Artinの定理を経由するGaloisの基本定理の証明

体のGalois拡大とGaloisの基本定理について、Artinの定理を経由するアプローチで詳細に解説します。Galois理論の目的は、体の拡大という代数的な対象を、Galois群という群論的な対象に翻訳して調べることです。この対応関係を確立するGaloisの基本定理を、Artinの定理を用いて鮮やかに証明してみましょう。そのための準備として、関連する基本概念の定義と、Dedekindの補題から始めます。

1. 基本概念の定義と例

定義 1.1 (体の拡大と自己同型群)

体 (field) L が体 K を部分体として含むとき、L を K の拡大体 (extension field) といい、L/K と表す。このとき L は自然に K 上のベクトル空間となる。その次元を拡大次数 (degree of extension) と呼び、$[L:K]$ で表す。$[L:K]$ が有限のとき有限次拡大 (finite extension) と呼ぶ。

体 L の自己同型 (automorphism) 全体のなす群を $\mathrm{Aut}(L)$ と書く。部分体 K の元を全て固定する自己同型のなす部分群を $\mathrm{Aut}(L/K)$ または $\mathrm{Gal}(L/K)$ と書き、L/K のGalois群 (Galois group) と呼ぶ。

有限群 $G \subset \mathrm{Aut}(L)$ に対して、G の全ての元で固定される L の元の集合を L^G と書き、G の不変体 (fixed field) と呼ぶ。

次に、Galois拡大を定義するために必要不可欠な「分離性」と「正規性」について定義します。

定義 1.2 (分離性と正規性、およびGalois拡大)

体 K 上の代数的な元 α に対して、α を根に持つ K 係数のモニック多項式のうち次数が最小のものを α の K 上の最小多項式 (minimal polynomial) と呼ぶ。

- **分離的 (separable):** 元 α の K 上の最小多項式が、代数閉包において重根を持たないとき、α は K 上分離的であるという。代数拡大 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) と呼ぶ。
- **正規 (normal):** 代数拡大 L/K について、K 上の任意の既約多項式が L に根を持つならば、その多項式が L 上で一次式の積に完全に分解されるとき、L/K を正規拡大 (normal extension) と呼ぶ。
- **Galois拡大 (Galois extension):** 有限次拡大 L/K が分離拡大かつ正規拡大であるとき、これを有限次Galois拡大と呼ぶ。

命題 1.3 (Galois群の共役元への推移的作用)

L/K が有限次Galois拡大であるとする。任意の $\alpha \in L$ と、α の K 上での任意の共役元 $\beta \in L$（すなわち α の K 上の最小多項式の根）に対して、ある $\sigma \in \mathrm{Gal}(L/K)$ が存在して $\sigma(\alpha) = \beta$ となる。

証明.

L/K は有限次分離拡大であるから、原始元定理により $L = K(\theta)$ となる元 $\theta \in L$ が存在する。
α と β は K 上共役であるため同じ最小多項式 $p(x) \in K[x]$ を持ち、$\alpha \mapsto \beta$ と写し K の元を固定する同型写像 $\phi : K(\alpha) \xrightarrow{\sim} K(\beta)$ が存在する。
ここで、θ の $K(\alpha)$ 上の最小多項式を $h_1(x) \in K(\alpha)[x]$ とする。同型写像 ϕ によって $h_1(x)$ の各係数を $K(\beta)$ の元に写して得られる多項式を $h_2(x) \in K(\beta)[x]$ とおく。
θ の K 上の最小多項式 $F(x) \in K[x]$ を考えると、$F(\theta) = 0$ であるため、$h_1(x)$ は $K(\alpha)[x]$ において $F(x)$ の約数である（$F(x) = h_1(x)q_1(x)$）。 $F(x)$ の係数は K に属するため ϕ によって不変であり、したがって $h_2(x)$ も $K(\beta)[x]$ において $F(x)$ の約数となる。
さて、L/K は正規拡大であるため、K 上の多項式 $F(x)$ は L 内で一次式に完全に分解する。よってその約数である $h_2(x)$ も L 内に根を持つ。その根の一つを $\theta' \in L$ とする。
多項式環の剰余環としての単拡大の構成定理より、以下の自然な同型の連鎖が得られる。

$$L = K(\alpha)(\theta) \cong K(\alpha)[x]/(h_1(x)) \xrightarrow{\tilde{\phi}} K(\beta)[x]/(h_2(x)) \cong K(\beta)(\theta')$$

ここで $\tilde{\phi}$ は ϕ から自然に誘導された同型写像である。
$\theta' \in L$ ゆえ $K(\beta)(\theta') \subseteq L$ であり、上の同型によって $[K(\beta)(\theta') : K] = [L : K]$ であるから、$K(\beta)(\theta') = L$ となる。
この連鎖を合成して得られる同型写像 $\sigma : L \xrightarrow{\sim} L$ は、K の元を固定し、θ を θ' に、そして α を $\phi(\alpha) = \beta$ に写す。したがって、σ は L の K-自己同型（すなわち $\sigma \in \mathrm{Gal}(L/K)$）であり、$\sigma(\alpha) = \beta$ を満たす。（証明終）

例 1.4 (複素数体と実数体の拡大)

複素数体 $\mathbb{C}$ と実数体 $\mathbb{R}$ の拡大 $\mathbb{C}/\mathbb{R}$ を考える。$\mathbb{C}$ の任意の元 $a + bi$ の $\mathbb{R}$ 上の最小多項式は高々2次であり、虚数部がゼロでなければ $(x - (a + bi))(x - (a - bi)) = x^2 - 2ax + a^2 + b^2$ となる。これは重根を持たず（分離的）、かつ $\mathbb{C}$ 上で完全に一次式に分解される（正規）。したがって $\mathbb{C}/\mathbb{R}$ はGalois拡大である。
$\mathbb{C}$ 上の自己同型で $\mathbb{R}$ を固定するものは、恒等写像 id と複素共役 $\sigma(a + bi) = a - bi$ のみである。したがって $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \sigma\}$ であり、不変体 $\mathbb{C}^{\{\mathrm{id},\sigma\}}$ は $\mathbb{R}$ に一致する。

2. Dedekindの補題と準備の補題

補題 2.1

体 Ω 上のベクトル空間 V の $v_1, \ldots, v_n \in V$ で張られる部分空間を W と書く。$i \neq j$ に対して W の一次変換 T_{ij} が与えられており、各 v_k は非ゼロベクトルであり、固有値 λ_k^{ij} を持つ T_{ij} の固有ベクトルであって、$\lambda_i^{ij} \neq \lambda_j^{ij}$ を満たしているとする。このとき以下が成立している。
(1) $i = 1, \ldots, n$ に対して W の一次変換 L_i を

$$L_i = \prod_{j \in \{1,\ldots,n\} \setminus \{i\}} \frac{T_{ij} - \lambda_j^{ij} \mathrm{id}_W}{\lambda_i^{ij} - \lambda_j^{ij}}$$

と定めると、$L_i v_j = \delta_{ij} v_i \quad (i, j = 1, \ldots, n)$ である。ここで δ_{ij} はKroneckerのデルタである。
(2) $v_1, \ldots, v_n$ は Ω 上一次独立 (linearly independent) である。

補題 2.1 の証明.

(1) 任意の $k \in \{1, \dots, n\}$ に対して $L_i v_k$ を計算する。$T_{ij} v_k = \lambda_k^{ij} v_k$ より、$(T_{ij} - \lambda_j^{ij} \mathrm{id}_W) v_k = (\lambda_k^{ij} - \lambda_j^{ij}) v_k$ である。 もし $k \neq i$ ならば、積 L_i の因子の中に $j = k$ となる項 $\frac{T_{ik} - \lambda_k^{ik} \mathrm{id}_W}{\lambda_i^{ik} - \lambda_k^{ik}}$ が存在する。この因子を v_k に作用させると、分子が $(\lambda_k^{ik} - \lambda_k^{ik}) v_k = 0$ となるため、$L_i v_k = 0$ である。 一方 $k = i$ の場合、すべての $j \neq i$ に対して分子は $(\lambda_i^{ij} - \lambda_j^{ij}) v_i$ となり、分母と完全に相殺される。したがって $L_i v_i = v_i$ である。 以上より $L_i v_j = \delta_{ij} v_i \quad (i, j = 1, \dots, n)$ が示された。

(2) Ω の元 $c_1, \dots, c_n$ を用いて $\sum_{j=1}^n c_j v_j = 0$ と表されているとする。この両辺に (1) で構成した L_i を作用させると、

$$L_i \left(\sum_{j=1}^n c_j v_j \right) = \sum_{j=1}^n c_j L_i v_j = c_i v_i = 0$$

となる。仮定より $v_i \neq 0$ であるから、$c_i = 0$ を得る。これが任意の $i = 1, \dots, n$ で成り立つため、$v_1, \dots, v_n$ は Ω 上一次独立である。（証明終）

定理 2.2 (Dedekindの補題)

半群 (semigroup) H から体 Ω への相異なる半群準同型 $\sigma_1, \dots, \sigma_n : H \to \Omega^\times$ は、H 上の Ω に値を持つ関数達として一次独立である。ただし $\Omega^\times = \Omega \setminus \{0\}$ は乗法群である。

Dedekindの補題の証明.

V を H から Ω への写像全体のなす Ω 上のベクトル空間とし、$v_k = \sigma_k \in V$ とおく。これらはゼロ写像ではないので非ゼロベクトルである。W を $v_1, \dots, v_n$ で張られる部分空間とする。 $\sigma_1, \dots, \sigma_n$ は相異なるので、任意の $i \neq j$ に対して、ある $h_{ij} \in H$ が存在して $\sigma_i(h_{ij}) \neq \sigma_j(h_{ij})$ を満たす。 W 上の一次変換 T_{ij} を、$(T_{ij} f)(x) = f(h_{ij} x)$ によって定義する。H は半群であるため $h_{ij} x \in H$ となり、この一次変換は well-defined である。 $v_k = \sigma_k$ に対して T_{ij} を作用させると、準同型の性質から

$$(T_{ij} \sigma_k)(x) = \sigma_k(h_{ij} x) = \sigma_k(h_{ij}) \sigma_k(x)$$

となる。すなわち $T_{ij} v_k = \sigma_k(h_{ij}) v_k$ であり、v_k は固有値 $\lambda_k^{ij} = \sigma_k(h_{ij})$ を持つ固有ベクトルである。 h_{ij} の選び方から $\lambda_i^{ij} = \sigma_i(h_{ij}) \neq \sigma_j(h_{ij}) = \lambda_j^{ij}$ が成り立つ。 したがって先の補題 2.1 の条件がすべて満たされるため、(2) より $v_1, \dots, v_n$ すなわち $\sigma_1, \dots, \sigma_n$ は Ω 上一次独立である。（証明終）

注意 (体の準同型とDedekindの補題)

体 L から体 Ω への体の準同型は、積の構造を保つため、L の乗法群 $H = L^\times$ から Ω の乗法群 $\Omega^\times$ への半群準同型を与えます（もちろん群準同型でもあります）。したがって、体 L から体 Ω への相異なる体の準同型たちは、Dedekindの補題によって、直ちに関数達として Ω 上一次独立であることが従います。

3. トレース写像の非退化性

命題 3.1

体 L とその自己同型の有限群 $G = \{\sigma_1, \dots, \sigma_n\}$、および不変体 $K = L^G$ を考える。トレース写像 $\mathrm{Tr}_{L/K} : L \to K$

を $\mathrm{Tr}_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x)$ で定義する。この写像が K 上の線形写像（K-linear map）であることは、各 σ_i が体同型であり K の元を固定することから従う。このとき、すべての $y \in L$ について $\mathrm{Tr}_{L/K}(xy) = 0$ となる $x \in L$ は $x = 0$ しかない。

証明.

ある $x \in L$ が存在して、すべての $y \in L$ に対して $\mathrm{Tr}_{L/K}(xy) = 0$ が成り立つと仮定する。このとき、自己同型の性質より

$$\mathrm{Tr}_{L/K}(xy) = \sum_{i=1}^{n} \sigma_i(xy) = \sum_{i=1}^{n} \sigma_i(x)\sigma_i(y) = 0$$

が任意の $y \in L$ について成り立つ。これは L の自己同型写像 $\sigma_1, \ldots, \sigma_n$ を乗法群 $H = L^{\times}$ 上の関数とみなしたとき、関数としての一次関係式 $\sum_{i=1}^{n} \sigma_i(x)\sigma_i = 0$ が成り立つことを意味する。 Dedekindの補題より、$\sigma_1, \ldots, \sigma_n$ は $L^{\times}$ 上の L に値を持つ関数達として一次独立である。したがって、すべての係数がゼロでなければならないため、各 i に対して $\sigma_i(x) = 0$ となる。 σ_i は同型写像であるから、これを満たすのは $x = 0$ のみである。したがって、条件を満たす x は 0 に限られる。（証明終）

4. Artinの定理の証明

定理 4.1 (Artinの定理)

体 L とその自己同型の位数 n の有限群 G、および不変体 $K = L^G$ を考える。このとき $[L : K] = n$ であり、L/K はGalois拡大である。さらに $G = \mathrm{Gal}(L/K)$ となる。

証明.

(1) まず $\dim_L \mathrm{End}_K(L) = [L : K]$ を示す。 $\mathrm{End}_K(L)$ は、K 上のベクトル空間 L の自己準同型全体のなす環であり、K だけでなく L 上のベクトル空間としても自然にみなせる（L の元を左から掛ける作用により）。 もし $[L : K] = m < \infty$ ならば、$\mathrm{End}_K(L)$ は K 上の $m \times m$ 行列環と同型であり、その K 上の次元は m^2 である。L の K 上の次元が m であるため、$\mathrm{End}_K(L)$ の L 上の次元は $m^2/m = m = [L : K]$ となる。 もし $[L : K] = \infty$ ならば、$\dim_L \mathrm{End}_K(L) = \infty$ となり、等式は成立する。

(2) 自然な写像 $\Phi : L[G] \to \mathrm{End}_K(L)$ が同型になることを示す。 G を基底とする L 上のベクトル空間を考え、その元 $\sum_{\sigma \in G} a_\sigma \sigma$ ($a_\sigma \in L$) に対して積を

$$(a\sigma)(b\tau) = a\sigma(b)\sigma\tau \quad (a, b \in L, \sigma, \tau \in G)$$

で定義する。これにより得られる単位元 1 を持つ結合代数（接合環 (crossed product) と呼ばれる）を $L[G]$ と書く。 写像 $\Phi : L[G] \to \mathrm{End}_K(L)$ を、$\Phi(\sum_{\sigma \in G} a_\sigma \sigma)(x) = \sum_{\sigma \in G} a_\sigma \sigma(x)$ によって定義する。

- **Φ が1を持つ結合代数の準同型であること：**
  任意の $x \in L$ に対して、$\Phi((a\sigma)(b\tau))(x) = \Phi(a\sigma(b)\sigma\tau)(x) = a\sigma(b)\sigma(\tau(x))$ となる。 一方、
  $\Phi(a\sigma)(\Phi(b\tau)(x)) = \Phi(a\sigma)(b\tau(x)) = a\sigma(b\tau(x)) = a\sigma(b)\sigma(\tau(x))$ となる。 したがって
  $\Phi((a\sigma)(b\tau)) = \Phi(a\sigma) \circ \Phi(b\tau)$ が成り立つ。単位元が保たれることも明らかであるため、Φ は準同型である。
- **Φ が単射であること：**
  $\Phi(\sum_{\sigma \in G} a_\sigma \sigma) = 0$ と仮定する。これは任意の $x \in L$ に対して $\sum_{\sigma \in G} a_\sigma \sigma(x) = 0$ を意味する。 Dedekindの補題

より、相異なる自己同型 $\sigma \in G$ たちは L 上一次独立である。したがって全ての $\sigma \in G$ について $a_\sigma = 0$ となり、Φ は単射である。

- **Φ が全射であることをGalois降下 (Galois descent) で示す：**
  写像 $\Psi : L \otimes_K L \to \mathrm{End}_K(L)$ を、$\Psi(a \otimes b)(x) = a\mathrm{Tr}_{L/K}(bx)$ によって定義する。 任意の $b \in L$ に対して $\mathrm{Tr}_{L/K}(bx) = \sum_{\sigma \in G} \sigma(bx) = \sum_{\sigma \in G} \sigma(b)\sigma(x)$ であるから、

$$\Psi(a \otimes b) = a \sum_{\sigma \in G} \sigma(b)\sigma \in \Phi(L[G])$$

  となる。したがって $\mathrm{Im}(\Psi) \subset \mathrm{Im}(\Phi)$ である。
  次に Ψ が単射であることを示す。$\sum_{i=1}^r a_i \otimes b_i \in \ker(\Psi)$ とし、$\{a_1, \ldots, a_r\}$ を K 上一次独立な L の元の集合として選ぶ。 任意の $x \in L$ に対して $\Psi(\sum_{i=1}^r a_i \otimes b_i)(x) = \sum_{i=1}^r a_i \mathrm{Tr}_{L/K}(b_i x) = 0$ となる。
  $\mathrm{Tr}_{L/K}(b_i x) \in K$ であり、a_i は K 上一次独立であるから、各 i に対して $\mathrm{Tr}_{L/K}(b_i x) = 0$ である。
  これが任意の $x \in L$ で成り立つため、トレース写像の非退化性より $b_i = 0$ である。よって Ψ は単射である。
  Ψ は左 L ベクトル空間としての単射準同型である。$L \otimes_K L$ の L 上の次元は $\dim_K L = [L : K]$ であり、(1) より $\mathrm{End}_K(L)$ の L 上の次元も $[L : K]$ である。次元が一致するため Ψ は全射（同型）である。 結果として、$\mathrm{End}_K(L) = \mathrm{Im}(\Psi) \subset \mathrm{Im}(\Phi) \subset \mathrm{End}_K(L)$ となり、Φ は全射であることが示された。

以上より $\Phi : L[G] \to \mathrm{End}_K(L)$ は同型写像である。
$L[G]$ の L 上の次元は基底 G の元の個数 $|G| = n$ である。一方 $\mathrm{End}_K(L)$ の L 上の次元は $[L : K]$ である。同型写像で次元が保たれるため、$[L : K] = n$ を得る。

(3) 最後に、L/K が分離的かつ正規拡大であることを示す。
任意の $\alpha \in L$ をとる。G の元によって α が移る先の要素の集合（軌道）を $\{\alpha_1, \ldots, \alpha_r\}$ とし（ただし $\alpha_1 = \alpha$ とする）、これらは互いに相異なるとする。 多項式 $f(x) = \prod_{i=1}^r (x - \alpha_i)$ を考える。G の任意の元 σ は根 $\{\alpha_1, \ldots, \alpha_r\}$ を並べ替えるだけなので、多項式 $f(x)$ の係数は G によってすべて固定される。 $K = L^G$ であるから、$f(x)$ の係数は K に属する。すなわち、$f(x) \in K[x]$ である。 α は $f(x)$ の根であるため、α の K 上の最小多項式 $p(x)$ は $f(x)$ を割り切る。 $f(x)$ の根は構成上すべて相異なり、かつすべて L に属している。したがってその約数である $p(x)$ も重根を持たず（分離的）、L において一次式の積に完全に分解される（正規）。 α は L の任意の元であったため、L/K は分離的かつ正規拡大であり、すなわち定義よりGalois拡大である。 $G \subset \mathrm{Gal}(L/K)$ は明らかであり、位数の比較から $[L : K] = n = |G| \leq |\mathrm{Gal}(L/K)| \leq [L : K]$ となるため、$G = \mathrm{Gal}(L/K)$ も成立する。（証明終）

5. Galoisの基本定理の証明

ここで、Galois対応の美しさを視覚的に捉えるために、基本定理の構造を思い浮かべてみましょう。体拡大の中間体は上にいくほど大きく、対応するGalois群の部分群は下にいくほど大きくなります。この反変的な対応関係が、一対一に結びつくのです。

定理 5.1 (Galoisの基本定理)

L/K を有限次Galois拡大とし、$G = \mathrm{Gal}(L/K)$ とする。このとき、L/K の中間体 M ($K \subset M \subset L$) 全体の集合と、G の部分群 H 全体の集合との間に、全単射（Galois対応 (Galois correspondence)）が存在する。対応は以下で与えられる。

$$\alpha(M) = \mathrm{Gal}(L/M)$$

$$\beta(H) = L^H$$

証明.

まず、定義から容易に導かれる包含関係の片側を示す。

1. $M \subset \beta(\alpha(M))$ **の証明：**
   $\alpha(M) = \mathrm{Gal}(L/M)$ は、定義により M の元を全て固定する L の自己同型のなす群である。したがって、任意の $x \in M$ は $\mathrm{Gal}(L/M)$ の全ての元によって固定される。これは $x \in L^{\mathrm{Gal}(L/M)} = \beta(\alpha(M))$ を意味する。よって $M \subset \beta(\alpha(M))$ である。
2. $H \subset \alpha(\beta(H))$ **の証明：**
   $\beta(H) = L^H$ は、H の全ての元によって固定される L の元の集合である。したがって、H の任意の元 σ は L^H の全ての元を固定するため、σ は $\mathrm{Gal}(L/L^H)$ に属する。すなわち $\sigma \in \alpha(\beta(H))$ であり、$H \subset \alpha(\beta(H))$ を得る。

次に、Artinの定理を用いて逆向きの包含関係（等号）を証明する。

- $H = \alpha(\beta(H))$ **の証明：**
  H を G の任意の部分群とし、不変体 $M' = \beta(H) = L^H$ を考える。 Artinの定理を体 L と自己同型の部分群 H に対して適用すると、L の L^H 上の拡大次数は $[L : L^H] = |H|$ であり、L/L^H は分離的かつ正規拡大、すなわちGalois拡大となる。 Artinの定理の帰結より $\mathrm{Gal}(L/L^H) = H$ が成り立つ。すなわち $\alpha(\beta(H)) = H$ である。
- $M = \beta(\alpha(M))$ **の証明：**
  $M' = \beta(\alpha(M))$ とおく。定義より $M \subset M'$ は明らかである。
  すでに証明した $H = \alpha(\beta(H))$ において、$H = \alpha(M)$ を代入すると、$\alpha(\beta(\alpha(M))) = \alpha(M)$ となる。すなわち $\alpha(M') = \alpha(M)$ であり、M を固定する自己同型群と M' を固定する自己同型群は完全に一致する。
  ここで、もし $M \subsetneq M'$ ならば、ある元 $\gamma \in M' \setminus M$ が存在する。 L/K は分離的かつ正規拡大であるため、その中間体 M 上の拡大 L/M もまた有限次Galois拡大（分離的正規拡大）である。 したがって、γ の M 上の最小多項式 $p(x)$ は分離的であり、L 内にすべての根を持つ。$\gamma \notin M$ より $\deg p \geq 2$ であるから、$p(x)$ は γ と異なる共役元 $\gamma' \in L$ を持つ。 ここで、**命題 1.3** を M 上のGalois拡大 L/M に適用すると、根 γ を共役元 γ' に移す L の M-自己同型 $\sigma \in \mathrm{Gal}(L/M) = \alpha(M)$ が存在する。 しかし $\alpha(M) = \alpha(M')$ であるため、σ は M' の元である γ を必ず固定しなければならず、$\sigma(\gamma) = \gamma$ となる。 これは $\sigma(\gamma) = \gamma' \neq \gamma$ に矛盾する。 したがって $M = M' = \beta(\alpha(M))$ である。

以上により、α と β は互いに逆写像であり、一対一の対応を与える。（証明終）

このように、Dedekindの補題から出発し、トレース写像の非退化性を利用したGalois降下で接合環の同型（Artinの定理）を導くことで、不変体に対する体の拡大が分離的かつ正規なGalois拡大になることが鮮やかに示されます。そしてそのArtinの定理から得られる $H = \alpha(\beta(H))$ という関係を巧みに適用し、分離的正規拡大の基本的な性質を用いることで、Galoisの基本定理における逆向きの包含関係が拡大次数の計算なしに自然に証明されるのです。代数学の構築美を感じられる素晴らしい証明ですね。

参考文献

Artin, E. (1971). *Galois Theory: Lectures Delivered at the University of Notre Dame* (Notre Dame Mathematical Lectures, Number 2). Project Euclid. https://projecteuclid.org/ebooks/notre-dame-mathematical-lectures/Galois-Theory/toc/ndml/1175197041

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