# 有限次 Galois 拡大における 4 つの同値条件の完全証明

自己完結版

June 14, 2026

# 目次

# 1. 基本概念の定義と具体例 I

本稿を通じて用いる基本的な代数的概念を厳密に定義する。以下、断りのない限り $L/K$ は体の拡大を表し、$[L : K]$ は $K$ 上のベクトル空間としての $L$ の次元（拡大次数）を表す。本稿では有限次拡大、すなわち $[L : K] < \infty$ の場合を扱う。また、$\mathrm{Aut}(L/K)$ は $K$ の各元を固定する $L$ の体自己同型全体のなす群を表す。

# 1. 基本概念の定義と具体例 II

## 定義 1 (基本概念の定義)

- **代数拡大 *(algebraic extension)***: 拡大 $L/K$ の任意の元 $\alpha \in L$ に対し、$\alpha$ を根に持つような $K$ 上の非零多項式 $f(x) \in K[x]$ が存在するとき、$L/K$ は代数拡大であるという。
- **最小多項式 *(minimal polynomial)***: 代数的な元 $\alpha \in L$ に対し、$\alpha$ を根に持つ $K[x]$ のモニックな既約多項式を $\alpha$ の $K$ 上の最小多項式と呼ぶ。
- **分離的 *(separable)***: 既約多項式 $f(x) \in K[x]$ がその代数閉包 $\overline{K}$ において重根を持たないとき、$f(x)$ は分離多項式であるという。元 $\alpha \in L$ の最小多項式が分離多項式であるとき、$\alpha$ は $K$ 上分離的であるという。$L$ のすべての元が $K$ 上分離的であるとき、拡大 $L/K$ は分離拡大であるという。
- **正規拡大 *(normal extension)***: 既約多項式 $f(x) \in K[x]$ が $L$ に少なくとも $1$ つの根を持つならば、$L[x]$ において一次式の積に完全に分解するとき、拡大 $L/K$ は正規拡大であるという。
- **最小分解体 *(splitting field)***: 多項式 $f(x) \in K[x]$ に対し、ある拡大

# 正規性と分離性の具体例 I

## 例 2 (正規性と分離性の具体例)

- $L = \mathbb{Q}(\sqrt[3]{2})$ と $K = \mathbb{Q}$ を考える。$\sqrt[3]{2}$ の $K$ 上の最小多項式は $x^3 - 2$ である。この多項式は $\mathbb{Q}$ 上既約であり、$\overline{\mathbb{Q}}$ における根は相異なる 3 つの複素数となるため分離的であるが、虚数根が $L$ に含まれないため、$L/K$ は正規拡大ではない。
- 標数 $p > 0$ の素体 $\mathbb{F}_p$ 上の一変数有理関数体 $K = \mathbb{F}_p(t^p)$ と、その拡大体 $L = \mathbb{F}_p(t)$ を考える。$t \in L$ の $K$ 上の最小多項式は $x^p - t^p$ であるが、これは $(x - t)^p$ と因数分解されるため、$t$ を $p$ 重根として持つ。したがって、この拡大は分離拡大ではない。

# 2. 前提となる定理・補題の証明 I

同値性の証明に先立ち、必要となるすべての基本定理を完全に証明し、自己完結した議論を行う。

## 補題 3 (Dedekind の写像の線形独立性)

$L, M$ を任意の体とする。$L$ から $M$ への相異なる体準同型 $\sigma_1, \ldots, \sigma_n$ は、$M$ 上線形独立である。すなわち、$\lambda_1, \ldots, \lambda_n \in M$ に対して、すべての $x \in L$ で $\sum_{i=1}^{n} \lambda_i \sigma_i(x) = 0$ が成り立つならば、$\lambda_1 = \cdots = \lambda_n = 0$ である。

# 2. 前提となる定理・補題の証明 II

## 証明.

非零の係数を持つ線形従属な関係式が存在すると仮定し、項数 $k$ が最小のものを $\sum_{i=1}^{k} \lambda_i \sigma_i(x) = 0$ とする。$\sigma_1 \neq \sigma_k$ より、ある $\alpha \in L$ が存在して $\sigma_1(\alpha) \neq \sigma_k(\alpha)$ となる。任意数 $x \in L$ に対し、上の式に $\alpha x$ を代入すると、

$$\sum_{i=1}^{k} \lambda_i \sigma_i(\alpha)\sigma_i(x) = 0$$

一方で、元の関係式に $\sigma_k(\alpha)$ を乗じると、

$$\sum_{i=1}^{k} \lambda_i \sigma_k(\alpha)\sigma_i(x) = 0$$

これら 2 式の差をとると、第 $k$ 項が相殺され、

$$\sum_{}^{k-1} \lambda_i(\sigma_i(\alpha) - \sigma_k(\alpha))\sigma_i(x) = 0$$

# Artin の定理 I

**定理 4 (Artin の定理)**

体 $L$ と、$\mathrm{Aut}(L)$ の有限部分群 $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ を考える。
$K = L^G$ とおくと、拡大次数について $[L : K] = n = |G|$ が成立する。

# Artin の定理 II

## 証明.

**(Step 1) $[L : K] \geq n$ の証明**
$[L : K] = m < n$ と仮定する。$K$ 上の $L$ の基底を $\omega_1, \ldots, \omega_m$ とする。次のような方程式系を考える：

$$\sum_{j=1}^{n} \sigma_j(\omega_i) x_j = 0 \quad (i = 1, \ldots, m)$$

式の数 $m$ が未知数の数 $n$ より少ないため、非自明な解 $(x_1, \ldots, x_n)$ を持つ。任意の $\alpha = \sum_{i=1}^{m} a_i \omega_i \in L$ に対し、$a_i \in K$ を乗じて $i$ について和をとると、

$$\sum_{j=1}^{n} \sigma_j(\alpha) x_j = 0$$

これは体自己同型が $L$ 上線形従属であることを意味し、補題 1 に矛盾する。したがって $[L : K] \geq n$。
**(Step 2) $[L : K] \leq n$ の証明**

# 埋め込みの数と根の数 I

## 補題 5 (単一拡大における埋め込みの数と根の数)

$K(\alpha)/K$ を単一拡大とし、$\alpha$ の $K$ 上の最小多項式を $p(x)$ とする。$K$ を固定する埋め込み $\sigma : K(\alpha) \to \overline{K}$ の総数は、$p(x)$ の $\overline{K}$ における相異なる根の数に等しい。また、この総数が $[K(\alpha) : K]$ と一致することと、$\alpha$ が $K$ 上分離的であることは同値である。

## 証明.

$K(\alpha)$ の任意の元は $g(\alpha)$ と表せる。$\sigma$ の効果は $\sigma(\alpha)$ の行き先だけで決定される。$0 = \sigma(p(\alpha)) = p(\sigma(\alpha))$ より、$\sigma(\alpha)$ は $p(x)$ の根でなければならない。逆に $p(x)$ の任意の根 $\beta$ に対し、$\alpha \mapsto \beta$ とする準同型が定まる。埋め込みの総数は相異なる根の数に等しく、これが次数と一致するのは重根を持たない（分離的）ことの定義そのものである。 □

# 分離次数の性質 I

## 定理 6 (分離次数の性質と分離元生成の拡大)

有限次拡大 $L/K$ に対し、$\overline{K}$ への $K$ 準同型の総数を分離次数 $[L : K]_s$ と定義する。

1. **乗法性**: 中間体 $M$ に対し $[L : K]_s = [L : M]_s[M : K]_s$
2. **次数不等式**: $[L : K]_s \leq [L : K]$ であり、等号成立は分離拡大と同値。
3. **分離元による生成**: $\alpha_1, \ldots, \alpha_r$ がすべて分離的であれば、$K(\alpha_1, \ldots, \alpha_r)/K$ も分離拡大。

# 分離次数の性質 II

**証明.**

1. 埋め込みの拡張と合成から明らか。
2. 単一拡大の塔に分解し、各段階で補題 3 を適用。等号成立は各段階の生成元が分離的であることと同値。
3. $\alpha_2$ の $K$ 上の最小多項式 $f(x)$ は重根を持たない。$M = K(\alpha_1)$ 上の最小多項式 $g(x)$ は $f(x)$ を割り切るため、やはり重根を持たない。乗法性と 2 より $K(\alpha_1, \alpha_2)/K$ は分離拡大。帰納法により成立。 □

# 最小分解体の正規性 I

## 定理 7 (最小分解体の正規性)

$L$ が多項式 $f(x) \in K[x]$ の $K$ 上の最小分解体であるならば、$L/K$ は正規拡大である。

## 証明.

$f(x)$ の $L$ における根全体を $\alpha_1, \ldots, \alpha_m$ とすると $L = K(\alpha_1, \ldots, \alpha_m)$。任意の $K$ 埋め込み $\sigma$ は根を置換するため $\sigma(L) = L$。$g(x) \in K[x]$ を $L$ に根 $\beta$ を持つ既約多項式とする。$\overline{K}$ の他の根 $\gamma$ への埋め込みを $L$ に拡張すると $\sigma(L) = L$ より $\gamma \in L$ となる。よって正規拡大。 □

# 4 つの条件

以下の 4 つの条件が互いに同値であることを、12 通りの含意について直接証明する。

## 同値な 4 条件

(1) $L/K$ は分離的正規拡大である。

(2) $L^G = K$ である。

(3) $[L : K] = |G|$ である。

(4) $L$ は重根を持たないある既約多項式 $f(x) \in K[x]$ の $K$ 上での最小分解体である。

# (1) ⇒ (2) の証明 I

**【分離次数を使わない証明】**
$L^G \subset K$ を示す。任意の $\alpha \in L \setminus K$ をとり、最小多項式を $p(x)$ とする。分離性より重根を持たず、正規性より $L$ で分解する。$\alpha \notin K$ より $\deg p \geq 2$ なので、異なる根 $\beta \in L$ が存在する。$\alpha \mapsto \beta$ となる $L$ の自己同型 $\sigma \in G$ が存在し $\sigma(\alpha) \neq \alpha$ となるため、$\alpha \notin L^G$。よって $L^G = K$。

**【分離次数を使う証明】**
分離性より $[L : K]_s = [L : K]$。正規性より $[L : K]_s = |G|$。ゆえに $[L : K] = |G|$。Artin の定理より $[L : L^G] = |G|$。次数の連鎖律 $[L : K] = [L : L^G][L^G : K]$ より $[L^G : K] = 1$。よって $L^G = K$。

# (1) ⇒ (3) の証明 I

**【分離次数を使わない証明】**
既に (1) ⇒ (2) により $L^G = K$ が示されている。Artin の定理より $[L : L^G] = |G|$ であるから、直ちに $[L : K] = |G|$ を得る。

**【分離次数を使う証明】**
分離性より $[L : K]_s = [L : K]$、正規性より $[L : K]_s = |G|$。これらを直接結ぶことで、$[L : K] = |G|$ が直ちに得られる。

# (1) ⇒ (4) の証明 I

**【分離次数を使わない証明】**
$L = K(\alpha_1, \ldots, \alpha_m)$ と表す。各 $\alpha_i$ の最小多項式 $p_i(x)$ は、分離性より重根を持たず、正規性より $L$ で分解する。$p_1(x) \cdots p_m(x)$ の無平方部分を $f(x)$ とすれば、$L$ は $f(x)$ の最小分解体となる。

**【分離次数を使う証明】**
分離性より（定理 2.4-2 から）各元の最小多項式は重根を持たない。正規性により $L$ で分解する。同様に無平方部分 $f(x)$ をとることで構成できる。

# (2) ⇒ (1) の証明 I

**【分離次数を使わない証明】**
任意の $\alpha \in L$ の軌道を $S = \{\sigma(\alpha) \mid \sigma \in G\} = \{\alpha_1, \ldots, \alpha_k\}$ とし、$g(x) = \prod_{i=1}^{k}(x - \alpha_i)$ を考える。係数は $G$ 不変であり、(2) より $L^G = K$ なので $g(x) \in K[x]$。構成から $g(x)$ は相異なる根のみを持ち完全に分解する。$\alpha$ の最小多項式は $g(x)$ を割り切るため、分離的かつ正規である。

**【分離次数を使う証明】**
Artin の定理 $[L : L^G] = |G|$ に $L^G = K$ を代入し $[L : K] = |G|$。一般に $|G| \leq [L : K]_s \leq [L : K]$ であるから、すべての不等号が等号になる。$[L : K]_s = [L : K]$ より分離的、$|G| = [L : K]_s$ より正規である。

# (2) ⇒ (3) の証明 I

**【分離次数を使わない証明 / 使う証明 (共通)】**
Artin の定理により $[L : L^G] = |G|$。ここに仮定 (2) である $L^G = K$ を直接代入することにより、直ちに $[L : K] = |G|$ が導かれる。

# (2) ⇒ (4) の証明 I

**【分離次数を使わない証明】**
(2) ⇒ (1) の証明により、$L/K$ が分離的かつ正規であることが示される。
その後は (1) ⇒ (4) と全く同じ手順で無平方部分 $f(x)$ を構成する。

**【分離次数を使う証明】**
(2) ⇒ (1) の分離次数を使う証明により分離的正規性を得て、同様に $f(x)$ を構成する。

# (3) ⇒ (1) の証明 I

**【分離次数を使わない証明】**
単一拡大の塔 $K_i = K_{i-1}(\beta_i)$ を考える。各段階の埋め込みの拡張数は最大で $[K_i : K_{i-1}]$ であり、重根を持たず根が $L$ に含まれるときに最大となる。$|G| \leq \prod[K_i : K_{i-1}] = [L : K]$ であり、仮定 (3) より等号が成立。すべての段階で拡張可能数は最大かつ像は $L$ に含まれるため、すべての元の最小多項式は重根を持たず $L$ で分解する。

**【分離次数を使う証明】**
$|G| \leq [L : K]_s \leq [L : K]$ において仮定より両端が一致するため、
$[L : K]_s = [L : K]$（分離的）および $|G| = [L : K]_s$（正規的）が同時に成立する。

# (3) ⇒ (2) の証明 I

**【分離次数を使わない証明 / 使う証明 (共通)】**
次数の連鎖律 $[L : K] = [L : L^G][L^G : K]$ に、Artin の定理 $[L : L^G] = |G|$ と仮定 (3) の $[L : K] = |G|$ を代入すると、$|G| = |G|[L^G : K]$。よって $[L^G : K] = 1$ となり $L^G = K$ を得る。

# (3) ⇒ (4) の証明 I

**【分離次数を使わない証明 / 使う証明 (共通)】**
(3) ⇒ (1) により、分離的かつ正規であることが示される。あとは (1) ⇒ (4) と同様に有限個の生成元の最小多項式から $f(x)$ を構成すればよい。

# (4) ⇒ (1) の証明 I

**【分離次数を使わない証明】**
定理 2.5 より正規拡大である。分離性について、$f(x)$ の根の塔を考えると、各段階の最小多項式は $f(x)$ を割り切るため重根を持たず、埋め込み総数は $[L : K]$ となる。正規性により $|G| = [L : K]$。Artin の定理より $L^G = K$ を得る。(2) ⇒ (1) と同様に軌道から $g(x)$ を構成することで、任意の元が分離的であることが示される。

**【分離次数を使う証明】**
定理 2.5 より正規拡大。$f(x)$ は重根を持たないため、その根は $K$ 上分離的。定理 2.4-3（分離的生成元による拡大は分離的）を適用することで、$L$ は分離拡大となる。

# (4) ⇒ (2) の証明 I

**【分離次数を使わない証明】**
(4) ⇒ (1) の途中で示した通り、埋め込みの数え上げから $|G| = [L : K]$。
Artin の定理 $[L : L^G] = |G|$ より $L^G = K$ を得る。

**【分離次数を使う証明】**
(4) ⇒ (1) により分離的かつ正規。分離性より $[L : K]_s = [L : K]$、正規性より $[L : K]_s = |G|$。よって $[L : K] = |G|$。Artin の定理より $L^G = K$。

# (4) ⇒ (3) の証明 I

**【分離次数を使わない証明】**
根を順に添加する塔において、各段階の最小多項式が重根を持たず、拡張可能数が正確に $[K_i : K_{i-1}]$ となる。これを掛け合わせることで埋め込み数が $[L : K]$ となり、正規性によりこれらがすべて自己同型となるため $|G| = [L : K]$ を得る。

**【分離次数を使う証明】**
(4) ⇒ (1) により分離的正規。分離次数の性質から $[L : K] = [L : K]_s$ かつ $[L : K]_s = |G|$。これらを直結させて $[L : K] = |G|$ が得られる。

# 引用文献


- Artin, E. (1944). *Galois Theory*. Notre Dame Mathematical Lectures, no. 2. University of Notre Dame Press.
- Milne, J. S. (2022). *Fields and Galois Theory*. Course Notes.
- Lang, S. (2002). *Algebra* (Revised 3rd ed.). Graduate Texts in Mathematics, 211. Springer-Verlag.