プレサマースクール—数論的な体の絶対ガロア群の構造への道先案内—

大阪大学　落合理

Contents

本論に入る前に, サマースクールのテーマとの結びつきに触れたい.
G を局所コンパクトな位相群, M を局所コンパクトな位相アーベル群とする. 連続写像の集合 $\mathrm{Map}(M,M)$ にはコンパクト開位相 (open compact topology) が入る. さらに M は可換環 R 上の有限生成加群であるとして, M の R-線形な自己準同型写像は連続写像であるとする. $\mathrm{Aut}_R(M) \subset \mathrm{End}_R(M) \subset \mathrm{Map}(M,M)$ には制限位相を入れる. このとき,

定義 0.1. 有限生成 R-加群 M に対して G が作用しているとする. このとき, 与えられた G の作用が連続であるとは対応する

$$\rho : G \longrightarrow \mathrm{Aut}_R(M)$$

が連続であることをいう.

実際, ガロア表現で考える場合にはたいてい次のような状況を考える.

(1) G は可換体 K（特に K は代数体, または局所体）の絶対ガロア群 G_K, または G_K の位相群としての部分商.
(2) R としては次のようなものを考える.
  (a) $\mathbb{Z}/l\mathbb{Z}$ やその持ち上げ環 $\mathbb{Z}/l^r\mathbb{Z}$, あるいはより一般に有限体 $\mathbb{F}_{l^n}$ やその持ち上げ環 $W_r(\mathbb{F}_{l^n})$. (R の位相は離散位相を考える)
  (b) $\mathbb{Z}_l$ や $\mathbb{Q}_l$. (R の位相は l 進位相を考える)
  (c) べき級数環 $\mathbb{Z}_l[[X_1,\cdots,X_m]]$ や $\mathbb{Z}_l[[X_1,\cdots,X_m]]$ 上有限な環[1]. (R の位相は極大イデアルのベキ乗を開集合とする位相で最も弱いものを考える)

[1] これらは肥田理論やガロア表現の変形などで現れる.

(d) 離散位相をいれた標数 0 の体[2].

(3) M はたいてい R 上の有限生成自由加群であるが, 必ずしも自由でない R-加群を扱うこともあり得る [3]. M には上で述べたような R の位相から引き起こされる位相を入れる.

これら各々の M や R に応じて, 本報告集の記事 [Ya] ではそれぞれの様子を入門的に紹介する. 同じく, 記事 [C] で基本的なことのいくらかが説明されている. 本報告集の他の記事では, [Ya], [C] を基にしてさらにガロア表現のテーマにおける様々なヴァリエーションが展開され, ときに Fermat 予想, Artin 予想, 佐藤-Tate 予想などへの応用にまで繋がっていくことが論じられる. そういった先の話を意識に置きながらも, 本記事では表現を考える群 G(上で述べたように数論的な体 K の絶対ガロア群 G_K を考える) 自身にはどのような構造があるのかを説明して後の記事への準備 (特に直後の [Ya] への準備) としたい.

1. 副有限群 (PROFINITE GROUP) とガロア理論

1.1. **副有限群の定義と特徴づけ.** 前節で現れた G としては実際は適当な体の絶対ガロア群の部分商を考えることになる. そのような群たちは全て副有限というクラスの群になるので, 本論に入る前に副有限について基本的なことをまとめておきたい.

定義 1.1. 位相群 G が**副有限群**であるとは, 有向順序集合 Λ で添え字づけられた有限群の集合 $\{G_\lambda\}_{\lambda\in\Lambda}$ が存在して, $G \cong \varprojlim_{\lambda\in\Lambda} G_\lambda$ となることをいう. (但し, G_λ は離散位相をもち逆極限には自然に誘導される位相を入れる)

副有限の特徴づけとして次がなりたつ:

定理 1.2. G を位相群とするとき次の 3 条件は同値である.

(1) G は副有限群である.

(2) G の位相はコンパクト, ハウスドルフであって, G の正規開部分群たちが G の単位元のまわりの基本開近傍系を与える.

(3) G の位相はコンパクト, ハウスドルフかつ全不連結である.

注意 1.3. 例えば無限離散群や実リー群などには副有限群の構造は入らない

上の定理の証明はしないが, 例えば [Sha, Chap. 1, §1, Theorem 2], [NSW, Prop. 1.1.3] などを参照されたい. 定義から全ての有限群は副有限群である. また, 副有限群についてはある程度有限群と似たような理論的な取り扱いができる.

先に進む前に, 一般的に通常の群が与えられるとその群を “完備化”することで副有限群が与えられることにも注意しておきたい.

定義 1.4. Γ を群とする.

[2]このような表現はアルチン表現とよばれる.

[3]肥田理論などで構成されるガロア表現では M が自由になるかわからない場合がある.

(1) 群 Γ に対して
$$\widehat{\Gamma} := \varprojlim \Gamma/H$$
(H は Γ の指数有限の正規部分群全てをわたる)
のことを Γ の**副有限完備化**とよぶことにする.
(2) 群 Γ に対して
$$\widehat{\Gamma}^{\mathrm{sol}} := \varprojlim \Gamma/H$$
(H は Γ の指数有限の正規部分群で Γ/H が可解なもの全てをわたる)
のことを Γ の**副有限可解完備化**とよぶことにする.
(3) 群 Γ に対して
$$\widehat{\Gamma}^{(p)} := \varprojlim \Gamma/H$$
(H は Γ の指数有限の正規部分群で Γ/H の指数が p ベキなもの全てをわたる)
のことを Γ の**副有限 p 完備化**とよぶことにする.

自然に全射たち
$$\widehat{\Gamma} \twoheadrightarrow \widehat{\Gamma}^{\mathrm{sol}} \twoheadrightarrow \widehat{\Gamma}^{(p)}$$
があることに注意したい.

1.2. **Krull 位相とガロア理論.** 有限次拡大のガロア理論はここでは復習せずある程度みとめてすすみたい. 無限次拡大のガロア理論について以下ごく簡単に主要な事柄を思い出しておきたい. (ここではあまり立ち入らないガロア理論の詳細については [Fu], [N] などを参照されたい)

定義 1.5 (有限次とは限らないガロア拡大)**.** (1) 勝手な代数拡大 L/K が**ガロア拡大**であるとは, 正規かつ分離であること (つまり少なくとも 1 つは L に根をもつ任意の既約多項式 $f \in K[X]$ が必ず $\deg f$ 個の異なる根を L にもつこと) をいう.
(2) L/K がガロア拡大のとき, L の上の自己同型全体のなす群を L/K の**ガロア群**とよび $\mathrm{Gal}(L/K)$ と記す.

実は, 上で定義されたガロア拡大 L は有限次ガロア拡大たちの合成体に他ならない.

定理 1.6. *K を体とするとき, K の拡大体 L で次をみたすものが存在する.*
(1) *L は K の分離代数拡大である.*
(2) *M/K を有限次分離拡大とするとき, K 上の埋め込み $M \hookrightarrow L$ が存在する.*

注意 1.7. (1) L, L' がともに上記の 2 つの条件をみたすとき L から L' への同型が存在することがわかる. つまりこれを**分離閉包**とよび K^{sep} と記される.
(2) K が完全体とするとき, 分離閉包 K^{sep} は代数閉包 $\overline{K}$ に他ならない.

K の分離閉包 K^{sep} はそれ自身 K のガロア拡大であり, K のガロア拡大たちの親玉である. $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ のことを K **の絶対ガロア群**とよび, G_K と記す. たいていの場合 G_K は無限群であり[4], K が数論的な体の時に G_K の構造を §§2–4 で述べる. 無限次拡大のガロア理論においては, 位相を入れて考えることで有限次拡大のときのガロア

[4]例えば, K の標数が正であるときは $K \subsetneq K^{\mathrm{sep}} \longleftrightarrow \sharp\mathrm{Gal}(K^{\mathrm{sep}}/K) = \infty$ である.

理論の一般化が成り立つことを以下で説明する. 以下の補題 1.8, 補題 1.10, 定理 1.12 らの証明は全て省略するがいずれも [Fu] の付録などを参照のこと.

補題 1.8. L/K を（必ずしも有限次とは限らない）ガロア拡大とする. $\mathrm{Gal}(L/K)$ には

$$\{\mathrm{Gal}(L/M) \subset \mathrm{Gal}(L/K) | M \text{ は } K \text{ の有限次拡大 }\}$$

を単位元の基本開近傍系とするような位相群の構造が $\mathrm{Gal}(L/K)$ に一意に定まる.

定義 1.9. 上の補題で定まる $\mathrm{Gal}(L/K)$ の位相を Krull 位相と呼ぶ.

補題 1.10. L/K を（必ずしも有限次とは限らない）ガロア拡大とする. $\mathrm{Gal}(L/K)$ は *Krull* 位相に関してコンパクト, ハウスドルフかつ全不連結である.

注意 1.11. 実は, $\mathrm{Gal}(L/K)$ は位相群として $\varprojlim \mathrm{Gal}(M/K)$ (M はに含まれる K 上有限次ガロア拡大すべてをわたる) と同型である. よってガロア群は常に副有限である. 無限離散群や実リー群などはガロア群とはなりえないこともわかる.

定理 1.12 (ガロア理論の基本定理)**.** L/K を必ずしも有限次とは限らないガロア拡大とする.

(1) 次のような一対一対応がある*:*

$$\{\mathrm{Gal}(L/K) \text{ の閉部分群 } H \text{ たち }\} \overset{\Phi}{\longleftrightarrow} \{L/K \text{ の中間体 } M \text{ たち }\}$$
$$H \overset{\Psi}{\longrightarrow} M = L^H$$
$$H = \mathrm{Gal}(L/M) \longleftarrow M.$$

この対応において, $\Psi \circ \Phi$, $\Phi \circ \Psi$ はともに恒等写像となる.

(2) 上の対応を特別な場合へと制限することで次の対応も成立する :

(a) $\{\mathrm{Gal}(L/K)$ の正規閉部分群 H たち $\} \longleftrightarrow \{L/K$ の K 上ガロアな中間体 M たち $\}$

(b) $\{\mathrm{Gal}(L/K)$ の開部分群 H たち $\} \longleftrightarrow \{L/K$ の K 上有限次な中間体 M たち $\}$

次の節以降で基本的な体の場合にどういった構造を持つかをより詳しくみていく.

2. 有限体のガロア群の構造について

最も素朴な対象は有限体である. 以下のことは証明しない.

事実

(1) K を有限体とするとき, K の標数はある素数 $p > 0$ であり, K の位数 q は p のベキとなる.

(2) 逆に q を素数 p のベキとする. 位数が丁度 q である有限体 $\mathbb{F}_q$ が必ず存在して, またそのようなものは同型を除いて一意である. これを $\mathbb{F}_q$ と記す.

(3) $K = \mathbb{F}_q$ とする. 各自然数 n ごとに K の n 次拡大が (同型を除いて) ただひとつ存在して $\mathbb{F}_{q^n}$ と同型である.

(4) $\mathbb{F}_{q^n}/\mathbb{F}_q$ はガロア拡大であり, そのガロア群は

$$\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z},\ \mathrm{Frob}_q \mapsto 1$$

なる同型をもつ. $\mathbb{F}_{q^n}/\mathbb{F}_q$ 上の**フロベニウス** Frob_q とは $\mathbb{F}_{q^n} \longrightarrow \mathbb{F}_{q^n},\ x \mapsto x^q$ で与えられる体の自己同型のことをいう.

(5) 絶対ガロア群 $G_{\mathbb{F}_q} = \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ は

$$\varprojlim \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \xrightarrow{\sim} \widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z} \cong \prod_{l:\text{素数}} \mathbb{Z}_l,\ \mathrm{Frob}_q \mapsto 1$$

なる同型をもつ.

(6) 各自然数 n ごとに

$$\mathbb{F}_{q^n} = \mathbb{F}_q(\zeta_{q^n-1})$$

が成り立つ. (但し, ζ_{q^n-1} は (代数閉包 $\overline{\mathbb{F}}_q$ における)1 の原始 q^n-1 乗根.)
また,

$$\overline{\mathbb{F}}_q = \bigcup_{p\nmid m} \mathbb{F}_q(\zeta_m)$$

が成り立つ. (但し, ζ_m は (代数閉包 $\overline{\mathbb{F}}_q$ における)1 の原始 m 乗根)

3. 局所体のガロア群の構造について

定義 3.1. K が (普通の意味での) 局所体とは K が完備離散付値体で剰余体 k が有限であるものをいう.

$R \subset K$ を付値環, $\varpi \in R$ を素元とする. 剰余体 $k := R/\varpi R$ は有限体なので k の標数はある素数 p である. このとき, 2 通りの場合が考えられる. (以下のように分類されることの証明は例えば [AM, 定理 2.5.1] などを参照のこと.)

(1) K の標数が 0 のとき.
K は自然に $\mathbb{Q}_p$ の有限次拡大となることがわかる. (このような K は混標数 $(0,p)$ の局所体とよばれる)

(2) K の標数が 0 でないとき.
K の標数は剰余体 k の標数 p と一致し, $R = k[[\varpi]]$ かつ $K = k((\varpi))$ となることもわかる. (このような K は等標数の局所体とよばれる)

注意 3.2.

(1) 実際には, 局所体に関するかなりの理論が混標数と等標数とに対して同様に成り立ち, 統一して記述できることが多い (この 2 つが唯一の非自明な局所コンパクト位相体である)

(2) 一方で場合によっては混標数の方が複雑なこともありより面白いこともある. また, 混標数の局所体は代数体の各素点における完備化として現れることからもより重要度が高い.

(3) また, Fontaine-Wintenberger による「ノルム体の理論」があり, 標数 0 の局所体 K の絶対ガロア群のある大きな閉部分群 $H \subset G_K$ に対して, ある等標数 p の局所体 K' が存在して

$$H \cong G_{K'}$$

となる驚くべき結果もあり, 混標数の局所体の問題が等標数の局所体の問題に帰着されることによる応用もある[5].

G_K のアーベル化については完全にわかっている. K^{ab} を K の最大アーベル拡大とするとき $(G_K)^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K)$ に対して次のことが成立する.

定理 3.3 (局所類体論)**.** K を局所体とするとき, 写像（相互写像）

$$\mathrm{rec}_K : \ K^\times \hookrightarrow (G_K)^{\mathrm{ab}}$$

があり, rec_K の像は $(G_K)^{\mathrm{ab}}$ の中で稠密で $K^\times$ の指数有限部分群たちと G_K^{ab} の開部分群は一対一に対応する. また, 勝手な有限次アーベル拡大 L/K に対して rec_K は同型

$$K^\times/\mathrm{Norm}_{L/K}(L^\times) \xrightarrow{\sim} \mathrm{Gal}(L/K)$$

をひきおこす.

実は, (今回は深くは立ち入らないが) おおまかに以下の 2 つのことがらがこの周辺のものごとの理解のために非常に大切である:

(1) 上述のアーベル拡大に対する類体論と類体論の証明の過程で現れるブラウアー群やコホモロジーなどに関すること
(2) 完備離散付値体 K の分岐理論や分岐群に関すること

こういった道具立てを用いることで次のことがわかる.

定理 3.4. K を混標数 $(0, p)$ の局所体とする. K の絶対ガロア群 G_K は位相的に有限生成な可解群である. より詳しく, 以下が成り立つ.

(1) $K \subset K^{\mathrm{unr}} \subset K^{\mathrm{tame}} \subset \overline{K}$ となる $\overline{K}/K$ の中間ガロア拡大体 K^{unr} (**最大不分岐拡大**とよばれる), K^{tame} (**最大順分岐拡大**とよばれる) があり, 対応するガロア群の列:
$$\{1\} \subset G_{K^{\mathrm{tame}}} \subset G_{K^{\mathrm{unr}}} \subset G_K$$
の各部分商は以下の様になる.
   (a) $G_K/G_{K^{\mathrm{unr}}} = \mathrm{Gal}(K^{\mathrm{unr}}/K)$ は剰余体の絶対ガロア群 $\mathrm{Gal}(\overline{\mathbb{F}}_q/k)$ と同型である.
   (b) $G_{K^{\mathrm{unr}}}/G_{K^{\mathrm{tame}}} = \mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}})$ は $\prod_{l \neq p} \mathbb{Z}_l$ と同型である.
   (c) $G_{K^{\mathrm{tame}}}$ は可算階数の自由群 $F_{\mathbb{N}}$ の p 進完備化 $\widehat{F}_{\mathbb{N}}^{(p)}$ と同型である.
(2) 部分商のみでない拡大に関する情報については以下が成り立つ.
   (a) $\mathrm{Gal}(K^{\mathrm{tame}}/K)$ は群の拡大 :
   $\{1\} \to \mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}}) \to \mathrm{Gal}(K^{\mathrm{tame}}/K) \to \mathrm{Gal}(K^{\mathrm{unr}}/K) \to \{1\}$
   をもち, $\mathrm{Gal}(K^{\mathrm{unr}}/K)$ の q 乗写像からくる位相的生成元 Frob_q の $g \in \mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}})$ への共役作用 $\mathrm{Frob}_q \cdot g$ は $g^q \in \mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}})$ で与え

[5]「ノルム体の理論」そのものについては例えば [W] などを参照のこと. 応用としては, p 進ホッジ理論の近年の発展で大事な役割を演じる Φ-Γ 理論などがノルム体の理論を元にして構成されている. (p 進ホッジ理論のもっとも基礎的な事柄については本報告集の記事 [Na] を参照のこと) それ以外にも explicit reciprocity law の研究においても混標数の explicit reciprocity law の研究を等標数の explicit reciprocity law の結果に帰着するなど個別の問題に応用されることがある.

られる. あるいは, 同じことであるが, 生成元と関係式の表示 $\langle \sigma, \tau | \sigma\tau\sigma^{-1} = \tau^q \rangle$ で与えられる群を Γ とするとき, σ を Frob_q に送るような同型 $\widehat{\Gamma} \cong \mathrm{Gal}(K^{\mathrm{tame}}/K)$ が存在する. [6]

(b) 群の拡大 :
$\{1\} \to G_{K^{\mathrm{tame}}} \to G_K \to \mathrm{Gal}(K^{\mathrm{tame}}/K) \to \{1\}$
は分裂する. つまり $H \cap G_{K^{\mathrm{tame}}} = \{1\}$ かつ $G_K = HG_{K^{\mathrm{tame}}}$ なる部分群 $H \subset G_K$ が存在する. 共役作用による H 加群として

$$(G_{K^{\mathrm{tame}}})^{\mathrm{ab}} \cong \mathbb{Z}_p \oplus (\mathrm{Cont}(H, \mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{PD}})^{[K:\mathbb{Q}_p]}$$

なる同型がある. 但し, $(\ \ )^{\mathrm{PD}}$ は Pontrjagin 双対をあらわす.

注意 3.5. しばしば, $G_{K^{\mathrm{unr}}}$ のことを K の**惰性群**と呼び I_K で記す. また, $G_{K^{\mathrm{tame}}}$ のことを K の**分岐群**と呼び P_K で記す.

証明のスケッチ.
p 進体の絶対ガロア群については, 注意 3.7 のように, 位相的に有限生成であるのみならず群としての表示までも知られている. 注意 3.7 の文献を参照してもらうことにより, 位相的に有限生成であることは省きたい. G_K の部分商の記述からみていくことにする.

まず,

K^{unr}: K 上の不分岐な拡大すべての合成体

K^{tame}: K 上で分岐指数が p と素な拡大すべての合成体

とする. 定義より $K \subset K^{\mathrm{unr}} \subset K^{\mathrm{tame}} \subset \overline{K}$ が成り立つ.

まず最初の記述 1 を示していきたい.

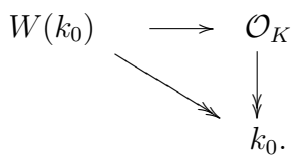
(a) の証明には, 一般に正標数の完全体 k_0 に対して Witt 環と呼ばれる環 $W(k_0)$ が構成され, 次の性質をもつ[7]:

(1) $W(k_0)$ は標数 0 の環で p を素元とする完備離散付値環となる.
(2) 剰余体 $W(k_0)/(p)$ は k_0 と同型.

今, 次の補題が成り立つ. (証明については [Ser] Chap. II §5 Theorem 4 を参照のこと)

補題 3.6. K を混標数 $(0, p)$ の完備離散付値体で剰余体が完全体 k_0 であるとする.

(1) このとき下の図式を可換にするような標準的な環の単射 $W(k_0) \hookrightarrow \mathcal{O}_K$ が存在する :



[6] τ は証明中にあらわれるような K^{unr} 上の Kummer 拡大のガロア群の生成元となる.
[7] Witt 環については例えば [Ser, Chap. II, §6] などを参照のこと

(2) 更に, K_0 を $W(k_0)$ の分数体とすると拡大 K/K_0 は完全分岐拡大である. (K_0 を K の**最大不分岐部分体**とよぶことにする.) K の素元 ϖ の K_0 上の最小多項式は Eisenstein 多項式となりその次数 d は $[K:K_0]$ に等しい. 逆に K_0 上の d 次 Eisenstein 多項式の根 α を K_0 に付けくわえた体 $K(\alpha)$ は K_0 の d 次完全分岐拡大で α は K の素元となる.

ある $\mathcal{O}_K$ の素元 ϖ があって $\mathcal{O}_K = W(k)[\varpi]$ となることもわかる. 今, L は K の不分岐拡大であるから, K の素元 ϖ は L の素元でもある. 補題 3.6 の (2) を用いると $[L:L_0] = [K:K_0]$ である. よって, $[L:K] = [L_0:K_0]$ である. L の剰余体を k' とすると, 補題 3.6 の (1) より $\mathcal{O}_{L_0}$ は $W(k')$ を含んでかつ以下の等号が成り立つ.

$$[L:K] = [L_0:K_0] = \mathrm{rank}_{\mathcal{O}_{K_0}}\mathcal{O}_{L_0} = \mathrm{rank}_{W(k)}W(k') = \dim_k k' \tag{1}$$

今, $\mathrm{Gal}(L/K)$ は自然に $\mathcal{O}_L$ に作用するので

$$\mathrm{Gal}(L/K) \xrightarrow{\sim} \mathrm{Aut}_{\mathcal{O}_K}\mathcal{O}_L \twoheadrightarrow \mathrm{Gal}(k'/k)$$

がある. 2 番目の写像の全射性は全射 $\mathcal{O}_L \twoheadrightarrow k'$ によって $\overline{\alpha} \in k'$ をある $\alpha \in \mathcal{O}_L$ に持ち上げて $\mathcal{O}_L$ 上での α の L における最小多項式やガロア作用を考えることから勝手な有限次拡大 L/K に対して成り立つことがわかる. 上の数式 (1) で等号が成り立つことより L/K はガロア拡大で $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(k'/k)$ となることが結論づけられる. 不分岐拡大 L/K たちに関する極限をとることで $\mathrm{Gal}(K^{\mathrm{unr}}/K) = \mathrm{Gal}(\overline{\mathbb{F}}_q/k)$ が得られる.

次に定理 3.4 の (1) の (b) の証明を論じたい. $p \nmid e$ とするとき, K^{unr} 上の分岐指数 e の拡大 M を考える. M の素元 ϖ' をとると, $K^{\mathrm{unr}}[(\varpi')^e]$ は不分岐拡大であるから, $(\varpi')^e \in K^{\mathrm{unr}}$ となる. K^{unr} は 1 の原始 e 乗根を含むので Kummer 理論より M/K^{unr} はガロア拡大でそのガロア群は μ_e と同型であることがわかる. $\varprojlim_{p\nmid e}\mu_e \cong \prod_{l\neq p}\mathbb{Z}_l$ より定理 3.4 の (1) の証明がしたがう.

定理 3.4 の (1) の (c) の記述である K^{tame} 上のガロア群 $G_{K^{\mathrm{tame}}}$ の構造については類体論やガロアコホモロジーといった少し深い理論を用いることによって調べられる. 岩澤による研究 (cf. [Iw53], [Iw55]) によって次のようなことが示されている:

勝手にとった可換体 $\widetilde{K}$ に対して次の (a)-(c) が成り立っているとする.

(a) $\widetilde{K}$ は 1 の原始 p 乗根 ζ_p を含む.
(b) $G_{\widetilde{K}}$ の 2 次ガロアコホモロジーが消える.
(c) $\widetilde{K}^\times/(\widetilde{K}^\times)^p$ が “十分大きい” [8]

このとき, $\widetilde{K}$ の上の最大 pro-p 拡大のガロア群は可算階数の自由群 $F_{\mathbb{N}}$ の副有限 p 完備化 $\widehat{F}_{\mathbb{N}}^{(p)}$ と同型である.

一方で, 混標数 $(0,p)$ の局所体に ζ_p を付け加える拡大は順分岐拡大であるから $\widetilde{K} = K^{\mathrm{tame}}$ のときには $\zeta_p \in K^{\mathrm{tame}}$ である. よって条件 (a) は満たされる. K^{tame} は先の (1)

[8] “十分大きい” の意味については論文 [Iw55] を参照のこと.

の (b) によってわかっており, $K^{\mathrm{tame}\times}/(K^{\mathrm{tame}\times})^p$ が “十分大きい” こともただちにわかり条件 (c) も満たされる. 条件 (b) に現れるような $\widetilde{K}$ の 2 次のコホモロジーはおおよそ $\widetilde{K}$ のブラウアー群と関係がある. 今考えているような拡大 K^{tame} 上ではブラウアー群は自明であり 2 次以上のコホモロジーが消えることが知られているので条件 (b) も確かめられる. かくして, K^{tame} は岩澤によって与えられた群論的な条件を満たし, 記述 (1) の (c) がしたがう.

定理 3.4 の (2) の (a) については, まず K^{tame} に含まれる K^{unr} の有限次拡大は必ず $K^{\mathrm{unr}}(\sqrt[e]{\varpi})$ なる巡回拡大となる. $\tau \in \mathrm{Gal}(K^{\mathrm{unr}}(\sqrt[e]{\varpi})/K^{\mathrm{unr}})$ を生成元とすると, $\tau(\sqrt[e]{\varpi}) = \zeta\sqrt[e]{\varpi}$ となる (ζ は 1 の原始 e 乗根). 一方で, $\mathrm{Frob}_q \in \mathrm{Gal}(K^{\mathrm{unr}}/K)$ の $g \in \mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}})$ への作用 $\mathrm{Frob}_q \cdot g$ は, 勝手な持ち上げ $\widetilde{\mathrm{Frob}}_q \in \mathrm{Gal}(K^{\mathrm{tame}}/K)$ を用いて

$$\mathrm{Frob}_q \cdot g := \widetilde{\mathrm{Frob}}_q g \widetilde{\mathrm{Frob}}_q^{-1}$$

で定義される. $(\zeta)^{\widetilde{\mathrm{Frob}}_q} = \zeta^q$ であることから

$$\begin{aligned}(\widetilde{\mathrm{Frob}}_q g \widetilde{\mathrm{Frob}}_q^{-1})(\sqrt[e]{\varpi}) &= (\widetilde{\mathrm{Frob}}_q g)(\widetilde{\mathrm{Frob}}_q^{-1}(\sqrt[e]{\varpi})) \\ &= \widetilde{\mathrm{Frob}}_q(\zeta \cdot (\widetilde{\mathrm{Frob}}_q^{-1}(\sqrt[e]{\varpi}))) = \zeta^q \cdot \sqrt[e]{\varpi} = g^q(\sqrt[e]{\varpi})\end{aligned}$$

となり, (2) の (a) がしたがう.

定理 3.4 の (2) の (b) については局所類体論を用いる. 詳しい議論については [Iw55] の Theorem 3 とその証明を参照のこと. □

注意 3.7. 定理 3.4 の (2) の (b) の記述やその証明の議論をより掘り下げた Jannsen-Wingberg の仕事 [JW82] によって $p \neq 2$ のときは混標数 $(0,p)$ の局所体の絶対ガロア群の生成元と関係式も完全にわかっている. このあたりの最も詳しい様子については教科書 [NSW] の 7 章を参照のこと.

ここから先は証明をしないが, さらに次のことがわかる.

定理 3.8. K を混標数 $(0,p)$ の局所体とし, $d = [K : \mathbb{Q}_p]$ とする.

(1) 素数 $l \neq p$ に対して G_K の最大 *pro-l* 商を $G_K(l)$ とすると,

$$G_K(l) \cong \begin{cases} \mathbb{Z}_l & \zeta_l \notin K \text{ のとき} \\ \widehat{\Gamma}^{(l)} & \zeta_l \in K \text{ のとき} \end{cases}$$

が成り立つ. 但し, Γ は定理 *3.4* において現れた群である. また, 前者のものは不分岐であることに注意したい.

(2) G_K の最大 *pro-p* 商を $G_K(p)$ とすると

$$G_K(p) \cong \begin{cases} \widehat{F}^{(p)}_{d+1} & \zeta_p \notin K \text{ のとき} \\ \widehat{F}^{(p)}_{d+2}/(\text{ある 1 つの関係式}) & \zeta_p \in K \text{ のとき} \end{cases}$$

が成り立つ. 但し, F_{d+1} は $d+1$ 文字の自由群とする. 後者のものは Demuskin 群というタイプの群である.

(3) L/K をガロア群が p-進リー群になるような完全分岐拡大とする. $G = \mathrm{Gal}(L/K)$ には 2 通りのフィルトレーションが入る. 片方は p 進リー群としての (Lazard などによって記述されている) p-進フィルトレーションである. もう一方は, [Ser] などに説明されている上付き分岐群によるフィルトレーションである. Sen によって 2 つの異なるフィルトレーションは同値であることが示されている.

上記定理の最初の二つの記述 (1),(2) は [NSW, Theorem 7.5.8] を参照のこと. 最後の記述 (3) は Sen の論文 [Sen] を参照のこと.

4. 代数体のガロア群と分解群について

K を代数体とする. 例えば以下のような状況によって, G_K の構造は有限体や局所体に比べて遥かに複雑である.

(1) 例えば以下のような (未解決の) 予想からも G_K は非常に複雑かつ豊富な構造をもつと考えられる.

予想 4.1 (ガロアの逆問題)**.** G を勝手な有限群とするとき, G は G_K の商となる.

(2) G_K は位相的に有限生成ではない.

補題 4.2. 今, 各素数 p に対して次の一対一対応がある.

$$\{K \text{ の素イデアル } \mathfrak{p} \text{ で } \mathfrak{p}|(p) \text{ なるもの }\} \Longleftrightarrow \{K \text{ の } \overline{\mathbb{Q}}_p \text{ への埋め込み }\}$$

証明のスケッチ. 簡単に補題の対応について補足しておきたい.
$\Longrightarrow$ の説明
$\mathfrak{p}|(p)$ なる素イデアル $\mathfrak{p}$ が与えられたとするとき $K_\mathfrak{p}$ を $\mathfrak{p}$-進位相での完備化とする. $K_\mathfrak{p}$ は p-進体より $\overline{\mathbb{Q}}_p$ の部分体と同一視される. よって $K \hookrightarrow K_\mathfrak{p} \hookrightarrow \overline{\mathbb{Q}}_p$ が引き起こされる.
$\Longleftarrow$ の説明 $K \hookrightarrow \overline{\mathbb{Q}}_p$ があったとき $\overline{\mathbb{Q}}_p$ 上の p 進付値を K に制限する. 以下, 各素点 $\mathfrak{p}$ を固定する. このとき, $\iota_\mathfrak{p} :\ \overline{K} \hookrightarrow \overline{\mathbb{Q}}_p = \overline{K}_\mathfrak{p}$ を決めるごとに

$$\iota_\mathfrak{p}^* :\ G_{K_\mathfrak{p}} \longrightarrow G_K$$

が引き起こされ, $G_{K_\mathfrak{p}}$ は $\mathfrak{p}$ での分解群と同一視される. 実際, $g \in \mathrm{Gal}(\overline{K}_\mathfrak{p}/K_\mathfrak{p})$ は部分体 $\overline{K} = \overline{\mathbb{Q}}$ の自己同型を引き起こす. $K \subset K_\mathfrak{p}$ より, $g \in \mathrm{Aut}(\overline{K})$ は K 上に自明な自己同型を引き起こす. よって, g は $\mathrm{Gal}(\overline{K}/K)$ の元を定める. □

L を K のガロア拡大で $\mathfrak{p}$ の上の素点で不分岐なものとする. このとき,

$$G_{K_\mathfrak{p}} \longrightarrow G_K \twoheadrightarrow \mathrm{Gal}(L/K)$$

は

$$G_{K_\mathfrak{p}} \twoheadrightarrow \mathrm{Gal}(K_\mathfrak{p}^{\mathrm{ur}}/K_\mathfrak{p}) \to \mathrm{Gal}(L/K)$$

と経由する. よって, 引き起こされる写像 $\mathrm{Gal}(K_\mathfrak{p}^{\mathrm{ur}}/K_\mathfrak{p}) \to \mathrm{Gal}(L/K)$ を再度 $\iota_\mathfrak{p}^*$ と記すことにすると $\mathrm{Frob}_q \in \mathrm{Gal}(K_\mathfrak{p}^{\mathrm{ur}}/K_\mathfrak{p})$ の像として $\iota_\mathfrak{p}^*(\mathrm{Frob}_q) \in \mathrm{Gal}(L/K)$ が定まる.

これを $\mathrm{Gal}(L/K)$ の $\mathfrak{p}$ **フロベニウス元**とよび $\mathrm{Frob}_{\mathfrak{p}}$ で記す.

まとめ

(1) $\mathfrak{p}$ が L/K において不分岐であるとすると, フロベニウス元 $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$ が定まる.
(2) $\iota_{\mathfrak{p}}$ を取り換えると $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$ も変わる. その意味で, $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$ は $\iota_{\mathfrak{p}}$ に依存しているが, 新しい $\mathrm{Frob}_{\mathfrak{p}}$ は以前のものと $\mathrm{Gal}(L/K)$ の内部自己同型でうつりあう. $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$ の共役類は $\iota_{\mathfrak{p}}$ に依存せずに well-defined である.

注意 4.3. (1) まとめの 2 番目の記述より, 特に L/K がアーベル拡大のときは (共役類でなく) フロベニウス元 $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$ 自身が well-defined である.
(2) 実は, Chebotarev の密度定理によって $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$ の共役元たちで生成される部分群 (但し, $\mathfrak{p}$ も L/K で不分岐な全ての素イデアルをわたる) は $\mathrm{Gal}(L/K)$ の中で稠密である. Chebotarev の密度定理のより正確な記述とそのガロア表現への応用は [C] で説明される.

局所体の場合と同様に K のアーベル拡大のガロア群はわかりやすい群によって制御される (大域類体論). それを説明するために, イデール群 $\mathbb{A}_K^\times$ を

$$\mathbb{A}_K^\times = \prod_{v:\ K\ \text{の素点}}{}' K_v^\times$$

で定める. ここで, 記号 $\prod'$ で表される積は制限直積というものであり, 各元 $(x_v)_v \in \mathbb{A}_K^\times$ は有限個の素点 v を除いて $x_v \in \mathcal{O}_{K_v}^\times$ となることを意味する. イデール群 $\mathbb{A}_K^\times$ は

$$\prod_{v:\ K\ \text{の無限素点}} K_v^\times \prod_{v:\ K\ \text{の有限素点}} \mathcal{O}_{K_v}^\times \subset \mathbb{A}_K^\times$$

に積位相を入れるような自然な位相によって局所コンパクトなアーベル群となっている. 今, $K^\times$ を $\mathbb{A}_K^\times$ に対角的に埋め込むとき $K^\times$ は $\mathbb{A}_K^\times$ の離散部分群となる. 商位相群 $\mathbb{A}_K^\times/K^\times$ を K のイデール類群とよぶ.

定理 4.4 (大域類体論)**.** K を代数体とするとき, 写像（相互写像）

$$\mathrm{rec}_K :\ \mathbb{A}_K^\times/K^\times \longrightarrow G_K^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

がある. rec_K は全射であってその核は $\mathbb{A}_K^\times/K^\times$ の単位元の連結成分に等しい. また, 勝手な有限次アーベル拡大 L/K に対して rec_K は同型

$$\mathbb{A}_K^\times/K^\times \mathrm{Norm}_{L/K}(\mathbb{A}_L^\times) \xrightarrow{\sim} \mathrm{Gal}(L/K)$$

をひきおこす.

予想 4.5 (Shafarevich)**.** $G_{K^{\mathrm{ab}}}$ は可算階数の自由群 $F_{\mathbb{N}}$ の副有限完備化 $\widehat{F_{\mathbb{N}}}$ と同型となるだろう.

定理 3.4 で現れたものと同じような道具立てを用いて次のことが知られている.

定理 4.6 (岩澤)**.** $G_{K^{\mathrm{ab}}}$ の最大可解商は可算階数の自由群 $F_{\mathbb{N}}$ の副有限可解完備化 $\widehat{F}_{\mathbb{N}}^{\mathrm{sol}}$ と同型となる.

また次のような予想もよく知られた予想であるが今のところ未解決である.

予想 4.7. Σ を K の素点の有限集合とし, K_Σ を Σ の外で不分岐な K の最大の代数拡大とする. このとき, $\mathrm{Gal}(K_\Sigma/K)$ は位相的に有限生成であろう.

最後になるが, 講演の準備の段階で局所体の絶対ガロア群の表示に関しての仕事の存在を指摘してくださった津田塾大学の松野一夫氏, 原稿に目を通して意見をくださった上智大学の角皆宏氏に感謝したい.

References

[AM] 足立恒雄, 三宅克哉, 類体論講義, 日評数学選書.
[C] 千田雅隆, ガロア表現の基礎 *II*, 本報告集.
[Fu] 藤崎源二郎, 体とガロア理論, 岩波書店
[Iw53] K. Iwasawa, *On solvable extensions of algebraic number fields*, Ann. Math. (2) 58, 548-572 (1953).
[Iw55] K. Iwasawa, *On Galois groups of local fields*, Trans. Amer. Math. Soc. 80 (1955), 448–469.
[JW82] U. Jannsen, K. Wingberg, *Die Struktur der absoluten Galoisgruppe* $\mathfrak{p}$*-adischer Zahlkorper*, Invent. Math. 70, 71-98 (1982).
[N] 永田雅宜, 可換体論, 裳華房
[Na] 中村健太郎, p 進ホッジ理論入門, 本報告集.
[NSW] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of number fields* Grundlehren der Mathematischen Wissenschaften. 323. Berlin: Springer. xv, 699 p.(2000).
[Ser] J-P. Serre, *Local Fields*, Graduate Texts in Mathematics, Springer.
[Sen] S. Sen, *Ramification in p-adic Lie extensions*, Invent. Math. 17, 44-50 (1972)
[Sha] S. Shatz, *Profinite groups, arithmetic, and geometry*, Annals of Mathematics Studies, No. 67. Princeton University Press, 1972.
[W] J-P. Wintenberger, *Le corps des normes de certaines extensions infinies de corps locaux*, Ann. Sci. Ec. Norm. Super. (4) 16, 59-89 (1983).
[Ya] 山内卓也, ガロア表現の基礎 *I*, 本報告集.