体の拡大とGalois理論・正規基底定理の完全解説

本稿では、体の有限次拡大におけるGalois理論について、代数閉包への埋め込みの数 h の評価から始まり、自己同型群による中間体の対応（Galoisの基本定理）、代数閉包の存在証明、さらには群環上の加群としての構造を決定する正規基底定理に至るまで、いかなる省略も行わず、自己完結的 (self-contained) かつ厳密な完全解説を行う。

1. 諸定義と基本概念

以後の議論で用いるすべての基本的な数学的対象を厳密に定義する。自己完結性を保つため、代数学の基本用語も網羅する。

定義 (体と拡大):

- **体 (field):** 四則演算（ゼロでの割り算を除く）が自由にできる可換環である。本解説では特に断らない限り、可換体のみを扱う。
- **体の拡大 (field extension):** 体 L とその部分体 K の組を L/K と表す。このとき L は自然にスカラー倍を K の元の乗法で定めることで、 K 上のベクトル空間となる。
- **拡大次数 (degree):** L の K 上のベクトル空間としての次元を $[L:K]$ と表す。これが有限のとき、 L/K を有限次拡大という。

定義 (代数拡大と最小多項式):

- **代数的な元 (algebraic element):** L/K を体の拡大とする。 $\alpha \in L$ が K 係数の非零な多項式の根となるとき、 α は K 上代数的であるという。
- **最小多項式 (minimal polynomial):** $\alpha \in L$ を根に持つ $K[x]$ の非零多項式のうち、モニック（最高次係数が1）で次数が最小のものを α の K 上の最小多項式と呼ぶ。これは既約多項式となる。
- **分解体 (splitting field):** 多項式 $F(x) \in K[x]$ のすべての根を K に添加して得られる拡大体を $F(x)$ の分解体と呼ぶ。

定義 (分離拡大と正規拡大):

- **分離多項式 (separable polynomial):** $K[x]$ の既約多項式で、代数閉包において重根を持たないものを分離多項式と呼ぶ。
- **分離拡大 (separable extension):** 代数拡大 L/K において、任意の $\alpha \in L$ の最小多項式が分離多項式であるとき、 L/K を分離拡大と呼ぶ。
- **正規拡大 (normal extension):** 代数拡大 L/K において、 $K[x]$ の任意の既約多項式が L に1つでも根を持てば、 L において一次式の積に完全に分解されるとき、正規拡大と呼ぶ。

定義 (代数閉包と自己同型群):

- **代数閉包 (algebraic closure):** 体 K を含む代数的な拡大体であって、それ自身が代数的閉体（任意の定数でない多項式がその体の中で根を持つ体）であるものを $\bar{K}$ と表す。
- **K代数準同型 (K-algebra homomorphism):** 体 L から別の環への環準同型であって、 K の元を動かさない（ $\forall c \in K, \sigma(c) = c$ ）ものを指す。
- **自己同型群 (automorphism group):** L から L 自身への同型写像であって、 K の元を動かさないもの全体のなす群を $G(L/K)$ と表す。
- **不変体 (invariant field):** L の自己同型のなす群 G に対して、 G のすべての元によって動かない L の元全体からなる部分体を L^G と表す。定義から明らかに $K \subset L^G$ である。

定義 (Galois拡大):
有限次拡大 L/K において、 L の自己同型群 $G(L/K)$ によって固定される L の元が K の元のみであるとき、すなわち $L^{G(L/K)} = K$ が成り立つとき、 L/K を**Galois拡大**と呼ぶ。後述の定理により、これは $[L:K] = |G(L/K)|$ であること、ならびに L/K が有限次分離かつ正規拡大であることと同値である。

例 (Galois拡大の例と非例):
複素数体 $\mathbb{C}$ は実数体 $\mathbb{R}$ の 2 次拡大であり、 $[\mathbb{C}:\mathbb{R}] = 2$ である。自己同型群 $G(\mathbb{C}/\mathbb{R})$ は恒等写像と複素共役の2つの元からなり、複素共役で不変なのは実数のみであるため、これはGalois拡大である。
一方、 $K = \mathbb{Q}$ とし、 $L = \mathbb{Q}(\sqrt[3]{2})$ を考える。 L は実数体に含まれるため、 $\sqrt[3]{2}$ を他の複素数根に写すような自己同型は L 上には存在しない。したがって $G(L/K)$ は恒等写像のみとなり、 $|G(L/K)| = 1 < 3 = [L:K]$ であるからGalois拡大ではない。これは正規拡大ではない（ $x^3 - 2$ の他の根が含まれない）ことに起因する。

定義 (群環と左加群・正規基底):

- **群環 (group ring):** 群 G と体 K に対し、 G の元を基底とし K の元を係数とする形式的和 $\sum_{\sigma \in G} a_\sigma \sigma$ ($a_\sigma \in K$) の全体からなるベクトル空間に、群の積を用いて自然に積を定義した環を $K[G]$ と表す。
- **左 $K[G]$ 加群:** Galois群 G を持つGalois拡大 L/K には、 $K[G]$ の元が $(\sum a_\sigma \sigma) \cdot x = \sum a_\sigma \sigma(x)$ ($x \in L$) として作用する。これにより L は左 $K[G]$ 加群となる。
- **正規基底 (normal basis):** Galois拡大 L/K において、ある元 $\alpha \in L$ が存在して、そのGalois軌道 $\{\sigma(\alpha) \mid \sigma \in G(L/K)\}$ が L の K 上のベクトル空間としての基底をなすとき、この基底を正規基底と呼ぶ。

2. Galois理論の3つの不等式と基本定理への準備

体の有限次拡大 L/K に対し、 L から K の代数閉包 $\bar{K}$ への K 代数の準同型の個数を h とすると、Galois理論の基礎となる以下の重要な不等式が成り立つ。

命題 (3つの不等式):
1. $|G(L/K)| \leq h \leq [L:K]$
2. (Artinの不等式) 有限群 $G \subset \mathrm{Aut}(L)$ に対し、 $K = L^G$ とすると $[L:K] \leq |G|$

証明: 埋め込みの個数 h と自己同型群の不等式

まず左の不等式 $|G(L/K)| \leq h$ を示す。自己同型群 $G(L/K)$ の各元は L から L への K 代数準同型である。 L は $\bar{K}$ の部分体とみなせるため、これらは自然に L から $\bar{K}$ への K 代数準同型を与える。したがって、そのような準同型の総数 h は $|G(L/K)|$ 以上となる。

次に右の不等式 $h \leq [L:K]$ を、拡大次数 $n = [L:K]$ に関する帰納法で示す。
$n = 1$ のときは $L = K$ であり、自明に $h = 1$ となり成立する。
$n > 1$ とし、 n 未満の拡大に対しては成立すると仮定する。 $\alpha \in L \setminus K$ をとり、 $K(\alpha)$ 上の最小多項式を $F(x) \in K[x]$ とし、その次数を d とする。 $\bar{K}$ における $F(x)$ の相異なる根の個数は高々 d 個であるため、 $K(\alpha)$ から $\bar{K}$ への K 代数準同型の個数は高々 $d = [K(\alpha):K]$ である。
ここで、 $K(\alpha)$ から $\bar{K}$ への任意の埋め込みを1つ固定したとき、それを L から $\bar{K}$ への埋め込みに拡張する方法の数は、帰納法の仮定より高々 $[L:K(\alpha)]$ 通りである。よって $h \leq [K(\alpha):K] \times [L:K(\alpha)] = [L:K]$ が示された。

□

証明: Artinの不等式 $[L:K] \leq |G|$

$G = \{\sigma_1, \ldots, \sigma_n\}$ とし、 $[L:K] > n$ と仮定して矛盾を導く。
次元の仮定から、 K 上 1 次独立な L の元 $x_1, \ldots, x_{n+1}$ がとれる。
変数 $y_1, \ldots, y_{n+1}$ についての n 個の一次方程式からなる連立方程式

$$\sum_{j=1}^{n+1} \sigma_i(x_j) y_j = 0 \quad (i = 1, \ldots, n)$$

を考える。変数の数 $n+1$ が方程式の数 n より多いため、この連立方程式は L において非自明な解を持つ。
そのような非自明な解 $(y_1, \ldots, y_{n+1})$ のうち、0でない成分の個数が最小のものをとる。必要ならば順番を入れ替えることで、 $y_1, \ldots, y_r$ が0でなく、 $y_{r+1} = \cdots = y_{n+1} = 0$ であるとしてよい。また全体を y_r で割ることで $y_r = 1$ と仮定できる。
$x_1, \ldots, x_{n+1}$ は K 上 1 次独立なので、 $y_1, \ldots, y_r$ がすべて K に属することはない（すべて K に属するなら、恒等写像 $\sigma_1 = \mathrm{id}$ に対応する式から $\sum x_j y_j = 0$ となり 1 次独立性に矛盾するため）。したがって、例えば $y_1 \notin K$ である。
$K = L^G$ の定義より、ある $\tau \in G$ が存在して $\tau(y_1) \neq y_1$ となる。
連立方程式の各辺に τ を作用させると、 $\tau G = G$ であることから方程式の順番が入れ替わるだけであり、

$$\sum_{j=1}^{r} \sigma_i(x_j) \tau(y_j) = 0$$

が得られる。元の式と辺々引くと、

$$\sum_{j=1}^{r-1} \sigma_i(x_j)(y_j - \tau(y_j)) = 0$$

となる（ $y_r = \tau(y_r) = 1$ であるため第 r 項は消える）。
これは変数の個数が $r-1$ 以下の新しい非自明な解（第1成分 $y_1 - \tau(y_1) \neq 0$ ）を与えており、解の最小性に矛盾する。よって $[L:K] \leq |G|$ である。

□

> **補題 (Dedekindの補題: 指標の 1 次独立性):**

> 体 L から体 M への相異なる環準同型の集合は、 M 上のベクトル空間における関数として 1 次独立である。特に、Galois 群の元 $\sigma_1, \ldots, \sigma_n$ は L 上 1 次独立である。

証明

相異なる環準同型の集合 S が 1 次従属であるとし、非自明な関係式 $\sum_{i=1}^{m} c_i\sigma_i = 0$ ($c_i \in M \setminus \{0\}$) を持つ部分集合のうち、元数 m が最小のものを選ぶ。
自明な準同型はないため $m \geq 2$ である。 $\sigma_1 \neq \sigma_2$ より、ある $x \in L$ が存在して $\sigma_1(x) \neq \sigma_2(x)$ となる。
任意の $y \in L$ に対し $\sum_{i=1}^{m} c_i\sigma_i(xy) = 0$ が成り立つため、 $\sum_{i=1}^{m} c_i\sigma_i(x)\sigma_i(y) = 0$ である。
元の関係式に $\sigma_1(x)$ を掛けた式 $\sum_{i=1}^{m} c_i\sigma_1(x)\sigma_i(y) = 0$ を辺々引くと、

$$c_2(\sigma_2(x) - \sigma_1(x))\sigma_2(y) + \cdots + c_m(\sigma_m(x) - \sigma_1(x))\sigma_m(y) = 0$$

となる。 $\sigma_2(x) - \sigma_1(x) \neq 0$ であり $c_2 \neq 0$ であるため、これは長さ $m-1$ 以下の非自明な関係式を与えており、最小性に矛盾する。よって 1 次独立性が示された。

□

自己準同型環 $A = \mathrm{Hom}_K(L, L)$ を用いた L/K がGalois拡大ならば $L^G = K$ の証明

L/K がGalois拡大、すなわち $[L : K] = |G|$ であるとき、不変体が K に一致することを示す。
$A = \mathrm{Hom}_K(L, L)$ は K 線形写像のなす空間であり、 L は K 上 $[L : K]$ 次元のベクトル空間であるため、 A の K 上の次元は $[L : K]^2$ である。 A は元 $l \in L$ を左から掛ける操作 $(l \cdot f)(x) = lf(x)$ によって左 L ベクトル空間となる。このとき $\dim_L A = \dim_K A / [L : K] = [L : K]$ となる。
$G = G(L/K)$ の各元は K 線形写像であるため $G \subset A$ である。Dedekindの補題により G は A の中で L 上 1 次独立である。
仮定より L/K はGalois拡大であるため、 $|G| = [L : K]$ である。次元の比較から、 1 次独立な部分集合 G は A の L 上の基底となる。

ここで不変体 L^G の元 x をとる。 x を掛ける写像を $\mu_x \in A$ とする。任意の $\sigma \in G$ と $y \in L$ に対し、 $x \in L^G$ であることから $\sigma(xy) = \sigma(x)\sigma(y) = x\sigma(y)$ が成り立つ。すなわち A において $\sigma \circ \mu_x = \mu_x \circ \sigma$ であり、 μ_x は G のすべての元と可換である。
また、明らかに μ_x は任意の μ_l ($l \in L$) とも可換である。
G が A の L 上の基底であることから、任意の $f \in A$ は $f = \sum l_i\sigma_i$ と書けるため、 μ_x は A のすべての元と可換となる。
すなわち μ_x は行列環 A の中心 $Z(A)$ に含まれる。

最後に $Z(A) = K$ を示す。 $f \in Z(A)$ をとる。 f は任意の μ_l ($l \in L$) と可換であるため、 $f(lx) = lf(x)$ が成り立つ。よって f は L 線形写像であり、 $k = f(1) \in L$ とおくと $f = \mu_k$ と書ける。
さらに f は任意の $g \in A$ と可換であるため、任意の $x \in L$ について $g(kx) = kg(x)$ となる。 $x = 1$ を代入して $g(k) = kg(1)$ を得る。
もし $k \notin K$ であれば、 1 と k は K 上 1 次独立であるため、 $g(1) = 1$ かつ $g(k) = 0$ となるような K 線形写像 $g \in A$ を構成できる。このとき $0 = g(k) = kg(1) = k \cdot 1 = k$ となり、 $k \notin K$ に矛盾する。
よって $k \in K$ であり、 $Z(A) \subset K$ が示された。
以上より $\mu_x \in Z(A) \implies x \in K$ となり、 $L^G \subset K$ が導かれる。 $K \subset L^G$ と合わせて $L^G = K$ の完全な証明が完了した。

□

3. 準同型の個数 h と多項式の根の置換の関係

Galois理論が方程式の根の置換の理論であることを明らかにするため、 K 代数準同型の個数 h の評価が、多項式の根の置換といかに結びついているかを解説する。

> **命題:** 分解体 $L = K(\alpha_1, \ldots, \alpha_r)$ において、 L から $\bar{K}$ への K 代数準同型 σ は、根の集合 $R = \{\alpha_1, \ldots, \alpha_r\}$ 上の置換（全単射）を引き起こし、 σ はその置換の振る舞いによって完全に決定される。

証明

多項式を $F(x) = c_n x^n + \cdots + c_1 x + c_0$ ($c_i \in K$) とする。
根 $\alpha \in R$ を任意にとると、 $F(\alpha) = 0$ である。
σ は K 代数準同型であるため、 K の元を動かさず ($\sigma(c_i) = c_i$)、和と積の演算を保存する。したがって、以下の等式が成り立つ。

$$F(\sigma(\alpha)) = c_n \sigma(\alpha)^n + \cdots + c_1 \sigma(\alpha) + c_0 = \sigma(c_n \alpha^n + \cdots + c_1 \alpha + c_0) = \sigma(F(\alpha)) = \sigma(0) = 0$$

ゆえに、 $\sigma(\alpha)$ もまた $F(x)$ の根であり、 $\sigma(\alpha) \in R$ となる。すなわち σ は R から R への写像 $\sigma|_R : R \to R$ を定める。
一般に体の準同型写像は単射であるため、その制限である $\sigma|_R$ は有限集合 R からそれ自身への単射となる。有限集合からそれ自身への単射は全単射であるから、 $\sigma|_R$ は根の集合 R 上の置換である。
また、 L の任意の元 y は、根 $\alpha_1, \ldots, \alpha_r$ と K の元を用いた有理式で表される。 σ は K の元を動かさず四則演算を保存するため、 y の像 $\sigma(y)$ は各根の像 $\sigma(\alpha_1), \ldots, \sigma(\alpha_r)$ によって一意に定まる。すなわち、 σ は R 上の置換としてどのように作用するかによって一意に決定される。

□

4. 体の代数閉包の存在証明

任意の体 K に対してその代数閉包 $\bar{K}$ が存在することを、Emil Artinの構成法およびErnst Steinitzの濃度評価による方法の2通りで証明する。

補助定理

> **定義 (Zornの補題):**
> 空でない半順序集合 X において、任意の全順序部分集合（鎖）が X 内に上界を持つならば、 X は極大元を持つ。

> **補題1 (代数拡大の推移性):** M/K を代数拡大とし、 α を M 上代数的な元とする。このとき α は K 上代数的である。
>
> *証明*
>
> α は M 上代数的であるため、あるモニック多項式 $x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 = 0$ ($c_i \in M$) を満たす。仮定より各係数 c_i は K 上代数的である。有限次拡大の塔
>
> $$K \subset K(c_0) \subset K(c_0, c_1) \subset \cdots \subset K(c_0, \ldots, c_{n-1})$$

を考えると、各段階は代数的な元の添加であるため有限次拡大である。ゆえに全体の拡大次数 $[K(c_0,\dots,c_{n-1}):K]$ は有限である。
さらに α は $K(c_0,\dots,c_{n-1})$ 上の多項式の根であるから、拡大次数 $[K(c_0,\dots,c_{n-1},\alpha):K(c_0,\dots,c_{n-1})]$ も有限である。
次元の乗法公式より $[K(c_0,\dots,c_{n-1},\alpha):K]$ は有限となる。有限次拡大は代数拡大であるため、その要素である α は K 上代数的である。

□

補題2 (有限個の多項式に対する分解体の存在): 体 K とその上の定数でない多項式の有限集合 $\{f_1,\dots,f_n\}$ が与えられたとき、 K の拡大体 L が存在して、各 f_i は L の中に少なくとも1つの根を持つ。

証明

多項式の個数 n に関する帰納法で示す。
$n=1$ のとき、 $f_1(x)\in K[x]$ の $K[x]$ における既約因子を $p(x)$ とする。剰余環 $L_1=K[x]/(p(x))$ は体となる。自然な単射準同型 $K\to L_1$ により L_1 を K の拡大体とみなすことができる。 L_1 において、元 $\bar{x}=x+(p(x))$ は $p(x)$ の根であり、したがって $f_1(x)$ の根となる。
$n=k$ まで成立すると仮定し、 $n=k+1$ の場合を考える。帰納法の仮定より、 $f_1,\dots,f_k$ がすべて根を持つような K の拡大体 L_k が存在する。 L_k 上の多項式として $f_{k+1}(x)$ を考え、 $n=1$ の場合と同様に $f_{k+1}(x)$ の $L_k[x]$ における既約因子による剰余体を構成することで、 L_k の拡大体 L_{k+1} が得られる。これを L とすればよい。

□

方法A: Artinの構成法

代数閉包の存在証明 (Artin)

1. **すべての多項式に対する変数の準備:** K 上のすべての定数でないモニック多項式の集合を S とする。各多項式 $f\in S$ に対して独立な不定元 x_f を用意し、巨大な多項式環 $R=K[\{x_f\}_{f\in S}]$ を構成する。

2. **真のイデアルの構成:** R において、すべての $f(x_f)$ によって生成されるイデアルを I とする。
この I が R の真のイデアル ($1\notin I$) であることを背理法で示す。もし $1\in I$ ならば、有限個の $f_1,\dots,f_n\in S$ と R の元 $g_1,\dots,g_n$ を用いて、

$$1=\sum_{i=1}^{n} g_i f_i(x_{f_i})$$

と表せる。補題2より、 $f_1,\dots,f_n$ のすべてが少なくとも1つの根を持つ K の拡大体 L が存在する。 f_i の L における根の1つを α_i とする。
多項式環の普遍性により、 $x_{f_i}\mapsto\alpha_i$ とし、それ以外の不定元 $x_f\mapsto 0$ とする環準同型 $\varphi:R\to L$ が一意に定まる。上の等式の両辺に φ を適用すると、 L において

$$1=\sum_{i=1}^{n} \varphi(g_i) f_i(\alpha_i)$$

となる。しかし $f_i(\alpha_i)=0$ であるため右辺は 0 となる。これは体 L において $1=0$ であることを意味し、矛盾である。したがって I は真のイデアルである。

3. **極大イデアルの存在:** Zornの補題により、 I を含む極大イデアル M が存在する。

4. **1段階目の拡大体 E_1 の構成:** M は極大イデアルであるため、剰余環 $E_1 = R/M$ は体となる。任意の $f \in S$ に対し、 E_1 における元 $\bar{x}_f = x_f + M$ は

$$f(\bar{x}_f) = f(x_f) + M = 0 + M$$

を満たすため、 f の根となる。すなわち、 K 係数のすべての定数でない多項式は、 E_1 の中に根を持つ。

5. **反復と極限:** $E_0 = K$ とし、 E_n から E_{n+1} を帰納的に構成し、体の昇鎖を得る。その和集合 $E = \bigcup E_n$ は代数的閉体となる。

6. **代数閉包 $\bar{K}$ の抽出:** E の中で K 上代数的な元だけを集めた部分体を $\bar{K}$ とする。補題1（代数拡大の推移性）により、 $\bar{K}$ は代数的閉体であり、かつ K の代数拡大であるため、これが求める代数閉包である。

□

方法B: Steinitzの濃度評価による別証明

代数閉包の存在証明 (Steinitz)

ステップ1 (濃度の評価): K 上の多項式環 $K[x]$ の濃度は $\kappa = \max(|K|, \aleph_0)$ である。 L/K を任意の代数拡大とすると、各元 $\alpha \in L$ は $K[x]$ 内の最小多項式 $p_\alpha(x)$ を持つ。1つの多項式が持つ根の数は有限であるため、 L の各元は $K[x]$ の元と有限個の選択肢の組として指定できる。ゆえに $|L| \leq |K[x]| \times \aleph_0 = \kappa$ である。

ステップ2 (Zornの補題の適用): 濃度が 2^κ であるような巨大な集合 Ω であって、 $K \subset \Omega$ を満たすものを固定する。 Ω の部分集合であって、 K を含み、かつ K の代数拡大となるような体構造を持つもの全体の集合を $\mathcal{A}$ とし、包含関係と体構造の拡張関係で半順序をいれる。鎖の和をとることで上界が存在するため、Zornの補題より極大元 $\bar{K}$ が存在する。

ステップ3 (代数閉性): もし $\bar{K}$ が代数的閉体でないなら、 $\bar{K}$ を真に含むような代数拡大 L が抽象的に構成できる。
$|L| \leq \kappa < 2^\kappa = |\Omega|$ であるため、 $L \setminus \bar{K}$ を $\Omega \setminus \bar{K}$ の中へ単射で写し、体構造を移植することで、 Ω 内部に $\bar{K}$ を真に含む代数拡大を構成できる。これは $\bar{K}$ の極大性に矛盾する。よって $\bar{K}$ は代数閉包である。

□

5. Galois理論の基本定理

Galois拡大における中間体と、自己同型群の部分群との間の双対性を証明する。

> **定理 (Galois理論の基本定理):**
> L/K を有限次Galois拡大とし、 $G = G(L/K)$ とする。中間体 M 全体の集合と、 G の部分群 H 全体の集合の間に、以下の全単射が存在する。
> 1. $H \mapsto M = L^H$
> 2. $M \mapsto H = G(L/M)$
> さらに、 $[L:M] = |G(L/M)|$ および $[M:K] = [G:G(L/M)]$ が成り立ち、 M/K が正規拡大であることと $G(L/M)$ が G の正規部分群であることは同値であり、このとき $G(M/K) \cong G/G(L/M)$ となる。

証明

ステップ1 (部分群 $\to$ 中間体 $\to$ 部分群):
部分群 H に対し $M = L^H$ とする。 H' = $G(L/M)$ とおく。 H の定義から $H \subset H'$ であり、 $|H| \leq |H'|$ である。
Artinの不等式より $[L:M] \leq |H|$ である。また一般論より $|H'| \leq [L:M]$ である。
これらを合わせると $|H| \leq [L:M] \leq |H'|$ となる。 $H \subset H'$ であるため、すべて等号となり、 $H = H'$ かつ $[L:M] = |H|$ が得られる。

ステップ2 (中間体の分離性と拡大次数の対応):
L/K はGalois拡大であるため、 $h_L = [L:K]$ である。任意の中間体 M に対して、埋め込みの数は乗法的に $h_L = h_M \times h_{L/M}$ となる。 $h_M \leq [M:K]$ および $h_{L/M} \leq [L:M]$ であり、 $[L:K] = [M:K] \times [L:M]$ であるため、 $h_M = [M:K]$ が従う。すなわち M/K は分離拡大である。

ステップ3 (中間体 $\to$ 部分群 $\to$ 中間体):
中間体 M に対し $H = G(L/M)$ とする。 L/K は正規拡大であるため、 M から $\bar{K}$ への h_M 個の任意の K 準同型は、 L の自己同型 $\sigma \in G$ の制限として得られる。
G の2つの元が M 上で同じ作用を持つのは、 $\sigma^{-1} \circ \sigma' \in G(L/M)$ のときである。したがって相異なる埋め込みの数は剰余類の個数 $[G : G(L/M)]$ に等しい。
ゆえに $[M:K] = h_M = |G|/|G(L/M)|$ である。 $[L:K] = [L:M] \times [M:K]$ と $|G| = [L:K]$ を用いると、 $|G(L/M)| = [L:M]$ となる。すなわち L/M はGalois拡大である。
Artinの定理（ $[L:M] \leq |G(L/M)|$ で等号成立時、 $L^{G(L/M)} = M$ ）により $L^{G(L/M)} = M$ であるため、 $L^H = M$ が示された。

ステップ4 (正規部分群と正規拡大):
$\sigma(M)$ を固定する群は $\sigma H \sigma^{-1}$ である。 M/K が正規拡大であること（任意の K 準同型の像が M に一致すること）は、任意の $\sigma \in G$ について $\sigma(M) = M$ となることと同値である。これは $\sigma H \sigma^{-1} = H$ 、すなわち H が正規部分群であることと同値である。
このとき制限制像 $\varphi : G \to G(M/K), \sigma \mapsto \sigma|_M$ の核は $H = G(L/M)$ であり、全射であることから準同型定理より $G/H \cong G(M/K)$ が成り立つ。

□

6. 正規基底定理

Galois拡大 L/K が、群環 $K[G]$ 上の加群としてどのような構造を持つかを決定する。最初のチャット内で言及された定理の完全かつ厳密な証明を与える。

> **定理 (正規基底定理):**
> 体の有限次Galois拡大 L/K において、ある元 $\alpha \in L$ が存在して、そのGalois軌道 $\{\sigma(\alpha) \mid \sigma \in G\}$ が L の K 上の基底（正規基底）をなす。これは左 $K[G]$ 加群として $L \cong K[G]$ であることと同値である。

証明

証明は基本体 K が無限体の場合と有限体の場合に分けて行う。

ケース1: K が無限体の場合
L/K のGalois群を $G = \{\sigma_1, \ldots, \sigma_n\}$ とする。
変数 Y_σ ($\sigma \in G$) からなる $n \times n$ 行列 $A(Y)$ を、その (i, j) 成分が $Y_{\sigma_i \sigma_j^{-1}}$ となるように定義する（群行列式）。群の乗積表の性質から各行・各列は変数の置換になり、行列式 $\det A(Y)$ を展開すると Y_{id}^n などの項が現れ相殺されないため、これは多項式環 $L[\{Y_\sigma\}]$ においてゼロ多項式ではない。

L の K 上の基底を $v_1, \ldots, v_n$ とし、独立な変数 $X_1, \ldots, X_n$ を用いて $x = \sum_{k=1}^n X_k v_k$ とおく。
ここで $Y_\sigma = \sigma(x) = \sum_{k=1}^n X_k \sigma(v_k)$ という変数変換を考える。
Dedekindの補題より、自己同型 $\sigma_1, \ldots, \sigma_n$ は L 上 1 次独立であるため、写像 $z \mapsto (\sigma_1(z), \ldots, \sigma_n(z))$ の像は L^n 全体を張る（もし真の部分空間に含まれるなら、非自明な線形関係 $\sum c_i \sigma_i(z) = 0$ が成立し矛盾する）。
これは、基底 $\{v_k\}$ を用いた行列 $(\sigma_i(v_k))_{i,k}$ が正則行列であることを意味し、したがって変数変換
$(X_1, \ldots, X_n) \mapsto (Y_{\sigma_1}, \ldots, Y_{\sigma_n})$ は全単射な線形変換である。

非ゼロ多項式 $\det A(Y)$ に対して正則な線形変換を施して得られる新しい多項式

$$d(X_1, \ldots, X_n) = \det \left(\sigma_i \sigma_j^{-1}(x) \right)_{1 \le i,j \le n} \in L[X_1, \ldots, X_n]$$

もまた、ゼロ多項式ではない。

K は無限体であるため、ゼロ多項式ではない $d(X_1, \ldots, X_n)$ に対して、 $d(a_1, \ldots, a_n) \neq 0$ となるような具体的な値 $a_1, \ldots, a_n \in K$ が存在する。
このとき $\alpha = \sum_{k=1}^n a_k v_k \in L$ とおけば、行列 $(\sigma_i \sigma_j^{-1}(\alpha))$ は正則行列となる。
行列式が 0 でないということは、列ベクトルである $\{\sigma_j(\alpha)\}_{j=1}^n = \{\sigma(\alpha) \mid \sigma \in G\}$ が L 上で 1 次独立であることを意味する。したがって部分体である K 上でも 1 次独立であり、元数が次元 $n = [L : K]$ に等しいことから、これは L の K 上の基底（正規基底）をなす。

ケース2: K が有限体の場合
以下の2つの定義と定理を準備する。

- **フロベニウス自己同型 (Frobenius automorphism):** 有限体 $K = \mathbb{F}_q$ (q は素数の冪 p^m) の代数拡大において、写像 $\sigma : x \mapsto x^q$ を考える。標数 p においては $(x+y)^p = x^p + y^p$ が成り立つため（Freshman's dream）、これは体の準同型となる。全単射性も容易に示され、これは自己同型となる。有限体のGalois群はこれにより生成される巡回群である。
- **単項イデアル整域 (PID):** 任意のイデアルがただ1つの元で生成される整域。多項式環 $K[T]$ は除法の原理が成り立つためPIDである。
- **PID上の有限生成加群の構造定理:** PID R 上の有限生成加群 M は、自由加群と有限個の巡回ねじれ加群の直和に同型である。すなわち $M \cong R^r \oplus R/(d_1) \oplus \cdots \oplus R/(d_k)$ （ただし $d_1 \mid d_2 \mid \cdots \mid d_k$ ）。

$K = \mathbb{F}_q$ とし、 L/K のGalois群 $G = \langle \sigma \rangle = \{\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$ を考える。 L は自己同型 σ の作用を通じて、多項式環 $K[T]$ 加群とみなすことができる。 T は σ として作用する。 $\sigma^n = \mathrm{id}$ であるため、 L は $K[\sigma] \cong K[T]/(T^n - 1)$ 上の加群となる。

Dedekindの補題より、 $\mathrm{id}, \sigma, \ldots, \sigma^{n-1}$ は L 上 1 次独立であるため、 σ は次数 n 未満のいかなる非ゼロ多項式も零化しない。すなわち、 σ の K 上の最小多項式 $p(T)$ の次数は n 以上でなければならない。
一方で $\sigma^n - 1 = 0$ を満たすため $p(T)$ は $T^n - 1$ を割り切る。よって $p(T) = T^n - 1$ である。

PID $K[T]$ 上の有限生成加群の構造定理をベクトル空間 L に適用する。 L は有限次元であるため $r = 0$ であり、 L は巡回加群の直和として

$$L \cong K[T]/(f_1(T)) \oplus \cdots \oplus K[T]/(f_k(T))$$

（ただし $f_1 \mid f_2 \mid \cdots \mid f_k$ ）と分解される。
このとき加群全体の零化イデアルの生成元である最小多項式は最大の因子 $f_k(T)$ に等しいため、 $f_k(T) = T^n - 1$ である。
両辺の K 上のベクトル空間としての次元を比較すると、

$$n = \dim_K L = \sum_{i=1}^{k} \deg f_i(T) \geq \deg f_k(T) = n$$

となり、等号が成立するためには $k = 1$ かつ $f_1(T) = T^n - 1$ でなければならない。

したがって、 $K[\sigma]$ 加群として

$$L \cong K[T]/(T^n - 1) \cong K[G]$$

が得られる。この同型において $1 \in K[T]/(T^n - 1)$ に対応する L の元を α とすると、 α は $K[G]$ 加群として L を生成し、 $\{\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha)\}$ は L の K 上の基底（正規基底）となる。

□

結論

無限体・有限体のいずれの場合においても、有限次Galois拡大 L/K は正規基底 $\{\sigma(\alpha) \mid \sigma \in G\}$ を持つことが厳密に示された。
これにより、写像

$$\varphi : K[G] \longrightarrow L, \quad \sum_{\sigma \in G} a_\sigma \sigma \longmapsto \sum_{\sigma \in G} a_\sigma \sigma(\alpha)$$

は左 $K[G]$ 加群としての完全な同型射を与える。よって $L \cong K[G]$ である。

参考文献

- Artin, E. (1998). *Galois Theory*. Dover Publications. [Link]
- Lang, S. (2002). *Algebra* (Revised 3rd ed.). Springer. [Link]
- Morandi, P. (1996). *Field and Galois Theory* (Graduate Texts in Mathematics, 167). Springer. [Link]