無限次ガロア理論と有限体の絶対ガロア群

1. 諸定義の準備

定義1：ガロア拡大

体拡大 L/K が代数拡大であり、かつ**正規拡大**（K 係数の既約多項式が L に根を持てば、L 上で完全に一次式に分解される）かつ**分離拡大**（すべての元の最小多項式が重根を持たない）であるとき、L/K をガロア拡大という。

定義2：代数閉包 (Algebraic Closure)

体 K の代数拡大 $\bar{K}$ であり、$\bar{K}$ 上の任意の定数でない多項式が $\bar{K}$ 内に根を持つ（代数的に閉じている）とき、$\bar{K}$ を K の代数閉包と呼ぶ。

定義3：射影極限（逆極限）とプロ有限群

半順序集合 I によって添字付けられた位相群の族 $\{G_i\}_{i\in I}$ と、$i \leq j$ に対して連続な準同型（制限写像） $\phi_{ji} : G_j \to G_i$ が存在し、$\phi_{ii} = \mathrm{id}$ かつ $\phi_{ki} = \phi_{ji} \circ \phi_{kj}$ が成り立つとする（逆系）。このとき、直積空間 $\prod_{i\in I} G_i$ の部分群として射影極限を次のように定義する：

$$\varprojlim_{i\in I} G_i = \left\{ (g_i)_{i\in I} \in \prod_{i\in I} G_i \quad \forall i \leq j, \phi_{ji}(g_j) = g_i \right\}$$

各 G_i が有限群（離散位相）であるとき、その射影極限として得られる位相群を**プロ有限群 (Profinite group)** と呼ぶ。

定義4：クルル位相 (Krull Topology)

無限次ガロア拡大 L/K のガロア群 $G = \mathrm{Gal}(L/K)$ に対し、L/K の有限次ガロア部分拡大 N をすべて取る。写像 $G \to \prod \mathrm{Gal}(N/K), \sigma \mapsto (\sigma|_N)$ による G の像に、直積空間の相対位相を入れたものをクルル位相と呼ぶ。これにより G はコンパクトかつ全不連結なハウスドルフ位相群（プロ有限群）となる。

2. 有限体の絶対ガロア群

有限体 k（要素数 q）とその代数閉包 $\bar{k}$ について、絶対ガロア群 $\mathrm{Gal}(\bar{k}/k)$ を決定する。

定理：有限体の絶対ガロア群

$$\mathrm{Gal}(\bar{k}/k) \cong \hat{\mathbb{Z}} = \varprojlim_{n} \mathbb{Z}/n\mathbb{Z}$$

証明

1. k の任意の有限次拡大は一意に定まり、その次数を n とすると拡大体 $k_n \cong \mathbb{F}_{q^n}$ となる。この拡大はガロア拡大であり、ガロア群 $\mathrm{Gal}(k_n/k)$ はフロベニウス自己同型 $\varphi_n : x \mapsto x^q$ によって生成される位数 n の巡回群である。
したがって、同型 $\mathrm{Gal}(k_n/k) \cong \mathbb{Z}/n\mathbb{Z}$ が $\varphi_n \leftrightarrow 1 \pmod{n}$ によって定まる。

2. 無限次ガロア拡大の理論により、$\mathrm{Gal}(\bar{k}/k) \cong \varprojlim_{n} \mathrm{Gal}(k_n/k)$ である。極限は $n \mid m$ となる体の包含 $k_n \subset k_m$ に対する制限写像で与えられる。

3. 制限写像 $\mathrm{Res}_{m,n} : \mathrm{Gal}(k_m/k) \to \mathrm{Gal}(k_n/k)$ について、k_m 上のフロベニウス写像 φ_m を k_n に制限すると k_n 上のフロベニウス写像 φ_n に一致する。これは $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, a \pmod{m} \mapsto a \pmod{n}$ という自然な射影に完全に対応する。

4. したがって、プロ有限整数群 $\hat{\mathbb{Z}}$ の定義そのものにより、

$$\mathrm{Gal}(\bar{k}/k) \cong \varprojlim_{n} \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$$

が成り立つ。（証明終）

3. 補題の証明

無限次ガロア理論の主定理を証明するために不可欠な2つの補題を示す。

補題A：自己同型の延長（ツォルンの補題の応用）

L/M を代数拡大とする。$\alpha, \beta \in L$ が M 上で同じ最小多項式を持つとき、M 上の同型写像 $\tau : M(\alpha) \to M(\beta)$ ($\tau(\alpha) = \beta$) は、L から L の中へのある埋め込み $\sigma : L \to \bar{L}$ に延長できる。特に L/M が正規拡大であれば σ は L 上の自己同型 $\sigma \in \mathrm{Gal}(L/M)$ となる。

補題Aの証明

集合 S を、「L の部分体 E ($M(\alpha) \subset E \subset L$) と、$\tau$ の延長となる埋め込み $\sigma_E : E \to \bar{L}$ の組 (E, σ_E) 全体」とする。S に順序を「延長関係」で入れる。任意の全順序部分集合に対し、それらの和集合を取ることで上界が存在する。ツォルンの補題より S には極大元 (E_{max}, σ_{max}) が存在する。
もし $E_{max} \neq L$ ならば、$x \in L \setminus E_{max}$ が存在する。L/M は代数拡大なので x は E_{max} 上代数的である。代数拡大の基本性質より σ_{max} は x を添加した体 $E_{max}(x)$ まで延長でき、極大性に矛盾する。よって $E_{max} = L$ である。L/M が正規であれば埋め込みの像は L 自身となり、自己同型となる。（証明終）

補題B：正規部分群とガロア拡大

L/K をガロア拡大、M を中間体とする。M/K がガロア拡大であることと、$\mathrm{Gal}(L/M)$ が $\mathrm{Gal}(L/K)$ の正規部分群であることは同値である。

補題Bの証明

任意の $\sigma \in \mathrm{Gal}(L/K)$ と $\tau \in \mathrm{Gal}(L/\sigma(M))$ に対して、$\sigma^{-1}\tau\sigma$ は M の元を固定するため、$\sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/M)$ すなわち $\tau \in \sigma\mathrm{Gal}(L/M)\sigma^{-1}$ となる。逆も同様に示せるため、

$$\mathrm{Gal}(L/\sigma(M)) = \sigma\mathrm{Gal}(L/M)\sigma^{-1}$$

が成り立つ。
M/K が正規拡大（ガロア拡大）である必要十分条件は、任意の $\sigma \in \mathrm{Gal}(L/K)$ に対して $\sigma(M) = M$ となることである。上の式より、これは $\mathrm{Gal}(L/M) = \sigma\mathrm{Gal}(L/M)\sigma^{-1}$、すなわち $\mathrm{Gal}(L/M)$ が正規部分群であることと同値である。（証明終）

4. クルルのガロア理論（主定理）

無限次ガロア拡大の主定理

L/K をガロア拡大とし、$G = \mathrm{Gal}(L/K)$ にクルル位相を入れる。
1. 中間体 M 全体と、G の**閉部分群** H 全体の間に包含関係を反転させる全単射 $M \mapsto \mathrm{Gal}(L/M), H \mapsto L^H$ が存在する。
2. M/K がガロア拡大 $\iff$ $\mathrm{Gal}(L/M)$ が G の正規部分群。このとき位相同型 $\mathrm{Gal}(M/K) \cong G/\mathrm{Gal}(L/M)$ が成り立つ。

主定理の証明

ステップ1：$\mathrm{Gal}(L/M)$ が閉部分群であること
M を有限次部分拡大 M_i の和集合 $\bigcup M_i$ とすると、$\mathrm{Gal}(L/M) = \bigcap \mathrm{Gal}(L/M_i)$ である。各 M_i を含む有限次ガロア拡大 N_i を取れば、$\mathrm{Gal}(L/N_i)$ はクルル位相の基本開近傍（かつ閉群）である。$\mathrm{Gal}(L/M_i)$ はその有限個の剰余類の和となるため閉群である。閉集合の共通部分は閉集合なので、$\mathrm{Gal}(L/M)$ は閉部分群である。

ステップ2：$L^{\mathrm{Gal}(L/M)} = M$ であること
自明な包含 $M \subset L^{\mathrm{Gal}(L/M)}$ の逆を示す。$\alpha \in L \setminus M$ とすると、最小多項式の次数は 2 以上。分離性より他の根 $\beta \neq \alpha$ が存在する。補題Aより、M を固定し α を β に移す τ を L 全体の自己同型 $\sigma \in \mathrm{Gal}(L/M)$ に延長できる。$\sigma(\alpha) = \beta \neq \alpha$ より α は固定されない。対偶より逆の包含が示され、両者は一致する。

ステップ3：閉群 H に対して $\mathrm{Gal}(L/L^H) = H$ であること
一般の部分群に対して $\mathrm{Gal}(L/L^H) = \bar{H}$ となることを示す。包含 $H \subset \mathrm{Gal}(L/L^H)$ は自明であり、ステップ1より右辺は閉なので $\bar{H} \subset \mathrm{Gal}(L/L^H)$。
逆に $\sigma \in \mathrm{Gal}(L/L^H)$ を取る。σ の任意の基本開近傍 $U = \sigma\mathrm{Gal}(L/N)$ を考える。$H|_N$ は有限次ガロア群 $\mathrm{Gal}(N/K)$ の部分群であり、有限次ガロア理論より $\mathrm{Gal}(N/N^{H|_N}) = H|_N$ である。不変体の定義から $N^{H|_N} = N \cap L^H$。σ は L^H を固定するので、$\sigma|_N$ は $N \cap L^H$ を固定する。つまり $\sigma|_N \in H|_N$。よって $\eta|_N = \sigma|_N$ となる $\eta \in H$ が存在し、これは $\eta \in U \cap H$ を意味する。したがって $\sigma \in \bar{H}$ であり、$\mathrm{Gal}(L/L^H) \subset \bar{H}$。よって H が閉群であれば $\mathrm{Gal}(L/L^H) = H$ となる。

ステップ4：正規性と同型
補題Bにより、M/K の正規性と $\mathrm{Gal}(L/M)$ の正規性は同値である。また制限写像 $G \to \mathrm{Gal}(M/K)$ の核は $\mathrm{Gal}(L/M)$ であり、第一同型定理より代数同型が得られる。クルル位相の性質（コンパクトからハウスドルフへの連続全射は開写像）により、これは位相同型となる。（証明終）