Artin の定理を経由する Galois の基本定理の証明

講義用スライド資料

代数学講義

June 13, 2026

目次

定義 1.1 (体の拡大と自己同型群)

定義 1.1

- 体 L が体 K を部分体として含むとき、L を K の**拡大体**といい、L/K と表す。
- L は K 上のベクトル空間であり、その次元 $[L:K]$ を**拡大次数**と呼ぶ。$[L:K] < \infty$ のとき**有限次拡大**と呼ぶ。
- 体 L の自己同型全体のなす群を $\mathrm{Aut}(L)$ と書く。
- 部分体 K の元を全て固定する自己同型のなす部分群を $\mathrm{Aut}(L/K)$ または $\mathrm{Gal}(L/K)$ と書き、L/K の **Galois 群**と呼ぶ。
- 有限群 $G \subset \mathrm{Aut}(L)$ に対して、$L^G = \{x \in L \mid \forall \sigma \in G, \sigma(x) = x\}$ を G の**不変体**と呼ぶ。

定義 1.2 (分離性と正規性、および Galois 拡大)

定義 1.2

体 K 上の代数的な元 α の K 上の最小多項式を考える。

- **分離的 (separable):** 最小多項式が代数閉包において重根を持たないとき、α は K 上分離的という。すべての元が分離的な拡大を**分離拡大**と呼ぶ。
- **正規 (normal):** K 上の任意の既約多項式が L に根を持つならば、その多項式が L 上で一次式の積に完全に分解されるとき、L/K を**正規拡大**と呼ぶ。
- **Galois 拡大 (Galois extension):** 有限次拡大 L/K が分離拡大かつ正規拡大であるとき、これを**有限次 Galois 拡大**と呼ぶ。

命題 1.3 (Galois 群の共役元への推移的作用)

命題 1.3

L/K が有限次 Galois 拡大であるとする。任意の $\alpha \in L$ と、α の K 上での任意の共役元 $\beta \in L$（すなわち α の K 上の最小多項式の根）に対して、ある $\sigma \in \mathrm{Gal}(L/K)$ が存在して

$$\sigma(\alpha) = \beta$$

となる。

命題 1.3 の証明 (1/2)

Proof.

L/K は有限次分離拡大であるから、**原始元定理**により $L = K(\theta)$ となる元 $\theta \in L$ が存在する。α と β は K 上共役であるため同じ最小多項式 $p(x) \in K[x]$ を持ち、$\alpha \mapsto \beta$ と写し K の元を固定する同型写像 $\phi : K(\alpha) \xrightarrow{\sim} K(\beta)$ が一意に存在する。

ここで、θ の $K(\alpha)$ 上の最小多項式を $h_1(x) \in K(\alpha)[x]$ とする。ϕ によって $h_1(x)$ の各係数を $K(\beta)$ の元に写して得られる多項式を $h_2(x) \in K(\beta)[x]$ とおく。

θ の K 上の最小多項式 $F(x) \in K[x]$ を考えると、$F(\theta) = 0$ であるため、$h_1(x)$ は $K(\alpha)[x]$ において $F(x)$ の約数である（$F(x) = h_1(x)q_1(x)$）。$F(x)$ の係数は K に属するため ϕ によって不変であり、したがって $h_2(x)$ も $K(\beta)[x]$ において $F(x)$ の約数となる。 □

命題 1.3 の証明 (2/2)

証明（続き）.

L/K は正規拡大であるため、K 上の多項式 $F(x)$ は L 内で一次式に完全に分解する。よってその約数である $h_2(x)$ も L 内に根を持つ。その根の一つを $\theta' \in L$ とする。
多項式環の剰余環としての単拡大の構成定理より、以下の自然な同型の連鎖が得られる：

$$L = K(\alpha)(\theta) \cong K(\alpha)[x]/(h_1(x)) \xrightarrow{\tilde{\phi}} K(\beta)[x]/(h_2(x)) \cong K(\beta)(\theta')$$

$\theta' \in L$ ゆえ $K(\beta)(\theta') \subseteq L$ であり、上の同型によって $[K(\beta)(\theta') : K] = [L : K]$ であるから、$K(\beta)(\theta') = L$ となる。
この連鎖を合成して得られる同型写像 $\sigma : L \xrightarrow{\sim} L$ は、K の元を固定し、$\theta \mapsto \theta'$、および $\alpha \mapsto \beta$ を満たす。したがって、$\sigma \in \mathrm{Gal}(L/K)$ であり、$\sigma(\alpha) = \beta$ が直接的に示された。 □

例 1.4 (複素数体と実数体の拡大)

例 1.4

複素数体 $\mathbb{C}$ と実数体 $\mathbb{R}$ の拡大 $\mathbb{C}/\mathbb{R}$ を考える。

- $\mathbb{C}$ の任意の元 $a + bi$ の $\mathbb{R}$ 上の最小多項式は高々 2 次であり、虚数部がゼロでなければ $x^2 - 2ax + a^2 + b^2$ となる。
- これは重根を持たず（分離的）、かつ $\mathbb{C}$ 上で完全に一次式に分解される（正規）。したがって $\mathbb{C}/\mathbb{R}$ は Galois 拡大。
- $\mathbb{C}$ 上の自己同型で $\mathbb{R}$ を固定するものは、恒等写像 id と複素共役 $\sigma(a + bi) = a - bi$ のみ。
- したがって $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \sigma\}$ であり、不変体 $\mathbb{C}^{\{\mathrm{id},\sigma\}}$ は $\mathbb{R}$ に一致する。

補題 2.1

体 Ω 上のベクトル空間 V の $v_1, \ldots, v_n \in V$ で張られる部分空間を W と書く。$i \neq j$ に対して W の一次変換 T_{ij} が与えられており、各 $v_k \neq 0$ は、固有値 λ_k^{ij} を持つ T_{ij} の固有ベクトルであって、$\lambda_i^{ij} \neq \lambda_j^{ij}$ を満たしているとする。このとき以下が成立する。

1. $i = 1, \ldots, n$ に対して W の一次変換 L_i を次で定めると、$L_i v_j = \delta_{ij} v_i$ である。

$$L_i = \prod_{j \in \{1,\ldots,n\} \setminus \{i\}} \frac{T_{ij} - \lambda_j^{ij} \mathrm{id}_W}{\lambda_i^{ij} - \lambda_j^{ij}}$$

2. $v_1, \ldots, v_n$ は Ω 上一次独立である。

補題 2.1 の証明

Proof.

(1) $(T_{ij} - \lambda_j^{ij}\mathrm{id}_W)v_k = (\lambda_k^{ij} - \lambda_j^{ij})v_k$ である。
$k \neq i$ ならば、積 L_i の因子の中に $j = k$ となる項が存在し、分子が $(\lambda_k^{ik} - \lambda_k^{ik})v_k = 0$ となるため、$L_i v_k = 0$ である。
$k = i$ の場合、すべての $j \neq i$ に対して分子は $(\lambda_i^{ij} - \lambda_j^{ij})v_i$ となり、分母と相殺される。したがって $L_i v_i = v_i$。以上より $L_i v_j = \delta_{ij} v_i$。
(2) $\sum_{j=1}^n c_j v_j = 0$ $(c_j \in \Omega)$ とする。この両辺に L_i を作用させると、

$$L_i \left(\sum_{j=1}^n c_j v_j \right) = \sum_{j=1}^n c_j L_i v_j = c_i v_i = 0$$

$v_i \neq 0$ より $c_i = 0$ を得る。これが任意の i で成り立つため一次独立。 □

定理 2.2 (Dedekind の補題)

定理 2.2 (Dedekind の補題)

半群 H から体 Ω への相異なる半群準同型 $\sigma_1, \ldots, \sigma_n : H \to \Omega^\times$ は、H 上の Ω に値を持つ関数達として一次独立である。ただし $\Omega^\times = \Omega \setminus \{0\}$。

Dedekind の補題の証明

Proof.

V を写像空間、$v_k = \sigma_k \in V$ $(v_k \neq 0)$、$W = \langle v_1, \ldots, v_n \rangle$ とする。
σ_i は相異なるので、$\forall i \neq j, \exists h_{ij} \in H$ s.t. $\sigma_i(h_{ij}) \neq \sigma_j(h_{ij})$。
W 上の一次変換 T_{ij} を $(T_{ij}f)(x) = f(h_{ij}x)$ で定義する。
準同型の性質から次が成り立つ：

$$(T_{ij}\sigma_k)(x) = \sigma_k(h_{ij}x) = \sigma_k(h_{ij})\sigma_k(x)$$

すなわち $T_{ij}v_k = \sigma_k(h_{ij})v_k$ であり、v_k は固有値 $\lambda_k^{ij} = \sigma_k(h_{ij})$ を持つ固有ベクトル。
h_{ij} の選び方から $\lambda_i^{ij} \neq \lambda_j^{ij}$。補題 2.1 より、$\sigma_1, \ldots, \sigma_n$ は一次独立。 □

注意 (体の準同型と Dedekind の補題)

注意

体 L から体 Ω への体の準同型は、積の構造を保つため、L の乗法群 $H = L^{\times}$ から Ω の乗法群 $\Omega^{\times}$ への半群準同型（群準同型）を与えます。

したがって、体 L から体 Ω への相異なる体の準同型たちは、**Dedekind の補題**によって、直ちに関数達として Ω 上一次独立であることが従います。

命題 3.1 (トレース写像の非退化性)

命題 3.1

体 L、自己同型群 $G = \{\sigma_1, \ldots, \sigma_n\}$、不変体 $K = L^G$ を考える。
トレース写像 $\mathrm{Tr}_{L/K} : L \to K$ を $\mathrm{Tr}_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x)$ で定義する（これは K 線形写像)。

このとき、すべての $y \in L$ について $\mathrm{Tr}_{L/K}(xy) = 0$ となる $x \in L$ は $x = 0$ しかない。

命題 3.1 の証明

Proof.

ある $x \in L$ について、任意の $y \in L$ に対して $\mathrm{Tr}_{L/K}(xy) = 0$ と仮定。

$$\mathrm{Tr}_{L/K}(xy) = \sum_{i=1}^{n} \sigma_i(xy) = \sum_{i=1}^{n} \sigma_i(x)\sigma_i(y) = 0$$

これは $L^\times$ 上の関数としての一次関係式 $\sum_{i=1}^{n} \sigma_i(x)\sigma_i = 0$ を意味する。
Dedekind の補題より、相異なる自己同型 $\sigma_1, \ldots, \sigma_n$ は L 上一次独立である。
したがって、すべての係数がゼロでなければならないため、各 i に対して $\sigma_i(x) = 0$ となる。
σ_i は同型写像であるから、これを満たすのは $x = 0$ のみである。 □

定理 4.1 (Artin の定理)

定理 4.1 (Artin の定理)

体 L とその自己同型の位数 n の有限群 G、および不変体 $K = L^G$ を考える。このとき

$$[L : K] = n$$

であり、L/K は Galois 拡大である。さらに $G = \mathrm{Gal}(L/K)$ となる。

Artin の定理の証明 (1)

Proof.

(1) まず $\dim_L \mathrm{End}_K(L) = [L : K]$ を示す。
$\mathrm{End}_K(L)$ は K 上の線形自己準同型環であり、左からの積作用により L 上のベクトル空間とみなせる。

- $[L : K] = m < \infty$ ならば、$\mathrm{End}_K(L) \cong M_m(K)$（行列環）であり、$\dim_K \mathrm{End}_K(L) = m^2$。よって $\dim_L \mathrm{End}_K(L) = m^2/m = m = [L : K]$。
- $[L : K] = \infty$ ならば、$\dim_L \mathrm{End}_K(L) = \infty$ となり成立。

□

Artin の定理の証明 (2) - 単射性

証明（続き）.

(2) 自然な写像 $\Phi : L[G] \to \mathrm{End}_K(L)$ が同型になることを示す。
接合環 $L[G]$ の元 $\sum_{\sigma \in G} a_\sigma \sigma$ に対し、$\Phi(\sum a_\sigma \sigma)(x) = \sum a_\sigma \sigma(x)$ とする。

- Φ は環準同型である（構造から容易に確認できる）。
- $\Phi(\sum_{\sigma \in G} a_\sigma \sigma) = 0$ とすると、任意の x で $\sum a_\sigma \sigma(x) = 0$。Dedekind の補題（一次独立性）より、すべての σ で $a_\sigma = 0$ となり、Φ **は単射**。

□

Artin の定理の証明 (2) - 全射性 (Galois 降下)

証明（続き）.

写像 $\Psi : L \otimes_K L \to \mathrm{End}_K(L)$ を $\Psi(a \otimes b)(x) = a\mathrm{Tr}_{L/K}(bx)$ と定義。

$$\Psi(a \otimes b) = a \sum_{\sigma \in G} \sigma(b)\sigma \in \Phi(L[G]) \implies \mathrm{Im}(\Psi) \subset \mathrm{Im}(\Phi)$$

$\sum_{i=1}^{r} a_i \otimes b_i \in \ker(\Psi)$ とし、$\{a_i\}$ を K 上一次独立とする。
$\forall x, \sum a_i \mathrm{Tr}_{L/K}(b_i x) = 0 \implies \forall i, \mathrm{Tr}_{L/K}(b_i x) = 0$ (a_i の一次独立性より)。
トレースの非退化性（命題 3.1）から $b_i = 0$ となり、Ψ は単射。
$\dim_L(L \otimes_K L) = [L : K] = \dim_L \mathrm{End}_K(L)$（有限次元の場合）より、$\Psi$ は全射（同型）。
したがって $\mathrm{End}_K(L) = \mathrm{Im}(\Psi) \subset \mathrm{Im}(\Phi) \subset \mathrm{End}_K(L)$ から Φ も全射。
次元を比較して、$[L : K] = \dim_L L[G] = |G| = n$。 □

Artin の定理の証明 (3) - Galois 拡大の導出

証明（続き）.

(3) L/K が分離的かつ正規拡大であることを示す。
任意の $\alpha \in L$ に対し、群作用による軌道を $\{\alpha_1, \ldots, \alpha_r\}$ $(\alpha_1 = \alpha)$ とする。
多項式 $f(x) = \prod_{i=1}^{r}(x - \alpha_i)$ は G の作用で不変。係数は $L^G = K$ に属するので $f(x) \in K[x]$。
α の K 上の最小多項式 $p(x)$ は $f(x)$ を割り切る。
$f(x)$ は重根を持たず（分離的）、L 内で完全に分解する（正規）。その約数である $p(x)$ も分離的かつ正規。
よって L/K は Galois 拡大。また $[L : K] = n = |G| \leq |\mathrm{Gal}(L/K)| \leq [L : K]$ より
$G = \mathrm{Gal}(L/K)$。 □

定理 5.1 (Galois の基本定理)

定理 5.1 (Galois の基本定理)

L/K を有限次 Galois 拡大、$G = \mathrm{Gal}(L/K)$ とする。
中間体 M ($K \subset M \subset L$) と、G の部分群 H の間に一対一の全単射（Galois 対応）が存在する。

$$\alpha(M) = \mathrm{Gal}(L/M), \quad \beta(H) = L^H$$

Galois の基本定理の証明 (1) - 包含関係

Proof.

包含関係の片側を定義から示す：

1. $M \subset \beta(\alpha(M))$ **の証明：**
   $\alpha(M) = \mathrm{Gal}(L/M)$ は M を固定する群。よって $\forall x \in M$ は $\mathrm{Gal}(L/M)$ で固定されるため、$x \in L^{\mathrm{Gal}(L/M)} = \beta(\alpha(M))$。
2. $H \subset \alpha(\beta(H))$ **の証明：**
   $\beta(H) = L^H$ は H で固定される体。よって H の任意の元 σ は L^H を固定するため、$\sigma \in \mathrm{Gal}(L/L^H) = \alpha(\beta(H))$。

□

Galois の基本定理の証明 (2) - $H = \alpha(\beta(H))$

証明（続き）.

$H = \alpha(\beta(H))$ の等号：
$H \subset G$ を任意の部分群とし、不変体 $M' = \beta(H) = L^H$ を考える。

Artin の定理（定理 4.1）を体 L と部分群 H に対し適用する。

- $[L : L^H] = |H|$ となる。
- さらに L/L^H は Galois 拡大であり、その Galois 群は H に一致する。

すなわち、$\mathrm{Gal}(L/L^H) = H$。
これは定義より $\alpha(\beta(H)) = H$ を意味する。 □

Galois の基本定理の証明 (3) - $M = \beta(\alpha(M))$

証明（続き）.

$M = \beta(\alpha(M))$ **の等号：**
$M' = \beta(\alpha(M))$ とおく。$M \subset M'$ は既知。
先ほどの結果に $H = \alpha(M)$ を代入すると、$\alpha(M') = \alpha(M)$ を得る。
もし $M \subsetneq M'$ ならば、ある $\gamma \in M' \setminus M$ が存在。
L/M も有限次 Galois 拡大であり、γ の M 上の最小多項式 $p(x)$ は $\deg p \geq 2$ かつ分離的。
よって $\gamma \neq \gamma'$ なる共役元 $\gamma' \in L$ を持つ。
ここで**命題 1.3** を L/M に適用すると、$\sigma(\gamma) = \gamma'$ となる $\sigma \in \mathrm{Gal}(L/M) = \alpha(M)$ が存在する。
しかし $\alpha(M) = \alpha(M')$ なので、σ は M' の元 γ を固定しなければならず、$\sigma(\gamma) = \gamma$。これは矛盾。
したがって $M = M' = \beta(\alpha(M))$。 □

参考文献

- Artin, E. (1971). *Galois Theory: Lectures Delivered at the University of Notre Dame* (Notre Dame Mathematical Lectures, Number 2). Project Euclid.
- Lang, S. (2002). *Algebra* (Revised 3rd ed.). Springer.