

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

目次

- 1 概要と解説の目的
- 2 基本概念の定義と準備
- 3 予備的補題とその証明
- 4 テンソル積の完全分解
- 5 応用としての次数の決定
- 6 自己準同型環の同型
- 7 中心化環と包含関係の反転機構
- 8 Galois の基本定理の現代的証明
- 9 現代数学における視点

概要と解説の目的 I

本講義では、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 理論の再構築を行う。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 対応の一対一性）の完成までを自己完結的 (self-contained) に解説する。

1. 基本概念の定義と準備 I

本講義において、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。

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。

1. 基本概念の定義と準備 II

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。

1. 基本概念の定義と準備 III

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

1. 基本概念の定義と準備 IV

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 I

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。

2. 予備的補題とその証明 II

補題 2.1 の証明

K が有限体の場合、拡大体 L も有限体。有限体の乗法群は巡回群であるため、生成元 g をとれば $L = K(g)$ 。

K が無限体の場合、 $L = K(\beta, \gamma)$ の場合を示せば帰納法により一般に帰着される。 β, γ の最小多項式を $p(X), q(X)$ とし、根をそれぞれ

$\beta = \beta_1, \dots, \beta_r$ および $\gamma = \gamma_1, \dots, \gamma_s$ とする。拡大の分離性より相異なる。任意の i および $j \geq 2$ に対して $\beta_i + c\gamma_j \neq \beta_1 + c\gamma_1$ となる $c \in K$ を選ぶ (有限個の禁止点を除く)。 $\alpha = \beta + c\gamma \in L$ と置く。

多項式 $h(X) = p(\alpha - cX)$ は $h(\gamma) = p(\beta) = 0$ 。 $h(X)$ と $q(X)$ の共通根を調べると、 c の選び方により共通根は γ のみとなる。よって $\gamma \in K(\alpha)$ 、 $\beta = \alpha - c\gamma \in K(\alpha)$ となり、 $L = K(\alpha)$ である。

2. 予備的補題とその証明 III

補題 2.2 (中国式剰余定理)

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。

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

2. 予備的補題とその証明 IV

補題 2.2 の証明

自然な環準同型写像 $\phi : R \rightarrow \prod_{k=1}^m R/I_k$ ($x \mapsto (x \bmod I_1, \dots)$) を考える。
核は明らかに $\bigcap_{k=1}^m I_k$ 。

$m = 2$ のとき、 $e_1 + e_2 = 1$ ($e_1 \in I_1, e_2 \in I_2$) より、 $x = r_2 e_1 + r_1 e_2$ と置けば $\phi(x) = (r_1 \bmod I_1, r_2 \bmod I_2)$ となり全射。

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

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

より I_1 と $\bigcap_{k=2}^m I_k$ は互いに素。帰納法により全射性が示される。

2. 予備的補題とその証明 V

補題 2.3 (Dedekind の指標の独立性定理)

相異なる体準同型 $\sigma_1, \dots, \sigma_m : L \rightarrow M$ 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 $c_i \in M$ はすべて 0。

2. 予備的補題とその証明 VI

補題 2.3 の証明

写像の個数 m による帰納法。 $m = 1$ のとき自明。

$m - 1$ で成立と仮定。 $\sum_{i=1}^m c_i \sigma_i(x) = 0$ とし、 c_i に非零が存在するとする。ある $y \in L$ で $\sigma_1(y) \neq \sigma_m(y)$ 。自変数を yx に代入した式から、元の式に $\sigma_m(y)$ を乗じたものを引くと、

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

帰納法の仮定より各係数は 0。特に $c_1 (\sigma_1(y) - \sigma_m(y)) = 0$ 。 $c_1 \neq 0$ と仮定していたため $\sigma_1(y) = \sigma_m(y)$ となり矛盾。

3. 主定理1：テンソル積 $L \otimes_K L$ の完全分解 I

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 Ψ は可換環の同型写像である。

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

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

定理 3.1 の証明

原始元定理より $L = K(\alpha)$ 。 α の最小多項式を $f(X) \in K[X]$ とすると $L \cong K[X]/(f(X))$ 。 Galois 拡大であるから $f(X)$ は完全に分解され $f(X) = \prod_{\sigma \in G} (X - \sigma(\alpha))$ 。

テンソル積の性質より同型 θ を得る。

$$\theta : L \otimes_K L \cong L[X]/(f(X)), \quad a \otimes g(\alpha) \mapsto a \cdot g(X) \pmod{f(X)}$$

中国剰余定理より同型 ω を得る。

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

合成写像 $\omega \circ \theta$ の行き先を計算すると、

$\omega(a \cdot g(X)) = (a \cdot g(\sigma(\alpha)))_{\sigma \in G} = (a\sigma(b))_{\sigma \in G}$ となり、これは ψ に一致する。 よって同型。

4. 応用としての次数の決定 I

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

同型 $\Psi : L \otimes_K L \xrightarrow{\cong} \prod_{\sigma \in G} L$ の両辺に、左から L の元 x を掛ける作用を定義し、左 L -ベクトル空間とみなす。 Ψ はこの作用と可換 ($\Psi(x \cdot (a \otimes b)) = x \cdot \Psi(a \otimes b)$) であるため、左 L -ベクトル空間としての同型。よって L 上の次元が一致する。

左辺について、 K 上の基底 v_1, \dots, v_n ($n = [L : K]$) を用いると、 $1 \otimes v_i$ は L 上の基底となるため、 $\dim_L(L \otimes_K L) = [L : K]$ 。

右辺について、 $|G|$ 個の L の直積であるため次元はそのまま成分の個数、 $\dim_L(\prod_{\sigma \in G} L) = |G|$ 。次元の比較より $[L : K] = |G|$ 。

5. 主定理 2 : 自己準同型環の同型 I

定理 5.1

有限次 Galois 拡大 L/K に対し、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 Φ は、環としての同型写像である。

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

5. 主定理 2 : 自己準同型環の同型 II

定理 5.1 の証明

積の保存は $\Phi(a\sigma(b)\sigma\tau)(x) = a\sigma(b\tau(x))$ より従う。和と分配法則も自明であり、 Φ は環準同型。

$\Phi(\sum a_\sigma\sigma) = 0$ とすると全 x で $\sum a_\sigma\sigma(x) = 0$ 。Dedekind の指標の独立性 (補題 2.3) より全 σ で $a_\sigma = 0$ となり、単射。

次元を比較する。定理 4.1 より $|G| = n = [L : K]$ と置くと、
 $\dim_K(L[G]) = n \times n = n^2$ 。また $\dim_K(\text{End}_K(L)) = n^2$ 。次元の一致と単射性より全射。よって同型。

6. 中心化環と包含関係の反転機構 I

定義 6.1 (中心化環)

環 A と部分集合 X に対し、 X の全元と可換な A の元全体のなす部分環 $C_A(X) = \{a \in A \mid ax = xa \quad (\forall x \in X)\}$ を中心化環と呼ぶ。

$A = \text{End}_K(L)$ を考える。 L の元 a による左乗算作用を $\lambda_a(x) = ax$ とし、これを $L_L \subset A$ と表す。中間体 M に対しても $M_L \subset A$ が定まる。

補題 6.2

中間体 M に対し、 $C_A(M_L) = \text{End}_M(L)$ が成り立つ。

補題 6.2 の証明

$f \in C_A(M_L)$ の条件は、任意の $m \in M$ に対し $f \circ \lambda_m = \lambda_m \circ f$ 。これは $f(mx) = mf(x)$ と同値であり、 f が M -線形写像である定義そのもの。

7. Galois の基本定理の現代的証明 I

定理 7.1 (Galois の基本定理)

中間体全体の集合 \mathcal{M} と部分群全体の集合 \mathcal{H} の間に、互いに逆の一一対応が存在する。

$$\mathcal{M} \longrightarrow \mathcal{H} \quad (M \mapsto \text{Gal}(L/M)), \quad \mathcal{H} \longrightarrow \mathcal{M} \quad (H \mapsto L^H)$$

7. Galois の基本定理の現代的証明 II

定理 7.1 の証明

同型 $\Phi : L[G] \cong A = \text{End}_K(L)$ のもと、部分環 $\text{End}_M(L)$ に対応する $L[G]$ の元 $\sum a_\sigma \sigma$ を調べる。 $\sum a_\sigma \sigma(mx) = m \sum a_\sigma \sigma(x)$ より

$a_\sigma \neq 0 \Rightarrow \sigma \in \text{Gal}(L/M)$ 。よって $\text{End}_M(L) \cong L[\text{Gal}(L/M)]$ 。

逆に、部分群 H に対し $L[H]$ の L_L における中心化環を考えると、

$x\sigma(y) = \sigma(xy)$ より $x = \sigma(x)$ となり、 $C_{L_L}(L[H]) = (L^H)_L$ 。

(1) M から出発して $H = \text{Gal}(L/M)$ とすると、二重中心化環の一般性質から $C_A(\text{End}_M(L)) = M_L$ 。これと L_L の交叉から $L^{\text{Gal}(L/M)} = M$ 。

(2) H から出発して $M = L^H$ とすると、 $L[H] \subset L[\text{Gal}(L/M)]$ 。次元を計算すると双方ともに等しくなるため、位数が一致し $H = \text{Gal}(L/L^H)$ が従う。

8. 現代数学における視点 I

本講義で展開した $L \otimes_K L \cong \prod L$ 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ある。

このアプローチは、N. Jacobson らによって **Jacobson-Bourbaki の定理** として一般化され、斜体拡大のガロア理論の構築へと繋がった。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る。