基本 $\mathbb{Z}_p$ 拡大上の馴分岐 pro-p ガロア群について

水澤 靖（名古屋工業大学）

2008 年 12 月 20 日

§1. 序

素数 p を固定し，素数の有限集合 S を考える．有限次とは限らない代数体 K に対して，混同を招く場合を除き，S 上の K の素点全体の集合 $S(K)$ も S で表すことにする．このとき，K の S 外不分岐最大 pro-p 拡大 K_S のガロア群 $G_S(K)$ を考える[1].

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

p 拡大で分岐し得る素数のみを考えて，S の元は p または $q \equiv 1 \pmod{p}$ と仮定する．

K が有限次代数体であるとき，$G_S(K)$ は pro-p 群として有限表示を持つことが知られている (cf. [5] §11, [6] etc.) が，その詳細な構造は，S が p を含むか否かによって趣きが大きく異なる．$p \in S$ である場合は，K_S が K の円分 $\mathbb{Z}_p$ 拡大 K_∞ を含むことから，岩澤理論とも関係して研究が進んでいる (cf. [6] etc.)．一方，$p \notin S$ であるとき，$G_S(K)$ は “fab” pro-p 群，即ち任意の開部分群 H のアーベル商 H^{ab} は有限となる．このとき，$G_S(K)$ は有限か否かという問題も自明でないが，$S = \emptyset$ のときは p-類体塔問題に他ならず，一般に $G_S(K)$ は有限にも無限にもなり得る．さらに Fontaine-Mazur 予想の帰結として，$G_S(K)$ は p 進解析的な無限商を持たないと予想されている (cf. [8] etc.).

例 1. $S = \{p\}$ のとき，$\mathbb{Q}_S$ は $\mathbb{Q}$ の $\mathbb{Z}_p$ 拡大 $\mathbb{Q}_\infty$ に等しく，$G_S(\mathbb{Q}) \simeq \mathbb{Z}_p$．この $\mathbb{Q}_\infty$ を基本 $\mathbb{Z}_p$ 拡大と呼び，有限次代数体 K との合成体 $K_\infty = K\mathbb{Q}_\infty$ が K の円分 $\mathbb{Z}_p$ 拡大である．

例 2. $p \neq 2$, $S = \{q\}$, $q \equiv 1 \pmod{p}$ のとき，$\mathbb{Q}_S$ は q 分体 $\mathbb{Q}(\zeta_q)$ に含まれる $\mathbb{Q}$ の最大 p 拡大 $\mathbb{Q}(q)$ に等しく，$G_S(\mathbb{Q})$ は有限巡回群.

例 3. $p \neq 2$, $S = \{q_1, q_2\}$, $q_i \equiv 1 \pmod{p}$, $q_i \not\equiv 1 \pmod{p^2}$ $(i = 1, 2)$, p 冪剰余記号 $(q_2/q_1)_p \neq 1$ のとき，$G_S(\mathbb{Q})$ は位数 p^3 の非可換有限群 (cf. [5] Example 11.15).

例 4. $p \neq 2$, $S = \{q_1, \cdots, q_m\}$, $q_i \equiv 1 \pmod{p}$ $(i = 1, \cdots, m)$, $m \geq 4$ のとき，Golod-Shafarevich 不等式により，$G_S(\mathbb{Q})$ は p 進解析的でない無限 pro-p 群 (cf. [4] [8] etc.).

ここで唐突ではあるが，馴分岐 pro-p ガロア群 $G_S(K)$, $p \notin S$ を岩澤理論的な対象と捉えて，次の問題を考える．

問題. 有限次代数体 K の円分 $\mathbb{Z}_p$ 拡大 K_∞ と，$q \equiv 1 \pmod{p}$ なる素数 q の有限集合 S に対して，$G_S(K_\infty)$ は—

(1) 有限表示を持つか？ 即ち，generator rank d と relation rank r は共に有限か？

[1] より一般には，代数体 K の素点の有限集合 $S = S(K)$ に対する $G_S(K)$ が興味の対象である．

(2) K が総実ならば fab pro-p 群か？

$S=\emptyset$ のとき，(1) の d の有限性は所謂 “$\mu=0$ 予想” と同値であり，r の有限性は [7] などで提示されている問題である．さらに (2) は，Greenberg 予想 [3] と同値である[2]．これらに対する肯定的具体例は多く存在するが，いずれも一般的な解決には至っていない．

一方，$K=\mathbb{Q}$ のとき，$S=\emptyset$ ならば $G_S(\mathbb{Q}_\infty)=\{1\}$ であるので自明な問題だが，$S\neq\emptyset$ の場合はそれほど明らかではない．しかしながら，(1) d の有限性，即ち $G_S(\mathbb{Q}_\infty)$ が有限生成であることは容易にわかり，$\mathbb{Q}$ 上の p 拡大を扱うことの利点も多い．また (2) が肯定的ならば，$G_S(\mathbb{Q}_\infty)$ の任意の不分岐アーベル部分商も有限なので，任意の $\mathbb{Q}$ 上 S 外不分岐ガロア p 拡大に対して Greenberg 予想が肯定的に成立することになるが，(2) が否定的であっても，その詳細な構造を調べることによって Greenberg 予想への貢献が期待できる．

本稿ではこの問題に対する一歩として，$K=\mathbb{Q}$, $\#S\leq 2$ の場合を考察する．

§2．結果[3]

$\#S=1$ の 場合として，次の結果が容易に得られる．

定理 1． 素数 $p\neq 2$ と素数の集合 $S=\{q\}$, $q\equiv 1\,(\mathrm{mod}\,p)$, $q\not\equiv 1\,(\mathrm{mod}\,p^2)$ に対し，p 冪剰余記号について $(p/q)_p\neq 1$ と仮定する．このとき，有理数体 $\mathbb{Q}$ の $\mathbb{Z}_p$ 拡大 $\mathbb{Q}_\infty$ 上の S 外不分岐最大 pro-p 拡大のガロア群 $G_S(\mathbb{Q}_\infty)$ は位数 p の巡回群である．特に，この場合の問題 (1)(2) の答は肯定的である．

p 冪剰余に関する条件を除いた場合でも，$S=\{q\}$, $q\equiv 1\,(\mathrm{mod}\,p)$, $q\not\equiv 1\,(\mathrm{mod}\,p^2)$ である場合は，以下の計算例から問題 (1)(2) ともに肯定的であると予想される．

例 5． pari/gp の `bnfinit`, `bnrinit`（option 無し，GRH より強い条件を仮定）によると，$p=3$ と $q\equiv 1\,(\mathrm{mod}\,p)$, $q\not\equiv 1\,(\mathrm{mod}\,p^2)$, $(p/q)_p=1$ である素数 $q=61,\,67,\,103,\,151$ について，$S=\{q\}$ とするとき, $A_S(\mathbb{Q}_1)\simeq A_S(\mathbb{Q}_2)\simeq\mathbb{Z}/p^2\mathbb{Z}$（記号は §3 参照）．この結果に [2] の定理（後述の定理 3）を適用すると，$G_S(\mathbb{Q}_\infty)$ は位数 p^2 の巡回群.

$\#S=2$ の 場合として，次の主結果が得られる．

定理 2． 素数 $p\neq 2$ と素数の集合 $S=\{q_1,q_2\}$, $q_i\equiv 1\,(\mathrm{mod}\,p)$, $q_i\not\equiv 1\,(\mathrm{mod}\,p^2)$ $(i=1,2)$ に対し，p 冪剰余記号について $(p/q_1)_p=1$, $(p/q_2)_p\neq 1$, $(q_2/q_1)_p\neq 1$ と仮定する．このとき，有理数体 $\mathbb{Q}$ の $\mathbb{Z}_p$ 拡大 $\mathbb{Q}_\infty$ 上の S 外不分岐最大 pro-p 拡大のガロア群 $G_S(\mathbb{Q}_\infty)$ は metacyclic pro-p 群である．特に，この場合の問題 (1) の答は肯定的である[4]．

---

[2] $G_S(K_\infty)$ が fab であることと，$K_{\infty,\emptyset}$ に含まれる任意の有限次代数体 F に対して，その円分 $\mathbb{Z}_p$ 拡大 F_∞ の岩澤不変量が “$\lambda=\mu=0$” をみたすことが同値である．

[3] $p=2$ の場合にも同様の結果が得られるが，簡単のために省略する．

[4] この場合の問題 (2) の答は否定的であることを，本稿執筆中に近畿大の尾崎学氏より御指摘いただきましたが，ここではその詳細は省略いたします.

ここに pro-p 群 G が metacyclic であるとは，ある正規部分群 N が存在し，N および G/N が共に pro-p 巡回群であることをいう．

§3．準備

素数の有限集合 $S=\{q_1,\cdots,q_d\}$, $q_i\equiv 1\,(\mathrm{mod}\,p)$ $(i=1,\cdots,d)$ と有限次代数体 K に対して，$\mathrm{mod}\ \mathfrak{m}=q_1\cdots q_d$ イデアル類群（ray class group）$Cl_{\mathfrak{m}}(K)$ に関する次の完全列が得られる．ここに，O_K は整数環, $Cl(K)$ は広義のイデアル類群である．

$$O_K^{\times}\longrightarrow(O_K/\mathfrak{m})^{\times}\longrightarrow Cl_{\mathfrak{m}}(K)\longrightarrow Cl(K)\longrightarrow 0$$

$\mathrm{Ker}((O_K/\mathfrak{m}^n)^{\times}\to(O_K/\mathfrak{m})^{\times})$ の位数が p と素であることに注意すると，類体論から $Cl_{\mathfrak{m}}(K)$ のシロー p 部分群 $A_S(K)$ は $G_S(K)^{ab}$ と同型である．

$\mathbb{Q}_\infty$ の p^n 次部分拡大を $\mathbb{Q}_n$ とし，有限次代数体 K との合成体を $K_n=K\mathbb{Q}_n$ とする．K_n は K_∞ の部分体であり，$K\cap\mathbb{Q}_\infty=\mathbb{Q}$ ならば $\mathrm{Gal}(K_n/K)\simeq\mathbb{Z}/p^n\mathbb{Z}$ である．$A_S(K_n)$ および $G_S(K_n)^{ab}$ は，n に関してノルムおよび制限写像による射影系を成し，$\Gamma=\mathrm{Gal}(K_\infty/K)$ 上の加群として $\varprojlim A_S(K_n)\simeq\varprojlim G_S(K_n)^{ab}\simeq G_S(K_\infty)^{ab}$ となる．その Γ 加群としての基本性質が，$Cl(K)$ のシロー p 部分群 $A(K_n)$ に対する岩澤加群 $\varprojlim A(K_n)\simeq G_\emptyset(K_\infty)^{ab}$ と共通することから，[2] の定理が同様に成立する．

定理 3 ([2])**．** K_∞ において分岐する K の素点はすべて完全分岐すると仮定する．
(1) ある n で $A_S(K_n)\simeq A_S(K_{n+1})$ ならば，$A_S(K_n)\simeq G_S(K_\infty)^{ab}$.
(2) ある n で $\mathrm{rank}\,A_S(K_n)=\mathrm{rank}\,A_S(K_{n+1})$ ならば，$\mathrm{rank}\,A_S(K_n)=\mathrm{rank}\,G_S(K_\infty)^{ab}$.
(3) その分岐素点が唯一つであるとき，ある n で $A_S(K_n)\simeq A_S(K_{n+1})$ かつ $A_S(K_n)$ の exponent が p^r ならば，持ち上げ写像 $A_S(K_n)\to A_S(K_{n+r})$ は零写像.

$q_i\not\equiv 1\,(\mathrm{mod}\,p^2)$ $(i=1,\cdots,d)$ であるとき，q_i は $\mathbb{Q}$ で不分解ゆえ，$O_{\mathbb{Q}_n}/q_i$ は有限体である．また $G_\emptyset(\mathbb{Q}_\infty)=\{1\}$ であるので，$A(\mathbb{Q}_n)=0$ である．よって $(O_{\mathbb{Q}_n}/\mathfrak{m})^{\times}\simeq\oplus_{i=1}^d(O_{\mathbb{Q}_n}/q_i)^{\times}$ であることから，$\mathrm{rank}\,A_S(\mathbb{Q}_n)\le d$ が導かれる．一方，$A_S(\mathbb{Q}_n)\simeq G_S(\mathbb{Q}_n)^{ab}\twoheadrightarrow G_S(\mathbb{Q})^{ab}\simeq\oplus_{i=1}^d G_{\{q_i\}}(\mathbb{Q})^{ab}\simeq(\mathbb{Z}/p\mathbb{Z})^d$ であるので，$\mathrm{rank}\,A_S(\mathbb{Q}_n)=d$ である．後述の Burnside の基定理から，次の命題を得る．

命題 1． $S=\{q_1,\cdots,q_d\}$, $q_i\equiv 1\,(\mathrm{mod}\,p)$, $q_i\not\equiv 1\,(\mathrm{mod}\,p^2)$ $(i=1,\cdots,d)$ に対して，$G_S(\mathbb{Q}_\infty)$ は d 元生成 pro-p 群である．

pro-p 群 G に対して，降中心列 $G_1=G$, $G_i=[G_{i-1},G]$ $(i\ge 2)$ および Frattini 部分群 $\Phi(G)=G^p[G,G]$ を定める．

Burnside の基定理． pro-p 群 G は，$d=\mathrm{rank}\,G/\Phi(G)$ 元生成である．

命題 2 (cf. [1] Theorem 2.3 etc.)**．** p 群 G が metacyclic であるための必要十分条件は，$G/\Phi(G_2)G_3$ が metacyclic であることである．

§4. 証明

（定理1の証明）p は $\mathbb{Q}_n$ で完全分岐し，$\mathbb{Q}_S$ で不分解である．$\mathbb{Q}_S$ は $\mathbb{Q}$ の p 次拡大であって，$(\mathbb{Q}_S)_n$ は $G_S(\mathbb{Q}_n)$ の極大部分群に対応する．命題1より $G_S(\mathbb{Q}_n) \simeq A_S(\mathbb{Q}_n)$ は巡回群であるので，$\mathbb{Q}_n$ の p 上の素点 $\mathfrak{p}$ は $(\mathbb{Q}_n)_S$ でも不分解である．よって，$A_S(\mathbb{Q}_n)$ は $\mathfrak{p}$ の冪の類で生成されるので，$\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = \gamma^{\mathbb{Z}_p}$ は $A_S(\mathbb{Q}_n)$ に自明に作用する．よって $A_S(\mathbb{Q}_n) \simeq A_S(\mathbb{Q}_n)_\Gamma = A_S(\mathbb{Q}_n)/A_S(\mathbb{Q}_n)^{\gamma-1} \simeq A_S(\mathbb{Q}) \simeq \mathbb{Z}/p\mathbb{Z}$．ゆえに，$G_S(\mathbb{Q}_\infty) \simeq \mathbb{Z}/p\mathbb{Z}$. □

（定理2の証明）補題を幾つか用意する．

補題1． $n \geq 1$ に対して，$G_{\{q_1\}}(\mathbb{Q}_n) \simeq A_{\{q_1\}}(\mathbb{Q}_n)$ は位数 p^2 以上の巡回群である．

（証明）$\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = \gamma^{\mathbb{Z}_p}$ とし，$A_{\{q_1\}}(\mathbb{Q}_n)$ の部分群を次のように定める．

$$B_n = A_{\{q_1\}}(\mathbb{Q}_n)^\Gamma = \{\, [\mathfrak{a}] \in A_{\{q_1\}}(\mathbb{Q}_n) \mid [\mathfrak{a}]^\gamma = [\mathfrak{a}] \,\}$$
$$B_n' = \{\, [\mathfrak{a}] \in B_n \mid \mathfrak{a}^\gamma = \mathfrak{a} \,\}$$

任意に $[\mathfrak{a}] \in B_n$ をとる．ある $\alpha \in \mathbb{Q}_n^\times$, $\alpha \equiv 1 \pmod{q_1}$ が存在して，$\alpha = \mathfrak{a}^{\gamma-1}$ である．$\mathbb{Q}$ へのノルム $N\alpha = \pm 1$ であるが，$N\alpha \equiv 1 \pmod{q_1}$ であるので，$N\alpha = 1$. Hilbert 90 より，ある $\delta \in \mathbb{Q}_n^\times$ が存在して，$\alpha = \delta^{\gamma-1}$ である．$q_1 = q_1^\gamma$ は $\mathbb{Q}_n$ の素点であるゆえ，δ は q_1 と素であるとしてよい．$\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ は剰余体のガロア群とみなせるので，$\delta \bmod q_1 \in O_{\mathbb{Q}_n}/q_1$, $\delta^\gamma \equiv \delta \pmod{q_1}$ であることから，$\delta \bmod q_1 \in \mathbb{Z}/q_1\mathbb{Z}$, 即ちある $z \in \mathbb{Z}$ が存在して，$\delta \equiv z \pmod{q_1}$．$\eta = \delta z^{-1} \equiv 1 \pmod{q_1}$ と定めると，$\eta^{\gamma-1} = \delta^{\gamma-1} = \alpha = \mathfrak{a}^{\gamma-1}$, $\eta^{-1} \equiv 1 \pmod{q_1}$ ゆえ，$\mathfrak{a}' = \mathfrak{a}\eta^{-1}$ について，$\mathfrak{a}'^\gamma = \mathfrak{a}'$, $[\mathfrak{a}] = [\mathfrak{a}'] \in B_n'$．ゆえに，$B_n = B_n'$ である．

命題1より $G_{\{q_1\}}(\mathbb{Q}_n) \simeq A_{\{q_1\}}(\mathbb{Q}_n)$ は巡回群であるが，その位数が p であると仮定する．すると $A_{\{q_1\}}(\mathbb{Q}_n) \simeq A_{\{q_1\}}(\mathbb{Q})$ であるので，$A_{\{q_1\}}(\mathbb{Q}_n) = B_n = B_n'$．$A_{\{q_1\}}(\mathbb{Q}_n)$ の生成元 $[\mathfrak{a}]$, $\mathfrak{a}^\gamma = \mathfrak{a}$ に対して，$\mathfrak{a}$ の素イデアル分解から，$[\mathfrak{a}] = i_{0,n}([\mathfrak{a}_0])[\mathfrak{p}_n]^z$ となる $[\mathfrak{a}_0] \in A_{\{q_1\}}(\mathbb{Q})$, $z \in \mathbb{Z}$ がとれる．ここに $i_{0,n} : A_{\{q_1\}}(\mathbb{Q}) \to A_{\{q_1\}}(\mathbb{Q}_n)$ は持ち上げ写像，$\mathfrak{p}_n$ は $\mathbb{Q}_n$ の p 上の素イデアルである．すると，仮定と定理3(3)から $[\mathfrak{a}] = [\mathfrak{p}_n]^z$ であり，ノルム写像 $N : A_{\{q_1\}}(\mathbb{Q}_n) \to A_{\{q_1\}}(\mathbb{Q})$ の全射性から，$N[\mathfrak{a}] = [p]^z$ が $A_{\{q_1\}}(\mathbb{Q})$ を生成する．ところが，$(p/q_1)_p = 1$ ゆえ p は $\mathbb{Q}_{\{q_1\}}$ で完全分解するので，矛盾である．ゆえに，$G_{\{q_1\}}(\mathbb{Q}_n)$ の位数は p^2 以上である． □

補題2． $n \geq 1$ に対して，$A_{\{q_2\}}((\mathbb{Q}_{\{q_1\}})_n)$ は巡回群である．

（証明）合成体 $K = \mathbb{Q}_{\{q_1\}}\mathbb{Q}_{\{q_2\}}$ は $\mathbb{Q}$ 上 (p,p) 拡大である．$K_n = (\mathbb{Q}_{\{q_1\}})_n\mathbb{Q}_{\{q_2\}}$ は $(\mathbb{Q}_{\{q_1\}})_n$ 上 $\{q_2\}$ 外不分岐 p 次拡大であり，ここで $(\mathbb{Q}_{\{q_1\}})_n$ の q_2 上の素点は完全分岐する．$A_{\{q_2\}}((\mathbb{Q}_{\{q_1\}})_n)$ が巡回群でないと仮定すると，K_n と異なる $(\mathbb{Q}_{\{q_1\}})_n$ 上 $\{q_2\}$ 外不分岐 p 次拡大 F が存在する．K_nF は $(\mathbb{Q}_{\{q_1\}})_n$ 上 $\{q_2\}$ 外不分岐 (p,p) 拡大であり，この拡大における q_2 上の素点の惰性群は巡回群でなければならないので，K_nF

は K_n 上不分岐 p 次拡大である．よって，$G_\emptyset(K_\infty) \neq \{1\}$ となるが，p 冪剰余に関する条件と [9] Theorem 1 から[5] $G_\emptyset(K_\infty) = \{1\}$ であることに矛盾する．よって，$A_{\{q_2\}}((\mathbb{Q}_{\{q_1\}})_n)$ は巡回群である． □

$n \geq 1$ とする．$G_S(\mathbb{Q}_n)^{ab}$ における q_1 上の素点の惰性群 I_{q_1} は唯一つなので，次の完全列が得られる．

$$0 \longrightarrow I_{q_1} \longrightarrow G_S(\mathbb{Q}_n)^{ab} \longrightarrow G_{\{q_2\}}(\mathbb{Q}_n)^{ab} \longrightarrow 0$$

I_{q_1} は馴分岐な素点の惰性群なので巡回群であり，定理 1 から $G_{\{q_2\}}(\mathbb{Q}_n)^{ab} \simeq \mathbb{Z}/p\mathbb{Z}$ である．命題 1 より $\operatorname{rank} G_S(\mathbb{Q}_n)^{ab} = 2$ であって，補題 1 から全射 $G_S(\mathbb{Q}_n)^{ab} \twoheadrightarrow G_{\{q_1\}}(\mathbb{Q}_n)^{ab} \twoheadrightarrow \mathbb{Z}/p^2\mathbb{Z}$ が存在するので，$G_S(\mathbb{Q}_n)^{ab} \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p^{N_n}\mathbb{Z}$, $(N_n \geq 2)$.

$G_S(\mathbb{Q}_n)^{ab}$ において，rank が 2 の極大部分群 $\overline{H}$ が唯一つ存在する．$(\mathbb{Q}_{\{q_2\}})_n(\mathbb{Q}_n)_{\{q_1\}}$ は $\mathbb{Q}_n$ 上および $(\mathbb{Q}_{\{q_1\}})_n$ 上 S 外不分岐アーベル p 拡大であって，補題1より $(\mathbb{Q}_{\{q_1\}})_n \subsetneq (\mathbb{Q}_n)_{\{q_1\}}$ ゆえ，$\operatorname{rank}\operatorname{Gal}((\mathbb{Q}_{\{q_2\}})_n(\mathbb{Q}_n)_{\{q_1\}}/(\mathbb{Q}_{\{q_1\}})_n) = 2$ である．よって，その極大部分群 $\overline{H}$ には $(\mathbb{Q}_{\{q_1\}})_n$ が対応する．

$G_S((\mathbb{Q}_{\{q_1\}})_n)^{ab}$ における q_1 上の素点の惰性群 I'_{q_1} も唯一つゆえ，次の完全列を得る．

$$0 \longrightarrow I'_{q_1} \longrightarrow G_S((\mathbb{Q}_{\{q_1\}})_n)^{ab} \longrightarrow A_{\{q_2\}}((\mathbb{Q}_{\{q_1\}})_n) \longrightarrow 0$$

I'_{q_1} は巡回群であり，補題2より $A_{\{q_2\}}((\mathbb{Q}_{\{q_1\}})_n)$ も巡回群．$G_S((\mathbb{Q}_{\{q_1\}})_n)^{ab} \twoheadrightarrow \overline{H}$ であるので，$\operatorname{rank} G_S((\mathbb{Q}_{\{q_1\}})_n)^{ab} = 2$ である．

$n \geq 1$ を固定し，$G = G_S(\mathbb{Q}_n)^{metab}$ (metabelian quotient)，$N = N_n \geq 2$ とすると，$G^{ab} \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p^{N_n}\mathbb{Z}$．$G$ の $(\mathbb{Q}_{\{q_1\}})_n$ に対応する極大部分群 H について，$H^{ab} \simeq G_S((\mathbb{Q}_{\{q_1\}})_n)^{ab}$ である．よって，次のような G の生成元 a, b が存在する．

$$G = \langle\, a, b \,\rangle\ ,\quad a^p, b^{p^N} \in G_2\ ,\quad H = \langle\, a, b^p, G_2 \,\rangle$$

双線形な全射 $[\ ,\ ] : G/G_2 \otimes G/G_2 \twoheadrightarrow G_2/G_3$ から，$[a, b^p] \equiv [a, b]^p \equiv [a^p, b] \equiv 1 \pmod{G_3}$, $G_2/G_3 = \langle\, [a, b]G_3 \,\rangle \simeq \mathbb{Z}/p\mathbb{Z}$ であるので，$H = \langle\, a, b^p, [a, b], G_3 \,\rangle$ であって，H/G_3 はアーベル群である．$H^{ab} \twoheadrightarrow H/G_3$ ゆえ $\operatorname{rank} H/G_3 = \dim_{\mathbb{F}_p} H/H^pG_3 = 2$ であるので，a, b^p, $[a, b]$ の間には次のような非自明な関係式が存在する．

$$a^x b^{py} [a, b]^z \equiv 1 \pmod{H^pG_3}\ ,\quad x, y, z \in \mathbb{Z}_p\ ,\quad (x, y, z) \not\equiv (0, 0, 0) \pmod{p}$$

$H^p = \langle\, a^p, b^{p^2}, G_3 \,\rangle$ ゆえ，$a^x b^{py} [a, b]^z \equiv a^{px'} b^{p^2 y'} \pmod{G_3}$, $x', y' \in \mathbb{Z}_p$，即ち $[a, b]^{-z} \equiv a^{x - px'} b^{p(y - py')} \pmod{G_3}$ となる．このとき，$a^{x-px'} b^{p(y-py')} \in G_2$ であるので，$x - px' \equiv 0 \pmod{p}$, $y - py' \equiv 0 \pmod{p^{N-1}}$．特に $x \equiv y \equiv 0 \pmod{p}$ ゆえ $z \in \mathbb{Z}_p^\times$ でなければならず，$x_1 = -(x - px')z^{-1}/p$, $x_2 = -(y - py')z^{-1}/p^{N-1} \in \mathbb{Z}_p$ とおけば

$$[a, b] \equiv a^{px_1} b^{p^N x_2} \pmod{G_3}$$

[5] $p_i = q_2$, $p_j = q_1$, $y = 0$ として，$(q_1/q_2)_p = (p/q_2)_p^{-x} \in \langle\, \zeta_p \,\rangle = \langle\, (p/q_2)_p \,\rangle$, $q_2 = q_1^{-z} \in 1 + p\mathbb{Z}_p = \langle\, q_1 \,\rangle$ となる x, z を選べばよい．

となる．一方，$a^p,\, b^{p^N} \in G_2$ ゆえ，次のように書ける．

$$a^p \equiv [a,b]^{z_1}\ ,\ b^{p^N} \equiv [a,b]^{z_2} \,(\mathrm{mod}\, G_3)\ ,\quad z_1, z_2 \in \mathbb{Z}_p$$

先の式に代入すると $[a,b]^{x_1z_1+x_2z_2} \equiv [a,b] \,(\mathrm{mod}\, G_3)$ ゆえ，$x_1z_1 + x_2z_2 \equiv 1 \,(\mathrm{mod}\, p)$ である．よって，$z_1,\, z_2$ のどちらか一方は $\mathbb{Z}_p^\times$ の元である．ゆえに，$C = \langle\, a, G_3 \,\rangle$ または $\langle\, b, G_3 \,\rangle$ について，$G_2/G_3 \subset C/G_3$ であり，C/G_3 は G/G_3 の正規部分群となる．$G/C,\, C/G_3$ はともに巡回群となり，完全列

$$1 \longrightarrow C/G_3 \longrightarrow G/G_3 \longrightarrow G/C \longrightarrow 1$$

から $G/G_3 = G/\Phi(G_2)G_3$ は metacyclic であるので，命題 2 より，G は metacyclic である．$G_S(\mathbb{Q}_n)$ の交換子群に Burnside の基定理を適用して，$G_S(\mathbb{Q}_n)$ も metacyclic であることがわかる．

制限写像に関して $G_S(\mathbb{Q}_\infty) \simeq \varprojlim G_S(\mathbb{Q}_n)$ であるので，$G_S(\mathbb{Q}_\infty)$ は pro-p 群として metacyclic である． □

参考文献

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

[2] T. Fukuda, *Remarks on $\mathbb{Z}_p$-extensions of number fields*, Proc. Japan Acad. Ser. A **70** (1994), 264–266.

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

[4] F. Hajir and C. Maire, *Unramified subextensions of ray class field towers*, J. Algebra **249** (2002), 528–543.

[5] H. Koch, *Galois theory of p-extensions*, Springer Monographs in Mathematics, Springer-Verlag Berlin Heidelberg, 2002.

[6] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields*, Grundl. Math. Wiss. **323**, Springer-Verlag Berlin Heidelberg, 2000.

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

[8] Y. Taguchi, “Fontaine-Mazur 予想の紹介”, 数理解析研究所講究録 **1097** (1999), 37–49.

[9] G. Yamamoto, *On the vanishing of Iwasawa invariants of absolutely abelian p-extensions*, Acta. Arith. **94** (2000), no. 4, 365–371.

Yasushi Mizusawa
Department of Mathematics
Nagoya Institute of Technology
Gokiso-cho, Showa-ku, Nagoya
Aichi 466-8555 JAPAN
mizusawa@nitech.ac.jp