岩澤理論における岩澤類数公式と岩澤不変量のPARI/GPによる計算について

高橋　和暉

新潟大学大学院自然科学研究科博士前期課程
数理物質科学専攻

2024年1月25日

概要

本論文は，岩澤健吉氏によって創始された岩澤理論における岩澤類数公式に焦点をあてて，著者が学んできたことを計算例とともにまとめたものである．

ガロア拡大 K/k のガロア群が p 進整数環 $\mathbb{Z}_p$ の加法群に位相同型であるとき，拡大 K/k を $\mathbb{Z}_p$ 拡大という．有限次代数体 k の $\mathbb{Z}_p$ 拡大体を K とすると，K/k の中間体は $k = k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_n \subset \cdots \subset K$（$k_n$ は k 上 p^n 次の中間体）とあらわせる．この中間体の類数の p 部分の挙動を記述するのが岩澤類数公式である．

1 章では，$\mathbb{Z}_p$ の元である p 進整数について解説する．まず 1.1 節では，p 進整数の定義と p 進整数のなす環 $\mathbb{Z}_p$ について復習する．また，p 進整数環 $\mathbb{Z}_p$ の商体である p 進数体 $\mathbb{Q}_p$ の異なった見方をそれぞれ 1.2 節と 1.3 節で与える．これにより p 進整数への理解がより深まることを期待している．

2 章では，実際に $\mathbb{Z}_p$ 拡大を構成する．2.1 節では，そのための準備として群論の命題を述べる．2.2 節では，2.1 節で与えた命題を用いて，基本的な $\mathbb{Z}_p$ 拡大である円分 $\mathbb{Z}_p$ 拡大を構成する．その際，p が 2 であるか奇素数であるかで違いが生じるので，その点を例 2.3 で紹介する．

3 章では，岩澤理論における一つの主人公である岩澤代数をあつかう．岩澤代数は，ある群環の逆極限として自然に現れる対象であるが，J-P. Serre によって一変数形式的冪級数環 Λ との間の同型が示された．これにより，一変数形式的冪級数環 Λ を調べることが重要となり，3.1 節では，Λ およびその中で重要な役割を演じる distinguished 多項式について述べる．また，証明は割愛したが，岩澤類数公式と本質的に関わりのある有限生成 Λ 加群の構造定理も紹介する．3.2 節では，4 章へ向けて岩澤代数の定義を紹介し，一変数冪級数環 Λ との間の同型を証明する．3 章を通じて $\mathbb{Z}_p$ をより一般化した，$\mathbb{Q}_p$ の有限次拡大体の整数環を扱う．この点で，Λ が UFD であることや補題 3.10 の証明においては，それぞれ参考とした [市村]，[福田 2] よりも一般的な形で説明するように工夫している．

4 章では，岩澤類数公式を示すことを目標とする．まず，4.1 節において岩澤理論におけるもう一つの主人公である岩澤加群をあつかう．これはイデアル類群の p 部分の逆極限として定義され，岩澤代数が自然に作用している．これはまた，類体論によってガロア群の p 部分の逆極限と同型である．4.2 節では，いよいよ岩澤類数公式を示す．岩澤加群への岩澤代数の作用をガロア群の p 部分の逆極限 X への Λ の作用としてとらえ，その作用の仕方を見ていく．X は有限生成ねじれ Λ 加群であることを示し，3 章の有限生成 Λ 加群の構造定理によって，そのおおまかな構造が得られる．この得られた構造などを調べる

ことによって，類数の p 部分への寄与をあぶりだし，岩澤類数公式が示される．4.3 節では，岩澤多項式に関する計算例を紹介する．不慣れな読者を想定して PARI/GP の基本的な使い方から説明するようにした．本題である計算の部分では，立教大学の水澤靖氏によって作成された，PARI/GP のプログラムである Iwapoly.gp を用い，$1 < m < 10^6$ の範囲において，虚 2 次体 $\mathbb{Q}(\sqrt{-m})$ の円分 $\mathbb{Z}_3$ 拡大の岩澤 λ 不変量と岩澤多項式を計算している．

5 章では，著者が岩澤理論を学んでいく中で興味をもった非アーベル岩澤理論に関する話題を扱う．早稲田大学の尾崎学氏が書かれた論文 [尾崎] に基づいて，比較的最近の研究結果などについて紹介する．

謝辞

指導教員である星明考先生には，学部 4 年生からの 3 年間，セミナーを通じて丁寧にご指導いただきました．様々な知識や考え方とともに示唆的な助言を数多くいただき，成長の機会に恵まれたおかげで，かけがえのない財産を得ることができました．ここに深く感謝の意を示します．

研究室 OB である金井和貴先輩と博士課程の池田愛輝先輩には，学部生の頃からお世話になり，修士論文執筆に際しても助言をいただきました．同期の渡邊崇弘君と後輩の飯田紘明君には，私の発表を聞いていただき，議論にも参加していただきました．ここに感謝申し上げます．

水澤靖先生，青木美穂先生，藤井俊先生には，本論文の草稿に対してアドバイスや励ましのことばをいただきました．また，水澤先生からは，Iwapoly.gp が水澤先生の researchmap 上にあることを教えていただき，4.3 節では Iwapoly.gp を用いて多くの計算を行なうことができました．青木先生からは，本論文の内容と関係している文献を紹介していただきました．藤井先生からは，本論文における例をより前進させるアイデアを紹介していただきました．ここに篤く感謝の意を示します．

最後に，心配ばかり掛けてしまいましたが，常に私を支え続けてくださった家族に，心より感謝申し上げます．

目次

1　p 進整数

1 章では，素数 p ごとに定まる p 進整数とその性質について復習する．1.1 節では p 進整数の定義とその基本的な性質について述べ，1.2 節，1.3 節では異なる視点からの p 進整数の捉え方について述べている．1 章の内容は主に [斎藤]，[ノイキルヒ] に基づいている．

1.1　p 進整数と p 進数

この節では，主に [斎藤, 7 章] に基づいて，p 進整数の定義と基本的な性質について述べる．

環 R に対し $R^\times$ で R の乗法群をあらわすこととする．

p を素数とする．非負整数 $0 \leq n \leq m$ に対し，$\mathbb{Z}/p^m\mathbb{Z}$ から $\mathbb{Z}/p^n\mathbb{Z}$ へは自然な準同型

$$\varphi_{n,m} \colon \mathbb{Z}/p^m\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}\ ;\ a \bmod p^m \longmapsto a \bmod p^n$$

が定まる．このとき $(\mathbb{Z}/p^n\mathbb{Z}, \varphi_{n,m})$ は逆系をなし，その逆極限 $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ を **p 進整数環**，$\mathbb{Z}_p$ の元を **p 進整数**という．$x = (x_n)_{n\geq 0} \in \mathbb{Z}_p$ に対し

$$x_n = x \bmod p^{n+1}$$

とかくことにする．単射準同型

$$\mathbb{Z} \longrightarrow \mathbb{Z}_p\ ;\ a \longmapsto (a, a, \ldots, a)$$

によって $\mathbb{Z}$ は $\mathbb{Z}_p$ の部分環となる．

$(a_k)_{k\geq 0}$ を整数の列とする．このとき各 $n \geq 0$ に対し

$$x_n = \sum_{k=0}^{n} a_k p^k \bmod p^{n+1}$$

とすれば $x = (x_n)_{n\geq 0} \in \mathbb{Z}_p$ となる．このとき

$$x = \sum_{k=0}^{\infty} a_k p^k$$

とかくことにする．

定理 1.1 ([斎藤, page 130, 定理 7.4] 参照)**.** p 進整数 $x \in \mathbb{Z}_p$ に対し，整数の列 $(a_k)_{k\geq 0}$ $(0 \leq a_k \leq p-1)$ が一意的に存在し

$$x = \sum_{k=0}^{\infty} a_k p^k$$

とかける．これを x の $\boldsymbol{p}$ **進展開**という．

証明. $x = (x_n)_{n\geq 0} \in \mathbb{Z}_p$ とする．各 $n \geq 0$ に対し

$$x_n = \sum_{k=0}^{n} a_k p^k \bmod p^{n+1}$$

を満たす数列 $(a_k)_{k\geq 0}$ $(0 \leq a_k \leq p-1)$ が一意的に存在することを示せばよい．$n = 0$ に対する条件を考えると $0 \leq a_0 \leq p-1$ は一意的に定まる．$n \geq 1$ に対し $a_0, \ldots, a_{n-1}$ が一意的に定まっているとする．このとき

$$\begin{aligned}
\varphi_{n-1,n}\left(x_n - \left(\sum_{k=0}^{n-1} a_k p^k \bmod p^{n+1}\right)\right) &= \varphi_{n-1,n}(x_n) - \varphi_{n-1,n}\left(\sum_{k=0}^{n-1} a_k p^k \bmod p^{n+1}\right) \\
&= x_{n-1} - \left(\sum_{k=0}^{n-1} a_k p^k \bmod p^n\right) \\
&= 0 \in \mathbb{Z}/p^n\mathbb{Z}
\end{aligned}$$

であるから $0 \leq a_n \leq p-1$ が存在し

$$x_n - \left(\sum_{k=0}^{n-1} a_k p^k \bmod p^{n+1}\right) = a_n p^n \bmod p^{n+1}$$

とかける．このとき

$$x_n = \sum_{k=0}^{n} a_k p^k \bmod p^{n+1}$$

が成り立つ．$0 \leq b_n \leq p-1$ に対しても

$$x_n = \sum_{k=0}^{n-1} a_k p^k + b_n p^n \bmod p^{n+1}$$

が成り立つとすると

$$p^n(a_n - b_n) \equiv 0 \pmod{p^{n+1}}$$

となるので

$$a_n - b_n \equiv 0 \pmod{p^n}$$

である．$0 \leq a_n, b_n \leq p-1$ なので $a_n = b_n$ である． □

命題 1.2 ([斎藤, page 131, 補題 7.5] 参照)**.** $x = \sum_{k=0}^{\infty} a_k p^k$ を $x \in \mathbb{Z}_p$ の p 進展開とする．このとき $p^n x$ の p 進展開は

$$b_k = \begin{cases} 0 & (0 \leq k \leq n-1), \\ a_{k-n} & (k \geq n) \end{cases}$$

と定めたとき

$$p^n x = \sum_{k=0}^{\infty} b_k p^k$$

によって与えられる．

証明. $m \geq 0$ に対し

$$\begin{aligned} p^n x \mod p^{m+1} &= (p^n \bmod p^{m+1}) \cdot (x \bmod p^{m+1}) \\ &= (p^n \bmod p^{m+1}) \cdot \left(\sum_{k=0}^{m} a_k p^k \bmod p^{m+1} \right) \\ &= \sum_{k=0}^{m} a_k p^{k+n} \bmod p^{m+1} \\ &= \sum_{k=n}^{m+n} a_{k-n} p^k \bmod p^{m+1} \\ &= \sum_{k=n}^{m+n} b_k p^k \bmod p^{m+1} \\ &= \sum_{k=0}^{m} b_k p^k \bmod p^{m+1} \end{aligned}$$

である． □

命題 1.3 ([斎藤, page 131, 補題 7.6] 参照)**.** p 進整数 $x = \sum_{k=0}^{\infty} a_k p^k$ $(0 \leq a_k \leq p-1)$ に対し以下は同値：

(1) $x \bmod p^n = 0 \in \mathbb{Z}/p^n\mathbb{Z}$;

(2) $a_0 = a_1 = \cdots = a_{n-1} = 0$;

(3) ある $y \in \mathbb{Z}_p$ が存在し $x = p^n y$ とかける．

証明. (1) $\Rightarrow$ (2) $\displaystyle\sum_{k=0}^{n-1} a_k p^k \equiv 0 \pmod{p^n}$ である．

$$0 \leq \sum_{k=0}^{n-1} a_k p^k \leq \sum_{k=0}^{n-1} (p-1)p^k = p^n - 1 < p^n$$

であるから $\displaystyle\sum_{k=0}^{n-1} a_k p^k = 0$，すなわち $a_k = 0$ $(0 \leq k \leq n-1)$ となる．

(2) $\Rightarrow$ (3) $y = \displaystyle\sum_{k=0}^{\infty} a_{k+n} p^k \in \mathbb{Z}_p$ とおけば $x = p^n y$ である．

(3) $\Rightarrow$ (1) p 進整数環 $\mathbb{Z}_p$ の定義から成り立つ． □

命題 1.4 ([斎藤, page 131, 補題 7.7] 参照)**.** $x \in \mathbb{Z}_p$ に対し，次は同値：

(1) $x \in \mathbb{Z}_p^{\times}$;

(2) $x \bmod p \in (\mathbb{Z}/p\mathbb{Z})^{\times}$;

(3) $x = py$ となる $y \in \mathbb{Z}_p$ が存在しない．

証明. (2) $\Leftrightarrow$ (3)　命題 1.3 より成り立つ．

(1) $\Rightarrow$ (2)　$x = (x_n)_{n\geq 0}$ とする．$y = (y_n)_{n\geq 0} \in \mathbb{Z}_p^{\times}$ が存在して $xy = 1 \in \mathbb{Z}_p$ とできる．このとき $x_0 y_0 = 1 \in \mathbb{Z}/p\mathbb{Z}$ である．よって $x \bmod p = x_0 \in (\mathbb{Z}/p\mathbb{Z})^{\times}$ である．

(2) $\Rightarrow$ (1)　$x = \displaystyle\sum_{k=0}^{\infty} a_k p^k$ を p 進展開とする．$x \bmod p = a_0 \bmod p \in (\mathbb{Z}/p\mathbb{Z})^{\times}$ なので，$b \in \mathbb{Z}$ が存在して $(b \bmod p)(a_0 \bmod p) = 1 \in \mathbb{Z}/p\mathbb{Z}$ とできる．このとき $1 - bx \in \mathbb{Z}_p$ に対し

$$\begin{aligned} 1 - bx \bmod p &= 1 - ba_0 \bmod p \\ &= 0 \in \mathbb{Z}/p\mathbb{Z} \end{aligned}$$

となるので，$z \in \mathbb{Z}_p$ が存在して $1 - px = pz$ とかける．

$$\begin{aligned} xb(1 + pz + \cdots + p^n z^n) &= (1 - pz)(1 + pz + \cdots + p^n z^n) \\ &= 1 - p^{n+1} z^{n+1} \end{aligned}$$

であるから，$y = (y_n)_{n\geq 0} \in \mathbb{Z}_p$ を

$$y_n = b(1 + pz + \cdots + p^n z^n) \bmod p^{n+1} \in \mathbb{Z}/p^{n+1}\mathbb{Z}$$

と定めれば（$\mathbb{Z}_p$ の元となることに注意）

$$\begin{aligned} xy \bmod p^{n+1} &= (x \bmod p^{n+1}) \cdot (b(1 + pz + \cdots + p^n z^n) \bmod p^{n+1}) \\ &= 1 - p^{n+1} z^{n+1} \bmod p^{n+1} \\ &= 1 \in \mathbb{Z}/p^{n+1}\mathbb{Z} \end{aligned}$$

となる．よって $xy = 1$. □

命題 1.5 ([斎藤, page 132, 補題 7.8] 参照)**.** $0 \neq x \in \mathbb{Z}_p$ に対し，非負整数 $n, u \in \mathbb{Z}_p^\times$ が一意的に存在し

$$x = p^n u$$

とかける．

証明. $x \neq 0$ なので $x \bmod p^k = 0$ となる最大の k が存在する．これを n とする．$u \in \mathbb{Z}_p$ が存在して $x = p^n u$ とかけるが，n の定め方から $u = pv$ となる $v \in \mathbb{Z}_p$ は存在しない．したがって $u \in \mathbb{Z}_p^\times$ である．非負整数 m，$v \in \mathbb{Z}_p^\times$ を用いて $x = p^m v$ とも表せたとする．一般性を失うことなく $n \leq m$ と仮定できる．このとき $p^n(u - p^{m-n}v) = 0$ であるから $u = p^{m-n}v$ となる．$u \in \mathbb{Z}_p^\times$ なので $m - n = 0$ であり，$u = v$ でもある． □

$\mathbb{Z}_p$ は整域であるが，$p \notin \mathbb{Z}_p^\times$ なので体ではない．$\mathbb{Z}_p$ の商体を $\mathbb{Q}_p$ とかき ***p* 進数体**という．また $\mathbb{Q}_p$ の元を ***p* 進数**という．

命題 1.6 ([斎藤, page 135, 補題 7.12] 参照)**.** $0 \neq x \in \mathbb{Q}_p$ に対し，$n \in \mathbb{Z}$, $u \in \mathbb{Z}_p^\times$ が一意的に存在し

$$x = p^n u$$

とかける．

1.2 形式的冪級数としての p 進数

p 進整数に対して p 進展開が一意的に与えられたが，逆に形式的な無限級数から p 進整数を構成することができる．この節では，この構成法について主に [ノイキルヒ, 2.1 節] に基づいて述べる．

整数の列 $(a_k)_{k\geq 0}$ $(0 \leq a_k \leq p-1)$ から定まる形式的な無限級数

$$\sum_{k=0}^{\infty} a_k p^k = a_0 + a_1 p + a_2 p^2 + \cdots$$

全体のなす集合には自然に和と積が定まり，この和と積によって整域となる．形式的な無限級数 $\sum_{k=0}^{\infty} a_k p^k$ に p 進整数 $x = \sum_{k=0}^{\infty} a_k p^k \in \mathbb{Z}_p$ を対応させる写像は，環の同型写像である．

$m \in \mathbb{Z}$ と整数 $0 \leq a_k \leq p-1$ に対し, 形式的な冪級数

$$\sum_{k=-m}^{\infty} a_k p^k = a_{-m}p^{-m} + \cdots + a_{-1}p^{-1} + a_0 + a_1 p + \cdots$$

全体のなす集合には自然に和と積が定まり，この和と積によって体となる．形式的な冪級数 $\sum_{k=-m}^{\infty} a_k p^k$ に p 進数 $x = p^{-1}\sum_{k=0}^{\infty} a_{k-m} p^k \in \mathbb{Q}_p$ を対応させる写像は，体の同型写像である．

1.3 p 進完備化としての p 進数体

有理数体 $\mathbb{Q}$ にはユークリッド距離が定まり，その完備化が実数体 $\mathbb{R}$ だった．$\mathbb{Q}$ 上には他に p 進距離が定まり，その完備化によって p 進数体 $\mathbb{Q}_p$ を定めることができる．この節では，このことについて主に [ノイキルヒ, 2.2 節] に基づいて述べる．

有理数 $x \neq 0$ に対し，$x = p^a \dfrac{n}{m}$（m, n は p で割れない有理整数）という形に表したとき，$v_p(x)$ を a で定める．また $v_p(0) = \infty$ と定めると関数

$$v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$$

が得られる．v_p を ***p* 進指数付値**という．v_p に対し

(1) $v_p(x) = \infty \Leftrightarrow x = 0$,
(2) $v_p(xy) = v_p(x) + v_p(y)$,
(3) $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$

が成り立つ．ただし $x \in \mathbb{Z}$ に対し $x + \infty = \infty$, $\infty + \infty = \infty$, $x < \infty$ とする．また，関数

$$|\quad|_p : \mathbb{Q} \longrightarrow \mathbb{R},\ x \longmapsto |x|_p = p^{-v_p(x)}$$

を ***p* 進絶対値**という．ただし $p^{-\infty} = 0$ とする．$|\quad|_p$ に対し

(1) $|x|_p = 0 \Leftrightarrow x = 0$,
(2) $|xy|_p = |x|_p |y|_p$,

(3) $|x+y|_p \leq \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$

が成り立つ．$x, y \in \mathbb{Q}$ に対し $d(x,y) = |x-y|_p$ と定めると，これは $\mathbb{Q}$ 上の距離となり，この距離を $\mathbb{Q}$ の $\boldsymbol{p}$ **進距離**という．$\mathbb{Q}_p$ は $\mathbb{Q}$ の p 進距離による完備化であり，$\mathbb{Z}_p$ は $\mathbb{Z}$ の p 進距離による完備化である．また，$\mathbb{Q}_p$ の元は $x - y = p^n u$ $(n \in \mathbb{Z},\, u \in \mathbb{Z}_p^{\times})$ と一意的に表せたが，このとき x と y の距離は $|x-y|_p = p^{-n}$ である．

2 $\mathbb{Z}_p$ 拡大

ガロア群が p 進整数環 $\mathbb{Z}_p$ の加法群に位相同型なガロア拡大を $\mathbb{Z}_{\boldsymbol{p}}$ **拡大**という．2 章では群論からの準備を通して，基本的な $\mathbb{Z}_p$ 拡大である円分 $\mathbb{Z}_p$ 拡大の定義を与える．主に 2.1 節の内容は [星]，[雪江 1] に，2.2 節の内容は Washington [Was]，[福田 2]，[雪江 2]，[青木] に基づいている．

2.1 群論からの準備

この節では，$\mathbb{Z}_p$ 拡大を導入するための準備として，群論の命題について述べる．この節の内容は主に [星, 9.4 節]，[雪江 1, 4.2 節] に基づいている．

命題 2.1 ([星, page 128, 定理 9.43], [雪江 1, page 175, 命題 4.2.2] 参照)**.**

(1) p を奇素数とし，$n > 0$ とする．このとき $(\mathbb{Z}/p^n\mathbb{Z})^\times$ は巡回群である．
(2) $n \geq 3$ とする．このとき $(\mathbb{Z}/2^n\mathbb{Z})^\times = \langle\overline{-1}\rangle \times \langle\overline{5}\rangle \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{n-2}\mathbb{Z}$ である．

証明. (1) $n = 1$ のときは有限体 $\mathbb{Z}/p\mathbb{Z}$ の乗法群なのでよい．$n \geq 2$ とする．$(\mathbb{Z}/p^n\mathbb{Z})^\times$ は位数 $\varphi(p^n) = p^{n-1}(p-1)$ である．ここで自然な準同型 $f : (\mathbb{Z}/p^n\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times = \langle g\rangle$ を考えると $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ の位数は $p-1$ なので，$(\mathbb{Z}/p^n\mathbb{Z})^\times$ にも位数 $p-1$ の元 x が存在する．次に $\overline{p+1} \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ の位数が p^{n-1} であることを示す．$k \geq 1$ に対し，$(p+1)^{p^{k-1}} \equiv 1 \pmod{p^k}$ かつ $(p+1)^{p^{k-1}} \not\equiv 1 \pmod{p^{k+1}}$ を示せばよい．$k = 1$ のときはよい．ある $k \geq 1$ で成り立つとすると $(p+1)^{p^{k-1}} = 1 + a_k p^k$, $\gcd(a_k, p) = 1$ とかけ，

$$\begin{aligned}(p+1)^{p^{k+1}} &= (1 + a_k p^k)^p \\ &= 1 + p \cdot a_k p^k + \binom{p}{2}(a_k p^k)^2 + \cdots + (a_k p^k)^p \\ &\begin{cases}\equiv 1 \pmod{p^{k+1}}, \\ \not\equiv 1 \pmod{p^{k+2}}.\end{cases}\end{aligned}$$

よって $k+1$ のときにも成り立つ．$\gcd(p^{n-1}, p-1) = 1$ なので $\overline{p-1} \cdot x \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ の位数は $p^{n-1}(p-1)$ である．よって $(\mathbb{Z}/p^n\mathbb{Z})^\times = \langle\overline{p-1} \cdot x\rangle$.

(2) まず $\overline{5} \in (\mathbb{Z}/2^n\mathbb{Z})^\times$ の位数は 2^{n-2} であることを示す．$k \geq 2$ に対し，$5^{2^{k-2}} \equiv 1 \pmod{2^k}$ かつ $5^{2^{k-2}} \not\equiv 1 \pmod{2^k+1}$ を示せばよい．$k = 2$ のときはよい．ある $k \geq 2$

で成り立つとすると $5^{2^{k-2}} = 1 + b_k 2^k$, $\gcd(b_k, 2) = 1$ とかけ，

$$5^{2^{k-1}} = (1 + b_k 2^k)^2 = 1 + 2 \cdot b_k 2^k + (b_k 2^k)^2$$
$$\begin{cases} \equiv 1 \pmod{2^{k+1}}, \\ \not\equiv 1 \pmod{2^{k+2}}. \end{cases}$$

よって $k+1$ のときにも成り立つ．ここで $(\mathbb{Z}/2^n\mathbb{Z})^\times$ の部分群を $H_n = \{\overline{4m+1} \mid m \in \mathbb{Z}\}$ で定義すると，$(\mathbb{Z}/2^n\mathbb{Z})^\times$ の元は $\overline{4m+1}$ か $\overline{4m+3} = \overline{-(4m'+1)}$ と表せるので，

$$\begin{aligned} (\mathbb{Z}/2^n\mathbb{Z})^\times &= \langle \overline{-1} \rangle \times H_n \\ &= \langle \overline{-1} \rangle \times \langle \overline{5} \rangle \\ &\simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{n-2}\mathbb{Z}. \end{aligned}$$

□

注意 2.2. 命題 2.1 により，奇素数 p に対しては，$(\mathbb{Z}/p^n\mathbb{Z})^\times \simeq \mathbb{Z}/\varphi(p^n)\mathbb{Z} \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/p^{n-1}\mathbb{Z})$ となる．一方で $p = 2$ に対しては，$\mathbb{Z}/2\mathbb{Z} \simeq (\mathbb{Z}/4\mathbb{Z})^\times$ であるから，$(\mathbb{Z}/2^n\mathbb{Z})^\times \simeq (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/2^{n-2}\mathbb{Z})$ となる．

2.2 円分 $\mathbb{Z}_p$ 拡大

この節では，前節の内容を用いて円分 $\mathbb{Z}_p$ 拡大を構成する．この節の内容は主に Washington [Was, page 128]，[福田 2, 5.1 節]，[雪江 2, 6.3 節] や [青木, 6.2 節] に基づいている．

p を素数とし，

$$q = \begin{cases} p & p \text{ が奇素数}, \\ 4 & p = 2 \end{cases}$$

とおく．このとき，注意 2.2 から

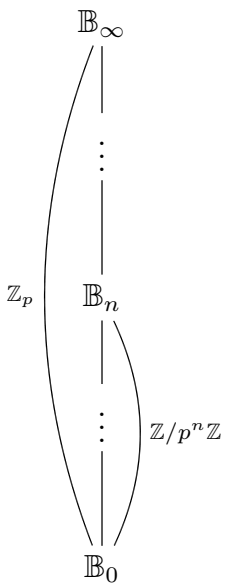
$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\zeta_{qp^n})/\mathbb{Q}) &\simeq (\mathbb{Z}/qp^n\mathbb{Z})^\times \\ &\simeq (\mathbb{Z}/q\mathbb{Z})^\times \times (\mathbb{Z}/p^n\mathbb{Z}) \end{aligned}$$

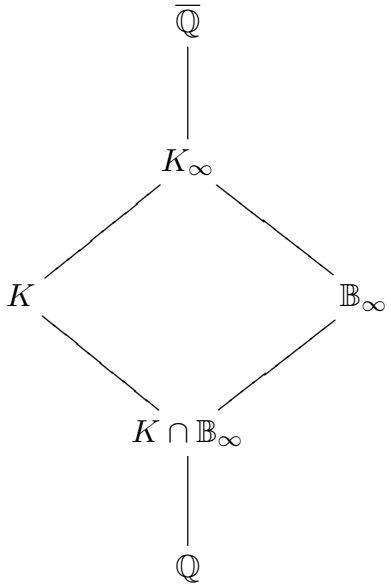
とできる．$\mathbb{B}_n := \mathbb{Q}(\zeta_{qp^n})^{(\mathbb{Z}/q\mathbb{Z})^\times}$ とおくと $\mathrm{Gal}(\mathbb{B}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$ である．$\mathbb{B}_\infty :=$

$\bigcup_{n=0}^{\infty} \mathbb{B}_n$, $\mathbb{B}_0 := \mathbb{Q}$ とおくと

$$\begin{aligned} \mathrm{Gal}(\mathbb{B}_\infty/\mathbb{Q}) &\simeq \varprojlim \mathrm{Gal}(\mathbb{B}_n/\mathbb{Q}) \\ &\simeq \varprojlim \mathbb{Z}/p^n\mathbb{Z} \\ &\simeq \mathbb{Z}_p \end{aligned}$$

となり，$\mathbb{B}_\infty/\mathbb{Q}$ は $\mathbb{Z}_p$ 拡大である．





K を有限次代数体とし，$K_\infty = K\mathbb{B}_\infty$ とする．このとき，

$$\begin{aligned} \mathrm{Gal}(K_\infty/K) &\simeq \mathrm{Gal}(\mathbb{B}_\infty/K \cap \mathbb{B}_\infty) \\ &\simeq p^e\mathbb{Z}_p \\ &\simeq \mathbb{Z}_p \end{aligned}$$

となる．Galois 拡大 K_∞/K を K の**円分 $\mathbb{Z}_p$ 拡大**という．

例 2.3. p が奇素数のときは，$\mathrm{Gal}(\mathbb{Q}(\zeta_{qp^n})/\mathbb{Q}) \simeq (\mathbb{Z}/qp^n\mathbb{Z})^\times$ は巡回群であったので，$\mathbb{B}_n$ は $\mathbb{Q}$ 上 p^n 次の中間体として一意的に定まる．

$p = 2$ のときは，奇素数のときとは異なり，$\mathbb{B}_n$ は $\mathbb{Q}$ 上 p^n 次の中間体として一意的には定まらない．$(\mathbb{Z}/q\mathbb{Z})^\times = \langle\overline{-1}\rangle$ であったことに注意すると，$\overline{-1}$ は $\mathrm{Gal}(\mathbb{Q}(\zeta_{qp^n})/\mathbb{Q})$ の元 $\sigma : \zeta_{qp^n} \mapsto \zeta_{qp^n}^{-1}$ に対応するので

$$\begin{aligned} \mathbb{B}_n &= \mathbb{Q}(\zeta_{qp^n})^{\langle\sigma\rangle} \\ &= \mathbb{Q}(\zeta_{qp^n} + \zeta_{qp^n}^{-1}) = \mathbb{Q}(\zeta_{qp^n}) \cap \mathbb{R} \end{aligned}$$

となる.

3 岩澤代数

3 章では岩澤理論において重要な概念である形式的冪級数環 $\Lambda = \mathcal{O}[[T]]$ について述べる．基本的な性質等について述べた後，Λ がある完備群環と同型であることを示す．主に 3 章の内容は [伊藤]，[福田 2]，Washington [Was]，[市村] に基づいている．

3.1 形式的冪級数環

この節では，Λ を導入し，Λ に関することについて述べていく．この節の内容は主に [伊藤]，[福田 2, 4.1 節]，Washington [Was] に基づいている．

$k/\mathbb{Q}_p$ を有限次拡大，$\mathcal{O}$ を k の整数環，$\mathfrak{p} = (\pi)$ を $\mathcal{O}$ の唯一の極大イデアルとする．($k = \mathbb{Q}_p$ とすれば $\mathcal{O} = \mathbb{Z}_p$, $\mathfrak{p} = (p)$ となる．)

定義 3.1 ([伊藤, page 8, 定義], [福田 2, page 25] 参照)**.** $P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0 \in \mathcal{O}[T]$ とする．$a_i \in \mathfrak{p}$ $(0 \leq i \leq n-1)$ が成り立つとき $P(T)$ を **distinguished 多項式**という．

一変数形式的冪級数環 $\mathcal{O}[[T]]$ を Λ で表す．

定理 3.2 (p-adic Weierstrass Preparation Theorem, [Was, page 115, Theorem 7.3], [伊藤, pages 8–9, Weierstrass の準備定理] 参照)**.** $f(T) = \sum_{i=1}^{\infty} a_i T^i \in \Lambda$ が $a_i \in \mathfrak{p}$ $(0 \leq i \leq n-1)$，$a_n \notin \mathfrak{p}$ を満たすとする．このとき

$$f(T) = P(T)U(T)$$

を満たす n 次 distinguished 多項式 $P(T)$ と $U(T) \in \Lambda^\times$ が一意的に存在する．

より一般に，$0 \neq f(T) \in \Lambda$ に対し

$$f(T) = \pi^\mu P(T)U(T)$$

を満たす distinguished 多項式 $P(T)$ と $U(T) \in \Lambda^\times$，非負整数 μ が一意的に存在する．

定理 3.2 の μ を $\boldsymbol{f(T)}$ **の** $\boldsymbol{\mu}$ **不変量**，$\deg f(T)$ を $\boldsymbol{f(T)}$ **の** $\boldsymbol{\lambda}$ **不変量**といい，それぞれ $\mu(f(T))$, $\lambda(f(T))$ で表す．また $P(T)$ を $\boldsymbol{f(T)}$ **に付随する多項式**という．

命題 3.3 ([Was, page 114, Proposition 7.2] 参照)．$f(T)$, $g(T) \in \Lambda$ とし，$f(T) = \sum_{i=0}^{\infty} a_i T^i$ は $a_i \in \mathfrak{p}$ $(0 \leq i \leq n-1)$, $a_n \notin \mathfrak{p}$ を満たすとする．このとき

$$g(T) = q(T)f(T) + r(T)$$

を満たす $q(T) \in \Lambda$ と $\deg r(T) < n$ である多項式 $r(T) \in \mathcal{O}[T]$ が一意的に存在する．

$0 \neq f(T) \in \Lambda$ は $f(T) = \pi^{\mu} P(T)U(T)$ と一意的に表せた．ここで $P(T) = f_1(T)f_2(T)$ であるとすると，分解の一意性から $\mu(P(T)) = \mu(f_1(T)) = \mu(f_2(T)) = 0$ である．したがって $f_i(T) = P_i(T)U_i(T)$ $(i = 1, 2)$ と分解でき $f(T) = \pi^{\mu} P(T)U(T) = \pi^{\mu} P_1(T)P_2(T)U_1(T)U_2(T)U(T)$ となる．分解の一意性から $P(T) = P_1(T)P_2(T)$ となるので，この操作を繰り返せば，既約かつ distinguished な多項式 $P_i(T)$ によって $f(T) = \pi^{\mu}\big(\prod P_i(T)\big)U(T)$ と表せる．したがって Λ は UFD である（[市村, 10.1 節] 参照)．

命題 3.4 ([伊藤, page 11, 命題 1.4] 参照)．Λ の素イデアルは $(0), (\pi), (P(T)), (\pi, T)$ である．ただし $P(T)$ は既約かつ distinguished な多項式である．また，(π, T) は Λ の唯一の極大イデアルである．

定義 3.5 ([伊藤, page 13, 定義] 参照)．M, M' を有限生成 Λ 加群とする．このとき Λ 準同型 $\varphi\colon M \to M'$ が擬同型であるとは，$\mathrm{Ker}\ \varphi$ と $\mathrm{Coker}\ \varphi$ が有限であるときをいう．

定理 3.6 ([伊藤, page 14, 有限生成 Λ 加群の構造定理] 参照)．M を有限生成 Λ 加群とする．このとき擬同型

$$M \longrightarrow \Lambda^{\oplus r} \oplus \Big(\bigoplus_{i=1}^{s} \Lambda/(\pi^{n_i})\Big) \oplus \Big(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j})\Big)$$

が存在する．ただし r, s, t, n_i, m_j は非負整数，$f_j(T)$ は既約かつ distinguished な多項式である．また，右辺は順序を除いて一意的に定まる．

定義 3.7 ([伊藤, page 14, 定義] 参照)．M を有限生成ねじれ Λ 加群とすると，擬同型

$$M \longrightarrow \Big(\bigoplus_{i=1}^{s} \Lambda/(\pi^{n_i})\Big) \oplus \Big(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j})\Big)$$

が存在する．このとき

$$\mathrm{char}_{\Lambda}(M) := \prod_{i=1}^{s} \pi^{n_i} \prod_{j=1}^{t} f_j(T)^{m_j}$$

を $\boldsymbol{M}$ の特性多項式といい，

$$(\mathrm{char}_\Lambda(M)) := \prod_{i=1}^{s}(\pi^{n_i})\prod_{j=1}^{t}(f_j(T)^{m_j})$$

を $\boldsymbol{M}$ の特性イデアルという．

定義 3.8 ([伊藤, page 15, 定義] 参照)．M を有限生成ねじれ Λ 加群とする．$\mathrm{char}_\Lambda(M) = \pi^\mu f(T)$ と書いたとき，μ を $\boldsymbol{M}$ の $\boldsymbol{\mu}$ 不変量，$\deg f(T)$ を $\boldsymbol{M}$ の $\boldsymbol{\lambda}$ 不変量といい，それぞれ $\mu(M)$, $\lambda(M)$ で表す．

$m \geq n \geq 0$ に対し

$$\begin{aligned}
\omega_n(T) &= (1+T)^{p^n} - 1 \\
&= \begin{cases} \left((1+T)^{p^n-p} + (1+T)^{p^n-2p} + \cdots + (1+T)^p + 1\right)\left((1+T)^p - 1\right) & (n \geq 1), \\ T & (n = 0), \end{cases} \\
\nu_{m,n}(T) &= \omega_m(T)/\omega_n(T) \\
&= \begin{cases} \dfrac{(1+T)^{p^m-p} + \cdots + (1+T)^{p^n-p} + \cdots + (1+T)^p + 1}{(1+T)^{p^n-p} + \cdots + (1+T)^p + 1} & (n \geq 1), \\ \omega_m(T)/T = \dfrac{(1+T)^{p^m} - 1}{(1+T) - 1} & (n = 0) \end{cases} \\
&= \sum_{i=0}^{\frac{p^m-p^n}{p^n}} (1+T)^{ip^n} \\
&= 1 + (1+T)^{p^n} + (1+T)^{2p^n} + \cdots + (1+T)^{(p^{m-n}-1)p^n}, \\
\nu_n(T) &= \nu_{n,0}(T) = \omega_n(T)/T
\end{aligned}$$

とする．

補題 3.9 ([藤井, page 32, 補題 2.1] 参照)．$\omega_n(T), \nu_{m,n}(T)$ は distinguished 多項式であり，

$$\omega_n(T) \in (\pi, T)^{n+1},\ \nu_{m,n}(T) \in (\pi, T)^{m-n}$$

である．

証明. $\mathcal{O}[T]$ において

$$\begin{aligned}
\omega_n(T) = (1+T)^{p^n} - 1 \equiv 1 + T^{p^n} - 1 = T^{p^n} \pmod{p}, \\
\nu_{m,n}(T) = \omega_m(T)/\omega_n(T) \equiv T^{p^m}/T^{p^n} = T^{p^n-m} \pmod{p}
\end{aligned}$$

であるから $\omega_n(T), \nu_{m,n}(T)$ は distinguished 多項式である．よって $\nu_{m,n}(T) \in (p,T)$，特に $\nu_1(T) \in (p,T)$ である．$\nu_n(T) \in (p,T)^n$ であると仮定すると，$\nu_{n+1}(T) = \nu_{n+1,n}(T)\nu_n(T) \in (p,T)^{n+1}$ である．帰納法により任意の n に対し $\nu_n(T) \in (p,T)^n$ である．以上より

$$\begin{aligned}\omega_n(T) &= T\nu_n(T) \in (p,T)^{n+1},\\ \nu_{m,n}(T) &= \nu_{m,m-1}(T)\nu_{m-1,m-2}(T)\cdots\nu_{n+2,n+1}(T)\nu_{n+1,n}(T) \in (p,T)^{m-n}\end{aligned}$$

である． □

補題 3.10 ([福田 2, page 23, 補題 4.1] 参照)**.** $\mathcal{O}[[T]]$ のイデアル (π,T) に対し，

$$\bigcap_{n=0}^{\infty}(\pi,T)^n = \{0\}$$

である．

証明. 任意の $0 \neq f(T) \in \mathcal{O}[[T]]$ に対し $f(T) \notin (\pi,T)^n$ となる n が存在することをいえばよい．

$$(\pi,T)^n = (\pi^n, \pi^{n-1}T, \pi^{n-2}T^2, \ldots, T^n)$$

であるから $(\pi,T)^{m+n} \subset (\pi^m, T^n)$ である．$\mathcal{O}$ の 0 でない元は $u\pi^m$ $(u \in \mathcal{O}^\times)$ と一意的に表せるので

$$f(T) = \pi^m T^n + a_{n+1}T^{n+1} + \cdots$$

と表せる．$u\pi^m T^n \notin (\pi^{m+1}, T^{n+1})$ であるから $f(T) \notin (\pi^{m+1}, T^{n+1})$ である．したがって，このような m,n に対して $f(T) \notin (\pi,T)^{m+n+2}$ である． □

この補題より $\mathcal{O}[[T]]$ には (π,T) 進距離が定義され，この距離に関し $\mathcal{O}[[T]]$ は完備である（[伊藤, page 6] 参照)．

3.2 完備群環

この節では，完備群環，特に岩澤代数を導入し，Λ との間の同型を示す．この節の内容は主に [伊藤]，[福田 2, 4.2 節]，Washington [Was, 7.1 節] に基づいている．

定義 3.11 ([黒川/栗原/斎藤, page 493] 参照)**.** R を可換環とする．G を profinite 群，すなわち有限群の逆系の逆極限 $G = \varprojlim G_i$ とする．このとき $R[[G]] = \varprojlim R[G_i]$ を $\boldsymbol{G}$ の $\boldsymbol{R}$ **上の完備群環**という．

定義 3.12 ([落合, page 21, 定義 2.8] 参照)**.** Γ を $\mathbb{Z}_p$ と位相同型な乗法群とし, $\Gamma_n = \Gamma/\Gamma^{p^n}$ とおく．このとき，完備群環 $\mathcal{O}[[\Gamma]] = \varprojlim \mathcal{O}[\Gamma_n]$ を**岩澤代数**という．

Γ を $\mathbb{Z}_p$ と位相同型な乗法群とし，γ を Γ の位相的生成元，すなわち $\langle\gamma\rangle \subset \Gamma$ が稠密となる元であるとする．

定理 3.13 (Serre [Ser, page 89, Lemme 3], [伊藤, page 9, 定理 1.3], [Was, page 114, Theorem 7.1] 参照)**.** 対応 $\gamma \leftrightarrow 1+T$ によって

$$\mathcal{O}[[\Gamma]] \simeq \mathcal{O}[[T]]$$

である．

証明. $\gamma \bmod \Gamma^{p^n}$ に $1+T \bmod \omega_n(T)$ を対応させる写像により

$$\mathcal{O}[\Gamma/\Gamma^{p^n}] \simeq \mathcal{O}[T]/(\omega_n(T))$$

である．実際 $\mathcal{O}[T]/(\omega_n(T))$ の元は $\displaystyle\sum_{0\le i\le p^{n-1}} a_i(1+T)^i \bmod \omega_n$ と一意的に表せるので全射性と単射性がいえる．$m > n$ に対し $\omega_n(T) \mid \omega_m(T)$ なので，自然な準同型

$$\mathcal{O}[T]/(\omega_m(T)) \longrightarrow \mathcal{O}[T]/(\omega_n(T))$$

が定義でき，図式

$$\begin{array}{ccc} \mathcal{O}[\Gamma/\Gamma^{p^m}] & \longrightarrow & \mathcal{O}[T]/(\omega_m(T)) \\ \downarrow & & \downarrow \\ \mathcal{O}[\Gamma/\Gamma^{p^n}] & \longrightarrow & \mathcal{O}[T]/(\omega_n(T)) \end{array}$$

は可換である．

$f(T) \in \mathcal{O}[[T]]$ に対し

$$f(T) = q_n(T)\omega_n(T) + f_n(T) \quad (q_n(T) \in \mathcal{O}[[T]],\ f_n(T) \in \mathcal{O}[T])$$

と表せる．このとき $(\overline{f_0(T)}, \overline{f_1(T)}, \ldots)$ は $\varprojlim \mathcal{O}[T]/(\omega_n(T))$ の元である．$f(T)$ に $(\overline{f_0(T)}, \overline{f_1(T)}, \ldots)$ を対応させる写像により

$$\mathcal{O}[[T]] \simeq \varprojlim \mathcal{O}[T]/(\omega_n(T))$$

である．まず単射性を示す．$f(T)$ をこの準同型の核からとると，各 n に対し $f_n(T) = 0$ である．したがって $f(T)$ はすべての $\omega_n(T)$ で割り切れる．一方で $\omega_n(T) \in (\pi, T)^{n+1}$

であるから

$$\bigcap_{n=0}^{\infty}(\omega_n(T)) \subset \bigcap_{n=0}^{\infty}(\pi,T)^{n+1} = \{0\}$$

となり $f(T) = 0$ である．次に全射性を示す．任意に $(\overline{g_0(T)}, \overline{g_1(T)}, \ldots) \in \varprojlim \mathcal{O}[T]/(\omega_n(T))$ をとると，逆極限の定義から $m \geq n$ に対し

$$g_m(T) \equiv g_n(T) \pmod{\omega_n(T)}$$

である．$\omega_n(T) \in (\pi,T)^{n+1}$ なので $(g_n(T))_{n\geq 0}$ は $\mathcal{O}[[T]]$ のコーシー列である．$\mathcal{O}[[T]]$ は (π,T) 進距離で完備なので，極限 $f(T) = \lim g_n(T)$ が存在する．

$$g_m(T) - g_n(T) = h_{m,n}(T)\omega_n(T) \quad (h_{m,n}(T) \in \mathcal{O}[T])$$

と表せるので $h_{m,n}(T) = \dfrac{g_m(T) - g_n(T)}{\omega_n(T)}$ は $\mathcal{O}[[T]]$ におけるコーシー列であり $m \to \infty$ とすると $\lim_{m\to\infty} h_{m,n} \in \mathcal{O}[[T]]$ である．したがって

$$f(T) - g_n(T) = \lim_{m\to\infty}(g_m(T) - g_n(T)) = \lim_{m\to\infty} h_{m,n}(T)\omega_n(T) \in (\omega_n(T))$$

となる．

$$f_n(T) - g_n(T) = (f_n(T) - f(T)) + (f(T) - g_n(T)) \in (\omega_n(T))$$

であるから $(\overline{f_0(T)}, \overline{f_1(T)}, \ldots) = (\overline{g_0(T)}, \overline{g_1(T)}, \ldots)$ である．

図式の左右の逆極限をとることで

$$\varprojlim \mathcal{O}[\Gamma/\Gamma^{p^n}] \simeq \varprojlim \mathcal{O}[T]/(\omega_n(T))$$

となり，$\gamma = (\overline{\gamma}, \overline{\gamma}, \ldots) \in \varprojlim \mathcal{O}[\Gamma/\Gamma^{p^n}]$ は $(\overline{1+T}, \overline{1+T}, \ldots) \in \varprojlim \mathcal{O}[T]/(\omega_n(T))$ に対応する． □

4　岩澤類数公式

4 章では岩澤類数公式について述べる．4 章の内容は主に [福田 2]，[藤井]，Washington [Was] に基づいている．4 章においては $\Lambda = \mathbb{Z}_p[[T]]$ とする．

4.1　岩澤加群

この節では，イデアル類群の p 部分から構成される岩澤加群と，ガロア群の p 部分から構成される対象との間の同型を示す．この節の内容は主に [藤井]，[福田 2, 5 章]，Washington [Was, 13.1 節，13.3 節] に基づいている．

p を素数とする．k を有限次代数体，k_∞/k を $\mathbb{Z}_p$ 拡大とし，$\Gamma = \mathrm{Gal}(k_\infty/k)$ とする．また，k_n を $\boldsymbol{k_\infty/k}$ **の** $\boldsymbol{n}$**-th layer**，すなわち k 上 p^n 次の中間体とし，$\Gamma_n = \mathrm{Gal}(k_n/k)$ とする．

命題 4.1 ([藤井, page 28, 命題 2.1] 参照)**.** k_∞/k は p の外不分岐拡大である．

命題 4.2 ([藤井, page 28, 命題 2.1] 参照)**.** k_∞/k で分岐する素点が存在する．さらに非負整数 e が存在し，k_∞/k_e で分岐する任意の素点は完全分岐する．

以降，定理 4.17 を証明するまでは，次を仮定する．

仮定（[藤井, page 29, 仮定] 参照）

k_∞/k で分岐する任意の素点は完全分岐する．

注意 4.3. 命題 4.2 から，k_∞/k_e が仮定を満たすような非負整数 e が存在する．k_∞/k_e は $\mathbb{Z}_p$ 拡大であるので，必要に応じて k を k_e にとりかえる．

A_n を k_n のイデアル類群 $Cl(k_n)$ の p 部分とする．

注意 4.4. A_n の位数は p 冪であり，$\mathbb{Z}_p$ の元は p 進展開により $\displaystyle\sum_{n=0}^{\infty} a_n p^n$ の形に表せたので，A_n は自然に $\mathbb{Z}_p$ 上の加群とみなせる．これはまた次のように言い表すこともできる．すなわち，アーベル群 A_n は $\mathbb{Z}$ 加群とみなせるので，準同型 $\mathbb{Z} \to \mathrm{End}(A_n)$ が定まる．

A_n の位数を p^e とすると，$\mathbb{Z}_p$ の元 $\sum_{n=0}^{\infty} a_n p^n$ による作用は実質的に有理整数 $\sum_{n=0}^{e} a_n p^n$ による作用と同じである．このことから，上で述べた $\mathbb{Z}_p$ の作用は，準同型の合成

$$\mathbb{Z}_p \longrightarrow \mathbb{Z}/p^e\mathbb{Z} \longrightarrow \mathrm{End}(A_n)$$

が定める $\mathbb{Z}_p$ の A_n への作用と一致する．

定義 4.5 ([藤井, page 29, 定義 2.1] 参照)**.** $m \geq n \geq 0$ に対し，ノルム写像を

$$N_{m,n} : A_m \longrightarrow A_n \ ; \ \overline{\mathfrak{a}} \longmapsto \overline{N_{k_m/k_n}\mathfrak{a}}$$

で定める．逆系 $(A_n, N_{m,n})$ の逆極限

$$X_{k_\infty} = \varprojlim A_n$$

を **k_∞/k の岩澤加群**という．

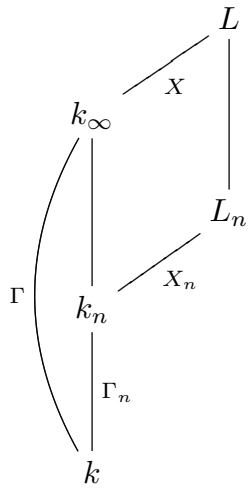
A_n には $\Gamma_n = \mathrm{Gal}(k_n/k)$ と $\mathbb{Z}_p$ が作用するので，$\mathbb{Z}_p[\Gamma_n]$ 加群となる．よって逆極限 X_{k_∞} は $\mathbb{Z}_p[[\Gamma]]$ 加群となる．

L_n を k_n の最大不分岐 Abel p 拡大とし，$X_n = \mathrm{Gal}(L_n/k_n)$ とする．

命題 4.6 ([藤井, pages 29–30, 命題 2.2] 参照)**.** L_n/k は Galois 拡大である．

証明. $\sigma : L_n \to \overline{\mathbb{Q}}$ を単射 k 準同型とする．k_n/k は Galois 拡大なので $\sigma(k_n) = k_n$ であり L_n の定め方から $\sigma(L_n) = L_n$ である．よって L_n/k は Galois 拡大である． □

$L = \bigcup_{n\geq 0} L_n$ とする．L_n/k は Galois 拡大なので L/k も Galois 拡大である．また，$k_n \subset L_n$ で $k_\infty = \bigcup_{n=0}^{\infty} k_n$ であるから $k \subset k_\infty \subset L$ であり，L/k_∞ は Galois 拡大である．$X = \mathrm{Gal}(L/k_\infty)$ とする．



命題 4.7 ([藤井, pages 29–30, 命題 2.2] 参照)**.** $x \in X_n$，$\sigma \in \Gamma_n$ とし，$\widetilde{\sigma} \in \mathrm{Gal}(L_n/k)$ を σ の任意の延長とする．このとき

$$\sigma \cdot x = \widetilde{\sigma} x \widetilde{\sigma}^{-1}$$

により Γ_n は X_n に作用する．

証明. σ の x への作用が延長の取り方に依らないことを示せばよい．$\widetilde{\sigma}_1$, $\widetilde{\sigma}_2$ を σ の延長とすれば，$\widetilde{\sigma}_2^{-1}\widetilde{\sigma}_1 \in \mathrm{Gal}(L_n/k_n) = X_n$ であるから，$\widetilde{\sigma}_1 x \widetilde{\sigma}_1^{-1} = \widetilde{\sigma}_2(\widetilde{\sigma}_2^{-1}\widetilde{\sigma}_1)x(\widetilde{\sigma}_2^{-1}\widetilde{\sigma}_1)^{-1}\widetilde{\sigma}_2^{-1} = \widetilde{\sigma}_2 x \widetilde{\sigma}_2^{-1}$ である． □

X_n には Γ_n と $\mathbb{Z}_p$ が作用するので，$\mathbb{Z}_p[\Gamma_n]$ 加群となる．

命題 4.8 ([藤井, page 29, 命題 2.2] 参照)**.** Artin 写像

$$A_n \longrightarrow X_n \ ; \ \overline{\mathfrak{a}} \longmapsto \left(\frac{L_n/k_n}{\mathfrak{a}}\right)$$

は $\mathbb{Z}_p[\Gamma_n]$ 加群としての同型である．

証明. $Cl(k_n)$ を k_n のイデアル類群，$\mathcal{L}_n$ を k_n の最大不分岐アーベル拡大とすると，類体論の相互写像により同型

$$Cl(k_n) \simeq \mathrm{Gal}(\mathcal{L}_n/k_n) \ ; \ \overline{\mathfrak{a}} \longleftrightarrow \left(\frac{\mathcal{L}_n/k_n}{\mathfrak{a}}\right)$$

が得られる．ここで A_n' を $Cl(k_n)$ の元で位数が p と素であるもの全体のなす部分群とすると

$$Cl(k_n) = A_n \oplus A_n'$$

となる．また，L'_n を k_n の不分岐アーベル拡大で拡大次数が p と素なもののうち最大のものとすると，

$$\begin{aligned}\mathrm{Gal}(\mathcal{L}_n/k_n) &\simeq \mathrm{Gal}(\mathcal{L}_n/L'_n) \oplus \mathrm{Gal}(\mathcal{L}_n/L_n)\\ &\simeq \mathrm{Gal}(L_n/k_n) \times \mathrm{Gal}(L'_n/k_n)\\ &= X_n \times \mathrm{Gal}(L'_n/k_n)\end{aligned}$$

となる．p 部分を比較することによって，群としての同型

$$A_n \simeq X_n\ ;\ \overline{\mathfrak{a}} \longleftrightarrow \left(\frac{L_n/k_n}{\mathfrak{a}}\right)$$

を得る．

$\mathfrak{p}$ を k_n の素イデアル，$\mathfrak{P}$ を $\mathfrak{p}$ の上にある L_n の素イデアルとする．$\sigma \in \Gamma_n$ とし，$\widetilde{\sigma} \in \mathrm{Gal}(L_n/k)$ を σ の任意の延長とする．このとき

$$\left(\frac{L_n/k_n}{\sigma(\mathfrak{p})}\right) = \left[\frac{L_n/k_n}{\widetilde{\sigma}(\mathfrak{P})}\right] = \widetilde{\sigma}\left[\frac{L_n/k_n}{\mathfrak{P}}\right]\widetilde{\sigma}^{-1} = \widetilde{\sigma}\left(\frac{L_n/k_n}{\mathfrak{p}}\right)\widetilde{\sigma}^{-1}$$

であるから $\mathbb{Z}_p[\Gamma_n]$ 同型である． □

命題 4.9 ([藤井, pages 29–30, 命題 2.2] 参照)．$m \geq n \geq 0$ に対し，$N_{m,n} : A_m \longrightarrow A_n$ をノルム写像， $r_{m,n} : X_m \longrightarrow X_n$, $r_{m,n}(x) = x|_{L_n}$ を Galois 群の制限写像とする．このとき図式

$$\begin{array}{ccc} A_m & \xrightarrow{\left(\frac{L_m/k_m}{*}\right)} & X_m \\ {\scriptstyle N_{m,n}}\downarrow & & \downarrow{\scriptstyle r_{m,n}} \\ A_n & \xrightarrow{\left(\frac{L_n/k_n}{*}\right)} & X_n \end{array}$$

は可換である．

証明. 素イデアルに関して示せば十分である．$\mathfrak{P}$ を k_m の素イデアル，$\mathfrak{p} = \mathfrak{P} \cap k_n$ を $\mathfrak{P}$ の下にある k_n の素イデアルとし，f を $\mathfrak{P}$, $\mathfrak{p}$ に関する相対次数とする．L_n の任意の整数 $\alpha \in \mathcal{O}_{L_n}$ に対し，

$$\left(\frac{L_m/k_m}{\mathfrak{P}}\right)\Bigg|_{L_n}(\alpha) \equiv \alpha^{N\mathfrak{P}} \pmod{\mathfrak{P}}$$

である．両辺とも L_n の元であるから

$$\left(\frac{L_m/k_m}{\mathfrak{P}}\right)\Bigg|_{L_n}(\alpha) \equiv \alpha^{N\mathfrak{P}} \pmod{\mathfrak{p}}$$

とできる．一方で

$$\left(\frac{L_n/k_n}{\mathfrak{p}}\right)(\alpha) \equiv \alpha^{N\mathfrak{p}} \pmod{\mathfrak{p}}$$

であるから

$$\left(\frac{L_m/k_m}{\mathfrak{P}}\right)\Big|_{L_n} = \left(\frac{L_n/k_n}{\mathfrak{p}}\right)^f = \left(\frac{L_n/k_n}{\mathfrak{p}^f}\right) = \left(\frac{L_n/k_n}{N_{m,n}\mathfrak{P}}\right)$$

である． □

命題 4.10 ([藤井, page 30, 定理 2.1] 参照)**.**

(1) $x \in X$, $\sigma \in \Gamma$ とし，$\widetilde{\sigma} \in \mathrm{Gal}(L/k)$ を σ の任意の延長とする．このとき

$$\sigma \cdot x = \widetilde{\sigma} x \widetilde{\sigma}^{-1}$$

により Γ は X に作用する．

(2) X は $\mathbb{Z}_p[[\Gamma]]$ 加群であり，X_{k_∞} と X は $\mathbb{Z}_p[[\Gamma]]$ 加群として同型である．

証明. (1) 先の命題と同様.

(2) 仮定より，$k_\infty \cap L_n = k_n$ となるので，Galois 群の制限写像

$$\mathrm{Gal}(L_n k_\infty/k_\infty) \longrightarrow X_n;\ x \longmapsto x|_{L_n}$$

は同型である．$L = \bigcup_{n=0}^{\infty} L_n k_\infty$ なので $X \simeq \varprojlim \mathrm{Gal}(L_n k_\infty/k_\infty)$ である．$L_n k_\infty/k_\infty$ はアーベル拡大なので，(1) と同様に $\mathrm{Gal}(k_\infty/k_n)$ が $\mathrm{Gal}(L_n k_\infty/k_\infty)$ に作用する．L_n/k_n，k_∞/k_n はアーベル拡大なので $L_n k_\infty/k_n$ はアーベル拡大であり，このことから $\mathrm{Gal}(L_n k_\infty/k_\infty)$ への $\mathrm{Gal}(k_\infty/k_n)$ の作用は自明作用となる．したがって，$\mathrm{Gal}(L_n k_\infty/k_\infty)$ に $\mathrm{Gal}(k_\infty/k)/\mathrm{Gal}(k_\infty/k_n) \simeq \Gamma_n$ が作用し，写像

$$\mathrm{Gal}(L_n k_\infty/k_\infty) \longrightarrow X_n;\ x \longmapsto x|_{L_n}$$

は $\mathbb{Z}_p[\Gamma_n]$ 加群としての同型であり，X は $\mathbb{Z}_p[[\Gamma]]$ 加群となる．可換図式

$$\begin{array}{ccccc} A_m & \xrightarrow{\simeq} & X_m & \xleftarrow{\simeq} & \mathrm{Gal}(L_m k_\infty/k_\infty) \\ \downarrow & & \downarrow & & \downarrow \\ A_n & \xrightarrow{\simeq} & X_n & \xleftarrow{\simeq} & \mathrm{Gal}(L_n k_\infty/k_\infty) \end{array}$$

の左右の逆極限をとり，$\mathbb{Z}_p[[\Gamma]]$ 加群しての同型 $X_{k_\infty} = \varprojlim A_n \simeq \varprojlim \mathrm{Gal}(L_n k_\infty/k_\infty) \simeq X$ を得る． □

4.2 岩澤類数公式とその証明

この節では，これまで述べてきた内容の結論として岩澤類数公式を導く．この節の内容は主に [藤井]，Washington [Was, 13.3 節] に基づいている．

$G = \mathrm{Gal}(L/k)$ とし，Γ の位相的生成元 γ を一つ固定する．$\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_s$ を k_∞/k で分岐する k の素点，$\mathfrak{P}_j$ を $\mathfrak{p}_j$ の上にある L の素点とし，$I_j \leq G$ を L/k における $\mathfrak{P}_j$ の惰性群とする．仮定より k_∞/k で分岐する任意の素点は完全分岐するので，k_∞/k における $\mathfrak{p}_j$ の惰性群は $\Gamma = \mathrm{Gal}(k_\infty/k)$ となる．惰性群の間の制限写像

$$I_j \longrightarrow \Gamma;\ \sigma \longmapsto \sigma|_{k_\infty}$$

は全射である．この準同型の核は $I_j \cap X$（L/k_∞ における $\mathfrak{P}_j$ の惰性群）であるが，L/k_∞ は不分岐拡大なので，$I_j \cap X = 1$ である．よって，これは同型 $I_j \simeq \Gamma \simeq G/X$ を与える．j は任意なので特に，

$$G = XI_1 = I_1X,\ X \cap I_1 = 1$$

である．I_j の γ に対応する位相的生成元を $\gamma_j \in I_j \leq G$ とする．$G = XI_1$ なので，各 j について $\gamma_j = g_j\gamma_1$ となる $g_j \in X$ がただ一つ存在する．

$\mathrm{Gal}(L/L_0)$ を計算する．$x \in L_0$, $\sigma, \tau \in G$ とすると，L_0/k はアーベル拡大だったので，$\sigma\tau\sigma^{-1}\tau^{-1}(x) = \sigma\tau\sigma^{-1}\tau^{-1}|_{L_0}(x) = x$ となる．したがって

$$[G, G] \leq \mathrm{Gal}(L/L_0)$$

である．また，$x \in L_0$, $\sigma \in I_j$, $g \in G$ とすると，L_0/k は不分岐拡大でもあったので，$g\sigma g^{-1}(x) = g\sigma g^{-1}|_{L_0}(x) = \sigma|_{L_0}(x) = x$ となる．したがって

$$gI_jg^{-1} \leq \mathrm{Gal}(L/L_0) \quad (1 \leq j \leq s,\ g \in G)$$

である．L_0/k は L/k における最大不分岐アーベル拡大なので，$I_j = \overline{\langle g_j\gamma_1 \rangle}$ に注意して

$$\begin{aligned}
\mathrm{Gal}(L/L_0) &= \overline{\langle [G, G],\ gI_jg^{-1} \mid 1 \leq j \leq s,\ g \in G \rangle} \\
&= \overline{\langle [G, G],\ I_j \mid 1 \leq j \leq s \rangle} \\
&= \overline{\langle [G, G],\ I_1,\ \langle g_j\gamma_1 \rangle \mid 2 \leq j \leq s \rangle} \\
&= \overline{\langle [G, G],\ I_1,\ g_j \mid 2 \leq j \leq s \rangle}
\end{aligned}$$

である．

補題 4.11 ([藤井, page 32, 補題 2.2] 参照)**.**

(1) $\overline{[G,G]} = TX = (\gamma - 1)X$.
(2) $Y := \overline{\langle TX, g_j \mid 2 \leq j \leq s \rangle} \leq X$ とおく．このとき

$$\mathrm{Gal}(L/L_0) = \overline{\langle [G,G], I_1, g_j \mid 2 \leq j \leq s \rangle} = YI_1$$

である.

$Y \leq X$ であり，$G = XI_1$, $X \cap I_1 = 1$ なので，$X \cap YI_1 = Y$ となることに注意すると

$$\begin{aligned} A_0 &\simeq X_0 \\ &= \mathrm{Gal}(L_0/k) \\ &\simeq G/\mathrm{Gal}(L/L_0) \\ &= XI_1/YI_1 \\ &\simeq X/X \cap YI_1 \\ &= X/Y \end{aligned}$$

となる．したがって $Y = \mathrm{Ker}\,(X \to X_0)$ である．より一般に次が成り立つ.

命題 4.12 ([藤井, page 34, 命題 2.3] 参照)**.** $A_n \simeq X_n \simeq X/\nu_n Y$.

次の中山の補題は定理 4.14 の証明に用いられる.

定理 4.13 (中山の補題, [Was, page 280, Lemma 13.16], [伊藤, page 11, 中山の補題] 参照)**.** X を compact Λ 加群とする．このとき X が有限生成であることと，$X/(p,T)X$ が有限であることは同値である.

定理 4.14 ([藤井, page 35, 定理 2.2] 参照)**.** X, Y は有限生成ねじれ Λ 加群である.

証明. $X/\nu_1(T)Y \simeq X_1$ は有限であり，$Y/\nu_1(T) \subset X/\nu_1(T)Y$ なので $Y/\nu_1(T)Y$ は有限である．$\nu_1(T) \in (p,T)$ なので，自然な全射準同型

$$Y/\nu_1(T)Y \longrightarrow Y/(p,T)Y$$

が定まり，$Y/(p,T)Y$ は有限となる．よって中山の補題より Y は有限生成 Λ 加群である．$X/Y \simeq X_0$ は有限なので X も有限生成 Λ 加群である.

有限生成 Λ 加群の構造定理から擬同型

$$Y \longrightarrow \Lambda^{\oplus r} \oplus \Big(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i})\Big) \oplus \Big(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j})\Big)$$

が存在する．両辺を $\nu_1(T)$ 倍で割ることで Λ 準同型

$$Y/\nu_1(T)Y \longrightarrow \big(\Lambda/\nu_1(T)\Lambda\big)^{\oplus r} \oplus \big(\bigoplus_{i=1}^{s} \Lambda/(\nu_1(T), p^{n_i}\big) \oplus \big(\bigoplus_{j=1}^{t} \Lambda/(\nu_1(T), f_j(T)^{m_j})\big)$$

が得られ，余核は有限となる．$\nu_1(T)$ は $p-1$ 次の distinguished 多項式なので，割り算原理を用い，$\mathbb{Z}_p$ 加群としての同型

$$\Lambda/\nu_1(T)\Lambda \simeq \mathbb{Z}_p^{\oplus p-1}$$

が成り立つ．ここでもし $r>0$ ならば，$Y/\nu_1(T)Y$ と余核が有限であることに反するので $r=0$ である．したがって Y はねじれ Λ 加群である．また，自然な単射準同型 $Y \longrightarrow X$ は $X/Y \simeq X_0$ が有限なので擬同型であり，X もねじれ Λ 加群である． □

Y は有限生成ねじれ Λ 加群なので，擬同型

$$\varphi : Y \longrightarrow \bigoplus_{i=1}^{s} \Lambda/(p^{n_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j})$$

が存在する．この右辺を $E = \bigoplus_{i=1}^{s} \Lambda/(p^{n_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j})$ とおく．

定理 4.15 ([藤井, page 36, 定理 3.1] 参照)．$\lambda = \sum_{j=1}^{t} m_j \deg f_j(T)$, $\mu = \sum_{i=1}^{s} n_i$ とする．このとき非負整数 n_0 と整数 ν が存在し，$n \geq n_0$ に対して

$$\#E/\nu_n(T)E = p^{\lambda n + \mu p^n + \nu}$$

である．

証明．$E/\nu_n(T)E = \bigoplus_{i=1}^{s} \Lambda/(\nu_n, p^{n_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(\nu_n(T), f_j(T)^{m_j})$ なので各部分の位数を考える．

$\Lambda/(\nu_n, p^{n_i})$ について．$\nu_n(T)$ は distinguished 多項式であるから割り算原理を用いて

$$\Lambda/(\nu_n(T), p^l) \simeq \mathbb{Z}_p[T]/(\nu_n(T), p^l)$$

が成り立つ．$\mathbb{Z}_p[T]/(p^l) \simeq (\mathbb{Z}_p/p^l\mathbb{Z}_p)[T]$ に注意して

$$\begin{aligned}
\mathbb{Z}_p[T]/(\nu_n(T), p^l) &\simeq (\mathbb{Z}_p[T]/(p^l))/(\overline{\nu_n(T)}) \\
&\simeq (\mathbb{Z}_p/p^l\mathbb{Z}_p)[T]/(\overline{\nu_n}(T)) \\
&\simeq (\mathbb{Z}/p^l\mathbb{Z})^{\oplus \deg \nu_n(T)}
\end{aligned}$$

が成り立つ．したがって

$$\#\Lambda/(\nu_n(T), p^l) = p^{l(p^n-1)} = p^{lp^n-l}$$

である．

$\Lambda/(\nu_n(T), f_j(T)^{m_j})$ について．$f(T) = f_j(T)^{m_j}$, $\deg f(T) = d$ とする．$(p-1)p^n > d$ とすると，$f(T)$, $\nu_{n+1,n}(T)$ は distinguished 多項式なので，定義から

$$\begin{aligned} f(T) &= T^d + pa(T), \\ \nu_{n+1,n}(T) &= T^{(p-1)p^n} + pb(T) \end{aligned}$$

となる多項式 $a(T), b(T) \in \mathbb{Z}_p[T]$ が存在する．

$$\begin{aligned} \nu_{n+1,n}(T) &= T^{p^n(p-1)-d}(T^d + pa(T)) + pb(T) - pT^{p^n(p-1)-d}a(T) \\ &= T^{p^n(p-1)-d}f(T) + p(b(T) - T^{p^n(p-1)-d}a(T)) \end{aligned}$$

と変形すると，$\nu_{n+1,n}(0) = p$ なので $b(0) = 1$ である．よって $b(T) - T^{p^n(p-1)-d}a(T) \in \Lambda^\times$ である．このことから

$$\begin{aligned} (\nu_{n+1}(T), f(T)) &= (\nu_{n+1,n}(T)\nu_n(T), f(T)) \\ &= \Big(\big(T^{p^n(p-1)-d}f + p(b(T) - T^{p^n(p-1)-d}a(T)\big)\nu_n(T), f(T)\Big) \\ &= \Big(p\big(b(T) - T^{p^n(p-1)-d}a(T)\big)\nu_n(T), f(T)\Big) \\ &= (p\nu_n(T), f(T)) \end{aligned}$$

とできる．$p^{n_0}(p-1) > d$ となる $n_0 \geq 0$ を固定し，$p^c = \#\Lambda/(\nu_{n_0}(T), f(T))$ とおく．このとき $n \geq n_0$ に対して

$$(\nu_n(T), f(T)) = (p^{n-n_0}\nu_{n_0}(T), f(T))$$

であるから，

$$\begin{aligned} \#\Lambda/(\nu_n(T), f(T)) &= \#\Lambda/(\nu_{n_0}(T), f(T)\#(\nu_{n_0}(T), f(T))/(\nu_n(T), f(T)) \\ &= p^c \cdot \#(\nu_{n_0}(T), f(T))/(p^{n-n_0}\nu_{n_0}(T), f(T)) \end{aligned}$$

である．ν_{n_0} と $f(T)$ は互いに素なので，ν_{n_0} 倍写像

$$\nu_{n_0} : \Lambda/(p^{n-n_0}, f(T)) \longrightarrow (\nu_{n_0}(T), f(T))/(p^{n-n_0}\nu_{n_0}(T), f(T))$$

は加群としての同型を与える．よって

$$\begin{aligned}
\#\Lambda/(\nu_n(T), f(T)) &= p^c \cdot \#(\nu_{n_0}(T), f(T))/(p^{n-n_0}\nu_{n_0}(T), f(T)) \\
&= p^c \cdot \#\Lambda/(p^{n-n_0}, f(T)) \\
&= p^c \cdot \#(\mathbb{Z}/p^{n-n_0}\mathbb{Z})[T]/(f(T)) \\
&= p^c \cdot p^{(n-n_0)\deg f(T)} \\
&= p^{n\deg f(T)+(c-n_0\deg f(T))}
\end{aligned}$$

である．

以上を併せて，$E = \bigoplus_{i=1}^{s} \Lambda/(p^{n_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j})$ に対し，非負整数 n_0 を $(p-1)p^{n_0} > \max\{m_j \deg f_j(T) \mid 1 \leq j \leq t\}$ となるように取る．このとき $n \leq n_0$ に対し

$$\begin{aligned}
\#E/\nu_n(T)E &= \#\bigoplus_{i=1}^{s} \Lambda/(\nu_n(T), p^{n_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(\nu_n(T), f_j(T)^{m_j}) \\
&= \Big(\prod_{i=1}^{s} \#\Lambda/(\nu_n(T), p^{n_i})\Big)\Big(\prod_{j=1}^{t} \#\Lambda/(\nu_n(T), f_j(T)^{m_j})\Big) \\
&= p^{\lambda n+\mu p^n+\nu}
\end{aligned}$$

となる． □

$A = \operatorname{Ker}\varphi$, $B = \operatorname{Coker}\varphi$, $Y' = Y/A$ とする．また，Λ 加群 M と $f(T) \in (p, T)$ に対し，$M[f(T)] = \{x \in M \mid f(T) \cdot x = 0\}$ とおく．このとき

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Y' & \longrightarrow & E & \longrightarrow & B & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \nu_n} & & \downarrow{\scriptstyle \nu_n} & & \downarrow{\scriptstyle \nu_n} & & \\
0 & \longrightarrow & Y' & \longrightarrow & E & \longrightarrow & B & \longrightarrow & 0
\end{array}$$

は完全可換図式である．

命題 4.16 (蛇の補題, [藤井, page 51, 命題 5.11] 参照)**.** R を可換環とし，A_i, B_i を R 加群 $(i = 1, 2, 3)$ とする．R 加群の完全可換図式

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A_1 & \xrightarrow{\varphi_1} & A_2 & \xrightarrow{\varphi_2} & A_3 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} & & \\
0 & \longrightarrow & B_1 & \xrightarrow{\psi_1} & B_2 & \xrightarrow{\psi_2} & B_3 & \longrightarrow & 0
\end{array}$$

があるとき，

$$0 \longrightarrow \mathrm{Ker}\, f_1 \longrightarrow \mathrm{Ker}\, f_2 \longrightarrow \mathrm{Ker}\, f_3 \longrightarrow \mathrm{Coker}\, f_1 \longrightarrow \mathrm{Coker}\, f_2 \longrightarrow \mathrm{Coker}\, f_3 \longrightarrow 0$$

が完全となる R 準同型 $\mathrm{Ker}\, f_3 \longrightarrow \mathrm{Coker}\, f_1$ が存在する．

命題 4.16（蛇の補題）から，完全系列

$$E[\nu_n] \longrightarrow B[\nu_n] \longrightarrow Y'/\nu_n Y' \longrightarrow E/\nu_n E \longrightarrow B/\nu_n B \longrightarrow 0$$

を得る．ν_n と $\mathrm{char}_\Lambda(Y)$ は互いに素なので

$$0 \longrightarrow E \xrightarrow{\nu_n} E$$

は完全である．よって $E[\nu_n] = 0$ となる．また，

$$0 \longrightarrow B[\nu_n] \longrightarrow B \xrightarrow{\nu_n} B \longrightarrow B/\nu_n B \longrightarrow 0$$

は完全であり，B は有限なので $\#B[\nu_n] = \#B/\nu_n B$ である．よって完全系列

$$0 \longrightarrow B[\nu_n] \longrightarrow Y'/\nu_n Y' \longrightarrow E/\nu_n E \longrightarrow B/\nu_n B \longrightarrow 0$$

から

$$\#Y'/\nu_n Y' = \#E/\nu_n E$$

が得られる．

次に，完全系列

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & Y & \longrightarrow & Y' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \nu_n} & & \downarrow{\scriptstyle \nu_n} & & \downarrow{\scriptstyle \nu_n} & & \\ 0 & \longrightarrow & A & \longrightarrow & Y & \longrightarrow & Y' & \longrightarrow & 0 \end{array}$$

に蛇の補題を適用して，完全系列

$$Y'[\nu_n] \longrightarrow A/\nu_n A \longrightarrow Y/\nu_n Y \longrightarrow Y'/\nu_n Y' \longrightarrow 0$$

が得られる．

$$0 \longrightarrow Y' \longrightarrow E$$

は完全で，$E[\nu_n] = 0$ だったので $Y'[\nu_n] = 0$ である．よって

$$0 \longrightarrow A/\nu_n A \longrightarrow Y/\nu_n Y \longrightarrow Y'/\nu_n Y' \longrightarrow 0$$

は完全である．また，A は有限なので，非負整数 m が存在し，$n \geq m$ に対して $(p,T)^n A = 0$ となる．$\nu_n \in (p,T)^n$ だったので，$n \geq m$ に対し $\nu_n A = 0$ となり，

$$\#Y/\nu_n Y = \#A \cdot \#Y'/\nu_n Y'$$

が得られる．

非負整数 n_0 を

$$n_0 > m, \quad (p-1)p^{n_0} > \max\{m_j \deg f_j(T) \mid 1 \leq j \leq t\}$$

を満たすように取ると，$n \geq n_0$ に対し

$$\begin{aligned}
\#A_n &= \#X_n \\
&= \#X/\nu_n Y \\
&= \#X/Y \cdot \#Y/\nu_n Y \\
&= \#A_0 \cdot \#A \cdot \#Y'/\nu_n Y' \\
&= \#A_0 \cdot \#A \cdot \#E/\nu_n E \\
&= \#A_0 \cdot \#A \cdot p^{\lambda n + \mu p^n + \nu}
\end{aligned}$$

が成り立つ．$\#A_0$, $\#A$ は n に依らないので

$$\#A_n = p^{\lambda(k_\infty/k)n + \mu(k_\infty/k)p^n + \nu(k_\infty/k)}$$

と表すことができる．以上により次の定理が示された．

定理 4.17 (岩澤 [Iwa1, page 224, Theorem 11])．A_n を k_n のイデアル類群の Sylow p 部分群とする．このとき k_∞/k のみに依存する非負整数 $\lambda(k_\infty/k)$, $\mu(k_\infty/k)$, n_0 と整数 $\nu(k_\infty/k)$ が存在し， $n \geq n_0$ に対して

$$\#A_n = p^{\lambda(k_\infty/k)n + \mu(k_\infty/k)p^n + \nu(k_\infty/k)}$$

が成り立つ．

定理 4.17 の $\lambda(k_\infty/k)$, $\mu(k_\infty/k)$, $\nu(k_\infty/k)$ を**岩澤不変量**といい，特に k_∞/k が円分 $\mathbb{Z}_p$ 拡大のとき $\lambda_p(k)$, $\mu_p(k)$, $\nu_p(k)$ とかく（[福田 1] 参照）．

Λ 加群の擬同型について推移律は成り立つが，対称律は一般には成り立たない．しかし，有限生成ねじれ Λ 加群 M, M' に対しては，$M \longrightarrow M$ が擬同型であることと $M' \longrightarrow M$

が擬同型であることは同値である（[伊藤, page 14, 注意]，[Was, page 272, Warning] 参照）．定理 4.14 とその証明から，X と Y は同じ特性多項式

$$\mathrm{char}_\Lambda(X) = \mathrm{char}_\Lambda(Y) = \prod_{i=1}^{s} p^{n_i} \prod_{j=1}^{t} f_j(T)^{m_j}$$

をもつ．これを $\boldsymbol{k_\infty/k}$ **の岩澤多項式**という（[福田 1] 参照）．

4.3 水澤靖氏による Iwapoly.gp とそれを用いた計算例

この節では水澤靖氏によって作成された，PARI/GP [PARI1] のプログラムである Iwapoly.gp [水澤] を用いて，岩澤多項式に関する計算例を紹介する．Iwapoly.gp は水澤靖氏の researchmap における資料公開 `https://researchmap.jp/read0206718/published_works` 上に公開されている．詳細については Mizusawa [Miz1] も見てほしい．Iwapoly.gp は Itoh [Ito] においても用いられている．

星研究室 OB である半内広貴先輩の修士論文 [半内] や，本節の内容と関わりの深い [田谷/福田] も参照してほしい．

Iwapoly.gp (水澤靖 [水澤], Mizusawa [Miz1])

```
Iwapoly(p,m,n,f)=
{
local(a,c,d,F,g,i,j,k,L,P,Q,q,r,s,t,u,v);
if(isprime(p)==0,error("not prime"));
d=quaddisc(-m);q=p;if(p==2,q=4;if(d%8==0,d=d\2));
if(d==-q,if(f==2,return(0));return([1,0]));
P=p^n;Q=P*q;if(f==1,g=Mod(1+lcm(q,abs(d)),Q),g=Mod(1+q,Q));
/* coefficients of Stickelberger elements */
if(p<4,a=Mod(1,Q),a=znprimroot(Q)^P);
F=listcreate(P);
s=1;u=(eulerphi(q)-2)\2;v=lcm(q,abs(d))\q-1;
for(i=0,P-1,
c=Mod(0,P);t=s;
for(k=0,u,
for(j=1,v,c=c+j*kronecker(d,t+j*Q));
t=lift(t*a)
);
listput(F,c);s=lift(s*g)
);
```

Iwapoly.gp (水澤靖 [水澤], Mizusawa [Miz1]) 続き

```
/* Iwasawa power series and lambda invariants */
c=Mod(0,P);for(i=0,P-1,c=c+F[i+1]);
if(c%p<>0,if(f==2,return(0));return([1,0]));
g=c;L=1;
while(L<P,
c=Mod(0,P);for(i=1,P-L,c=c+F[i+1]*binomial(P-i,L));
g=g+c*x^L;if(c%p<>0,break);L=L+1
);
if(L==P,if(f==2,return(-1),return([0,0])));
if(f==2,return(L));
if(L==1 & kronecker(d,p)==1,return([x,0]));
r=1;while(L>p^r,r=r+1);
if(n==r,return([x^L,1]));
Q=p^(n-r+1);s=(n-r)*L;
for(k=L+1,min(P-1,s-1+L),
c=Mod(0,Q);for(i=1,P-k,c=c+F[i+1]*binomial(P-i,k));
g=g+c*x^k
);
/* distinguished polynomials */
F=g%x^L;v=1/(g\x^L+O(x^s));g=F*v+O(x^s);u=1;t=1;
for(j=1,n-r-1,
t=truncate(-g*t+O(x^(s+L-j*L)))\x^L+O(x^(s-j*L));
u=u+t
);
P=x^L+truncate(F*(u*v+O(x^L))+O(x^L));
return([lift(P),n-r+1])
}
```

水澤靖氏が作成した Iwapoly.gp を用いて，$1 \leq m \leq 10^6$ の範囲で $k = \mathbb{Q}(\sqrt{-m})$ の円分 $\mathbb{Z}_3$ 拡大 k_∞/k の λ 不変量 $\lambda = \lambda_3(k)$ が 10 以上となる m をまとめたものが次の表である．なお，$\lambda = 8$ となる m は 142 個，$\lambda = 9$ となる m は 45 個，$\lambda = 10$ となる m は 19 個，$\lambda = 11$ となる m は 6 個，$\lambda = 12$ となる m は 1 個，$\lambda = 13$ となる m は 0 個，$\lambda = 14$ となる m は 1 個であった．

表 1　$\lambda_3(k) \geq 10$ となる $k = \mathbb{Q}(\sqrt{-m})$ $(1 \leq m \leq 10^6)$

$\lambda = \lambda_3(k)$	$m : k = \mathbb{Q}(\sqrt{-m})$
10	$23834 = 2 \cdot 17 \cdot 701$, $155677 = 41 \cdot 3797$, $192257 = 13 \cdot 23 \cdot 643$, $200651 = 11 \cdot 17 \cdot 29 \cdot 37$, $315503 = 17 \cdot 67 \cdot 277$, $346847 = 151 \cdot 2297$, $352718 = 2 \cdot 31 \cdot 5689$, $373990 = 2 \cdot 5 \cdot 149 \cdot 251$, $431803 = 431803$, $441299 = 37 \cdot 11927$, $484397 = 484397$, $614217 = 3 \cdot 53 \cdot 3863$, $629105 = 5 \cdot 125821$, $646546 = 2 \cdot 323273$, $667001 = 73 \cdot 9137$, $704474 = 2 \cdot 352237$, $835310 = 2 \cdot 5 \cdot 7 \cdot 11933$, $839737 = 617 \cdot 1361$, $892631 = 709 \cdot 1259$
11	$53301 = 3 \cdot 109 \cdot 163$, $287423 = 197 \cdot 1459$, $550538 = 2 \cdot 275269$, $580037 = 23 \cdot 25219$, $818615 = 5 \cdot 7 \cdot 19 \cdot 1231$, $896771 = 896771$
12	$721981 = 13 \cdot 19 \cdot 37 \cdot 79$
13	
14	$956238 = 2 \cdot 3 \cdot 197 \cdot 809$

[田谷/福田, page 302], [福田 1, page 128] では $0 < m < 10^7$ の範囲での λ の分布を与えているが，具体的な m の値についてはいくつかの例が紹介されているのみである．しかし，それぞれの例においてはイデアル類群の p 部分の構造を決定していたりと，大変興味深いので是非参考にしてほしい．

以下では表 1 を得るために，水澤靖氏の作成した Iwapoly.gp [水澤] をどのように用いるかを説明する．

まず，コンピュータに PARI/GP [PARI1] をインストールする必要がある．PARI/GP については [福田 2, 第 16 章] も参考にしてほしい．インストールが完了したら，PARI/GP のショートカットのプロパティで作業フォルダを指定し，作業フォルダーの中に Iwapoly.gp をおく（拡張子は gp とする）．PARI/GP を起動すると

```
gp >
```

と表示されるので

```
gp > read("Iwapoly.gp");
```

として Enter キーを押して実行すると Iwapoly.gp が読み込まれる．ここで用いる関数について説明すると `Iwapoly(`p`,`m`,`n`,2)` は $\lambda < p^n$ となる n に対して，$k = \mathbb{Q}(\sqrt{-m})$ の円分 $\mathbb{Z}_p$ 拡大 k_∞/k の λ 不変量 $\lambda = \lambda_p(k)$ を返す．また，`Iwapoly(`p`,`m`,`n`,1)` は $\lambda < p^n$ となる n に対して，k_∞/k の岩澤多項式 $P(x)$ の近似を返す．より詳しいことは Mizusawa [Miz1] を見てほしい．試しに

```
gp > Iwapoly(3,23834,3,2)
```

として実行すると

```
10
```

と出力され，$\lambda_3(\mathbb{Q}(\sqrt{-23834})) = 10$ であることがわかる．

```
gp > Iwapoly(3,23834,3,1)
```

として実行すると

```
[x^10, 1]
```

と出力され，$P(x) \equiv x^{10} \pmod{3^1}$ であることがわかる．また，PARI/GP を起動した際に

```
parisize = 8000000
```

のように表示されるが，これは PARI/GP に割り当てられたメモリのサイズを表しており，必要に応じて

```
gp > allocatemem(2*10^9)
  ***   Warning: new stack size = 2000000000 (1907.349 Mbytes).
```

のようにしてメモリを確保してほしい．次に，表 1 を得るために以下のプログラムを実行する．

```
gp > {
```

```
for(m=1,10^6,
  if(m%10^5==0,
    print("m = ",m)
  );
  if(issquarefree(-m),,next); \\ -m が squarefree でないならば，次の m
  n=1;
  lambda=Iwapoly(3,m,n,2);
  while(lambda<0,
    n=n+1;
    lambda=Iwapoly(3,m,n,2)
  ); \\ lambda = Iwapoly(3,m,n,2) が lambda 不変量
  if(lambda>7,
    Iwasawapolynomial=Iwapoly(3,m,n,1);
    print("m = ",m," = ",factor(m),
    ", lambda = ",lambda,",",Iwasawapolynomial);
    write("example.log","m = ",m," = ",factor(m),
    ", lambda = ",lambda,",",Iwasawapolynomial)
  )
)}
```

プログラムをこのように{}で括ることでコマンドプロンプト内で改行ができるようになる（[PARI2, 2.2.3, Special editing characters] を参考にしてほしい）．また，write の部分によって，表示結果と同じものがファイル example.log に書き出されるようになっている．実行結果として，$1 \leq m \leq 10^6$ の範囲で $\lambda \geq 8$ となる m, m の素因数分解，λ, Iwapoly(3,m,n,1) が以下のように表示される．

```
m = 2789 = Mat([2789, 1]), lambda = 8, [x^8, 1]
m = 7646 = [2, 1; 3823, 1], lambda = 8, [x^8, 1]
m = 14493 = [3, 1; 4831, 1], lambda = 8, [x^8, 1]
m = 15294 = [2, 1; 3, 1; 2549, 1], lambda = 8, [x^8, 1]
m = 21107 = Mat([21107, 1]), lambda = 8, [x^8, 1]
m = 23834 = [2, 1; 17, 1; 701, 1], lambda = 10, [x^10, 1]
m = 35967 = [3, 1; 19, 1; 631, 1], lambda = 8, [x^8, 1]
m = 41570 = [2, 1; 5, 1; 4157, 1], lambda = 8, [x^8, 1]
m = 53301 = [3, 1; 109, 1; 163, 1], lambda = 11,[x^11, 1]
m = 55274 = [2, 1; 29, 1; 953, 1], lambda = 8, [x^8, 1]
m = 69061 = Mat([69061, 1]), lambda = 9, [x^9 + 3*x^8 + 3*x^5 + 3*x^4 + 3*x +
```

```
6, 2]
m = 73067 = [31, 1; 2357, 1], lambda = 8, [x^8, 1]
m = 73817 = [97, 1; 761, 1], lambda = 8, [x^8, 1]
m = 87414 = [2, 1; 3, 1; 17, 1; 857, 1], lambda = 8, [x^8, 1]
m = 99653 = [227, 1; 439, 1], lambda = 8, [x^8, 1]
m = 100000
m = 106282 = [2, 1; 11, 1; 4831, 1], lambda = 8, [x^8, 1]
m = 114113 = Mat([114113, 1]), lambda = 8, [x^8, 1]
m = 117782 = [2, 1; 7, 1; 47, 1; 179, 1], lambda = 8, [x^8, 1]
m = 119681 = [19, 1; 6299, 1], lambda = 8, [x^8, 1]
m = 122846 = [2, 1; 239, 1; 257, 1], lambda = 8, [x^8, 1]
m = 128222 = [2, 1; 61, 1; 1051, 1], lambda = 9, [x^9 + 6*x^8 + 3*x^7 + 3*x^6
+ 6*x^5 + 3*x^4 + 6*x, 2]
m = 136499 = [11, 1; 12409, 1], lambda = 9, [x^9 + 3*x^8 + 6*x^6 + 6*x^2, 2]
m = 145769 = [13, 1; 11213, 1], lambda = 9, [x^9 + 6*x^8 + 6*x^7 + 6*x^5 + 6*x
^4 + 3*x^3 + 3*x, 2]
m = 154589 = Mat([154589, 1]), lambda = 9, [x^9 + 3*x^8 + 3*x^7 + 6*x^2, 2]
m = 155677 = [41, 1; 3797, 1], lambda = 10, [x^10, 1]
m = 160417 = [19, 1; 8443, 1], lambda = 8, [x^8, 1]
m = 165810 = [2, 1; 3, 1; 5, 1; 5527, 1], lambda = 8, [x^8, 1]
m = 170913 = [3, 1; 23, 1; 2477, 1], lambda = 8, [x^8, 1]
m = 174767 = Mat([174767, 1]), lambda = 8, [x^8, 1]
m = 183158 = [2, 1; 17, 1; 5387, 1], lambda = 8, [x^8, 1]
m = 190515 = [3, 1; 5, 1; 13, 1; 977, 1], lambda = 8, [x^8, 1]
m = 192257 = [13, 1; 23, 1; 643, 1], lambda = 10, [x^10, 1]
m = 200000
m = 200651 = [11, 1; 17, 1; 29, 1; 37, 1], lambda = 10, [x^10, 1]
m = 201023 = [41, 1; 4903, 1], lambda = 8, [x^8, 1]
m = 203178 = [2, 1; 3, 1; 33863, 1], lambda = 8, [x^8, 1]
m = 214822 = [2, 1; 37, 1; 2903, 1], lambda = 9, [x^9 + 3*x^6 + 6*x^5 + 3*x^4
+ 6*x^3 + 6*x^2 + 3, 2]
m = 220233 = [3, 1; 13, 1; 5647, 1], lambda = 8, [x^8, 1]
m = 228403 = [7, 1; 67, 1; 487, 1], lambda = 8, [x^8, 1]
m = 240617 = [13, 1; 83, 1; 223, 1], lambda = 8, [x^8, 1]
m = 241683 = [3, 1; 13, 1; 6197, 1], lambda = 9, [x^9 + 6*x^8 + 3*x^4 + 6*x^3,
 2]
m = 254442 = [2, 1; 3, 1; 42407, 1], lambda = 9, [x^9 + 3*x^8 + 3*x^7 + 6*x^6
+ 3*x^5 + 3*x^3 + 3*x^2 + 3*x, 2]
m = 262166 = [2, 1; 47, 1; 2789, 1], lambda = 8, [x^8, 1]
m = 268078 = [2, 1; 134039, 1], lambda = 8, [x^8, 1]
```

```
m = 271103 = [7, 1; 38729, 1], lambda=9, [x^9 + 6*x^7 + 6*x^5 + 6*x^3 + 6*x, 2
]
m = 271299 = [3, 1; 7, 1; 12919, 1], lambda = 8, [x^8, 1]
m = 279722 = [2, 1; 139861, 1], lambda = 8, [x^8, 1]
m = 287423,factor(m) = [197, 1; 1459, 1], lambda = 11, [x^11, 1]
m = 293165 = [5, 1; 17, 1; 3449, 1], lambda = 8, [x^8, 1]
m = 293306 = [2, 1; 13, 1; 29, 1; 389, 1], lambda = 8, [x^8, 1]
m = 298241 = [23, 1; 12967, 1], lambda = 8, [x^8, 1]
m = 300000
m = 301341 = [3, 1; 100447, 1], lambda = 9, [x^9 + 6*x^6 + 6*x^5 + 3*x^4 + 3*x
^3 + 3*x, 2]
m = 304430 = [2, 1; 5, 1; 7, 1; 4349, 1], lambda = 9, [x^9 + 6*x^8 + 6*x^7 + 6
*x^6 + 3*x^5 + 3*x, 2]
m = 305183 = [61, 1; 5003, 1], lambda = 8, [x^8, 1]
m = 312377 = [13, 1; 24029, 1], lambda = 8, [x^8, 1]
m = 312794 = [2, 1; 29, 1; 5393, 1], lambda = 8, [x^8, 1]
m = 315503 = [17, 1; 67, 1; 277, 1], lambda = 10, [x^10, 1]
m = 318959 = [31, 1; 10289, 1], lambda = 9, [x^9 + 3*x^8 + 6*x^6 + 3*x^5 + 6*x
^4 + 3*x^3 + 3*x, 2]
m = 323582 = [2, 1; 7, 1; 29, 1; 797, 1], lambda = 8, [x^8, 1]
m = 338135 = [5, 1; 7, 1; 9661, 1], lambda = 8, [x^8, 1]
m = 340201 = Mat([340201, 1]), lambda = 9, [x^9 + 3*x^8 + 6*x^6 + 6*x^3 + 3*x
+ 3, 2]
m = 345718 = [2, 1; 172859, 1], lambda = 8, [x^8, 1]
m = 346847 = [151, 1; 2297, 1], lambda = 10, [x^10, 1]
m = 352718 = [2, 1; 31, 1; 5689, 1], lambda = 10, [x^10, 1]
m = 367310 = [2, 1; 5, 1; 23, 1; 1597, 1], lambda = 8, [x^8, 1]
m = 369478 = [2, 1; 17, 1; 10867, 1], lambda = 8, [x^8, 1]
m = 370461 = [3, 1; 7, 1; 13, 1; 23, 1; 59, 1], lambda = 8, [x^8, 1]
m = 372515 = [5, 1; 11, 1; 13, 1; 521, 1], lambda = 8, [x^8, 1]
m = 373990 = [2, 1; 5, 1; 149, 1; 251, 1], lambda = 10, [x^10, 1]
m = 377023 = [181, 1; 2083, 1], lambda = 8, [x^8, 1]
m = 399653 = [17, 1; 23509, 1], lambda = 8, [x^8, 1]
m = 399730 = [2, 1; 5, 1; 71, 1; 563, 1], lambda = 9, [x^9 + 6*x^8 + 6*x^5 + 6
*x^3 + 3*x + 3, 2]
m = 400000
m = 403206 = [2, 1; 3, 1; 17, 1; 59, 1; 67, 1], lambda = 8, [x^8, 1]
m = 407677 = [17, 1; 23981, 1], lambda = 8, [x^8, 1]
m = 407927 = [13, 1; 31379, 1], lambda = 8, [x^8, 1]
m = 408022 = [2, 1; 31, 1; 6581, 1], lambda = 9, [x^9 + 3*x^8 + 3*x^7 + 3*x^5
```

```
+ 6*x^4 + 3*x, 2]
m = 411059 = [11, 1; 37369, 1], lambda = 9, [x^9 + 3*x^7 + 6*x^6 + 6*x^3 + 3*x
^2, 2]
m = 415379 = Mat([415379, 1]), lambda = 9, [x^9 + 3*x^7 + 6*x^5 + 6*x^2, 2]
m = 421598 = [2, 1; 71, 1; 2969, 1], lambda = 8, [x^8, 1]
m = 422495 = [5, 1; 84499, 1], lambda = 8, [x^8, 1]
m = 425157 = [3, 1; 141719, 1], lambda = 8, [x^8, 1]
m = 428057 = [7, 1; 61151, 1], lambda = 8, [x^8, 1]
m = 429278 = [2, 1; 214639, 1], lambda = 9, [x^9 + 3*x^8 + 6*x^7 + 6*x^6 + 3*x
^5 + 3*x^3, 2]
m = 431803 = Mat([431803, 1]), lambda = 10, [x^10, 1]
m = 435866 = [2, 1; 217933, 1], lambda = 8, [x^8, 1]
m = 441299 = [37, 1; 11927, 1], lambda = 10, [x^10, 1]
m = 451789 = [13, 1; 23, 1; 1511, 1], lambda = 9, [x^9 + 3*x^8 + 6*x^7 + 6*x^5
 + 3*x^3 + 6, 2]
m = 456961 = [43, 1; 10627, 1], lambda = 8, [x^8, 1]
m = 460709 = Mat([460709, 1]), lambda = 8, [x^8, 1]
m = 462503 = [317, 1; 1459, 1], lambda = 9, [x^9 + 6*x^8 + 3*x^7 + 3*x^6 + 6*x
^5 + 6*x^4 + 6*x^3 + 6*x^2, 2]
m = 465302 = [2, 1; 73, 1; 3187, 1], lambda = 8, [x^8, 1]
m = 474490 = [2, 1; 5, 1; 23, 1; 2063, 1], lambda = 8, [x^8, 1]
m = 480030 = [2, 1; 3, 1; 5, 1; 16001, 1], lambda = 8, [x^8, 1]
m = 481603 = [29, 1; 16607, 1], lambda = 8, [x^8, 1]
m = 482606 = [2, 1; 241303, 1], lambda = 9, [x^9 + 6*x^8 + 6*x^7 + 3*x^5 + 6*x
, 2]
m = 484397 = Mat([484397, 1]), lambda = 10, [x^10, 1]
m = 490163 = [47, 1; 10429, 1], lambda = 9, [x^9 + 3*x^8 + 3*x^5 + 6*x^4 + 3*x
^2, 2]
m = 497494 = [2, 1; 41, 1; 6067, 1], lambda = 8, [x^8, 1]
m = 500000
m = 509030 = [2, 1; 5, 1; 109, 1; 467, 1], lambda = 8, [x^8, 1]
m = 516323 = Mat([516323, 1]), lambda = 8, [x^8, 1]
m = 516671 = [47, 1; 10993, 1], lambda = 9, [x^9 + 6*x^7 + 6*x^5 + 3*x^4 + 3*x
^3 + 6*x^2 + 6*x, 2]
m = 531213 = [3, 1; 113, 1; 1567, 1], lambda = 8, [x^8, 1]
m = 531533 = [461, 1; 1153, 1], lambda = 8, [x^8, 1]
m = 545057 = Mat([545057, 1]), lambda = 8, [x^8, 1]
m = 550538 = [2, 1; 275269, 1], lambda = 11, [x^11, 1]
m = 551965 = [5, 1; 101, 1; 1093, 1], lambda = 9, [x^9 + 3*x^6 + 3*x^3 + 3*x^2
 + 3*x, 2]
```

```
m = 554511 = [3, 1; 184837, 1], lambda = 8, [x^8, 1]
m = 569930 = [2, 1; 5, 1; 56993, 1], lambda = 9, [x^9 + 6*x^8 + 6*x^7 + 3*x^6
+ 3*x^3 + 3*x^2, 2]
m = 580037 = [23, 1; 25219, 1], lambda = 11, [x^11, 1]
m = 580133 = Mat([580133, 1]), lambda = 8, [x^8, 1]
m = 582014 = [2, 1; 291007, 1], lambda = 8, [x^8, 1]
m = 583643 = [409, 1; 1427, 1], lambda = 8, [x^8, 1]
m = 586253 = [107, 1; 5479, 1], lambda = 8, [x^8, 1]
m = 587438 = [2, 1; 419, 1; 701, 1], lambda = 8, [x^8, 1]
m = 587963 = [577, 1; 1019, 1], lambda = 8, [x^8, 1]
m = 588741 = [3, 1; 196247, 1], lambda = 8, [x^8, 1]
m = 592247 = [47, 1; 12601, 1], lambda = 8, [x^8, 1]
m = 593065 = [5, 1; 11, 1; 41, 1; 263, 1], lambda = 8, [x^8, 1]
m = 598673 = [59, 1; 73, 1; 139, 1], lambda = 9, [x^9 + 6*x^8 + 3*x^3 + 6*x^2
+ 3*x, 2]
m = 599258 = [2, 1; 11, 1; 27239, 1], lambda = 8, [x^8, 1]
m = 600000
m = 600749 = [31, 1; 19379, 1], lambda = 8, [x^8, 1]
m = 601070 = [2, 1; 5, 1; 60107, 1], lambda = 8, [x^8, 1]
m = 601338 = [2, 1; 3, 1; 31, 1; 53, 1; 61, 1], lambda = 8, [x^8, 1]
m = 608915 = [5, 1; 193, 1; 631, 1], lambda = 8, [x^8, 1]
m = 609190 = [2, 1; 5, 1; 60919, 1], lambda = 8, [x^8, 1]
m = 614217 = [3, 1; 53, 1; 3863, 1], lambda = 10, [x^10, 1]
m = 614573 = [353, 1; 1741, 1], lambda = 8, [x^8, 1]
m = 619351 = [89, 1; 6959, 1], lambda = 8, [x^8, 1]
m = 624635 = [5, 1; 11, 1; 41, 1; 277, 1], lambda = 8, [x^8, 1]
m = 627074 = [2, 1; 7, 1; 47, 1; 953, 1], lambda = 8, [x^8, 1]
m = 629105 = [5, 1; 125821, 1], lambda = 10, [x^10, 1]
m = 629174 = [2, 1; 7, 1; 13, 1; 3457, 1], lambda = 8, [x^8, 1]
m = 630506 = [2, 1; 367, 1; 859, 1], lambda = 8, [x^8, 1]
m = 630635 = [5, 1; 126127, 1], lambda = 8, [x^8, 1]
m = 635666 = [2, 1; 59, 1; 5387, 1], lambda = 9, [x^9 + 6*x^8 + 6*x^7 + 3*x^6
+ 6*x^5 + 6*x^4 + 3*x^3 + 3*x, 2]
m = 641705 = [5, 1; 128341, 1], lambda = 8, [x^8, 1]
m = 643415 = [5, 1; 128683, 1], lambda = 8, [x^8, 1]
m = 645899 = [709, 1; 911, 1], lambda = 8, [x^8, 1]
m = 646409 = [373, 1; 1733, 1], lambda = 8, [x^8, 1]
m = 646546 = [2, 1; 323273, 1], lambda = 10, [x^10, 1]
m = 655961 = Mat([655961, 1]), lambda = 8, [x^8, 1]
m = 664367 = [11, 1; 60397, 1], lambda = 8, [x^8, 1]
```

```
m = 667001 = [73, 1; 9137, 1], lambda = 10, [x^10, 1]
m = 677297 = [17, 1; 39841, 1], lambda = 9, [x^9 + 3*x^8 + 6*x^7 + 6*x^6 + 6*x
^5, 2]
m = 679199 = [419, 1; 1621, 1], lambda = 8, [x^8, 1]
m = 685137 = [3, 1; 137, 1; 1667, 1], lambda = 8, [x^8, 1]
m = 693857 = [79, 1; 8783, 1], lambda = 8, [x^8, 1]
m = 696190 = [2, 1; 5, 1; 11, 1; 6329, 1], lambda = 8, [x^8, 1]
m = 698279 = [47, 1; 83, 1; 179, 1], lambda = 8, [x^8, 1]
m = 700000
m = 700985 = [5, 1; 140197, 1], lambda = 8, [x^8, 1]
m = 701365 = [5, 1; 7, 1; 29, 1; 691, 1], lambda = 9, [x^9 + 3*x^8 + 3*x^6 + 3
*x^5 + 6*x^4 + 3*x + 6, 2]
m = 704474 = [2, 1; 352237, 1], lambda = 10, [x^10, 1]
m = 707902 = [2, 1; 13, 1; 19, 1; 1433, 1], lambda = 8, [x^8, 1]
m = 721866 = [2, 1; 3, 1; 31, 1; 3881, 1], lambda = 8, [x^8, 1]
m = 721981 = [13, 1; 19, 1; 37, 1; 79, 1], lambda = 12, [x^12, 1]
m = 728135 = [5, 1; 107, 1; 1361, 1], lambda = 9, [x^9 + 3*x^6 + 3*x^5 + 6*x^4
 + 3*x, 2]
m = 728701 = Mat([728701, 1]), lambda = 8, [x^8, 1]
m = 736714 = [2, 1; 11, 1; 33487, 1], lambda = 8, [x^8, 1]
m = 738746 = [2, 1; 29, 1; 47, 1; 271, 1], lambda = 9, [x^9 + 3*x^6 + 3*x^5 +
6*x^4 + 6*x^3 + 3*x, 2]
m = 745667 = [13, 1; 41, 1; 1399, 1], lambda = 8, [x^8, 1]
m = 759341 = [11, 1; 69031, 1], lambda = 8, [x^8, 1]
m = 767089 = Mat([767089, 1]), lambda = 8, [x^8, 1]
m = 771629 = Mat([771629, 1]), lambda = 8, [x^8, 1]
m = 782165 = [5, 1; 311, 1; 503, 1], lambda = 8, [x^8, 1]
m = 792461 = Mat([792461, 1]), lambda = 8, [x^8, 1]
m = 796361 = Mat([796361, 1]), lambda = 8, [x^8, 1]
m = 796922 = [2, 1; 7, 1; 56923, 1], lambda = 9, [x^9 + 3*x^8 + 6*x^7 + 3*x^6
+ 6*x^5 + 6*x^4 + 3*x^3 + 3*x^2 + 3*x, 2]
m = 800000
m = 809009 = [823, 1; 983, 1], lambda = 8, [x^8, 1]
m = 809043 = [3, 1; 61, 1; 4421, 1], lambda = 9, [x^9 + 6*x^6 + 3*x^5 + 3*x^4
+ 3*x^2 + 3*x + 3, 2]
m = 818615 = [5, 1; 7, 1; 19, 1; 1231, 1], lambda = 11, [x^11, 1]
m = 821234 = [2, 1; 410617, 1], lambda = 8, [x^8, 1]
m = 828419 = [19, 1; 59, 1; 739, 1], lambda = 8, [x^8, 1]
m = 833290 = [2, 1; 5, 1; 23, 1; 3623, 1], lambda = 8, [x^8, 1]
m = 835310 = [2, 1; 5, 1; 7, 1; 11933, 1], lambda = 10, [x^10, 1]
```

```
m = 836223 = [3, 1; 278741, 1], lambda = 8, [x^8, 1]
m = 838730 = [2, 1; 5, 1; 83873, 1], lambda = 8, [x^8, 1]
m = 839737 = [617, 1; 1361, 1], lambda = 10, [x^10, 1]
m = 846098 = [2, 1; 11, 1; 38459, 1], lambda = 8, [x^8, 1]
m = 853334 = [2, 1; 131, 1; 3257, 1], lambda = 8, [x^8, 1]
m = 853382 = [2, 1; 426691, 1], lambda = 8, [x^8, 1]
m = 856439 = [37, 1; 79, 1; 293, 1], lambda = 9, [x^9 + 6*x^8 + 6*x^5 + 6*x^4
+ 3*x^3 + 3*x^2 + 6*x, 2]
m = 858286 = [2, 1; 11, 1; 13, 1; 3001, 1], lambda = 8, [x^8, 1]
m = 861854 = [2, 1; 7, 1; 61561, 1], lambda = 9, [x^9 + 3*x^8 + 6*x^5 + 6*x^3
+ 3*x, 2]
m = 863489 = [11, 1; 23, 1; 3413, 1], lambda = 8, [x^8, 1]
m = 869327 = [431, 1; 2017, 1], lambda = 8, [x^8, 1]
m = 876515 = [5, 1; 175303, 1], lambda = 8, [x^8, 1]
m = 885683 = [17, 1; 53, 1; 983, 1], lambda = 8, [x^8, 1]
m = 888002 = [2, 1; 444001, 1], lambda = 8, [x^8, 1]
m = 892631 = [709, 1; 1259, 1], lambda = 10, [x^10, 1]
m = 896771 = Mat([896771, 1]), lambda = 11, [x^11, 1]
m = 896879 = Mat([896879, 1]), lambda = 8, [x^8, 1]
m = 900000
m = 900174 = [2, 1; 3, 1; 11, 1; 23, 1; 593, 1], lambda = 9, [x^9 + 3*x^8 + 6*
x^3 + 3*x^2, 2]
m = 900559 = [11, 1; 81869, 1], lambda = 8, [x^8, 1]
m = 902435 = [5, 1; 101, 1; 1787, 1], lambda = 9, [x^9 + 3*x^7 + 6*x^6 + 6*x^2
 + 3*x, 2]
m = 909971 = Mat([909971, 1]), lambda = 8, [x^8, 1]
m = 916691 = [17, 1; 53923, 1], lambda = 9, [x^9 + 6*x^5 + 3*x^4 + 6*x^2 + 6*x
, 2]
m = 916985 = [5, 1; 183397, 1], lambda = 9, [x^9 + 6*x^8 + 3*x^6 + 3*x^3 + 3*x
^2, 2]
m = 921089 = [13, 1; 70853, 1], lambda = 8, [x^8, 1]
m = 934667 = [19, 1; 49193, 1], lambda = 9, [x^9 + 3*x^4 + 3*x^2, 2]
m = 937339 = [13, 1; 72103, 1], lambda = 8, [x^8, 1]
m = 945307 = [11, 1; 19, 1; 4523, 1], lambda = 8, [x^8, 1]
m = 945358 = [2, 1; 47, 1; 89, 1; 113, 1], lambda = 8, [x^8, 1]
m = 955418 = [2, 1; 607, 1; 787, 1], lambda = 9, [x^9 + 3*x^8 + 3*x^7 + 6*x^4
+ 3*x^3 + 3*x^2 + 3*x, 2]
m = 956238 = [2, 1; 3, 1; 197, 1; 809, 1], lambda = 14, [x^14, 1]
m = 959090 = [2, 1; 5, 1; 11, 1; 8719, 1], lambda = 8, [x^8, 1]
m = 960914 = [2, 1; 67, 1; 71, 1; 101, 1], lambda = 8, [x^8, 1]
```

```
m = 963023 = [613, 1; 1571, 1], lambda = 9, [x^9 + 6*x^8 + 6*x^6 + 3*x^5 + 3*x
^4 + 3*x^2, 2]
m = 967001 = [7, 1; 138143, 1], lambda = 9, [x^9 + 3*x^7 + 3*x^6 + 6*x^4 + 3*x
^3, 2]
m = 975455 = [5, 1; 13, 1; 43, 1; 349, 1], lambda = 9, [x^9 + 3*x^7 + 3*x^6 +
6*x^5 + 3*x, 2]
m = 977773 = [127, 1; 7699, 1], lambda = 9, [x^9 + 6*x^8 + 6*x^7 + 3*x^6 + 6*x
^4 + 6*x^3 + 6*x^2 + 3*x, 2]
m = 979907 = Mat([979907, 1]), lambda = 8, [x^8, 1]
m = 980682 = [2, 1; 3, 1; 73, 1; 2239, 1], lambda = 8, [x^8, 1]
m = 981565 = [5, 1; 13, 1; 15101, 1], lambda = 8, [x^8, 1]
m = 982430 = [2, 1; 5, 1; 17, 1; 5779, 1], lambda = 8, [x^8, 1]
m = 990101 = [7, 1; 141443, 1], lambda = 8, [x^8, 1]
m = 1000000
```

このプログラムとほぼ同等のプログラムによる計算には Intel(R) Core(TM) i5-7200U CPU (2.50GHz, 8.00 GB RAM, Windows) 搭載のノートパソコンで 3 週間ほど時間を要した．この結果から $\lambda \geq 10$ となる m をまとめたものが表 1 である．また，

```
gp > #
```

として実行すると

```
   timer = 1 (on)
```

と表示され，以後の計算にかかった時間が表示されるようになる．岩澤多項式 $P(x)$ のより詳細な近似が知りたいときは，n の値を大きくすればよい．

```
gp > Iwapoly(3,721981,4,1)
time = 2min, 19,109 ms.
[x^12 + 3*x^10 + 3*x^9 + 6*x^8 + 3*x^7 + 3*x^6 + 3*x^4 + 3*x^3 + 6*x^2
 + 3*x + 3, 2]
```

では

$$P(x) \equiv x^{12} + 3x^{10} + 3x^9 + 6x^8 + 3x^7 + 3x^6 + 3x^4 + 3x^3 + 6x^2 + 3x + 3 \pmod{3^2}$$

が出力され，

```
gp > Iwapoly(3,721981,5,1)
time = 7min, 2,453 ms.
[x^12 + 21*x^10 + 3*x^9 + 24*x^8 + 3*x^7 + 3*x^6 + 21*x^4 + 3*x^3 + 6*
x^2 + 3*x + 3, 3]
```

では

$$P(x) \equiv x^{12} + 21x^{10} + 3x^9 + 24x^8 + 3x^7 + 3x^6 + 21x^4 + 3x^3 + 6x^2 + 3x + 3 \pmod{3^3}$$

が出力されているが，11 次の項と 5 次の項が消えている．

```
gp > Iwapoly(3,721981,6,1)
time = 22min, 24,829 ms.
[x^12 + 27*x^11 + 75*x^10 + 30*x^9 + 51*x^8 + 3*x^7 + 3*x^6 + 54*x^5 +
 75*x^4 + 57*x^3 + 60*x^2 + 3*x + 57, 4]
```

では

$$P(x) \equiv x^{12} + 27x^{11} + 75x^{10} + 30x^9 + 51x^8 + 3x^7 + 3x^6 + 54x^5 + 75x^4 + 57x^3 + 60x^2 + 3x + 57 \pmod{3^4}$$

が出力され，すべての項が現れている．表 1 で最大の $\lambda = 14$ となる $m = 956238$ に対しても

```
gp > Iwapoly(3,956238,5,1)
time = 7min, 5,125 ms.
[x^14 + 9*x^13 + 24*x^12 + 18*x^11 + 24*x^10 + 12*x^9 + 15*x^8 + 21*x^
7 + 21*x^6 + 12*x^5 + 3*x^4 + 3*x^3 + 15*x^2 + 24*x + 21, 3]
```

や

```
gp > Iwapoly(3,956238,6,1)
time = 9min, 45,344 ms.
[x^14 + 63*x^13 + 51*x^12 + 72*x^11 + 24*x^10 + 39*x^9 + 69*x^8 + 75*x
^7 + 75*x^6 + 39*x^5 + 30*x^4 + 30*x^3 + 69*x^2 + 24*x + 75, 4]
```

のように計算できる．この計算を例としてまとめておく．

例 **4.18.**

(1) $k = \mathbb{Q}(\sqrt{-721981})$ の円分 $\mathbb{Z}_3$ 拡大に対して $\lambda = \lambda_3(k) = 12$ であり，岩澤多項式 $P(x)$ について

$$P(x) \equiv x^{12} + 27x^{11} + 75x^{10} + 30x^9 + 51x^8 + 3x^7 + 3x^6 + 54x^5 + 75x^4 + 57x^3 + 60x^2 + 3x + 57 \pmod{3^4}.$$

(2) $k = \mathbb{Q}(\sqrt{-956238})$ の円分 $\mathbb{Z}_3$ 拡大に対して $\lambda = \lambda_3(k) = 14$ であり，岩澤多項式 $P(x)$ について

$$P(x) \equiv x^{14} + 63x^{13} + 51x^{12} + 72x^{11} + 24x^{10} + 39x^9 + 69x^8 + 75x^7 + 75x^6 + 39x^5 + 30x^4 + 30x^3 + 69x^2 + 24x + 75 \pmod{3^4}.$$

5　非アーベル岩澤理論

5 章では，著者が岩澤理論について学んでいて興味を持った非アーベル岩澤理論について，主に [尾崎] に基づいて紹介する．岩澤理論にはその非可換化が複数考えられており，その中で非アーベル岩澤理論は「作用される群の非可換化」を目指したもの（[尾崎, page 313] 参照）である．

pro-finite 群などについては [足立, 7.3 節] や Neukirch-Schmidt-Wingberg [NSW] を参照してほしい．

5.1　記号の準備

p を素数，k を有限次代数体とし，K/k を $\mathbb{Z}_p$ 拡大とする．また，k_n を n-th layer とする．ここで，分岐する素点に条件を付けるために次の記号を用意する．

F を有限次とは限らない一般の代数体，S を F の素点からなる集合とし，$F_S(p)$ を F の最大 S 分岐 p 拡大とする．ここで S 分岐とは，S に含まれる素点以外は不分岐であると定義する．また，$G_{F,S}(p) = \mathrm{Gal}(F_S(p)/F)$ とおく．

$S = \varnothing$ の場合として，有限次代数体 k の最大不分岐 p 拡大 $k_\varnothing(p)/k$ のガロア群 $G_{k,\varnothing}(p)$ については以下のことが知られている（[尾崎, page 315] 参照）．

(1) $G_{k,\varnothing}(p)$ は有限表示 pro-p 群である．すなわち，pro-p 群の完全系列

$$1 \to R \to F_d \to G_{k,\varnothing}(p) \to 1$$

が存在する．ここで F_d は有限階数 d の自由 pro-p 群であり，R は有限個の元 $t_1, t_2, \ldots, t_r$ で F_d の正規閉部分群として生成される：

$$R = (t_1, t_2, \ldots, t_r)_{F_d} := \langle g t_i g^{-1} \mid g \in F_d,\ 1 \le i \le r \rangle.$$

(2) $G_{k,\varnothing}(p)$ は FAb 群 (Finite Abelianization group) である．すなわち，$G_{k,\varnothing}(p)$ の任意の開部分群 H のアーベル化 $H^{\mathrm{ab}} = H/[H,H]$ は有限である（[H,H] は閉包をとっている）．

(3) $G_{k,\varnothing}(p)$ は無限になり得る（Golod-Šafarevič [GS]）．

さらに次の定理が尾崎学氏によって与えられている．

定理 5.1 (尾崎 [Oza2, page 650, Theorem I])**.** 任意の有限 p 群は，ある有限次代数体 k に対する $G_{k,\varnothing}(p)$ として実際に現れる．

ここで，

$$L_S = K_S(p),\ L_{n,S} = (k_n)_S(p),$$
$$G = G_{K,S}(p) = \mathrm{Gal}(K_S(p)/K) = \mathrm{Gal}(L_S/K),$$
$$G_n = G_{k_n,S}(p) = \mathrm{Gal}((k_n)_S(p)/k_n) = \mathrm{Gal}(L_{n,S}/k_n)$$

とおく．また，群 H に対し，H の降中心列

$$H = C_1(H) \supseteq C_2(H) \supseteq \cdots \supseteq C_i(H) \supseteq \cdots$$

を

$$C_1(H) = H, \quad C_{i+1}(H) = [C_i(H), H]$$

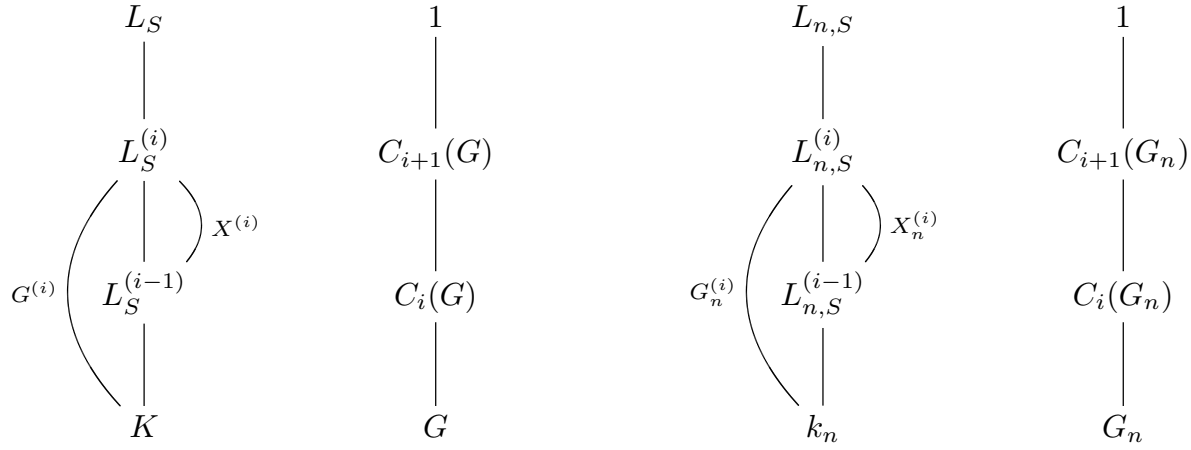
で定める（位相群 H に対しては，交換子群は閉包をとる）．このとき，$i \geq 0$ に対して，

$$L_S^{(i)} = L_S^{C_{i+1}(G)},\ L_{n,S}^{(i)} = L_{n,S}^{C_{i+1}(G_n)},$$

$i \geq 1$ に対して，

$$G^{(i)} = \mathrm{Gal}(L_S^{(i)}/K) \simeq G/C_{i+1}(G),\ G_n^{(i)} = \mathrm{Gal}(L_{n,S}^{(i)}/k_n) \simeq G_n/C_{i+1}(G_n),$$
$$X^{(i)} = \mathrm{Gal}(L_S^{(i)}/L_S^{(i-1)}) \simeq C_i(G)/C_{i+1}(G),\ X_n^{(i)} = \mathrm{Gal}(L_{n,S}^{(i)}/L_{n,S}^{(i-1)}) \simeq C_i(G_n)/C_{i+1}(G_n)$$

とおく．



$X^{(i)}$ は $\Lambda = \mathbb{Z}_p[[\Gamma]]$ 上の加群となり，これを**第 i 次岩澤加群**という． $S = \varnothing$ とすると，$X^{(1)}$ は先に述べた岩澤加群であり，$X_n^{(1)}$ は X_n である．

5.2 非アーベル岩澤公式

この節では $S = \varnothing$ の場合をあつかう．

各 $n \geq 0$, $i \geq 1$ に対し，$X_n^{(i)}$ は有限アーベル p 群，$G_n^{(i)}$ は有限 p 群である．実際，$L_{n,\varnothing}^{(1)}/k_n$ は（最大）不分岐アーベル拡大なので有限次拡大である．また，$L_{n,\varnothing}^{(i)}/L_{n,\varnothing}^{(i-1)}$ も同様に不分岐アーベル拡大である．よって有限次拡大となり，$C_i(G_n)$ は G_n の開部分群である．G_n が FAb 群であることから有限性が，pro-p 群であることから p 群であることがしたがう．

定理 5.2 (尾崎 [Oza1, page 62, Proposition 1, Proposition 2, page 66, Proposition 3], [尾崎, page 318, 命題 3.1] 参照)．$\mu(K/k)$ を K/k の岩澤 μ 不変量とする．

(1) $\mu(K/k) = 0$ ならば，各 $i \geq 1$ に対して $X^{(i)}$ は有限生成ねじれ Λ 加群であり $\mathbb{Z}_p$ 上でも有限生成である．
(2) $\mu(K/k) > 0$ ならば，各 $i \geq 2$ に対して $X^{(i)}$ はねじれ Λ 加群であるが Λ 上有限生成ではない．
(3) $\lambda^{(i)} := \mathrm{rank}_{\mathbb{Z}_p} X^{(i)}$ は有限である．

定理 5.2 の $\lambda^{(i)}$ を**第 i 次岩澤 λ 不変量**という（[Oza1, page 68] 参照)．

次の定理 5.3 が尾崎学氏によって与えられた非アーベル岩澤公式である．

定理 5.3 (尾崎 [Oza1, page 68, Theorem 1, page 60, Theorem II], [尾崎, page 319, 定理 3.2] 参照)．$\mathbb{Z}_p$ 拡大 K/k の岩澤 μ 不変量が 0 であると仮定する．このとき，各 $i \geq 2$ に対して，整数 $\nu^{(i)}$ と非負整数 $n_0^{(i)}$ が存在し，$n \geq n_0^{(i)}$ に対して

$$\#X_n^{(i)} = p^{\lambda^{(i)} n + \nu^{(i)}}$$

が成り立つ．$G_n^{(i)}$ の位数については，各 $i \geq 1$ に対して，非負整数 $m_0^{(i)}$ が存在して，$n \geq m_0^{(i)}$ に対して

$$\#G_n^{(i)} = p^{(\sum_{j=1}^{i} \lambda^{(j)})n + \sum_{j=1}^{i} \nu^{(j)}}$$

が成り立つ．

岩澤 μ 不変量が $\mu > 0$ のときは，特殊な $\mathbb{Z}_p$ 拡大について次の定理が成り立つ．

定理 5.4 (尾崎 [Oza1, page 75, Theorem 2], [尾崎, page 320, 定理 3.4] 参照)**.** p を奇素数とする．$\mathbb{Z}_p$ 拡大 K/k が条件

(1) K/k の岩澤加群 X が $(\Lambda/p)^{\oplus\mu}$ と同型（このとき $\mu(K/k)=\mu$)，
(2) K の p 上の素点は唯一つ

を満たすとき，非負整数 $\kappa(K/k)$, n_0 と整数 $\nu^{(2)}(K/k)$ が存在し，$n \geq n_0$ に対して

$$\#X_n^{(2)} = p^{(\frac{\mu p^n-1}{2}\mu)p^n-\kappa(K/k)p^n+\nu^{(2)}(K/k)}$$

が成り立つ.

$\lambda^{(i)}$ については次の定理が成り立つ.

定理 5.5 (尾崎 [Oza1, page 85, Proposition 7], [尾崎, page 323, 命題 4.3], [Iwa2] 参照)**.** k を有限次代数体とする．p は k で完全分解し，$\mathbb{Z}_p$ 拡大 K/k で p 上の素点はすべて分岐すると仮定する．また，r_1, r_2 をそれぞれ k の実無限素点，複素無限素点の個数とする．このとき,

$$\lambda^{(1)} \geq r_2, \quad \lambda^{(2)} \geq \frac{r_2(r_2-1)}{2} - (r_1+r_2)$$

が成り立つ．特に $\lambda^{(1)}$, $\lambda^{(2)}$ が随意に大きくなるような K/k が存在する.

5.3 $G_{K,\varnothing}(p)$ について

定理 5.6 (水澤-尾崎 [MO, page 450, Theorem 2], [尾崎, page 324, 定理 5.3] 参照)**.** $k=\mathbb{Q}(\sqrt{-m})$ を虚 2 次体（m は平方因子を持たない正の奇数)，k_∞/k を円分 $\mathbb{Z}_2$ 拡大とする．p, q, q', q'' を素数とするとき，$G = G_{k_\infty,\varnothing}(2)$ がアーベル群となるための必要十分条件は以下のいずれかが成り立つことである：

(1)（$G=1$）$m=1$ または $m=q\equiv 3 \pmod 8$;
(2)（$G\simeq\mathbb{Z}/2\mathbb{Z}$）$m=p\equiv 5 \pmod 8$;
(3)（$G\simeq\mathbb{Z}_2$）$m=pq$, $p\equiv 5$, $q\equiv 3 \pmod 8$ または $m=q\equiv 7 \pmod{16}$;
(4)（$G\simeq\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}_2$）$m=qq'$, $q\equiv q'\equiv 3 \pmod 8$ または $m=p\equiv 9 \pmod{16}$, $2^{\frac{p-1}{4}}\equiv 1 \pmod p$;
(5)（$G\simeq\mathbb{Z}_2^{\oplus 2}$）$m=qq'q''$, $q\equiv q'\equiv q''\equiv 3 \pmod 8$ または $m=pq$, $p\equiv 9 \pmod{16}$, $q\equiv 3 \pmod 8$, $2^{\frac{p-1}{4}}\equiv 1 \pmod p$;

(6) ($G \simeq \mathbb{Z}_2^{\oplus 3}$) $m = q \equiv 15 \pmod{32}$．さらに k_∞/k の岩澤多項式 $P(T)$ について $P(-1) \equiv 1 \pmod 4$.

注意 5.7. 虚 2 次体 $\mathbb{Q}(\sqrt{-m})$, $\mathbb{Q}(\sqrt{-2m})$ は同じ円分 $\mathbb{Z}_2$ 拡大を持つ（[福田 2, page 128] 参照）．このことから，定理 5.6 はすべての虚 2 次体について，G がアーベル群となるための必要十分条件を述べていることになる．

定理 5.8 (岡野 [Oka, pages 363–364, Theorem 1.1], [尾崎, page 324, 定理 5.4] 参照)**.** k を虚 2 次体，p を奇素数とし，k_∞/k を円分 $\mathbb{Z}_p$ 拡大とする．このとき，$G = G_{k_\infty,\varnothing}(p)$ がアーベル群になるための必要十分条件は以下のいずれかが成り立つことである：

(1) ($G = 1$ または $G \simeq \mathbb{Z}_p$) k_∞/k の岩澤 λ 不変量 $\lambda(k_\infty/k)$ が 1 以下である；
(2) ($G \simeq \mathbb{Z}_p \oplus \mathbb{Z}_p$) $\lambda(k_\infty/k) = 2$ かつ k のイデアル類群の p 部分が p 上の素イデアルの冪を含む類たちで生成される（言い換えると，k 上の不分岐アーベル p 拡大で k の p 上の素点がすべて完全分解するようなものは自明な拡大以外に存在しない）.

$G_{k_\infty,\varnothing}(p)$ の構造が決定可能であり，非アーベル群になる例として以下が知られている．

定理 5.9 (水澤 [Miz2, page 94, Theorem 1], [Miz3, page 118, Theorem 2.1, Theorem 2.2], [尾崎, page 326, 定理 5.7] 参照)**.**

(1) p_1, p_2, q を $p_1 \equiv p_2 \equiv 5 \pmod 8$, $q \equiv 3 \pmod 8$ である相異なる素数とし，$\left(\dfrac{p_1p_2}{q}\right) = -1$, $\left(\dfrac{p_1}{p_2}\right) = 1$ と仮定する．さらに $\mathbb{Q}(\sqrt{p_1p_2})$ の基本単数の $\mathbb{Q}$ へのノルムが 1 であると仮定する．このとき，$k = \mathbb{Q}(\sqrt{p_1p_2q})$ 上の円分 $\mathbb{Z}_2$ 拡大 k_∞/k について
$$G_{k_\infty,\varnothing}(2) \simeq D_{2^m}$$
が成り立つ．ここで D_{2^m} は位数 2^m の正 2 面体群であり，$m \geq 3$ は 2^{m-2} が $\mathbb{Q}(\sqrt{p_1p_2})$ の類数の 2 部分となるような整数である．
(2) $k = \mathbb{Q}(\sqrt{-m})$, $0 < m \equiv 1 \pmod 4$ は平方因子を持たないとする．さらに，円分 $\mathbb{Z}_2$ 拡大 k_∞/k の λ 不変量が 1 であると仮定する．このとき，
$$G_{k_\infty,\varnothing}(2) \simeq \langle a, b \mid bab^{-1} = a^{-1},\, a^{2d} = 1\rangle^{\text{pro-2}}$$
が成り立つ．ここで $d < \infty$ は $\mathbb{Q}(\sqrt{m})$ の円分 $\mathbb{Z}_2$ 拡大の岩澤加群の位数である．
(3) q_1, q_2 を $q_1 \equiv 3 \pmod 8$, $q_2 \equiv 7 \pmod{16}$ である素数とする．このとき， $k =$

$\mathbb{Q}(\sqrt{-q_1q_2})$ 上の円分 $\mathbb{Z}_2$ 拡大 k_∞ について

$$G_{k_\infty,\varnothing}(2) \simeq \langle a,b,c \mid bab^{-1}=a^{-1},\ [b,c]=a^2,\ [a,c]=1\rangle^{\text{pro-2}}$$

が成り立つ.

5.4 今後について

4.3 節において水澤靖氏によって作成された Iwapoly.gp を用い，虚 2 次体の円分 $\mathbb{Z}_3$ 拡大の岩澤 λ 不変量と岩澤多項式を調べた．今回の計算では叶わなかったが，$\lambda_3(k) \geq 15$ となる λ 不変量を見つけ出し，また，どのような条件で λ 不変量が大きくなるのかなどについて考察したい．さらに，Iwapoly.gp では 3 以外の素数 p に対する円分 $\mathbb{Z}_p$ 拡大についても計算することができるので，より広範囲な計算を試してみたい．

また，藤井俊氏から，例 4.18 において k_n のイデアル類群の 3 部分が計算できるのではないかという指摘をいただいたが，そのことを本論文に反映させるまでに至れなかった．[田谷/福田, 5.1 節] などを参考にして，理解と考察をさらに深めていきたい．

5 章に関連する話題として，Mizusawa [Miz4] にも興味を抱いたので，こちらも読み進めていきたい．

参考文献

[青木] 青木 美穂，p 進ゼータ関数 久保田-レオポルドから岩澤理論へ，日本評論社，2019，192 ページ.

[足立] 足立 恒雄，ガロア理論講義 [増補版]，日本評論社，2003，248 ページ.

[市村] 市村 文男，岩澤理論入門，都立大学数学教室セミナー報告，1996，72 ページ.

[伊藤] 伊藤 剛司，有限生成 Λ 加群の構造定理，2003 年度整数論サマースクール「岩澤理論」報告集，5–26，
https://www.sci.u-toyama.ac.jp/~iwao/SS2003/#abstracts.

[尾崎] 尾崎 学，Z_p-拡大の非アーベル岩澤理論—概説と展望（Non-abelian Iwasawa theory of Z_p-extensions—overview and outlook），Algebraic number theory and related topics 2014，数理解析研究所講究録別冊，B64, (2017), 313–330,
http://hdl.handle.net/2433/243676.

[落合] 落合 理，岩澤理論とその展望（上），岩波書店，2014，196 ページ.

[黒川/栗原/斎藤] 黒川 信重，栗原 将人，斎藤 毅，数論 II 岩澤理論と保型形式，岩波書店，2005，254 ページ.

[斎藤] 斎藤 秀司，整数論，共立出版株式会社，1997，248 ページ.

[田谷/福田] 田谷 久雄，福田 隆，岩澤不変量の計算，日本応用数理学会論文誌，Vol. 12，2002，293–306.

[ノイキルヒ] J. ノイキルヒ，代数的整数論（足立恒雄監修，梅垣敦紀訳），丸善出版，2012，600 ページ.

[半内] 半内 広貴，Galois コホモロジーの類体論における諸問題への応用について，新潟大学大学院自然科学研究科修士論文，2022，
http://mathweb.sc.niigata-u.ac.jp/~hoshi/HannaiNiigataMasterThesis2022.pdf.

[福田 1] 福田 隆，岩澤による p-進 L-函数の構成の応用 (I) 岩澤不変量の決定，2003 年度整数論サマースクール「岩澤理論」報告集，123–129，
https://www.sci.u-toyama.ac.jp/~iwao/SS2003/#abstracts.

[福田 2] 福田 隆，重点解説 岩澤理論 理論から計算まで，サイエンス社，2019，216 ページ.

[藤井] 藤井 俊，岩澤類数公式，2003 年度整数論サマースクール「岩澤理論」報告集，27–52，
https://www.sci.u-toyama.ac.jp/~iwao/SS2003/#abstracts.

[星] 星 明考，群論序説，日本評論社，2016，280 ページ．

[水澤] 水澤 靖，Iwapoly.gp （PARI/GP のプログラム），
https://researchmap.jp/read0206718/published_works.

[雪江 1] 雪江 明彦，整数論 2 代数的整数論の基礎，日本評論社，2013，336 ページ．

[雪江 2] 雪江 明彦，整数論 3 解析的整数論への誘い，日本評論社，2014，312 ページ．

[GS] E. S. Golod, I. R. Šafarevič, *On the class field tower*, Izv. Akad. Nauk SSSR Ser. Mat. **28** (1964), 261–272.

[Ito] T. Itoh, *On the structure of the Galois group of the maximal pro-p extension with restricted ramification over the cyclotomic $\mathbb{Z}_p$-extension*, Tokyo J. Math. **43** (2020), 181–204.

[Iwa1] K. Iwasawa, *On Γ-extensions of algebraic number fields*, Bull. Amer. Math. Soc. **65** (1959), 183–226.

[Iwa2] K. Iwasawa, *On $\mathbf{Z}_l$-extensions of algebraic number fields*, Ann. of Math. (2) **98** (1973), 246–326.

[Miz1] Y. Mizusawa, *Notes on computing Iwasawa polynomials by PARI/GP*,
https://researchmap.jp/read0206718/published_works.

[Miz2] Y. Mizusawa, *On the maximal unramified pro-2-extension of $\mathbb{Z}_2$-extensions of certain real quadratic fields II*, Acta Arith. **119** (2005), 93–107.

[Miz3] Y. Mizusawa, *On the maximal unramified pro-2-extension over the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field*, J. Théor. Nombres Bordeaux **22** (2010), 115–138.

[Miz4] Y. Mizusawa, *On metabelian 2-class field towers over $\mathbb{Z}_2$-extensions of real quadratic fields*, Canad. Math. Bull. **65** (2022), 795–805.

[MO] Y. Mizusawa, M. Ozaki, *Abelian 2-class field towers over the cyclotomic $\mathbb{Z}_2$-extensions of imaginary quadratic fields*, Math. Ann. **347** (2010), 437–453.

[NSW] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields*, Second edition, Grundlegren Math. Wiss., 323, Springer-Verlag, Berlin, 2008, xvi+825 pp.

[Oka] K. Okano, *Abelian p-class field towers over the cyclotomic $\mathbb{Z}_p$-extensions of imaginary quadratic fields*, Acta Arith. **125** (2006), 363–381.

[Oza1] M. Ozaki, *Non-abelian Iwasawa theory of $\mathbb{Z}_p$-extensions*, J. Reine Angew. Math. **602** (2007), 59–94.

[Oza2] M. Ozaki, *Construction of maximal unramified p-extensions with prescribed Galois groups*, Invent. Math. **183** (2011), 649–680.

[PARI1] The PARI Group, PARI/GP version `2.13.2`, Univ. Bordeaux, 2021, `http://pari.math.u-bordeaux.fr/`.

[PARI2] The PARI Group, *User's Guide to PARI/GP* (*version* 2.13.2), Univ. Bordeaux, 2021, `http://pari.math.u-bordeaux.fr/`.

[Ser] J-P. Serre, *Classes des corps cyclotomiques* (*d'après K. Iwasawa*), Séminaire Bourbaki, Vol. 5, Exp. No. 174, 83–93, Société Mathématique de France, Paris, 1995.

[Was] L. C. Washington, *Introduction to Cyclotomic Fields*, Second edition, Springer-Verlag, New York, 1997, xiv+487 pp.

追記（2024 年 3 月 8 日）

福田隆先生に修士論文を見ていただき，アドバイスをいただくことができた．ここに感謝申し上げます．特に `subcycloiwasawa` を教えていただけたので，星先生に研究室のコンピュータを用いてもらうことで，より高速に計算を行なうことができた．（`subcycloiwasawa` は PARI/GP [PARI3], [PARI4], [PARI5] の最新版で利用できる．[PARI6] も参照してほしい．）以下に `subcycloiwasawa` で得られた結果を紹介する．$\lambda_3(k) \geq 8$ なる $k = \mathbb{Q}(\sqrt{-m})$ $(1 \leq m \leq 10^6$: 平方因子を持たない$)$ を計算してみると，次の表 2 が得られる．これは 4.3 節の Iwapoly.gp による結果と一致している．

表 2　$\lambda_3(k) \geq 8$ となる $k = \mathbb{Q}(\sqrt{-m})$ の個数 $(1 \leq m \leq 10^6$: 607926 個中$)$

$\lambda = \lambda_3(k)$	8	9	10	11	12	13	14	計
#	142	45	19	6	1	0	1	214

$\lambda_3(k) \geq 8$ なる $k = \mathbb{Q}(\sqrt{-m})$ $(1 \leq m \leq 10^7$: 平方因子を持たない$)$ を計算してみると，次の表 3 が得られる．これは [田谷/福田, 5.1 節] による結果と一致している．

表 3　$\lambda_3(k) \geq 8$ となる $k = \mathbb{Q}(\sqrt{-m})$ の個数 $(1 \leq m \leq 10^7$: 6079291 個中$)$

$\lambda = \lambda_3(k)$	8	9	10	11	12	13	14	計
#	1486	473	175	64	11	6	5	2220

さらに `subcycloiwasawa` による計算を続けていくことで，次の表 4，表 5，表 6 を得ることができた．

表 4　$\lambda_3(k) \geq 8$ となる $k = \mathbb{Q}(\sqrt{-m})$ の個数 $(10^7 \leq m \leq 2 \cdot 10^7$: 6079284 個中$)$

$\lambda = \lambda_3(k)$	8	9	10	11	12	13	14	計
#	1422	445	177	60	13	5	1	2123

表 5　$\lambda_3(k) \geq 8$ となる $k = \mathbb{Q}(\sqrt{-m})$ の個数 $(2 \cdot 10^7 \leq m \leq 3 \cdot 10^7$: 6079254 個中$)$

$\lambda = \lambda_3(k)$	8	9	10	11	12	13	14	15	16	計
#	1470	522	159	67	18	4	1	4	1	2246

表 6　$\lambda_3(k) \geq 8$ となる $k = \mathbb{Q}(\sqrt{-m})$ の個数 $(3 \cdot 10^7 \leq m \leq 4 \cdot 10^7 : 6079224$ 個中)

$\lambda = \lambda_3(k)$	8	9	10	11	12	13	14	15	計
#	1521	508	175	52	14	5	3	1	2279

$\lambda_3(k) = 17$ となる $k = \mathbb{Q}(\sqrt{-m})$ も計算を進めれば見つかるだろうと予想している．m を動かしたとき $\lambda = \lambda_3(k)$ に上界があるのかについては見当もつかないが，いくらでも大きい λ が存在するのではないかと思っている．

Iwapoly.gp を用い，$1 \leq m \leq 4 \cdot 10^7$ の範囲で $\lambda_3(k) \geq 15$ となる 6 個の $k = \mathbb{Q}(\sqrt{-m})$ について計算すると以下のようになる．

```
gp > Iwapoly(3,20526146,6,1)
time = 14h, 10min, 46,906 ms.
[x^15 + 51*x^14 + 15*x^13 + 48*x^11 + 21*x^10 + 54*x^9 + 9*x^8 + 27*x^
7 + 18*x^6 + 78*x^5 + 12*x^4 + 48*x^3 + 54*x^2 + 36*x, 4]
gp > Iwapoly(3,22485319,6,1)
time = 4h, 29,578 ms.
[x^15 + 6*x^14 + 60*x^13 + 75*x^12 + 60*x^11 + 12*x^10 + 21*x^9 + 33*x
^8 + 27*x^7 + 78*x^6 + 30*x^5 + 45*x^4 + 66*x^3 + 27*x^2 + 24*x + 63, 4]
gp > Iwapoly(3,26113301,6,1)
time = 14h, 14min, 19,172 ms.
[x^15 + 39*x^14 + 24*x^13 + 39*x^12 + 57*x^11 + 12*x^10 + 36*x^9 + 6*x
^8 + 72*x^7 + 18*x^6 + 36*x^5 + 57*x^4 + 9*x^3 + 72*x^2 + 60*x, 4]
gp > Iwapoly(3,26761961,6,1)
time = 14h, 37min, 16,062 ms.
[x^16 + 15*x^15 + 27*x^14 + 27*x^13 + 9*x^12 + 3*x^11 + 72*x^10 + 15*x
^9 + 30*x^8 + 57*x^7 + 36*x^6 + 57*x^5 + 63*x^4 + 18*x^3 + 6*x^2 + 51*
x, 4]
gp > Iwapoly(3,29856379,6,1)
time = 5h, 9min, 18,265 ms.
[x^15 + 54*x^14 + 45*x^13 + 60*x^12 + 51*x^11 + 18*x^10 + 42*x^9 + 18*
x^8 + 42*x^7 + 3*x^6 + 66*x^5 + 36*x^4 + 66*x^3 + 12*x^2 + 60*x + 12,
4]
```

```
gp > Iwapoly(3,35695991,6,1)
time = 6h, 15min, 5,970 ms.
[x^15 + 18*x^14 + 75*x^13 + 51*x^12 + 18*x^11 + 12*x^10 + 42*x^9 + 57*
x^8 + 66*x^7 + 69*x^6 + 12*x^5 + 72*x^4 + 42*x^3 + 18*x^2 + 39*x, 4]
```

5 章と同じように，この計算からわかることを例としてまとめておく．

例 A.1.

(1) $k = \mathbb{Q}(\sqrt{-20526146})$ の円分 $\mathbb{Z}_3$ 拡大に対して $\lambda = \lambda_3(k) = 15$ であり，岩澤多項式 $P(x)$ について

$$P(x) \equiv x^{15} + 51x^{14} + 15x^{13} + 48x^{11} + 21x^{10} + 54x^9 + 9x^8 + 27x^7 + 18x^6 + 78x^5 + 12x^4 + 48x^3 + 54x^2 + 36x \pmod{3^4}.$$

(2) $k = \mathbb{Q}(\sqrt{-22485319})$ の円分 $\mathbb{Z}_3$ 拡大に対して $\lambda = \lambda_3(k) = 15$ であり，岩澤多項式 $P(x)$ について

$$P(x) \equiv x^{15} + 6x^{14} + 60x^{13} + 75x^{12} + 60x^{11} + 12x^{10} + 21x^9 + 33x^8 + 27x^7 + 78x^6 + 30x^5 + 45x^4 + 66x^3 + 27x^2 + 24x + 63 \pmod{3^4}.$$

(3) $k = \mathbb{Q}(\sqrt{-26113301})$ の円分 $\mathbb{Z}_3$ 拡大に対して $\lambda = \lambda_3(k) = 15$ であり，岩澤多項式 $P(x)$ について

$$P(x) \equiv x^{15} + 39x^{14} + 24x^{13} + 39x^{12} + 57x^{11} + 12x^{10} + 36x^9 + 6x^8 + 72x^7 + 18x^6 + 36x^5 + 57x^4 + 9x^3 + 72x^2 + 60x \pmod{3^4}.$$

(4) $k = \mathbb{Q}(\sqrt{-26761961})$ の円分 $\mathbb{Z}_3$ 拡大に対して $\lambda = \lambda_3(k) = 16$ であり，岩澤多項式 $P(x)$ について

$$P(x) \equiv x^{16} + 15x^{15} + 27x^{14} + 27x^{13} + 9x^{12} + 3x^{11} + 72x^{10} + 15x^9 + 30x^8 + 57x^7 + 36x^6 + 57x^5 + 63x^4 + 18x^3 + 6x^2 + 51x \pmod{3^4}.$$

(5) $k = \mathbb{Q}(\sqrt{-29856379})$ の円分 $\mathbb{Z}_3$ 拡大に対して $\lambda = \lambda_3(k) = 15$ であり，岩澤多項式 $P(x)$ について

$$P(x) \equiv x^{15} + 54x^{14} + 45x^{13} + 60x^{12} + 51x^{11} + 18x^{10} + 42x^9 + 18x^8 + 42x^7 + 3x^6 + 66x^5 + 36x^4 + 66x^3 + 12x^2 + 60x + 12 \pmod{3^4}.$$

(6) $k=\mathbb{Q}(\sqrt{-35695991})$ の円分 $\mathbb{Z}_3$ 拡大に対して $\lambda=\lambda_3(k)=15$ であり，岩澤多項式 $P(x)$ について

$$P(x)\equiv x^{15}+18x^{14}+75x^{13}+51x^{12}+18x^{11}+12x^{10}+42x^9+57x^8+66x^7 \\ +69x^6+12x^5+72x^4+42x^3+18x^2+39x \pmod{3^4}.$$

追記（2024 年 3 月 25 日）

その後，さらに `subcycloiwasawa` による計算を続けていくことで，次の表 7 を得ることができた．もし今後の研究の役に立つようであれば，大変嬉しく思います．

表 7　$\lambda_3(k)\geq 8$ となる $k=\mathbb{Q}(\sqrt{-m})$ の個数 ($4\cdot 10^7\leq m\leq 5\cdot 10^7$: 6079291 個中)

$\lambda=\lambda_3(k)$	8	9	10	11	12	13	14	計
#	1623	489	180	48	15	8	2	2365

参考文献

[PARI3] The PARI Group, PARI/GP version `2.15.4` (Stable 64-bit version), Univ. Bordeaux, 2023, `http://pari.math.u-bordeaux.fr/`.

[PARI4] The PARI Group, PARI/GP version `2.16.1` (Development 64-bit version), Univ. Bordeaux, 2024, `http://pari.math.u-bordeaux.fr/`.

[PARI5] The PARI Group, PARI/GP latest version (64-bit version), Univ. Bordeaux, 2024 (March), `http://pari.math.u-bordeaux.fr/pub/pari/windows/snapshots/gp64-gmp-git-latest.exe`.

[PARI6] Karim Belabas, PARI/GP Atelier (13/01/2022) [Tutorial] The subcyclo package, 2022, `https://pari.math.u-bordeaux.fr/Events/PARI2022/talks/subcyclo.pdf`.