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）

本稿では、体の有限次拡大におけるGalois理論の基本定理の根幹をなす、4つの条件の同値性について解説する。外部の定理（例えば「原始元定理」や「分離的な元から生成された体は分離拡大になること」など）を一切ブラックボックスとして引用せず、前提となる補題や定理をすべて事前に本稿の内部で証明した、完全に自己完結的 (self-contained) な記述となっている。提示された4つの条件の間にある12通りの含意 $(k) \Rightarrow (l)$ を、「分離次数を用いない初等的な証明」と「分離次数の性質を活用する証明」の2通りのアプローチですべて直接的に証明する。

1. 基本概念の定義と具体例

まず、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。

定義 1.1 (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、α 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。有限次拡大は常に代数拡大である。
- **最小多項式 (minimal polynomial)**: 代数的な元 $\alpha \in L$ に対し、α を根に持つ $K[x]$ のモニック（最高次係数が 1）な既約多項式を α 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 K 上の最小多項式が分離多項式であるとき、α 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、ある拡大体 L/K が $f(x)$ のすべての根 $\alpha_1, \dots, \alpha_n$ を含み、かつ $L = K(\alpha_1, \dots, \alpha_n)$ と表されるとき、L を $f(x)$ の K 上の最小分解体と呼ぶ。
- **不変体 (fixed field)**: 自己同型群の有限部分群 $G \subset \mathrm{Aut}(L)$ に対し、$L^G = \{x \in L \mid \forall \sigma \in G, \sigma(x) = x\}$ と定義される体を G の不変体と呼ぶ。これは常に L の部分体となる。

例 1.2 (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

同値性の証明に先立ち、必要となるすべての基本定理をここで完全に証明する。これにより、外部の定理に依存しない自己完結した議論が可能となる。

補題 2.1 (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 $\sigma_1, \dots, \sigma_n$ は、M 上線形独立である。すなわち、$\lambda_1, \dots, \lambda_n \in M$ 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。

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、そのような関係式のうち、現れる項数 k が最小のものを $\sum_{i=1}^{k} \lambda_i \sigma_i(x) = 0$（$\forall x \in L, \lambda_i \neq 0$）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 αx を代入すると、

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

となる。一方で、元の関係式に $\sigma_k(\alpha)$ を乗じると、

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

となる。これら2式の差をとると、第 k 項が相殺され、

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

を得る。$i = 1$ のとき $\lambda_1(\sigma_1(\alpha) - \sigma_k(\alpha)) \neq 0$ であるため、これは項数が k 未満の自明でない線形従属関係式となり、最小性に矛盾する。　□

定理 2.2 (Artinの定理)

体 L と、$\mathrm{Aut}(L)$ の有限部分群 $G = \{\sigma_1 = 1, \sigma_2, \dots, \sigma_n\}$ 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。

証明

$[L : K] = n$ を示すため、$[L : K] < n$ および $[L : K] > n$ の両方が矛盾を導くことを示す。

(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 $\omega_1, \dots, \omega_m$ とする。次のような L の元 $x_1, \dots, x_n$ を未知数とする方程式系を考える：

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

これは式の数 m が未知数の数 n より少ない線形同次方程式系であるため、すべてが 0 ではない解 $(x_1, \dots, x_n) \in L^n$ を持つ。任意の $\alpha \in L$ は $a_i \in K$ を用いて $\alpha = \sum_{i=1}^{m} a_i \omega_i$ と書ける。$\sigma_j(a_i) = a_i$ であることに注意して、方程式に a_i を乗じて i について和をとると、

$$0 = \sum_{i=1}^{m} a_i \sum_{j=1}^{n} \sigma_j(\omega_i) x_j = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} \sigma_j(a_i \omega_i) \right) x_j = \sum_{j=1}^{n} \sigma_j(\alpha) x_j$$

これが任意の $\alpha \in L$ で成り立つことは、相異なる自己同型 $\sigma_1, \ldots, \sigma_n$ が L 上線形従属であることを意味し、補題 2.1 に矛盾する。したがって $[L : K] \geq n$ である。

(Step 2) $[L : K] \leq n$ の証明
$[L : K] > n$ と仮定する。このとき K 上線形独立な元の集合 $\alpha_1, \ldots, \alpha_{n+1} \in L$ が存在する。次の方程式系を考える：

$$\sum_{i=1}^{n+1} \sigma_j(\alpha_i) y_i = 0 \quad (j = 1, \ldots, n)$$

これは式が n 個、未知数 y_i が $n+1$ 個であるため、自明でない解 $(y_1, \ldots, y_{n+1}) \in L^{n+1}$ を持つ。非零の成分の個数が最小となる解を選び、必要ならば番号を付け替えて $y_1, \ldots, y_r \neq 0$ かつ $y_{r+1} = \cdots = y_{n+1} = 0$ とし、さらに全体を y_r で割ることで $y_r = 1$ としてよい。このとき方程式系は、

$$\sum_{i=1}^{r-1} \sigma_j(\alpha_i) y_i + \sigma_j(\alpha_r) = 0 \quad (j = 1, \ldots, n)$$

となる。$\sigma_1 = 1$ に対する式は $\sum_{i=1}^{r-1} \alpha_i y_i + \alpha_r = 0$ である。α_i たちは K 上線形独立なので、すべての y_i が K に属することはあり得ない。よって、ある y_1 は $K = L^G$ に属さない。すなわち、ある $\sigma_k \in G$ が存在して $\sigma_k(y_1) \neq y_1$ となる。上記の方程式系全体に σ_k を作用させると、G の元の積 $\sigma_k \sigma_j$ は再び G 全体を走るため、

$$\sum_{i=1}^{r-1} \sigma_j(\alpha_i) \sigma_k(y_i) + \sigma_j(\alpha_r) = 0 \quad (j = 1, \ldots, n)$$

を得る。これと元の式との差をとると、

$$\sum_{i=1}^{r-1} \sigma_j(\alpha_i) (y_i - \sigma_k(y_i)) = 0 \quad (j = 1, \ldots, n)$$

となる。これは元の解より非零の項数が少なく、かつ $i = 1$ の項は $y_1 - \sigma_k(y_1) \neq 0$ より消滅していない。これは解の非零成分数の最小性に矛盾する。したがって $[L : K] \leq n$ である。 $\square$

補題 2.3 (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、α 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、この総数が拡大次数 $[K(\alpha) : K]$ と一致することと、α 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 $g(\alpha)$ ($g(x) \in K[x]$) と一意的に表せる。K 上の埋め込み σ は、$\sigma(g(\alpha)) = g(\sigma(\alpha))$ を満たすため、σ の効果は $\sigma(\alpha)$ の行き先だけで完全に決定される。また $0 = \sigma(p(\alpha)) = p(\sigma(\alpha))$ より、$\sigma(\alpha)$ は必ず $p(x)$ の $\overline{K}$ における根でなければならない。逆に $p(x)$ の任意の根 $\beta \in \overline{K}$ に対し、$\alpha \mapsto \beta$ とする K 準同型写像 $\sigma_\beta : K(\alpha) \to \overline{K}$ が well-defined に定まる。したがって、埋め込みの総数は $p(x)$ の相異なる根の数に完全に一致する。多項式 $p(x)$ の根の数が次数 $\deg p = [K(\alpha) : K]$ と一致することは、重根を持たないこと、すなわち α が分離的であることの定義そのものである。 $\square$

定理 2.4 (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 準同型写像の総数を分離次数 $[L : K]_s$ と定義する。このとき以下が成り立つ。

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**: 常に $[L:K]_s \leq [L:K]$ であり、等号成立は L/K が分離拡大であることと同値。
3. **分離元による生成**: $\alpha_1, \ldots, \alpha_r \in L$ がすべて K 上分離的であるならば、$K(\alpha_1, \ldots, \alpha_r)/K$ も分離拡大である。

証明

1. 乗法性: M の K 上の埋め込み全体を $\tau_1, \ldots, \tau_m$ ($m = [M:K]_s$) とする。各 τ_i は $\overline{K}$ の自己同型に拡張できる。L の M 上の埋め込み全体を $\rho_1, \ldots, \rho_n$ ($n = [L:M]_s$) とするとき、合成写像 $\tau_i \circ \rho_j$ はすべて相異なる L の K 上の埋め込みを与え、逆に任意の K 準同型はこの形で一意に表せる。よって総数は積になる。
2. 不等式と等号条件: L/K を単一拡大の塔 $K = K_0 \subset K_1 = K(\beta_1) \subset \cdots \subset K_k = L$ に分解する。補題 2.3 より、各段階で $[K_i : K_{i-1}]_s \leq [K_i : K_{i-1}]$ が成り立ち、等号成立は β_i が K_{i-1} 上分離的であることと同値。乗法性により、全体でも $[L:K]_s \leq [L:K]$ が成り立ち、等号成立はすべての β_i が各段階で分離的であることと同値。これは拡大全体が分離拡大であることと同値となる。
3. 分離元による生成: α_1, α_2 が K 上分離的であるとき、$M = K(\alpha_1)$ とおく。α_2 の K 上の最小多項式 $f(x)$ は重根を持たない。α_2 の M 上の最小多項式 $g(x)$ は $M[x]$ において $f(x)$ を割り切るため、やはり重根を持たない。よって α_2 は M 上分離的である。補題 2.3 と乗法性より、

$$[K(\alpha_1,\alpha_2):K]_s = [K(\alpha_1,\alpha_2):M]_s[M:K]_s = [K(\alpha_1,\alpha_2):M][M:K] = [K(\alpha_1,\alpha_2):K]$$

となり、2 より $K(\alpha_1, \alpha_2)/K$ は分離拡大である。数学的帰納法により有限個の生成元でも同様に成立する。 □

定理 2.5 (最小分解体の正規性)

L がある多項式 $f(x) \in K[x]$ 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 $L = K(\alpha_1, \ldots, \alpha_m)$ である。任意の K 準同型 $\sigma : L \to \overline{K}$ を考える。
$f(x) \in K[x]$ の係数は σ で動かないため、σ は根の集合 $\{\alpha_1, \ldots, \alpha_m\}$ をそれ自身の中に写す（根の置換を引き起こす）。L はこれらの根によって生成されているため、

$$\sigma(L) = K(\sigma(\alpha_1), \ldots, \sigma(\alpha_m)) = K(\alpha_1, \ldots, \alpha_m) = L$$

が成り立つ。いま、$g(x) \in K[x]$ を L に少なくとも1つの根 β を持つ任意の既約多項式とする。$\overline{K}$ における $g(x)$ の他の任意の根を γ とすると、同型の拡張定理より β を γ に写す K 準同型 $\sigma : L(\beta) \to \overline{K}$ が存在する。これを L 全体へ拡張した埋め込みを改めて $\sigma : L \to \overline{K}$ とおくと、上述の議論より $\sigma(L) = L$ でなければならない。$\beta \in L$ より $\gamma = \sigma(\beta) \in \sigma(L) = L$ となり、$g(x)$ のすべての根が L に含まれることが示された。よって L/K は正規拡大である。 □

3. 4つの条件の同値性の直接証明 (12通り×2)

これより、以下の4つの条件が互いに同値であることを、12通りの個別の含意についてそれぞれ「分離次数を使わない証明」と「分離次数を使う証明」の2つの方法で直接証明する。ここでは外部の定理（原始元定理など）を一切用いず、すべて本稿内で証明された事実のみを用いて構成する。

- **(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 K 上のある既約多項式 $f(x) \in K[x]$ の K 上での最小分解体である。

(1) ⇒ (2) の証明

【分離次数を使わない証明】

$K \subset L^G$ は定義より自明であるため、$L^G \subset K$ を示す。任意の $\alpha \in L \setminus K$ をとる。α の K 上の最小多項式を $p(x)$ とする。条件 (1) の分離性より $p(x)$ は重根を持たず、正規性より $p(x)$ は L 内で完全に分解する。$\alpha \notin K$ より $\deg p \geq 2$ であるため、L 内には α とは異なる $p(x)$ の根 β が存在する。補題 2.3 の証明と同様に、$\alpha \mapsto \beta$ となる K 準同型 $\sigma : K(\alpha) \to L$ が存在する。L/K は正規であるため、この埋め込みは L の自己同型 $\tilde{\sigma} \in G$ に拡張できる。このとき $\tilde{\sigma}(\alpha) = \beta \neq \alpha$ となるため、α は G で固定されない。すなわち $\alpha \notin L^G$ である。対偶をとれば $L^G \subset K$ となり、$L^G = K$ が示された。

【分離次数を使う証明】

条件 (1) の分離性より、定理 2.4-2 から $[L:K]_s = [L:K]$ である。また正規性より、埋め込みの像が体の中に閉じることから $[L:K]_s = |G|$ である。ゆえに $[L:K] = |G|$ を得る。ここで定理 2.2 (Artinの定理) より、群 G の不変体 L^G に対して $[L:L^G] = |G|$ が成り立つ。次数の連鎖律 $[L:K] = [L:L^G][L^G:K]$ にこれらを代入すると、$|G| = |G|[L^G:K]$ となり、$[L^G:K] = 1$ が導かれる。したがって $L^G = K$ である。

(1) ⇒ (3) の証明

【分離次数を使わない証明】

「分離次数を使わない証明」により (1) ⇒ (2) は既に示されているため、$L^G = K$ である。ここで定理 2.2 (Artinの定理) より、$\mathrm{Aut}(L)$ の有限部分群 G とその不変体 L^G の間には $[L:L^G] = |G|$ が成り立つ。$L^G = K$ であるから、直ちに $[L:K] = |G|$ を得る。

【分離次数を使う証明】

(1) より L/K は分離的であるため定理 2.4-2 より $[L:K]_s = [L:K]$ であり、正規的であるため $[L:K]_s = |G|$ である。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

【分離次数を使わない証明】

L/K は有限次拡大であるため、有限個の生成元を用いて $L = K(\alpha_1, \ldots, \alpha_m)$ と表せる。各 α_i の K 上の最小多項式を $p_i(x)$ とする。条件 (1) の分離性より各 $p_i(x)$ は重根を持たず、正規性よりすべての根は L に含まれる。多項式 $p_1(x)p_2(x)\cdots p_m(x)$ から重複する既約因子を除いた無平方部分 (square-free part) を $f(x)$ とする。$f(x)$ は重根を持たない K 上の多項式であり、すべての根は L 内にある。さらに L は $f(x)$ の根の一部である $\alpha_1, \ldots, \alpha_m$ を含み、それらで生成されるため、L は $f(x)$ の K 上の最小分解体である。

【分離次数を使う証明】

アプローチは同じく生成元をとって最小多項式を考えることである。(1) より L/K は分離的であるため、各元の最小多項式は重根を持たない（定理 2.4-2 から直ちに従う）。さらに正規性により最小多項式は L で分解する。それらの積の無平方部分 $f(x)$ をとることで、(4) を満たす多項式が構成できる。

(2) ⇒ (1) の証明

【分離次数を使わない証明】

任意の $\alpha \in L$ をとる。有限群 G の作用による α の軌道を $S = \{\sigma(\alpha) \mid \sigma \in G\} = \{\alpha_1 = \alpha, \alpha_2, \dots, \alpha_k\}$ とする。多項式 $g(x) = \prod_{i=1}^{k}(x - \alpha_i)$ を構成する。任意の $\sigma \in G$ を $g(x)$ の係数に作用させると、これは根の置換を引き起こすだけであるため、係数はすべて G で不変である。仮定 (2) より $L^G = K$ であるから、$g(x) \in K[x]$ となる。構成から $g(x)$ は相異なる根のみを持ち（重根を持たない）、かつ L 内で完全に一次式に分解する。α の K 上の最小多項式 $p(x)$ は $g(\alpha) = 0$ より $g(x)$ を割り切る。重根を持たず完全に分解する多項式の因子もまた、重根を持たず完全に分解するため、$p(x)$ は重根を持たず L 内で分解する。これが任意の α で成り立つため、L/K は分離的かつ正規である。

【分離次数を使う証明】

定理 2.2 (Artinの定理) より $[L : L^G] = |G|$ が成り立つ。仮定 (2) の $L^G = K$ を代入すると $[L : K] = |G|$ を得る。ここで、一般に自己同型写像は $\overline{K}$ への埋め込みの一部であるから $|G| \leq [L : K]_s$ であり、定理 2.4-2 より $[L : K]_s \leq [L : K]$ である。これらを組み合わせると、

$$|G| \leq [L : K]_s \leq [L : K]$$

となるが、最初と最後が $|G| = [L : K]$ で等しいため、間の不等号はすべて等号となる。$[L : K]_s = [L : K]$ より L/K は分離拡大であり、$|G| = [L : K]_s$ より L/K は正規拡大である。

(2) ⇒ (3) の証明

【分離次数を使わない証明 / 使う証明 (共通)】

定理 2.2 (Artinの定理) によれば、$\mathbf{Aut}(L)$ の有限部分群 G について $[L : L^G] = |G|$ が成立する。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

【分離次数を使わない証明】

(2) ⇒ (1) の「分離次数を使わない証明」により、L/K が分離的かつ正規であることが示されている。その後は (1) ⇒ (4) の「分離次数を使わない証明」と全く同じ手順により、生成元の最小多項式を用いて無平方部分 $f(x)$ を構成することで、最小分解体となる。

【分離次数を使う証明】

(2) ⇒ (1) の「分離次数を使う証明」により、不等式の狭み撃ちから分離的正規性を得る。その後は同様に $f(x)$ を構成する。

(3) ⇒ (1) の証明

【分離次数を使わない証明】

任意の $\alpha \in L$ をとる。L/K の基底を適切にとり直すことで、$K_1 = K(\alpha)$ から始まる塔 $K = K_0 \subset K_1 \subset K_2 \cdots \subset K_n = L$ を構成できる（ただし $K_i = K_{i-1}(\beta_i)$）。補題 2.3 より、K_{i-1} の $\overline{K}$ への埋め込みを K_i へ拡張する方法の数は最大で $[K_i : K_{i-1}]$ であり、最大値に達するのは β_i の最小多項式が重根を持たないときである。さらにこれらが L の自己同型になるためには、すべての根が L に含まれなければならない。 したがって、K 上の自己同型群 G の位数は、各段階の拡張可能数の積を超えないため、

$|G| \leq \prod_{i=1}^{n}[K_i : K_{i-1}] = [L : K]$ となる。仮定 (3) より $|G| = [L : K]$ であるから、すべての段階において拡張可能数は最大値 $[K_i : K_{i-1}]$ と一致し、かつ像は L に含まれていなければならない。特に最初の段階 $K_1 = K(\alpha)$ において、α の最小多項式は重根を持たず、そのすべての根は L に含まれる。α は任意であったため、L のすべての元の最小多項式は重根を持たず L で分解する。よって L/K は分離的かつ正規である。

【分離次数を使う証明】

自己同型群の位数、分離次数、拡大次数の間には、常に $|G| \leq [L : K]_s \leq [L : K]$ という関係が成り立つ（定理 2.4-2 等より）。仮定 (3) は $|G| = [L : K]$ であるから、この不等式の両端が一致する。したがって、中間にある $[L : K]_s$ も等号で結ばれ、$[L : K]_s = [L : K]$（分離拡大の定義）および $|G| = [L : K]_s$（正規拡大の定義）が同時に成立する。

(3) ⇒ (2) の証明

【分離次数を使わない証明 / 使う証明 (共通)】

不変体の定義から、$K \subset L^G \subset L$ という中間体が存在する。次数の連鎖律から $[L : K] = [L : L^G][L^G : K]$ が成り立つ。ここで定理 2.2 (Artinの定理) より、$[L : L^G] = |G|$ である。これらを仮定 (3) の $[L : K] = |G|$ と組み合わせると、$|G| = |G|[L^G : K]$ となる。$|G| \geq 1$ であるから両辺を割ることができ、$[L^G : K] = 1$ を得る。これにより $L^G = K$ が確定する。

(3) ⇒ (4) の証明

【分離次数を使わない証明】

(3) ⇒ (1) の「分離次数を使わない証明」により、L/K が分離的かつ正規であることが示される。あとは (1) ⇒ (4) の「分離次数を使わない証明」と同様に、有限個の生成元の最小多項式の積から無平方部分 $f(x)$ を構成すればよい。

【分離次数を使う証明】

(3) ⇒ (1) の「分離次数を使う証明」により $|G| \leq [L : K]_s \leq [L : K]$ の等号成立から分離的正規性を導く。その後は上記と同様。

(4) ⇒ (1) の証明

【分離次数を使わない証明】

L は重根を持たない K 上の既約多項式 $f(x)$ の最小分解体である。まず定理 2.5 により L/K は正規拡大であることがわかる。
次に分離性を示す。$f(x)$ の根を $\alpha_1, \ldots, \alpha_n$ とし、塔 $K = K_0 \subset K_1 \subset \cdots \subset K_n = L$（$K_i = K_{i-1}(\alpha_i)$）を考える。各段階において、$\alpha_i$ の K_{i-1} 上の最小多項式 $p_i(x)$ は $f(x)$ の因子である。$f(x)$ は重根を持たないため、$p_i(x)$ も重根を持たない。したがって補題 2.3 により、K_{i-1} からの埋め込みを K_i へ拡張する方法は正確に $[K_i : K_{i-1}]$ 通りある。これを繰り返すことで、全体の K 埋め込みの総数は次数の積 $[L : K]$ となる。正規性によりこれらはすべて L の自己同型となるため、$|G| = [L : K]$ である。
ここで定理 2.2 (Artinの定理) より $[L : L^G] = |G|$ であるから、$|G| = [L : K]$ を代入して $L^G = K$ を得る。さて、任意の $\alpha \in L$ について、その G による軌道 $S = \{\sigma(\alpha) \mid \sigma \in G\}$ を考える。多項式 $g(x) = \prod_{\beta \in S}(x - \beta)$ は係数が G で不変であるため、$L^G = K$ により $g(x) \in K[x]$ である。$g(x)$ は構成上重根を持たず L で分解する。α の最小多項式は $g(\alpha) = 0$ より $g(x)$ を割り切るため、やはり重根を持たない。α は任意であるから、L/K は分離的である。以上より分離的かつ正規である。

【分離次数を使う証明】

L は重根を持たない既約多項式 $f(x)$ の最小分解体である。最小分解体であることから、定理 2.5 により L/K は正規拡大となる。
また $f(x)$ は重根を持たないため、その根 $\alpha_1, \ldots, \alpha_n$ の最小多項式（これは $f(x)$ 自身）は重根を持たず、各 α_i は K 上分離的であ

る。ここで定理 2.4-3（分離的な元によって生成された有限次拡大体のすべての元は分離的である）を適用することにより、$L = K(\alpha_1, \ldots, \alpha_n)$ は分離拡大となる。以上より、L/K は分離的かつ正規である。

(4) ⇒ (2) の証明

【分離次数を使わない証明】

(4) ⇒ (1) の「分離次数を使わない証明」の途中で示した通り、$f(x)$ の根からなる塔を考えることで、埋め込みの拡張の数え上げから $|G| = [L : K]$ が得られる。定理 2.2 (Artinの定理) により $[L : L^G] = |G|$ であるから、次数の連鎖律に代入してただちに $L^G = K$ を得る。

【分離次数を使う証明】

(4) ⇒ (1) の「分離次数を使う証明」により L/K は分離的かつ正規である。分離性より定理 2.4-2 から $[L : K]_s = [L : K]$、正規性より $[L : K]_s = |G|$ である。これらより $[L : K] = |G|$ となる。定理 2.2 (Artinの定理) より $[L : L^G] = |G|$ であるから、これを代入して $L^G = K$ を得る。

(4) ⇒ (3) の証明

【分離次数を使わない証明】

L は重根を持たない $f(x)$ の最小分解体である。(4) ⇒ (1) の「分離次数を使わない証明」で用いた議論と全く同様に、根 α_i を順に添加する塔 $K_i = K_{i-1}(\alpha_i)$ を考える。各段階での最小多項式が $f(x)$ を割り切るため重根を持たず、埋め込みの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、全体の埋め込み数が $[L : K]$ となり、定理 2.5 (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、拡大 L/K は分離的かつ正規であることが既に示されている。したがって、分離次数の基本性質（定理 2.4-2）から $[L : K] = [L : K]_s$、および正規性から $[L : K]_s = |G|$ が同時に成り立つ。これら2つの等式を直結させることで、$[L : K] = |G|$ が直ちに得られる。

引用文献

Artin, E. (1944). *Galois Theory*. Notre Dame Mathematical Lectures, no. 2. University of Notre Dame Press. https://projecteuclid.org/euclid.ndml/1175197041

Milne, J. S. (2022). *Fields and Galois Theory*. Course Notes. https://www.jmilne.org/math/CourseNotes/FT.pdf

Lang, S. (2002). *Algebra* (Revised 3rd ed.). Graduate Texts in Mathematics, 211. Springer-Verlag. https://link.springer.com/book/10.1007/978-1-4613-0041-0