ある種の実2次体の円分$\mathbb{Z}_2$拡大における岩澤λ不変量について

田中 修平

平成22年1月29日

目 次

1　はじめに

1.1　本修士論文の目的

本修士論文は福田氏，小松氏による共著論文 [2] の解説論文である．この論文では p を $p \equiv 1 \pmod{16}$ を満たす素数としたときの，実 2 次体 $\mathbb{Q}(\sqrt{p})$ の円分 $\mathbb{Z}_2$-拡大における岩澤 λ-不変量について述べている．

岩澤健吉氏が 1959 年に証明した岩澤類数公式とは，$\mathbb{Z}_p$-拡大 K/k における中間体 k_n のイデアル類群の位数の p-部分について記述した公式である．この p-部分を表わす際に用いられる不変量 μ,λ,ν について，それらがどのような整数になるかを調べることは長らく研究されてきた．しかし一般に λ-不変量は μ-不変量に比べて調べることが難しく，一般的な結果はまだほとんど得られていない．λ-不変量については Greenberg 予想と呼ばれる重要な予想が立てられており，Greenberg 予想の解決を目標として研究が進められている．

予想 1.1 (Greenberg 予想). 有限次代数体 k が総実であるとは，k の $\mathbb{Q}$ 上の共役体が全て実数体 $\mathbb{R}$ に含まれることをいう．任意の総実代数体 k と任意の素数 p に対して，$\mu_p(k) = \lambda_p(k) = 0$ である．

Greenberg 予想に関しては任意の素数 p について $\mu_p(\mathbb{Q}) = \lambda_p(\mathbb{Q}) = 0$ となることが証明されているが，他には一般に証明された事実がない．しかし，以下の 2 つの方法が Greenberg 予想の解決に有効であると考えられる：

(1) λ に対してできるだけ小さい上限を求める，

(2) $\lambda = 0$ となる具体的な場合を求める．

福田-小松 [2] ではこの (1),(2) の方法どちらに対しても新しい結果を与えている．

先ほど μ-不変量が λ-不変量よりも多くの結果が得られていると述べたが，μ-不変量については岩澤の予想と呼ばれる予想が立てられており，それが部分的に解決されているのである．

予想 1.2 (岩澤の予想). 任意の有限次代数体 k と任意の素数 p に対して，$\mu_p(k) = 0$ である．

岩澤氏はこの予想が k が Galois p-拡大の場合に成り立つことを示した．今回は 2 次体の円分 $\mathbb{Z}_2$-拡大に対して λ-不変量を調べており，μ-不変量に対する岩澤氏の方法の類似となっている．

1.2　記号の約束と一般的な定理の紹介

ここでは本論文内で用いる記号と定理の紹介をする．

定義 1.3 (Euler 関数). m を $m \geq 2$ なる整数とする．環 $(\mathbb{Z}/m\mathbb{Z})$ の乗法群 $(\mathbb{Z}/m\mathbb{Z})^\times$ の位数 $\sharp(\mathbb{Z}/m\mathbb{Z})^\times$ を，$\phi(m)$ で表わす．この ϕ を Euler 関数と呼ぶ．ただし，$\phi(1) = 1$ と約束し，Euler 関数 ϕ は自然数全体に対して定義されていると考えることにする．

簡単に言えば，$\phi(m)$ とは $1 \leq a < m$ を満たす整数 a の内，m と互いに素となるものの個数を表わしている．Euler 関数の例としては，$\phi(10) = 4$，$\phi(20) = 8$，また，素数 p に対し $\phi(p) = p - 1$ 等が考えられる．

代数体 K に対し，その整数環を O_K と表わすことにする．

定義 1.4 (整数基). K を n 次の代数体とするとき，その整数環 O_K は階数 n の自由加群である．よって，ある O_K の元 $w_1, \ldots, w_n$ が存在して，

$$O_K = \mathbb{Z}w_1 + \cdots + \mathbb{Z}w_n$$

であって，かつ O_K の任意の元 α に対して有理整数 $a_1, \ldots, a_n$ が一意的に存在して，

$$\alpha = a_1w_1 + \cdots + a_nw_n,$$

と表わせる．このような $\{w_1, \ldots, w_n\}$ を代数体 K の整数基という．

上で定義した整数基より代数体の判別式が定義される．

定義 1.5 (代数体の判別式). K を代数体，$\{w_1, \ldots, w_n\}$ を K の整数基とする．さらに，w_i の n 個の共役元を $w_i^{(1)}, \ldots, w_i^{(n)}$ と表わすことにする．このとき

$$D_K = \begin{vmatrix} w_1^{(1)} & \cdots & w_n^{(1)} \\ \vdots & & \vdots \\ w_1^{(n)} & \cdots & w_n^{(n)} \end{vmatrix}^2$$

と定義し，D_K を代数体 K の判別式と呼ぶ．判別式 D_K は K の整数基のとり方によらず K のみにより定まり，また，0 でない有理整数になる．

例 1.6. 2 次の代数体 $\mathbb{Q}(\sqrt{-1})$ の整数環 $O_{\mathbb{Q}(\sqrt{-1})}$ は $\mathbb{Z}[\sqrt{-1}]$ で，整数基は $\{1, \sqrt{-1}\}$ となる．また，$\sqrt{-1}$ の共役元は $\sqrt{-1}$ と $-\sqrt{-1}$ である．よって $\mathbb{Q}(\sqrt{-1})$ の判別式は，

$$D_{\mathbb{Q}(\sqrt{-1})} = \begin{vmatrix} 1 & \sqrt{-1} \\ 1 & -\sqrt{-1} \end{vmatrix}^2 = (-2\sqrt{-1})^2 = -4$$

となる．

本論文では代数体 K の単数群を $O_K^\times$ と表わすことにする．

次に代数体の整数環における素イデアル分解について説明する．一般に代数体の整数環では素元分解は成立しない．しかし，そのかわりに素イデアル分解が成立するのである．代数体 K の有限個の元 $\alpha_1, \ldots, \alpha_n$ に対し，

$$O_K\alpha_1 + \cdots + O_K\alpha_n = \{a_1\alpha_1 + \cdots + a_n\alpha_n |\ a_1, \ldots, a_n \in O_K\}$$

を $\alpha_1, \ldots, \alpha_n$ で生成される K の分数イデアルといい，$(\alpha_1, \ldots, \alpha_n)$ と書く．分数イデアルと区別するため，O_K のイデアルを整イデアルとよび，以降 K の分数イデアルを単に K のイデアルとよぶことにする．また，O_K の素イデアルを K の素イデアルとよぶ．I_K を 0 でない K の分数イデアル全体とする．このとき I_K の元 $A = (\alpha_1, \ldots, \alpha_n)$, $B = (\beta_1, \ldots, \beta_m)$ に対し，A と B の積を

$$AB = (\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_1\beta_m, \alpha_2\beta_1, \ldots, \alpha_n\beta_m)$$

と定義することにより，I_K は Abel 群となる．I_K を K のイデアル群という．代数体の整数環は Dedekind 環なので，素イデアル分解の一意性が成り立っている．

定理 1.7 (素イデアル分解の一意性)**.** K を代数体，A を O_K の 0 でないイデアルとする．このとき，A に対して O_K の素イデアル $P_1, \ldots, P_g$，整数 $e_1, \ldots, e_g$ が存在して，

$$A = P_1^{e_1} \cdots P_g^{e_g}$$

と分解できる．この分解は素イデアルの順序を除いて一意的である．

特に A が整イデアルであることと，$e_1, \ldots, e_g$ が全て非負整数であることは同値である．

次に代数体の類数を紹介する．

定義 1.8. K を代数体，I_K を K のイデアル群とする．このとき，K の 0 でない単項イデアル全体 $P_K = \{\alpha O_k |\ \alpha \in K^\times\}$ は I_K の部分群となり，I_K の P_K による剰余群 $\mathrm{Cl}(K) = I_K/P_K$ を K のイデアル類群，各剰余類を K のイデアル類とよぶ．また，$\mathrm{Cl}(K)$ の位数 $h_K = \sharp\mathrm{Cl}(K)$ を K の類数という．

類数とは素元分解がどれだけ成り立たないかを表わす数であり，h_k が 1 であることと O_K が単項イデアル整域であることは同値である．

次に代数体の整数環における素数 p の分解の様子を説明する．A を素数 p の単項イデアル $(p) = pO_K$ としたとき，その分解を

$$(p) = P_1^{e_1(P_1/p)} \cdots P_g^{e_g(P_g/p)} \tag{1.1}$$

と表わし，P_i を p の上の素イデアル，$e_i(P_i/p)$ を素イデアル P_i の分岐指数とよぶ．また，素イデアル分解 (1.1) を考えたとき，O_K/P_i は $\mathbb{F}_p$ の有限次拡大となっており，その拡大次数 $f_i = [O_K/P_i : \mathbb{F}_p]$ を素イデアル P_i の次数という．

定理 1.9. K を n 次の代数体とし，素数 p で生成される単項イデアル $(p) = pO_K$ の素イデアル分解が (1.1) で与えられているとする．各 P_i の次数を f_i とすると，

$$\sum_{i=1}^{g} e_i(P_i/p) f_i = n \tag{1.2}$$

が成立する．特に，$K/\mathbb{Q}$ が Galois 拡大のとき，$e_1(P_1/p) = \cdots = e_g(P_g/p)$，$f_1 = \cdots = f_g$ が成立している．このとき $1 \le i \le g$ なる任意の i に対して全て一致している $e_i(P_i/p)$，f_i をそれぞれ e，f とおくと，(1.2) より $efg = n$ が成り立つ．

定義 1.10. 素イデアル分解 (1.1) において，$e_i(P_i/p) = 1$ となる P_i は不分岐であるという．$1 \leq i \leq g$ なる任意の i について不分岐であるとき，素数 p は $K/\mathbb{Q}$ で不分岐であるという．P_i が不分岐でないとき，つまり $e_i(P_i/p) > 1$ が成り立つとき，P_i は $K/\mathbb{Q}$ で不分岐であるという．

$K/\mathbb{Q}$ で p が分岐するかどうかを判定するには，次の Dedekind の判別定理が有用である．

定理 1.11 (Dedekind の判別定理)**.** 代数体 K の判別式を D_K とする．p が $K/\mathbb{Q}$ で分岐することと，$p \mid D_K$ であることは同値である．したがって $K/\mathbb{Q}$ で分岐する素数は有限個である．

例 1.12. 例 1.4 より，$D_{\mathbb{Q}(\sqrt{-1})} = -4$ なので，$\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ で分岐する素数は 2 のみであることが分かる．

次に 2 次体における素数 p の単項イデアル (p) の分解を判定できる Kronecker 記号を紹介する．

定理 1.13 (藤崎-山本-森田 [15])**.** m を平方因子を持たない整数，$K = \mathbb{Q}(\sqrt{m})$，D_K を K の判別式とする．このとき素数 p に対し，Kronecker 記号 $\left(\frac{D_K}{p}\right)$ を以下のように定義する．

(1) p が奇素数のとき，$\left(\frac{D_K}{p}\right)$ は通常の Legendre 記号と見なす.

(2) $p = 2$ のとき，$p \equiv 1 \pmod 8$ ならば $\left(\frac{D_K}{2}\right) = 1$，$p \equiv 5 \pmod 8$ ならば $\left(\frac{D_K}{2}\right) = -1$，$2 \mid D_K$ ならば $\left(\frac{D_K}{2}\right) = 0$ と定義する．

Kronecker 記号の値により，$(p) = pO_K$ の素イデアル分解は以下のように定まる．

(A) $\left(\frac{D_K}{p}\right) = 1$ であることと (p) が完全分解すること，すなわち相異なる O_K の素イデアル P, P' が存在して $(p) = PP'$ となることは同値である．

(B) $\left(\frac{D_K}{p}\right) = -1$ であることと (p) が素イデアルで $f = [O_K/(p) : \mathbb{F}_p] = 2$ であることは同値である．

(C) $\left(\frac{D_K}{p}\right) = 0$ であることと (p) が完全分岐すること，すなわち O_K の素イデアル P が存在して $(p) = P^2$ となることは同値である．

次に有限 Abel p-群の p-rank を紹介する．

定義 1.14. p を素数，A を有限 Abel p-群とする．このとき A に対しある正の整数 a_i が存在して，

$$A \simeq \bigoplus_{a_i} \mathbb{Z}/p^{a_i}\mathbb{Z}$$

と表わせる．$a_i \geq 1$ を満たす i の個数，すなわち右辺の直和因子の個数を p-rank$A$ と表わす.

最後に p-進単数基準について述べる．K を代数体，$\overline{\mathbb{Q}}_p$ を $\mathbb{Q}_p$ の代数的閉包，$\mathbb{C}_p$ を p-進絶対付値に関しての $\overline{\mathbb{Q}}_p$ の完備化とする．$\mathbb{C}_p$ から $\mathbb{C}$ への埋め込みを一つ固定すると，K から $\mathbb{C}_p$ への埋め込みを考えることは K から $\mathbb{C}$ への埋め込みを考えることになる．r_1, r_2 をそれぞれ K の $\mathbb{Q}$ 上の共役体で実共役体であるものの個数，複素共役体の組の個数とし，$r = r_1 + r_2 - 1$ とおく．K から $\mathbb{C}_p$ への埋め込みで実共役なものを $\sigma_1, \ldots, \sigma_{r_1}$，複素共役なものを $\sigma_{r_1+1}, \overline{\sigma}_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma}_{r_1+r_2}$ とする．δ_i を σ_i が実ならば $\delta_i = 1$，σ_i が複素ならば $\delta_i = 2$ と定義する．$\varepsilon_1, \ldots, \varepsilon_r$ を K の単数として，

$$R_{K,p}(\varepsilon_1, \ldots, \varepsilon_r) = \det(\delta_i \log_p(\sigma_i \varepsilon_j))_{1 \leq i,j \leq r}$$

と定義する．

定義 1.15 (p-進単数基準)**.** $\{\varepsilon_1, \ldots, \varepsilon_r\}$ を K の単数基とする．このとき，$R_p(K) = R_{K,p}(\varepsilon_1, \ldots, \varepsilon_r)$ と定義し，$R_p(K)$ を K の p-進単数基準と呼ぶ.

謝辞

末筆になりましたが，2 年間に渡り御指導下さいました雪江明彦教授に心から感謝申し上げます．また，セミナー等でお世話になりました田嶋和明先輩，奈良忠央先輩，五十嵐健太君，小島聡史君，佐々木万喜夫君，山田洋輔君，キン ショウヒ君，吉田宏大君にも感謝します.

2　$\mathbb{Z}_p$-拡大の岩澤理論

この章では $\mathbb{Z}_p$-拡大の岩澤理論を紹介する．詳しい内容については [12] の 13 節を参照されたい．

2.1　岩澤類数公式

まず初めに代数体の $\mathbb{Z}_p$-拡大を定義する．

定義 2.1 ($\mathbb{Z}_p$-拡大)．p を素数，$\mathbb{Z}_p$ を p 進整数環とする．有限次代数体 k に対し，その拡大 K/k が $\mathbb{Z}_p$-拡大であるとは，K/k が Galois 拡大で，かつ位相群として $\mathrm{Gal}(K/k) \simeq \mathbb{Z}_p$ が成り立つことをいう．

$\mathbb{Z}_p$ の閉部分群は $\{0\}$ と $p^n\mathbb{Z}_p$ $(n \geq 0)$ のみである．よって K/k を $\mathbb{Z}_p$-拡大とし，k_n を $p^n\mathbb{Z}_p$ に対応する K/k の中間体とすると，

$$k = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_n \subseteq \cdots \subseteq \bigcup_{n\geq 0} k_n = K, \quad \mathrm{Gal}(k_n/k) \simeq \mathbb{Z}/p^n\mathbb{Z}$$

となっている．

任意の代数体 k は少なくとも一つの $\mathbb{Z}_p$-拡大を持つことが知られている．それは以下に紹介する円分 $\mathbb{Z}_p$-拡大と呼ばれる拡大である．

例 2.2 (円分 $\mathbb{Z}_p$-拡大)．p が奇素数であるとき，$n \geq 0$ に対して $\mathbb{Q}$ 上 p^n 次である $\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}$ の唯一の中間体を $\mathbb{Q}^{(n)}$ とおく．$p = 2$ の場合は $\mathbb{Q}^{(n)} = \mathbb{Q}(\cos(\frac{2\pi}{2^{n+2}}))$ とおく．このとき，

$$\mathbb{Q} = \mathbb{Q}^{(0)} \subseteq \mathbb{Q}^{(1)} \subseteq \cdots \subseteq \mathbb{Q}^{(n)} \subseteq \cdots \subseteq \mathbb{Q}_\infty = \bigcup_{n\geq 0} \mathbb{Q}^{(n)},$$

$$\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = \varprojlim \mathbb{Z}/p^n\mathbb{Z} \simeq \mathbb{Z}_p$$

が成り立っている．この拡大 $\mathbb{Q}_\infty/\mathbb{Q}$ を有理数体 $\mathbb{Q}$ の円分 $\mathbb{Z}_p$-拡大という．

任意の有限次代数体 k に対しては，$k_\infty = k\mathbb{Q}_\infty$ とおくと，Galois 拡大の推進定理より，

$$\mathrm{Gal}(k_\infty/k) = \mathrm{Gal}(k\mathbb{Q}_\infty/k) = \mathrm{Gal}(\mathbb{Q}_\infty/k \cap \mathbb{Q}_\infty) \simeq \mathbb{Z}_p$$

が成立し，k_∞ は k の円分 $\mathbb{Z}_p$-拡大となる．ただし，中間体 k_n に関しては $k_n = k\mathbb{Q}^{(n)}$ となるとは限らない．ある n に対して $\mathbb{Q}^{(n)} \subseteq k$ となる場合があり，このときは番号がずれてしまう．

次に岩澤類数公式を紹介する．k_n のイデアル類群の唯一の p-Sylow 部分群を A_n とおく．A_n は $\mathrm{Gal}(k_n/k)$ が作用するので $\mathbb{Z}_p[\mathrm{Gal}(k_n/k)]$-加群となる．岩澤理論では A_n を個別に考えるのではなく，各 n に対しての A_n を一つのまとまりとして考えることにその特徴がある．

定理 2.3 (岩澤類数公式 [12]，1959)．A_n の位数を p^{e_n} とするとき，n に依存しない非負整数 $\mu_p(K/k)$，$\lambda_p(K/k)$ および整数 $\nu_p(K/k)$ が存在して，十分大きな n に対して

$$e_n = \mu_p(K/k)p^n + \lambda_p(K/k)n + \nu_p(K/k)$$

が成り立つ．

整数 $\mu_p(K/k)$，$\lambda_p(K/k)$，$\nu_p(K/k)$ は素数 p と $\mathbb{Z}_p$-拡大 K/k によってのみ定まる定数で，それぞれ岩澤 μ-不変量，岩澤 λ-不変量，岩澤 ν-不変量と呼ぶ．3 つの岩澤不変量の内，μ-不変量と λ-不変量の 2 つは岩澤加群と呼ばれる加群の構造に深く関係している．

2.2 Λ-加群の構造

Λ を形式的冪級数環 $\mathbb{Z}_p[[T]]$ とおく．岩澤類数公式の証明は岩澤加群の構造を調べることによってなされるが，後に示すように岩澤加群は Λ-加群とみなせる．そこでこの節では Λ-加群の構造について説明することにする．

まず初めに Λ の性質について述べる．Λ は Noether 環であるが Euclid 環ではない．したがって一般に Λ の任意の元同士での割り算はできないが，以下に紹介する distinguished 多項式による割り算は可能である．

定義 2.4 (distinguished 多項式)．$P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0 \in \Lambda$ が distinguished 多項式であるというのは，$p|a_i$ $(0 \leq i \leq n-1)$ が成り立つことである．

例 2.5. $p = 2$ のとき，任意の $n \in \mathbb{Z}_{\geq 1}$ に対し $(T+2)^n$ は distinguished 多項式である．また，p が奇素数のとき，$(T+1)^p + p - 1$ は distinguished 多項式となる．

定理 2.6 (割り算定理)．$P(T) \in \Lambda$ を distinguished 多項式とする．このとき任意の $f(T) \in \Lambda$ に対し，$q(T) \in \Lambda$，$\deg(r(T)) < \deg(P(T))$ なる $r(T) \in \mathbb{Z}_p[T]$ が存在して，$f(T) = q(T)P(T) + r(T)$ の形に一意的に表わせる．

証明. [12] の Proposition 7.2 を参照せよ． □

定理 2.7 (Weierstrass の p-進準備定理)．任意の $f(T) \in \Lambda\backslash\{0\}$ は，distinguished 多項式 $P(T) \in \Lambda$，$U(T) \in \Lambda^\times$，$\mu \in \mathbb{Z}_{\geq 0}$ を用いて $f(T) = p^\mu P(T)U(T)$ の形に一意的に表わせる．この分解において $\mu(f) = \mu$，$\lambda(f) = \deg P(T)$ とおき，それぞれ $f(T)$ の μ-不変量，λ-不変量とよぶ．

証明. [12] の Theorem 7.3 を参照せよ． □

定理 2.7 の系として以下のことがわかる．

系 2.8. Λ は一意分解整域であり，その素元は p と既約 distinguished 多項式に限る．

distinguished 多項式は monic であるため p では割り切れない．したがって任意の distinguished 多項式は既約 distinguished 多項式のみによって分解されることが分かる．すなわち定理 2.7 において．$f(T)$ が distinguished ならば，$\mu = 0$.

次に Λ のイデアルについて説明する．ここで紹介する補題は岩澤類数公式の証明に用いられる．

補題 2.9. $(f(T), g(T)) = 1$，すなわち $f(T)$ と $g(T)$ が共通因子を持たないとき，$\sharp\Lambda/(f(T), g(T)) < \infty$.

証明. [12] の Lemma 13.7 を参照せよ． □

Λ の素イデアルについては，以下の通り．

補題 2.10. Λ の素イデアルは 0，(p, T)，(p)，$(P(T))$（ただし $P(T)$ は既約 distinguished 多項式）に限る．また，(p, T) は Λ の唯一の極大イデアルである．

証明. [12] の Proposition 13.9 を参照せよ． □

(p, T) は単項イデアルでないので Λ は単項イデアル整域ではない．よって Euclid 環でないことが分かる．節冒頭で Λ は Euclid 環でないと述べた根拠は補題 2.10 にある．

補題 2.11. $f(T) \in \Lambda$，$f(T) \notin \Lambda^\times$ ならば $\sharp\Lambda/(f(T)) = \infty$.

証明. [12] の Lemma 13.10 を参照せよ． □

Λ の性質を一通り紹介したので，次に Λ-加群の間に成り立つ擬同型の概念を紹介する．

定義 2.12 (擬同型). M, M' を Λ-加群とする．M が M' に擬同型であるとは，Λ-準同型 $M \longrightarrow M'$ が存在し，かつその kernel と cokernel が共に有限であることをいう．この条件は有限 Λ-加群 A, B が存在し，さらに Λ-加群の完全系列

$$0 \longrightarrow A \longrightarrow M \longrightarrow M' \longrightarrow B \longrightarrow 0$$

が成り立つこと，と言い換えることができる．M が M' に擬同型であることを $M \sim M'$ と表わすことにする．

注 2.13. 擬同型は反射律と推移律については成り立っているが，対称律は成り立たない．すなわち，$M \sim M'$ が成立しても $M' \sim M$ とは限らない．

例 2.14. $(p, T) \sim \Lambda$ は成り立つが，$\Lambda \sim (p, T)$ は成立しない．

証明. 自然な写像 $(p, T) \hookrightarrow \Lambda$ を考えれば，$(p, T) \sim \Lambda$ が成立することは明らか．$\Lambda \sim (p, T)$ が成立するかどうかを考える．$\Lambda \sim (p, T)$ と仮定し，Λ-準同型 $\varphi : \Lambda \longrightarrow (p, T)$ が $\varphi(1) = f(T) \in (p, T)$ を満たすとする．このとき $\varphi(\Lambda) = (f(T)) \subseteq (p, T)$．$(p, T)$ は極大イデアルなので $f(T) \notin \Lambda'$ である．よって補題 2.11 より $\sharp\Lambda/(f(T)) = \infty$ なので，$\sharp(p, T)/(f(T)) = \infty$ となる．したがって cokernel が無限となり矛盾する．以上により $\Lambda \sim (p, T)$ は成立しないことが示された． □

次に有限生成 Λ-加群の構造定理を紹介する．

定理 2.15 (Cohen)．M を有限生成 Λ-加群とする．このとき，

$$M \sim \Lambda^r \oplus \left(\bigoplus_{i=0}^{s} \Lambda/(p^{n_i}) \right) \oplus \left(\bigoplus_{j=0}^{t} \Lambda/(P_j(T)^{m_j}) \right)$$

が成り立つ．ここで，$r, s, t, n_i, m_j \in \mathbb{Z}_{\geq 0}$ であり，$P(T)$ は既約 distinguished 多項式である．この直和分解は M により $P_j(T)$ の単元倍を除いて一意的に定まる．

ここでは証明の概略を述べる．詳細については [23] の Theorem 13.12 を参照されたい．M は有限生成なので有限個の生成元 $u_1, \cdots, u_n$ が存在する．$\lambda_i \in \Lambda$ に対し，

$$R = \left\{ (\lambda_1, \cdots, \lambda_n) \in \Lambda^n \middle| \sum_{i=1}^{n} \lambda_i u_i = 0 \right\}$$

とおくと，R は Λ^n の部分加群であり，Λ は Noether 環より有限生成である．したがって，

$$\Lambda^m \xrightarrow{\phi} \Lambda^n \longrightarrow M \longrightarrow 0$$

が完全系列となる準同型写像 ϕ が存在する．この ϕ を標準基底に関して行列表示して，

$$T = \begin{pmatrix} \lambda_{1,1} & \cdots & \lambda_{1,n} \\ \vdots & & \vdots \\ \lambda_{m,1} & \cdots & \lambda_{m,n} \end{pmatrix}$$

とおく．T を M の生成系 $\{u_i\}$ に関する行列という．T を基本変形を用いて対角化することにより定理 2.15. が証明できる．以下にここで用いる基本変形を紹介する．

定義 2.16 (行列の基本変形)．行列 T に対し，以下の変形を基本変形とよぶ：

(A) 行同士，列同士は交換できる．

(B) ある行のスカラー倍を別の行に加える．列についても同様.

(C) ある行を単元倍する．列についても同様.

(1) T が行 $(\lambda_1, p\lambda_2, \cdots, p\lambda_n)$ を含むとき，この $(\lambda_1, p\lambda_2, \cdots, p\lambda_n)$ を $(\lambda_1, \cdots, \lambda_n)$ とし，その行を除く全ての行の第一成分を p 倍する．つまり，

$$T = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \lambda_1 & p\lambda_2 & \cdots & p\lambda_n \\ \vdots & \vdots & & \vdots \\ \beta_1 & \beta_2 & \cdots & \beta_n \end{pmatrix} \longrightarrow T' = \begin{pmatrix} p\alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & & \vdots \\ \lambda_1 & \lambda_2 & \cdots & \lambda_n \\ \vdots & \vdots & & \vdots \\ p\beta_1 & \beta_2 & \cdots & \beta_n \end{pmatrix}$$

と変形する．

(2) T が p^k で割れる行と列を持ち，かつその行と列が交差する成分が p^{k+1} でわりきれないとき，p^k で割り切れる行 $(p^k\lambda_1, \cdots, p^k\lambda_n)$ を $(\lambda_1, \cdots, \lambda_n)$ に変形する．つまり，

$$T = \begin{pmatrix} \alpha_1 & \cdots & p^k\alpha_j & \cdots & \alpha_n \\ \vdots & & \vdots & & \vdots \\ p^k\lambda_1 & \cdots & p^k\lambda_j & \cdots & p^k\lambda_n \\ \vdots & & \vdots & & \vdots \\ \beta_1 & \cdots & p^k\beta_j & \cdots & \beta_n \end{pmatrix} \longrightarrow T' = \begin{pmatrix} \alpha_1 & \cdots & p^k\alpha_j & \cdots & \alpha_n \\ \vdots & & \vdots & & \vdots \\ \lambda_1 & \cdots & \lambda_j & \cdots & \lambda_n \\ \vdots & & \vdots & & \vdots \\ \beta_1 & \cdots & p^k\beta_j & \cdots & \beta_n \end{pmatrix}$$

と変形する．

(3) T が行 $(p^k\lambda_1, \cdots, p^k\lambda_n)$ を含み，$p \nmid \lambda$ なる λ に対し $(\lambda\lambda_1, \cdots, \lambda\lambda_n) \in R$ である，すなわち $\sum_{i=1}^n \lambda\lambda_i u_i = 0$ を満たすとき，$(p^k\lambda_1, \cdots, p^k\lambda_n)$ を $(\lambda_1, \cdots, \lambda_n)$ に変形する．つまり，

$$T = \begin{pmatrix} \vdots & & \vdots \\ p^k\lambda_1 & \cdots & p^k\lambda_n \\ \vdots & & \vdots \end{pmatrix} \longrightarrow T' = \begin{pmatrix} \vdots & & \vdots \\ \lambda_1 & \cdots & \lambda_n \\ \vdots & & \vdots \end{pmatrix}$$

と変形する．

六つの基本操作の内，(A)〜(C) の三つは単項イデアル整域に対しても用いられる．擬同型という概念が加わったことにより，操作 (1)〜(3) が新たに必要となっているのである．

有限生成 Λ-加群 M, M' に対し，Λ-準同型 ϕ, ϕ' を

$$\Lambda^m \xrightarrow{\phi} \Lambda^n \longrightarrow M \longrightarrow 0$$

$$\Lambda^m \xrightarrow{\phi'} \Lambda^n \longrightarrow M' \longrightarrow 0$$

ととるとき，M の生成系 $\{u_i\}$ に関する行列を T，M' の生成系 $\{u_i'\}$ に関する行列を T' とおく．

定義 2.16. で紹介した六つの基本変形によって T を T' に変形できた場合，T は T' に擬同型になることが証明される．

定義 2.17 (Weierstrass degree)**.** $f \in \Lambda$ に対し，

$$\deg_w f = \begin{cases} \infty & \mu(f) > 0 \text{ のとき}, \\ \lambda(f) & \mu(f) = 0 \text{ のとき} \end{cases}$$

を f の Weierstrass degree とよぶ．

また，M の生成系 $\{u_i\}$ に関する行列 $T=(\lambda_{i,j})$ に対し，$\deg^{(k)}(T)=\min_{i,j\geq k}\deg_w\lambda_{i,j}$ とおくことにする．

定義 2.18 (normal form)**.** 行列 T が

$$\begin{pmatrix} \lambda_{1,1} & \cdots & 0 & \\ \vdots & \ddots & \vdots & \mathbf{0} \\ 0 & \cdots & \lambda_{r-1,r-1} & \\ & * & & * \end{pmatrix} = \begin{pmatrix} D_{r-1} & \mathbf{0} \\ A & B \end{pmatrix} \tag{2.3}$$

の形をしているとき，T は $r-1$ の normal form に入るという．ただし $\lambda_{k,k}$ は distinguished 多項式であり，かつ $1\leq k\leq r-1$ に対して $\deg(\lambda_{k,k})=\deg_w\lambda_{k,k}=\deg^{(k)}(T)$ を満たすものとする．

補題 2.19. $(2,1)$ において，$B\neq 0$ と仮定する．このとき T は基本変形を用いることにより，始めの $r-1$ 個の対角成分は不変で，かつ r の normal form に入る行列 T' に変形できる．

証明. [12] の p.275 の Claim を参照せよ． □

以上で定理 2.15 を証明する準備が整った．以下で証明を述べる．

M の生成系 $\{u_i\}$ に関する行列 T に対し，補題 2.19. を繰り返し用いることにより行列

$$\begin{pmatrix} \lambda_{1,1} & & & \mathbf{0} \\ & \ddots & & \\ & & \lambda_{r,r} & \\ A & & & \mathbf{0} \end{pmatrix}$$

を得る．ここで $\lambda_{j,j}$ は distinguished 多項式であり，$j\leq r$ に対して $\deg\lambda_{j,j}=\deg^{(j)}(T)$ を満たす．また，割り算定理より行列の成分 $\lambda_{i,j}$ は多項式で，$i\neq j$ に対して $\deg\lambda_{i,j}<\deg\lambda_{j,j}$ と仮定してよい．

目標は T の対角化なので，$A=\mathbf{0}$ を示したい．背理法を用いる．

ある $i\neq j$ に対し，$\lambda_{i,j}\neq 0$ と仮定する．このとき $\deg_w\lambda_{j,j}$ が最小であるから，$p|\lambda_{i,j}$ が成立する．したがって $(\lambda_{i,1},\cdots,\lambda_{i,r},0,\cdots,0)\in R$ は p で割り切れることが分かる．今 $\lambda=\lambda_{1,1}\cdots\lambda_{r,r}$ とおくと，各 $\lambda_{j,j}$ は distinguished 多項式なので λ は p で割り切れない．そして $\lambda_{j,j}u_j=0$ より $\sum_j\lambda\frac{1}{p}\lambda_{i,j}=0$ なので，

$$\left(\lambda\frac{1}{p}\lambda_{i,1},\cdots,\lambda\frac{1}{p}\lambda_{i,r},0,\cdots,0\right)\in R$$

を得る．よって基本変形 (3) を用いることにより，ある j に対して $p\nmid\lambda_{i,j}$ としてよい．このとき

$$\deg_w\lambda_{i,j}\leq\deg\lambda_{i,j}<\deg\lambda_{j,j}=\deg^{(j)}(T)$$

となるが，これは仮定に矛盾する．よって，$A = \mathbf{0}$ となる．

以上により T の対角化

$$T \longrightarrow \begin{pmatrix} \lambda_{1,1} & & & \mathbf{0} \\ & \ddots & & \\ & & \lambda_{r,r} & \\ \mathbf{0} & & & \end{pmatrix}$$

が得られた．対角化された行列に対応する Λ-加群を考えると

$$\Lambda^{n-r} \oplus \Lambda/(\lambda_{1,1}) \oplus \cdots \oplus \Lambda/(\lambda_{r,r})$$

となる．基本変形 (2) により $\Lambda/(p^k)$ という因子は取り除いていたのでそれを戻し，さらに $\lambda_{i,i}$ を既約 distinguished 多項式の積に分解して以下の補題を適用すると

$$M \sim \Lambda^r \oplus \left(\bigoplus_{i=0}^{s} \Lambda/(p^{n_i}) \right) \oplus \left(\bigoplus_{j=0}^{t} \Lambda/(P_j(T)^{m_j}) \right)$$

が得られる．

補題 2.20. $f, g \in \Lambda$，$(f, g) = 1$ ならば，

(1) $\Lambda/(fg) \sim \Lambda/(f) \oplus \Lambda/(g)$,

(2) $\Lambda/(f) \oplus \Lambda/(g) \sim \Lambda/(fg)$,

が成り立つ．

証明. [12] の Lemma13.8 を参照せよ． □

2.3 岩澤類数公式の証明

この節では岩澤類数公式の証明を説明する．まず初めに必要な記号と類体論の結果を紹介する．

K/k を $\mathbb{Z}_p$-拡大，$\Gamma = \mathrm{Gal}(K/k) \simeq \mathbb{Z}_p$，$\gamma_0$ を Γ の位相的生成元とする．

L_n を最大不分岐 Abel p-拡大とする．拡大 L_n/k_n が p-拡大であるとは，Galois 群 $\mathrm{Gal}(L_n/k_n)$ の位数が p 冪であることをいう．A_n を k_n のイデアル類群の p-Sylow 部分群とすると，類体論により

$$X_n = \mathrm{Gal}(L_n/k_n) \simeq A_n$$

が成り立っている．

$L = \bigcup_{n \geq 0} L_n$，$X = \mathrm{Gal}(L/K)$ とする．各 n に対し，L_n の最大性より L_n/k は Galois 拡大となる．よって L/k もまた Galois 拡大である．$G = \mathrm{Gal}(L/k)$ とおく．

記号の準備ができたので証明の指針を述べる．

始めに X が Γ-加群であることを示し，それにより Λ-加群になることを示す．その後有限生成であることを示し，前節の内容を用いて X がねじれ加群，すわなち $\Lambda/(p^k)$ と $\Lambda/(P(T)^k)$ の形のイデアルの直和に擬同型となることを示す．こうして得られた $\Lambda/(p^k)$ と $\Lambda/(P(T)^k)$ の形の直和において，X_n に対応する n 番目の層で何が起こるかを計算し，各 n の結果を X に持ち上げることで定理が得られる．

最初の目標は X が Γ-加群であることを示すことである．まずは $\mathbb{Z}_p$-拡大における分岐に関する命題を紹介する．

命題 2.21. K/k を $\mathbb{Z}_p$-拡大とする．

(1) K/k において，少なくとも一つの素イデアルは分岐する．また，p の上の素イデアル以外は全て不分岐である．

(2) ある正の整数 e が存在して，K/k_e において分岐する素イデアルは全て完全分岐する．

証明. [12] の Proposition 13.2 と Proposition 13.3 を参照せよ． □

議論を考えやすくするため，以下の仮定をおくことにする．後に仮定を外した場合についても述べる．

仮定 2.22. K/k で分岐する素イデアルは完全分岐する．

この仮定は，命題 2.21(2) において常に $e = 0$ ととれると主張している．仮定 2.22 の下で，K/k が不分岐拡大であるとすると，k の類数が無限になるので矛盾する．したがって仮定 2.22 を認めると K/k は不分岐拡大にならない．よって $k_{n+1} \bigcap L_n = k_n$ となる．したがって，$X_n = \mathrm{Gal}(L_n/k_n) \simeq \mathrm{Gal}(L_n k_{n+1}/k_{n+1})$ が得られた．$\mathrm{Gal}(L_n k_{n+1}/k_{n+1})$ は X_{n+1} の商であるから，写像 $X_{n+1} \longrightarrow X_n$ が存在し，これはイデアル類群における $A_{n+1} \longrightarrow A_n$ のノルム写像に対応している．各 n に対して $k_n \subseteq L_n$ が成り立っているので，$K \subseteq L$ である．このことより

$$L = \bigcup_{n \geq 0} L_n \subseteq \bigcup_{n \geq 0} L_n K \subseteq L$$

が従うので，$L = \bigcup_{n \geq 0} L_n K$ が成り立つ．よって $X_n = \mathrm{Gal}(L_n/k_n) \simeq \mathrm{Gal}(L_n k_{n+1}/k_{n+1})$ より，

$$\varprojlim X_n = \mathrm{Gal}\Big(\Big(\bigcup_{\geq 0} L_n K\Big)/K\Big) = \mathrm{Gal}(L/K) = X \tag{2.4}$$

となる．

$\gamma \in \Gamma_n = \Gamma/\Gamma^{p^n} = \mathrm{Gal}(k_n/k)$ とする．この γ を $\mathrm{Gal}(L_n/k)$ の元 $\tilde{\gamma}$ に拡張する．$x \in X_n$ に対して，γ の x への作用は $\gamma x = \tilde{\gamma} x \tilde{\gamma}^{-1}$ となっている．

この作用が well-defined であることを確かめる．$\tilde{\gamma}_1, \tilde{\gamma}_2$ を γ の二つの拡張とする．このときある $\tau \in \mathrm{Gal}(L_n/k_n)$ が存在して $\tilde{\gamma}_1 = \tilde{\gamma}_2\tau$ となり，また，$\mathrm{Gal}(L_n/k_n)$ は Abel 群なので $\tau x \tau^{-1} = x$ となる．よって

$$\gamma_1 x = \tilde{\gamma}_1 x \tilde{\gamma}_1^{-1} = \tilde{\gamma}_2 \tau x (\tilde{\gamma}_2 \tau)^{-1} = \tilde{\gamma}_2 \tau x \tau^{-1} \tilde{\gamma}_2^{-1} = \tilde{\gamma}_2 x \tilde{\gamma}_2^{-1} = \gamma_2 x$$

が成立する．したがって γx は well-defined である．

以上により X_n は $\mathbb{Z}_p[\Gamma_n]$-加群であることが分かった．X は $X \simeq \varprojlim X_n$ であるから，X の元をベクトルの形 $(x_0, x_1, \cdots)$ のように表わし，その n 番目の成分に $\mathbb{Z}_p[\Gamma_n]$ を作用させることにより $\varprojlim \mathbb{Z}_p[\Gamma_n]$ 上の加群とみなせる．$\varprojlim \mathbb{Z}_p[\Gamma_n] = \mathbb{Z}_p[[\Gamma]]$ と表わすことにする．

X が Γ-加群であることを示したので，次にこれが Λ-加群になることを説明する．X が Λ-加群になることは以下の定理より従う．

定理 2.23 (Serre)**.** $\mathbb{Z}_p[[\Gamma]] = \varprojlim \mathbb{Z}_p[\Gamma_n]$，$\Lambda = \mathbb{Z}_p[[T]]$ とする．γ_0 を一つの固定した $\mathbb{Z}_p[[\Gamma]]$ の位相的生成元とすると，位相環としての同型

$$\mathbb{Z}_p[[\Gamma]] \xrightarrow{\sim} \Lambda; \quad \gamma_0 \longmapsto 1 + T$$

が成立している．

証明. [12] の Theorem 7.1 を参照せよ． □

$\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ を K/k で分岐する素イデアル，$\tilde{\mathfrak{p}}_i$ を $\mathfrak{p}_i$ の上の L の素イデアルとする．また，$I_i \subseteq G$ を $\tilde{\mathfrak{p}}_i$ の惰性群とする．L/K は不分岐拡大なので，$I_i \bigcap X = 1$ となっている．また，仮定 2.22 より K/k で $\mathfrak{p}_i$ は完全分岐しているので，写像

$$I_i \hookrightarrow G/X = \Gamma$$

は全射になる．よってこの写像は全単射であることが分かる．したがって，$1 \leq i \leq s$ なる任意の i に対し，$G = XI_i = I_iX$ が成立する．上の写像で γ_0 に写る I_i の元を σ_i とする．考えている写像は全単射で，また γ_0 は Γ の位相的生成元なので，σ_i は I_i の位相的生成元でなければならない．よって $I_i \subseteq XI_i$ より，ある $a_i \in X$ が存在して $\sigma_i = a_i\sigma_1$ が成り立つ．$a_1 = 1$ であることに注意する．

補題 2.24. Y_0 を $\{a_i | 2 \leq i \leq s\}$ と $(\gamma_0 - 1)X = TX$ で生成される X の $\mathbb{Z}_p$-部分加群とする．

$$\nu_n = 1 + \gamma_0 + \gamma_0^2 + \cdots + \gamma_0^{p^n - 1} = \frac{(1+T)^{p^n} - 1}{T}$$

とおき，さらに $Y_n = \nu_n Y_0$ とする．このとき任意の $n \geq 0$ に対し，

$$X_n \simeq X/Y_n$$

が成立する．

証明. [12] の Lemma 13.15 を参照せよ. □

次に，X が有限生成（Λ-加群）であることを示す.

補題 2.25 (中山の補題). X をコンパクト Λ-加群とする．このとき，X が有限生成 Λ-加群であることと $\sharp X/(p,T) < \infty$ であることは同値である.

証明. [12] の Lemma 13.16 を参照せよ. □

この補題を用いて次の命題が得られる.

命題 2.26. X は有限生成 Λ-加群である.

証明. $\nu_1 = \frac{(1+T)^p-1}{T} \in (p,T)$ より $Y_0/(p,T)Y_0$ は $Y/\nu_1 Y$ の剰余群として表わせる．$Y_0/\nu_1 Y_0 = Y_0/Y_1 \subseteq X/Y_1 = X_1$ が成り立ち，X_1 は有限生成であるから中山の補題より Y_0 も有限生成となる．さらに，$X/Y_0 = X_0$ も有限生成であるので，X は有限生成でなければならない. □

以上により X が有限生成 Λ-加群であることが分かったが，ここまでの議論は全て仮定 2.22 の下に行われていた．仮定 2.22 を外しても同様の結果が得られることを説明する.

一般の $\mathbb{Z}_p$-拡大の場合，命題 2.21(2) よりある $e \geq 0$ が存在して，K/k_e の分岐する素イデアルは全て完全分岐している．したがって K/k_e に対してはこれまでの議論がそのまま成り立つ.

$n \geq e$ に対し,

$$\nu_{n,e} = \frac{\nu_n}{\nu_e} = 1 + \gamma_0^{p^e} + \cdots + \gamma_0{}^{(p^{n-e}-1)p^e}$$

とおく．$\gamma_0^{p^e}$ は $\mathrm{Gal}(K/k_e)$ を生成するので，これまで ν_n で考えていた部分は全て $\nu_{n,e}$ として考えなければならない．また，X の部分加群で，これまで Y_0 として扱っていたものに相当するものがあり，それを Y_e とする．このとき，$n \geq e$ に対して,

$$Y_n = \nu_{n,e} Y_e, \quad X_n \simeq X/Y_n$$

が成り立つ．このときも X/Y_e，Y_e が共に有限生成であることから X が有限生成であることが分かる．これで仮定 2.22 を外しても同じ結果が得られたことになる.

一般の $\mathbb{Z}_p$-拡大についても有限生成 Λ-加群であることが示せたので，X の Λ-加群としての構造を見ることにする．X/Y_e は有限なので $Y_e \sim X$ が成立していることに注意する．X に定理 2.15 を適用すると,

$$Y_e \sim X \sim \Lambda^r \oplus \left(\bigoplus_{i=0}^{s} \Lambda/(p^{n_i}) \right) \oplus \left(\bigoplus_{j=0}^{t} \Lambda/(P_j(T)^{m_j}) \right) \tag{2.5}$$

が成り立つ．V を (2.3) の右辺の直和因子の一つとして $\sharp V/\nu_{n,e} V$ を計算する.

(1) $V = \Lambda$ の場合.

$$\nu_{n,e} = \frac{(1+T)^{p^n} - 1}{(1+T)^{p^e} - 1}$$

を計算すると，$\nu_{n,e}$ は distinguished 多項式になるので Λ の単元にはならない．よって補題 2.11 より $\sharp\Lambda/(\nu_{n,e}) = \infty$ となる．しかし $Y_e/\nu_{n,e}Y_e$ は全て有限なので，$r = 0$ でなければならない．よって (2.3) の右辺に Λ は現れない．以上で X はねじれ加群となることが示された.

(2) $V = \Lambda/(p^k)$ の場合.

$$V/\nu_{n,e}V = (\Lambda/(p^k))/(\nu_{n,e}(\Lambda/(p^k))) \simeq \Lambda/(\nu_{n,e}, p^k)$$

が成立している．$\nu_{n,e}$ は distinguished 多項式なので，割り算定理より $\Lambda/(\nu_{n,e}, p^k)$ の任意の元は，$\deg \nu_{n,e} = p^n - p^e$ より次数の低い多項式を p^k を法として計算したものとして一意的に表わされる．よって $c = -kp^e$ とおくと，

$$\sharp V/\nu_{n,e}V = p^{k(p^n - p^e)} = p^{kp^n + c}$$

と書ける.

(3) $V = \Lambda/(f(T)^m)$ の場合．$g(T) = f(T)^m$，$d = \deg g(T)$ とおく．$f(T)$ は distinguished 多項式なので，$g(T)$ もまた distinguished 多項式となる．よって $T^d \equiv p \cdot (\text{多項式}) \pmod{g(T)}$ と書くことができる．したがって $k \geq d$ ならば，

$$T^k \equiv p \cdot (\text{多項式}) \pmod{g(T)}$$

と書ける．よって $p^n \geq d$ なる n に対し，

$$\begin{aligned}(1+T)^{p^n} &= 1 + p \cdot (\text{多項式}) + T^{p^n} \\ &\equiv 1 + p \cdot (\text{多項式}) \pmod{g(T)}\end{aligned}$$

となる．上式より

$$\begin{aligned}(1+T)^{p^{n+1}} &\equiv (1 + p \cdot (\text{多項式}))^p \pmod{g(T)} \\ &\equiv 1 + p^2 \cdot (\text{多項式}) \pmod{g(T)}\end{aligned}$$

が成立する．ここで $P_n(T) = (1+T)^{p^n} - 1$ とおくと，

$$\begin{aligned}P_{n+2}(T) &= (1+T)^{p^{n+2}} - 1 \\ &= ((1+T)^{(p-1)p^{n+1}} + \cdots + (1+T)^{p^{n+1}} + 1) \cdot ((1+T)^{p^{n+1}} - 1) \\ &\equiv (1 + \cdots + 1 + p^2 \cdot (\text{多項式})) \cdot P_{n+1}(T) \pmod{g(T)} \\ &\equiv (p + p^2 \cdot (\text{多項式})) \cdot P_{n+1}(T) \pmod{g(T)} \\ &\equiv p(1 + p \cdot (\text{多項式})) \cdot P_{n+1}(T) \pmod{g(T)}\end{aligned}$$

となる．$1+p\cdot(\text{多項式})\in\Lambda^\times$ なので，$\frac{P_{n+2}(T)}{P_{n+1}(T)}$ は $V=\Lambda/(g(T))$ において $p\cdot(\text{単数})$ と表わされる．そこで $n_0\geq e$ を $p^{n_0}\geq d$ となるようにとり，$n\geq n_0$ と仮定する．このとき

$$\frac{\nu_{n+2,e}}{\nu_{n+1,e}}=\frac{\nu_{n+2}}{\nu_{n+1}}=\frac{P_{n+2}(T)}{P_{n+1}(T)}$$

が成り立つから，

$$\nu_{n+2,e}V=\frac{P_{n+2}(T)}{P_{n+1}(T)}\nu_{n+1,e}V=p\cdot(\nu_{n+1,e}V)$$

と表わされる．したがって $n\geq n_0$ に対し，

$$\sharp V/\nu_{n+2,e}V=\sharp V/pV\cdot\sharp pV/p\nu_{n+1,e}V \tag{2.6}$$

となる．$g(T)$ は distinguished 多項式なので $(g(T),p)=1$ であり，このことから V における p 倍写像は単射である．よって

$$\sharp pV/p\nu_{n+1,e}V=\sharp V/\nu_{n+1,e}V$$

が導かれる．割り算定理より $V/pV\simeq\Lambda/(p,g(T))=\Lambda/(p,t^d)$ が得られているので，$n\geq n_0$ に対し $\sharp V/pV=p^d$ となる．よって (2.6) は

$$\sharp V/\nu_{n+2,e}V=p^d\cdot\sharp pV/p\nu_{n+1,e}V \tag{2.7}$$

と表わされる．(2.7) を繰り返し用いることによって $n\leq n_0+1$ に対し，

$$\sharp V/\nu_{n,e}V=p^{d(n-n_0-1)}\sharp V/\nu_{n_0+1,e}V \tag{2.8}$$

が得られる．(2.8) の右辺が有限のとき，$c=-d(n_0+1)$ とおくと $n\leq n_0+1$ に対し，

$$\sharp V/\nu_{n,e}V=p^{dn+c}$$

が得られる．(2.8) の右辺は無限になることもあるが，これは補題2.9より，$(\nu_{n,e},g(T))\neq 1$ の場合にのみ起こることが分かる．

以上をまとめると次の命題を得る．

命題 2.27. r,s,t,k_i,m_j を整数，$f_j(T)$ を distinguished 多項式，$g_j(T)=f_j(T)^{m_j}$

$$E=\Lambda^r\oplus\left(\bigoplus_{i=1}^{s}\Lambda/(p^{k_i})\right)\oplus\left(\bigoplus_{j=1}^{t}\Lambda/(g_j(T))\right)$$

とする．さらに $\mu=\sum_{i=1}^s k_i$，$\lambda=\sum_{j=1}^t\deg g_j=\sum_{j=1}^t m_j\deg f_j$ とおき，任意の n に対し $\sharp E/\nu_{n,e}E<\infty$ と仮定する．このとき $r=0$ であり，ある $n_0\geq 0$ と整数 c が存在して，

$$\sharp E/\nu_{n,e}E=p^{\mu p^n+\lambda n+c},\qquad n\geq n_0 \tag{2.9}$$

が成り立つ．

$\sharp E/\nu_{n,e}E$ が得られたので，次に $\sharp Y_e/\nu_{n,e}Y_e$ を求める．擬同型 $Y_e \sim E$ が成立しているので，$\sharp Y_e/\nu_{n,e}Y_e$ は $\sharp E/\nu_{n,e}E$ を用いて表わされるのである．次の命題により $\sharp E/\nu_{n,e}E$ が求められる．

命題 2.28. Y, E を $Y \sim E$ 満たす Λ-加群で，$n \geq e$ なる n に対し $Y/\nu_{n,e}Y$ が有限であると仮定する．このとき，ある整数 b, n_0 が存在して，$n \geq n_0$ に対して

$$\sharp Y/\nu_{n,e}Y = p^b \cdot \sharp E/\nu_{n,e}E$$

が成り立つ．

証明. $Y \sim E$ なので，ある有限 Λ-加群 A, B が存在して，完全系列

$$0 \longrightarrow A \longrightarrow Y \xrightarrow{\phi} B \longrightarrow B \longrightarrow 0$$

が成り立つ．この完全系列より可換図式

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \nu_{n,e}Y & \longrightarrow & Y & \longrightarrow & Y/\nu_{n,e}Y & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi'_n} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi''_n} & & \\ 0 & \longrightarrow & \nu_{n,e}E & \longrightarrow & E & \longrightarrow & E/\nu_{n,e}E & \longrightarrow & 0 \end{array} \tag{2.10}$$

を得る．このとき，次の性質が成り立つ：

(1) $\sharp \ker \phi'_n \leq \sharp \ker \phi$,

(2) $\sharp \mathrm{coker}\phi'_n \leq \sharp \mathrm{coker}\phi$,

(3) $\sharp \mathrm{coker}\phi''_n \leq \sharp \mathrm{coker}\phi$,

(4) $\sharp \ker \phi''_n \leq \sharp \ker \phi \cdot \sharp \mathrm{coker}\phi$.

証明. (1) $\ker \phi'_n \subseteq \sharp \ker \phi$ より明らか．
(2) $\mathrm{coker}\phi'_n$ の元を $\nu_{n,e}$ 倍すれば $\sharp\mathrm{coker}\phi$ の元になるので明らか．
(3) $Y \longrightarrow Y/\nu_{n,e}Y$，$Y \longrightarrow E/\nu_{n,e}E$ が共に全射であることより $\mathrm{coker}\phi$ の代表元が $\mathrm{coker}\phi''_n$ の代表元を与えるので成り立つ．
(4) snake lemma より

$$0 \longrightarrow \ker \phi'_n \longrightarrow \ker \phi \longrightarrow \ker \phi''_n \xrightarrow{\delta} \mathrm{coker}\phi'_n \longrightarrow \mathrm{coker}\phi \longrightarrow \mathrm{coker}\phi''_n \longrightarrow 0$$

は完全系列である．このとき，$\sharp \ker \phi''_n \leq \ker \phi \cdot \sharp \mathrm{coker}\phi''_n$ が成り立つ．よって (3) が適用でき，$\sharp \ker \phi''_n \leq \sharp \ker \phi \cdot \sharp \mathrm{coker}\phi$ が得られる． □

次に，$m \geq n \geq 0$ とすると次が成り立つ：

(a) $\sharp \ker \phi'_n \geq \sharp \ker \phi'_m$,

(b) $\sharp\mathrm{coker}\phi'_n \geq \sharp\mathrm{coker}\phi'_m$,

(c) $\sharp\mathrm{coker}\phi''_n \leq \sharp\mathrm{coker}\phi''_m$.

証明. (a) $\nu_{m,e} = \frac{\nu_{m,e}}{\nu_{n,e}}\nu_{n,e}$ より $\nu_{m,e}Y \subseteq \nu_{n,e}Y$ が成立するので，$\ker\phi'_m \subseteq \ker\phi'_n$.
(b) $\nu_{m,e}y \in \nu_{m,e}E$ とする．このとき，$\mathrm{coker}\phi'_n$ での $\nu_{n,e}$ の代表元を $z \in \nu_{n,e}E$ とするとある $x \in Y$ が存在して，$\nu_{n,e}y - z = \phi(\nu_{n,e}x)$ が成り立つ．この両辺を $\frac{\nu_{m,e}}{\nu_{n,e}}$ 倍すれば,

$$\begin{aligned}\nu_{m,e}y - \frac{\nu_{m,e}}{\nu_{n,e}}z &= \frac{\nu_{m,e}}{\nu_{n,e}}\nu_{n,e}y - \frac{\nu_{m,e}}{\nu_{n,e}} \\ &= \frac{\nu_{m,e}}{\nu_{n,e}}\phi(\nu_{n,e}x) \\ &= \nu_{m,e}\phi(x) = \phi(\nu_{m,e}x) \\ &= \phi'_m(\nu_{m,e}x)\end{aligned}$$

を得る．つまり，$\mathrm{coker}\phi'_n$ の代表元を $\frac{\nu_{m,e}}{\nu_{n,e}}$ 倍すると $\mathrm{coker}\phi'_m$ の代表元となる．したがって (b) が成り立つ．
(c) は $\nu_{m,e}E \subseteq \nu_{n,e}E$ より明らかである． □

(1)-(4),(a)-(c) を用いることにより，$\sharp\ker\phi'_n$,$\sharp\mathrm{coker}\phi'_n$, $\sharp\mathrm{coker}\phi''_n$ は十分大きな n に対して一定になることが分かる．さらに，snake lemma を用いて,

$$\sharp\ker\phi'_n \cdot \sharp\ker\phi''_n \cdot \sharp\mathrm{coker}\phi = \sharp\mathrm{coker}\phi'_n \cdot \sharp\mathrm{coker}\phi''_n \cdot \sharp\ker\phi$$

が得られるので，$\sharp\ker\phi''_n$ もまた十分大きな n に対して一定になることが分かる．よって完全系列

$$0 \longrightarrow \ker\phi''_n \longrightarrow Y/\nu_{n,e}Y \longrightarrow E/\nu_{n,e}E \longrightarrow \mathrm{coker}\phi''_n \longrightarrow 0$$

を考えると，十分大きな n に対して,

$$\begin{aligned}\sharp Y/\nu_{n,e}Y &= \sharp\ker\phi''_n \cdot (\mathrm{coker}\phi''_n)^{-1} \cdot \sharp E/\nu_{n,e}E \\ &= p^b \cdot \sharp E/\nu_{n,e}E\end{aligned}$$

が得られる． □

今考えている Y_e は命題 2.28 の仮定を満たしているので，ある $n_1 \geq 0$ が存在して，$n \geq n_1$ なる n に対して $\sharp Y_e/\nu_{n,e}Y_e = p^b \cdot \sharp E/\nu_{n,e}E$ と表わせることが分かった．以下 n_1 と命題 2.27 における n_0 に対し，n を $n \geq \max\{n_0, n_1\}$ を満たすようにとる．これまでの結果をまとめると,

$$\begin{aligned}\sharp A_n = \sharp X_n &= \sharp X/\nu_{n,e}Y_e \\ &= \sharp X/Y_e \cdot \sharp Y_e/\nu_{n,e}Y_e \\ &= p^a \cdot (p^b \cdot \sharp E/\nu_{n,e}E) \\ &= p^a \cdot p^b \cdot p^{\mu p^n + \lambda n + c} \\ &= p^{\mu p^n + \lambda n + (a+b+c)}\end{aligned}$$

となるので，$\nu = a + b + c$ とおくと，十分大きな n に対し，

$$\sharp A_n = p^{\mu p^n + \lambda n + \nu}$$

が得られる．以上で岩澤類数公式が証明された．証明の中で定義された μ, λ, ν をそれぞれ岩澤 μ-不変量，岩澤 λ-不変量，岩澤 ν-不変量という．μ, λ は命題 2.27 における $\mu = \sum_{i=1}^{s} k_i$，$\lambda = \sum_{j=1}^{t} \deg g_j = \sum_{j=1}^{t} m_j \deg f_j$ のことであり，Λ-加群 X の構造不変量としての意味を持っている．

3　$\mathbb{Q}(\sqrt{p})$ の円分 $\mathbb{Z}_2$-拡大における岩澤 λ-不変量

この章では福田-小松 [2] について解説する．

2 章でも述べたように，岩澤不変量 $\mu_p(K/k)$，$\lambda_p(K/k)$，$\nu_p(K/k)$ は素数 p と $\mathbb{Z}_p$-拡大 K/k にのみ依存して定まる．一般に代数体 k の $\mathbb{Z}_p$-拡大は複数個存在しうるため，各不変量に対し $\mathbb{Z}_p$-拡大 K/k を明示する必要がある．しかし円分 $\mathbb{Z}_p$-拡大は k に対し唯一つ定まり，本章では円分 $\mathbb{Z}_p$-拡大のみを取り扱うので，以降各不変量を $\mu_p(k)$，$\lambda_p(k)$，$\nu_p(k)$ と表わすことにする．

3.1　主定理 1 の紹介と証明の指針

初めに本修士論文の目的である主定理 1 を紹介する．これはある種の実 2 次体の岩澤 λ-不変量について上界を与える定理であり，また，λ-不変量が 0 になる場合についても述べられている．

定理 3.1 (主定理1, 福田-小松[2]). p を $p \equiv 1 \pmod{16}$ を満たす素数，$s = \mathrm{ord}_2(p-1)$，ε_0 を $\mathbb{Q}(\sqrt{p})$ の基本単数，$\varepsilon_0' = a + b\sqrt{2p}$ を $\mathbb{Q}(\sqrt{2p})$ の基本単数，ここで $a \in \mathbb{Z}_{\geq 0}$，$b \in \mathbb{Z}$ とする．このとき，$\mathbb{Q}(\sqrt{p})$ の岩澤 λ-不変量に関する以下の判定法が成立する：

(1) $a \equiv 1 \pmod{p}$ であれば，$\lambda_2(\mathbb{Q}(\sqrt{p})) \leq 2^{s-2} - 3$.

(2) $a^2 \equiv -1 \pmod{p}$ かつ $\varepsilon_0^2 \not\equiv -1 \pmod{32}$ とする．ここで $\varepsilon_0^2 \not\equiv -1 \pmod{32}$ とは，$O_{\mathbb{Q}(\sqrt{p})}/32O_{\mathbb{Q}(\sqrt{p})}$ の元として $\varepsilon_0^2 + 32O_{\mathbb{Q}(\sqrt{p})} \neq -1 + 32O_{\mathbb{Q}(\sqrt{p})}$ であることをいう．このとき $\lambda_2(\mathbb{Q}(\sqrt{p})) = 0$.

この節では主定理 1(1) について証明の指針を述べる．まずは準備として以下の記号を用意する．

$n \in \mathbb{Z}_{\geq 0}$，$\alpha_n = 2\cos(2\pi/2^{n+2})$，$\mathbb{Q}^{(n)} = \mathbb{Q}(\alpha_n)$ とおく．$\mathbb{Q}^{(n)}$ は円分体 $\mathbb{Q}(\zeta_{2^{n+2}})$ の最大総実部分体であり，その拡大次数は $[\mathbb{Q}^{(n)} : \mathbb{Q}] = 2^n$ となる．$\alpha_{n+1} = \sqrt{2 + \alpha_n}$ より $\mathbb{Q}^{(n)} \subset \mathbb{Q}^{(n+1)}$ となる．よって $\mathbb{Q}_\infty = \bigcup_{n=0}^{\infty} \mathbb{Q}^{(n)}$ とおくと，$\mathbb{Q}_\infty$ は $\mathbb{Q}$ の唯一の $\mathbb{Z}_2$-拡大となる．これは $\mathbb{Q}$ の円分 $\mathbb{Z}_2$-拡大と呼ばれる．

注 3.2. 例 2.2 では $\mathbb{Q}$ に $2\cos(2\pi/2^{n+2})$ ではなく $\cos(2\pi/2^{n+2})$ を付加して円分 $\mathbb{Z}_2$-拡大を作っていた．ここで $\cos(2\pi/2^{n+2})$ に 2 をかけている理由は漸化式 $\alpha_{n+1} = \sqrt{2 + \alpha_n}$ を得るためである．この漸化式は補題 3.27 を証明する際に用いられるが，もし $\cos(2\pi/2^{n+2})$ を $\mathbb{Q}$ に付加して考えると漸化式は $\alpha_{n+1} = \sqrt{\frac{1}{2}(1 + \alpha_n)}$ となり都合が悪い．

補題 3.3. α_n は $\mathbb{Q}^{(n)}$ の素元である．

証明. まず始めに円分体に関する以下の定理を用いる．

定理 3.4 (Neukirch[10]). p を素数，$m = p^n$，ζ_m を 1 の原始 m 乗根とする．このとき，$(1 - \zeta_m)$ は $O_{\mathbb{Q}(\zeta_m)}$ の素イデアルであり，$pO_{\mathbb{Q}(\zeta_m)} = (1 - \zeta_m)^{[\mathbb{Q}(\zeta_m):\mathbb{Q}]}$ が成り立つ．つまり p は $\mathbb{Q}(\zeta_m)$ で完全分岐する．

定理 3.4 を $\mathbb{Q}(\zeta_{2^{n+2}})$ に適用すると，素イデアル分解 $2O_{\mathbb{Q}(\zeta_{2^{n+2}})} = (1-\zeta_{2^{n+2}})^{2^{n+1}}$ が得られる．$\mathbb{Q}^{(n)}$ は $\mathbb{Q}(\zeta_{2^{n+2}})$ の部分体なので，2 は $\mathbb{Q}^{(n)}$ でも完全分岐する．よって 2 の上の $\mathbb{Q}^{(n)}$ の素イデアルは 1 つしかなく，それを P とおくことにする．2 は $\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}^{(n)}$ でも完全分岐しているので，相対次数 $f = [\mathbb{Q}(\zeta_{2^{n+2}}) : \mathbb{Q}^{(n)}] = 1$ である．よって，$(1-\zeta_{2^{n+2}})$ の相対ノルム $N_{\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}^{(n)}}$ をとると，$N_{\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}^{(n)}}((1-\zeta_{2^{n+2}})) = P$ が成立している．実際に $N_{\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}^{(n)}}((1-\zeta_{2^{n+2}}))$ を計算する．a の複素共役を $\bar{a}$ とあらわすことにすると，

$$\begin{aligned} N_{\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}^{(n)}}((1-\zeta_{2^{n+2}})) &= (1-\zeta_{2^{n+2}})\overline{(1-\zeta_{2^{n+2}})} \\ &= (1-\zeta_{2^{n+2}})(1-\zeta_{2^{n+2}}^{-1}) \\ &= 1-(\zeta_{2^{n+2}}-\zeta_{2^{n+2}}^{-1})+1 \\ &= 2-\alpha_n \end{aligned}$$

となり，$P = (2-\alpha_n)$ が得られる．$P = (2-\alpha_n)$ は 2 の上の $\mathbb{Q}^{(n)}$ の素イデアルなので，$2 \in (2-\alpha_n)$ であり，よって $(\alpha_n) = (2-\alpha_n)$ となる．したがって (α_n) もまた $\mathbb{Q}^{(n)}$ の素イデアルになるので，α_n は $\mathbb{Q}^{(n)}$ の素元であることが分かった．

□

p を奇素数，$k = \mathbb{Q}(\sqrt{p})$，$k_n = k(\alpha_n)$，$k_\infty = k\mathbb{Q}_\infty$ とおくと，k_∞ は k の円分 $\mathbb{Z}_2$-拡大となる．

注 3.5. 一般にはこのような中間体 k_n のとり方は成り立たない．それは n が条件とずれてしまうからであるが，今回は以下の補題によりずれないことが分かる．

補題 3.6. $k \cap \mathbb{Q}_\infty = \mathbb{Q}$.

証明. $[k:\mathbb{Q}] = 2$ なので $k/\mathbb{Q}$ の中間体は k か $\mathbb{Q}$ のどちらかとなる．よって $k \cap \mathbb{Q}_\infty = k$ または $\mathbb{Q}$ である．一方，$\mathbb{Q}_\infty/\mathbb{Q}$ の中間体で $\mathbb{Q}$ 上の拡大次数が 2 以下のものは $\mathbb{Q}^{(1)} = \mathbb{Q}(\sqrt{2})$ か $\mathbb{Q}$ のどちらかしかない．p は奇素数なので $k \neq \mathbb{Q}(\sqrt{2})$ である．よって $k \cap \mathbb{Q}_\infty = \mathbb{Q}$ が成り立つ． □

M_n を 2 の外で不分岐な k_n の最大 Abel 2-拡大，L_n を k_n の最大不分岐 Abel 2-拡大とする．このとき $M_\infty = \bigcup_{n=1}^{\infty} M_n$，$L_\infty = \bigcup_{n=1}^{\infty} L_n$ とおくと，M_∞ は 2 の外で不分岐な k_∞ の最大 Abel 2-拡大，L_∞ は k_∞ の最大不分岐 Abel 2-拡大となる．さらに $I_n = G(M_n/L_n)$，$I_\infty = G(M_\infty/L_\infty)$，$\mathfrak{X}_\infty = G(M_\infty/k_\infty)$，$X_\infty = G(L_\infty/k_\infty)$ とおく．

通常，$G(k_\infty/k)$ の 1 つの固定した位相的生成元 γ と $\Lambda = \mathbb{Z}_2[[T]]$ の位相的生成元 $1+T$ を対応させることにより，$\mathfrak{X}_\infty$ を Λ-加群とみなす．L_∞/k_∞ は Galois 拡大なので，$G(M_\infty/L_\infty)$ は $G(M_\infty/k_\infty)$ の正規部分群である．よって以下の同型が成り立つ．

$$G(M_\infty/k_\infty)/G(M_\infty/L_\infty) \cong G(L_\infty/k_\infty)$$

この同型より以下の完全系列が得られる．

$$1 \longrightarrow I_\infty \longrightarrow \mathfrak{X}_\infty \longrightarrow X_\infty \longrightarrow 1 \tag{3.11}$$

命題 3.7. $\mathfrak{X}_\infty$ は有限生成自由 $\mathbb{Z}_2$-加群である．

証明. $k=\mathbb{Q}(\sqrt{p})$ だから $k(\sqrt{-1})$ は $\mathbb{Q}$ 上 biquadratic である．よって $k(\sqrt{-1})$ は $\mathbb{Q}$ 上 Abel だから以下の Ferrero-Washington の定理が適用できる．

定理 3.8 (Ferrero-Washington の定理)**.** $\mathbb{Q}$ 上 Abel な任意の代数体 k と任意の素数 p に対し，$\mu_p(k)=0$.

よって $\mu_2(k(\sqrt{-1}))=0$ が得られる．一般に $\mathbb{Z}_p$-拡大 K/k において，$\mu_p(k)=0$ であるとは，命題 2.27 における $(\bigoplus_{i=1}^{s}\Lambda/(p^{k_i}))$ の部分が無いということであり，この部分は $\mathbb{Z}_p$-加群としては巡回 p-群の無限直和と同型である．つまり μ-不変量は K/k から定まる Λ-加群 X の無限部分に対応しているので，$\mu_2(k(\sqrt{-1}))=0$ より $\mathfrak{X}_\infty$ は有限生成であることが分かる．

また，$\mathfrak{X}_\infty$ は有限な部分 Λ-加群を持たない．これは以下の定理より得られる．

定理 3.9 (Greenberg[5])**.** K/k を $\mathbb{Z}_p$-拡大，r_2 を虚な共役体の組の数，$G=\mathrm{Gal}(K/k)$，Λ_G を G の $\mathbb{Z}_p$ 上の完備群環とする．さらに M_K を p を割り切る素点の集合の外で不分岐な K の最大 Abel pro-p-拡大体，$X_K=\mathrm{Gal}(M_K/K)$ とする．k が $\mathbb{Q}$ 上 Abel 拡大ならば，X_K は Λ_G-加群として rank r_2 を持ち，かつ自明でない有限部分 Λ_G-加群を持たない．

今 $k=\mathbb{Q}(\sqrt{p})$ なので $\mathbb{Q}$ 上 Abel である．よって定理 3.9 が適用できる． □

$\lambda(I_\infty)$ を I_∞ の $\mathbb{Z}_2$-rank，$\lambda(\mathfrak{X}_\infty)$ を $\mathfrak{X}_\infty$ の $\mathbb{Z}_2$-rank，$\lambda(X_\infty)$ を X_∞ の $\mathbb{Z}_2$-rank とする．短完全系列の rank に関する交代和は 0 なので，(3.11) より

$$\lambda(\mathfrak{X}_\infty)=\lambda(X_\infty)+\lambda(I_\infty) \tag{3.12}$$

が得られる．

定義より $\lambda_2(k)=\lambda(X_\infty)$ である．$s\leq 3$ の場合に対しては，以下の定理が知られている．

定理 3.10 (尾崎-田谷 [11], 1997)**.** p が以下の条件のいずれか 1 つを満たすものとする．

(1) $p\equiv 3 \pmod 4$

(2) $p\equiv 5 \pmod 8$

(3) $p\equiv 9 \pmod{16}$

(4) $p\equiv 1 \pmod{16}$ かつ $2^{\frac{p-1}{4}}\equiv -1 \pmod p$

このとき，$\lambda_2(\mathbb{Q}(\sqrt{p}))=0$.

p は奇素数なので $s \geq 1$ である．よって $1 \leq s \leq 3$ の範囲で考えることにする．$s = 1$ とすると $2 \mid p-1$ かつ $4 \nmid p-1$．よって $p = 1 + 2l$ $(l \in \mathbb{Z})$ とあらわせ，$4 \nmid p-1$ より l は奇数である．$l = 2l' + 1$ $(l' \in \mathbb{Z})$ とおくと $p = 1 + 2(2l'+1)$ より $p = 4l' + 3$. よって $p \equiv 3 \pmod 4$ となり定理 3.10(1) が適用できる．同様にして $s = 2$ の場合は定理 3.10(2)，$s = 3$ の場合は定理 3.10(3) が適用でき，$1 \leq s \leq 3$ なる任意の s に対し，$\lambda_2(k) = 0$ であることが分かる．

よって以下 $s \geq 4$ であると仮定する．$s \geq 4$ は $p \equiv 1 \pmod{16}$ と同値である．

[8] の Theorem 1 と [14] より $s \geq 2$ に対し以下の結果が得られている：

命題 3.11. $\lambda(\mathfrak{X}_\infty) = 2^{s-2} - 1$.

(3.12)，命題 3.11 より，

$$\lambda_2(k) = 2^{s-2} - 1 - \lambda(I_\infty) \tag{3.13}$$

が得られた．(3.13) より $\lambda(I_\infty)$ の下界を求められれば $\lambda_2(k)$ の上界が得られることが分かる．$\lambda(I_\infty)$ を求めるには，写像 $I_\infty \longrightarrow G(M_n/L_n)$ を考え，I_∞ の像の 2-rank を考えればよい．この写像は全射である．

3.2 p の上の素イデアルについて

この節でも $s \geq 4$ であると仮定して議論をする．

十分大きな n に対して，p の上の k_n の素イデアル $\mathfrak{p}_i$ を考えることにする．この $\mathfrak{p}_i$ が，λ-不変量の考察に重要な役割を果たすのである．まず始めに p の k_{s-2} での素イデアル分解の様子を示す．

補題 3.12. $\mathbb{Q}(\zeta_{2^n})$ の判別式 $D_{\mathbb{Q}(\zeta_{2^n})}$ は，$n = 2$ のとき $D_{\mathbb{Q}(\zeta_{2^2})} = -4$，$n \neq 2$ のとき $D_{\mathbb{Q}(\zeta_{2^n})} = 2^{2^{n-1}(n-1)}$ となる．

証明. 円分体の判別式に関して以下の定理を用いる．

定理 3.13. p を素数とすると，円分体 $\mathbb{Q}(\zeta_{p^n})$ の判別式 $D_{\mathbb{Q}(\zeta_{p^n})}$ は，

$$D_{\mathbb{Q}(\zeta_{p^n})} = \pm p^{p^{n-1}(pn-n-1)},$$

ただし符号が $-$ となるのは $p^n = 4$ または $p \equiv 3 \pmod 4$ の場合に限る．

よって求める判別式 $D_{\mathbb{Q}(\zeta_{2^n})}$ は，$n = 2$ のとき，

$$D_{\mathbb{Q}(\zeta_{2^2})} = -2^{2^{2-1}(4-2-1)} = -4$$

$n \neq 2$ のとき，

$$D_{\mathbb{Q}(\zeta_{2^n})} = 2^{2^{n-1}(n-1)}$$

となる． □

補題 3.12 より $\mathbb{Q}(\zeta_{2^n})/\mathbb{Q}$ で分岐する素数は 2 のみであることが分かる．

補題 3.14. p は $\mathbb{Q}^{(s-2)}$ で完全分解する．

証明. $\mathbb{Q}^{(s-2)}$ は $\mathbb{Q}(\zeta_{2^s})$ の部分体なので，p が $\mathbb{Q}(\zeta_{2^s})$ で完全分解することを示せばよい．以下の定理を用いる．

定理 3.15 (円分体の類体論). ϕ を Euler 関数とする．$\mathbb{Q}(\zeta_m)$ において，p を $p \nmid m$ なる素数，f を $p^f \equiv 1 \pmod{m}$ を満たす最小の正の整数とする．このとき p は $\mathbb{Q}(\zeta_m)$ において $g = \phi(m)/f$ 個の素イデアルに分解される．各素イデアルの次数は f．特に，p が $\mathbb{Q}(\zeta_m)$ において完全分解であることと，$p \equiv 1 \pmod{m}$ であることは同値である．

上の定理において，$m = 2^s$ とすると s は $p-1$ を割り切る 2 の最大のべきなので $p \equiv 1 \pmod{2^s}$．よって p は $\mathbb{Q}(\zeta_{2^s})$ で完全分解する．以上で題意は示された． □

補題 3.16. 任意の n に対し，p の上の $\mathbb{Q}^{(n)}$ の素イデアルは $k_n/\mathbb{Q}^{(n)}$ で分岐する．

証明. k の判別式を D_k とすると，$p \equiv 1 \pmod{16}$ より $p \equiv 1 \pmod{4}$ なので $D_k = p$ となる．Dedekind の判別定理より p は $k/\mathbb{Q}$ で分岐するので，$k_n/\mathbb{Q}$ でも分岐する．同様に補題 3.12 と Dedekind の判別定理より $\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}$ において p は不分岐なので，$\mathbb{Q}^{(n)}/\mathbb{Q}$ で p は不分岐である．以上をまとめると，p は $k_n/\mathbb{Q}$ で分岐かつ $\mathbb{Q}^{(n)}/\mathbb{Q}$ で不分岐なので，p の上の $\mathbb{Q}^{(n)}$ の素イデアルは全て $k_n/\mathbb{Q}^{(n)}$ で分岐することが分かる． □

命題 3.17. k_{s-2} の相異なる素イデアル $\mathfrak{p}_1,\mathfrak{p}_2,\cdots,\mathfrak{p}_{2^{s-2}}$ が存在して，素イデアル分解 $\sqrt{p}O_{k_{s-2}} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_{2^{s-2}}$ が成立する．

証明. 補題 3.14 より p は $\mathbb{Q}^{(s-2)}$ で不分岐で完全分解する．よってその素イデアル分解は

$$pO_{\mathbb{Q}^{(s-2)}} = P_1\cdots P_{2^{s-2}}$$

となるので，分岐指数 $e(P_i/p) = 1$，P_i の次数 $f = [O_{\mathbb{Q}^{(s-2)}}/P_i : \mathbb{F}_p] = 1$，素イデアルの個数 $g = 2^{s-2}$ となる．補題 3.9 より p は $k_{s-2}/\mathbb{Q}^{(s-2)}$ で分岐する．$[k_{s-2} : \mathbb{Q}^{(s-2)}] = 2$ なので，P_i の上の k_{s-2} の素イデアルを $\mathfrak{p}_i$ とすると，その素イデアル分解は，

$$pO_{k_{s-2}} = \mathfrak{p}_1^2\cdots\mathfrak{p}_{2^{s-2}}^2$$

となる．すなわち分岐指数 $e'(\mathfrak{p}_i/p) = 2$，$\mathfrak{p}_i$ の次数 $f' = [O_{k_{s-2}}/\mathfrak{p}_\mathrm{i} : \mathbb{F}_p] = 1$ である．素イデアルの個数は $g' = 2^{s-2}$ となる．$\sqrt{p}$ の k_{s-2} での素イデアル分解を

$$\sqrt{p}O_{k_{s-2}} = {\mathfrak{p}'_1}^{e''}\cdots{\mathfrak{p}'_{g''}}^{e''}$$

とすると, 両辺を 2 乗して

$$pO_{k_{s-2}} = {\mathfrak{p}'_1}^{2e''}\cdots{\mathfrak{p}'_{g''}}^{2e''}$$

となる．よって素イデアル分解の一意性より $e'' = 1$, $g'' = 2^{s-2}$ が得られる．したがって

$$\sqrt{p}O_{k_{s-2}} = \mathfrak{p}_1\cdots\mathfrak{p}_{2^{s-2}}$$

が成立する． □

命題 3.18. $n \geq s-2$ なる任意の n に対し，$\mathfrak{p}_i O_{k_n}$ は k_n の素イデアルとなる．

証明. 補題3.16 より p は $k_n/\mathbb{Q}^{(n)}$ で完全分岐するので，$\mathbb{Q}^{(n)}$ での分解を考えればよい．$n \geq s-2$ に対し，p の素イデアル分解は

$$pO_{\mathbb{Q}^{(n)}} = P_1 \cdots P_{2^{s-2}},$$

すなわち分岐指数 $e(P_i/p) = 1$，P_i の次数 $f = [O_{\mathbb{Q}^{(n)}}/P_i : \mathbb{F}_p] = 2^{n-(s-2)}$，素イデアルの個数 $g = 2^{s-2}$ であることを帰納法で示す．$n = s-2$ の場合は明らか．$l \geq s-2$ とし，$n = l$ のとき成り立つ，すなわち $e(P_i/p) = 1,\ f = [O_{\mathbb{Q}^{(n)}}/P_i : \mathbb{F}_p] = 2^{l-(s-2)}$, $g = 2^{s-2}$ と仮定する．

以下の定理を用いる．

定理 3.19 (円分体の類体論：最大総実部分体の場合)．$\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ において，p を $p \nmid m$ なる素数，f を $p^f \equiv \pm 1 \pmod{m}$ を満たす最小の正の整数とする．このとき p は $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ において $g = \phi(m)/f$ 個の素イデアルに分解される（ϕ は Euler 関数）．各素イデアルの次数は f．特に，p が $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ において完全分解することと $p \equiv \pm 1 \pmod{m}$ であることは同値である．

$n = l+1$ の時，$p^{f'} \equiv \pm 1 \pmod{2^{l+3}}$ を満たす最小の正の整数 f' を探す．$p \equiv 1 \pmod{2^{l+3}}$ と仮定すると，$\mathrm{ord}_2(p-1) \geq l+3 \geq s+1$ となり矛盾する．よって $p \not\equiv 1 \pmod{2^{l+3}}$ である．次に $p \equiv -1 \pmod{2^{l+3}}$ と仮定すると，ある整数 m が存在して $p = 2^{l+3}m - 1$ とあらわせる．$p-1 = 2^{l+3}m - 2$ として両辺の ord_2 をとると，

$$\mathrm{ord}_2(p-1) = \mathrm{ord}_2(2(2^{l+2}m-1)) = \mathrm{ord}_2 2 + \mathrm{ord}_2(2^{l+2}m-1) = 1+0 = 1$$

となるが，今 $\mathrm{ord}_2(p-1) = s \geq 4$ と仮定しているので矛盾する．したがって $f' \neq 1$ であることが分かった．今 $p^{2^{l-(s-2)}} \equiv \pm 1 \pmod{2^{l+2}}$ なので，ある奇数 m が存在して，$p^{2^{l-(s-2)}} = \pm 1 + 2^{(l+2)}m$ とあらわせる．両辺を 2 乗すると，$p^{2^{l-(s-2)+1}} = 1 \pm 2^{l+3}m + 2^{(l+2)}m^2$ となる．よって $f' = 2$ が得られた．以上より $n \geq s-2$ なる任意の n について $e(P_i/p) = 1, f = [O_{\mathbb{Q}^{(n)}}/P_i : \mathbb{F}_p] = 2^{n-(s-2)}, g = 2^{s-2}$ であることが示された．$g = 2^{s-2}$ より p はこれ以上分解しないので，$\mathfrak{p}_i O_{k_n}$ も k_n の素イデアルである． □

$\mathbb{Q}^{(s-2)}$ の類数について，以下の定理を用いる．

定理 3.20 (岩澤 [6],1956)．p を素数，k を有限次代数体，K を k の p 冪次巡回拡大とし，K/k で分岐する素数がただ一つであるとする．このとき，k の類数が p と素ならば K の類数もまた p と素である．

定理 3.20 より 2 は $\mathbb{Q}^{(s-2)}$ の類数を割り切らないので，ある奇数 t が存在して，p の上にある $\mathbb{Q}^{(s-2)}$ の素イデアル P_i $(1 \leq i \leq 2^{s-2})$ に対し，P_i^t が単項イデアルになる．この t に対し，$\mathfrak{p}_i$ は $k_{s-2}/\mathbb{Q}^{(s-2)}$ で完全分岐するので，$[k_{s-2} : \mathbb{Q}^{(s-2)}] = 2$ と併せて $\mathfrak{p}_i^{2t} O_{k_{s-2}}$ は k_{s-2} の単項イデアルとなることが分かる．

[7, pp. 272,287] と [3] の Lemma 3.3 より得られる結果を紹介する．$\mathrm{cl}(\mathfrak{p}_i^t O_{k_n})$ を $\mathfrak{p}_i^t O_{k_n}$ で代表される k_n のイデアル類，ρ_n を k_n のイデアル類群における部分群 $\langle\ \mathrm{cl}(\mathfrak{p}_1^t O_{k_n}), \mathrm{cl}(\mathfrak{p}_2^t O_{k_n}), \ldots, \mathrm{cl}(\mathfrak{p}_{2^{s-2}}^t O_{k_n})\ \rangle$ の 2-rank とする．k は $\mathbb{Q}$ 上 Abel 拡大なので, Ferrero-Washington の定理より $\mu_2(k) = 0$ となる．よって十分大きな n に対してイデアル類群 $\mathrm{Cl}(k_n)$ の 2-rank が一定であり，また ρ_n もまた一定となる．より正確には，以下の補題が成り立っている．

補題 3.21. ある整数 $N \geq s-2$ が存在して，$n \geq N$ なる任意の n に対してイデアル類群 $\mathrm{Cl}(k_n)$ の 2-rank が一定であり，$\rho_n = \lambda_2(k)$ が成り立つ．

3.3 具体的な元から求める 2-rank

σ を $G(k_\infty/\mathbb{Q}_\infty)$ の生成元，$\mathfrak{l}_n$ を 2 の上の k_n の素イデアルとする．このとき $\mathfrak{l}_n \neq \mathfrak{l}_n^\sigma$ であり，また，補題 3.3 の証明より，$n \geq 1$ に対し $\alpha_n O_{k_n}$ は k_n の 2 の上の素イデアルなので，$\mathfrak{l}_n\mathfrak{l}_n^\sigma = \alpha_n O_{k_n}$ が成立する．2 の分解については以下の通り．

補題 3.22. k_n での 2 の素イデアル分解は $2O_{k_n} = \mathfrak{l}_n\mathfrak{l}_n^\sigma$ となる．

証明. 2 は $\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}$ で完全分岐するので，$\mathbb{Q}^{(n)}/\mathbb{Q}$ でも完全分岐する．2 の上の $\mathbb{Q}^{(n)}$ の素イデアルを P とおくと，$2O_{\mathbb{Q}^{(n)}} = P^{2^n}$ と表わせる．一方，$D_k = p \equiv 1 \pmod{16}$ より Kronecker 記号 $(\frac{D_k}{2}) = 1$ なので，2 は $k/\mathbb{Q}$ 上分解する．よって 2 は $k_n/\mathbb{Q}^{(n)}$ で分解する．$[k_n : \mathbb{Q}^{(n)}] = 2$ より P の上の素イデアルは 2 つしかなく，その内の 1 つを $\mathfrak{l}_n$ とすると，$G(k_\infty/\mathbb{Q}_\infty)$ の生成元 σ を用いて $PO_{k_n} = \mathfrak{l}_n\mathfrak{l}_n^\sigma$ と表わされる（今 $G(k_n/\mathbb{Q}^{(n)}) = G(k_\infty/\mathbb{Q}_\infty) = \{1, \sigma | \sqrt{5}^\sigma = -\sqrt{5}\}$ である）．よって $2O_{k_n} = (\mathfrak{l}_n\mathfrak{l}_n^\sigma)^{2^n}$ となる． □

E_n を整数環 O_{k_n} の単数群，$k_{n,\mathfrak{l}_n}$ を $\mathfrak{l}_n$ における k_n の完備化，$O^\times_{k_n,\mathfrak{l}_n}$ を整数環 $O_{k_n,\mathfrak{l}_n}$ の単数群，$U_n = O^\times_{k_n,\mathfrak{l}_n} \times O^\times_{k_n,\mathfrak{l}_n}$ とする．今 E_n を単射準同型

$$\varphi \colon E_n \ni \varepsilon \longmapsto (\varepsilon, \varepsilon^\sigma) \in O^\times_{k_n,\mathfrak{l}_n} \times O^\times_{k_n,\mathfrak{l}_n}$$

によって U_n に埋め込む．以下の補題を用いる．

補題 3.23 (Washington[12]). K を代数体，H を K の最大不分岐 Abel 拡大，F を p の外で不分岐な最大不分岐 Abel 拡大とする．さらに E を整数環 O_K の単数群，$\mathfrak{p}$ を p の上の K の素イデアル，$K_\mathfrak{p}$ を $\mathfrak{p}$ における K の完備化，$O_{K,\mathfrak{p}}$ を $K_\mathfrak{p}$ の整数環，$O^\times_{K,\mathfrak{p}}$ を $O_{K,\mathfrak{p}}$ の単数群とする．単射準同型

$$\psi \colon E \ni \varepsilon \longmapsto (\varepsilon, \ldots, \varepsilon) \in \prod_{\mathfrak{p}|p} O^\times_{K,\mathfrak{p}}$$

によって E を $\prod_{\mathfrak{p}|p} O^\times_{K,\mathfrak{p}}$ に埋め込む．このとき同型

$$G(F/H) \simeq \Big(\prod_{\mathfrak{p}|p} O^\times_{K,\mathfrak{p}}\Big)/\overline{\psi(E)}$$

が成立する．ここで $\overline{\psi(E)}$ は $\prod_{\mathfrak{p}|p} O^\times_{K,\mathfrak{p}}$ における $\psi(E)$ の位相的閉包である．

補題 3.23 を k_n に適用すると，同型

$$G(M_n/L_n) \simeq \left(O^{\times}_{k_n,\mathfrak{l}_n} \times O^{\times}_{k_n,\mathfrak{l}_n^{\sigma}}\right)/\overline{\psi(E_n)} \tag{3.14}$$

が得られる．$\mathfrak{m}_n$ を $\mathbb{Q}^{(n)}$ の素イデアル (α_n)，$\mathbb{Q}^{(n)}_{\mathfrak{m}_n}$ を $\mathfrak{m}_n$ における $\mathbb{Q}^{(n)}$ の完備化とすると，$\mathfrak{l}_n$,$\mathfrak{l}_n^{\sigma}$ は $\mathfrak{m}_n$ の上の k_n の素イデアルであり，補題 3.22 の証明より $\mathfrak{m}_n$ は $k_n/\mathbb{Q}^{(n)}$ で完全分解するので，同型 $\mathbb{Q}^{(n)}_{\mathfrak{m}_n} \simeq k_{n,\mathfrak{l}_n}$，$\mathbb{Q}^{(n)}_{\mathfrak{m}_n} \simeq k_{n,\mathfrak{l}_n^{\sigma}}$ が成立する．したがって $k_{n,\mathfrak{l}_n} \simeq k_{n,\mathfrak{l}_n^{\sigma}}$ より $O^{\times}_{k_n,\mathfrak{l}_n} \times O^{\times}_{k_n,\mathfrak{l}_n^{\sigma}} \simeq O^{\times}_{k_n,\mathfrak{l}_n} \times O^{\times}_{k_n,\mathfrak{l}_n}$ であることが分かる．写像 f, g をそれぞれ

$$f : O^{\times}_{k_n,\mathfrak{l}_n} \times O^{\times}_{k_n,\mathfrak{l}_n^{\sigma}} \ni (\varepsilon,\varepsilon) \longmapsto (\varepsilon,\varepsilon^{\sigma}) \in O^{\times}_{k_n,\mathfrak{l}_n} \times O^{\times}_{k_n,\mathfrak{l}_n},$$

$$g : \psi(E_n) \ni (\varepsilon,\varepsilon) \longmapsto (\varepsilon,\varepsilon^{\sigma}) \in \varphi(E_n)$$

と定義する．f は同型写像である．このとき以下の可換図式が成り立つ：

$$\begin{array}{ccc} \psi(E_n) & \longrightarrow & O^{\times}_{k_n,\mathfrak{l}_n} \times O^{\times}_{k_n,\mathfrak{l}_n^{\sigma}} \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle f} \\ \varphi(E_n) & \longrightarrow & O^{\times}_{k_n,\mathfrak{l}_n} \times O^{\times}_{k_n,\mathfrak{l}_n} \end{array} \tag{3.15}$$

(3.15) より，同型

$$\left(O^{\times}_{k_n,\mathfrak{l}_n} \times O^{\times}_{k_n,\mathfrak{l}_n^{\sigma}}\right)/\psi(E_n) \simeq U_n/\varphi(E_n)$$

が成り立つので，$\overline{\varphi(E_n)}$ を $O^{\times}_{k_n,\mathfrak{l}_n} \times O^{\times}_{k_n,\mathfrak{l}_n}$ における $\varphi(E_n)$ の位相的閉包として，同型

$$\left(O^{\times}_{k_n,\mathfrak{l}_n} \times O^{\times}_{k_n,\mathfrak{l}_n^{\sigma}}\right)/\overline{\psi(E_n)} \simeq U_n/\overline{\varphi(E_n)} \tag{3.16}$$

が成立している．(3.14), (3.16) より，同型

$$G(M_n/L_n) \simeq U_n/\overline{\varphi(E_n)}$$

が得られる．

補題 3.24. $(1,-1) \in U_n$ は $\overline{\varphi(E_n)}$ に属さない．

証明. 背理法を用いる．k_n は総実代数体なので基本単数の個数は $2^{n+1}-1$ 個である．よって $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_{2^{n+1}-1}$ を k_n の基本単数とする．$(1,-1) \in \overline{\varphi(E_n)}$ と仮定すると，ある 2-進整数 $x_1, x_2, \cdots, x_{2^{n+1}-1}$ が存在して，

$$(1,-1) = \pm(\varepsilon_1,\varepsilon_1^{\sigma})^{x_1}(\varepsilon_2,\varepsilon_2^{\sigma})^{x_2}\cdots(\varepsilon_{2^{n+1}-1},\varepsilon_{2^{n+1}-1}^{\sigma})^{x_{2^{n+1}-1}}$$

が成立する．よって両辺を 2 乗して各成分に注目すると，

$$\prod_{i=1}^{2^{n+1}-1} {\varepsilon_i}^{2x_i} = 1 \quad \text{かつ} \quad \prod_{i=1}^{2^{n+1}-1} ({\varepsilon_i}^{\sigma})^{2x_i} = 1$$

を得る．$\mathbb{Q}_2$ を 2-進数体，γ を $G(k_{n,\mathrm{l}_n}/\mathbb{Q}_2)$ の生成元とし，各成分に γ を作用させると，$1 \leq j \leq 2^n$ に対して

$$\prod_{i=1}^{2^{n+1}-1} (\varepsilon_i{}^{\gamma^j})^{2x_i} = 1 \quad \text{かつ} \quad \prod_{i=1}^{2^{n+1}-1} (\varepsilon_i{}^{\sigma\gamma^j})^{2x_i} = 1$$

が得られる．それぞれ両辺の 2-進対数 $\log_2$ をとると，

$$\sum_{i=1}^{2^{n+1}-1} x_i \log_2(\varepsilon_i^{\gamma^j})^2 = 0 \quad \text{かつ} \quad \sum_{i=1}^{2^{n+1}-1} x_i \log_2(\varepsilon_i^{\sigma\gamma^j})^2 = 0 \tag{3.17}$$

となる．(3.17) より

$$\begin{pmatrix} \log_2(\varepsilon_1^{\gamma^1}) & \cdots & \log_2(\varepsilon_{2^{n+1}-1}^{\gamma^1}) \\ \vdots & \ddots & \vdots \\ \log_2(\varepsilon_1^{\gamma^j}) & \cdots & \log_2(\varepsilon_{2^{n+1}-1}^{\gamma^j}) \\ \log_2(\varepsilon_1^{\sigma\gamma^1}) & \cdots & \log_2(\varepsilon_{2^{n+1}-1}^{\sigma\gamma^1}) \\ \vdots & \ddots & \vdots \\ \log_2(\varepsilon_1^{\sigma\gamma^j}) & \cdots & \log_2(\varepsilon_{2^{n+1}-1}^{\sigma\gamma^j}) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_{2^{n+1}-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \tag{3.18}$$

が得られる．(3.18) 左辺の一つ目の行列を A とおく．ここで Leopoldt 予想に関する結果を用いる．

予想 3.25 (Leopoldt 予想)**.** 任意の素数 p と任意の代数体 K に対し，K の p-進単数基準 $R_p(K) \neq 0$ であろう．

Leopoldt 予想については，以下の結果が得られている．

定理 3.26 (Brumer[1])**.** 任意の素数 p に対し，代数体 K が $\mathbb{Q}$ 上実 Abel であれば $R_p(K) \neq 0$ となる．

定理 3.26 より $\det A \neq 0$ となるので，(3.18) より

$$x_1 = x_2 = \cdots = x_{2^{n+1}-1} = 0$$

が得られるが，これは $(1,-1) = (1,1)$ となり矛盾する． □

$(1,-1)$ は 2 乗すると $(1,1) \in \overline{\varphi(E_n)}$ となるので位数 2 の元．同型 $G(M_n/L_n) \simeq U_n/\overline{\varphi(E_n)}$ より $(1,-1)$ に対応する $G(M_n/L_n)$ の元 σ' が唯一つ存在する．今全射 $I_\infty \longrightarrow G(M_n/L_n)$ を考えるので，σ' に写る I_∞ の元が少なくとも 1 つ存在する．よって $\lambda(I_\infty) \geq 1$ であることが分かった．

3.4 主定理の証明

主定理の証明のため，いくつかの準備をする．
$W_n = \{u \in O^\times_{\mathbb{Q}_2(\alpha_n)} |\ u \equiv 1 \pmod{4\alpha_n}\}$ とおく．

補題 3.27. $O^\times_{\mathbb{Q}_2(\alpha_n)} = \langle 3\rangle O^\times_{\mathbb{Q}^{(n)}} W_n$.

証明. 2 の外で不分岐な $\mathbb{Q}$ の最大 2-拡大は $\mathbb{Q}_\infty$ なので，2 の外で不分岐な $\mathbb{Q}^{(n)}$ の最大 2-拡大もまた $\mathbb{Q}_\infty$ である．よって $G(\mathbb{Q}_\infty/\mathbb{Q}^{(n)}) \simeq O^\times_{\mathbb{Q}_2(\alpha_n)}/\overline{O^\times_{\mathbb{Q}^{(n)}}}$ を得る．$O^\times_{\mathbb{Q}_2(\alpha_n)}/\overline{O^\times_{\mathbb{Q}^{(n)}}}$ は位相群として $3\overline{O^\times_{\mathbb{Q}^{(n)}}}$ で生成されるので，$O^\times_{\mathbb{Q}_2(\alpha_n)} = \langle 3\rangle\overline{O^\times_{\mathbb{Q}^{(n)}}}$．$W_n$ は $O^\times_{\mathbb{Q}_2(\alpha_n)}$ の開部分群なので, $\langle 3\rangle O^\times_{\mathbb{Q}^{(n)}} W_n$ も開部分群である．位相群において開部分群は閉部分群でもあるので $\langle 3\rangle O^\times_{\mathbb{Q}^{(n)}} W_n$ は閉部分群になる．したがって $\overline{\langle 3\rangle\overline{O^\times_{\mathbb{Q}^{(n)}}}} \subset \langle 3\rangle O^\times_{\mathbb{Q}^{(n)}} W_n$ が成り立つ．よって $O^\times_{\mathbb{Q}_2(\alpha_n)} = \langle 3\rangle O^\times_{\mathbb{Q}^{(n)}} W_n$ となる． □

補題 3.28. 任意の $u \in W_n$ に対し，$N_{\mathbb{Q}_2(\alpha_n)/\mathbb{Q}_2}(u) \equiv 1 \pmod{2^{n+3}}$.

証明. v_n を正規化された $\mathbb{Q}^{(n)}$ の加法的 α_n-進付値，γ を $G(\mathbb{Q}^{(n)}/\mathbb{Q})$ の生成元とする．
初めに $1 \le i \le 2^n - 1$ に対し

$$v_n(\alpha_n^{\gamma^i} - \alpha_n) \le 2^n + 1$$

が成り立つことを n についての帰納法により示す．$(\gamma^{2^{n-1}})^2 = \gamma^{2^n} = 1$ より，$\gamma^{2^{n-1}}$ の位数は 2 なので，$\alpha_n^{\gamma^{2^{n-1}}} = -\alpha_n$ となる．よって $v_n(\alpha_n^{\gamma^{2^{n-1}}} - \alpha_n) = v_n(-2\alpha_n) = 2^n + 1$. よって $n = 1$ のとき $v_1(\alpha_1^\gamma - \alpha_1) = 2 + 1 = 3$. $m < n$，$1 \le i \le 2^m + 1$ に対して $v_m(\alpha_m^{\gamma^i} - \alpha_m) \le 2^m + 1$ と仮定する．$\alpha_n^2 = \alpha_{n-1} + 2$ より，$1 \le i \le 2^n - 1$，$i \ne 2^{n-1}$ に対して $v_n(\alpha_n^{\gamma^i} + \alpha_n) \ge 1$ であることに注意すると，

$$\begin{aligned} v_n(\alpha_n^{\gamma^i} - \alpha_n) + v_n(\alpha_n^{\gamma^i} + \alpha_n) &= v_n(\alpha_n^{2\gamma^i} - \alpha_n^2) \\ &= v_n(\alpha_{n-1}^{\gamma^i} - \alpha_{n-1}) \\ &= 2v_{n-1}(\alpha_{n-1}^{\gamma^i} - \alpha_{n-1}) \le 2^n + 2 \end{aligned}$$

が成り立つ．以上により $1 \le i \le 2^n - 1$ に対して $v_n(\alpha_n^{\gamma^i} - \alpha_n) \le 2^n + 1$ が成り立つことが示された．

よって [13, p. 233] の Corollary 1(1) より $N_{\mathbb{Q}_2(\alpha_n)/\mathbb{Q}_2}(u) \equiv 1 \pmod{2^{n+3}}$ が成り立つ． □

補題 3.29. $\mathbb{F}_2$ を標数 2 の素体，G を γ で生成される位数 2^n の巡回群，$V = \mathbb{F}_2[G]$ を $\mathbb{F}_2$ 上 G の群環とする．$i_1, i_2, \cdots, i_r \in \mathbb{Z}$ を $0 \le i_1 < i_2 < \cdots < i_r \le 2^n - 1$ を満たすようにとり，さらに $v \in V$ を，これら $i_1, i_2, \cdots, i_r$ に対して $v = \gamma^{i_1} + \gamma^{i_2} + \cdots + \gamma^{i_r}$ とおく．r が奇数であるとすれば，V は $\mathbb{F}_2$ 上のベクトル空間として $\{\gamma^i v \mid 0 \le i \le 2^n - 1\}$ で生成される．

証明. 関数 $f : G \longrightarrow \mathbb{C}$ を以下のように定義する．$i \in \mathbb{Z}$ を $0 \leq i \leq 2^n - 1$ とし，$i = i_1, i_2, \cdots, i_r$ に対し $f(\gamma^i) = 1$，$i \neq i_1, i_2, \cdots, i_r$ に対し $f(\gamma^i) = 0$．このとき [12, p. 71] より

$$\det(f(\gamma^{i-j}))_{0 \leq i,j \leq 2^n-1} = \prod_{\chi \in \hat{G}} \sum_{i=0}^{2^n-1} \chi(\gamma^i) f(\gamma^i) \equiv r^{2^n} \equiv 1 \pmod{\zeta_{2^n} - 1}$$

ここで $\hat{G}$ は G の指標群である． □

今，φ は E_n を U_n に埋め込む単射準同型

$$\varphi : E_n \ni \varepsilon \longmapsto (\varepsilon, \varepsilon^\sigma) \in O^\times_{k_n, \mathfrak{l}_n} \times O^\times_{k_n, \mathfrak{l}_n}$$

であることに注意する．

補題 3.30. $n \geq s - 2$ に対し $\mathfrak{p}_1^t O_{k_n}$ が k_n の単項イデアルでないとする．このとき，$N_{k_n/\mathbb{Q}^{(n)}}(\varepsilon) = 1$ を満たす k_n の任意の単数 ε に対し，ある $c \in O^\times_{\mathbb{Q}^{(n)}}$ が存在して $\phi(\varepsilon c)$ が U_n の平方数となる．

証明. $N_{k_n/\mathbb{Q}^{(n)}}(\varepsilon) = 1$ より $\varepsilon = \alpha^{\sigma-1}$ となる $\alpha \in O_{k_n}$ が存在する．初めに $n \geq s - 2$ と仮定する．$\mathfrak{p}_1 O_{k_n}, \mathfrak{p}_2 O_{k_n}, \cdots, \mathfrak{p}_{2^{s-2}} O_{k_n}$ は k_n の素イデアルであり，$\mathbb{Q}^{(n)}$ 上 k_n で分岐するので，αO_{k_n} は $\mathfrak{p}_i O_{k_n}$ の有限個の積であると仮定してよい．各 $\mathfrak{p}_i O_{k_n}$ は k 上 $\mathfrak{p}_1 O_{k_n}$ と共役かつ k_n において単項でないので，補題 3.29 より αO_{k_n} は $\mathfrak{p}_i O_{k_n}$ の偶数個の積になると分かる．よって $p \equiv 1 \pmod{2^s}$ と $s \geq 3$ より

$$N_{k_n/\mathbb{Q}}(\alpha) \equiv \pm 1 \pmod{2^{n+3}} \tag{3.19}$$

が得られる．今補題 3.27 より $\alpha\alpha^\sigma \in O^\times_{\mathbb{Q}^{(n)}} W_n$ または $\alpha\alpha^\sigma \in 3O^\times_{\mathbb{Q}^{(n)}} W_n$ である．$\alpha\alpha^\sigma \in 3O^\times_{\mathbb{Q}^{(n)}} W_n$ と仮定すると，補題 3.28 より

$$N_{\mathbb{Q}^{(n)}/\mathbb{Q}}(\alpha\alpha^\sigma) \equiv \pm(1 + 2^{n+2}) \pmod{2^{n+3}} \tag{3.20}$$

が得られるが，これは (3.19) と矛盾する．よって $\alpha\alpha^\sigma \in O^\times_{\mathbb{Q}^{(n)}} W_n$ を得る．[12, p. 183] より W_n の任意の元は $O^\times_{k_n, \mathfrak{l}_n}$ の平方数なので，ある $c \in O^\times_{\mathbb{Q}^{(n)}}$ が存在して，$\varepsilon c = \alpha\alpha^\sigma c/\alpha^2$ が成り立つ．またこのとき $\varepsilon^\sigma c = \alpha\alpha^\sigma c/(\alpha^\sigma)^2$ である．$\alpha\alpha^\sigma c/\alpha^2$，$\alpha\alpha^\sigma c/(\alpha^\sigma)^2$ は共に $O^\times_{k_n, \mathfrak{l}_n}$ の平方数である．

$s - 2 > n$ と仮定する．$\alpha\alpha^\sigma \in 3O^\times_{\mathbb{Q}^{(n)}} W_n$ とすると再び (3.20) が成り立ち，$p \equiv 1 \pmod{2^s}$ に矛盾する．よって $\alpha\alpha^\sigma \in O^\times_{\mathbb{Q}^{(n)}} W_n$ が得られ，以下同様の議論によって結論が得られる． □

E_n^2 を k_n の単数の平方からなる集合，$c_1, c_2, \ldots, c_{2^n-1}$ を $\mathbb{Q}^{(n)}$ の基本単数とする．$\mathfrak{p}_1 O_{k_n}, \mathfrak{p}_2 O_{k_n}, \ldots, \mathfrak{p}_{2^{s-2}} O_{k_n}$ は $\mathbb{Q}^{(n)}$ 上 k_n で分岐するので，$c_1 E_n^2, c_2 E_n^2, \cdots, c_{2^n-1} E_n^2$ は $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ 上独立である．よって，$\eta_1 O^\times_{\mathbb{Q}^{(n)}} E_n^2, \ldots, \eta_{2^n} O^\times_{\mathbb{Q}^{(n)}} E_n^2 \in O_{k_n}/O^\times_{\mathbb{Q}^{(n)}} E_n^2$ が $\mathbb{F}_2$ 上独立となる O_{k_n} の単数 $\eta_1, \ldots, \eta_{2^n}$ が存在する．

以上の準備より，$\lambda_2(k)$ に上界を与える主定理 2 を示すことができる．主定理 1(1) は主定理 2 より導かれる．

定理 3.31 (主定理 2，福田-小松 [2])．$m_n \in \mathbb{Z}_{\geq 0}$，$m_n \leq 2^{s-2}-2$ として，$\varepsilon_1, \ldots, \varepsilon_{m_n}$ を k_n の単数で，$\varepsilon_1 O_{\mathbb{Q}_n}^{\times} E_{k_n}^2, \cdots, \varepsilon_{m_n} O_{\mathbb{Q}_n}^{\times} E_{k_n}^2 \in E_{k_n}/O_{\mathbb{Q}_n}^{\times} E_{k_n}^2$ が $\mathbb{F}_2$ 上独立であるものとする．$1 \leq i \leq m_n$ に対し，$N_{k_n/\mathbb{Q}^{(n)}}(\varepsilon_i) = 1$ かつ $N_{k_n/k}(\varepsilon_i) = \pm 1$ ならば，$\lambda_2(k) \leq 2^{s-2} - m_n - 2$ が成り立つ．

証明．$\mathfrak{p}_1^t O_{k_n}$ が O_{k_n} の単項イデアルであるならば，補題 3.21 より $\lambda_2(k) = 0$ となるので不等式は自明である．よって以下 $\mathfrak{p}_1^t O_{k_n}$ は O_{k_n} の単項イデアルでないとする．$k_{n,\mathfrak{l}_n}$ と $\mathbb{Q}_2(\alpha_n)$ を同一視する．$\varepsilon_i \in O_{\mathbb{Q}_2(\alpha_n)}^{\times}$ かつ $N_{\mathbb{Q}_2(\alpha_n)/\mathbb{Q}}(\varepsilon_i) = N_{k_n/k_0}(\varepsilon_i) = \pm 1$ なので，類体論より $\varepsilon_i \in \overline{O_{\mathbb{Q}_n}^{\times}}$ を得る．補題 3.30 より $\varepsilon_i c_i' \in {O_{\mathbb{Q}_2(\alpha_n)}^{\times}}^2$ を満たす c_i' が存在する．$O_{\mathbb{Q}_2(\alpha_n)}^{\times}/\overline{O_{\mathbb{Q}^{(n)}}^{\times}} \simeq G(\mathbb{Q}_\infty/\mathbb{Q}) \simeq \mathbb{Z}_2$ であるので，ε_i, c_i' に対してある $c_i'' \in \overline{O_{\mathbb{Q}^{(n)}}^{\times}}$ が存在して，$\varepsilon_i c_i' = (c_i'')^2$ となる．よって $(\varepsilon_i c_i', \varepsilon_i^\sigma c_i') = ((c_i'')^2, (c_i''/\varepsilon_i)^2)$ が成り立つ．$(c_i'', c_i''/\varepsilon_i) \equiv (1, 1/\varepsilon_i) \pmod{\overline{\varphi(E_n)}}$ より，$(c_i'', c_i''/\varepsilon_i)\overline{\varphi(E_n)}$ は $G(M_n/k_\infty)$ における $\mathfrak{l}_n^\sigma$ の惰性群の元で，その位数は 2 となる．惰性群は最大不分岐部分体に対応しており，M_n/k_∞ の最大不分岐部分体は L_n なので，$G(M_n/k_\infty)$ における $\mathfrak{l}_n^\sigma$ の惰性群とは $G(M_n/L_n)$ のことである．今 $G(M_n/L_n)$ で位数 2 の元を m_n 個見つけたので，I_∞ の像の 2-rank が m_n 以上であることが分かる．よって補題 3.24 と併せて，$I_\infty G(M_\infty/M_n)/G(M_\infty/M_n)$ のねじれ部分の 2-rank は $m_n + 1$ 以上であることが分かる．$\lambda(I_\infty) \geq m_n + 1$ が示されたので，$\lambda_2(k) \leq 2^{s-2} - m_n - 2$ が得られた． □

不等式 $\lambda_2(k) \leq 2^{s-2} - m_n - 2$ は任意の $n \geq 1$ に対して成立している．λ-不変量についてはできるだけ小さい上限が欲しいので，$n \geq 1$ に対して m_n がどれだけ大きな値をとるかを調べることは重要である．計算機を用いて実際に計算した結果，$p < 10^4$ の範囲で $p \equiv 1 \pmod{16}$ なる全ての素数 p について，ある n_0 が存在して $m_{n_0} = 2^{s-2} - 2$ となることが確認された [2]．しかしその計算結果から m_n について記述する公式を発見することは難しい．主定理 1(1) は m_1 について実際に数値を与えることができる場合を述べている．

最後に主定理 1 を証明する．

主定理 1 の証明．(1)　ε_0' は $\mathbb{Q}(\sqrt{2p})$ の単数なので，$N_{\mathbb{Q}(\sqrt{2p})/\mathbb{Q}}(\varepsilon_0') = a^2 - 2pb^2 = \pm 1$ となる．よって $a \equiv \pm 1 \pmod{p}$ である．$a \equiv 1 \pmod{p}$ と仮定する．このとき $a^2 - 2pb^2 = 1$ となる．$a+1$ と $a-1$ の最大公約数 $\gcd(a+1, a-1) = 2$ であることに注意する．$\varepsilon_1 = \frac{\sqrt{a+1}}{2}\sqrt{2} + \frac{b}{\sqrt{a+1}}\sqrt{p}$ とおくと，

$$\begin{aligned}
\varepsilon_1^2 &= \frac{a+1}{2} + b\sqrt{2p} + \frac{b^2}{a+1}p \\
&= \frac{(a+1)^2 + 2b^2 p}{2(a+1)} + b\sqrt{2p} \\
&= \frac{(a+1)^2 + a^2 - 1}{2(a+1)} + b\sqrt{2p} \\
&= a + b\sqrt{2p} = \varepsilon_0'
\end{aligned}$$

となる．ε_0' は代数的整数なので，ε_1 もまた代数的整数である．今 $a \equiv 1 \pmod 4$ と仮定すると，$4 \mid a-1$ かつ $\gcd(a+1, a-1) = 2$ より，$2 \mid a+1$ かつ $4 \nmid a+1$ となる．よって $\frac{a+1}{2}$ は奇数である．また，$a \equiv 1 \pmod p$，$a \equiv 1 \pmod 4$ より $\frac{a-1}{4p}$ は有理整数であり，$(\frac{a+1}{2}, \frac{a-1}{4p}) = 1$ である．よって

$$\frac{a+1}{2}\frac{a-1}{4p} = \left(\frac{b}{2}\right)^2$$

より $\frac{a+1}{2}$，$\frac{a-1}{4p}$ は共に有理整数の平方数となる．したがって $\sqrt{\frac{a+1}{2}}, \sqrt{\frac{a-1}{4p}}$ は有理整数である．今 $\frac{\sqrt{a+1}}{2}\sqrt{2}$ が有理整数であることが得られた．$\sqrt{\frac{a+1}{2}} = t$ とおくと，t は有理整数であり，

$$\begin{aligned}\frac{b}{a+1}\sqrt{p} &= \frac{b\sqrt{p}}{t\sqrt{2}} \\ &= \frac{b}{2t}\sqrt{2p}\end{aligned}$$

が成り立つ．よって $\frac{b}{2t}$ が有理数であることより，ε_1 が $\mathbb{Q}(\sqrt{2p})$ の元になると導かれるが，これは ε_0' が基本単数であることに矛盾する．よって $a \equiv -1 \pmod 4$ である．$\frac{a+1}{4} = t$，$\frac{a-1}{2p} = s$ とおく．s, t は共に有理整数である．また，$\gcd(a+1, a-1) = 2$ かつ $4 \mid a+1$ より s は奇数である．このとき $\frac{a+1}{2}\frac{a-1}{4p} = (\frac{b}{2})^2$ を t, s を用いて変形して，

$$ts = \left(\frac{b}{2}\right)^2$$

を得る．ts は有理整数かつ $\frac{b}{2}$ は有理数なので，$(\frac{b}{2})^2$ は有理整数の平方数となる．$\gcd(a+1, a-1) = 2$ なので，t, s は互いに素で，共に有理整数の平方数である．よって

$$\sqrt{t} = \pm\frac{\sqrt{a+1}}{2}$$

が有理整数であることが分かる．$\frac{\sqrt{a+1}}{2} = t'$ とおくと，$\sqrt{a+1} = 2t'$ は有理整数となる．よって

$$\frac{b}{\sqrt{a+1}} = \frac{b}{2t'}$$

より $\frac{b}{\sqrt{a+1}}$ は有理数になることが分かる．今 $\frac{\sqrt{a+1}}{2}$ は有理整数で，$\sqrt{2}$ は代数的整数なので，$\frac{\sqrt{a+1}}{2}\sqrt{2}$ もまた代数的整数となる．ε_1 も代数的整数なので，

$$\frac{b}{\sqrt{a+1}}\sqrt{p} = \varepsilon_1 - \frac{\sqrt{a+1}}{2}\sqrt{2}$$

もまた代数的整数であることが分かる．$\frac{b}{\sqrt{a+1}}\sqrt{p}$ を 2 乗すると，$\frac{b^2}{a+1}p = \frac{a-1}{2}$ となり，$\frac{b^2}{a+1}p$ が有理整数であることが分かる．仮定より $(a+1, p) = 1$ なので，$\frac{b^2}{a+1}p$ は有理整数

となり，したがって $\frac{b}{\sqrt{a+1}}\sqrt{p}$ は 2 乗すると有理整数なので代数的整数である．$\frac{b}{\sqrt{a+1}}\sqrt{p}$ は有理数かつ代数的整数なので，有理数となる．以上により

$$\frac{\sqrt{a+1}}{2}, \frac{b}{\sqrt{a+1}}\sqrt{p} \in \mathbb{Z} \tag{3.21}$$

が得られた．[9] より (3.21) は $\varepsilon_0, \varepsilon_1, 1+\sqrt{2}$ が $\mathbb{Q}(\sqrt{p}, \sqrt{2})$ の基本単数であることを導く．$N_{k_1/\mathbb{Q}^{(1)}}(\varepsilon_1) = 1$ かつ $N_{k_1/k}(\varepsilon_1) = -1$ なので，定理 3.31 より $\lambda_2(k) \leq 2^{s-2} - 3$ が得られる．

(2)　$a^2 \equiv -1 \pmod{p}$ と仮定する．これは $a^2 - 2pb^2 = -1$ を導く．h_k を k の類数とする．今 h_k が奇数であることに注意する．よって種数公式より $\mathbb{Q}(\sqrt{2p})$ のイデアル類群において $(\mathfrak{l}_n \cap \mathbb{Q}(\sqrt{2p}))^{h_k}$ を含むイデアル類の位数は 2 であることが分かる．これは k_n のイデアル類群の 2-Sylow 部分群 A_n において，$\mathrm{cl}(\mathfrak{l}_n^{h_k})$ が自明でないことを意味している．$\varepsilon_0^2 \not\equiv 1 \pmod{32}$ なので，

$$B_n = \{a \in A_n | a^\tau = a, \forall \tau \in G(k_n/k)\}$$

の位数は 2 以下である．よって $B_n = \langle \mathrm{cl}(\mathfrak{l}_n^{h_k}) \rangle$ となる．ここで以下の定理を用いる．

定理 3.32 (Greenberg[4]). p を素数，k を p が完全分岐する総実代数体とする．また，A_n を k_n のイデアル類群の唯一の p-Sylow 部分群，$B_n = \{a \in A_n | a^\tau = a, \forall \tau \in G(k_n/k)\}$ とし，さらに，k に対して Leopoldt 予想が成り立つと仮定する．このとき，以下の条件 (1), (2) は同値であり，この条件を満たすならば $\mu_p(k) = \lambda_p(k) = 0$ となる．

(1)　$n \longrightarrow \infty$ のとき $\sharp A_n$ は有界となる，

(2)　十分大きな n に対し，B_n の各類は p の上の素イデアルを含む．

今 $k = \mathbb{Q}(\sqrt{p})$ は 2 次体なので $\mathbb{Q}$ 上 Abel であり，よって定理 3.26 が適用できるので Leopoldt 予想が成り立つことが分かる．また，$B_n = \langle \mathrm{cl}(\mathfrak{l}_n^{h_k}) \rangle$ より十分大きな n に対して B_n の各類が 2 の上の素イデアルを含んでいることは明らかである．したがって定理 3.32(2) の条件を満たすので，$\lambda_2(k) = 0$ となることが分かる．　□

参考文献

[1] Armand Brumer. On the units of algebraic number fields. *Mathematika*, Vol. 14, pp. 121–124, 1967.

[2] Takashi Fukuda and Keiichi Komatsu. On the Iwasawa λ-invariant of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{p})$. *Math. Comp.*, Vol. 78, No. 267, pp. 1797–1808, 2009.

[3] Takashi Fukuda, Keiichi Komatsu, Manabu Ozaki, and Hisao Taya. On Iwasawa λ_p-invariants of relative real cyclic extensions of degree p. *Tokyo J. Math.*, Vol. 20, No. 2, pp. 475–480, 1997.

[4] Ralph Greenberg. On the Iwasawa invariants of totally real number fields. *Amer. J. Math.*, Vol. 98, No. 1, pp. 263–284, 1976.

[5] Ralph Greenberg. On the structure of certain Galois groups. *Invent. Math.*, Vol. 47, No. 1, pp. 85–99, 1978.

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

[7] Kenkichi Iwasawa. Riemann-Hurwitz formula and p-adic Galois representations for number fields. *Tôhoku Math. J. (2)*, Vol. 33, No. 2, pp. 263–288, 1981.

[8] Yûji Kida. Cyclotomic $\mathbf{Z}_2$-extensions of J-fields. *J. Number Theory*, Vol. 14, No. 3, pp. 340–352, 1982.

[9] Tomio Kubota. Über den bizyklischen biquadratischen Zahlkörper. *Nagoya Math. J.*, Vol. 10, pp. 65–85, 1956.

[10] J. Neukirch and N. Schappacher. *Algebraic number theory*. Springer, 1999.

[11] Manabu Ozaki and Hisao Taya. On the Iwasawa λ_2-invariants of certain families of real quadratic fields. *Manuscripta Math.*, Vol. 94, No. 4, pp. 437–444, 1997.

[12] Lawrence C. Washington. *Introduction to cyclotomic fields*, Vol. 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[13] André Weil. *Basic number theory*. Springer-Verlag, New York, third edition, 1974. Die Grundlehren der Mathematischen Wissenschaften, Band 144.

[14] A. Wiles. The Iwasawa conjecture for totally real fields. *Ann. of Math. (2)*, Vol. 131, No. 3, pp. 493–540, 1990.

[15] 藤崎源二郎, 森田康夫, 山本芳彦. 数論への出発 増補版, 2004.