois群 (Galois group) と呼び、 $G = \text{Gal}(L/K)$ で表す。

### 定義 1.2 (テンソル積代数)

$K$ を体とし、 $A, B$ を $K$ 上の可換代数とする。 $A$ と $B$ の $K$ 上のベクトル空間としてのテンソル積 (tensor product)  $A \otimes_K B$ に対し、乗法を

$$(a_1 \otimes b_1)(a_2 \otimes b_2) = (a_1 a_2) \otimes (b_1 b_2) \quad (a_1, a_2 \in A, b_1, b_2 \in B)$$

により定めた環構造を $K$ 上のテンソル積代数と呼ぶ。

### 定義 1.3 (ひねり群環 / 接合積)

有限次Galois拡大 $L/K$ とそのGalois群 $G = \text{Gal}(L/K)$ に対し、各 $\sigma \in G$ に対応する記号を $\sigma$ そのもので表す。 $L$ 上のベクトル空間としての直和

$$L[G] = \bigoplus_{\sigma \in G} L\sigma$$

に対し、乗法規則を

$$(a\sigma)(b\tau) = a\sigma(b)\sigma\tau \quad (a, b \in L, \sigma, \tau \in G)$$

および分配法則によって定義した非可換環をひねり群環 (skew group ring) または接合積 (crossed product) と呼ぶ。

### 定義 1.4 (自己準同型環)

$L$ を $K$ 上のベクトル空間とみなしたとき、 $L$ から $L$ への $K$ -線形写像全体のなす集合を $\text{End}_K(L)$ と表す。写像の和と合成

(積) に関して  $\text{End}_K(L)$  は非可換環となり、これを  $K$  上の自己準同型環 (endomorphism ring) と呼ぶ。

## 2. 予備的補題とその証明

主定理の構成に必要な3つの決定的な補題について、詳細な証明を与える。

### 補題 2.1 (原始元定理)

$L/K$  が有限次分離拡大であるならば、ある単一の元  $\alpha \in L$  が存在して  $L = K(\alpha)$  と表される。

#### 補題 2.1 の証明

$K$  が有限体である場合、拡大体  $L$  も有限体である。有限体の乗法群  $L^\times = L \setminus \{0\}$  は巡回群であるため、その生成元を  $g$  とすれば  $L = K(g)$  が成り立ち、題意は示される。

$K$  が無限体である場合を考える。有限次拡大であるから、 $L = K(\beta, \gamma)$  の場合を示せば、帰納法により任意の有限個の生成元の場合に帰着される。 $\beta, \gamma$  の  $K$  上の最小多項式をそれぞれ  $p(X), q(X)$  とし、その  $K$  の代数閉包におけるすべての根を  $\beta = \beta_1, \beta_2, \dots, \beta_r$  および  $\gamma = \gamma_1, \gamma_2, \dots, \gamma_s$  とする。拡大の分離性より、これらはすべて相異なる。 $K$  は無限体であるため、任意の  $i \in \{1, \dots, r\}$  および  $j \in \{2, \dots, s\}$  に対して

$$\beta_i + c\gamma_j \neq \beta_1 + c\gamma_1$$

を満たす元  $c \in K$  を選ぶことができる (各  $i, j$  について高々1つの  $c$  が上式を等号にするため、有限個の禁止点を除けばよい)。ここで  $\alpha = \beta + c\gamma \in L$  と置く。当然  $K(\alpha) \subset K(\beta, \gamma)$  である。

多項式  $h(X) = p(\alpha - cX) \in K(\alpha)[X]$  を考えると、 $h(\gamma) = p(\beta) = 0$  である。また  $q(\gamma) = 0$  である。ゆえに  $\gamma$  は  $h(X)$  と  $q(X)$  の共通の根である。もし  $\gamma_j$  ( $j \neq 1$ ) も共通の根であるならば、 $h(\gamma_j) = p(\alpha - c\gamma_j) = 0$  となり、ある  $i$  に対して  $\alpha - c\gamma_j = \beta_i$ 、すなわち  $\beta + c\gamma - c\gamma_j = \beta_i$  より  $\beta + c(\gamma - \gamma_j) = \beta_i$  となるが、これは  $c$  の選択に矛盾する。したがって、 $L$  の代数閉包において  $h(X)$  と  $q(X)$  の共通根は  $\gamma$  のみである。したがって、 $\gamma$  の  $K(\alpha)$  上の最小多項式は一次式であり、 $\gamma \in K(\alpha)$  となる。これより  $\beta = \alpha - c\gamma \in K(\alpha)$  も従うため、 $K(\beta, \gamma) \subset K(\alpha)$  となり、 $L = K(\alpha)$  が示された。

### 補題 2.2 (中国剰余定理)

可換環  $R$  のイデアル  $I_1, I_2, \dots, I_m$  がどの2つも互いに素である (すなわち  $i \neq j$  ならば  $I_i + I_j = R$ ) とする。このとき、以下の環同型が成り立つ。

$$R / \left( \bigcap_{k=1}^m I_k \right) \cong \prod_{k=1}^m R / I_k$$

#### 補題 2.2 の証明

自然な環準同型写像  $\phi : R \rightarrow \prod_{k=1}^m R / I_k$  ( $x \mapsto (x \bmod I_1, \dots, x \bmod I_m)$ ) を考える。この写像の核  $\text{Ker}(\phi)$  が  $\bigcap_{k=1}^m I_k$  であることは定義から明らかである。したがって、 $\phi$  が全射であることを示せば、準同型定理より同型が従う。

$m = 2$  のとき、 $I_1 + I_2 = R$  より  $e_1 + e_2 = 1$  を満たす  $e_1 \in I_1, e_2 \in I_2$  が存在する。このとき  $e_1 \equiv 0 \pmod{I_1}$  かつ  $e_1 \equiv 1 \pmod{I_2}$  であり、逆に  $e_2 \equiv 1 \pmod{I_1}$  かつ  $e_2 \equiv 0 \pmod{I_2}$  である。任意の  $(r_1 \bmod I_1, r_2 \bmod I_2)$  に対し、 $x = r_2 e_1 + r_1 e_2$  と置けば、 $\phi(x) = (r_1 \bmod I_1, r_2 \bmod I_2)$  となり全射性が示される。

$m > 2$  のとき、各  $k \geq 2$  に対して  $I_1 + I_k = R$  より  $u_k + v_k = 1$  ( $u_k \in I_1, v_k \in I_k$ ) が存在する。このとき

$$1 = \prod_{k=2}^m (u_k + v_k) \in I_1 + \prod_{k=2}^m I_k \subset I_1 + \bigcap_{k=2}^m I_k$$

となるため、 $I_1$ と $\bigcap_{k=2}^m I_k$ は互いに素である。これと数学的帰納法を組み合わせることで、任意の元への移行が可能となり、全射性が完全に証明される。 ■

### 補題 2.3 (Dedekindの指標の独立性定理)

$L, M$ を体とする。相異なる体準同型 $\sigma_1, \sigma_2, \dots, \sigma_m : L \rightarrow M$ は、 $M$ 上線形独立である。すなわち、 $\sum_{i=1}^m c_i \sigma_i(x) = 0$  ( $\forall x \in L$ )を満たす $c_i \in M$ は $c_1 = c_2 = \dots = c_m = 0$ に限られる。

### 補題 2.3の証明

写像の個数 $m$ に関する数学的帰納法で示す。 $m = 1$ のとき、 $\sigma_1$ は体準同型ゆえ $\sigma_1(1) = 1 \neq 0$ であり、 $c_1 \sigma_1(1) = 0$ より $c_1 = 0$ となり成り立つ。

$m - 1$ 個のとき線形独立であると仮定し、 $m$ 個の間に線形従属関係 $\sum_{i=1}^m c_i \sigma_i(x) = 0$  ( $\forall x \in L$ )が存在すると仮定する。ただしすべての $c_i$ は0でないとしてよい。 $\sigma_1 \neq \sigma_m$ より、ある $y \in L$ が存在して $\sigma_1(y) \neq \sigma_m(y)$ となる。任意の $x \in L$ に対し、自変数を $yx$ と置き換えることで以下を得る。

$$\sum_{i=1}^m c_i \sigma_i(yx) = \sum_{i=1}^m c_i \sigma_i(y) \sigma_i(x) = 0$$

一方で、元の関係式全体に $\sigma_m(y)$ を乗じることで以下を得る。

$$\sum_{i=1}^m c_i \sigma_m(y) \sigma_i(x) = 0$$

上の式から下の式を差し引くことで、末尾の項が消去され、次の関係式が導かれる。

$$\sum_{i=1}^{m-1} c_i (\sigma_i(y) - \sigma_m(y)) \sigma_i(x) = 0$$

帰納法の仮定より $\sigma_1, \dots, \sigma_{m-1}$ は線形独立であるため、その係数はすべて0でなければならない。特に $i = 1$ のとき $c_1 (\sigma_1(y) - \sigma_m(y)) = 0$ となる。 $c_1 \neq 0$ と仮定していたため $\sigma_1(y) = \sigma_m(y)$ となり、これは $y$ の選定に矛盾する。したがって、相異なる体準同型は線形独立である。 ■

## 3. 主定理1：テンソル積 $L \otimes_K L$ の完全分解

現代的なガロア理論の出発点となる、テンソル積が直積環へと同型写像によって分解されるという事実を証明する。

### 定理 3.1

$L/K$ を有限次Galois拡大とし、 $G = \text{Gal}(L/K)$ とする。このとき、以下の写像 $\Psi$ は可換環の同型写像である。

$$\Psi : L \otimes_K L \longrightarrow \prod_{\sigma \in G} L, \quad a \otimes b \longmapsto (a\sigma(b))_{\sigma \in G}$$

### 定理 3.1 の証明

原始元定理 (補題 2.1) より、 $L = K(\alpha)$  となる  $\alpha \in L$  をとる。 $\alpha$  の  $K$  上の最小多項式を  $f(X) \in K[X]$  と置くと、多項式環の剰余環の性質より  $L \cong K[X]/(f(X))$  である。 $L/K$  は Galois 拡大であるため、 $f(X)$  は  $L[X]$  においてすべての根が異なり、完全に一次式の積へと因数分解される。すなわち、以下が成り立つ。

$$f(X) = \prod_{\sigma \in G} (X - \sigma(\alpha))$$

ここで、以下の2つの環同型写像の合成を考える。

#### ステップ 1: 拡張にともなうテンソル積の同型写像 $\theta$

テンソル積の底の変換 (スカラー拡大) の一般性質から、次のような自然な同型が存在する。

$$\theta: L \otimes_K L \cong L \otimes_K (K[X]/(f(X))) \cong L[X]/(f(X))$$

任意の  $b \in L$  はある多項式  $g(X) \in K[X]$  を用いて  $b = g(\alpha)$  と表されるため、 $\theta$  の具体的な対応規則は

$$\theta(a \otimes b) = a \cdot g(X) \pmod{f(X)}$$

となる。

#### ステップ 2: 中国剰余定理にともなう同型写像 $\omega$

$L[X]$  において、各  $\sigma \in G$  に対する一次式  $X - \sigma(\alpha)$  たちは、根  $\sigma(\alpha)$  がすべて相異なることから、生成するイデアルが互いに素である。したがって、中国剰余定理 (補題 2.2) から次の同型が従う。

$$L[X]/(f(X)) \cong \prod_{\sigma \in G} L[X]/(X - \sigma(\alpha))$$

各成分  $L[X]/(X - \sigma(\alpha))$  は  $X \mapsto \sigma(\alpha)$  という評価写像によって体  $L$  と同型であるため、全体として次の同型写像  $\omega$  が定まる。

$$\omega: L[X]/(f(X)) \longrightarrow \prod_{\sigma \in G} L, \quad H(X) \pmod{f(X)} \longmapsto (H(\sigma(\alpha)))_{\sigma \in G}$$

#### ステップ 3: 合成写像 $\omega \circ \theta$ の算出

任意の元  $a \otimes b \in L \otimes_K L$  (ただし  $b = g(\alpha)$ ,  $g(X) \in K[X]$ ) に対する合成写像の挙動を追跡する。

$$\theta(a \otimes b) = a \cdot g(X) \pmod{f(X)}$$

$$\omega(a \cdot g(X) \pmod{f(X)}) = (a \cdot g(\sigma(\alpha)))_{\sigma \in G}$$

ここで多項式  $g(X)$  の係数はすべて基礎体  $K$  の元であり、 $\sigma \in G$  の作用で不変であるため、 $g(\sigma(\alpha)) = \sigma(g(\alpha)) = \sigma(b)$  が成り立つ。よって、

$$\omega(\theta(a \otimes b)) = (a\sigma(b))_{\sigma \in G} = \Psi(a \otimes b)$$

となる。写像  $\Psi$  は同型写像  $\theta$  と  $\omega$  の合成写像  $\omega \circ \theta$  に他ならないため、 $\Psi$  は可換環としての同型写像である。 ■

### 例 3.2

$K = \mathbb{Q}$ 、 $L = \mathbb{Q}(\sqrt{2})$  の拡大を考える。Galois 群は  $G = \{\text{id}, \sigma\}$  (ただし  $\sigma(\sqrt{2}) = -\sqrt{2}$ ) である。このとき、定理 3.1 が主張する同型は  $\mathbb{Q}(\sqrt{2}) \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(\sqrt{2}) \times \mathbb{Q}(\sqrt{2})$  である。具体的な元として  $\sqrt{2} \otimes \sqrt{2}$  の行き先を計算すると、

$$\Psi(\sqrt{2} \otimes \sqrt{2}) = (\sqrt{2}\text{id}(\sqrt{2}), \sqrt{2}\sigma(\sqrt{2})) = (\sqrt{2} \cdot \sqrt{2}, \sqrt{2} \cdot (-\sqrt{2})) = (2, -2)$$

となり、完全に直積環の元に分解される。

## 4. 応用としての次数の決定

定理 3.1 の構造同型を用いることで、拡大次数に関する重要な等式を、次数の不等式評価を伴うことなく直ちに導くことができる。

### 定理 4.1

有限次Galois拡大 $L/K$ に対し、拡大次数 $[L : K]$ はGalois群の位数 $|G|$ と一致する。

### 定理 4.1の証明

定理 3.1 で確立された可換環の同型写像 $\Psi : L \otimes_K L \rightarrow \prod_{\sigma \in G} L$ の両辺に、以下のように $L$ の元 $x$ による左乗算作用を定義することで、双方の空間を左 $L$ -ベクトル空間とみなす。

$$\begin{aligned} x \cdot (a \otimes b) &:= (xa) \otimes b \quad (a \otimes b \in L \otimes_K L) \\ x \cdot (y_\sigma)_{\sigma \in G} &:= (xy_\sigma)_{\sigma \in G} \quad \left( (y_\sigma)_{\sigma \in G} \in \prod_{\sigma \in G} L \right) \end{aligned}$$

このとき、写像 $\Psi$ が左 $L$ -作用と可換であることは、次の計算から明らかである。

$$\Psi(x \cdot (a \otimes b)) = \Psi(xa \otimes b) = (xa\sigma(b))_{\sigma \in G} = x \cdot (a\sigma(b))_{\sigma \in G} = x \cdot \Psi(a \otimes b)$$

したがって、 $\Psi$ は左 $L$ -ベクトル空間としての同型写像を誘導する。よって、両辺の $L$ 上のベクトル空間としての次元 $\dim_L$ は等しい。各辺の次元を個別に評価する。

左辺について、 $L$ の $K$ 上のベクトル空間としての基底を $\{v_1, v_2, \dots, v_n\}$ と置く（ただし $n = [L : K]$ ）。テンソル積の普遍性より、 $L \otimes_K L$ の任意の元は $\sum_{i=1}^n \alpha_i (1 \otimes v_i)$  ( $\alpha_i \in L$ )の形に一意的に表される。したがって、

$\{1 \otimes v_1, \dots, 1 \otimes v_n\}$ は $L \otimes_K L$ の左 $L$ -ベクトル空間としての基底であり、 $\dim_L(L \otimes_K L) = [L : K]$ である。

右辺について、体 $L$ の $|G|$ 個の直積空間を $L$ 上のベクトル空間とみなしたときの次元は、明らかに成分の個数そのものであるため、 $\dim_L(\prod_{\sigma \in G} L) = |G|$ である。

両者の次元を比較することで、 $[L : K] = |G|$ が導かれる。 ■

## 5. 主定理2：自己準同型環の同型 $L[G] \cong \text{End}_K(L)$

Galoisの基本定理を、写像の中心化という性質に還元するためのもう一つの主定理を証明する。

### 定理 5.1

有限次Galois拡大 $L/K$ に対し、定義 1.3 で定めたひねり群環 $L[G]$ から、自己準同型環 $\text{End}_K(L)$ への以下の写像 $\Phi$ は、環としての同型写像である。

$$\Phi : L[G] \longrightarrow \text{End}_K(L), \quad \Phi \left( \sum_{\sigma \in G} a_\sigma \sigma \right) (x) = \sum_{\sigma \in G} a_\sigma \sigma(x) \quad (x \in L)$$

### 定理 5.1 の証明

まず、 $\Phi$  が環準同型であることを確認する。乗法の保存性を示すため、単項元  $a\sigma$  と  $b\tau$  をとる。任意の  $x \in L$  に対して、

$$\Phi((a\sigma)(b\tau))(x) = \Phi(a\sigma(b)\sigma\tau)(x) = a\sigma(b)\sigma(\tau(x))$$

一方で、写像の合成としての挙動を計算すると、

$$(\Phi(a\sigma) \circ \Phi(b\tau))(x) = \Phi(a\sigma)(b\tau(x)) = a\sigma(b\tau(x)) = a\sigma(b)\sigma(\tau(x))$$

となり、これらは完全に一致する。和の保存性および分配法則は定義から自明であるため、 $\Phi$  は環準同型写像である。

次に、 $\Phi$  の単射性を示す。 $\Phi(\sum_{\sigma \in G} a_\sigma \sigma) = 0$  と仮定すると、すべての  $x \in L$  に対して  $\sum_{\sigma \in G} a_\sigma \sigma(x) = 0$  が成り立つ。

しかし、補題 2.3 (Dedekind の指標の独立性定理) より、相異なる自己同型写像  $\sigma \in G$  は  $L$  上線形独立である。したがって、すべての  $\sigma \in G$  に対して  $a_\sigma = 0$  でなければならず、 $\text{Ker}(\Phi) = \{0\}$  より  $\Phi$  は単射である。

最後に、全射性を示す。 $L$  の  $K$  上の次元を  $n = [L : K]$  と置くと、定理 4.1 より  $|G| = n$  である。このとき、 $L[G]$  の  $K$  上のベクトル空間としての次元は  $\dim_K(L[G]) = |G| \cdot [L : K] = n^2$  である。一方、自己準同型環  $\text{End}_K(L)$  の  $K$  上の次元も  $\dim_K(\text{End}_K(L)) = (\dim_K L)^2 = n^2$  である。 $\Phi$  は有限次元ベクトル空間の間の単射  $K$ -線形写像であるため、次元の一致から自動的に全射となり、環同型であることが証明された。 ■

## 6. 中心化環と包含関係の反転機構

Galois の基本定理の核心となる「2回裏返すと元に戻る」という対応を、環論における中心化の概念を用いて定式化する。

### 定義 6.1 (中心化環)

環  $A$  とその部分集合  $X$  に対し、 $X$  のすべての元と可換であるような  $A$  の元全体のなす部分環

$$C_A(X) = \{a \in A \mid ax = xa \quad (\forall x \in X)\}$$

を、 $X$  の  $A$  における中心化環 (centralizer) と呼ぶ。

自己準同型環  $A = \text{End}_K(L)$  を考える。体  $L$  の各元  $a \in L$  は、 $L$  の元に左から掛け算を行うという線形変換  $\lambda_a(x) = ax$  を通じて、 $A$  の部分環とみなすことができる。以下、これを  $L_L \subset A$  と表記する。体の中間体  $M$  ( $K \subset M \subset L$ ) に対しても同様に  $M_L \subset A$  が定まる。

### 補題 6.2

中間体  $M$  に対し、部分環  $M_L$  の  $A = \text{End}_K(L)$  における中心化環は、 $M$ -線形な自己準同型環と完全に一致する。すなわち、

$$C_A(M_L) = \text{End}_M(L)$$

### 補題 6.2 の証明

$f \in A = \text{End}_K(L)$  が  $C_A(M_L)$  に属するための必要十分条件は、すべての  $m \in M$  に対して  $f \circ \lambda_m = \lambda_m \circ f$  が成り立つことである。任意の  $x \in L$  を代入すると、これは  $f(mx) = mf(x)$  と同値である。この性質は  $f$  が  $M$ -線形写像であることの定義そのものであるため、 $C_A(M_L) = \text{End}_M(L)$  が成り立つ。 ■

## 7. Galoisの基本定理の現代的証明

定理 5.1 の同型  $\Phi : L[G] \cong \text{End}_K(L)$  のもとで、中間体と Galois 群の部分群の一対一対応 (Galois 対応) が、計算を伴うことなく綺麗に導かれることを示す。

### 定理 7.1 (Galoisの基本定理)

$L/K$  を有限次 Galois 拡大とし、 $G = \text{Gal}(L/K)$  とする。このとき、

$$\mathcal{M} = \{M \mid K \subset M \subset L \text{ (中間体)}\}$$

$$\mathcal{H} = \{H \mid H \subset G \text{ (部分群)}\}$$

の間に、以下の互いに逆をなす一対一の写像 (バイジェクション) が存在する。

$$\mathcal{M} \longrightarrow \mathcal{H} \quad (M \longmapsto \text{Gal}(L/M))$$

$$\mathcal{H} \longrightarrow \mathcal{M} \quad (H \longmapsto L^H = \{x \in L \mid \sigma(x) = x \text{ } (\forall \sigma \in H)\})$$

### 定理 7.1 の証明

$A = \text{End}_K(L)$  と置く。定理 5.1 より、環の同型  $\Phi : L[G] \cong A$  が存在する。中間体  $M \in \mathcal{M}$  を固定したとき、補題 6.2 より  $C_A(M_L) = \text{End}_M(L)$  である。この部分環  $\text{End}_M(L)$  に対応する  $L[G]$  の部分集合を調べる。

$L[G]$  の元  $\sum_{\sigma \in G} a_\sigma \sigma$  が  $\text{End}_M(L)$  に属するための必要十分条件は、任意の  $m \in M$  および  $x \in L$  に対して

$$\sum_{\sigma \in G} a_\sigma \sigma(mx) = m \sum_{\sigma \in G} a_\sigma \sigma(x) \implies \sum_{\sigma \in G} a_\sigma \sigma(m)\sigma(x) = \sum_{\sigma \in G} a_\sigma m\sigma(x)$$

が成り立つことである。これが任意の  $x$  で成立するためには、各  $\sigma$  について  $a_\sigma \sigma(m) = a_\sigma m$ 、すなわち  $a_\sigma \neq 0$  であるならば  $\sigma(m) = m$  がすべての  $m \in M$  で成立しなければならない。これは  $\sigma \in \text{Gal}(L/M)$  であることと同値である。したがって、同型  $\Phi$  を通じて次の対応が得られる。

$$\text{End}_M(L) \cong L[\text{Gal}(L/M)] = \bigoplus_{\sigma \in \text{Gal}(L/M)} L\sigma$$

ここで、部分群  $H \in \mathcal{H}$  に対し、対応する部分環  $L[H] = \bigoplus_{\sigma \in H} L\sigma$  を考える。このとき、 $L[H]$  の  $L_L$  における中心化環  $C_{L_L}(L[H])$  を計算する。 $A$  の元としての左乗算  $\lambda_x$  ( $x \in L$ ) が  $L[H]$  のすべての元と可換であるとは、任意の  $\sigma \in H$  および  $y \in L$  に対して  $\lambda_x(\sigma(y)) = \sigma(\lambda_x(y))$ 、すなわち  $x\sigma(y) = \sigma(xy) = \sigma(x)\sigma(y)$  が成り立つことである。これが任意の  $y$  で成立することから  $x = \sigma(x)$  が導かれ、これは  $x \in L^H$  であることを意味する。ゆえに、以下が成り立つ。

$$C_{L_L}(L[H]) = (L^H)_L$$

以上の対応を組み合わせる。

- 中間体  $M$  に対し、 $H = \text{Gal}(L/M)$  と置く。このとき上記より  $\text{End}_M(L) \cong L[H]$  である。二重中心化環の一般性質 (あるいは  $M$  上の有限次元線形代数の議論) から、 $C_A(\text{End}_M(L)) = M_L$  が成り立つ。これの  $L_L$  内での交叉を考えると、

$$(L^H)_L = C_{L_L}(L[H]) = C_A(L[H]) \cap L_L = C_A(\text{End}_M(L)) \cap L_L = M_L \cap L_L = M_L$$

となり、各辺の元を比較することで  $L^H = M$ 、すなわち  $L^{\text{Gal}(L/M)} = M$  が得られる。

2. 部分群  $H$  に対し、 $M = L^H$  と置く。このとき上記より  $L[H] \subset L[\text{Gal}(L/M)]$  である。双方の  $K$  上の次元を比較する。定理 4.1 を中間体  $M$  に適用することで、 $[L : M] = |\text{Gal}(L/M)|$  である。また、自己準同型環の次元の性質から  $\dim_M(\text{End}_M(L)) = [L : M]^2$  であり、これより  $\dim_K(\text{End}_M(L)) = [L : M] \cdot [L : K]$  となる。一方で、ひねり群環の構成から  $\dim_K(L[\text{Gal}(L/M)]) = |\text{Gal}(L/M)| \cdot [L : K]$  である。これらが一致すること、および  $L[H]$  の次元が  $|H| \cdot [L : K]$  であることから、包含関係  $L[H] \subset L[\text{Gal}(L/M)]$  において双方の次元が一致するためには  $|H| = |\text{Gal}(L/M)|$  でなければならない。有限集合の部分群で位数が一致するため、 $\text{Gal}(L/L^H) = H$  が成り立つ。

一連の対応により、写像が互いに逆写像であることが示され、Galois 対応の一对一性が完全に証明された。 ■

## 8. 現代数学における視点

本稿で展開した  $L \otimes_K L \cong \prod L$  および  $L[G] \cong \text{End}_K(L)$  を経由する証明手法は、方程式の個別の根の計算を完全にバイパスし、空間の持つ対称性そのものを「環の分解」および「自己準同型環の表現」という強力な道具で記述するものです。

このアプローチは、N. Jacobson らによって **Jacobson-Bourbaki の定理 (Jacobson-Bourbaki theorem)** として一般化され、体が非可換である場合（斜体拡大）のガロア理論の構築へと繋がりました。さらに、A. Grothendieck による **エタール被覆 (étale coverings)** の理論の基礎となり、現代の代数幾何学におけるエタール基本群の定義へと直接的に直結しています。基礎を可換環上の拡大（ガロア被覆）へと拡張する際にも、このテンソル積と自己準同型環を用いた定式化がそのまま標準的な言語として使用されます。

### 参考文献

- Lang, S. (2002). *Algebra* (Revised 3rd ed.). Graduate Texts in Mathematics, Springer.  
<https://link.springer.com/book/10.1007/978-1-4613-0041-0>  
(代数学の世界的標準書。第6章においてGalois拡大にともなうテンソル積の完全分解およびひねり群環の同型が詳しく論じられている)
- Milne, J. S. (2022). *Fields and Galois Theory*.  
<https://www.jmilne.org/math/CourseNotes/FT.pdf>  
(洗練された現代的な記述が特徴の講義ノート。指標の独立性から導かれる構造同型や、Grothendieck的アプローチへの繋がりが自己完結的にまとめられている)
- Jacobson, N. (1964). *Lectures in Abstract Algebra: III. Theory of Fields and Galois Theory*. Graduate Texts in Mathematics, Springer.  
<https://link.springer.com/series/1387>  
(自己準同型環の性質と中心化環の理論を用いたガロア対応の構成、すなわち本稿のベースとなったJacobson-Bourbaki理論の古典的かつ詳細な教科書)