Galois理論と正規底の定理：群環加群の代数構造、Galois対応の証明および計算例

体 K の有限次Galois拡大 L/K と、そのGalois群 G に対する K 上の群環 $K[G] = \bigoplus_{g \in G} Kg$ の理論の関係について詳細に解説する。Galois理論において、拡大体 L は基礎体 K 上のベクトル空間であるだけでなく、Galois群 G の作用を受ける構造を持つ[cite: 1]。群環 $K[G]$ を用いると、この G の作用と K 上のベクトル空間としての構造を「 $K[G]$ 加群 ($K[G]$-module)」という1つの代数構造として統合的に扱うことができる[cite: 1]。

この観点から得られる最も重要な代数的帰結が「正規底の定理 (normal basis theorem)」である。この定理は、直観的 (intuitive) には「拡大体 L と群環 $K[G]$ は、 $K[G]$ 加群として全く同じ構造を持っている」ということを主張する。本稿では、基礎概念の定義から出発し、Dedekindの指標の独立定理、正規底の定理の完全な証明（無限体および有限体の場合）、Galois対応の基本定理への応用、そして様々な体拡大における具体的な計算例を完全に書き下す。

1. 基礎概念の定義と群環加群としての構造

定義 1.1 (分離拡大・正規拡大・Galois拡大)
体 K の拡大体 L を考える。

- L/K が代数的拡大であり、 L の任意の元 a の K 上の最小多項式 $f(X) \in K[X]$ が重根を持たない（すなわち $\gcd(f(X), f'(X)) = 1$ である）とき、 L/K を**分離的拡大 (separable extension)** という[cite: 1]。
- K 係数の既約多項式 $f(X) \in K[X]$ が L 内に1つの根を持てば、 $f(X)$ のすべての根が L に属するとき（すなわち $f(X)$ が $L[X]$ 内で一次式の積に分解するとき）、 L/K を**正規拡大 (normal extension)** という[cite: 1]。
- 有限次拡大 L/K が分離的かつ正規であるとき、 L/K を**有限次Galois拡大 (Galois extension)** という。

このとき、 L の自己同型であって K の元を点ごとに固定するものの全体は群をなす。これを L/K の**Galois群 (Galois group)** と呼び、 $G = \mathrm{Gal}(L/K)$ と表す。Galois理論の基本性質より、 L の K 上のベクトル空間としての次元（拡大次数） $[L:K]$ はGalois群の位数 $|G|$ に等しい。

定義 1.2 (群環と左加群構造)
G を有限群、 K を体とするとき、 G の K 上の**群環 (group ring)** を $K[G]$ と書く。これは、集合としては G の元を基底とする K 上のベクトル空間

$$K[G] = \bigoplus_{g \in G} Kg = \left\{ \sum_{g \in G} a_g g \quad a_g \in K \right\}$$

であり、 $K[G]$ における2元の積は、分配法則および G の群としての演算規則を線形に拡張することで定義される。すなわち、 $\sum_{g \in G} a_g g$ と $\sum_{h \in G} b_h h$ の積は

$$\left(\sum_{g \in G} a_g g \right) \left(\sum_{h \in G} b_h h \right) = \sum_{g,h \in G} (a_g b_h)(gh) = \sum_{x \in G} \left(\sum_{g \in G} a_g b_{g^{-1}x} \right) x$$

で与えられる。
L/K を有限次Galois拡大、 $G = \mathrm{Gal}(L/K)$ とするとき、 L には自然に $K[G]$ 上の左加群 (left $K[G]$-module) の構造が入る[cite: 1]。作用は、 $\lambda = \sum_{g \in G} a_g g \in K[G]$ と $x \in L$ に対して、

$$\lambda \cdot x = \sum_{g \in G} a_g g(x)$$

と定義される。

2. Dedekindの指標の独立定理

正規底の定理の証明およびGalois理論全般において決定的な役割を果たす、体の準同型の線形独立性に関するDedekindの定理を証明する。

補題 2.1 (Dedekindの指標の独立定理)
L と E を体とし、 $\sigma_1, \dots, \sigma_m$ を L から E への相異なる体の準同型（単射）とする。このとき、これらは E 上のベクトル空間 $\mathrm{Map}(L, E)$ の元として線形独立である。すなわち、 $a_1, \dots, a_m \in E$ について、すべての $x \in L$ に対して

$$a_1\sigma_1(x) + a_2\sigma_2(x) + \cdots + a_m\sigma_m(x) = 0$$

が成り立つならば、 $a_1 = a_2 = \cdots = a_m = 0$ である。

証明:
背理法によって証明する。相異なる準同型 $\sigma_1, \dots, \sigma_m$ の間に非自明な線形従属関係が存在すると仮定する。そのような関係式の中で、非零の係数の個数が最小（これを r とする）であるものを1つ選ぶ。適当に番号を付け替えることで、これを

$$a_1\sigma_1(x) + a_2\sigma_2(x) + \cdots + a_r\sigma_r(x) = 0 \quad (\text{すべての } x \in L) \quad \cdots (2.1)$$

とする。ここで $r \geq 1$ であり、各 $a_i \in E$ はすべて 0 でない。
もし $r = 1$ ならば、 $a_1\sigma_1(x) = 0$ である。 $x = 1$ を代入すると $\sigma_1(1) = 1 \neq 0$ より $a_1 = 0$ となり矛盾する。よって $r \geq 2$ である。
σ_1 と σ_r は相異なる準同型であるから、ある $y \in L$ が存在して $\sigma_1(y) \neq \sigma_r(y)$ となる（体の準同型は 0 を 0 に送るため $y \neq 0$ である）。
任意に $x \in L$ をとる。式 (2.1) に yx を代入すると、 σ_i は体の準同型であるから $\sigma_i(yx) = \sigma_i(y)\sigma_i(x)$ となり、

$$a_1\sigma_1(y)\sigma_1(x) + a_2\sigma_2(y)\sigma_2(x) + \cdots + a_r\sigma_r(y)\sigma_r(x) = 0 \quad \cdots (2.2)$$

が得られる。一方で、元の式 (2.1) の両辺に $\sigma_r(y) \in E$ を掛けると、

$$a_1\sigma_r(y)\sigma_1(x) + a_2\sigma_r(y)\sigma_2(x) + \cdots + a_r\sigma_r(y)\sigma_r(x) = 0 \quad \cdots (2.3)$$

となる。式 (2.2) から式 (2.3) を引くと、第 r 項が相殺されて

$$a_1(\sigma_1(y) - \sigma_r(y))\sigma_1(x) + a_2(\sigma_2(y) - \sigma_r(y))\sigma_2(x) + \cdots + a_{r-1}(\sigma_{r-1}(y) - \sigma_r(y))\sigma_{r-1}(x) = 0$$

が得られる。これはすべての $x \in L$ に対して成立する。
ここで第1項の係数に着目すると、 $a_1 \neq 0$ かつ $\sigma_1(y) - \sigma_r(y) \neq 0$ であるため、 $a_1(\sigma_1(y) - \sigma_r(y)) \neq 0$ である。これは長さが $r-1$ （ $1 \leq r-1 < r$ ）の非自明な線形従属関係を意味し、 r の最小性に矛盾する。したがって、相異なる準同型は常に線形独立である。（証明終）

3. 正規底の定理 (Normal Basis Theorem)

定理 3.1 (正規底の定理)
L/K を有限次Galois拡大とし、 $G = \mathrm{Gal}(L/K)$ とする。このとき、 L は $K[G]$ 加群として $K[G]$ 自身（正則加群）と同型で

ある。すなわち、 $L \cong K[G]$ である[cite: 1]。
言い換えると、ある元 $\alpha \in L$ が存在して、集合

$$\{\sigma(\alpha) \mid \sigma \in G\}$$

は L の K 上のベクトル空間としての基底をなす。このような基底を **正規底 (normal basis)** と呼び、 α を正規底を生成する元と呼ぶ。

証明を完結にするため、有限体の場合の証明で必要となる線形代数学の補助定理をあらかじめ証明しておく。

補題 3.2 (巡回ベクトルの存在)
V を体 K 上の n 次元ベクトル空間とし、 $T : V \to V$ を K 線形変換とする。 T の最小多項式 (minimal polynomial) の次数が n に等しいならば、ある $v \in V$ が存在して、 $\{v, T(v), T^2(v), \ldots, T^{n-1}(v)\}$ は V の基底をなす（このとき v を T に関する巡回ベクトルと呼ぶ）。

補題 3.2 の証明:
体 K 上の主理想整域 $K[X]$ 上の有限生成モジュールに関する構造定理（単因子論）を V に適用する。 V は $X \cdot v = T(v)$ により $K[X]$ 加群とみなせる。構造定理により、 V は

$$V \cong K[X]/(f_1(X)) \oplus K[X]/(f_2(X)) \oplus \cdots \oplus K[X]/(f_k(X))$$

と分解される。ここで $f_1(X), \ldots, f_k(X) \in K[X]$ はモニック多項式であり、 $f_1(X) \mid f_2(X) \mid \cdots \mid f_k(X)$ を満たす。
この分解において、 T の最小多項式は最大単因子 $f_k(X)$ に等しい。条件より最小多項式の次数は $n = \dim_K V$ であるから、 $\deg f_k(X) = n$ である。
一方、 $\dim_K V = \sum_{i=1}^{k} \deg f_i(X)$ である。 $\deg f_i(X) \geq 1$ かつ $\deg f_k(X) = n$ であることから、直和の項数は $k = 1$ でなければならない。
したがって、 $K[X]$ 加群として $V \cong K[X]/(f_k(X))$ である。この同型において $1 \bmod (f_k(X))$ に対応する V の元を v とおくと、 $\{v, T(v), \ldots, T^{n-1}(v)\}$ は V の K 上の基底を構成する。（証明終）

以下、基礎体 K が無限体の場合と有限体の場合に分けて、正規底の定理の完全な証明を与える。

定理 3.1 の証明 (基礎体 K が無限体の場合):
$n = [L : K] = |G|$ とする。 $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ とし、 $\sigma_1 = \mathrm{id}$ （等同写像）とする。 L の K 上の任意の基底 $u_1, u_2, \ldots, u_n$ を1つ固定する。
$n \times n$ 行列 $A = (\sigma_i(u_j))_{1 \leq i,j \leq n}$ を考える。この行列の行列式は非零、すなわち $\det A \neq 0$ である。なぜなら、もし $\det A = 0$ ならば、行ベクトルが線形従属となり、すべてが 0 ではない $c_1, \ldots, c_n \in L$ が存在して、すべての $j\,(1 \leq j \leq n)$ について $\sum_{i=1}^{n} c_i \sigma_i(u_j) = 0$ となる。任意の $x \in L$ は $x = \sum_{j=1}^{n} b_j u_j$ （ $b_j \in K$ ）と書けるため、

$$\sum_{i=1}^{n} c_i \sigma_i(x) = \sum_{i=1}^{n} c_i \sigma_i \left(\sum_{j=1}^{n} b_j u_j \right) = \sum_{j=1}^{n} b_j \left(\sum_{i=1}^{n} c_i \sigma_i(u_j) \right) = 0$$

となり、相異なる Galois 群の元の線形独立性（補題 2.1）に矛盾するからである。

次に、 n 個の独立変数 $X_1, \ldots, X_n$ に対し、行列 $M(X_1, \ldots, X_n)$ の (i, j) 成分を

$$M(X_1, \ldots, X_n)_{i,j} = \sigma_i \sigma_j^{-1} \left(\sum_{k=1}^{n} X_k u_k \right)$$

と定義する。その行列式 $P(X_1, \ldots, X_n) = \det M(X_1, \ldots, X_n)$ は $L[X_1, \ldots, X_n]$ の元である。この多項式 P が零多項式で

ないことを示す。

A は正則行列であるから逆行列 $A^{-1} = (v_{k,j})_{1 \le k,j \le n} \in M_n(L)$ が存在する。定義より $\sum_{k=1}^{n} \sigma_i(u_k) v_{k,j} = \delta_{i,j}$ （Kroneckerのデルタ）である。ここで線形変数変換

$$X_k = \sum_{j=1}^{n} v_{k,j} Y_j \quad (1 \le k \le n)$$

を導入する。これを代入すると、

$$\sum_{k=1}^{n} X_k \sigma_i(u_k) = \sum_{k=1}^{n} \left(\sum_{j=1}^{n} v_{k,j} Y_j \right) \sigma_i(u_k) = \sum_{j=1}^{n} Y_j \left(\sum_{k=1}^{n} \sigma_i(u_k) v_{k,j} \right) = \sum_{j=1}^{n} Y_j \delta_{i,j} = Y_i$$

となる。特に $\sigma_1 = \mathrm{id}$ より $\sum_{k=1}^{n} X_k u_k = Y_1$ である。
$\sigma_i \sigma_j^{-1} \in G$ であるから、ある一意的な添字 l $(1 \le l \le n)$ が定まり $\sigma_i \sigma_j^{-1} = \sigma_l$ となる。したがって、変数変換後の行列の (i,j) 成分は

$$M_{i,j} = \sigma_l \left(\sum_{k=1}^{n} X_k u_k \right) = \sum_{k=1}^{n} X_k \sigma_l(u_k) = Y_l$$

となる。対角成分 $(i = j)$ では $\sigma_i \sigma_i^{-1} = \mathrm{id} = \sigma_1$ より成分は常に Y_1 である。非対角成分 $(i \neq j)$ では $\sigma_i \sigma_j^{-1} \neq \sigma_1$ より成分は Y_1 以外の変数 Y_l $(l \neq 1)$ となる。

行列式の定義に従って展開すると、

$$\det M = \sum_{\pi \in S_n} \mathrm{sgn}(\pi) M_{1,\pi(1)} M_{2,\pi(2)} \cdots M_{n,\pi(n)}$$

恒等置換 $\pi = \mathrm{id}$ に対応する項は対角成分の積 Y_1^n であり、その係数は 1 である。 $\pi \neq \mathrm{id}$ である置換については、固定されない添字が少なくとも2つ存在するため、対応する項における Y_1 の次数は $n-2$ 以下である。したがって、 $\det M$ は $Y_1, \ldots, Y_n$ の多項式として Y_1^n の項をもち、零多項式ではない。変数変換が正則であるため、元の多項式 $P(X_1, \ldots, X_n)$ も零多項式ではない。

K は無限体であるため、零多項式でない多項式 $P \in L[X_1, \ldots, X_n]$ が K^n 上で恒等的に 0 となることはない[cite: 1]。したがって、ある $c_1, \ldots, c_n \in K$ が存在して $P(c_1, \ldots, c_n) \neq 0$ となる。
$\alpha = \sum_{k=1}^{n} c_k u_k \in L$ とおく。このとき行列 $M(\alpha) = (\sigma_i \sigma_j^{-1}(\alpha))_{1 \le i,j \le n}$ は正則である。もし $\{\sigma_j^{-1}(\alpha)\}_{1 \le j \le n}$ （これは $\{\sigma(\alpha)\}_{\sigma \in G}$ と集合として一致する）が K 上線形従属であれば、ある $a_1, \ldots, a_n \in K$ （すべてが 0 でない）が存在して $\sum_{j=1}^{n} a_j \sigma_j^{-1}(\alpha) = 0$ となる。各 σ_i を作用させると $\sum_{j=1}^{n} a_j \sigma_i \sigma_j^{-1}(\alpha) = 0$ となり、行列 $M(\alpha)$ の列ベクトルが線形従属となって $\det M(\alpha) \neq 0$ に反する。
ゆえに $\{\sigma(\alpha) \mid \sigma \in G\}$ は K 上線形独立であり、要素数が $|G| = n$ であるから L の K 上の基底（正規底）を構成する。（証明終）

定理 3.1 の証明 (基礎体 K が有限体の場合):
$K = \mathbb{F}_q$ とし、 $L = \mathbb{F}_{q^n}$ をその n 次拡大体とする。有限体の理論より L/K はGalois拡大であり、そのGalois群 $G = \mathrm{Gal}(L/K)$ は Frobenius 自己同型

$$\phi : L \to L, \quad x \mapsto x^q$$

によって生成される位数 n の巡回群 $G = \langle \phi \rangle = \{\mathrm{id}, \phi, \phi^2, \ldots, \phi^{n-1}\}$ である。
群環 $K[G]$ は多項式環のイデアルによる商環 $K[X]/(X^n - 1)$ と同型である。したがって、 L を ϕ の作用によって $K[X]$ 加群とみなす（ $X \cdot x = \phi(x) = x^q$ ）。

補題 2.1 (Dedekindの独立定理) より、相異なる自己同型 $\mathrm{id}, \phi, \phi^2, \ldots, \phi^{n-1}$ は K 上線形独立である。これは、 $n-1$ 次以下の任意の非零多項式 $g(X) \in K[X]$ に対して $g(\phi) \neq 0$ であることを意味する。したがって、線形変換 $\phi : L \to L$ の最小多項式 $m_\phi(X) \in K[X]$ の次数は n 以上である。
一方、 $\phi^n = \mathrm{id}$ より $\phi^n - \mathrm{id} = 0$ であるから、最小多項式 $m_\phi(X)$ は $X^n - 1$ を割り切る。モニック多項式の次数の比較より、最小多項式は

$$m_\phi(X) = X^n - 1$$

である。

最小多項式の次数が $\dim_K L = n$ に等しいため、補題 3.2 (巡回ベクトルの存在) より、ある $\alpha \in L$ が存在して、集合

$$\{\alpha, \phi(\alpha), \phi^2(\alpha), \ldots, \phi^{n-1}(\alpha)\}$$

は L の K 上の基底を構成する。これはまさに G による α の軌道であり、 α は正規底を生成する。（証明終）

4. 正規底を用いたGalois対応の証明

正規底の定理を用いることで、Galois対応の基本定理（部分群と中間体の1対1対応および次数の公式）を、群環の構造解析を通じて直接かつ構成的に証明することができる[cite: 1]。

定義 4.1 (固定体)
L/K を Galois 拡大、 $G = \mathrm{Gal}(L/K)$ とする。 G の任意の部分群 $H \subset G$ に対して、 H の作用で不変な L の元の全体

$$L^H = \{x \in L \mid \text{すべての } h \in H \text{ に対して } h(x) = x\}$$

を H の**固定体 (fixed field)** と呼ぶ。 L^H は $K \subset L^H \subset L$ を満たす中間体となる。

定理 4.2 (Galois対応の基本定理の次元公式)
L/K を有限次Galois拡大、 $G = \mathrm{Gal}(L/K)$ とする。 G の任意の部分群 $H \subset G$ に対して、次が成り立つ。

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

証明:
群環 $K[G]$ への H の左作用を考える。 $h \in H$ と $v = \sum_{g \in G} a_g g \in K[G]$ に対し、 $h \cdot v = \sum_{g \in G} a_g (hg)$ である。この作用による固定部分空間を $(K[G])^H = \{v \in K[G] \mid \forall h \in H, h \cdot v = v\}$ とする。

G を H の右剰余類 (right coset) に分解する。 $m = [G : H] = |G|/|H|$ とし、右剰余類の代表元を $g_1, g_2, \ldots, g_m \in G$ とすると、

$$G = \coprod_{i=1}^{m} H g_i$$

と表される。元 $v = \sum_{g \in G} a_g g$ を剰余類ごとに整理すると、

$$v = \sum_{i=1}^{m} \sum_{h' \in H} a_{h' g_i} (h' g_i)$$

となる。任意の $h \in H$ を作用させると、 $hH = H$ より

$$h \cdot v = \sum_{i=1}^{m} \sum_{h' \in H} a_{h' g_i} (h h' g_i)$$

これが常に v と一致するための必要十分条件は、各剰余類 Hg_i 上で係数 a_g が一定であること、すなわちすべての $h', h'' \in H$ に対して $a_{h' g_i} = a_{h'' g_i}$ が成り立つことである。
各剰余類 Hg_i 上の一定の係数を $c_i \in K$ と置くと、 $(K[G])^H$ の任意の元は

$$v = \sum_{i=1}^{m} c_i \left(\sum_{h \in H} h g_i \right)$$

と一意に書ける。元 $\eta_i = \sum_{h \in H} h g_i \in K[G]$ $(1 \le i \le m)$ を定義すると、 $\{\eta_1, \eta_2, \dots, \eta_m\}$ は $(K[G])^H$ の K 上の基底となる。したがって、

$$\dim_K (K[G])^H = m = [G : H] = \frac{|G|}{|H|}$$

である。

定理 3.1 (正規底の定理) より、正規底の生成元 $\alpha \in L$ が存在する。これを用いて定義される K 線形写像

$$\Phi : K[G] \to L, \quad \sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g g(\alpha)$$

は、 $K[G]$ 加群としての全単射同型を与える[cite: 1]。 Φ は G の作用と可換であるため、 H による固定部分空間同士の同型 $(K[G])^H \cong L^H$ を誘導する。
よって、 L^H の K 上のベクトル空間の次元は

$$[L^H : K] = \dim_K L^H = \dim_K (K[G])^H = \frac{|G|}{|H|}$$

である。拡大次数の連鎖律 $[L : K] = [L : L^H][L^H : K]$ および $[L : K] = |G|$ を用いると、

$$[L : L^H] = \frac{[L : K]}{[L^H : K]} = \frac{|G|}{|G|/|H|} = |H|$$

が得られ、主張 1 が示された。

次に主張 2 を示す。 L/K は Galois 拡大であるから、中間体拡大 L/L^H も分離的かつ正規、すなわち Galois 拡大である。したがって $|\mathrm{Gal}(L/L^H)| = [L : L^H] = |H|$ である。
固定体の定義より明らかに $H \subset \mathrm{Gal}(L/L^H)$ である。有限群の包含関係において位数が等しいため、 $\mathrm{Gal}(L/L^H) = H$ が成り立つ。（証明終）

5. 固定体の基底構成アルゴリズムと具体例

前節の証明により、固定体 L^H の K 上の基底は、正規底生成元 $\alpha \in L$ と右剰余類代表元 $g_1, \dots, g_m$ を用いて

$$\beta_i = \Phi(\eta_i) = \sum_{h \in H} (h g_i)(\alpha) \quad (1 \le i \le m)$$

として構成的に得られる[cite: 1]。以下に様々な拡大における計算例を完全に提示する。

例 5.1 (2次拡大：$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$)
$K=\mathbb{Q}$, $L=\mathbb{Q}(\sqrt{2})$ とする。 Galois 群は $G=\{\mathrm{id},\sigma\}$ （ $\sigma(\sqrt{2})=-\sqrt{2}$ ）である。
標準基底 $\{1,\sqrt{2}\}$ に対し、 1 の軌道は $\{1\}$ であり基底をなさない。 $\alpha=1+\sqrt{2}$ をとると、その軌道は $\{1+\sqrt{2},1-\sqrt{2}\}$ となる。

$$c_1(1+\sqrt{2})+c_2(1-\sqrt{2})=(c_1+c_2)+(c_1-c_2)\sqrt{2}=0 \iff c_1+c_2=0 \text{ かつ } c_1-c_2=0 \iff c_1=c_2=0$$

となり、 $\{1+\sqrt{2},1-\sqrt{2}\}$ は $\mathbb{Q}$ 上線形独立で正規底をなす。

例 5.2 (2次拡大：有限体 $\mathbb{F}_4/\mathbb{F}_2$)
$K=\mathbb{F}_2$, $L=\mathbb{F}_4=\mathbb{F}_2(\zeta)$ （ $\zeta^2+\zeta+1=0$ ）とする。 Galois 群は $G=\{\mathrm{id},\phi\}$ （ $\phi(x)=x^2$ ）である。
$\alpha=\zeta$ とおくと、 $\phi(\zeta)=\zeta^2=\zeta+1$ （標数2ゆえ $-1=1$ ）である。
$c_1\zeta+c_2(\zeta+1)=(c_1+c_2)\zeta+c_2=0 \implies c_2=0$ かつ $c_1=0$ であるから、 $\{\zeta,\zeta^2\}$ は $\mathbb{F}_2$ 上の正規底である。

例 5.3 (重2次拡大：$\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$)
$K=\mathbb{Q}$, $L=\mathbb{Q}(\sqrt{2},\sqrt{3})$ とする。 Galois 群は $G=\{\mathrm{id},\sigma,\tau,\sigma\tau\}$ （ Kleinの四元群）であり、作用は

$$\sigma(\sqrt{2})=-\sqrt{2},\ \sigma(\sqrt{3})=\sqrt{3};\quad \tau(\sqrt{2})=\sqrt{2},\ \tau(\sqrt{3})=-\sqrt{3}$$

で定まる。正規底生成元として $\alpha=(1+\sqrt{2})(1+\sqrt{3})=1+\sqrt{2}+\sqrt{3}+\sqrt{6}$ をとる。
部分群 $H=\{\mathrm{id},\sigma\}$ による固定体 L^H の基底を求める。右剰余類分解 $G=H\mathrm{id}\coprod H\tau$ より代表元は $g_1=\mathrm{id}, g_2=\tau$ である。

$$\begin{aligned}\beta_1&=\mathrm{id}(\alpha)+\sigma(\alpha)=(1+\sqrt{2}+\sqrt{3}+\sqrt{6})+(1-\sqrt{2}+\sqrt{3}-\sqrt{6})=2+2\sqrt{3}\\ \beta_2&=\tau(\alpha)+\sigma\tau(\alpha)=(1+\sqrt{2}-\sqrt{3}-\sqrt{6})+(1-\sqrt{2}-\sqrt{3}+\sqrt{6})=2-2\sqrt{3}\end{aligned}$$

得られた $\{2+2\sqrt{3},2-2\sqrt{3}\}$ は $\mathbb{Q}$ 上線形独立であり、固定体 $\mathbb{Q}(\sqrt{3})$ の基底を構成する。

例 5.4 (円分体：$\mathbb{Q}(\zeta_5)/\mathbb{Q}$ と最大実部分体)
$K=\mathbb{Q}$, $L=\mathbb{Q}(\zeta_5)$ （ $\zeta_5=e^{2\pi i/5}$ ）とする。 Galois 群は $G=\{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$ （ $\sigma_k(\zeta_5)=\zeta_5^k$ ）である。
円分多項式 $\Phi_5(X)=X^4+X^3+X^2+X+1$ より、 $\alpha=\zeta_5$ の軌道 $\{\zeta_5,\zeta_5^2,\zeta_5^3,\zeta_5^4\}$ は正規底をなす。
複素共役部分群 $H=\{\sigma_1,\sigma_4\}$ （ Galois群の位数2の部分群）の固定体の基底を求める。右剰余類分解 $G=H\sigma_1\coprod H\sigma_2$ より代表元は $g_1=\sigma_1, g_2=\sigma_2$ である。

$$\begin{aligned}\beta_1&=\sigma_1(\zeta_5)+\sigma_4(\zeta_5)=\zeta_5+\zeta_5^4=2\cos\left(\frac{2\pi}{5}\right)\\ \beta_2&=\sigma_2(\zeta_5)+\sigma_4(\sigma_2(\zeta_5))=\zeta_5^2+\zeta_5^3=2\cos\left(\frac{4\pi}{5}\right)\end{aligned}$$

$\beta_1+\beta_2=-1$, $\beta_1\beta_2=-1$ より、これらは $X^2+X-1=0$ の根 $\frac{-1\pm\sqrt{5}}{2}$ であり、最大実部分体 $\mathbb{Q}(\sqrt{5})$ の基底を与える。

例 5.5 (有限体の拡大：$\mathbb{F}_{16}/\mathbb{F}_2$)
$K=\mathbb{F}_2$, $L=\mathbb{F}_{16}=\mathbb{F}_2(\alpha)$ （ $\alpha^4+\alpha+1=0$ ）とする。 Galois 群は Frobenius 自我同型 $\phi(x)=x^2$ による $G=\{\mathrm{id},\phi,\phi^2,\phi^3\}$ である。
$\beta=\alpha^3$ とおくと、その軌道は $\{\alpha^3,\alpha^3+\alpha^2,\alpha^3+\alpha^2+\alpha+1,\alpha^3+\alpha\}$ となり、これらは $\mathbb{F}_2$ 上線形独立で正規底を構成する。

部分群 $H = \{\mathrm{id}, \phi^2\}$ による固定体 $L^H = \mathbb{F}_4$ の基底を求める。右剰余類分解 $G = H\mathrm{id} \coprod H\phi$ より、

$$\gamma_1 = \mathrm{id}(\beta) + \phi^2(\beta) = \alpha^3 + (\alpha^3 + \alpha^2 + \alpha + 1) = \alpha^2 + \alpha + 1$$
$$\gamma_2 = \phi(\beta) + \phi^3(\beta) = (\alpha^3 + \alpha^2) + (\alpha^3 + \alpha) = \alpha^2 + \alpha$$

が得られる。 $\phi^2(\gamma_2) = (\alpha+1)^2 + (\alpha+1) = \alpha^2 + \alpha = \gamma_2$ より確かに $\mathbb{F}_4$ に属し、基底をなす。

例 5.6 (非Abel Galois拡大： 3次対称群 S_3 の場合)
$K = \mathbb{Q}$, $L = \mathbb{Q}(\rho, \omega)$ （ $\rho = \sqrt[3]{2}, \omega = e^{2\pi i/3}$ ）とする。 L/K は多項式 $X^3 - 2$ の最小分解体であり、 Galois 群 $G = \mathrm{Gal}(L/\mathbb{Q}) \cong S_3$ は

$$\sigma(\rho) = \rho\omega,\ \sigma(\omega) = \omega; \quad \tau(\rho) = \rho,\ \tau(\omega) = \omega^2$$

で生成される。 $G = \{\mathrm{id}, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$ である。

正規底の独立性の検証:
$\alpha = \omega(1 + \rho + \rho^2) = \omega + \rho\omega + \rho^2\omega$ とおく。 G による6個の共役元を標準基底 $\{1, \omega, \rho, \rho\omega, \rho^2, \rho^2\omega\}$ の各成分ベクトルとして行列に並べると、

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & -1 \\ -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & 0 & 1 & 1 & 0 \\ -1 & -1 & 1 & 0 & -1 & -1 \end{pmatrix}$$

となり、この行列式を計算すると非零（値は 81 ）となる。したがって $\{g(\alpha) \mid g \in G\}$ は $\mathbb{Q}$ 上線形独立であり、正規底をなす。

非正規部分群 $H = \langle\tau\rangle = \{\mathrm{id}, \tau\}$ の固定体 $\mathbb{Q}(\sqrt[3]{2})$ の基底計算:
右剰余類分解 $G = H\mathrm{id} \coprod H\sigma \coprod H\sigma^2$ の代表元 $g_1 = \mathrm{id}, g_2 = \sigma, g_3 = \sigma^2$ を用いる。

$$\beta_1 = \mathrm{id}(\alpha) + \tau(\alpha) = (\omega + \rho\omega + \rho^2\omega) + (\omega^2 + \rho\omega^2 + \rho^2\omega^2) = -1 - \rho - \rho^2$$
$$\beta_2 = \sigma(\alpha) + \tau\sigma(\alpha) = (\omega + \rho\omega^2 + \rho^2) + (\omega^2 + \rho\omega + \rho^2) = -1 - \rho + 2\rho^2$$
$$\beta_3 = \sigma^2(\alpha) + \tau\sigma^2(\alpha) = (\omega + \rho + \rho^2\omega^2) + (\omega^2 + \rho + \rho^2\omega) = -1 + 2\rho - \rho^2$$

これらは線形独立であり、固定体 $L^H = \mathbb{Q}(\sqrt[3]{2})$ の基底を構成する。

正規部分群 $N = \langle\sigma\rangle = \{\mathrm{id}, \sigma, \sigma^2\}$ の固定体 $\mathbb{Q}(\omega)$ の基底計算:
右剰余類分解 $G = N\mathrm{id} \coprod N\tau$ より代表元 $g_1 = \mathrm{id}, g_2 = \tau$ を用いる。 $N \triangleleft G$ より $N\tau = \tau N$ である。

$$\gamma_1 = \mathrm{id}(\alpha) + \sigma(\alpha) + \sigma^2(\alpha) = 3\omega$$
$$\gamma_2 = \tau(\alpha) + \sigma\tau(\alpha) + \sigma^2\tau(\alpha) = \tau(\gamma_1) = 3\omega^2 = -3 - 3\omega$$

これらは固定体 $L^N = \mathbb{Q}(\omega)$ の $\mathbb{Q}$ 上の基底を構成する。

参考文献

- [1] Lang, Serge. *Algebra*. Revised Third Edition, Graduate Texts in Mathematics, Vol. 211, Springer-Verlag, New York, 2002. https://link.springer.com/book/10.1007/978-1-4613-0041-0

- [2] Milne, James S. *Fields and Galois Theory* (v5.10). Course Notes, 2022. https://www.jmilne.org/math/CourseNotes/ft.html
- [3] Dummit, David S., and Foote, Richard M. *Abstract Algebra*. 3rd Edition, John Wiley & Sons, Inc., Hoboken, NJ, 2004.
- [4] Artin, Emil. *Galois Theory*. Second Edition, Notre Dame Mathematical Lectures, No. 2, University of Notre Dame, 1944.