RIMS Kôkyûroku Bessatsu
B86 (2021), 107–119

代数体の様々な分岐条件付き副 p 拡大について — 概説
On various pro-p-extensions of number fields with restricted ramification — a survey

By

水澤　靖 *
Yasushi Mizusawa

Abstract

This is a survey article of several topics on pro-p-extensions of number fields with restricted ramification, particularly concerning explicit presentations of various pro-p Galois groups by generators and relations.

§1. 序

素数 p に対して、ガロア群が副 p 群であるガロア拡大を副 p 拡大といい、有限次副 p 拡大を p 拡大という．代数体の副 p 拡大の魅力のひとつは、副 p 群の扱いやすさによって、高次や無限次の様子が比較的捉えやすいことではないかと思う．この概説論文では、その魅力が感じられるような話題を幾つか選び、著者による結果も交えて、その進展について概観したい．

代数体（有理数体 $\mathbb{Q}$ の有限次拡大）k の素点からなる有限集合 S と、k の代数拡大 K に対して、K の最大 S 外不分岐副 p 拡大を K_S で表し、$G_S(K) = \mathrm{Gal}(K_S/K)$ とおく．ここでは k の副 p 拡大の部分拡大のみを扱うため、k の如何なる副 p 拡大でも分岐しない素点 ([25, §11.2]) は、最初から S に含めなくてよい．そこで、S には次の 2 条件を仮定する．

- 有限素点 $v \in S$ が p 上の素イデアルでないならば、整数環 $\mathcal{O}_k$ の素イデアル v による剰余環 $\mathcal{O}_k/v$ の位数は $|\mathcal{O}_k/v| \equiv 1 \pmod{p}$ をみたす．

Received March 26, 2019. Revised June 1, 2019.
2020 Mathematics Subject Classification(s): Primary 11R32, Secondary 11R23, 11R37.
Key Words: *Pro-p-extension, Galois group, Restricted ramification.*
Partially supported by JSPS KAKENHI Grant Numbers JP17K05167, JP17K05168.
*名古屋工業大学 466-8555 愛知県名古屋市昭和区御器所町
Nagoya Institute of Technology, Gokiso, Showa, Nagoya, Aichi, 466-8555, Japan.
e-mail: mizusawa.yasushi@nitech.ac.jp

- S が無限素点 v を含むならば、$p=2$ かつ v は実素点である.

副 p ガロア群 $G_S(k)$ の閉部分群 H の固定体を $K=(k_S)^H$ とすると、$H=G_S(K)$ である. 特に H が開部分群のとき、その最大不分岐副 p アーベル商の型がわかれば、それと同型な、K のイデアル類群の p-Sylow 部分群 $A(K)$ の型もわかることになる. このように、$G_S(k)$ の副 p 群としての構造 (特に '群表示') が興味の対象となる.

副 p 群 G の閉部分群 H に対して、$\{h^p \mid h\in H\}$ を含む最小の閉部分群を H^p で表す. 閉部分群 H_1, H_2 に対して、$H_1\cup H_2$ を含む最小の閉部分群を H_1H_2 で表し、$\{h_1^{-1}h_2^{-1}h_1h_2 \mid h_1\in H_1, h_2\in H_2\}$ を含む最小の閉部分群を $[H_1,H_2]$ で表す. $\mathbb{F}_p$ 係数 1 次コホモロジーの次元 ('generator rank')

$$d_1=d_1(G)=\dim_{\mathbb{F}_p} H^1(G,\mathbb{F}_p)=\dim_{\mathbb{F}_p}(G/G^p[G,G])^\vee$$

が有限であるとき、G は副 p 群として有限生成である. ($^\vee$ は Pontryagin 双対を表す.) このことは、次の定理から従う (e.g., [7, Prop.1.9, Prop.1.13]).

定理 1.1 (Burnside の基定理). $d_1=d_1(G)$ が有限で、$\{g_iG^p[G,G]\}_{1\le i\le d_1}$ が $\mathbb{F}_p$ ベクトル空間 $G/G^p[G,G]$ の基底ならば、$\{g_i\}_{1\le i\le d_1}$ は G の最小生成系である. 特に、階数 d_1 の自由副 p 群 $F=\langle\{x_i\}_{1\le i\le d_1}\rangle^{\text{pro-}p}$ から G への準同型 $\pi: F\twoheadrightarrow G: x_i\mapsto g_i$ は全射である.

この副 p 群の定理の応用例として、次の基本的な定理 (e.g., [15]) の別証明が導かれる. p 進整数環 $\mathbb{Z}_p$ はしばしば加法群 (階数 1 の自由副 p 群) とみなす.

定理 1.2 (Weber, 岩澤). $\mathbb{Q}$ の円分 $\mathbb{Z}_p$ 拡大 $\mathbb{Q}^{\text{cyc}}$ の任意の有限次部分拡大の類数は p と素である.

証明. $G=G_{\{p\}}(\mathbb{Q})=\mathrm{Gal}(\mathbb{Q}_{\{p\}}/\mathbb{Q})$ とおく. Kronecker-Weber の定理から、$[G,G]$ の固定体は $\mathbb{Q}^{\text{cyc}}$ であり、全射準同型 $G\twoheadrightarrow G/[G,G]\simeq\mathbb{Z}_p$ が存在する. $d_1=1$ ゆえ、定理 1.1 から、全射準同型 $\mathbb{Z}_p\twoheadrightarrow G$ が存在する. よって $G\simeq\mathbb{Z}_p$ であり、特に $\mathbb{Q}^{\text{cyc}}=\mathbb{Q}_{\{p\}}$ である. $\mathbb{Q}_{\{p\}}$ の最大性から、$\mathbb{Q}^{\text{cyc}}$ 上には非自明な (p 外) 不分岐 p 拡大は存在しない. $\mathbb{Q}^{\text{cyc}}/\mathbb{Q}$ は p で完全分岐するので、主張を得る. □

定理 1.1 の全射準同型 π の核を $R=\mathrm{Ker}\,\pi$ とするとき、同型 $G\simeq F/R$ (またはそれを与える短完全列) を G の副 p 群としての (最小) 群表示という. R が $\{r_j\}_j$ を含む最小の F の閉正規部分群であるとき、群表示は $G\simeq\langle\{x_i\}_{1\le i\le d_1}\mid\{r_j\}_j\rangle^{\text{pro-}p}$ または

$$G\simeq\langle\, x_1,\dots,x_{d_1}\mid\dots,r_j,\dots\rangle^{\text{pro-}p}$$

とも表される. 2 次コホモロジーの次元 ('relation rank')

$$d_2=d_2(G)=\dim_{\mathbb{F}_p} H^2(G,\mathbb{F}_p)=\dim_{\mathbb{F}_p}(R/R^p[F,R])^\vee$$

が有限ならば、G は副 p 群として有限表示される．実際、$\{r_j R^p[F,R]\}_{1\le j\le d_2}$ が $\mathbb{F}_p$ ベクトル空間 $R/R^p[F,R]$ の基底であるとき、R は $\{r_j\}_{1\le j\le d_2}$ を含む最小の F の閉正規部分群である (e.g., [44, III§9])．Shafarevich [55] は、$G_S(k)$ が有限表示副 p 群であることを示すとともに、$d_2 = d_2(G_S(k))$ の上限と $d_1 = d_1(G_S(k))$ の明示公式を与えた．それでも関係式 $\{r_j\}_{1\le j\le d_2}$ を完全に記述することは一般には難しいが、特に $k = \mathbb{Q}$ の場合には、Fröhlich と Koch による次の定理がある (e.g., [25])．$\mathbb{Q}$ の無限素点を ∞ で表す．

定理 1.3 (Fröhlich, Koch)． $k = \mathbb{Q}$ とする．素数からなる有限集合 $S^* \subset \{p\} \cup \{1 + pz \,|\, 0 \le z \in \mathbb{Z}\}$ に対して、$p = 2 \notin S^*$ ならば素点 $v \in \{\infty\} \cup \{3 + 4z \,|\, 0 \le z \in \mathbb{Z}\} \setminus S^*$ をひとつ選んで $S = S^* \cup \{v\}$ とし、その他の場合は $S = S^*$ とする．このとき

$$d_1(G_S(\mathbb{Q})) - d_2(G_S(\mathbb{Q})) = |S \cap \{p\}| \in \{0, 1\}$$

であり、$G_S(\mathbb{Q})$ は群表示

$$G_S(\mathbb{Q}) \simeq F/R = \langle \{x_\ell\}_{\ell\in S^*} \,|\, \{x_\ell^\ell y_\ell x_\ell^{-1} y_\ell^{-1}\}_{\ell\in S^*\setminus\{p\}} \rangle^{\text{pro-}p}$$

を持つ．この $x_\ell R$ と $y_\ell R$ は、それぞれ ℓ 上素点の惰性群の元とフロベニウスに対応する．(y_ℓ は $\{x_\ell\}_{\ell\in S^*}$ で生成される自由副 p 群 F の元である．)

この種の群表示は 'Koch 型' と呼ばれる．絡み目群の Milnor 型群表示の類似として捉えられ、森下 [40, 41] らの研究に見られるように、数論的トポロジーの視点からも多くの発展をもたらした．一方、この群表示の概形だけからは判断できないが、$p \in S$ か否かで $G_S(\mathbb{Q})$ の構造は大きく異なる．Labute [26] は、$p \notin S$ かつ $G_S(\mathbb{Q})$ が mild 副 p 群[1] (特にコホモロジー次元が 2) である S の存在を初めて示した．その副 p 群の mildness の判定法は、Schmidt [53, Th.5.5] らによって一般化されている ([18, 'cup-product criterion'])．

次節以降では、この Koch 型群表示にまつわる幾つかの話題について、p 上素点の分岐がない場合 (§2) とある場合 (§3) に分けて概観する．

§2. p 上不分岐な場合

代数体 k の p 上素点 (素イデアル) 全体の集合を P とし、以下では $S \cap P = \emptyset$ と仮定する．このとき、$G_S(k)$ は fab 副 p 群である．副 p 群 G が fab であるとは、任意の開部分群 $H \subset G$ の副 p アーベル商 $H^{\text{ab}} = H/[H,H]$ が有限であることをいう．実際に開部分群 $H \subset G_S(k)$ に対して、$K = (k_S)^H$ の因子 $\prod_{v\in S} v$ を法とした射類群の p-Sylow 部分群 $A_S(K)$ は、H^{ab} と同型である．

副 p 群 G に対して、交換子群列 $\{G^{(n)}\}_{0\le n\in\mathbb{Z}}$ が $G^{(0)} = G$, $G^{(n+1)} = [G^{(n)}, G^{(n)}]$ で定まる．特に $G = G_\emptyset(k)$ に対して、対応する k の不分岐 p 拡大の列 $\{(k_\emptyset)^{G^{(n)}}\}_{0\le n\in\mathbb{Z}}$ は k の p-類体塔と呼ばれ、Golod と Shafarevich によって、無限列になり得ること、即ち $G_\emptyset(k)$ が無限群である p と k の存在が示された．それを導いた群論的結果は、現在では次のように一般化されている (e.g., [7, Th.D1])．

[1] F の次数付き Lie 環化の中で R が '強い独立性' を持つ副 p 群 $G \simeq F/R$ として定義される．

命題 2.1 (Golod-Shafarevich 不等式)**.** p 進解析的副 p 群 G に対して、$d_1(G) \geq 2$ ならば、$d_2(G) \geq \frac{1}{4}d_1(G)^2$ が成り立つ.(等号は $d_1(G) = 2$, $d_2(G) = 1$ のときに限る.)

副 p 群 G が p 進解析的(p 進 Lie 群)であるための必要十分条件は、$G \subset \mathrm{GL}_n(\mathbb{Z}_p)$ となる n が存在することである (e.g., [7, Interlude A]). 特に、有限 p 群は p 進解析的である. この不等式を $G_\emptyset(k)$ に適用すると、イデアル類群の p-階数 $d_1(G_\emptyset(k)) = \dim_{\mathbb{F}_p} A(k)/A(k)^p$ が単数群 $\mathcal{O}_k^\times$ の p-階数に比べて十分に大きいならば、$G_\emptyset(k)$ は p 進解析的でないこと(特に無限群であること)が導かれる. さらに $G_\emptyset(k)$ だけでなくその商に関しても、より一般に次のように予想されている (e.g., [44]).

予想 2.2 (Fontaine-Mazur)**.** $S \cap P = \emptyset$ のとき、$G_S(k)$ は p 進解析的副 p 無限商を持たない. 即ち ([7, §8 Ex.7])、任意の n に対して、表現 $\rho : G_S(k) \to \mathrm{GL}_n(\mathbb{Q}_p)$ の像は有限である.

このように、$G_S(k)$ として現れ得る副 p 群が制限される一方で、次の定理が示されている.

定理 2.3 (尾崎 [50])**.** 任意の有限 p 群が $G_\emptyset(k)$ として現れ得る. 即ち任意の有限 p 群 G に対して、$G_\emptyset(k) \simeq G$ である代数体 k が存在する.

他方、$\mathcal{O}_k^\times$ の p-階数(または拡大次数 $[k : \mathbb{Q}]$)を指定すると、Golod-Shafarevich 不等式から、$G_\emptyset(k)$ として現れ得る有限 p 群 G の $d_1(G)$ も制限される. そのため $G_S(k)$ が有限 p 群になる場合に限っても、次の問題が考えられてきた.

問題 2.4. 与えられた k と S に対して、$G_S(k)$ の同型類を決定せよ.

この問題には、「指数の小さな開部分群のアーベル商から、元の副 p 群を特定する」という方法が、類体塔の研究が始まった頃からもよく使われてきた ([58] etc.). $G_S(k)$ に適用すると、「低次の拡大から、未だ見ぬ(具体的に構成されていない)高次の拡大の様子がわかる」ことになる. 現在でも、次の命題に基づいた多くの結果がある.

命題 2.5 (e.g., [23, 58])**.** 副 2 群 G に対して、G^{ab} が $[2, 2]$ 型アーベル群であるための必要十分条件は、G が次のいずれかと同型であることである: Klein 四元群 $[2, 2]$, 位数 $2^n \geq 2^3$ の二面体群 D_{2^n}, 副 2 無限二面体群 D_{2^∞}, 四元数群 Q_8, 位数 $2^n \geq 2^4$ の一般四元数群 Q_{2^n}, 位数 $2^n \geq 2^4$ の準二面体群 SD_{2^n}.

2-類体塔のガロア群 $G_\emptyset(k)$ に適用すると、もし $A(k) \simeq [2, 2]$ ならば、$G_\emptyset(k)$ は上のいずれかの有限 2-群と同型であることになる. Kisilevsky [23] は、k の不分岐 2 次拡大 K でのイデアルの単項化の様子と $A(K)$ から、その同型類を特定できることを示した.

以下で述べる O'Brien [46] の p 群生成アルゴリズムの応用は、この種の方法が発展したものである. 副 p 群 G に対して、p-降中心列 $\{P_n(G)\}_{0 \leq n \in \mathbb{Z}}$ が $P_0(G) = G$, $P_{n+1}(G) = P_n(G)^p[P_n(G), G]$ で定まる. 副 p 群の扱いやすさのひとつとして、$\bigcap_{n=0}^{\infty} P_n(G) = \{1\}$ である. そのため G が有限生成ならば、p-降中心列は $1 \in G$ の開近傍系をなす ([44, Prop.3.8.2]). 有限 p 群 G に対して、$\min\{0 \leq n \in \mathbb{Z} \,|\, P_n(G) \simeq 1\}$ を G の p-class という.

定理 2.6 (O'Brien [46])**.** 次のようなアルゴリズムが存在する.

入力 : *p-class* が i である有限 p 群 G_i

出力 : *p-class* が $i+1$ かつ $G_{i+1}/P_i(G_{i+1}) \simeq G_i$ である有限 p 群 G_{i+1} の同型類すべて

このアルゴリズムは GAP [17] にも ANUPQ package [16] として実装されている. 初等アーベル p 群 $G_1 = (\mathbb{Z}/p\mathbb{Z})^d$ から始めて帰納的に適用すれば、$d_1(G) = d$ である有限 p 群 G すべての同型類のリストを構成してゆくことができる. Boston と Leedham-Green は、このアルゴリズムを初めて問題 2.4 に応用した ([3]). 2-類体塔の長さ $\min\{0 \le n \in \mathbb{Z} \,|\, G_\emptyset(k)^{(n)} \simeq 1\}$ が 3 である虚 2 次体 k を初めて発見した Bush [5] の結果など、追随する多くの結果 ([4, 6, 8, 28, 45, 57] etc.) があるが、ここでは次の定理を例として挙げる.

定理 2.7 ([34])**.** $p = 2$, $k = \mathbb{Q}$ とし、素数 ℓ, q, r は次をみたすとする: $\ell \equiv 5 \pmod 8$, $q \equiv r \equiv 3 \pmod 4$, $(qr)^{(\ell-1)/4} \equiv 1 \pmod \ell$, $|A(\mathbb{Q}(\sqrt{\ell qr}))| = 4$. このとき $S = \{\ell, q, r\}$ に対して、$G_S(\mathbb{Q})$ は位数 512, 交換子群列の長さ 3, *p-class* 6 の有限 2 群であり、抽象群としての群表示

$$G_S(\mathbb{Q}) \simeq \langle\, a, b \,|\, a^4b^{-2}a^{-1}b^2a,\ b^2a^{-1}b^{-1}aba^{-1}b^{-1}a^{-1}ba^6 \,\rangle$$

を持つ.(この群の同型類の代表を G_6^+ で表す.)

証明は、[3] およびその拡張である Eick-Koch [8] の結果と同じ方針である. 次の補題によって、$G_S(\mathbb{Q})$ の商になり得る有限 2 群だけを、p 群生成アルゴリズムで構成してゆく.

補題 2.8 ([3] etc.)**.** 定理 1.3 の状況において $p \notin S$ とし、$\mathbb{Q}_S$ の p^n 次部分アーベル拡大 $K/\mathbb{Q}$ 全体の集合を $\mathcal{K}_n$ とする. p-class が 2 以上の有限 p 群 G に対して、G/H が位数 p^n のアーベル群であるような G の正規部分群 H 全体の集合を $\mathcal{H}_n$ とする. このとき、$d_1(G) = d_1(G_S(\mathbb{Q}))$ かつ G が $G_S(\mathbb{Q})$ の商と同型ならば、以下が成り立つ.

- I_n. 次をみたす単射 $\varphi_n : \mathcal{H}_n \hookrightarrow \mathcal{K}_n$ が存在する: $K = \varphi_n(H)$ ならば、$G/H \simeq \mathrm{Gal}(K/\mathbb{Q})$ であり、かつ H^{ab} は $A_S(K)$ の商と同型.
- II. G は次のような生成系 $\{\mathsf{x}_\ell\}_{\ell \in S^*}$ を持つ: $\mathsf{x}_\ell^{1+|\mathbb{Z}_p/(\ell-1)\mathbb{Z}_p|}\mathsf{y}_\ell\mathsf{x}_\ell^{-1}\mathsf{y}_\ell^{-1} = 1$ をみたす $\mathsf{y}_\ell \in G$ が各 $\ell \in S^*$ に対して存在する.
- III. G の p-multiplicator 階数 $\mu(G) = \dim_{\mathbb{F}_p} H_2(G, \mathbb{F}_p)$ と 'nuclear' 階数 $\nu(G)$ (e.g., [46]) は、不等式 $\mu(G) - \nu(G) \le d_1(G_S(\mathbb{Q}))$ をみたす.

$\mathsf{II}, \mathsf{III}$ は定理 1.3 から導かれ、特に III の不等式は、$d_1(G_S(\mathbb{Q})) = d_2(G_S(\mathbb{Q}))$ であることから導かれる ([3, Lemma]). G_{i+1} が I_n をみたすならば、その商である $G_i \simeq G_{i+1}/P_i(G_{i+1})$ も I_n をみたす. 定理 2.7 の実際の証明のステップは、以下のとおりである.(計算には [9, 16, 17] を用いた.)

i. 各 $K \in \bigcup_{n\leq 2} \mathcal{K}_n$ に対して、次の完全列を用いて $A_S(K)$ の型を計算しておく.

$$\mathcal{O}_K^\times \longrightarrow \prod_{v\in S}(\mathcal{O}_K/v)^\times \otimes \mathbb{Z}_2 \longrightarrow A_S(K) \longrightarrow A(K) \longrightarrow 0$$

ii. $G_1 = [2,2]$ とおく. p-class $i \geq 2$ に関して帰納的に、I_0, I_1, I_2, II, III をみたす有限 2 群 G_i を構成してゆく. すると、そのような p-class 7 の有限 2 群 G_7 は存在しなかった.[2]

iii. 得られた p-class $i \leq 6$ の有限 2 群 G_i のうち、$d_1(G_i) = d_2(G_i)$ をみたすものは、よく似た 2 つの群 G_6^+, G_6^- のみであった. $G_S(\mathbb{Q}) \simeq G_6^+$ または $G_S(\mathbb{Q}) \simeq G_6^-$ である.

iv. $G_S(\mathbb{Q}) \simeq G_6^+$ なら $U^{\mathrm{ab}} \simeq [2,2,4]$, $G_S(\mathbb{Q}) \simeq G_6^-$ なら $U^{\mathrm{ab}} \simeq [4,4]$ であるような指数 8 の部分群 $U \subset G_S(\mathbb{Q})$ が存在する. S 上素点の分岐と分解の様子から、$K = (\mathbb{Q}_S)^U$ が特定でき、$A_S(K) \not\simeq [4,4]$ であることがわかる. よって $G_S(\mathbb{Q}) \simeq G_6^+$ である.

v. G_6^+ の polycyclic 群としての関係式を G_6^- のそれと比較したところ、異なる箇所は 2 本だけであった. その 2 本だけを関係式とする階数 2 の自由群の商を構成してみたら、副 2 完備化せずとも G_6^+ と同型であった.[3]

この証明の要点は、有限 p 群を構成してゆく際に、条件 I_n, II, III をみたさないものを省いてゆくことである. 特に II, III の条件を課すことによって、残る候補が少数に絞られる. Boston [2] が 'NT 群' と呼んでいるように、Koch 型群表示は $G_S(\mathbb{Q})$ の構造を強く特徴付けていると考えられる.

§3. p 上(円分的)分岐する場合

前節と同じく $S \cap P = \emptyset$ であるとし、$\Sigma = S \cup P$ とおく. $\Sigma = P$ のとき、$G_\Sigma(k)$ は自由副 p 群や中心自明 (center-free) 副 p 群にもなり得る (e.g., [11, 60, 61]). $\Sigma \neq P$ であっても、例えば $p \neq 2$ かつ $k = \mathbb{Q}$ のとき、$G_\Sigma(\mathbb{Q})$ の閉部分群 $G_\Sigma(\mathbb{Q}^{\mathrm{cyc}})$ は有限生成自由副 p 群である ([44, Cor.10.5.7]). このように $G_\Sigma(k)$ の構造は、fab 副 p 群 $G_S(k)$ よりも比較的捉えやすい.

この捉えやすさの由来のひとつは、k_Σ が k の円分 $\mathbb{Z}_p$ 拡大 $k^{\mathrm{cyc}} = k\mathbb{Q}^{\mathrm{cyc}}$ を含むことであると考えられる. すると、そのような最も堅い分岐条件を持つ副 p 拡大、即ち p 上円分的分岐 ('cyclotomically ramified at p') かつ Σ 外不分岐な最大副 p 拡大 $(k^{\mathrm{cyc}})_S/k$ のガロア群

$$\widetilde{G}_S(k) = \mathrm{Gal}((k^{\mathrm{cyc}})_S/k)$$

が興味の対象となる. 実際、$G = \widetilde{G}_S(k)$ の閉部分群 $H = G_S(k^{\mathrm{cyc}})$ のアーベル商 $H^{\mathrm{ab}} \simeq \varprojlim A_S(k_n)$ が S 分岐岩澤加群であり、$\Gamma = G/H \simeq \mathrm{Gal}(k^{\mathrm{cyc}}/k)$ が作用する. k_n/k は

[2] もし $G_S(\mathbb{Q})$ が無限群だったなら、このステップは永遠に終了しない.

[3] もし G_6^- が候補に残っていなかったら、G_6^+ の抽象群表示の発見は困難であった.

k^{cyc}/k の p^n 次部分拡大を表し、$\varprojlim$ はノルム写像による射影極限である．$S=\emptyset$ のとき、岩澤類数公式 (e.g., [15]) や次の定理 3.1 は、副 p 群 $G/[H,H]$ の構造、即ち H^{ab} の $\mathbb{Z}_p[[\Gamma]]$ 加群構造から導かれていた．

定理 3.1 (福田 [14])．　k^{cyc}/k で任意の分岐素点が完全分岐し、かつ $|A(k)|=|A(k_1)|$ ならば、すべての $n\geq 0$ に対して $A(k_n)\simeq A(k)$ であり、特に $G_\emptyset(k^{\mathrm{cyc}})^{\mathrm{ab}}\simeq A(k)$ である．

この定理は、「低次の拡大から高次（無限次）の拡大の様子がわかる」例でもあり、円分でない $\mathbb{Z}_p$ 拡大でも同様に成立する．特に円分 $\mathbb{Z}_p$ 拡大の場合には、以下のような予想がある (e.g., [15] etc.)．

予想 3.2 (岩澤)．　$d_1(G_S(k^{\mathrm{cyc}}))$ は有限（即ち、$G_S(k^{\mathrm{cyc}})$ は有限生成副 p 群）．

予想 3.3 (Greenberg [20])．　k が総実ならば、$|G_\emptyset(k^{\mathrm{cyc}})^{\mathrm{ab}}|$ は有限．

すべての総実な k に対する予想 3.3 は、$G_\emptyset(k^{\mathrm{cyc}})$ が fab 副 p 群であることも導く (e.g., [31, Prop.1])．円分 $\mathbb{Z}_p$ 拡大 k^{cyc}/k で完全分解する有限素点は存在しないため、すべての k に対する予想 3.2 は、$S=\emptyset$ の場合に帰着される．[4] 特に、$k/\mathbb{Q}$ がアーベル拡大ならば予想 3.2 は肯定的である (Ferrero-Washington [10])．その予想 3.2 が肯定的であるとき、H^{ab} だけでなく、$H=G_S(k^{\mathrm{cyc}})\simeq\varprojlim G_S(k_n)$ そのものを '副 p-Γ 作用素群'([44, Def.4.3.8]) として扱うことによって、次の非アーベル岩澤公式が導かれる．この $\varprojlim$ は制限写像による射影極限である．副 p 群 G に対して、降中心列 $\{C_i(G)\}_{0\leq i\in\mathbb{Z}}$ が $C_0(G)=G$, $C_{i+1}(G)=[C_i(G),G]$ で定まる．

定理 3.4 (尾崎 [49])．　$d_1(G_S(k^{\mathrm{cyc}}))$ が有限ならば、各 $1\leq i\in\mathbb{Z}$ に対して、

$$|G_S(k_n)/C_i(G_S(k_n))|=p^{\lambda_{i,S}(k^{\mathrm{cyc}}/k)n+\nu_{i,S}(k^{\mathrm{cyc}}/k)}\quad(\forall\, n\gg 0)$$

であるような整数 $\lambda_{i,S}(k^{\mathrm{cyc}}/k)$, $\nu_{i,S}(k^{\mathrm{cyc}}/k)$ が存在する．[5]

その $G_S(k^{\mathrm{cyc}})$ の構造に関しても、次の問題が提起されている (cf. [48, 49] etc.)．

問題 3.5.　$d_2(G_S(k^{\mathrm{cyc}}))$ は有限か？（即ち、$G_S(k^{\mathrm{cyc}})$ は有限表示副 p 群か？）

この問の答えが肯定的ならば、$G_S(k^{\mathrm{cyc}})$ の構造の捉えやすさも期待できるが、その一方で、次の問題も提起（現在では予想）され、'一般 Greenberg 予想' からの肯定的結果もある (e.g., [12])．

予想 3.6 (尾崎)．　$d_1(G_\emptyset(k^{\mathrm{cyc}}))\geq 2$ ならば $d_2(G_\emptyset(k^{\mathrm{cyc}}))\neq 0$（即ち、$G_\emptyset(k^{\mathrm{cyc}})$ は非可換自由副 p 群でない）．

---

[4] 全射 $G_S(k^{\mathrm{cyc}})^{\mathrm{ab}}\to G_{S\cap\{v|\infty\}}(k^{\mathrm{cyc}})^{\mathrm{ab}}$ の核は $\mathbb{Z}_p$ 上有限生成である．$S\cap\{v|\infty\}\neq\emptyset$ なら $p=2$ であるが、$(k^{\mathrm{cyc}})_{S\cap\{v|\infty\}}\subset(k(\sqrt{-1})^{\mathrm{cyc}})_\emptyset$ ゆえ、$\sqrt{-1}\in k$ かつ $S=\emptyset$ である場合の予想 3.2 の主張から、$\sqrt{-1}\notin k$ である場合の予想 3.2 の主張が導かれる．

[5] [49] では $S=\emptyset$ としているが、仮定 $S\cap P=\emptyset$ から $G_S(k_n)$ は fab 副 p 群ゆえ、同じ議論で証明される．

$S \neq \emptyset$ でも $G_S(k^{\mathrm{cyc}})$ は非可換自由副 p 群でないと予想されるが、より強く、階数 3 以上の Demuškin 副 p 群でもないことを予感させる結果もある ([21])．このように $G_S(k^{\mathrm{cyc}})$ の具体的な構造に関する結果も多々ある ([13, 22, 29, 30, 31, 33, 35, 37, 38, 42, 43, 47, 52, 56] etc.) が、その中でも、$\widetilde{G}_\emptyset(k)$ の群表示まで明示した次の例がある．

定理 3.7 ([32])． $p = 2$ とし、$\ell_1 \equiv 3 \pmod 8$, $\ell_2 \equiv 7 \pmod{16}$ をみたす素数 ℓ_1, ℓ_2 に対して $k = \mathbb{Q}(\sqrt{-\ell_1\ell_2})$ とおく．このとき、$G_\emptyset(k^{\mathrm{cyc}})$ と $\widetilde{G}_\emptyset(k)$ はそれぞれ次の群表示を持つ：

$$G_\emptyset(k^{\mathrm{cyc}}) \simeq \langle\, a, b, c \,|\, ab^{-1}ab,\ a^{-2}b^{-1}c^{-1}bc,\ a^{-1}c^{-1}ac \,\rangle^{\text{pro-2}},$$

$$\widetilde{G}_\emptyset(k) \simeq \left\langle a, b, \gamma \;\middle|\; \begin{array}{l} ab^{-1}ab,\ a^{-2}b^{-1}\gamma b^{-1}\gamma^{-1}b\gamma b\gamma^{-1},\ a^{-1}\gamma b^{-1}\gamma^{-1}bab^{-1}\gamma b\gamma^{-1}, \\ a^{-1}\gamma^{-1}a\gamma,\ a^{C_1}b^{-C_0}(\gamma b^{-1}\gamma^{-1}b)^{C_1}b^{-1}\gamma b\gamma b^{-1}\gamma^{-1}b\gamma^{-1} \end{array} \right\rangle^{\text{pro-2}}.$$

この $C_0, C_1 \in 2\mathbb{Z}_2$ は不分岐岩澤加群 $X = G_\emptyset(k^{\mathrm{cyc}})^{\mathrm{ab}}$ の岩澤多項式 $\Delta(T) = T^2 + C_1T + C_0$ の係数であり、包含 $G_\emptyset(k^{\mathrm{cyc}}) \subset \widetilde{G}_\emptyset(k)$ は $c \mapsto b^{-1}\gamma b\gamma^{-1}$ で与えられる．

この群表示の例は Koch 型からは遠いが、Salle [51] は一般に、$\widetilde{G}_S(k)$ が有限表示副 p 群であることを $d_1(\widetilde{G}_S(k))$, $d_2(\widetilde{G}_S(k))$ の Shafarevich 型公式とともに示した．Golod-Shafarevich 不等式と合わせると、$|\Sigma|$ が単数群 $\mathcal{O}_k^\times$ の p-階数に比べて十分に大きいならば、$\widetilde{G}_S(k)$ も $G_S(k^{\mathrm{cyc}})$ も p 進解析的でないことが導かれる ([1, Cor.3.11], [36, Cor.2.7])．さらに Blondeau, Lebacque, Maire [1] は cup-product criterion を用いて、$\widetilde{G}_S(k)$ が mild 副 p 群（特にコホモロジー次元が 2）である例も与えた．これらの結果に追随して、$\widetilde{G}_S(k)$ の Koch 型群表示も得られており、特に $k = \mathbb{Q}$ のとき次の定理が成り立つ．

定理 3.8 ([36])． $k = \mathbb{Q}$ とし、$\ell_0 = p$, $1 \leq d \in \mathbb{Z}$, $\infty \notin S^* = \{\ell_1, \ldots, \ell_d\} \neq \emptyset$ とする．$p \neq 2$ ならば $S = S^*$ とし、$p = 2$ ならば $S = S^* \cup \{\infty\}$ とする．このとき $d_1(\widetilde{G}_S(\mathbb{Q})) = d + 1$ であり、$\widetilde{G}_S(\mathbb{Q})$ は群表示

$$\widetilde{G}_S(\mathbb{Q}) \simeq F/R = \langle\, x_0, x_1, \ldots, x_d \,|\, x_0y_0x_0^{-1}y_0^{-1}, x_1^{\ell_1}y_1x_1^{-1}y_1^{-1}, \ldots, x_d^{\ell_d}y_dx_d^{-1}y_d^{-1} \,\rangle^{\text{pro-}p}$$

を持つ．この x_iR と y_iR は、それぞれ ℓ_i 上素点の惰性群の元とフロベニウスに対応する．

定理 1.3 の群表示がそうであった ([25, 40, 41] etc.) ように、この定理 3.8 の群表示も、素数の絡み数（まつわり数, linking number）l_{ij} を用いて

$$y_i \equiv \textstyle\prod_{j=0}^{d} x_j^{l_{ij}} \bmod [F, F] \tag{3.1}$$

であるように定めることができる．その l_{ij} は次のように定義される： 各 $j \neq 0$ に対して素数 ℓ_j の原始根 α_j を固定し、$p = 2$ なら $\alpha_0 = 5^{-1}$, $p \neq 2$ なら $\alpha_0 = (1+p)^{-1}$ とおく．$i \neq j \neq 0$ なら、l_{ij} は $\ell_i^{-1} \equiv \alpha_j^{l_{ij}} \mod \ell_j$ かつ $0 \leq l_{ij} < \ell_j - 1$ をみたす離散対数である．$i \neq j = 0$ なら、l_{ij} は p 進対数を用いて $l_{i0} = \log_p(\ell_i^{-1})/\log_p(\alpha_0) \in \mathbb{Z}_p$ で定義する．$i = j$ のときは $l_{ij} = 0$ とする．このとき x_i, y_i は、$\bmod [F, F]$ でイデールとしての α_i, ℓ_i に対応するように定めることになる ([36, §3.2])．

S 外不分岐アーベル p 拡大 $K/\mathbb{Q}$ に対して、$G_\emptyset(K)$ は $G_S(\mathbb{Q})$ の部分商であり、$G_\emptyset(K^{\mathrm{cyc}})$ は $\widetilde{G}_S(\mathbb{Q})$ の部分商である．$[K:\mathbb{Q}]=p$ のとき、Fröhlich と Koch は $G_\emptyset(K)$ の群表示を $G_S(\mathbb{Q})$ の Koch 型群表示から導いた．その方法 ([24, 25, 59]) に倣うと、以下のような応用が得られる．まず、次の定理の別証明が得られる ([39])．そこに現れる条件 (3.2) は、$G_S(\mathbb{Q})$ や $\widetilde{G}_S(\mathbb{Q})$ が mild 副 p 群となる十分条件 ('circular set', e.g., [27]) の一部に似通っている．

定理 3.9 (山本 [62, 63])．　定理 *3.8* と *(3.1)* の状況で、$\ell_0=p\neq 2$, $S=\{\ell_1,\ell_2\}$ とし、唯一の S 外不分岐 p^2 次基本アーベル拡大を $K/\mathbb{Q}$ とする．このとき、$G_\emptyset(K^{\mathrm{cyc}})\simeq 1$ であるための必要十分条件は、絡み数が

$$l_{01}l_{12}l_{20}\not\equiv l_{02}l_{21}l_{10}\pmod{p} \tag{3.2}$$

をみたすことである．

$p=2$ のときは、定理 1.3 の群表示でもそうである ([40, 41]) ように、$y_i \bmod [[F,F],F]$ を記述することで、$\widetilde{G}_S(\mathbb{Q})$ やその部分商 $G_{\{\infty\}}(K^{\mathrm{cyc}})$ を詳しく調べることができる．実際、

$$y_i\equiv x_d^{l_{id}}\cdots x_1^{l_{i1}}x_0^{l_{i0}}\textstyle\prod_{a<b}(x_ax_bx_a^{-1}x_b^{-1})^{c_{iab}}\mod [[F,F],F] \tag{3.3}$$

と表したとき、$l_{ab}\equiv l_{ba}\equiv l_{ia}\equiv l_{ib}\equiv 0\pmod 2$ である a,b について、$(-1)^{c_{iab}}=[\ell_a,\ell_b,\ell_i]=\pm 1$ は Rédei 記号である (e.g., [36, Prop.3.7])．$\ell_j\equiv 3\pmod 4$ なら $\ell_j^*=-\ell_j$ とし、そうでないなら $\ell_j^*=\ell_j$ とする．$\mathbb{Q}(\sqrt{\ell_a^*\ell_b^*})$ 上唯一の ∞ 外不分岐 4 次巡回拡大 $L_{a,b}$ は $\mathbb{Q}$ 上 D_8 拡大であり、Rédei 拡大と呼ばれる．このとき $[\ell_a,\ell_b,\ell_i]=1$ であるための必要十分条件は、ℓ_i 上の素点が $L_{a,b}/\mathbb{Q}(\sqrt{\ell_a^*\ell_b^*})$ で完全分解することである．Rédei 記号は、特別な場合には 4 冪剰余記号で記述できるため、副 p Fox 微分 (e.g., [41]) の計算と合わせることによって、次の系が得られる．平方剰余記号が $\left(\frac{z}{\ell}\right)=1$ である z と素数 $\ell\equiv 1\pmod 4$ に対して、4 冪剰余記号は $\left(\frac{z}{\ell}\right)_4=\pm 1\equiv z^{(\ell-1)/4}\pmod\ell$ で定まる．

系 3.10 ([36])．　定理 *3.8* と *(3.1), (3.3)* の状況で、$\ell_0=p=2$, $S=\{\ell_1,\ell_2,\infty\}$ とし、$K=\mathbb{Q}(\sqrt{\ell_1^*\ell_2^*})$ とする．このとき、$\gamma=(x_0R)|_{K^{\mathrm{cyc}}}$ の $X=G_{\{\infty\}}(K^{\mathrm{cyc}})^{\mathrm{ab}}$ への作用に関する *monic* な特性多項式（岩澤多項式）$\Delta(T)=\det(1+T-\gamma\,|X\otimes\mathbb{Q}_p)\equiv T^{\deg\Delta}\pmod p$ について、以下が成り立つ：

- $\ell_1\equiv 9\pmod{16}$, $\ell_2\equiv 3\pmod 8$, $\left(\frac{\ell_2}{\ell_1}\right)=1$ ならば、$c_{012}+c_{201}\equiv\frac{1}{2}\left(1+\left(\frac{2}{\ell_1}\right)_4\right)\pmod 2$ かつ $\Delta(T)\equiv T^2+\left(1+\left(\frac{2}{\ell_1}\right)_4\right)T+2\left(1-\left(\frac{\ell_2}{\ell_1}\right)_4\right)\pmod{4\mathbb{Z}_2T+8\mathbb{Z}_2}$.
- $\ell_1\equiv 7\pmod{16}$, $\ell_2\equiv 5\pmod 8$, $\left(\frac{\ell_1}{\ell_2}\right)=1$ ならば、$c_{012}+c_{201}\equiv 0\pmod 2$ かつ $\Delta(T)\equiv T^2+2\left(1-\left(\frac{-\ell_1}{\ell_2}\right)_4\right)\pmod{4\mathbb{Z}_2T+8\mathbb{Z}_2}$.

さらに、次が成り立つ：

- $\ell_1\equiv 7\pmod{16}$, $\ell_2\equiv 3\pmod 8$ ならば、$G_{\{\infty\}}(K^{\mathrm{cyc}})\simeq D_{2^\infty}$ であり、

$$\widetilde{G}_{\{\infty\}}(K)\simeq\langle\, a,b\,|\,b^2,\ b^{-1}a^{-1}ba^{-1}b^{-1}aba\,\rangle^{\text{pro-2}}.$$

この系の証明において、$l_{ij} \bmod 2$ と c_{iab} を用いた $\Delta(T)$ に関する公式が、副 p Fox 微分から得られる．その公式は上記の 3 つの場合に共通であり、特に $\ell_1^*\ell_2^*$ の正負に依らず、l_{ij} や c_{iab} は Greenberg 予想（予想 3.3）に反しないように振舞っている．また、$c_{012}+c_{201}$ に関する主張は、32 次拡大 $L_{0,1}L_{1,2}/\mathbb{Q}$ での素数の分解法則のひとつを表している．Rédei 記号が定義されない状況で、岩澤理論から分解法則が記述された例である．

$p \neq 2$ かつ k が虚 2 次体のとき、$\widetilde{G}_\emptyset(k)$ の Koch 型群表示から Gold [19] の定理の別証明も得られる ([36, Th.4.2])．Koch 型群表示には、他にも様々な応用が期待できる．

§4. 問題提起

p 群生成アルゴリズムと補題 2.8 のアイデアを用いた方法では、よく似た丁度 2 つの同型類の候補に辿り着くことが多い (e.g., [3, 5, 6] etc.)．その根拠も知りたいところであるが、次の問題は、その同型類の特定にも何らかの関わりがあるように思われる．

問題 4.1 (cf. [54, I§4.4, p.34])．　副 p 群 $G = G_S(\mathbb{Q})$ は、$d_1(G)$ 個の生成元と $d_2(G)$ 本の関係式で定義される抽象群の副 p 完備化と同型か？ そのとき G が有限 p 群なら、副 p 完備化せずとも同型か？

定理 2.7 は、この問が肯定的な例である．その証明の最後のステップにおいて、G_6^- についても関係式 2 本の抽象群表示を試みたが、うまくいかなかった．$p = 2$ のとき、次のような例もある ([17])：$G_{\{3,7,11\}}(\mathbb{Q}) \simeq Q_8 \simeq \langle\, a, b \,|\, abab^{-1}, baba^{-1} \,\rangle$.

また、$\widetilde{G}_S(k)$ を考えることで、Greenberg 予想（予想 3.3）も Fontaine-Mazur 予想（予想 2.2）のような捉え方ができないか、という期待から、次の問題も考えられる．

問題 4.2.　k は総実で、$S = \emptyset$ とする．このとき $\widetilde{G}_S(k)$ は、次元が 2 以上の p 進解析的副 p 商を持たないのではないか？ 即ち、任意の n に対して、表現 $\widetilde{\rho}\colon \widetilde{G}_S(k) \to \mathrm{GL}_n(\mathbb{Q}_p)$ の像の次元は高々 1 であろうか？

この問題の主張が肯定的ならば、Greenberg 予想も肯定的である．$S \neq \emptyset$ のときには否定的な例があるが、より一般に、$\widetilde{G}_S(k)$ は何次元の p 進解析的副 p 商を持ち得るか？という問題や、像の大きな表現 $\widetilde{\rho}$ を具体的に構成する問題も考えられる．

謝辞

機会をくださった山崎隆雄さん、尾崎学さん、山本修司さんと、問題 4.2 の設定に関してご助言くださった星裕一郎さんに感謝いたします．尾崎さんには、問題 4.1 と [54] の一文との関連性もご指摘いただきました．また、原稿の改訂においてご指摘とご助言をくださった査読者の方に感謝いたします．

参考文献

[1] Blondeau, J., Lebacque, P. and Maire, C., On the cohomological dimension of some pro-p-extensions above the cyclotomic $\mathbb{Z}_p$-extension of a number field, Mosc. Math. J. **13** (2013), no. 4, 601–619.

[2] Boston, N., Reducing the Fontaine-Mazur conjecture to group theory, Progress in Galois theory, 39–50, Dev. Math. **12**, Springer, New York, 2005.

[3] Boston, N. and Leedham-Green, C., Explicit computation of Galois p-groups unramified at p, J. Algebra **256** (2002), no. 2, 402–413.

[4] Boston, N. and Nover, H., Computing pro-p Galois groups, Algorithmic number theory, 1–10, Lecture Notes in Comput. Sci. **4076**, Springer, Berlin, 2006.

[5] Bush, M. R., Computation of Galois groups associated to the 2-class towers of some quadratic fields, J. Number Theory **100** (2003), no. 2, 313–325.

[6] Bush, M. R. and Mayer, D. C., 3-class field towers of exact length 3, J. Number Theory **147** (2015), 766–777.

[7] Dixon, J. D., du Sautoy, M. P. F., Mann, A. and Segal, D., Analytic pro-p groups, Second edition, Cambridge Studies in Advanced Mathematics **61**, Cambridge University Press, Cambridge, 1999.

[8] Eick, B. and Koch, H., On maximal 2-extensions of $\mathbb{Q}$ with given ramification, Proceedings of the St. Petersburg Mathematical Society, Vol. XII, 87–102, Amer. Math. Soc. Transl. Ser. 2, **219**, Amer. Math. Soc., Providence, RI, 2006.

[9] Ellis, G., HAP – Homological Algebra Programming – a GAP package, Version 1.10.12, 2013.

[10] Ferrero, B. and Washington, L. C., The Iwasawa invariant μ_p vanishes for abelian number fields. Ann. of Math. (2) **109** (1979), no. 2, 377–395.

[11] Fujii, S., On the maximal pro-p extension unramified outside p of an imaginary quadratic field, Osaka J. Math. **45** (2008), no. 1, 41–60.

[12] Fujii, S., On the depth of the relations of the maximal unramified pro-p Galois group over the cyclotomic $\mathbb{Z}_p$-extension, Acta Arith. **149** (2011), no. 2, 101–110.

[13] Fujii, S. and Okano, K., Some problems on p-class field towers, Tokyo J. Math. **30** (2007), no. 1, 211–222.

[14] Fukuda, T., Remarks on $\mathbf{Z}_p$-extensions of number fields, Proc. Japan Acad. Ser. A Math. Sci. **70** (1994), no. 8, 264–266.

[15] 福田隆, 重点解説 岩澤理論 — 理論から計算まで —, SGC ライブラリ **145**, 臨時別冊・数理科学 2019 年 1 月, サイエンス社.

[16] Gamble, G., Nickel, W., O'Brien, E. and Horn, M., ANUPQ – ANU p-Quotient – a GAP package, Version 3.0, 2006.

[17] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.6.5; 2013. `https://www.gap-system.org`

[18] Gärtner, J., Higher Massey products in the cohomology of mild pro-p-groups, J. Algebra **422** (2015), 788–820.

[19] Gold, R., The nontriviality of certain $\mathbf{Z}_l$-extensions, J. Number Theory **6** (1974), 369–373.

[20] Greenberg, R., On the Iwasawa invariants of totally real number fields, Amer. J. Math. **98** (1976), no. 1, 263–284.

[21] Itoh, T., On the structure of the Galois group of the maximal pro-p extension with restricted ramification over the cyclotomic $\mathbb{Z}_p$-extension, Tokyo J. Math. **43** (2020), no. 1, 181–204.

[22] Itoh, T. and Mizusawa, Y., On tamely ramified pro-p-extensions over $\mathbb{Z}_p$-extensions of $\mathbb{Q}$, Math. Proc. Cambridge Philos. Soc. **156** (2014), no. 2, 281–294.
[23] Kisilevsky, H., Number fields with class number congruent to 4 mod 8 and Hilbert's theorem 94, J. Number Theory **8** (1976), no. 3, 271–279.
[24] Koch, H., On p-extensions with given ramification, Appendix 1 in; Haberland, K., Galois cohomology of algebraic number fields, VEB Deutscher Verlag der Wissenschaften, Berlin, 1978.
[25] Koch, H., Galois theory of p-extensions, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002.
[26] Labute, J., Mild pro-p-groups and Galois groups of p-extensions of $\mathbb{Q}$, J. Reine Angew. Math. **596** (2006), 155–182.
[27] Labute, J., Linking numbers and the tame Fontaine-Mazur conjecture, Ann. Math. Qué. **38** (2014), no. 1, 61–71.
[28] Mayer, D. C., New number fields with known p-class tower, Tatra Mt. Math. Publ. **64** (2015), 21–57.
[29] Mizusawa, Y., On the maximal unramified pro-2-extension of $\mathbb{Z}_2$-extensions of certain real quadratic fields II, Acta Arith. **119** (2005), no. 1, 93–107.
[30] Mizusawa, Y., On unramified pro-p Galois groups over cyclotomic $\mathbb{Z}_p$-extensions — a survey, Proceedings of the Symposium on Algebraic Number Theory and Related Topics, 223–233, RIMS Kôkyûroku Bessatsu, **B4**, Res. Inst. Math. Sci. (RIMS), Kyoto, 2007.
[31] Mizusawa, Y., On unramified Galois 2-groups over $\mathbb{Z}_2$-extensions of real quadratic fields, Proc. Amer. Math. Soc. **138** (2010), no. 9, 3095–3103.
[32] Mizusawa, Y., On the maximal unramified pro-2-extension over the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field, J. Théor. Nombres Bordeaux **22** (2010), no. 1, 115–138.
[33] Mizusawa, Y., A note on semidihedral 2-class field towers and $\mathbb{Z}_2$-extensions, Ann. Math. Qué. **38** (2014), no. 1, 73–79.
[34] Mizusawa, Y., On certain 2-extensions of $\mathbb{Q}$ unramified at 2 and ∞, Osaka J. Math. **53** (2016), no. 4, 1063–1088.
[35] Mizusawa, Y., Tame pro-2 Galois groups and the basic $\mathbb{Z}_2$-extension, Trans. Amer. Math. Soc. **370** (2018), no. 4, 2423–2461.
[36] Mizusawa, Y., On pro-p link groups of number fields, Trans. Amer. Math. Soc. **372** (2019), no. 10, 7225–7254.
[37] Mizusawa, Y. and Ozaki, M., Abelian 2-class field towers over cyclotomic $\mathbb{Z}_2$-extensions of imaginary quadratic fields, Math. Ann. **347** (2010), 437–453.
[38] Mizusawa, Y. and Ozaki, M., On tame pro-p Galois groups over basic $\mathbb{Z}_p$-extensions, Math. Z. **273** (2013), no. 3-4, 1161–1173.
[39] Mizusawa, Y. and Yamamoto, G., Iwasawa invariants and linking numbers of primes, Development of Iwasawa theory — the Centennial of K. Iwasawa's Birth (Tokyo, 2017), 639–654, Adv. Stud. Pure Math. **86**, Math. Soc. Japan, Tokyo, 2020.
[40] Morishita, M., On certain analogies between knots and primes, J. Reine Angew. Math. **550** (2002), 141–167.
[41] Morishita, M., Knots and primes, An introduction to arithmetic topology, Universitext, Springer, London, 2012. （森下昌紀, 結び目と素数, 丸善出版, 2009.）
[42] Mouhib, A., Sur la 2-extension maximale non ramifiée de la $\mathbf{Z}_2$-extension cyclotomique de certains corps quadratiques, An. St. Univ. Ovidius Constanta **22** (2014), no. 1, 207–214.
[43] Mouhib, A. and Movahhedi, A., On the p-class tower of a $\mathbf{Z}_p$-extension, Tokyo J. Math.

31 (2008), no. 2, 321–332.
[44] Neukirch, J., Schmidt, A. and Wingberg, K., Cohomology of number fields, Second edition, Grundlehren der Mathematischen Wissenschaften **323**, Springer-Verlag, Berlin, 2008.
[45] Nover, H., Computation of Galois groups associated to the 2-class towers of some imaginary quadratic fields with 2-class group $C_2 \times C_2 \times C_2$, J. Number Theory **129** (2009), no. 1, 231–245.
[46] O'Brien, E. A., The p-group generation algorithm, Computational group theory, Part 1., J. Symbolic Comput. **9** (1990), no. 5–6, 677–698.
[47] Okano, K., Abelian p-class field towers over the cyclotomic $\mathbb{Z}_p$-extensions of imaginary quadratic fields, Acta Arith. **125** (2006), 363–381.
[48] 尾崎学, $\mathbb{Z}_p$-拡大の非アーベル岩澤理論（「整数論のこの主題, 自分はこう考える」若手発表会, 京都大学, 2001）, 数理解析研究所講究録, **1256** (2002), 25–37.
[49] Ozaki, M., Non-abelian Iwasawa theory of $\mathbb{Z}_p$-extensions. J. Reine Angew. Math. **602** (2007), 59–94.
[50] Ozaki, M., Construction of maximal unramified p-extensions with prescribed Galois groups, Invent. Math. **183** (2011), no. 3, 649–680.
[51] Salle, L., Sur les pro-p-extensions à ramification restreinte au-dessus de la $\mathbb{Z}_p$-extension cyclotomique d'un corps de nombres, J. Théor. Nombres Bordeaux **20** (2008), no. 2, 485–523.
[52] Salle, L., On maximal tamely ramified pro-2-extensions over the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field, Osaka J. Math. **47** (2010), no. 4, 921–942.
[53] Schmidt, A., Rings of integers of type $K(\pi, 1)$, Doc. Math. **12** (2007), 441–471.
[54] Serre, J.-P., Galois cohomology, Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002.
[55] Shafarevich, I. R., Extensions with prescribed ramification points, Publications mathématiques de l'I.H.É.S., **18** (1963), 71–92.
[56] Sharifi, R. T., On Galois groups of unramified pro-p extensions, Math. Ann. **342** (2008), 297–308.
[57] Steurer, A., On the Galois groups of the 2-class towers of some imaginary quadratic fields, J. Number Theory **125** (2007), no. 1, 235–246.
[58] Taussky, O., A remark on the class field tower, J. London Math. Soc. **12** (1937), no. 2, 82–85.
[59] Vogel, D., On the Galois group of 2-extensions with restricted ramification, J. Reine Angew. Math. **581** (2005), 117–150.
[60] Yamagishi, M., On the center of Galois groups of maximal pro-p extensions of algebraic number fields with restricted ramification, J. Reine Angew. Math. **436** (1993), 197–208.
[61] Yamagishi, M., A survey of p-extensions, Class field theory — its centenary and prospect (Tokyo, 1998), 107–121, Adv. Stud. Pure Math. **30**, Math. Soc. Japan, Tokyo, 2001.
[62] Yamamoto, G., Linking numbers for primes and $\mathbf{Z}_p$-extensions of abelian p-extension fields, a talk at Muroran Number Theory Conference, Muroran Institute of Technology, March 2004.
[63] 山本現, 素数のまつわり数と $\mathbf{Z}_p$ 拡大について（第 11 回北陸数論研究集会, 金沢, 2012）, 報告集 (2013), 8–20.