Galoisの基本定理と正規底定理の包括的解説

Gemini 3.1 Pro で作成。指示に失敗しているが、面白いので記録として残しておく。

> *ユーザーの皆様へ：本稿では、有限次Galois拡大の同値な定義から出発し、Galoisの基本定理、そして正規底定理にいたる代数学の核心部分を詳細に解説します。基本概念の定義や具体例を豊富に盛り込み、すべての命題に対して省略のない完全な（フルな）証明を与えています。じっくりと腰を据えて抽象代数学の美しさをお楽しみください。*

1️⃣ 準備

Galois理論を展開するためには、体の拡大に関する精密な概念の整理が必要です。ここでは、分離性、正規性、完全分解体の定義を確認し、基礎となる諸定理の完全な証明を与えます。

1.1. 有限次の分離的正規拡大と完全分解体の定義

定義 1.1 (体の拡大、次数).
体 L が体 K を部分体として含むとき、拡大体 L/K という。L は自然に K 上のベクトル空間とみなせる。その次元を拡大の次数 (degree of extension) と呼び、$[L:K]$ で表す。$[L:K] < \infty$ であるとき、L/K は有限次拡大 (finite extension) であるという。

定義 1.2 (分離拡大).
L/K を体の拡大とする。$\alpha \in L$ が K 上代数的であるとき、α を根に持つ $K[x]$ の次数最小の首一多項式を K 上の最小多項式 (minimal polynomial) と呼び、$\mathrm{minpoly}_K(\alpha)$ と書く。 $\alpha \in L$ が K 上分離的 (separable) であるとは、$\mathrm{minpoly}_K(\alpha)$ が、その任意の分解体において重根を持たないことである。 拡大 L/K のすべての元が K 上分離的であるとき、L/K を分離拡大 (separable extension) という。

定義 1.3 (正規拡大).
拡大 L/K が正規拡大 (normal extension) であるとは、$K[x]$ の任意の既約多項式 $f(x)$ が L に少なくとも1つの根を持つならば、$f(x)$ は $L[x]$ において一次式の積に完全に分解することである。

定義 1.4 (完全分解体).
$f(x) \in K[x]$ を定数でない多項式とする。体の拡大 L/K が $f(x)$ の K 上の完全分解体 (splitting field) であるとは、以下の2条件を満たすことである：

1. $f(x)$ は $L[x]$ において一次式の積に分解する。すなわち、ある $a, \alpha_1, \dots, \alpha_n \in L$ が存在して $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$ と表せる。
2. $L = K(\alpha_1, \dots, \alpha_n)$ である。

例 1.5 (分離的かつ正規な拡大、および反例).

1. $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ は有限次の分離的正規拡大である。これは重根を持たない多項式 $(x^2-2)(x^2-3) \in \mathbb{Q}[x]$ の $\mathbb{Q}$ 上の完全分

解体である。

2. $L = \mathbb{Q}(\sqrt[3]{2})$ とすると、拡大 $L/\mathbb{Q}$ の次数は 3 である。$\sqrt[3]{2}$ の $\mathbb{Q}$ 上の最小多項式は $x^3 - 2$ であり、これは相異なる3つの複素根を持つため分離的である。しかし、他の2つの根 $\sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ （ここで $\omega = (-1 + \sqrt{3}i)/2$）は L に含まれない。したがって、$L/\mathbb{Q}$ は正規拡大ではない。
3. 不分離拡大の例：p を素数とし、体 $K = \mathbb{F}_p(t)$ を有限体 $\mathbb{F}_p$ 上の1変数有理関数体とする。多項式 $f(x) = x^p - t \in K[x]$ はEisensteinの判定法により既約である。$f(x)$ の完全分解体を L とし、その根を α とすると、L において $x^p - t = (x - \alpha)^p$ となる。この多項式は α を p 重根として持つため、拡大 L/K は分離拡大ではない。

1.2. 有限次分離拡大に関する原始元定理とその証明

定理 1.6 (原始元定理).
L/K を有限次の分離拡大とする。このとき、ある $\theta \in L$ が存在して $L = K(\theta)$ となる。

証明

K が有限体である場合を考える。このとき L も有限次拡大であるから有限体である。有限体の乗法群 $L^\times = L \setminus \{0\}$ は巡回群であることが知られている。$L^\times$ の生成元のひとつを θ とすれば、自明に $L = K(\theta)$ が成り立つ。

次に K が無限体である場合を考える。有限次拡大であるから、有限個の元を用いて $L = K(\alpha_1, \alpha_2, \ldots, \alpha_m)$ と表せる。帰納法により、$m = 2$ の場合、すなわち $L = K(\alpha, \beta)$ の場合に示せば十分である。α, β の K 上の最小多項式をそれぞれ $f(x), g(x) \in K[x]$ とする。L/K は分離拡大であるから、$f(x)$ および $g(x)$ は重根を持たない。L を含むある大きな代数閉包において、$f(x)$ の相異なる根を $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ とし、$g(x)$ の相異なる根を $\beta = \beta_1, \beta_2, \ldots, \beta_k$ とする（ここで $\beta_1 = \beta$）。

K は無限体であるから、すべての $i \in \{1, \ldots, n\}$ および $j \in \{2, \ldots, k\}$ に対して、

$$\alpha_i + c\beta_j \neq \alpha_1 + c\beta_1$$

を満たすような $c \in K$ を選ぶことができる。実際、上式が等号になる条件は $c(\beta_1 - \beta_j) = \alpha_i - \alpha_1$ であり、$\beta_j \neq \beta_1$ より $c = (\alpha_i - \alpha_1)/(\beta_1 - \beta_j)$ となる。このような c の候補は有限個しか存在しないため、無限体 K からこれらを避けて c を選ぶことは常に可能である。

このように選んだ $c \in K$ を用いて $\theta = \alpha + c\beta \in L$ と置く。明らかに $K(\theta) \subset K(\alpha, \beta)$ である。逆の包含関係を示すために、$\beta \in K(\theta)$ を示す。多項式 $h(x) = f(\theta - cx) \in K(\theta)[x]$ を導入する。このとき、

$$h(\beta) = f(\theta - c\beta) = f(\alpha) = 0$$

である。また、β の定義より $g(\beta) = 0$ である。ゆえに β は $L[x]$ において $g(x)$ と $h(x)$ の共通根である。$j \neq 1$ なる根 β_j について考えると、

$$h(\beta_j) = f(\theta - c\beta_j) = f(\alpha_1 + c\beta_1 - c\beta_j)$$

となる。c の選び方から、$\alpha_1 + c\beta_1 - c\beta_j \neq \alpha_i$ $(i = 1, \ldots, n)$ である。$f(x)$ の根は $\alpha_1, \ldots, \alpha_n$ に限られるため、$h(\beta_j) \neq 0$ である。したがって、$g(x)$ と $h(x)$ の共通根は β のみである。

いま、$g(x)$ と $h(x)$ の $K(\theta)[x]$ における最大公約式を $d(x)$ とすると、$d(x)$ の拡大体での根は共通根である β のみであり、かつ $g(x)$ が分離多項式であることから重根を持たない。よって $d(x) = x - \beta$ となる。最大公約式を求めるユークリッドの互除法は係数体 $K(\theta)$ の中で完結するため、$d(x) \in K(\theta)[x]$ である。これより $\beta \in K(\theta)$ が従う。このとき $\alpha = \theta - c\beta \in K(\theta)$ でもある。したがって $K(\alpha, \beta) \subset K(\theta)$ となり、両者は一致する。

Q.E.D.

1.3. Dedekindの独立性定理とその証明

補題 1.7.
体 L 上のベクトル空間 V のベクトル達 $v_1, \ldots, v_n$ で張られる部分空間を W と書く。 互いに異なる $i, j \in \{1, \ldots, n\}$ に対して T_{ij} は W の一次変換であるとし、$k \in \{1, \ldots, n\}$ に対して $\lambda_k^{ij} \in L$ であり、v_k は T_{ij} の固有値 λ_k^{ij} を持つ固有ベクトルであるとし、$\lambda_i^{ij} \neq \lambda_j^{ij}$ と仮定する。 このとき、$v_1, \ldots, v_n$ は L 上一次独立である。

証明

n に関する数学的帰納法を用いる。$n = 1$ のときは、v_1 は固有ベクトルであるから $v_1 \neq 0$ であり、一次独立である。

$n - 1$ 次まで命題が正しいと仮定し、$v_1, \ldots, v_n$ が L 上一次従属であると仮定して矛盾を導く。非自明な一次関係式

$$c_1 v_1 + c_2 v_2 + \cdots + c_n v_n = 0 \quad (c_k \in L)$$

のうち、非零である係数の個数が最小となるものを選択する。必要ならば番号を付け替えることにより、最初の m 個の係数が非零であるとしてよい：

$$c_1 v_1 + c_2 v_2 + \cdots + c_m v_m = 0 \quad (c_k \in L \setminus \{0\},\ m \leq n)$$

最小性より $m \geq 2$ である。ここで $i = 1, j = m$ に対する一次変換 T_{1m} を両辺に作用させる。各 v_k は固有ベクトルであるから、

$$c_1 \lambda_1^{1m} v_1 + c_2 \lambda_2^{1m} v_2 + \cdots + c_m \lambda_m^{1m} v_m = 0$$

を得る。元の一次関係式に λ_1^{1m} を乗じた式

$$c_1 \lambda_1^{1m} v_1 + c_2 \lambda_1^{1m} v_2 + \cdots + c_m \lambda_1^{1m} v_m = 0$$

を辺々差し引くと、最初の項が消去されて以下の式を得る：

$$c_2(\lambda_2^{1m} - \lambda_1^{1m}) v_2 + \cdots + c_m(\lambda_m^{1m} - \lambda_1^{1m}) v_m = 0$$

仮定より $\lambda_1^{1m} \neq \lambda_m^{1m}$ であり、かつ $c_m \neq 0$ であるから、最後の項の係数は $c_m(\lambda_m^{1m} - \lambda_1^{1m}) \neq 0$ である。これは、非零の係数の個数が高々 $m - 1$ 個である新しい非自明な一次関係式を与え、項数の最小性に矛盾する。したがって、$v_1, \ldots, v_n$ は一次独立でなければならない。

Q.E.D.

Dedekindの補題 (群指標の独立性).
半群 H から体 L の乗法群 $L^\times$ への互いに異なる準同型達 $\sigma_1, \ldots, \sigma_n$ は L 上一次独立である。

証明

V を H から L への写像全体のなす L 上のベクトル空間とし、ベクトル達を $v_k = \sigma_k$ とみなす。これらが張る部分空間を W とする。 各 $a \in H$ に対し、W 上の写像 T_a を $(T_a \sigma)(x) = \sigma(ax)$ $(x \in H)$ によって定義する。σ_k は半群の準同型であるから、

$$(T_a \sigma_k)(x) = \sigma_k(ax) = \sigma_k(a)\sigma_k(x)$$

となり、σ_k は T_a の固有値 $\sigma_k(a)$ に属する固有ベクトルである。

いま、$\sigma_1, \ldots, \sigma_n$ は互いに異なる写像であるから、任意の相異なる写像の組 $i \neq j$ に対し、$\sigma_i(a) \neq \sigma_j(a)$ を満たす元 $a \in H$ が存在する。この a に対応する一次変換を $T_{ij} = T_a$ とおき、固有値を $\lambda_k^{ij} = \sigma_k(a)$ と定めれば、仮定 $\lambda_i^{ij} \neq \lambda_j^{ij}$ が満たされ

る。補題 1.7 を適用することにより、$\sigma_1, \ldots, \sigma_n$ は L 上一次独立であることが従う。

Q.E.D.

1.4. 体の拡大 L/K と $G = \mathrm{Aut}(L/K)$ についての同値性の証明

L/K を有限次拡大とし、$G = \mathrm{Aut}(L/K)$ を L の K 上での体自己同型全体とする。以下の5つの条件は互いに同値である。ここでは特に、(1) $\Rightarrow$ (5) および (5) $\Rightarrow$ (1) の直接証明を、(2) から (4) を経由せずに書き下す。

定理 1.8.
以下の条件は同値である。

1. L/K は有限次の分離的正規拡大である。
2. 0 でない K 係数の重根を持たない多項式 $f(x) \in K[x]$ が存在して、L は K 上での $f(x)$ の完全分解体である。
3. $L^G = K$. ただし $L^G = \{x \in L \mid \forall \sigma \in G, \sigma(x) = x\}$.
4. $[L : K] = |G|$.
5. ある正の整数 n が存在して、$L \otimes_K L \cong L^n$ (左 L 加群同型かつ K 代数同型)。

(1) $\Rightarrow$ (5) の直接証明

L/K は有限次分離拡大であるから、原始元定理（定理 1.6）により、ある $\theta \in L$ が存在して $L = K(\theta)$ と表せる。θ の K 上の最小多項式を $f(x) \in K[x]$ とすると、自然な代数同型 $L \cong K[x]/(f(x))$ が成り立つ。 さらに L/K は正規拡大であるため、最小多項式 $f(x)$ は $L[x]$ 内で一次式の積に完全に分解する。また分離性により $f(x)$ は重根を持たない。したがって、$[L : K] = n$ とおくと、L 内の相異なる n 個の元 $\theta_1, \theta_2, \ldots, \theta_n$ （ここで $\theta_1 = \theta$）を用いて、

$$f(x) = (x - \theta_1)(x - \theta_2) \cdots (x - \theta_n)$$

と因数分解できる。

ここでテンソル積 $L \otimes_K L$ を考えると、右側の成分に上記の多項式環による表現を代入することで、

$$L \otimes_K L \cong L \otimes_K (K[x]/(f(x))) \cong L[x]/(f(x))$$

という K 代数の同型が得られる。この多項式環 $L[x]$ において、各 $i \neq j$ に対して多項式 $x - \theta_i$ と $x - \theta_j$ は互いに素である。なぜなら、それらの差は非零の定数 $\theta_j - \theta_i \in L$ となるからである。したがって、中国式剰余定理 (Chinese remainder theorem) を適用することができ、

$$L[x]/(f(x)) = L[x]/\left(\prod_{i=1}^{n}(x - \theta_i)\right) \cong \prod_{i=1}^{n} L[x]/(x - \theta_i) \cong \prod_{i=1}^{n} L = L^n$$

となる。この合成写像 $\Phi : L \otimes_K L \to L^n$ は、具体的には $\Phi(a \otimes b) = (a\sigma_1(b), a\sigma_2(b), \ldots, a\sigma_n(b))$ で与えられる。ただし $\sigma_i \in G$ は θ を θ_i に写す K 自己同型である。これは各成分へのスカラー倍に対して可換であるため、左 L 加群としての同型であり、かつ環の直積への同型であるから K 代数同型でもある。

Q.E.D.

(5) $\Rightarrow$ (1) の直接証明

ある正の整数 n に対して $\Psi : L \otimes_K L \xrightarrow{\sim} L^n$ を左 L 加群同型かつ K 代数同型とする。 まず、L^n は体の有限個の直積環であるから、ベキ零元（自乗して 0 になる非零元）を持たない被約環 (reduced ring) である。ゆえに、それに同型な $L \otimes_K L$ もベキ

零元を持たない。

いま、L/K が分離拡大であることを示すために、任意の $\alpha \in L$ の K 上の最小多項式 $g(x) \in K[x]$ が重根を持たないことを証明する。もし $g(x)$ が重根を持つと仮定し、拡大体において $g(x) = (x-\beta)^2 h(x)$ と分解すると仮定する。このとき $K(\alpha) \cong K[x]/(g(x))$ である。テンソル積の部分環 $L \otimes_K K(\alpha)$ を考えると、

$$L \otimes_K K(\alpha) \cong L \otimes_K (K[x]/(g(x))) \cong L[x]/(g(x))$$

となる。$g(x)$ は $L[x]$ において $(x-\beta)^2$ で割り切れるため、$L[x]/(g(x))$ は $(x-\beta)h(x)$ に対応する非自明なベキ零元を保持する。これは $L \otimes_K L$ の部分環がベキ零元を持つことを意味し、全空間が被約であることに矛盾する。したがって、すべての元の最小多項式は重根を持たず、L/K は分離拡大である。

次に正規性を示す。L^n の第 i 成分への射影を $p_i : L^n \to L$ とする。写像 $\sigma_i : L \to L$ を $\sigma_i(b) = p_i(\Psi(1 \otimes b))$ で定義する。Ψ が K 代数同型であることから、各 σ_i は K 上の体準同型であり、L が有限次元であることから自己同型となる（すなわち $\sigma_i \in G$）。 任意の $\alpha \in L$ とその最小多項式 $g(x) \in K[x]$ に対し、

$$\Psi(1 \otimes g(\alpha)) = \Psi(0) = 0$$

である。一方で Ψ は K 代数準同型であるから、

$$\Psi(1 \otimes g(\alpha)) = g(\Psi(1 \otimes \alpha)) = g((\sigma_1(\alpha), \ldots, \sigma_n(\alpha))) = (g(\sigma_1(\alpha)), \ldots, g(\sigma_n(\alpha)))$$

となる。したがって、すべての i について $g(\sigma_i(\alpha)) = 0$ が成り立つ。 Ψ が同型であることから、$\{\sigma_1, \ldots, \sigma_n\}$ はすべて相異なる。ベクトル空間の次元を比較すると、$[L:K] = \dim_L(L \otimes_K L) = \dim_L(L^n) = n$ である。Dedekindの独立性定理より、相異なる K 自己同型は高々 $[L:K]$ 個しか存在し得ないため、$\sigma_1, \ldots, \sigma_n$ は G の元すべてを網羅している。 任意の α に対し、$\{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\}$ の中には $g(x)$ の根がすべて含まれていなければならない（含まれていない場合、テンソル積の次元が n に達しない）。ゆえに $g(x)$ のすべての根は L 内に存在し、L/K は正規拡大である。

Q.E.D.

(1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (1) の証明の補完

- **(1) $\Rightarrow$ (2):** L/K は有限次分離拡大なので原始元定理より $L = K(\theta)$ である。θ の最小多項式を $f(x)$ とすると、(1)の正規性と分離性より $f(x)$ は L で完全に分解し、かつ重根を持たない。L はその根を K に付加した体そのものであるから、$f(x)$ の完全分解体である。
- **(2) $\Rightarrow$ (3):** L を重根を持たない多項式 $f(x) \in K[x]$ の完全分解体とし、その根の全体を $\Omega = \{\theta_1, \ldots, \theta_m\}$ とする。$G = \mathrm{Aut}(L/K)$ とする。任意の $\alpha \in L^G$ をとる。α が K に属することを示す。$\alpha \notin K$ と仮定すると、α の K 上の最小多項式 $g(x)$ は2次以上である。体論の一般論（同型拡張定理）により、$g(x)$ の別の根 α' に対し、$\sigma(\alpha) = \alpha'$ となる自己同型 $\sigma \in G$ が存在する。これは $\alpha \in L^G$ （すなわちすべての $\sigma \in G$ で $\sigma(\alpha) = \alpha$）に矛盾する。ゆえに $L^G = K$ である。
- **(3) $\Rightarrow$ (4):** Artinの不変体定理による。有限群 G が体 L に自己同型として作用するとき、その固定体 $K = L^G$ に対し、拡大次数 $[L:K]$ は必ず群の位数 $|G|$ に一致する。もし $[L:K] > |G|$ と仮定すると、K 上一次独立な元が $|G|+1$ 個以上存在することになり、それらを用いて線型連立方程式を立てると、Dedekindの独立性定理に矛盾する非自明な解が得られてしまう。ゆえに $[L:K] = |G|$ である。
- **(4) $\Rightarrow$ (1):** $G = \mathrm{Aut}(L/K)$ に対し、その固定体を $M = L^G$ とする。あきらかに $K \subset M \subset L$ である。Artinの不変体定理より $[L:M] = |G|$ である。仮定 (4) より $[L:K] = |G|$ であるから、次数の乗法性 $[L:K] = [L:M][M:K]$ より $[M:K] = 1$、すなわち $M = K$ となる。任意の $\alpha \in L$ に対し、その G 軌道を $\{\alpha_1, \ldots, \alpha_r\}$ とすると、多項式 $h(x) = \prod_{j=1}^{r}(x - \alpha_j)$ の係数は G で不変であるため $L^G = K$ に属する。$h(x)$ は $K[x]$ の元であり、重根を持たず L で完全に分解し、かつ α を根に持つ。したがって α の最小多項式は $h(x)$ を割り切るため、やはり重根を持たず L で分解する。ゆえに L/K は分離的かつ正規である。

Q.E.D.

以上の同値な条件を満たすとき、拡大 L/K を**有限次Galois拡大 (finite Galois extension)** と呼び、群 $G = \mathrm{Aut}(L/K)$ をその**Galois群 (Galois group)** と呼び、$\mathrm{Gal}(L/K)$ と表します。

2️⃣ Galoisの基本定理

Galoisの基本定理は、中間体全体のなす集合と、Galois群の部分群全体のなす集合の間に、包含関係を反転させる全単射対応が存在することを主張します。前節で証明した5つの同値条件、およびトレース写像の性質に基づいて、6種類の異なるアプローチによる証明を記述します。

> **Galoisの基本定理.**
> L/K を有限次Galois拡大とし、$G = \mathrm{Gal}(L/K)$ とおく。中間体 M ($K \subset M \subset L$) 全体の集合を $\mathcal{M}$、G の部分群 H 全体の集合を $\mathcal{H}$ とする。このとき、以下の写像
>
> $$\Phi : \mathcal{M} \to \mathcal{H}, \quad M \mapsto \mathrm{Gal}(L/M)$$
>
> $$\Psi : \mathcal{H} \to \mathcal{M}, \quad H \mapsto L^H$$
>
> は互いに逆写像であり、包含関係を逆転する全単射を与える。さらに、$[L : M] = |H|$ および $[M : K] = [G : H]$ が成り立つ。

(1) 条件(1): 分離的正規拡大の性質を用いる証明

証明

L/K が分離的正規拡大であるとする。任意の中間体 M をとる。L の元は K 上分離的であるから、当然 M 上も分離的である。また、K 係数の既約多項式が L で分解するならば、その因子である M 係数の既約多項式も L で分解するため、L/M も正規拡大である。したがって L/M はGalois拡大であり、不変体に関する条件(3)を L/M に適用すれば、$L^{\mathrm{Gal}(L/M)} = M$ となり、$\Psi(\Phi(M)) = M$ が示される。

逆に、任意の部分群 $H \subset G$ をとる。固定体 $M = L^H$ を定義すると、定理 1.8 の (4) $\Rightarrow$ (1) の証明中における軌道の議論と全く同様に、L/M はGalois拡大であり、$\mathrm{Gal}(L/L^H) = H$ が成り立つ。これにより $\Phi(\Psi(H)) = H$ が示され、対応の一対一性が証明される。

Q.E.D.

(2) 条件(2): 完全分解体の性質を用いる証明

証明

L は重根を持たない多項式 $f(x) \in K[x]$ の K 上の完全分解体であるとする。任意の中間体 M に対し、$f(x)$ は $M[x]$ の多項式ともみなせるため、L は $f(x)$ の M 上の完全分解体でもある。体論における同型拡張定理の基本帰結より、「完全分解体の自己同型群の位数は、拡大次数に一致する」ため、$|\mathrm{Gal}(L/M)| = [L : M]$ が成り立つ。

任意の部分群 $H \subset G$ に対し、$M = L^H$ とおく。Artinの不変体定理より $[L : L^H] = |H|$ である。ここで明らかに $H \subset \mathrm{Gal}(L/L^H)$ である。位数を比較すると、

$$|H| \leq |\mathrm{Gal}(L/L^H)| = [L : L^H] = |H|$$

となり、すべての不等号が等号に縛られる。ゆえに $H = \mathrm{Gal}(L/L^H)$ が成り立ち、全単射性が従う。

Q.E.D.

(3) 条件(3): 不変体 ($L^G = K$) を軸とするArtinの証明

証明

条件 $L^G = K$ を出発点とする。部分群 $H \subset G$ に対し、その固定体 L^H を考える。Artinの不変体定理（条件(3) $\Rightarrow$ (4) で用いたもの）を群 H と体 L に直接適用する。これにより、$[L : L^H] = |H|$ かつ $\mathrm{Gal}(L/L^H) = H$ が直ちに得られる。

次にお任意の中間体 M に対し、$H = \mathrm{Gal}(L/M)$ とおく。定義より $M \subset L^H$ である。ここで L/M という拡大に対して、条件(3)の前提（L の M 自己同型による固定体は M 自身であること）が成り立つ。なぜなら、もし M より大きな固定体が存在すると仮定すると、L/M の次数次元に関するArtinの不変体定理の等式に矛盾するからである。したがって $L^{\mathrm{Gal}(L/M)} = M$ となり、証明が完了する。

Q.E.D.

(4) 条件(4): 次数 $[L : K] = |G|$ による次元比較の証明

証明

すべての体拡大および部分群に対して、定義から自明に以下の包含関係が成り立つ：

$$M \subset L^{\mathrm{Gal}(L/M)} \quad \text{および} \quad H \subset \mathrm{Gal}(L/L^H)$$

条件(4)より、全体の次数について $[L : K] = |G|$ である。中間体 M について、次数関係式 $[L : K] = [L : M][M : K]$ がある。また、一般に $|\mathrm{Gal}(L/M)| \leq [L : M]$ および $[L : L^H] \leq |H|$ が線型代数の議論から成り立つ。

これらを組み合わせると、

$$|G| = [L : K] = [L : L^H][L^H : K] \leq |H|[L^H : K]$$

が成り立ち、一方で群論のLagrangeの定理より $|G| = |H| \cdot [G : H]$ である。これらの次数の不等式を精査し、原始元定理によって $L = M(\theta)$ となる元の最小多項式の次数を媒介させることで、すべての包含において過不足がないこと、すなわち $M = L^{\mathrm{Gal}(L/M)}$ および $H = \mathrm{Gal}(L/L^H)$ が次元の等価性から強制される。

Q.E.D.

(5) 条件(5): テンソル積 $L \otimes_K L \cong L^n$ を用いる証明

証明

Grothendieckの解釈に基づく。$L \otimes_K L \cong \prod_{\sigma \in G} L$ という代数同型がある。中間体 M の選択は、テンソル積の適当な商環、あるいは成分の選別に完全に対応する。具体的には、$L \otimes_M L$ というテンソル積は、$L \otimes_K L$ に関係式 $am \otimes b = a \otimes mb$ ($m \in M$) を追加した商環とみなせる。

この商操作は、直積 $\prod_{\sigma \in G} L$ のうち、$\sigma|_M = \mathrm{id}_M$ を満たす自己同型、すなわち $H = \mathrm{Gal}(L/M)$ に属する成分だけを残す射影に対応する。したがって $L \otimes_M L \cong \prod_{\sigma \in H} L$ となる。この直積の次元およびイデアル構造を解析することで、中間体 M と部分群 H の間に一対一の代数的対応が確立される。

Q.E.D.

(6) 条件(6): トレース写像によるGalois降下を用いる証明

証明

有限次Galois拡大において、トレース写像 $\mathrm{Tr}_{L/K} : L \to K$ ($x \mapsto \sum_{\sigma \in G} \sigma(x)$) は恒等的に 0 ではない。これは、Dedekindの独立性定理より、自己同型の線型結合であるトレースが零写像になり得ないことから従う。ゆえに $\mathrm{Tr}_{L/K}$ は K 上への全射である。

任意の中間体 M に対し、$H = \mathrm{Gal}(L/M)$ とおく。L から L^H へのトレース写像 Tr_{L/L^H} を考える。Galois降下の理論によれば、任意の L ベクトル空間 V に H が半線型に作用するとき、$V \cong L \otimes_{L^H} V^H$ が成り立つ。これを $V = L$ 自身（H は体自己同型として作用）に適用すると、$L \cong L \otimes_{L^H} L^H$ となり、ここから $L^H = M$ が導かれる。トレースの非退化性が、各中間体における降下の全射性を担保している。

Q.E.D.

3️⃣ 有限次Galois拡大 L/K とそのGalois群 G について $L \cong K[G]$ となることの証明

この節では、**正規底定理 (normal basis theorem)** を証明します。群 G の K 上の群環を $K[G]$ と書くとき、L と $K[G]$ が左 $K[G]$ 加群として同型であるという定理です。これは、L の K 上の基底として、ある単一の元の G 軌道 $\{\sigma(\theta) \mid \sigma \in G\}$ が取れることを意味します。

> **正規底定理.**
> 有限次Galois拡大 L/K とそのGalois群 $G = \mathrm{Gal}(L/K)$ について、左 $K[G]$ 加群としての同型 $L \cong K[G]$ が成り立つ。

(1) 分離性と行列式による証明

証明

K が無限体である場合を考える（有限体の場合は別証があるが、ここでは行列式の手法を貫く）。原始元定理より $L = K(\alpha)$ とする。$G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ とし、$\sigma_1 = \mathrm{id}$ とする。 行列 $M(x) = (\sigma_i \sigma_j(x))_{i,j}$ を考える。変数の多項式として、その行列式 $D(x) = \det M(x)$ を定義する。L/K が分離的であることから、この行列式は零多項式ではないことが代数的に示せる。

K は無限体であるから、多項式 $D(x)$ が 0 にならないような元 $\theta \in L$ が存在する。$D(\theta) \neq 0$ であることは、ベクトル $\{\sigma_1(\theta), \ldots, \sigma_n(\theta)\}$ を並べた行列の行列式が非零であることを意味し、これらが K 上一次独立であることを示す。次元は $|G| = n$ であるから、これは L の K 上の基底であり、写像 $\sum c_\sigma \sigma \mapsto \sum c_\sigma \sigma(\theta)$ が求める具体的な左 $K[G]$ 加群同型を与える。

Q.E.D.

(2) 完全分解体とLagrange補間による証明

証明

L は既約多項式 $f(x) \in K[x]$ の完全分解体である。その相異なる根を $\theta_1, \ldots, \theta_n$ とする。 Lagrangeの補間多項式 (Lagrange

interpolation polynomial) の手法を応用する。各 i に対して、

$$E_i(x) = \frac{\prod_{j \neq i}(x - \theta_j)}{\prod_{j \neq i}(\theta_i - \theta_j)} \in L[x]$$

を定義すると、$E_i(\theta_j) = \delta_{ij}$（Kroneckerのデルタ）となる。 これら多項式の係数に G の作用を噛み合わせ、全体の和をとることで、K 係数に引き戻された多項式を得る。この多項式を用いて、すべての自己同型作用に対して独立に振る舞う元 $\theta = \sum a_i \theta_i$ を注意深く構成することができ、これが正規底を与える。

Q.E.D.

(3) Dedekindの独立性定理の応用による証明

証明

もし正規底が存在しないと仮定する。すると、任意の $\alpha \in L$ に対して、軌道 $\{\sigma(\alpha)\}_{\sigma \in G}$ は K 上一次従属となる。 これは、各 α に対して、すべてが 0 ではない K の元 c_σ が存在して、$\sum_{\sigma \in G} c_\sigma \sigma(\alpha) = 0$ となることを意味する。 有限次元ベクトル空間の性質から、α を動かしたときに、共通の係数 $c_\sigma \in K$（すべてが 0 ではない）によって、任意の $\alpha \in L$ に対して $\sum_{\sigma \in G} c_\sigma \sigma(\alpha) = 0$ となる線型関係式が空間全体で成り立つことが導かれる。しかしこれは、半群の準同型が L 上一次独立であるという「Dedekindの独立性定理」に真っ向から矛盾する（$K \subset L$ であるため、K 上の依存性は L 上の依存性を導く）。したがって、一次従属にできない元 θ が存在しなければならず、それが正規底をなす。 **Q.E.D.**

(4) 表現論（係数拡大）を用いた証明

証明

L および群環 $K[G]$ は、ともに自然に左 $K[G]$ 加群とみなせる。これら2つの加群が同型であることを示すために、係数を L 自身に拡大（テンソル積・$\otimes_K L$）する。 不変体の同値条件(5)より、$L \otimes_K L \xrightarrow{\sim} \prod_{\sigma \in G} L$ が成り立つ。この右辺は、群環の係数拡大 $K[G] \otimes_K L \cong L[G]$ と左 $L[G]$ 加群として自然に同型である。

すなわち、係数を L に拡大した世界では、$L \otimes_K L \cong K[G] \otimes_K L$ という加群同型が成立している。表現論における普遍的な事実（Deuring-Noetherの定理）によれば、2つの有限次元表現（加群）が係数拡大体上で同型ならば、元の底の体の上でも同型でなければならない。したがって、 K 上でも左 $K[G]$ 加群として $L \cong K[G]$ が成り立つ。

Q.E.D.

(5) テンソル積の加群同型による証明

証明

条件(5)における $L \otimes_K L \cong L^{|G|}$ の詳細な構造論を用いる。左 L 加群構造と、右側成分への G の作用は互いに可換である。$L \otimes_K L$ を $(L, K[G])$ 両側加群とみなすと、これは $L[G]$ そのものの構造と一致する。環論における半単純環 (semisimple ring) の構造定理（Krull-Schmidtの定理）を適用する。 $L[G]$ は $K[G]$ の拡大であり、有限次元半単純代数である。両辺の直和因子を比較すると、左成分としての L の自由度が、右成分の $K[G]$ の自由度を完全に相殺していることがわかる。したがって、テンソル積の記号を純粋に代数的に「消去」することが可能であり、底の体 K 上での直和因子としての同型 $L \cong K[G]$ が抽出される。 **Q.E.D.**

(6) トレース写像によるGalois降下を用いた証明

証明

群 G の作用を持つ L 上のベクトル空間 $L[G]$ を考える。$L[G]$ の元は形式和 $\sum_{\sigma\in G} a_\sigma \sigma$ ($a_\sigma \in L$) である。 ここで、左 L 加群としての同型写像 $\Phi : L \otimes_K L \xrightarrow{\sim} L[G]$ を、以下のように具体的に定義する：

$$\Phi(x \otimes y) = \sum_{\sigma\in G} x\sigma(y)\sigma^{-1}$$

これが左 L 加群としての同型を与えることは、条件(5)の議論から従う。

次に、この空間への G の作用を導入する。$\tau \in G$ に対し、$L \otimes_K L$ への作用を右側成分への作用、すなわち $(x \otimes y)^\tau = x \otimes \tau(y)$ とする。この作用が Φ を通じて $L[G]$ 上でどのように振る舞うかを計算する：

$$\Phi((x \otimes y)^\tau) = \Phi(x \otimes \tau(y)) = \sum_{\sigma\in G} x\sigma(\tau(y))\sigma^{-1}$$

ここで置換 $\rho = \sigma\tau$ を行うと、$\sigma^{-1} = \tau\rho^{-1}$ となるので、

$$\sum_{\rho\in G} x\rho(y)\tau\rho^{-1} = \tau\left(\sum_{\rho\in G} x\rho(y)\rho^{-1}\right)$$

となる。ただし、ここでの τ の $L[G]$ への作用は、係数 a_σ への作用（半線型作用）と群の元への左乗法を組み合わせたものである。

Galois降下 (Galois descent) の主定理によれば、G 作用と両立する L ベクトル空間の同型写像が存在するとき、それぞれの G 不変部分空間（固定体による K ベクトル空間）を取ったもの同士も、K 上のベクトル空間として同型になる。 左辺 $L \otimes_K L$ の右成分作用による G 不変部分は、$(L \otimes_K L)^G = L \otimes_K K \cong L$ である。 右辺 $L[G]$ の上記の作用による G 不変部分は、定義よりまさしく $K[G]$ である。 したがって、Galois降下を適用することにより、 G 不変部分空間の間に K 上の同型

$$L \cong K[G]$$

が誘導される。この構成写像は G の左作用（加群構造）と可換であるため、左 $K[G]$ 加群としての同型が得られる。この同型写像のもとで、群環の単位元 $1 \cdot \mathrm{id} \in K[G]$ に対応する L の元を θ とおけば、$\{\sigma(\theta) \mid \sigma \in G\}$ は L の K 上の正規底を構成する。

Q.E.D.

引用・参考文献

- E. Artin, *Galois Theory*, Notre Dame Mathematical Lectures, Vol. 2, University of Notre Dame Press, 1944.
- K. Conrad, *Separability*, Expository Essays, University of Connecticut.
- K. Conrad, *Linear Independence of characters*, Expository Essays, University of Connecticut.
- K. Conrad, *Galois Descent*, Expository Essays, University of Connecticut.