基本$\mathbb{Z}_p$拡大上の馴分岐pro-p拡大について

伊藤 剛司 (千葉工業大学)　水澤 靖 (名古屋工業大学)

1　序

素数 p を固定し, 素数の有限集合 S と代数体 K に対して, K の最大 S 外不分岐 pro-p 拡大 K_S のガロア群

$$G_S(K) = \mathrm{Gal}(K_S/K)$$

を考える. K が $\mathbb{Q}$ 上有限次であるとき, $G_S(K)$ は pro-p 群として有限表示を持つことが知られており, その構造を降中心列を通して記述する研究は, Fröhlich [2], Koch [7] らによって古くから進められてきた. 特に $K = \mathbb{Q}$ などのとき, その群表示の関係式の記述には, $q \in S$ に関する p 冪剰余記号などが現れる (cf. [8] etc.).

$p \in S$ であるとき, $G_S(K)$ の研究は比較的進んでおり, 岩澤理論においても行われてきた. 例えば $G_{\{p\}}(\mathbb{Q}) \simeq \mathbb{Z}_p$ であり, $\mathbb{Q}_{\{p\}} = \mathbb{Q}_\infty$ は $\mathbb{Q}$ の $\mathbb{Z}_p$ 拡大 (基本 $\mathbb{Z}_p$ 拡大) である. 有限次代数体 K との合成体 $K_\infty = K\mathbb{Q}_\infty$ は K の円分 $\mathbb{Z}_p$ 拡大であり, $K \subset K_\infty \subset K_{\{p\}} \subset K_S$ である. よって $G_S(K)$ を調べることは, その閉部分群 $G_S(K_\infty)$ とそれへの $\Gamma = \mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$ の作用を調べることに他ならない. 例えば $p \neq 2$ のとき, $G_S(\mathbb{Q}_\infty)$ は有限生成 free pro-p 群であり, Γ の作用を記述せよという問題も提示されている (cf. [15] X §5 p.651). また小松 [9], 藤井 [3] らにより, 2 次体 K に対して $G_{\{p\}}(K)$ の関係式を記述する研究も行われている.

$p \notin S$ であるとき, 有限次代数体 K に対して $G_S(K)$ は ray p-類体塔のガロア群に他ならず, 関連する未解決問題も多い. この $p \notin S$ である場合にも, 岩澤理論の視点から $G_S(K)$ を理解する試みとして, 円分 $\mathbb{Z}_p$ 拡大 K_∞ に対して $G_S(K_\infty)$ を考察したい. $S = \emptyset$ である場合は, 尾崎 [17] を始めとして [11] などの研究があり, そこではアーベル商 $G_\emptyset(K_\infty)^{ab}$ の岩澤加群としての構造と p 進 L 関数とを結びつける Mazur-Wiles の定理 (岩澤主予想) なども有効であった. その一方で「K が総実ならば, $G_\emptyset(K_\infty)^{ab}$ は有限であろう」と主張する Greenberg 予想 (cf. [4]) の難しさも直接影響する. また虚 2 次体 K に対して, $p = 2$, $S \neq \emptyset$ である場合が Salle [18] によって扱われている.

ここでは $p \neq 2$, $p \notin S$, $K = \mathbb{Q}$ である場合を

— $G_S(\mathbb{Q}_\infty)$ の構造を, p 冪剰余記号や p 進 L 関数などを通して記述したい

— $G_S(\mathbb{Q}_\infty)$ の部分商として, $G_\emptyset(K_\infty)^{ab}$ の有限性を調べたい

という目標の下で考察し, [13] から始まった研究 [14] の延長として $G_S(\mathbb{Q}_\infty)$ が (pro-)metacyclic pro-p 群であるような S を分類した. 以下では S に対して,

$$S' = \{\, q \in S \mid q \equiv 1 \pmod{p} \,\}$$

と定める. このとき $G_S(\mathbb{Q}_\infty) = G_{S'}(\mathbb{Q}_\infty)$ であるので, $S = S'$ と仮定してよい. また, $G_S(\mathbb{Q}_\infty) = 1$ であるための必要十分条件は, $S' = \emptyset$ である.

2　結果

主結果. $p \neq 2$, $S = S' \neq \emptyset$ と仮定する. このとき, $G_S(\mathbb{Q}_\infty)$ が metacyclic pro-p 群であるための必要十分条件は, S が以下の定理 1, 2, 3 の条件 (iii) のいずれかをみたすことである.

Greenberg 予想への応用として, 次の系が得られる. 証明は [14] の系と同様である.

系. $p \neq 2$ であるとき, $G_S(\mathbb{Q}_\infty)$ が metacyclic pro-p 群ならば, $\mathbb{Q}_{\infty,S}/\mathbb{Q}$ の任意の有限次部分拡大 $K/\mathbb{Q}$ に対して, $G_\emptyset(K_\infty)^{ab}$ は有限である.

以下では $S = S' \neq \emptyset$ に対して,

$$k/\mathbb{Q} \text{ は最大 } S \text{ 外不分岐 elementary アーベル } p\text{-拡大}$$

を表すことにする. このとき, $\mathrm{Gal}(k/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^{|S|}$, $\mathbb{Q} \subset k \subset \mathbb{Q}(\zeta_q \,|\, q \in S)$ である. また, $q \in S'$ に対して, p 冪剰余記号を $(\ \ /q)_p$ で表す. このとき $a \in \mathbb{Z}$ に対して,

$$(a/q)_p \equiv a^{(q-1)/p} \pmod{q}$$

である.

定理 1. $p \neq 2$, $S = S'$, $|S| = 1$ であるとき, 次の 3 条件は同値である.
(i) $G_S(\mathbb{Q}_\infty)$ は cyclic
(ii) $G_\emptyset(k_\infty) = 1$
(iii) $S = \{q\}$, $q \not\equiv 1 \pmod{p^2}$ または $S = \{q\}$, $(p/q)_p \neq 1$
さらにこのとき, $G_S(\mathbb{Q}_\infty)$ は有限であり, $(p/q)_p \neq 1$ ならば $G_S(\mathbb{Q}_\infty) \simeq G_S(\mathbb{Q}) \simeq \mathbb{Z}_p/(q-1)\mathbb{Z}_p$ である.

注意 1. (ii) と (iii) の同値性は, 岩澤 [6] および山本 [20] による.

記号. 有限次代数体 K に対して, O_K を整数環, $E(K)$ を単数群, $E'(K) = O_K[1/p]^\times$ を p-単数群, $A_S(K)$ を $\prod_{q \in S} q$ を法とした ray イデアル類群の p-Sylow 部分群, $D_S(K)$ を p とのみ有縁なイデアルの類で生成される $A_S(K)$ の部分群とし, p-イデアル類群を $A'_S(K) = A_S(K)/D_S(K)$ とおく. このとき, $G_S(K)^{ab} \simeq A_S(K)$ である. また, $\mathbb{Q}_\infty/\mathbb{Q}$ の p^n 次部分拡大を $\mathbb{Q}_n/\mathbb{Q}$ とし, $K_n = K\mathbb{Q}_n$ とおく. v_p は $v_p(p) = 1$ と正規化された加法付値を表す.

$q \equiv 1 \pmod{p^2}$, $(p/q)_p = 1$ である $S = \{q\}$ に対して, 栗原 [10] の不変量 κ を導入する. 完全列

$$E'(\mathbb{Q}_n) \otimes \mathbb{Z}_p \xrightarrow{\Phi'_n} (O_{\mathbb{Q}_n}/q)^\times \otimes \mathbb{Z}/p\mathbb{Z} \to A'_S(\mathbb{Q}_n)/p \to 0$$

において, $\mathrm{Im}\,\Phi'_n \neq 0$ である $n \geq 0$ が存在するなら

$$\kappa = \dim \mathrm{Coker}\,\Phi'_n = p\text{-rank}\, A'_S(\mathbb{Q}_n)$$

と定め, そうでないなら $\kappa = \infty$ と定める. この $\kappa < \infty$ の定義は, n の選び方に依らない (cf. [10] Lemma 1.1). またこのとき, Dirichlet 指標 $\chi : \mathrm{Gal}(k/\mathbb{Q}) \hookrightarrow \overline{\mathbb{Q}}_p^\times$ と Teichmüller 指標 ω に対して, p 進 L 関数 $L_p(s, \chi)$ は

$$L_p(0, \chi) = -B_{1,\chi\omega^{-1}} \in \mathbb{Z}_p[\zeta_p]$$

をみたす. ここに, $B_{1,\chi\omega^{-1}}$ は一般ベルヌーイ数である.

定理 2. $p \neq 2$, $S = S'$, $|S| = 1$ であるとき, 次の 3 条件は同値である.
(i) $G_S(\mathbb{Q}_\infty)$ は noncyclic metacyclic
(ii) $G_\emptyset(k_\infty) \simeq \mathbb{Z}/p\mathbb{Z}$
(iii) $S = \{q\}$, $q \equiv 1 \pmod{p^2}$, $(p/q)_p = 1$, $\kappa = 1$, $B_{1,\chi\omega^{-1}} \not\equiv 0 \pmod{(1-\zeta_p)^2}$
さらにこのとき, $G_S(\mathbb{Q}_\infty)$ は有限である.

注意 2. 条件 (ii) は, $G_\emptyset(k_\infty)$ が非自明 cyclic であることと同値である. (ii) と (iii) の同値性は, 本質的には尾崎-山本 [16] および栗原 [10] による. (iii) の条件 $\kappa = 1$ は, 次のように言い換えることができる (cf. [10]).

$$\kappa = 1 \ \Leftrightarrow \ \dim \mathrm{Coker}\, \Phi'_1 = 1 \ \Leftrightarrow \ A'_\emptyset(k_1) = 0$$

さらに $p = 3$ の場合には, q の原始根 g に対して $z = g^{(q-1)/p^2}$ とおくと,

$$\kappa = 1 \ \Leftrightarrow \ \left(\frac{(z^2-1)(z^{-2}-1)}{(z-1)(z^{-1}-1)}\right)^{(q-1)/p} \not\equiv 1 \pmod{q}$$

とも言い換えられる (cf. [16], [10]). また, (iii) の条件 $B_{1,\chi\omega^{-1}} \not\equiv 0 \pmod{(1-\zeta_p)^2}$ は, 田谷 [19] の結果を介して, $v_p(R_p(k)) = p$ で置き換えることもできる. ここに, $R_p(k)$ は k の p 進 regulator を表す.

定理 3. $p \neq 2$, $S = S'$, $|S| = 2$ であるとき, 次の 3 条件は同値である.
(i) $G_S(\mathbb{Q}_\infty)$ は metacyclic
(ii) $G_\emptyset(k_\infty) = 1$
(iii) $S = \{q_1, q_2\}$, $(p/q_1)_p \neq 1$, $(q_1/q_2)_p \neq 1$, $q_2 \not\equiv 1 \pmod{p^2}$, ある x, y, z に対して

$$(q_2 p^x/q_1)_p = 1,\ (pq_1^y/q_2)_p = 1,\ q_1 q_2^z \equiv 1 \pmod{p^2},\ xyz \not\equiv -1 \pmod{p}$$

さらにこのとき, $m = v_p(q_1 - 1)$ とすると, pro-p 群表示

$$G_S(\mathbb{Q}_\infty) = \left\langle a,\, b \;\middle|\; a^{p^{m+1}} = 1,\ b^{-1}ab = a^{1+p^m} \right\rangle^{\text{pro-}p}$$

が得られる.

注意 3. (ii) と (iii) の同値性は, 山本 [20] による. [13] では, (iii) かつ $y = 0$, $m = 1$ ならば, (i) が成り立つことを示している. [14] では, (iii) かつ $m = 1$ ならば, (i) とともに群表示が得られることを示している.

3 証明

ここでは, 主結果の証明の概略について述べる. 証明では, 以下が有効に使われる.

1. 完全列

$$E(K) \otimes \mathbb{Z}_p \to (O_K/\textstyle\prod_{q\in S} q)^\times \otimes \mathbb{Z}_p \to A_S(K) \to A_\emptyset(K) \to 0$$

が得られる. これを用いて, $A_S(K)$ へのガロア作用などを把握することができる.

2. K の $q \in S$ 上の素点 Q に対して, その $G_S(K)^{ab}$ における惰性群 I_Q は cyclic であり, 完全列

$$0 \to I_Q \to A_S(K) \to A_{S\setminus\{Q\}}(K) \to 0$$

が得られる. これを用いて, p-rank $A_S(K)$ が評価できる.

3. [13] から派生した研究 [5] において, 公式

$$\mathbb{Z}_p\text{-rank}\, G_S(\mathbb{Q}_\infty)^{ab} = \sum_{q\in S'} p^{v_p(q-1)-1} - \max_{q\in S'}\left\{p^{v_p(q-1)-1}\right\}$$

が得られている. 特に, $|S'|=1$ ならば $G_S(\mathbb{Q}_\infty)^{ab}$ は有限である.

4. 位数 p^3 の p-群 G について, 以下は同値である.
(1) G の exponent は p^2
(2) G は metacyclic
(3) $G\simeq \mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p^2\mathbb{Z}$ または $G\simeq \left\langle\, a,\, b \;\middle|\; a^{p^2}=b^p=1,\ b^{-1}ab=a^{1+p}\,\right\rangle$
さらにこのとき, G の cyclic でない極大部分群は唯一つである.

5. pro-p 群 G に対して, $G_2=[G,G]$, $G_3=[G,G_2]$, $\Phi(G_2)=G_2^p[G_2,G_2]$ とおく. このとき,

$$G \text{ が metacyclic } \Leftrightarrow\ G/\Phi(G_2)G_3 \text{ が metacyclic}$$

である (cf. [1] etc.). また, metacyclic pro-p 群の部分商は metacyclic である.

まず, $G_S(\mathbb{Q})^{ab}/p\simeq \mathrm{Gal}(k/\mathbb{Q})$ なので, $|S'|>2$ ならば $G_S(\mathbb{Q}_\infty)$ は metacyclic にはなり得ない. よって, $|S'|\le 2$ の場合のみを考察すればよい. そこで, (ii) と (iii) の同値性および注意で述べたことは既知として, 定理 1, 2, 3 の証明の方針を述べる.

(i) $\Rightarrow$ (ii), (iii). 定理 1: $\mathbb{Q}_{\infty,S}/\mathbb{Q}_\infty$ で q は完全分岐するので, その部分商 $G_\emptyset(k_\infty)=1$ である.
定理 2: $G_\emptyset(k_\infty)$ が cyclic でないとすると, 最大不分岐 elementary アーベル p-拡大 L/k_∞ について, $\mathrm{Gal}(L/\mathbb{Q}_\infty)$ は metacyclic かつ位数 p^3 である. $L/\mathbb{Q}_\infty$ での分岐の様子を調べると, 矛盾が生じている.
定理 3: $\mathbb{Z}_p\text{-rank}\, G_S(\mathbb{Q}_\infty)^{ab}\le 2$ なので, $S=\{q_1,q_2\}$, $q_2\not\equiv 1 \pmod{p^2}$ となる. 最大 S 外不分岐アーベル p-拡大 $K/\mathbb{Q}$ に対して, 最大不分岐 elementary アーベル p-拡大 L/K_∞ を考える. このとき $\mathrm{Gal}(L/K_\infty)\simeq G_\emptyset(K_\infty)^{ab}/p$ であり, $r=p\text{-rank}\,\mathrm{Gal}(L/K_\infty)\le 2$ とおく. $r=2$ のとき, $\mathrm{Gal}(L/\mathbb{Q}_{\{q_1\},\infty})$ は metacyclic かつ位数 p^3 であり, $L/\mathbb{Q}_{\{q_1\},\infty}$ での分岐の様子を調べると, 矛盾が生じている. $r=1$ のとき, $\mathbb{Q}_\infty\subset M\subset\mathbb{Q}_{\{q_1\},\infty}$ である p 次拡大 $\mathbb{Q}_{\{q_1\},\infty}/M$ について, $\mathrm{Gal}(L/M)$ は metacyclic かつ位数 p^3 であり, L/M での分岐の様子を調べると, やはり矛盾が生じている. よって $r=0$, 即ち $G_\emptyset(K_\infty)=1$ であり, 山本 [20] より (iii) が成り立つ. □

(ii), (iii) $\Rightarrow$ (i). 定理 1: $G_S(\mathbb{Q}_\infty)$ が cyclic でないとすると, S 外不分岐 (p,p) 拡大 $F/\mathbb{Q}_\infty$ で, $k_\infty\subset F$ であるものが存在するが, このとき F/k_∞ は不分岐である. また, $(p/q)_p\ne 1$ のときは $A_S(\mathbb{Q}_n)=D_S(\mathbb{Q}_n)$ となり, これへの $\Gamma=\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ の作用は自明なので, $G_S(\mathbb{Q}_\infty)\simeq G_S(\mathbb{Q})$ も導かれる.
定理 2, 3: 基本的なアイデアは [11], [12], [13], [14] と同様である. 定理 2 では $F=k$ とし, 定理 3 では $k/\mathbb{Q}$ における p の分解体を F とする. このとき $F/\mathbb{Q}$ は p 次拡大であり, (ii) と (iii) から次の補題を導くことができる.

補題. すべての $n\ge 1$ に対して, $p\text{-rank}\, A_S(\mathbb{Q}_n)=p\text{-rank}\, A_S(F_n)=2$.

$H=G_S(F_\infty)$ は $G=G_S(\mathbb{Q}_\infty)$ の極大部分群であり, $G^{ab}\simeq \varprojlim A_S(\mathbb{Q}_n)$, $H^{ab}\simeq\varprojlim A_S(F_n)$ である. 補題より G は 2 元生成であり,

$$G=\left\langle\, a,\, b\,\right\rangle^{\text{pro-}p},\ H=\left\langle\, a,\, b^p,\, G_2\,\right\rangle^{\text{pro-}p}=\left\langle\, a,\, b^p,\, [a,b],\, \Phi(G_2)G_3\,\right\rangle^{\text{pro-}p}$$

であるような生成元 a, b を選ぶことができる. このとき, $H/\Phi(G_2)G_3$ はアーベルであり, 補題より p-rank $H^{ab} = 2$ なので, a, b^p, $[a,b]$ の間には $\Phi(G_2)G_3$ を法として非自明な関係式が存在する. 生成元 a, b を適当に取り替えることによって, ある $m \geq 0$ に対して

$$[a,b] = a^{-1}b^{-1}ab \equiv a^{p^m} \pmod{\Phi(G_2)G_3}$$

が成り立つことがわかる. よって, G は metacyclic であり, 再び a, b を取り替えることによって, $b^{-1}ab = a^{1+p^m}$ となる. 特に, $G_2 = \langle a^{p^m} \rangle^{\text{pro-}p}$ である. さらに, $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ の $(O_{\mathbb{Q}_n}/\prod_{q\in S} q)^\times \otimes \mathbb{Z}_p$ への作用を調べることにより, Γ の標準的な生成元 γ の G^{ab} への作用が記述できる. 適切な N に対して $\sigma = \gamma^{p^N}$ とおいて計算すると, ある $0 \neq z \in \mathbb{Z}_p$ に対して

$$1 = {}^\sigma 1 = {}^\sigma(a^{-(1+p^m)}b^{-1}ab) = \cdots = a^z$$

となり, a の位数の有限性, 即ち G_2 の有限性がわかる. 定理 3 においては,

$$\mathrm{Tor}_{\mathbb{Z}_p} G^{ab} \simeq \varprojlim D_S(\mathbb{Q}_n) \simeq \mathbb{Z}/p^m\mathbb{Z}\ ,\ \ m = v_p(q_1 - 1)$$

であることが示され, $N = 0$ として計算すると $v_p(z) = m + 1$ となる. $G_S(\mathbb{Q})$ がアーベルでないこと (cf. [7] etc.) から $a^{p^m} \neq 1$ であり, 群表示も得られる. □

謝辞

講演の機会をくださった世話人の皆様, ご清聴くださった参加者の皆様, 準備の際に有益なご助言をくださった山岸正和先生に感謝いたします. この研究の一部は, 科学研究費補助金 (No. 22740010) および千葉工業大学附属総合研究所助成金の支援を受けています.

参考文献

[1] N. Blackburn, *On prime-power groups with two generators*, Proc. Cambridge Philos. Soc. **54** (1958), 327–337.

[2] A. Fröhlich, *On fields of class two*, Proc. London Math. Soc. (3) **4** (1954), 235–256.

[3] S. Fujii, *On the maximal pro-p extension unramified outside p of an imaginary quadratic field*, Osaka J. Math. **45** (2008), 41–60.

[4] R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), 263–284.

[5] T. Itoh, Y. Mizusawa and M. Ozaki, *On the $\mathbb{Z}_p$-ranks of tamely ramified Iwasawa modules*, preprint.

[6] K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg **20** (1956), 257–258.

[7] H. Koch, *l-Erweiterungen mit vorgegebenen Verzweigungsstellen*, J. Reine Angew. Math. **219** (1965), 30–61.

[8] H. Koch, Galois theory of p-extensions, Springer-Verlag, Berlin, 2002.

[9] K. Komatsu, *On the maximal p-extensions of real quadratic fields unramified outside p*, J. Algebra **123** (1989), 240–247.

[10] M. Kurihara, *Remarks on the λ_p-invariants of cyclic fields of degree p*, Acta Arith. **116** (2005), 199–216.

[11] Y. Mizusawa, *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), 115–138.

[12] Y. Mizusawa, *On unramified Galois 2-groups over $\mathbb{Z}_2$-extensions of real quadratic fields*, Proc. Amer. Math. Soc. **138** (2010), 3095–3103.

[13] Y. Mizusawa, 基本 $\mathbb{Z}_p$ 拡大上の馴分岐 pro-p ガロア群について, 鏡ヶ池の整数論セミナー報告集 (2008), 115–120. `http://hdl.handle.net/2237/11242`

[14] Y. Mizusawa and M. Ozaki, *On tame pro-p Galois groups over basic $\mathbb{Z}_p$-extensions*, preprint.

[15] J. Neukirch, A. Schmidt and K. Wingberg, Cohomology of number fields, Second edition, Grundlehren der Mathematischen Wissenschaften, 323, Springer-Verlag, Berlin, 2008.

[16] M. Ozaki and G. Yamamoto, *Iwasawa λ_3-invariants of certain cubic fields*, Acta Arith. **97** (2001), 387–398.

[17] M. Ozaki, *Non-Abelian Iwasawa theory of $\mathbb{Z}_p$-extensions*, J. Reine Angew. Math. **602** (2007), 59–94.

[18] L. Salle, *On maximal tamely ramified pro-2-extensions over the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field*, Osaka J. Math. **47** (2010), 921–942.

[19] H. Taya, *On p-adic zeta functions and $\mathbf{Z}_p$-extensions of certain totally real number fields*, Tohoku Math. J. (2) **51** (1999), 21–33.

[20] G. Yamamoto, *On the vanishing of Iwasawa invariants of absolutely abelian p-extensions*, Acta. Arith. **94** (2000), 365–371.