数理解析研究所講究録
1521 巻 2006 年 170-175

Construction of maximal unramified p-extensions with prescribed Galois group

近畿大学　理工学部　尾崎 学 (Manabu Ozaki)
Department of Mathematics, Kinki Univ.

1. 問題とその現状

代数体の最大不分岐拡大は，その研究の質・量・歴史の長さにも拘らず，未だ理解は不十分と言わざるを得ない状況で，多くの興味深く困難な問題が残されている．本稿では最大不分岐拡大のガロワ群，およびその最大 pro-p 商に関してのそのような問題の内より次のものを考察する：

問題 代数体（有限次，無限次）の最大不分岐 (p-) 拡大のガロワ群として現れる群を特徴付けよ．

この問題は二つの部分に分けられる：

問題 1 代数体（有限次，無限次）の最大不分岐 (p-) 拡大のガロワ群として現れるような群は一般にどのような性質を持つのかできるだけ詳しく記述せよ．

問題 2 代数体（有限次，無限次）の最大不分岐 (p-) 拡大のガロワ群として実際に現れる群（及びその性質）をできるだけ沢山挙げよ．

言い換えれば，問題 1 は代数体（有限次，無限次）の最大不分岐 (p-) 拡大のガロワ群として現れるような群の同型類の集合を上から評価する問題であり，問題 2 はそれを下から評価する問題である．

上の問題は考える代数体が有限次の場合と無限次代数体も含める場合とでは大きく異なるので，まず有限次代数体に関するこれらの問題の現状について述べたいと思う．以下では，有限次代数体 k と素数 p に対して，$\tilde{G}_k$ と $\tilde{G}_k(p)$ でそれぞれ k の最大不分岐拡大と最大不分岐 p-拡大のガロワ群を表すことにする．

まず問題 1 に関しては，類数の有限性と不分岐類体論により直ちに

事実 1 $\tilde{G}_k$（あるいは $\tilde{G}_k(p)$）の任意の開部分群 H に対し，H のアーベル化 H^{ab} は有限．

という事実が導かれる．これが問題1に対する歴史上最初の結果であろう．また$G=\tilde{G}_k(p)$については類体論により，そのgenerator rank $d(G)=\dim_{\mathbb{F}_p} G^{\mathrm{ab}}/p$（$=G$の極小生成系に含まれる元の個数）とrelation rank $r(G)=\dim_{\mathbb{F}_p} H^2(G,\mathbb{F}_p)$（$=G$を$d(G)$個の生成元で表示したときの関係式の個数）としたとき，

事実2 $d(\tilde{G}_k(p))$と$r(\tilde{G}_k(p))$は共に有限で，

$$0\leq r(\tilde{G}_k(p))-d(\tilde{G}_k(p))\leq r_1(k)+r_2(k)+\delta(k)$$

を満たす．ここで，$r_1(k)$, $r_2(k)$はそれぞれkの実無限素点，虚無限素点の個数で$\delta(k)$はkが1の原始p乗根を含むときは1でそうでないときは0を表す．

現在に至っても上の事実1，2以上の$\tilde{G}_k$の持つ一般の性質は知られていないと言っても良い．

また類体論成立当初より，有限次代数体の最大不分岐可解拡大（類体塔）は常に有限次であろうか？という問題があり長らく未解決であったが，1964年に至ってGolodとShafarevich [2]によって$\tilde{G}_k(p)$が無限群となるような有限次代数体kが構成された．しかし，無限群となる$\tilde{G}_k(p)$で，その構造が完全に決定されているようなものは現在のところ一つもない．

このように問題1に関して言えば$\tilde{G}_k$が持つ一般的な性質は事実1，2以外には知られていないが，次のような予想がある：

予想 (Fontaine-Mazur) 有限次代数体k，素数pと$n\in\mathbb{Z}_{\geq 0}$に対して，連続準同型

$$\rho:\tilde{G}_k(p)\longrightarrow GL_n(\mathbb{Z}_p)$$

の像は常に有限であろう．言い換えれば，$\tilde{G}_k(p)$のp-進解析商は常に有限であろう．

この予想の反例は知られていないし，反例が存在したとしても現時点ではそれを構成する手段が無い：現状で知られている無限群となる$\tilde{G}_k(p)$は，Golod-Shafarevichの定理

$$G\text{が pro-}p\text{-群},\ r(G)\leq\frac{d(G)^2}{4}\Longrightarrow G\text{は無限群}$$

(あるいはこれの精密版)の前提条件の不等式を満たす開部分群を持つもののみであるが，この条件をみたす群はp-進解析的ではない．

問題2に関して言えば，本稿では詳細を省略するが，多くの具体的な代数体の最大不分岐拡大，最大不分岐p-拡大のガロワ群が，それが有限の場合に決定されている．この研究の歴史も古く，例えば既に1934年にはScholzとTaussky [3]によって虚二次体$k=\mathbb{Q}(\sqrt{-4027})$について$\tilde{G}_k(3)$

の構造が決定されていた: $\tilde{G}_k(3) \simeq \langle x, y | \ (x,y)^{-1}y(x,y) = y^{-2}, x^3 = y^3 \rangle$ で，この群は位数 3^5 で交換子群が可換（つまり k の 3-類体塔は第 2 段で停止）となるような非可換有限群である．また，判別式の絶対値が比較的小さい虚二次体 k については（これらの虚二次体では $\tilde{G}_k$ は有限），山村 [6]，[7] によって $\tilde{G}_k$ の構造が決定されている．

問題 2 に関連して次のような事実も知られている：

定理 (Fröhlich [1]) 任意の有限群 G に対し，$\tilde{G}_k$ が G を剰余群に持つような有限次代数体 k が存在する．

この定理でいつでも $\tilde{G}_k \simeq G$ とできるかどうかは知られていないし，最大アーベル商に関してさえも，

類群問題 任意の有限アーベル群 A に対し，$\tilde{G}_k^{\mathrm{ab}} \simeq A$ となるような有限次代数体 k は存在するか？

という問題があるが未解決である．しかし，問題を素数 p-部分に限定すれば，肯定的に解決されている：

定理 (矢作 [5]) p を素数とする．任意に与えられたの有限アーベル p-群 A に対し $\tilde{G}_k(p)^{\mathrm{ab}} \simeq A$ となるような有限次代数体 k が存在する．

一方，k が無限次の代数体の場合は有限次の場合と随分状況が異なる．そもそも $\tilde{G}_k$, $\tilde{G}_k(p)$ は有限生成と限らないし，例え有限生成であっても有限表示とは限らない．しかし，特別な無限次代数体 k については良く研究がなされている．その最たるものは k が有限次代数体 F の $\mathbb{Z}_p$-拡大体の場合で，$\tilde{G}_k(p)^{\mathrm{ab}}$ については岩澤理論によりかなり深い理解が得られている: $\mathbb{Z}_p$-加群として

$$\tilde{G}_k(p)^{\mathrm{ab}} \simeq \mathbb{Z}_p^{\oplus\lambda} \oplus T, \quad \exists e \geq 0 : p^e T = 0.$$

(上の T は有限にも無限にもなり得る．また，より詳しく $\tilde{G}_k(p)^{\mathrm{ab}}$ の $\mathrm{Gal}(k/F)(\simeq \mathbb{Z}_p)$-加群としての構造についても分かる)．さらに最近の研究で $\tilde{G}_k(p)$ 自体の構造についても実例を含めて新たな事実が発見されつつある．

また，全円分体 $k = \mathbb{Q}(\mu_\infty)$ (μ_∞:すべての 1 の冪根）については内田 [4] により $\tilde{G}_k$ の最大 pro-solvable 商が可算無限生成の自由 pro-solvable 群（従って $\tilde{G}_k(p)$ は自由 pro-p-群）になることが示されている．この二つの例からも分かるように，無限次代数体については Fontaine-Mazur の予想の主張はそのままには成立しないことに注意しよう．

このように無限次代数体の場合には上の問題について現在までのところ多くは知られていないし，具体的な予想も無かったようである（無

限次代数体全体は一括して考察するには広範すぎると思われるので，当然とも言える）．以下本稿では $\tilde{G}_k(p)$ に対する問題2を考察して得られた結果について解説してゆく．

2. 結果

まず，有限次代数体に関しては次を示すことができる：

定理1 p を次の条件 C(p) を満たす素数とする：
C(p): 円の p 分体 $\mathbb{Q}(\mu_p)$ 上のの最大不分岐 p-拡大は有限次拡大．
このとき，任意の有限 p-群 G に対して，$\tilde{G}_k(p) \simeq G$ を満たす有限次代数体 k が存在する．

まず，素数に関する条件 C(p) について注意をしておく：この条件は望みの代数体を Kummer 拡大を用いて構成するための技術的仮定で本質的なものではないように思われる．従って，これは将来取り除かれることが望ましい．それから，p が正則ならばもちろん C(p) は成立するし．$\mathbb{Q}(\mu_p)$ のイデアル類群の p-部分が巡回群でも成立する．よって少なくとも 157 未満の素数 p について C(p) は成立する（$\mathbb{Q}(\mu_{157})$ のイデアル類群の 157-部分は $(\mathbb{Z}/157)^{\oplus 2}$ と同型）．また C(p) を満たさない素数 p の実例は今のところ知られていない．

定理1は素数 p に条件は付いているが，全ての有限 p-群が $\tilde{G}_k(p)$ として実際に現れるということで，問題2への部分的な回答になっている．また，これは前節で紹介した矢作の定理の拡張にもなっていることに注意しよう．

無限次代数体も含めた場合には次のことが分かる：

定理2 p を C(p) が成立するような素数とする．このとき任意の可算生成 pro-p-群 G に対して，$\tilde{G}_k(p) \simeq G$ を満たす代数体 k（有限次とは限らない）が存在する．

代数体のガロワ拡大のガロワ群は可算生成であることに注意すれば，この定理は $\tilde{G}_k(p)$ として原理的に現れる可能性のある pro-p-群は例外なく全て実際に現れるということを意味している．従って，これは $\tilde{G}_k(p)$ ($[k:\mathbb{Q}] \leq \infty$) に関する問題への完全な回答になっている．

定理2によって無限次代数体上の不分岐 p-拡大の研究への興味は少しも損なわれることはないと思われる．寧ろ，今後の為すべき研究の方向付けがより鮮明になったように感ぜられる：それは，全ての無限次代数体 k を考えれば全ての原理的に可能性のある群が $\tilde{G}_k(p)$ として現れるのであるが，考察すべき無限次代数体を十分に制限して考えれば，十分に面白い現象がそこでは起きているように思われるからである．特に有限次代数体の $\mathbb{Z}_p$-拡大体について考察することが重要である

と考える．それはそのような代数体が（$\mathbb{Z}_p$-拡大が無限次の真の中間体を持たないという意味で）“minimal な”無限次代数体であるから，古典的な岩澤理論で既に実証されているように有限次代数体の性質と密接に結びつくと考えられるからである．実際，有限次代数体の $\mathbb{Z}_p$-拡大体 k については，$\tilde{G}_k(p)$ はその $\mathbb{Z}_p$-拡大の岩澤 μ-不変量が 0 であれば有限生成であるが，すべての有限生成 pro-p-群が $\tilde{G}_k(p)$ として現れる訳ではなく，かなりの制約を受けているものと思われる．それがどのような制約であるかということが，有限次代数体の Fontaine-Mazur 予想などにも関連して大変興味深く，その解明が望まれる．

3. 定理の証明の方針

第 1 節で紹介したように（Fröhlich の定理），与えられた有限群をガロワ群に持つ不分岐拡大は比較的容易に構成できる：まず，分岐を無視してそのようなガロワ群を持つガロワ拡大を構成して，その後基礎体を拡大して分岐を消せば良い．困難なのはそうして作った不分岐拡大を最大不分岐拡大にすることであり，それができないから類群問題も未だに解けていないのである．しかし，問題を p-拡大に限定すれば，矢作の定理でもそうであったように，この困難は克服できる．

定理 1 の証明の概略を以下で述べる．定理 2 は定理 1 の証明から直ぐに従う．証明は非常に技術的なので，大雑把に方針を述べることにする．以下，p は条件 C(p) が成立するような素数とする．定理 1 の有限 p-群 G に対して，有限 p-群の全射からなる系列

$$1 = G_0 \longleftarrow G_1 \longleftarrow \cdots \longleftarrow G_n \longleftarrow G_{n+1} \longleftarrow \cdots \longleftarrow G_{r-1} \longleftarrow G_r = G$$

で $\ker(G_{n+1} \longrightarrow G_n) \simeq \mathbb{Z}/p$ $(0 \leq n \leq r-1)$ となるものが存在する．従って，

命題 1　$0 \leq n \leq r-1$ について，有限次代数体 k_n が $\tilde{G}_{k_n} \simeq G_n$，$\mu_p \subseteq k_n$ （＋ある技術的な条件）を満たすならば，有限次拡大 k_{n+1}/k_n で，$\tilde{G}_{k_{n+1}} \simeq G_{n+1}$ （＋ある技術的な条件）となるものが存在する．

を示せば，帰納法で $k = k_r$ が望みの有限次代数体となる．ここで，k_0 としては，条件 C(p) より $\mathbb{Q}(\mu_p)$ の最大不分岐 p-拡大体（もしくはその適当な有限次拡大体）をとることができることに注意しよう．

次の代数体の埋め込み問題からの定理が命題 1 を示す鍵となる：

定理　M/F を有限次代数体の不分岐ガロワ p-拡大とする．このとき任意の完全系列

$$1 \longrightarrow \mathbb{Z}/p \longrightarrow H \longrightarrow \mathrm{Gal}(E/F) \longrightarrow 1$$

に対して，p-次巡回拡大 L/M で，L/F は $\mathrm{Gal}(L/F) \simeq H$ を満たすガロワ拡大となるようなものが存在する．

この定理を，M/F を k_n の最大不分岐 p-拡大，$H = G_{n+1}$ として適用して得られる L/k_n は，もちろん不分岐にはならない．そこで，うまく k_n の拡大体 k_{n+1} を選んでやると，Lk_{n+1}/k_{n+1} が不分岐で $\mathrm{Gal}(Lk_{n+1}/k_{n+1}) \simeq \mathrm{Gal}(L/k_n) \simeq G_{n+1}$ となる．不分岐にするだけならば容易であるが，さらに Lk_{n+1}/k_{n+1} が最大不分岐拡大になるように，k_{n+1} を選ぶことができる．その方法に使われる原理を大雑把に説明しよう：類数が p と素な有限次代数体 F と F の素点の有限集合 S について F の最大 S-分岐 ($= S$ の外の素点は不分岐) 基本アーベル p-拡大 E/F を考える．中心拡大の理論より，$\mathrm{Gal}(E/F)$ が S に比べて“十分小さい”ならば（例えば巡回群），E の類数も p と素であることが示される．この原理を用いて不分岐拡大が必要以上に大きくなるのを抑制することができる．

定理 2 については，定理 1 で帰納的に行った拡大の構成のプロセスを無限に繰り返せばよい：位数が無限の可算生成 pro-p-群 G は，有限 p-群 G_n $(n \in \mathbb{Z}_{\geq 0}, G_0 = 1)$ と，核が $\mathbb{Z}/p$ と同型であるような全射準同型 $G_{n+1} \to G_n$ からなる射影系の射影的極限として表される．従って，定理 1 の証明と同様に有限次代数体の列

$$k_0 \subseteq k_1 \subseteq k_2 \subseteq \cdots \subseteq k_n \subseteq \cdots$$

で $\tilde{G}_{k_n} \simeq G_n$ となるようなものが構成できるので，$k = \bigcup_{n \geq 0} k_n$ とおけば，$\tilde{G}_k = \varprojlim \tilde{G}_{k_n} \simeq \varprojlim \tilde{G}_n = G$ となって，この k が求める代数体となる．

References

[1] A. Fröhlich, On non-ramified extensions with prescribed Galois group, Mathematika **9** (1962), 133–134.

[2] E. S. Golod, I. R. Shafarevich, On class field towers (Russian), Izv. Akad. Nauk SSSR, Ser. Mat. **28** (1964), 261-272.

[3] A. Scholz, O. Taussky, Die Hauptideale der kubischen Klassenkörper imaginärquadratischer Zahlkörper: ihre rechnerische Bestimmung und ihr Einfluß auf den Klassenkörperturm, J. Reine Angew. Math. **171** (1934), 19-41.

[4] K. Uchida, Galois groups of unramified solvable extensions, Tohoku Math. J. **34** (1982), 311-317.

[5] O. Yahagi, Construction of Number fields with prescribed l-class groups, Tokyo J. of Math. **1** (1978), 275–283.

[6] K. Yamamura, Maximal unramified extensions of imaginary quadratic number fields of small conductors, J. Theor. Nombres Bordeaux **9** (1997), 405–448.

[7] K. Yamamura, Maximal unramified extensions of imaginary quadratic number fields of small conductors II, J. Theor. Nombres Bordeaux **13** (2001), 633–649.

尾崎　学
近畿大学理工学部理学科
〒 577-8502 東大阪市小若江 3-4-1
e-mail: ozaki@math.kindai.ac.jp