数理解析研究所講究録 1451 巻 2005 年 225-232

虚 2 次体の円分 $\mathbb{Z}_2$ 拡大上の可換 2-類体塔

Abelian 2-class field towers over the cyclotomic $\mathbb{Z}_2$-extensions of imaginary quadratic fields

早稲田大学　理工　学振　水沢　靖 (Yasushi Mizusawa)
Department of Mathematical Sciences, Waseda Univ.

島根大学　総合理工　尾崎　学 (Manabu Ozaki)
Department of Mathematics, Shimane Univ.

§1. Introduction

素数 l（後に $l=2$）を固定して考える．代数体 k に対して、その最大不分岐 pro-l 拡大 $\widetilde{L}(k)/k$ の Galois 群 $G=\mathrm{Gal}(\widetilde{L}(k)/k)$ を考える．その閉交換子群を $G^{(1)}=(G,G)$ と定め、各自然数 i に対して帰納的に $G^{(i+1)}=(G^{(i)},G^{(i)})$ と定める．すると以下のように G の交換子群列が得られるが、各 $G^{(i)}$ の固定体を $L^i(k)$ と定めることにより、対応する k 上不分岐な拡大体の列が得られる：

$$\begin{array}{ccccccccc} G & \supseteq & G^{(1)} & \supseteq & \cdots & \supseteq & G^{(i)} & \supseteq & \cdots & \supseteq & \{1\} \\ & & & & \updownarrow & & & & & & \\ k & \subseteq & L(k) & \subseteq & \cdots & \subseteq & L^i(k) & \subseteq & \cdots & \subseteq & \widetilde{L}(k) \end{array}$$

ここに $L(k)=L^1(k)$ は k の最大不分岐アーベル pro-l 拡大体であり、$L^{i+1}(k)=L(L^i(k))$ である．特に有限次代数体 k に対して $L(k)$ はその Hilbert l-類体に他ならず、Galois 群 $\mathrm{Gal}(L(k)/k)\simeq G/G^{(1)}$ は k のイデアル類群の l-Sylow 部分群 $A(k)$ と同型である．上の不分岐拡大の列は l-類体を次々に取ることによって得られていることから、k の「l-類体塔」と呼ばれている．

その研究の歴史からも見てとれるように、l-類体塔の Galois 群は非常に “mysterious” な対象である．有限次代数体 k に対して l-類群 $A(k)$ の階数が単数群 $E(k)$ の階数に比べて十分大きい時に、l-類体塔の Galois 群 G が無限群となることを示したのが Golod-Šafarevič の結果であった．その一方で、l-類体塔の Galois 群 G の構造には様々な有限 l-群も表れる．その中でも Galois 群 G がアーベル群（即ち $G\simeq A(k)$）であるとき「k は可換 l-類体塔を持つ」といい、特に可換 2-類体塔を持つ 2 次体は全て決定され、無数に存在することが示されている（Benjamin-Lemmermeyer-Snyder [1] [2] 等参照）．一般に Galois 群 G の構造を完全に記述することは難しい課題であるが、その一部として、Galois 群 G はいつアーベル群となるか？（何が Galois 群 G をアーベル群と成らしめているか？）という問題が考えられる．

本稿では [6] [7] 等における非アーベル岩澤理論研究の中の一つとして、この問題を「円分 $\mathbb{Z}_l$ 拡大（特に $l=2$）」の上で考える．l-類体塔の Galois 群はその代数体に付随する pro-l 基本群として見ることもでき、また関数体の係数拡大との類似の観点からも、l-類体塔を個々の代数体に対して考えるだけでなく円分 $\mathbb{Z}_l$ 拡大の上で考察することにより、より深く捉えることができるのではないかという期待がある．その一歩として本稿では

$l=2$ の場合を考え、虚 2 次体 k の円分 $\mathbb{Z}_2$ 拡大体 k_∞ に対して、Galois 群 $\mathrm{Gal}(\widetilde{L}(k_\infty)/k_\infty)$ がアーベル群となるための必要十分条件を与える.

§ 2. Results

正整数 m は平方因子を持たないとして、虚 2 次体 $k=\mathbb{Q}(\sqrt{-m})$ を考える. 各非負整数 $n\geq 0$ に対して、k に $\cos(2\pi/2^{n+2})$ を添加した体を k_n とし、それら全ての合成体を $k_\infty=k\bigl(\cos(2\pi/2^{n+2})\bigm| n\geq 0\bigr)$ とおく. すると

$$k\subset k_1\subset k_2\subset\cdots\subset k_n\subset\cdots\subset k_\infty$$

なる拡大体の列が得られるが、k_n/k は 2^n 次巡回拡大であり、無限次拡大 k_∞/k の Galois 群は 2-進整数環 $\mathbb{Z}_2$ の加法群と位相群として同型である. この k_∞ が、k の円分 $\mathbb{Z}_2$ 拡大体に他ならない. 我々は k_∞ および各中間体 k_n に対して、その最大不分岐 pro-2 拡大（即ち 2-類体塔）の Galois 群

$$\widetilde{G}=\mathrm{Gal}(\widetilde{L}(k_\infty)/k_\infty)\,,\quad \widetilde{G}_n=\mathrm{Gal}(\widetilde{L}(k_n)/k_n)$$

を考える. Galois 群 $\widetilde{G}$ のアーベル商 $\widetilde{G}/\widetilde{G}^{(1)}$ は、岩澤加群 $X=\varprojlim A(k_n)$（ノルム写像による射影極限）と同型である. Ferrero-Washington の定理によって岩澤加群 X は有限生成 $\mathbb{Z}_2$ 加群であることがわかり、さらに Ferrero [4] の定理によって、その $\mathbb{Z}_2$ 加群としての構造は完全に記述できる. 特に、Galois 群 $\widetilde{G}$ は有限生成 pro-2 群である. ここで

$$X^{(2)}=\widetilde{G}^{(1)}/(\widetilde{G}^{(1)},\widetilde{G})\,,\quad X_n^{(2)}=\widetilde{G}_n^{(1)}/(\widetilde{G}_n^{(1)},\widetilde{G}_n)$$

と定める. 前者は [6] [7] 等で定義された「2 次岩澤加群」であり、制限写像から誘導される射影極限によって $X^{(2)}=\varprojlim X_n^{(2)}$ と表される. このことから直ちに、

> Galois 群 $\widetilde{G}$ がアーベル群であることと、十分大きな全ての n に対して $\widetilde{G}_n$ がアーベル群である（即ち k_n が可換 2-類体塔を持つ）ことは同値である

という事実が導かれる. 本稿の主結果は、次の定理である.

定理. 虚 2 次体 k に対して、その円分 $\mathbb{Z}_2$ 拡大体 k_∞ の最大不分岐 pro-2 拡大の Galois 群 $\widetilde{G}=\mathrm{Gal}(\widetilde{L}(k_\infty)/k_\infty)$ がアーベル群となるための必要十分条件は、k の判別式の最大奇数因子 m^* が以下の表のいずれかのように素因数分解されることであり、また各場合における $\widetilde{G}$ の（pro-2 群としての）構造も表の通りである. ここに p, q, q_i は奇素数を表し、$P(T)\in\mathbb{Z}_2[T]$ は岩澤加群 $X\simeq\widetilde{G}/\widetilde{G}^{(1)}$ に付随する「岩澤多項式」である.

虚 2 次体 $k=\mathbb{Q}(\sqrt{-m})$ に対して $k_1=k(\sqrt{2})$ であるので、k と $k^\vee=\mathbb{Q}(\sqrt{-2m})$ は円分 $\mathbb{Z}_2$ 拡大を共有する. よって上の定理に関しては、m は奇数（即ち $m^*=m$）であるという仮定の下で議論してよい. 円分 $\mathbb{Z}_2$ 拡大 k_∞/k における分岐素点は素数 2 の上の素イデアルのみであるが、この仮定の下、それらは k_∞/k において完全分岐する. 岩澤多項式に

m^*	素因子などの条件	$\widetilde{G} \simeq$
1 または q	$q \equiv 3\,(\bmod 8)$	0
p	$p \equiv 5\,(\bmod 8)$	$\mathbb{Z}/2\mathbb{Z}$
q	$q \equiv 7\,(\bmod 16)$	$\mathbb{Z}_2$
pq	$p \equiv 5,\ q \equiv 3\,(\bmod 8)$	
q_1q_2	$q_1 \equiv q_2 \equiv 3\,(\bmod 8)$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}_2$
p	$p \equiv 9\,(\bmod 16),\ 2^{\frac{p-1}{4}} \equiv 1\,(\bmod p)$	
$q_1q_2q_3$	$q_1 \equiv q_2 \equiv q_3 \equiv 3\,(\bmod 8)$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$
pq	$q \equiv 3\,(\bmod 8),\ p \equiv 9\,(\bmod 16),\ 2^{\frac{p-1}{4}} \equiv 1\,(\bmod p)$	
q	$q \equiv 15\,(\bmod 32),\ P(-1) \equiv 1\,(\bmod 4)$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

関する条件は $m^* = q \equiv 15\,(\bmod 32)$ の場合にのみ表れているが、一般に岩澤多項式 $P(T)$ は次のように定義される．

$\Gamma = \mathrm{Gal}(k_\infty/k) \simeq \mathbb{Z}_2$ の位相的生成元 γ として、全ての $n \geq 0$ に対して $\gamma\big(\cos(2\pi/2^{n+2})\big) = \cos(5\cdot 2\pi/2^{n+2})$ なるものを取る．この γ と $1+T$ を対応させることにより、完備群環 $\mathbb{Z}_2[[\Gamma]]$ と冪級数環 $\Lambda = \mathbb{Z}_2[[T]]$ との間の同型を固定し、必要に応じてこの両者を同一視する．岩澤加群 X は有限生成捩れ Λ 加群であり、その特性多項式

$$P(T) = \det\big(T\cdot id - (\gamma-1)\,\big|\, X \otimes_{\mathbb{Z}_2} \mathbb{Q}_2\big) \ \in \mathbb{Z}_2[T] \subset \Lambda$$

として、岩澤多項式が定まる．m は奇数であるとして、虚 2 次体 k に対応する Dirichlet 指標を χ とする．4 を法として定義される Teichmüller 指標を ω とすると、対応する 2 進 L 関数は岩澤冪級数 $f_\chi(T) \in \Lambda$ を用いて

$$L_2(s, \omega\chi^{-1}) = f_\chi(5^s - 1)$$

と表される．Mazur-Wiles の定理（岩澤主予想）により、岩澤多項式 $P(T)$ はこの岩澤冪級数 $f_\chi(T)$ の distinguihed 多項式部分に等しい：

$$\frac{1}{2}f_\chi(T) = P(T) \times \big(\text{ある}\ \Lambda\ \text{の単数}\big)$$

特に $m = m^* = q \equiv 15\,(\bmod 32)$ である時、Ferrero [4] の定理から $P(T)$ は 3 次の多項式かつ $P(0) = 0$ であることがわかり、Λ 加群として $X \simeq \Lambda/P(T)\Lambda$ であることも示される．岩澤多項式を

$$P(T) = (1+T)^3 + b_2(1+T)^2 + b_1(1+T) + b_0 \qquad \big(\, b_i \in \mathbb{Z}_2^\times \,\big)$$

と表したとき、$P(-1) = b_0 \equiv 1\,(\bmod 2)$ である．岩澤冪級数 $f_\chi(T)$ は Stickelberger 元の極限として得られており、その計算によって、岩澤多項式 $P(T)$ の係数を 2 進近似計算することができる．実際の計算から、$m = q = 47,\ 271,\ 367, \ldots$ に対して $P(-1) \equiv 1\,(\bmod 4)$ 即

ち $\widetilde{G}$ はアーベル群であり、一方 $m=q=79,\ 239,\ 431,\ldots$ に対しては $P(-1)\equiv 3\ (\mathrm{mod}\,4)$ 即ち $\widetilde{G}$ は非可換であることが確認できる.

§ 3. Outline of The Proof

本節では、定理の証明の概略を簡潔に述べる. $m=m^*$ は平方因子をもたない奇数として、虚2次体 $k=\mathbb{Q}(\sqrt{-m})$ を考える. $m=1$ である場合は $\widetilde{G}=\{1\}$ であることが知られているので、以下、$m>1$ であると仮定する.

$\boxed{\textbf{Step 1}}$ Schur multiplier に関する議論（中心拡大の理論）から、k_n が可換2-類体塔を持つならば $\operatorname{rank}A(k_n)\le(1+\sqrt{1+8\operatorname{rank}(E(k_n)/E(k_n)^2)})/2$ であることが知られている（[2] Prop. 4 等参照）. ここでは円分 $\mathbb{Z}_2$ 拡大上において、その不等式を精密化する.

各 n に対して $E(k_n)$ はほぼ「円単数」で生成されるので、その性質から

$$\mathcal{H}=\varprojlim(\,E(k_n)/E(k_n)\cap N_{L(k_n)/k_n}L(k_n)^{\times}\,)$$

（ノルム写像による射影極限）が定義され、Λ 加群として巡回的であることがわかる. さらに中心拡大の理論から、Λ 加群としての完全列

$$0\to\mathcal{H}\to H_2(X,\mathbb{Z}_2)\to X^{(2)}\to 0$$

が導かれる（[7] 等を参照）. ここに $H_2(X,\mathbb{Z}_2)\simeq X\wedge X=X\otimes X/\langle\, x\otimes x\,|\,x\in X\,\rangle$ であり、Λ の作用は $\boldsymbol{\gamma}\cdot(x\wedge y)=(\boldsymbol{\gamma}\cdot x)\wedge(\boldsymbol{\gamma}\cdot y)$（$x,\,y\in X$）なる $\boldsymbol{\gamma}$ の作用から誘導される.

ここで $\widetilde{G}$ がアーベル群であるとすると、$X^{(2)}=0$ であるので、$H_2(X,\mathbb{Z}_2)$ も Λ 加群として巡回的、即ち $(X/2X)\wedge(X/2X)$ は $\mathbb{F}_2[[T]]$ 加群として巡回的である. このことから、$\operatorname{rank}X=\dim_{\mathbb{F}_2}(X/2X)\le 3$ でなければならないことが導かれる. よって以下では、$\operatorname{rank}X\le 3$ なる虚2次体 $k=\mathbb{Q}(\sqrt{-m})$ について $\widetilde{G}$ がアーベル群かどうかを調べればよい. Ferrero [4] の定理を用いてそのような m を分類すると、以下の表のようになる.

$\boxed{\textbf{Step 2}}$ Step 1 で得た分類表の各場合において、$\widetilde{G}$ がアーベル群かどうかを調べる. 表の S2, I1, S9 の場合を除いて、$k(\sqrt{d})$ が k 上不分岐となるような m の約数 $d>1$ が存在する. そのような d を表のように取り、$F=k(\sqrt{d})$、$k'=\mathbb{Q}(\sqrt{-m/d})$ と定める. その円分 $\mathbb{Z}_2$ 拡大の 2^n 次部分拡大 F_n/F, k'_n/k' は、有理数体の円分 $\mathbb{Z}_2$ 拡大の 2^n 次中間体 $\mathbb{Q}_n=\mathbb{Q}\bigl(\cos(2\pi/2^{n+2})\bigr)$ との合成で得られる. k_n, F_n, k'_n は総虚な $\mathbb{Q}$ 上アーベル拡大体であり、その相対類数は一般 Bernoulli 数などを用いて表される（[10] Th. 4.17 等参照）. それを用いて相対類数を比較すると、

$$\#A(F_n)=\frac{1}{2}\#A(k_n)\cdot\bigl(\,Q(F_n)\#A(F_n^+)\#A(k'_n)\,\bigr)$$

なる等式を得る. ここに $Q(F_n)=(\,E(F_n)\,:\,W(F_n)E(F_n^+)\,)\le 2$ であり、$F_n^+=\mathbb{Q}_n(\sqrt{d})$ は F_n の最大実部分体、$W(F_n)$ は F_n に含まれる1の冪根全体の成す群である. この式と [2] Prop. 7 などの群論的な議論により、次の事実が得られる.

[rank $X \leq 3$ なる虚2次体 $k=\mathbb{Q}(\sqrt{-m})$ を与える $m>1$]

	m	素因子に関する条件	$X \simeq$	d	$\widetilde{G} \simeq X$?
R1	p	$p \equiv 5 \pmod 8$	$\mathbb{Z}/2\mathbb{Z}$	p	Yes
R2	q_1q_2	$q_1 \equiv q_2 \equiv 3 \pmod 8$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}_2$	q_2	
R3	p	$p \equiv 9 \pmod{16}$		p	Yes/No
R4	p_1p_2	$p_1 \equiv p_2 \equiv 5 \pmod 8$		p_1	No
R5	pq_1q_2	$p \equiv 5,\ q_1 \equiv q_2 \equiv 3 \pmod 8$	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}_2^{\oplus 2}$	q_1q_2	
R6	$p_1p_2p_3$	$p_1 \equiv p_2 \equiv p_3 \equiv 5 \pmod 8$		p_1p_2	
R7	q_1q_2	$q_1 \equiv 3 \pmod 8,\ q_2 \equiv 7 \pmod{16}$		q_1	
R8	p_1p_2	$p_1 \equiv 5 \pmod 8,\ p_2 \equiv 9 \pmod{16}$		p_1	
S1	pq	$p \equiv 5,\ q \equiv 3 \pmod 8$	$\mathbb{Z}_2$	p	Yes
S2	q	$q \equiv 7 \pmod{16}$		無し	
I1	q	$q \equiv 3 \pmod 8$	0		
I2	$q_1q_2q_3$	$q_1 \equiv q_2 \equiv q_3 \equiv 3 \pmod 8$	$\mathbb{Z}_2^{\oplus 2}$	q_2q_3	
I3	pq	$p \equiv 9 \pmod{16},\ q \equiv 3 \pmod 8$		p	Yes/No
I4	p_1p_2q	$p_1 \equiv p_2 \equiv 5,\ q \equiv 3 \pmod 8$		p_1	No
I5	pq	$p \equiv 5\,(8),\ q \equiv 7 \pmod{16}$		p	
S3	$p_1p_2p_3q$	$p_1 \equiv p_2 \equiv p_3 \equiv 5,\ q \equiv 3 \pmod 8$	$\mathbb{Z}_2^{\oplus 3}$	p_1	
S4	$pq_1q_2q_3$	$p \equiv 5,\ p_1 \equiv p_2 \equiv p_3 \equiv 3 \pmod 8$		p	
S5	p_1p_2q	$p_1 \equiv 5,\ q \equiv 3 \pmod 8,\ p_2 \equiv 9 \pmod{16}$		p_2	
S6	p_1p_2q	$p_1 \equiv p_2 \equiv 5 \pmod 8,\ q \equiv 7 \pmod{16}$		p_1	
S7	$q_1q_2q_3$	$q_1 \equiv q_2 \equiv 3 \pmod 8,\ q_3 \equiv 7 \pmod{16}$		q_1q_2	
S8	pq	$p \equiv 9,\ q \equiv 7 \pmod{16}$		p	
S9	q	$q \equiv 15 \pmod{32}$		無し	**Step 3**

整数 m は平方因子を持たない奇数とし、p, p_i, q, q_i は素数を表す. また、各場合の R$*$, I$*$, S$*$ はそれぞれ、$k/\mathbb{Q}$ において素数2が分岐, 惰性, 分解する場合であることを表す.

$\widetilde{G}_n$ がアーベル群であるならば、$\#A(F_n)=\frac{1}{2}\#A(k_n)$ 即ち $Q(F_n)=\#A(F_n^+)=\#A(k'_n)=1$ である．rank $X\leq 2$ ならば、この逆も成り立つ．

この条件が全ての n に対して成り立つかどうかを、Ferrero [4] の定理および尾崎-田谷 [8] の定理を用いて検証することにより、d が存在するものについては $\widetilde{G}$ がアーベル群であるかどうか（即ち $\widetilde{G}\simeq X$ かどうか）を判定できる．特に R3, I3 の場合には、全ての n に対して $Q(F_n)=\#A(k'_n)=1$ が成り立っており、$\widetilde{G}$ がアーベル群であることは、全ての n に対して $\#A(F_n^+)=1$ 即ち $2^{\frac{p-1}{4}}\equiv 1\pmod p$（[8] 参照）であることと同値となる．この R3, I3 の場合を除いて $\widetilde{G}$ がアーベル群でないことが帰結される場合（表で「No」となっている場合）は全て、ある $n\geq 0$ に対して $\#A(k'_n)\neq 1$ であることから判定できる．d が存在しない S2, I1 および R1, S1 の場合は、岩澤加群 X が巡回群なので明らかに $\widetilde{G}\simeq X$ である．よって残るは、S9 の場合の判定である．

$\boxed{\textbf{Step 3}}$ 以下、m は素数 $q\equiv 15\pmod{32}$ であると仮定し、表の S9 の場合を考える．一般に、pro-2 群 G の閉部分群X, Y とその元 $x\in \mathsf{X}$, $y\in \mathsf{Y}$ に対して $(x,y)=xyx^{-1}y^{-1}$、${}^{x}y=xyx^{-1}$ と定め、(X,Y) はそのような (x,y) で生成される G の閉部分群とする．さらに 有限2-群 G に対して、その位数2の元で生成される部分群を $G\{2\}$、平方元で生成される部分群を G^2 で表す．

十分大きな n に対して、Galois 群 $G_n=\mathrm{Gal}(L(k_n)/\mathbb{Q})$ を考える．2-拡大 $L(k_n)/\mathbb{Q}$ において分岐する素数は2と q のみであり、その上の $L(k_n)$ の素イデアルを一つ固定して、その分解群を Z_2, Z_q、惰性群を I_2, I_q とおく．惰性群はそれぞれ位数 2^n, 2 の巡回群であり、その生成元を $\overline{\gamma}\in I_2$, $\overline{\delta}\in I_q$ と定める．但し、$\overline{\gamma}\big(\cos(2\pi/2^{n+2})\big)=\cos(5\cdot 2\pi/2^{n+2})$ なるものとする．交換子群 (G_n,G_n) の固定体は k_n であり、G_n は $\overline{\gamma}$, $\overline{\delta}$ で生成される階数2の有限2-群であることがわかる．この $\overline{\gamma}$ は先に定めた Γ の生成元 $\boldsymbol{\gamma}$ と対応し、$\overline{x}\in(G_n,G_n)$ に対して Γ の作用を $\boldsymbol{\gamma}\cdot\overline{x}={}^{\overline{\gamma}}\overline{x}=\overline{\gamma}\,\overline{x}\,\overline{\gamma}^{-1}$ で定める．さらに $\nu_n=((1+T)^{2^n}-1)/T\in\Lambda$ と定めると、Λ 加群として

$$(G_n,G_n)\simeq A(k_n)\simeq X/\nu_nX\simeq \Lambda/(\nu_n,P(T))$$

となり、$\overline{\boldsymbol{x}}=(\overline{\gamma},\overline{\delta})$ は (G_n,G_n) の Λ 上の生成元となる．

2つの文字 γ,δ で生成される自由 pro-2 群を $F=\langle\gamma,\ \delta\rangle$ とする．γ,δ をそれぞれ $\overline{\gamma}$, $\overline{\delta}$ に送ることにより、群の表示

$$1\to R\to F\to G_n\to 1$$

が得られる．一般に $x\in F$ に対して $\overline{x}=xR\in G_n$ と表し、(F,F) の元 $\boldsymbol{x}=(\gamma,\delta)$、${}^{P(T)}\boldsymbol{x}=\boldsymbol{x}^{b_0}({}^{\gamma}\boldsymbol{x})^{b_1}({}^{\gamma^2}\boldsymbol{x})^{b_2}({}^{\gamma^3}\boldsymbol{x})$、$\beta={}^{P(T)/T}\boldsymbol{x}=\boldsymbol{x}^{1+b_1+b_2}({}^{\gamma}\boldsymbol{x})^{1+b_2}({}^{\gamma^2}\boldsymbol{x})$ を定める．上で述べた (G_n,G_n) の Λ 加群構造をふまえることにより、F の正規部分群 R は次のように、4つの元の共役元で生成されることが導かれる：

$$R=\left\langle\ \gamma^{2^n},\ \delta^2,\ (\boldsymbol{x},{}^{\gamma}\boldsymbol{x}),\ {}^{P(T)}\boldsymbol{x}\ \right\rangle_F$$

さらに、$L(k_n)/\mathbb{Q}$ における素イデアルの分解状況を調べることにより、分解群 Z_2, Z_q はそれぞれ $\{\,\overline{\gamma},\ \overline{\beta}\,\}$, $\{\,\overline{\gamma}^4\overline{\alpha},\ \overline{\delta}\,\}$ で生成される階数 2 のアーベル群であることがわかる．この $\overline{\alpha}$ は、$(\overline{\gamma}^4\overline{\alpha}, \overline{\delta}) = 1$ なる性質を持つ (G_n, G_n) の元、即ち $(\gamma^4\alpha, \delta) \in R$ なる $\alpha \in (F, F)$ で代表される元であるが、このような $\overline{\alpha}$ は $(G_n, G_n)\{2\}$ を法として一意的に定まることがわかる．ここで $N = 2^n - 1$, $\nu_2 = ((1+T)^4 - 1)/T$ とし、

$$F(T) = \frac{\nu_n}{\nu_2}\cdot\left(\frac{P(T)-\nu_2}{2}\right) = \sum_{i=0}^{N} d_i(1+T)^i \ \in \Lambda$$

と定める．各 i に対して $\mathbf{i} \equiv i \pmod 4$ なる $0 \le \mathbf{i} \le 3$ を定め、便宜上 $b_3 = 1$ とすると、$d_i = (b_{\mathbf{i}} - 1)/2$ である．Λ 加群構造から $A(k_n)\{2\} = F(T)A(k_n)$ であることが示せるので、$t = \boldsymbol{x}^{d_0}({}^{\gamma}\boldsymbol{x})^{d_1}({}^{\gamma^2}\boldsymbol{x})^{d_2}\cdots({}^{\gamma^N}\boldsymbol{x})^{d_N}$ の像 $\overline{t}$ は $(G_n, G_n)\{2\}$ の Λ 上の生成元となる．さらに $\alpha_0 = {}^{\gamma^{-4}}\big(\boldsymbol{x}^{d_0}({}^{\gamma}\boldsymbol{x})^{d_1}({}^{\gamma^2}\boldsymbol{x})^{d_2}\big) \in (F, F)$ は $(\overline{\gamma}^4\overline{\alpha_0}, \overline{\delta}) = 1$ を満たすことがわかるので、ある $\varepsilon_0, \varepsilon_1, \varepsilon_2 \in \{0, 1\}$ と $r \in R$ とによって、$\alpha = \alpha_0\big(t^{\varepsilon_0}({}^{\gamma}t)^{\varepsilon_1}({}^{\gamma^2}t)^{\varepsilon_2}\big)r$ と表される．

ここで、2-拡大 $L(k_n)/\mathbb{Q}$ に関する中心類体 L_n^{c} を考える．中心拡大の理論により、Galois 群 $\mathcal{K} = \mathrm{Gal}(L_n^{\mathrm{c}}/L(k_n))$ は $L(k_n)/\mathbb{Q}$ に関する「Scholz の number knot」と同型であり、

$$H_2(Z_2, \mathbb{Z}) \oplus H_2(Z_q, \mathbb{Z}) \xrightarrow{\phi} H_2(G_n, \mathbb{Z}) \to \mathcal{K} \to 0$$

なる完全列が導かれる（[5] 等参照）．Hopf の定理から $H_2(G_n, \mathbb{Z}) \simeq R \cap (F, F)/(R, F)$ であり、$\mathcal{R} = (R \cap (F, F))^2(R, F)$ と定めると、計算により $(\gamma, \beta) \equiv {}^{P(T)}\boldsymbol{x}\cdot(\boldsymbol{x}, {}^{\gamma}\boldsymbol{x}) \mod \mathcal{R}$、即ち $R \cap (F, F)/\mathcal{R} = \langle\,(\gamma, \beta),\ (\boldsymbol{x}, {}^{\gamma}\boldsymbol{x})\,\rangle\mathcal{R}/\mathcal{R}$ となる．よって ϕ から

$$0 \to \langle\,(\gamma, \beta),\ (\gamma^4\alpha, \delta)\,\rangle\mathcal{R}/\mathcal{R} \xrightarrow{\Phi} \langle\,(\gamma, \beta),\ (\boldsymbol{x}, {}^{\gamma}\boldsymbol{x})\,\rangle\mathcal{R}/\mathcal{R} \to \mathcal{K}/\mathcal{K}^2 \to 0$$

なる完全列が誘導される．k_n が可換 2-類体塔を持つことは、$L(k_n)$ の類数が奇数であることと同値である．G_n が有限 2-群であるという事実から、これは $L(k_n) = L_n^{\mathrm{c}}$ であること、即ち $\mathcal{K}/\mathcal{K}^2 = \{0\}$ であることとも同値である．よって、k_n が可換 2-類体塔を持つことは、Φ が全射であることと同値となる．n は十分大きく取っていることから、群論的計算により

$$(\gamma^4\alpha, \delta) \equiv (\gamma, \beta)\cdot(\boldsymbol{x}, {}^{\gamma}\boldsymbol{x})^{1+(b_0-1)/2} \mod \mathcal{R}$$

となる．（ε_0, ε_1 ε_2 および r の値に依存しない！）半直積を用いて $G_n = (X_n \rtimes \Gamma_n) \rtimes \Delta$（ここに、$\Gamma_n = \langle\overline{\gamma}\rangle, \Delta = \langle\overline{\delta}\rangle$）と表し、[3], [9] の結果を用いて $H_2(G_n, \mathbb{Z})$ の階数を計算すると、

$$n \text{ が十分大きく } b_0 \not\equiv 1 \pmod 4 \text{ ならば、} (\gamma, \beta) \not\equiv (\boldsymbol{x}, {}^{\gamma}\boldsymbol{x}) \mod \mathcal{R}$$

であることがわかる．これらのことから、$P(-1) = b_0 \equiv 1 \pmod 4$ であることと、Galois 群 $\widetilde{G}$ がアーベル群であること（十分大きな全ての n に対して Galois 群 $\widetilde{G}_n$ がアーベル群であること）が同値となる．こうして表の S9 の場合が判定され、定理の証明が完了する．

References

[1] E. Benjamin and F. Lemmermeyer and C. Snyder, *Imaginary quadratic fields k with cyclic* $\mathrm{Cl}_2(k^1)$, J. Number Theory **67** (1997), 229–245.

[2] E. Benjamin and F. Lemmermeyer and C. Snyder, *Real quadratic fields with abelian 2-class field tower*, J. Number Theory **73** (1998), 182–194.

[3] L. Evens, *The Schur multiplier of a semi-direct product*, Illinois J. Math. **16** (1972), 166–181.

[4] B. Ferrero, *The cyclotomic* $\mathbb{Z}_2$*-extension of imaginary quadratic fields*, Amer. J. Math. **102** (1976), 447–459.

[5] A. Fröhlich, *Central extensions, Galois groups, and ideal class groups of number fields*, Contemp. Math. vol. **24**, Amer. Math. Soc., Rhode Island (1983).

[6] M. Ozaki, *Non-abelian Iwasawa formulae for unramified p-extensions*, 京都大学数理解析研究所講究録 **1376**「代数的整数論とその周辺」, (2004), 13–19.

[7] M. Ozaki, *Non-Abelian Iwasawa theory of* $\mathbb{Z}_p$*-extensions*, preprint.

[8] M. Ozaki and H. Taya, *On the Iwasawa* λ_2*-invariants of certain families of real quadratic fields*, Manuscripta Math. **94** (1997), 437–444.

[9] K. Tahara, *On the second cohomology groups of semidirect products*, Math. Z. **129** (1972), 365–379.

[10] L. C. Washington, *Introduction to Cyclotomic Fields* (2nd. Edition), Graduate Texts in Math. vol. **83**, Springer (1997).

[11] K. Yamamura, 代数体の類体塔について–入門, 早稲田大学整数論研究集会 2001 報告集, Institute of Mathematics, Waseda University (2001), 161–172.

YASUSHI MIZUSAWA

(supported by JSPS Research Fellowships for Young Scientists)

Department of Mathematical Sciences, School of Science and Engineering,
Waseda University, Okubo 3-4-1, Shinjuku-Ku, Tokyo, 169-8555 Japan
E-mail : `mizusawa@akane.waseda.jp`

MANABU OZAKI
Department of Mathematics, Faculty of Science and Engineering,
Shimane University, Nishikawatsu-Cho 1060, Matsue, 690-8504 Japan
E-mail : `ozaki@math.shimane-u.ac.jp`

※ 本稿の著者は水沢です．また、所属は 2005 年 3 月 31 日現在のものです．