無限次ガロア理論

荒井勇人 *

2020.01.30

代数方程式の解の公式の研究から生まれた，ガロア理論という分野があります．五次以上の代数方程式が冪根による解の公式を持たないことがガロア理論により示されますが，ガロア理論そのものは体の拡大の中間体と群の部分群の対応として抽象的に定式化されるものです．今回の記事では，入門書の多くにガロア理論として書かれている「有限次ガロア理論」を前提に，より一般の無限次ガロア理論を紹介します．

1　有限次ガロア理論

無限次の話を始める前に，有限次ガロア理論を復習しておきましょう．詳しくは [1] を参照してください．

Def. 1. L/K を体の代数拡大，$\overline{K}$ を K の代数閉包とする．

(1) L が K ベクトル空間として有限次元のとき，L/K を有限次拡大という．
(2) $\alpha \in L$ の K 上の最小多項式 $f \in K[X]$ が $\overline{K}$ で重根を持たないとき，α は K 上分離的であるという．
(3) L の全ての元が K 上分離的なとき，L/K を分離拡大という．
(4) 全ての $\alpha \in L$ に対し，α の K 上の共役元が全て L に含まれるとき，L/K を正規拡大という．
(5) L/K が分離拡大かつ正規拡大のとき，ガロア拡大という．
(6) L/K がガロア拡大のとき，L の K 代数としての自己同型全体のなす群 $\mathrm{Aut}_K L$ を $\mathrm{Gal}(L/K)$ と書き，L/K のガロア群という．
(7) L の体としての自己同型全体のなす群 $\mathrm{Aut}\, L$ とその部分群 H に対し，$L^H = \{\alpha \in L \mid$ 全ての $\sigma \in H$ について $\sigma(\alpha) = \alpha\}$ は L の部分体になる．これを H の不変体という．

* 東大理学部数学科 B3．twitter:@alskdjfhg9.

Prop. 2. 代数拡大 L/K に対し，以下は同値.

(1) L/K は正規拡大.
(2) 全ての $\sigma \in \mathrm{Hom}_K(L, \overline{K})$ について，$\sigma(L) \subset L$.
(3) 全ての $\sigma \in \mathrm{Hom}_K(L, \overline{K})$ について，$\sigma(L) = L$.

ただし $\mathrm{Hom}_K(L, \overline{K})$ は L から $\overline{K}$ への K 代数準同型全体の集合.

Thm. 3 (有限次ガロア理論)**.** L/K を有限次ガロア拡大，$G = \mathrm{Gal}(L/K)$ とする．$\mathcal{M}$ を L/K の中間体全体の集合，$\mathcal{H}$ を G の部分群全体の集合とする．このとき

$$\Phi\colon \mathcal{M} \to \mathcal{H}, \quad M \mapsto \mathrm{Gal}(L/M)$$
$$\Psi\colon \mathcal{H} \to \mathcal{M}, \quad H \mapsto L^H$$

は互いに逆写像である．さらにこれにより中間体 M と部分群 H が対応するとき，M/K がガロア拡大であることと H が G の正規部分群であることは同値であり，このとき自然に

$$\mathrm{Gal}(M/K) \cong G/H$$

となる.

Thm. 4 (推進定理)**.** L/K を体の拡大，M, N を中間体とする.

(1) M/K が有限次ガロア拡大なら MN/N もそうで,

$$\mathrm{Gal}(MN/N) \cong \mathrm{Gal}(M/M \cap N)$$

である.
(2) M/K, N/K が有限次ガロア拡大なら MN/K もそうで，さらに $M \cap N = K$ なら

$$\mathrm{Gal}(MN/K) \cong \mathrm{Gal}(M/K) \times \mathrm{Gal}(N/K)$$

である.

Ex. 5. $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ とすると L/K は有限次ガロア拡大で，$\mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ である．よって $\mathrm{Gal}(L/K)$ は五つの部分群を持ち，対応して五つの中間体 $K = \mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6}), L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ を持つ.

このように有限次ガロア拡大においては中間体とガロア群の部分群が対応します．では無限次ガロア拡大でも中間体と部分群は対応するかというとそうではなく，次のような例があります.

Ex. 6. p を素数，l を奇素数とする．i を 0 以上の整数として $K_i = \mathbb{F}_{p^{l^i}}$, $K = K_0 = \mathbb{F}_p$, $L = \bigcup_{i=0}^{\infty} K_i$ とおく．$K_i = \{x \in \overline{K} \mid x^{p^{l^i}} - x = 0\}$ より L/K は正規拡大．K は有限体だか

ら L/K は分離拡大．よって L/K はガロア拡大で，無限次拡大でもある．$G = \mathrm{Gal}(L/K)$ とし $\varphi \in G$ を

$$\varphi\colon L \to L, \quad x \mapsto x^p$$

と定めると well-defined である（Frobenius 準同型という）．H を φ が生成する G の部分群とする．このとき $K = \{x \in L \mid x^p - x = 0\} = L^H$ である．しかし実は $H \subsetneq G$ であることが次のように示せる．

$k_i = 1 + l + \cdots + l^{i-1}$ とおくと，$\varphi^{k_{i+1}}|_{K_i} = \varphi^{k_i}|_{K_i}$ を満たす．よって $\sigma \in G$ を K_i 上で φ^{k_i} となるよう定めることができる．これが H に入らないことを示す．入ったと仮定して $\sigma = \varphi^n, n \in \mathbb{Z}$ とする．このとき K_i 上 $\varphi^{k_i} = \sigma = \varphi^n$ となるから，K_i と φ の定義より $k_i \equiv n \bmod l^i$ が全ての i で成り立つ．すると両辺に $1-l$ をかけることで $1 \equiv (1-l)n \bmod l^i$ となり, 結局 $1 = (1-l)n$ である．一方 l は奇素数だからこれは不可能である．よって $H \subsetneq G$ である．

したがってこの場合有限次ガロア理論の主張はそのままでは成り立たない．

このように無限次ガロア拡大においては単純に中間体と部分群が対応するわけではありません．では上の例で何がうまくいかなかったかというと，異なる部分群が同じ不変体を定めているということです．そこで，部分群の方に何らかの制限を加えて個数を減らしてやればうまくいくのではないかという考えに至ります．具体的にはガロア群に位相を入れて閉部分群のみを考えていきます．

2 profinite 群

この節では profinite 群を定義し，その性質を調べていきます．次節でガロア群に位相を導入して調べるときに使う結果が述べてあります．圏論の知識があると読みやすいかもしれません．

Def. 7. G を群とする．G が位相空間で，積および逆元をとる写像

$$\begin{aligned} \cdot \ &: G \times G \to G, \quad (g,h) \mapsto gh \\ (\cdot)^{-1}&: G \to G, \quad g \mapsto g^{-1} \end{aligned}$$

が連続になるとき，G を位相群という．位相群 G と H の間に同相な群同型があるとき，同型であるという．

Def. 8 (射影系)**.** I を半順序集合とし，全ての $i, j \in I$ に対しある $k \in I$ が存在して $i, j \leq k$ が成り立つとする．このとき I で添字づけられた群の族 $(G_i)_{i\in I}$ と，$\{(i,j) \in I \times I \mid i \leq j\}$ で添字づけられた群準同型の族 $(\varphi_{ij}\colon G_j \to G_i)$ の組 (G_i, φ_{ij}) であって，$i \leq j \leq k$ のとき $\varphi_{ij} \circ \varphi_{jk} = \varphi_{ik}$ を満たすものを，（I で添字づけられた）群の射影系という

同様にして位相空間と連続写像により位相空間の射影系を，位相群と連続群準同型により位相群の射影系を定める．[*1]

Def. 9 (射影極限)．(G_i, φ_{ij}) を群の射影系とする．次の性質（普遍性という）を満たす群と群準同型の族の組 $(\lim G_i, \varphi_i)$ が存在するとき，それをこの射影系の射影極限という．

(1) $\varphi_i \colon \lim G_i \to G_i$ で，$i \leq j$ のとき $\varphi_i = \varphi_{ij} \circ \varphi_j$ を満たす．
(2) 群と群準同型の族の組 $(H, \psi_i \colon H \to G_i)$ が，$i \leq j$ のとき $\psi_i = \psi_{ij} \circ \psi_j$ を満たすとする．このとき群準同型 $\psi \colon H \to \lim G_i$ で，任意の i について $\psi_i = \varphi_i \circ \psi$ を満たすようなものが一意に存在する．

同様に位相空間と連続写像，位相群と連続群準同型を使って位相空間，位相群の射影極限を定義する．[*2]

このようなものが実際に存在するか，また存在したとして簡単な構成があるかは非自明ですが，幸いにも群，位相空間，位相群の場合は次のような簡単な構成が存在します．

Prop. 10. 群の射影系 (G_i, φ_{ij}) についてその射影極限は存在し，次で与えられる．

$$\lim G_i = \{(x_i)_i \in \prod_i G_i \mid i \leq j \text{ のとき } x_i = \varphi_{ij}(x_j)\}$$

$$\varphi_i \colon \lim G_i \to G_i, \qquad (x_i)_i \mapsto x_i$$

位相空間，位相群でも同じ構成により射影極限が得られる．ただし $\lim G_i$ には $\prod_i G_i$ の直積位相からの相対位相を入れる．

Proof. 群，位相空間の場合は認めて位相群の場合のみ示す．

まず $\prod_i G_i$ は直積位相により位相群となることが簡単に確かめられる．すると $\lim G_i$ は位相群 $\prod_i G_i$ の部分群だから相対位相により位相群となる．φ_i が連続群準同型で射影極限の定義 (1) を満たすのは明らか．

次に射影極限の定義 (2) における (H, ψ_i) を任意にとる．$\lim G_i$ は G_i たちの群としての射影極限だから，射影極限の定義 (2) のような群準同型 $\psi \colon H \to G$ が一意に存在する．一方これは，$\lim G_i$ を G_i たちの位相空間としての射影極限と見たときに，射影極限の定義 (2) により存在する写像でもあるから連続である．よって $\lim G_i$ は G_i たちの位相群としての射影極限である． □

以降単に $\lim G_i$, $\varphi_i \colon \lim G_i \to G_i$ と書いたときはこの構成をとるものとする．

[*1] より一般に圏 $\mathcal{C}$ 上の射影系を考えることができます．
[*2] こちらも一般に圏 $\mathcal{C}$ 上の射影極限を考えることができます．

Def. 11 (profinite 群)**.** 位相群 G は，離散位相の入った有限群のある射影系 (G_i, φ_{ij}) の，位相群としての射影極限 $\lim G_i$ と位相群として同型なとき，profinite 群（副有限群）という．

Ex. 12. l を素数とすると，$(\mathbb{Z}/l^n\mathbb{Z}, \varphi_n)_{n\in\mathbb{N}}$，ただし

$$\varphi_n \colon \mathbb{Z}/l^n\mathbb{Z} \to \mathbb{Z}/l^{n-1}\mathbb{Z}, \qquad x + l^n\mathbb{Z} \mapsto x + l^{n-1}\mathbb{Z}$$

は有限群の射影系．これの射影極限を $\mathbb{Z}_l$ と書き，l 進整数環という（位相群構造を延長するような位相環構造が入る）．これは定義より profinite 群である．

Lem. 13. (G_i, φ_{ij}) を有限群の射影系，$G = \lim G_i$ を profinite 群，$\varphi_i \colon G \to G_i$ とする．このとき $S = \{\mathrm{Ker}\, \varphi_i\}_i$ は G における 1 の基本開近傍系をなす．

Proof. 直積位相の定義と G_i が離散空間であることより，$\prod_i G_i$ における 1 の基本開近傍系として

$$U_{i_1 \dots i_t} = \prod_{i \neq i_1, \dots, i_t} G_i \times \{1\}_{Gi_1} \times \cdots \times \{1\}_{Gi_t}, \quad t \text{ は 0 以上の整数，} i_1, \dots, i_t \text{ は全て異なる}$$

の形の開集合の族が取れる．ここで $i_0 \geq i_1, \dots, i_t$ となるように i_0 をとると，G の定義により $G \cap U_{i_0} \subset G \cap U_{i_1 \dots i_t}$ となる．$G \cap U_{i_0} = \mathrm{Ker}\, \varphi_{i_0}$ だから S は G における 1 の基本開近傍系である． □

$\lim G_i$ は位相群だから，$\in G$ の基本開近傍系として $xS = \{xU \mid U \in S\}$ がとれることに注意しましょう．

Prop. 14. profinite 群はコンパクトハウスドルフかつ完全不連結[*3]である．

Proof. G_i を有限群，$G = \lim G_i$ を profinite 群とする．

まず G_i は離散位相を考えているのでハウスドルフ．するとその直積 $\prod_i G_i$ もハウスドルフ．よってその部分空間 G もハウスドルフ．

次にコンパクト性を示す．G_i は有限群だからコンパクトで，チコノフの定理より $\prod_i G_i$ もコンパクト．よって G が $\prod_i G_i$ の中で閉集合であることを示せば十分．$i \leq j$ に対し

$$\begin{aligned} V_{ij} &= \left\{ (x_k)_k \in \prod_k G_k \mid x_i = \varphi_{ij}(x_j) \right\} \\ &= \bigcup_{x_j \in G_j} \left(\prod_{k \neq i,j} G_k \times \{\varphi_{ij}(x_j)\}_{G_i} \times \{x_j\}_{G_j} \right) \end{aligned}$$

[*3] 任意の連結成分が一点集合であるという性質．

は G_j が有限集合だから $\prod_k G_k$ の閉集合の有限和となり，閉集合である．すると

$$G = \bigcap_{i \leq j} V_{ij}$$

も閉集合.

最後に完全不連結であることを示す．G は位相群だから，1 を含む連結成分のみ考えれば良い．N を G の 1 を含む連結成分とすると，位相群の一般論より N は G の部分群となる．N=$\{1\}$ を示す．$U \in S = \{\mathrm{Ker}\,\varphi_i \colon G \to G_i\}_i$ を任意にとる．$U_N = U \cap N$ は空でない N の開集合である．また $V_N = \bigcup_{x \in N \setminus U} xU_N$ もまた N の開集合である．そしてこのとき $N = U_N \sqcup V_N$ である.

実際，$N = U_N \cup V_N$ は明らか．また

$$U_N \cap V_N \subset U \cap \left(\bigcup_{x \notin U} xU \right) = \bigcup_{x \notin U} (U \cap xU) = \emptyset$$

より $U_N \cap V_N = \emptyset$ である（最後の等号は U が G の部分群であることを使った）．すると N は連結なので $N = U_N \subset U$ であり，$N \subset \bigcap_{U \in S} U$ となるが，G はハウスドルフだから右辺は $\{1\}$ である．よって $N = \{1\}$ である． □

3 無限次ガロア理論

この節では有限次とは限らないガロア拡大を調べていきます．ガロア群が profinite 群になることを示し，前節の結果を使って主定理を示します.

Prop-Def. 15. L/K をガロア拡大とする．包含関係による半順序集合

$$B = \left\{ M \mid M \text{ は } L/K \text{ の中間体で } M/K \text{ は有限次ガロア拡大} \right\}$$

で添字づけられた有限群の射影系を,

$M \in B$ に対し $G_M = \mathrm{Gal}(M/K)$，$M, M' \in B$ で $M \subset M'$ のとき

$$\varphi_{MM'} \colon G_{M'} \to G_M, \qquad \sigma \mapsto \sigma|_M$$

と定める．このとき自然な射による群の同型

$$\mathrm{Gal}(L/K) \cong \lim G_M$$

が存在する．これにより $\mathrm{Gal}(L/K)$ に profinite 群としての位相群構造を定義する.

Proof. まず $\{G_M, \varphi_{MM'}\}$ が群の射影系となるのは明らか．群準同型

$$\varphi_M \colon \mathrm{Gal}(L/K) \to G_M, \quad \sigma \mapsto \sigma|_M$$

により誘導される射を $\varphi \colon \mathrm{Gal}(L/K) \to \lim G_M$ とする．すなわち

$$\varphi \colon \mathrm{Gal}(L/K) \to \lim G_M, \quad \sigma \mapsto (\sigma|_M)_M$$

とする．

単射性を示す．$\sigma \in Gal(L/K)$ とし，全ての $M \in B$ について $\sigma|_M = \mathrm{id}_M$ だとする．$\alpha \in L$ を任意にると，α を含む $M \in B$ が存在する．実際，α の K 上の共役元全体が生成する L/K の中間体 M をとれば良い．すると

$$\sigma(\alpha) = \sigma|_M(\alpha) = \alpha$$

となり，$\alpha \in L$ は任意だったので $\sigma = \mathrm{id}_L$ である．

全射性を示す．$(\sigma_M)_M \in \lim G_M$ を任意にとる．このとき $\sigma \in \mathrm{Gal}(L/K)$ を，$\alpha \in L$ に対し α を含む $M \in B$ をひとつとり，$\sigma(\alpha) = \sigma_M(\alpha)$ と定めると $\lim G_M$ の構成により well-defined となり，$(\sigma_M)_M$ の逆像となる． □

Cor. 16. L/K がガロア拡大のとき，$S = \{\mathrm{Gal}(L/M) \mid M \in B\}$ は $\mathrm{Gal}(L/K)$ における 1 の基本開近傍系をなす．

Proof. Lem.13 よりよい． □

Rem. 17. (1) L/K が有限次ガロア拡大のとき $\mathrm{Gal}(L/K)$ に入る位相は離散位相である．これは $\{1\}$ の基本開近傍系 S が $\mathrm{Gal}(L/L) = \{1\}$ を含むことと $\mathrm{Gal}(L/K)$ が有限集合であることからわかる．特にこのとき任意の部分群は閉部分群である．

(2) $\sigma, \tau \in \mathrm{Gal}(L/K)$ とする．σ の基本開近傍 $\sigma\,\mathrm{Gal}(M/K) \in \sigma S$ について，$\tau \in \sigma\,\mathrm{Gal}(L/M)$ と $\sigma|_M = \tau|_M$ は同値である．つまり，大きい中間体 M で一致しているとき，σ と τ を近いと思うような位相を考えていることになる．

Cor. 18. L/K がガロア拡大のとき，$\mathrm{Gal}(L/K)$ はコンパクトハウスドルフかつ完全不連結である．

Proof. $\mathrm{Gal}(L/K)$ は profinite 群だから Prop.14 よりよい． □

Lem. 19. $K \subset M \subset L$ を体の拡大とし，L/K はガロア拡大だとする．このとき埋め込み $H = \mathrm{Gal}(L/M) \hookrightarrow G = \mathrm{Gal}(L/K)$ は，両方に profinite 群としての位相を考えたときに像への同相である．特に $\mathrm{Gal}(L/M)$ は $\mathrm{Gal}(L/K)$ の閉部分群である．

Proof. 連続性を示す．位相群の間の群準同型だから，単位元での連続性を確かめればよい．1_G の基本開近傍 $\mathrm{Gal}(L/N), N \in B$ の引き戻しは

$$\mathrm{Gal}(L/M) \cap \mathrm{Gal}(L/N) = \mathrm{Gal}(L/MN)$$

であり，推進定理 Thm.4 よりと B の定義より MN/M は有限次ガロア拡大である．よって $\mathrm{Gal}(L/MN)$ は 1_H の基本開近傍となるので，連続である．するとこれはコンパクト空間からハウスドルフ空間への連続単射なので閉な像への同相である． □

Lem. 20. L/K をガロア拡大とする．このとき

$$\{\mathrm{Gal}(L/K) \text{ の開部分群 }\} = \{\mathrm{Gal}(L/M) \mid M \text{ は } L/K \text{ の中間体で } M/K \text{ は有限次拡大 }\}$$

が成り立つ．

Proof. $G = \mathrm{Gal}(L/K)$ とおく．

まず L/K の中間体 M で M/K が有限次拡大であるものを任意にとる．$\tilde{M}$ を，$M \subset \tilde{M}$ で $\tilde{M}/K$ が有限次ガロア拡大となるようにとる．例えば $M = K(\alpha_1, \ldots, \alpha_n)$ と表して $\tilde{M}$ を α_i たちの K 上の共役元全体が生成する L/K の中間体とすればよい．すると

$$\mathrm{Gal}(L/\tilde{M}) \subset \mathrm{Gal}(L/M) \subset G$$

は部分群の列で,

$$\mathrm{Gal}(L/M) = \bigcup_{\sigma \in \mathrm{Gal}(L/M)} \sigma\,\mathrm{Gal}(L/\tilde{M})$$

となる．$\tilde{M}/K$ は有限次ガロア拡大だから $\mathrm{Gal}(L/\tilde{M})$ は G の開集合で，σ を左からかける写像は G の自己同相だから $\sigma\,\mathrm{Gal}(L/\tilde{M})$ は G の開集合である．よって $\mathrm{Gal}(L/M)$ も G の開集合である．部分群なのは明らか．

次に $H \subset G$ を開部分群とする．H は 1 の開近傍だから Cor.16 よりある L/K の中間体 $\tilde{M}$ があり $\tilde{M}/K$ は有限次ガロア拡大で $\mathrm{Gal}(L/\tilde{M}) \subset H$ となるものがとれる．このとき定義域の制限による全射準同型 $G \to \mathrm{Gal}(\tilde{M}/K)$ により，H は $\mathrm{Gal}(\tilde{M}/K)$ の部分群 H' に対応する．有限次ガロア理論より $\tilde{M}/K$ の中間体 M があり $H' = \mathrm{Gal}(\tilde{M}/M)$ となる．すると

$$H = \{\sigma \in G \mid \sigma|_M\} = \mathrm{Gal}(L/M)$$

とかける． □

いよいよ主定理です．

Thm. 21 (ガロア理論)**.** L/K をガロア拡大，$G = \mathrm{Gal}(L/K)$ とする．$\mathcal{M}$ を L/K の中間体全体の集合，$\mathcal{H}$ を G の閉部分群全体の集合とする．このとき

$$\Phi\colon \mathcal{M} \to \mathcal{H}, \qquad M \mapsto \mathrm{Gal}(L/M)$$
$$\Psi\colon \mathcal{H} \to \mathcal{M}, \qquad H \mapsto L^H$$

は互いに逆写像である．さらにこれにより中間体 M と閉部分群 H が対応するとき，

(1) M/K が有限次拡大であることと H が G の開部分群であることは同値である．
(2) M/K がガロア拡大であることと H が G の正規部分群であることは同値であり，このとき位相群として自然に
$$\mathrm{Gal}(M/K) \cong G/H$$
となる．ただし G/H には G からの商位相を入れて考える．

Proof. まず Lem.19 より Φ は well-defined である．Ψ が well-defined なことは明らかである．次に Φ と Ψ が互いに逆であることを示す．

$M \in \mathcal{M}$, $H = \mathrm{Gal}(L/M)$ とする．$M \subset L^H$ は明らか．$\alpha \in L^H$ を任意にとる．$\beta \in L$ を α の M 上の共役とすると，ある $\sigma \in \mathrm{Gal}(L/M) = H$ が存在し $\sigma(\alpha) = \beta$ となる．一方 $\alpha \in L^H$ より $\sigma(\alpha) = \alpha$ だから $\beta = \alpha$ となる．α は M 上分離的であることと合わせて，α の M 上の最小多項式は一次式であることがわかる．よって $\alpha \in M$ となり $L^H \subset M$ である．つまり $\Psi \circ \Phi = \mathrm{id}_{\mathcal{M}}$ である．

$H \in \mathcal{H}$, $M = L^H$ とする．$H \subset \mathrm{Gal}(L/M)$ は明らか．$\sigma \in \mathrm{Gal}(L/M)$ を任意にとる．H は閉だから，σ の任意の近傍が H と交わることを言えば十分．σ の基本開近傍 $\sigma\,\mathrm{Gal}(L/N) \in \sigma S$ を任意にとる（S の定義より N/K は有限次ガロア拡大）．全射準同型 $G \to \mathrm{Gal}(N/K)$ による H の像を H' とする．$N^{H'} = N \cap L^H = N \cap M$ だから，有限次ガロア理論より $H' = \mathrm{Gal}(N/N \cap M)$ となる．すると $\sigma \in \mathrm{Gal}(L/M)$ より $\sigma|_N \in H'$，つまりある $\tau \in H$ が存在して $\sigma|_N = \tau|_N$ となる．これは $\tau \in \sigma\,\mathrm{Gal}(L/N)$ と同値で，$\tau \in H$ より $\sigma\,\mathrm{Gal}(L/N) \cap H \neq \emptyset$ である．よって σ の任意の近傍は H と交わる．

以上より Φ と Ψ は互いに逆写像である．そしてこれにより L/K の中間体 M と G の閉部分群が対応するとする．

M/K が有限次拡大であることと H が G の開部分群であることが同値なのは，Lem.20 と対応関係を合わせて考えれば明らか．

M/K がガロア拡大だとする. 特に正規拡大だから任意の $\sigma \in \mathrm{Gal}(L/K) = \mathrm{Aut}_K L = \mathrm{Hom}_K(L, \overline{K})$ について $\sigma(M) = M$．すると任意の $\tau \in \mathrm{Gal}(L/M)$ について $\sigma^{-1}\tau\sigma|_M = \mathrm{id}_M$ となり $\sigma^{-1}\tau\sigma \in \mathrm{Gal}(L/M)$，つまり $H = \mathrm{Gal}(L/M)$ は $G = \mathrm{Gal}(L/K)$ の正規部分群である．

逆に H が G の正規部分群だとする．M/K が正規拡大であることを示せばよい．Prop.2(2) の条件を示す．$\sigma \in \mathrm{Hom}_K(M, \overline{K})$ とし σ の L への延長のひとつを $\tilde{\sigma} \in \mathrm{Hom}_K(L, \overline{K}) = \mathrm{Gal}(L/K) = G$ とする．H は G の正規部分群だから，任意の $\tau \in H$ について $\tilde{\sigma}^{-1}\tau\tilde{\sigma} \in H$．これを $\tau' \in H$ とすると，任意の $\alpha \in M$ について

$$\tau(\sigma(\alpha)) = \tau(\tilde{\sigma}(\alpha)) = \tilde{\sigma}(\tau'(\alpha)) = \tilde{\sigma}(\alpha) = \sigma(\alpha)$$

となる（ただし左から 3 つ目の等号は $\alpha \in M = L^H$ と $\tau' \in H$ を使った）．$\tau \in H$ は任意だったから，この式は $\sigma(\alpha) \in L^H$ を意味する．よって M/K は Prop.2(2) の条件を満たすから正規拡大である．

そして M/K がガロア拡大のとき，全射かつ連続な準同型 $G \to \mathrm{Gal}(M/K), \sigma \mapsto \sigma_M$ が存在する（連続性はそれぞれの位相の定義から簡単にわかる）．準同型定理を使うと群として $G/H \cong \mathrm{Gal}(M/K)$ であり，商位相の定義より同型射 $G/H \to \mathrm{Gal}(M/K)$ は連続である．よってこれはコンパクト空間からハウスドルフ空間への連続全単射だから同相であり，位相群の同型である． □

Rem. 22. Rem.17(1) より，Thm.21 は有限次ガロア理論 Thm.3 の一般化になっていることがわかる．

この定理を踏まえて Ex.6 をもう一度考察してみましょう．L/K を Ex.6 のものとすると，K_i/K たちが全ての有限次ガロアな中間体で，有限体の拡大のガロア群は巡回群であることから

$$\mathrm{Gal}(L/K) \cong \lim \mathrm{Gal}(K_i/K) \cong \lim \mathbb{Z}/l^i\mathbb{Z} \cong \mathbb{Z}_l$$

となることがわかります．Frobenius 準同型 φ は各 $\mathrm{Gal}(K_i/K)$ の生成元だから，$\mathbb{Z}_l$ においては 1 に対応します．すると φ の生成する部分群 H は $\mathbb{Z}_l$ の稠密な部分群 $\mathbb{Z}$ に対応し，$\sigma \in G\backslash H$ は $1 + l + l^2 + \cdots \in \mathbb{Z}_l\backslash\mathbb{Z}$ に対応します．Ex.6 でうまくいかなかったのは，$H \cong \mathbb{Z}$ とその閉包である $G \cong \mathbb{Z}_l$ が同じ不変体を定めていたからですが，これに関連して次の命題が成り立ちます．

Prop. 23. L/K をガロア拡大，$G = \mathrm{Gal}(L/K)$ とする．

(1) G の位相は任意の $\alpha \in L$ に対し

$$\mathrm{ev}_\alpha \colon \mathrm{G} \to \mathrm{L}, \quad \sigma \mapsto \sigma(\alpha)$$

が連続となるような最弱の位相（各点収束位相）である．ただし L には離散位相を入れて考える．

(2) H を G の部分群とし，$\overline{H}$ をその閉包とする．このとき $L^H = L^{\overline{H}}$ である．

Proof. (1) [3] Lem.3.2.4 を参照．

(2) [4] Proposision.7.10 を参照．

□

つまり，気持ちとしては H の元の極限である[*4] $\overline{H}$ もまた L^H の元を固定するため，同じ不変体を与えてしまうということが起きていたわけです．

[*4] これは一般の位相空間では成り立たず，第一可算性が必要ですが，$\mathbb{Z}_l$ は第一可算なので大丈夫です．

最後に面白い定理をひとつ紹介します.

Thm. 24 (Leptin)**.** 任意の profinite 群に対して，それと同型なガロア群を持つガロア拡大が存在する．特に任意の有限群はガロア群として現れる.

Proof. [2]Theorem.1.15 を参照. □

参考文献

[1] 雪江明彦,『代数学 2　環と体とガロア理論』，日本評論社，2010.

[2] Luis Ribes, *Introduction to Profinite Groups*, Travaux mathematiques, 2013. https://wwwfr.uni.lu/content/download/75427/940970/file/Ribes.pdf

[3] Borceux, Janelidze, *Galois Theories*, Cambridge Studies in Advanced Mathematics, 2008.

[4] J.S.Milne, *Fields and Galois Theory*, https://www.jmilne.org/math/CourseNotes/FT421.pdf