

# 学位論文

Generalized Pell's equations and  
symmetrized poly-Bernoulli polynomials  
(拡張ペル方程式と対称化多重ベルヌーイ多項式)

2024年3月

吉崎彪雅

# Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	Generalized Pell's equations and Weber's class number problem . . . . .	3
1.2	Bijjective enumerations for symmetrized poly-Bernoulli polynomials . . .	6
<b>2</b>	<b>Generalized Pell's equations and Weber's class number problem</b>	<b>10</b>
2.1	Classical method . . . . .	10
2.2	Generalized Pell's equation . . . . .	11
2.2.1	Algebraic aspects of $X_n$ . . . . .	12
2.2.2	New continued fraction . . . . .	12
2.2.3	$\mathbb{Z}[X_{n-1}]$ -solutions . . . . .	16
2.3	Weber's class number problem . . . . .	16
2.3.1	Some known results . . . . .	18
2.3.2	Proof of Theorem 2.3.5 . . . . .	19
2.4	Results on the explicit unit $\epsilon_n$ . . . . .	20
2.4.1	The minimality of $\epsilon_n$ in $RE_n^+$ . . . . .	20
2.4.2	Observations on the sizes of $\epsilon_n$ . . . . .	23
2.5	The ratios of the class numbers . . . . .	25
2.6	The $p$ -adic limits of class numbers in $\mathbb{Z}_p$ -towers . . . . .	27
2.7	Global fields . . . . .	29
2.8	3-manifolds . . . . .	31
2.9	Alternative proofs . . . . .	33
2.10	Cyclic resultants . . . . .	35
2.10.1	Signatures . . . . .	35
2.10.2	$p$ -adic convergence . . . . .	35
2.10.3	Explicit formula . . . . .	37
2.11	Knots . . . . .	39
2.11.1	Alexander polynomial and Fox–Weber's formula . . . . .	40
2.11.2	Torus knots . . . . .	40
2.11.3	Twist knots . . . . .	41
2.11.4	Livingston's results . . . . .	47
2.12	Algebraic curves . . . . .	48
2.12.1	A formula for function fields . . . . .	49
2.12.2	Elliptic curves . . . . .	50

<b>3</b>	<b>Bijjective enumerations for symmetrized poly-Bernoulli polynomials</b>	<b>56</b>
3.1	A bijection between two combinatorial models . . . . .	56
3.1.1	Double Callan permutations . . . . .	56
3.1.2	Alternative tableaux . . . . .	58
3.1.3	A combinatorial bijection . . . . .	59
3.2	A sequence of bijections . . . . .	61
3.2.1	Packed alternative tableaux . . . . .	61
3.2.2	Double alternative trees . . . . .	62
3.3	Further combinatorial models and weights . . . . .	65
3.3.1	Excedance set of permutations . . . . .	65
3.3.2	Another proof by a combinatorial bijection . . . . .	68
3.4	An application and remarks . . . . .	70
3.4.1	Combinatorial explanation of the duality . . . . .	70
3.4.2	Concluding remarks . . . . .	71

# Chapter 1

## Introduction

This thesis consists of two chapters except for this chapter. Chapter 2 gives a new approach to Weber's class number problem that asks whether specific infinitely many number fields have the class number 1. Chapter 3 studies a combinatorial aspect of some special polynomials in number theory. This thesis consists of the author's three works [95], [96] (Chapter 2), and [30] (Chapter 3).

### 1.1 Generalized Pell's equations and Weber's class number problem

A number field is a finite extension over the rational number field  $\mathbb{Q}$ . The ring of integers of a number field is the set of roots in the number field of monic polynomials with integer coefficients. The ring of integers is a generalization of the ring of rational integers  $\mathbb{Z}$ . Indeed the ring of integers of the rational number field is the ring of rational integers. The ring of rational integers has a very important property, the uniqueness of the prime factorization. However, the uniqueness of the prime factorization no longer holds for the ring of integers in general. This fact was a major difficulty in the early days of the study of the Fermat conjecture. The class number is an invariant of a number field that determines whether the ring of integers has the uniqueness of the prime factorization. The class number is defined by the size of the ideal class group, that is, the quotient group of the group of fractional ideals and the group of principal ideals of the number field. It is well-known that the class number of a number field is 1 if and only if the ring of integers has the uniqueness of the prime factorization. Against this background, the class number has long attracted attention as a major research subject in number theory. However, the simple and important question of how many number fields of class number 1 exist is unsolved at the granularity of finite or infinite. Weber's class number problem (conjecture) asks whether specific infinitely many number fields have the class number 1. Let  $p$  be a prime number. Let  $\mathbb{Z}_p$  denote the ring of  $p$ -adic integers. A  $\mathbb{Z}_p$ -extension over a number field is an infinite Galois extension whose Galois group is isomorphic to the additive group  $\mathbb{Z}_p$  as topological groups. The statement of Weber's

problem is as follows.

**Problem 1.1.1.** *Determine the class number of each intermediate field in the  $\mathbb{Z}_2$ -extension over  $\mathbb{Q}$ . Is the class number of any intermediate field 1?*

For odd prime numbers  $p$ , similar problems have also been studied for  $\mathbb{Z}_p$ -extensions over  $\mathbb{Q}$ . Therefore, such problems are sometimes collectively referred to as Weber's problem. In Chapter 2, up to Section 2.5, we deal only with the case  $p = 2$ , and from Section 2.6 we deal with all prime numbers. If we describe the intermediate fields of  $\mathbb{Z}_2$ -extension over  $\mathbb{Q}$  from small degree, we have

$$\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{2 + \sqrt{2}}), \mathbb{Q}(\sqrt{2 + \sqrt{2 + \sqrt{2}}}), \dots$$

There are many studies on Weber's problem and we summarize the history here. It all started in 1886, when Weber [92, Theorem C] proved that the class number of all intermediate fields are odd, and calculated the class numbers of the first, second, and third intermediate fields. The fourth and subsequent ones require computer power, the fourth was calculated by Bauer [6, Ergebnis] and Masley [47, Theorem 3.2], the fifth by Linden [86, Theorem 1], and the sixth, the most recent, was calculated by Miller [54, Theorem 2.1] in 2014. In that paper, Miller also computed up to the seventh (in [54, Theorem 2.2]), assuming the generalized Riemann hypothesis. These methods first calculate the upper bound of prime numbers that may divide the class numbers, and then verify that each prime number below the upper bound does not divide the class numbers, using the analytic class number formula, the class field theory, and other methods. Since the upper bound increases with the degree of number fields, this method cannot hope to solve the Weber's problem. Recent studies have focused on the properties of prime numbers that do not divide the class numbers of the intermediate fields. By measuring the "size" of a special unit, Horie [32, Theorem 3] gave a congruence condition for prime numbers that do not divide the class numbers of all intermediate fields. Horie's method was refined by Morisawa–Okazaki [55, Corollary B], and it is now proved that all prime numbers that are not congruent to 1,  $-1$  modulo 64 do not divide the class numbers of all intermediate fields. By make use of generalized Bernoulli numbers, Fukuda–Komatsu [24, Theorem 1.2] proved that for each prime number  $p$  there exists a positive integer  $m$  satisfies that if  $p$  does not divide the class number of the  $m$ th intermediate field, then  $p$  does not divide the class numbers of all intermediate fields. Moreover Fukuda–Komatsu [24, Section 3] developed the algorithm which verifies a given prime number does not divide the class number of a given intermediate field. By using the algorithm, it is now proved that all prime numbers less than  $10^9$  do not divide the class numbers of all intermediate fields. These are all strong results that provide convincing affirmation of the Weber's conjecture. However, all of them require the help of a computer, and a complete solution to Weber's conjecture with these methods is also difficult. Therefore, new methods are needed to promote Weber's conjecture.

In this thesis, we study Weber's problem from another point of view from previous studies. Set  $X_n = 2 \cos(2\pi/2^{n+2})$  for each  $n \geq 0$ . Then we have

$$X_1 = \sqrt{2}, \quad X_2 = \sqrt{2 + \sqrt{2}}, \quad X_3 = \sqrt{2 + \sqrt{2 + \sqrt{2}}}, \dots \quad (1.1)$$

Weber's problem follows from the  $\mathbb{Z}[X_{n-1}]$ -solutions of the equation

$$x^2 - X_n^2 y^2 = 1 \quad (1.2)$$

(see Section 2.3). In the case of  $n = 1$ , Eq. (1.2) becomes  $x^2 - 2y^2 = 1$ . In general, for a non-square positive integer  $m$ , the equation  $x^2 - my^2 = 1$  is called Pell's equation. There is a one-to-one corresponding between the solutions of Pell's equation and a subgroup of the group of units of  $\mathbb{Q}(\sqrt{m})$ . By Dirichlet's unit theorem, there is a generator of such a subgroup, and we call the corresponding solution a fundamental solution. There is a classical algorithm to find a fundamental solution of Pell's equation by using the regular continued fraction expansion of  $\sqrt{m}$ . We note that the algorithm is based on the theory of approximation, which is called the best approximation theorem.

Our strategy for solving Eq. (1.2) is to imitate the aforementioned classical algorithm. We summarize our results as follows.

- By generalizing the classical continued fraction expansion algorithm, we obtain a new continued fraction expansion of  $X_n$  over  $\mathbb{Z}[X_{n-1}]$  (Definition 2.2.1 and Theorem 2.2.4).
- We conjecture that our new continued fraction gives a *generator* of Eq. (1.2), and we show that the conjecture is equivalent to Weber's conjecture (Conjecture 2.2.6 and Theorem 2.3.5).
- By using the element that is given by our new continued fraction, we show that the sequence of class numbers converges in  $\mathbb{Z}_2$  (Theorem 2.5.1).

The last result is a special case of H. Kisilevsky's work ([40, Corollary 2]). We rediscover Kisilevsky's result by a different proof (Theorem 2.7.1). Moreover we show that the  $p$ -adic convergence of the certain analogues of the class numbers also holds for 3-manifolds in the spirit of arithmetic topology (Theorem 2.8.1). It is natural to consider that the analogues of the ideal class groups of number fields in 3-manifolds are the first homology groups. Then the analogues of the class numbers are the sizes of the torsion parts of the first homology groups. We also call the sizes of the torsion parts of the first homology groups the class numbers of 3-manifolds. The analogues of  $\mathbb{Z}_p$ -extensions are the system of  $p$ -power cyclic covers of 3-manifolds. Then we call the system of  $p$ -power cyclic covers of the 3-manifolds  $\mathbb{Z}_p$ -covers of the 3-manifolds.

In the latter half of Chapter 2 (from Section 2.6), we study the  *$p$ -adic limits of class numbers*. Our results are summarized as follows.

- We show that the sequences of the class numbers of the intermediate fields in  $\mathbb{Z}_p$ -extensions over global fields converge in  $\mathbb{Z}_p$  (Theorem 2.7.1, this is a rediscovery of [40, Corollary 2]).
- We show that the sequences of the class numbers of the subcoverings in  $\mathbb{Z}_p$ -covers over compact 3-manifolds converge in  $\mathbb{Z}_p$  (Theorem 2.8.1).
- We show that the sequences of the  $p$ -power cyclic resultants of integer coefficients polynomials converge in  $\mathbb{Z}_p$  (Theorem 2.10.3).
- We get the formula of the  $p$ -adic limits of the  $p$ -power cyclic resultants (Theorem 2.10.7).

Here the cyclic resultant of polynomial  $f(t)$  is defined by

$$\text{Res}(t^n - 1, f(t)) = \prod_{\zeta^n=1} f(\zeta)$$

for each positive integer  $n$ . By Fox–Weber’s formula, the class number of the cyclic coverings of  $S^3$  branched along knots can be computed by the cyclic resultants of the Alexander polynomials of the knots. It is also well-known that the class numbers of the constant extensions of function fields can be computed by the cyclic resultants of the Frobenius polynomials of the algebraic curves correspond to the base fields. Therefore, we can calculate the  $p$ -adic limits of the class numbers numerically for the  $\mathbb{Z}_p$ -covers of  $S^3$  branched along knots and the constant  $\mathbb{Z}_p$ -extensions of function fields. We position a study of the  $p$ -adic limits as a variant of Weber’s problem and obtain the following results.

- We determine when the  $p$ -adic limits are 1 for the constant  $\mathbb{Z}_p$ -extensions over function fields of genus 1 (Proposition 2.12.8 and Proposition 2.12.10).
- We determine when the  $p$ -adic limits are 1 for the  $\mathbb{Z}_p$ -covers over  $S^3$  branched along twist knots (Corollary 2.11.11).

## 1.2 Bijective enumerations for symmetrized poly-Bernoulli polynomials

For each non-negative integer  $n$ , the Bernoulli number  $B_n$  is a rational number defined by a recurrence formula

$$\sum_{i=0}^n \binom{n+1}{i} B_i = n+1$$

where  $\binom{n}{i}$  denotes binomial coefficients. There are various generalizations of the Bernoulli number, each of which has been studied in a variety of way. For example, the generalized Bernoulli number played an important role in the history of Weber’s problem ([24,

Theorem 1.2]). The poly-Bernoulli number has also been studied from a combinatorial perspective. In Chapter 3, we study the symmetrized poly-Bernoulli polynomial which is a generalization of the poly-Bernoulli number. We summarize some properties of the poly-Bernoulli number and the history of a combinatorial study. For each integer  $k$  and non-negative integer  $n$ , Kaneko [36] defined the poly-Bernoulli number  $B_n^{(k)}$  as the coefficient of the series

$$\frac{\text{Li}_k(1 - e^{-x})}{1 - e^{-x}} = \sum_{n=0}^{\infty} B_n^{(k)} \frac{x^n}{n!}$$

where  $\text{Li}_k(t)$  denotes the poly-logarithm series

$$\text{Li}_k(z) = \sum_{i=1}^{\infty} \frac{z^i}{i^k}.$$

Kaneko [36, Theorem 2] showed that for every positive integer  $n, k$ , we have

$$B_n^{(-k)} = B_k^{(-n)}.$$

This interesting property is called the duality of the poly-Bernoulli number. Poly-Bernoulli numbers also have the explicit formula and satisfy the recurrence relation. We note that in the case of  $k < 0$ ,  $B_n^{(k)}$  is a positive integer. Since Brewbaker [14] and Launois [44] pointed out that poly-Bernoulli numbers appear in enumeration problems, poly-Bernoulli numbers have been studied from a combinatorial viewpoint (see [8]). For example, Brewbaker found that the number of specific matrices (lonesum matrix) coincides with a poly-Bernoulli number, and the duality follows very naturally from this perspective.

Just as the Bernoulli polynomial is defined from the Bernoulli number, the poly-Bernoulli polynomial is also defined from the poly-Bernoulli number;

$$e^{-xt} \frac{\text{Li}_k(1 - e^{-t})}{1 - e^{-t}} = \sum_{n=0}^{\infty} B_n^{(k)}(x) \frac{t^n}{n!}.$$

Since  $B_n^{(k)}(0) = B_n^{(k)}$  the duality also holds for the special values in  $x = 0$  of poly-Bernoulli polynomials. In fact, the duality also holds for  $x = 1$  by the following form;

$$B_n^{(-k-1)}(1) = B_k^{(-n-1)}(1).$$

However, it no longer holds for  $x \geq 2$ . Kaneko–Sakurai–Tsumura [37, Corollary 2.2] showed that a weighted sum of special values of poly-Bernoulli polynomials

$$\mathcal{B}_n^{(-k)}(m) := \sum_{j=0}^m \binom{m}{j} B_m^{-k-j}(m)$$

satisfies the duality

$$\mathcal{B}_n^{(-k)}(m) = \mathcal{B}_k^{(-n)}(m)$$



for each positive integer  $n$ ,  $k$  and non-negative integer  $m$ . Here,  $\begin{bmatrix} n \\ j \end{bmatrix}$  is the Stirling number of the first kind (see [2, Section 2.1]). Since  $\mathcal{B}_n^{(-k)}(0) = B_n^{(-k)}(0) = B_n^{(-k)}$  and  $\mathcal{B}_n^{(-k)}(1) = B_n^{(-k-1)}(1)$ , this is a generalization of the duality of the poly-Bernoulli polynomial. They also defined a polynomial

$$\widehat{\mathcal{B}}_n^k(x) = \sum_{j=0}^{\min(n,k)} j!(x+1)^{\bar{j}} \begin{Bmatrix} n+1 \\ j+1 \end{Bmatrix} \begin{Bmatrix} k+1 \\ j+1 \end{Bmatrix} \in \mathbb{Z}[x]. \quad (1.3)$$

Here,  $\begin{Bmatrix} n \\ j \end{Bmatrix}$  is the Stirling number of the second kind, and  $(x+1)^{\bar{j}} = (x+1)(x+2)\cdots(x+j)$  is the rising factorial. This is the (normalized) *symmetrized poly-Bernoulli polynomial*. We note that  $\widehat{\mathcal{B}}_n^k(m) = \mathcal{B}_n^{(-k)}(m)/m!$ . By definition, the coefficients of symmetrized poly-Bernoulli polynomials are non-negative integers. Therefore, it is natural to ask about their combinatorial meanings.

Recently, Bényi–Matsusaka [11] introduced two combinatorial objects to answer this question. Inspired by their research, we provide further combinatorial aspects for the symmetrized poly-Bernoulli polynomial. Furthermore, we answer some Bényi–Matsusaka’s problems left unsolved. First, we recall the two combinatorial objects, (barred) Callan sequences  $\mathcal{C}_n^k$  and alternative tableaux  $\mathcal{T}_n^k$  in Section 3.1. Bényi–Matsusaka [11] showed that both of these objects define the same polynomial  $\widehat{\mathcal{B}}_n^k(x)$ . However their proof is indirect due to using recurrence relations and it is unsolved to give a ”combinatorial” proof. We success to present two types of combinatorial bijections between the combinatorial models of Bényi–Matsusaka. By using our bijections, we give a combinatorial proof of Bényi–Matsusaka’s result.

To state our results more precisely, we introduce the following.

**Definition 1.2.1.** For a pair  $(\mathcal{P}, w)$  of a finite set of combinatorial objects and a weight function  $w : \mathcal{P} \rightarrow \mathbb{Z}_{\geq 0}$ , we define the polynomial

$$\mathcal{P}(x) = \mathcal{P}(x; w) = \sum_{\lambda \in \mathcal{P}} x^{w(\lambda)}.$$

Let  $(\mathcal{P}_1, w_1)$  and  $(\mathcal{P}_2, w_2)$  be two such pairs. A function  $f : \mathcal{P}_1 \rightarrow \mathcal{P}_2$  is called a *bijection between  $(\mathcal{P}_1, w_1)$  and  $(\mathcal{P}_2, w_2)$*  if  $f$  is bijective and satisfies  $w_2(f(\lambda)) = w_1(\lambda)$  for any  $\lambda \in \mathcal{P}_1$ .

If there exists a bijection between  $(\mathcal{P}_1, w_1)$  and  $(\mathcal{P}_2, w_2)$ , then we obtain the equation  $\mathcal{P}_1(x; w_1) = \mathcal{P}_2(x; w_2)$ . In Section 3.1.3, we construct a direct bijection  $(\mathcal{C}_n^k, w_{\mathcal{C}}^{\text{lr}}) \rightarrow (\mathcal{T}_n^k, w_{\mathcal{T}}^{\text{st}})$ , where  $w_{\mathcal{C}}^{\text{lr}}$  and  $w_{\mathcal{T}}^{\text{st}}$  are weight functions introduced in [11]. In Section 3.2, we give another bijection  $(\mathcal{T}_n^k, w_{\mathcal{T}}^{\text{st}}) \rightarrow (\mathcal{C}_n^k, w_{\mathcal{C}}^{\text{lr}})$  via a sequence of bijections.

Throughout this Chapter 3, we provide various combinatorial objects and weights. The following table lists the models considered herein.

Section	$(\mathcal{P}, w)$
Section 3.1	$(\mathcal{C}_n^k, w_{\mathcal{C}}^{\text{lr}}), (\mathcal{T}_n^k, w_{\mathcal{T}}^{\text{st}})$
Section 3.2.1	$(\mathcal{T}_n^k, w_{\mathcal{T}}^{\leftarrow}), (\tilde{\mathcal{T}}_n^k, w_{\tilde{\mathcal{T}}}^{\leftarrow})$
Section 3.2.2	$(\mathcal{G}_n^k, w_{\mathcal{G}}^{\text{ch}}), (\mathcal{C}_n^k, w_{\mathcal{C}}^{\text{br}})$
Section 3.3.1	$(\mathcal{E}_n^k, w_{\mathcal{E}}^{\text{lr}})$
Section 3.3.2	$(\mathcal{C}_n^k, w_{\mathcal{C}}^{\text{RL}})$
Section 3.4.1	$(\tilde{\mathcal{T}}_n^k, w_{\tilde{\mathcal{T}}}^{\downarrow})$

Summarizing the results (Theorems 3.1.5, 3.1.9, 3.1.13, 3.2.1, 3.2.6, 3.2.7, 3.3.4 and 3.3.7) in Chapter 3, we have the following.

- The polynomials  $\mathcal{P}(x; w)$  defined from the above nine combinatorial models all coincide with the symmetrized poly-Bernoulli polynomial  $\widehat{\mathcal{B}}_n^k(x)$ .

As we can see from (1.3),  $\widehat{\mathcal{B}}_n^k(x)$  satisfies the duality  $\widehat{\mathcal{B}}_n^k(x) = \widehat{\mathcal{B}}_k^n(x)$ . However the duality does not follow immediately from the combinatorial models of Bényi–Matsusaka. As an application of our results, we explain the duality combinatorially in Section 3.4.1.

# Chapter 2

## Generalized Pell's equations and Weber's class number problem

### 2.1 Classical method

We briefly recall the classical method for Pell's equation (see [59, Ch.7, §7.8] for detail). For a non-square positive integer  $m$ , we consider Pell's equation

$$x^2 - my^2 = 1. \tag{2.1}$$

By mapping  $(x, y)$  to  $x + \sqrt{m}y$ , the solutions of Pell's equation are embedded in  $\mathbb{Z}[\sqrt{m}]$ , and we set  $P_m$  its image. Since  $P_m$  forms a subgroup of the multiplicative group  $\mathbb{Z}[\sqrt{m}]^*$  and has a torsion element  $-1$ ,  $P_m$  is isomorphic to  $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$  by Dirichlet's unit theorem. A *fundamental solution* of Pell's equation is defined as a corresponding solution to a generator of  $P_m/(\mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}$ . It is classically known that a fundamental solution is given by the regular continued fraction of  $\sqrt{m}$ .

Let

$$[a_0, a_1, a_2, \dots] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ddots}}$$

be a continued fraction ( $a_i \in \mathbb{Z}$ ). Let  $p_{-1} = 1, p_0 = a_0$  and  $q_{-1} = 0, q_0 = 1$ . For a positive integer  $k$ , we define  $p_k$  and  $q_k$  as follows:

$$p_k = a_k p_{k-1} + p_{k-2},$$

$$q_k = a_k q_{k-1} + q_{k-2}.$$

Then, it holds  $p_k/q_k = [a_0, \dots, a_k]$ , and the rational number  $p_k/q_k$  is called the  $k$ -th convergent of the continued fraction. It is well-known that the regular continued fraction expansion of  $\sqrt{m}$  is of the form

$$\sqrt{m} = [a_0, \overline{a_1, \dots, a_l}] := [a_0, a_1, \dots, a_l, a_1, \dots, a_l, \dots]$$

and  $l$  is called the period of  $\sqrt{m}$  if we take the minimal  $l$ . Then we obtain a fundamental solution of Pell's equation

$$(p, q) = \begin{cases} (p_{l-1}, q_{l-1}) & (l: \text{even}) \\ (p_{2l-1}, q_{2l-1}) & (l: \text{odd}). \end{cases}$$

In Section 2.4.2, we observe a characterization of a fundamental solution of Eq. (1.2). For comparison, we explain why the regular continued fraction expansion of  $\sqrt{m}$  gives a fundamental solution. A solution  $(a, b)$  is a fundamental solution if and only if

$$|\log |a + \sqrt{mb}|| = \min\{|\log |x + \sqrt{my}|| \mid x, y \in \mathbb{Z}, x^2 - my^2 = 1\}, \quad (2.2)$$

or equivalently,

$$|a| = \min\{|x| \in \mathbb{Z} \mid x \neq 1, x^2 - my^2 = 1\}.$$

On the other hand, the regular continued fraction of  $\sqrt{m}$  gives a best approximation to  $\sqrt{m}$  in the following sense.

**Definition 2.1.1** (best approximation, cf. [42, p.9]). Let  $\alpha$  be an irrational number. A best approximation to  $\alpha$  is a rational number  $p/q$  ( $q > 0$ ) such that for any rational number  $p'/q' \neq p/q$  with  $1 \leq q' \leq q$ , we have

$$|q\alpha - p| < |q'\alpha - p'|.$$

**Theorem 2.1.2** (cf. [42, Theorem 6]). *All of best approximations to an irrational number  $\alpha$  are convergents of the regular continued fraction expansion of  $\alpha$ .*

Let  $(x, y) \neq (\pm 1, 0)$  be a solution of the Eq. (2.1) with  $x/y > 0$ . Then  $x/y$  satisfies

$$\left| \sqrt{m} - \frac{x}{y} \right| < \frac{1}{2y^2}. \quad (2.3)$$

If a rational number satisfies the inequality (2.3), then the rational number is a best approximation to  $\sqrt{m}$  (cf. [42, Corollary 2]). Thus we see that  $x/y$  is a convergent of  $\sqrt{m}$ , and there exists an integer  $n$  such that  $x/y = p_n/q_n$ . By the theory of continued fraction, if the period  $l$  of the regular continued fraction expansion of  $\sqrt{m}$  is even (resp. odd), then  $l - 1$  (resp.  $2l - 1$ ) is the index of the convergent which has the smallest numerator in the set of convergents that can be solutions to Eq. (2.1), that is,  $(p_{l-1}, q_{l-1})$  (resp.  $(p_{2l-1}, q_{2l-1})$ ) is a fundamental solution.

## 2.2 Generalized Pell's equation

We study the generalized Pell's equation

$$x^2 - X_n^2 y^2 = 1$$

with the  $\mathbb{Z}[X_{n-1}]$ -solutions by imitating the classical method. We obtained a continued fraction expansion of  $X_n$  over  $\mathbb{Z}[X_{n-1}]$  by a new algorithm. First, we prepare the algebraic property of  $X_n$ .

### 2.2.1 Algebraic aspects of $X_n$

For non-negative integer  $n$ , set  $\mathbb{B}_n = \mathbb{Q}(X_n)$ . Since  $X_n = \zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1}$  we see that  $\mathbb{B}_n$  is the maximal real subfield of  $\mathbb{Q}(\zeta_{2^{n+2}})$  where  $\zeta_{2^{n+2}} := \exp(2\pi\sqrt{-1}/2^{n+2})$ . By the theory of cyclotomic field (see [90, Ch.2] in detail), we have that  $\mathbb{B}_n$  is an algebraic number field of degree  $2^n$ , and Galois extension over  $\mathbb{Q}$  with Galois group  $\mathbb{Z}/2^n\mathbb{Z}$ , and the ring of integers of  $\mathbb{B}_n$  is  $\mathbb{Z}[X_n]$ . We see that  $\mathbb{B}_n$  is a relative quadratic extension over  $\mathbb{B}_{n-1}$ .

### 2.2.2 New continued fraction

We define a new continued fraction expansion algorithm over  $\mathbb{Z}[X_{n-1}]$ . For  $n \geq 1$ , we set  $\beta_0 = 1$  and  $\beta_k = 2 \cos(k\pi/2^n)$  for each  $1 \leq k \leq 2^{n-1} - 1$ . Then,

$$\mathcal{B}_{n-1} = \{\beta_k \mid k = 0, 1, \dots, 2^{n-1} - 1\} \quad (2.4)$$

is an integral basis of  $\mathbb{Z}[X_{n-1}]$ . By embedding

$$\phi_n : \mathbb{B}_{n-1} \longrightarrow \mathbb{R}^{2^{n-1}}; a \mapsto (\tau(a))_{\tau \in \text{Gal}(\mathbb{B}_{n-1}/\mathbb{Q})},$$

the basis  $\mathcal{B}_{n-1}$  is orthogonal in  $\mathbb{R}^{2^{n-1}}$  (cf. [56, Lemma 6.3]), and  $\mathbb{Z}[X_{n-1}]$  forms a complete lattice in  $\mathbb{R}^{2^{n-1}}$ . Recall  $X_n = \sqrt{2 + X_{n-1}}$ . We define

$$\phi_n(X_n) = (\sqrt{2 + \tau(X_{n-1})})_{\tau \in \text{Gal}(\mathbb{B}_{n-1}/\mathbb{Q})}$$

and extend  $\phi_n$  to

$$\phi_n : \mathbb{B}_n \rightarrow \mathbb{R}^{2^{n-1}}; a + X_n b \mapsto \phi_n(a) + \phi_n(X_n)\phi_n(b)$$

for each  $a, b \in \mathbb{B}_{n-1}$  where the sum and the multiplication are component-wise. For each  $x \in \mathbb{R}$ , let  $\text{round}(x)$  denote the integer in  $(x - 1/2, x + 1/2]$ . We note that for each  $\alpha \in \mathbb{B}_n$ , there are unique  $r_k \in \mathbb{R}$  such that  $\phi_n(\alpha) = \sum_{k=0}^{2^{n-1}-1} r_k \phi_n(\beta_k)$ .

**Definition 2.2.1.** For  $\alpha \in \mathbb{B}_n$  such that  $\phi_n(\alpha) = \sum_{k=0}^{2^{n-1}-1} r_k \phi_n(\beta_k)$ , we define  $\lfloor \alpha \rfloor = \sum_{k=0}^{2^{n-1}-1} \text{round}(r_k) \beta_k \in \mathbb{Z}[X_{n-1}]$  and the sequence  $(a_k)_{k \geq 0}$  as

$$\begin{aligned} \alpha_0 &= \alpha, a_0 = \lfloor \alpha_0 \rfloor, \\ \alpha_m &= (\alpha_{m-1} - a_{m-1})^{-1}, a_m = \lfloor \alpha_m \rfloor \quad (m \geq 1). \end{aligned}$$

If  $\alpha_{m-1} \in \mathbb{Z}[X_{n-1}]$  then  $a_{m-1} = \alpha_{m-1}$  and  $\alpha_m$  is not defined.

**Remark 2.2.2.** By the orthogonality of  $\phi_n(\mathcal{B}_{n-1})$ ,  $\phi_n(\lfloor \alpha \rfloor)$  is one of the closest points to  $\phi_n(\alpha)$  in  $\phi_n(\mathbb{Z}[X_{n-1}])$  for Euclidean distance of  $\mathbb{R}^{2^{n-1}}$ .

Before stating the next proposition, we note that  $1 + X_{n-1} \in \mathbb{Z}[X_{n-1}]$  is a unit. It will be explained in Section 2.3.

**Proposition 2.2.3.** *Let  $\alpha = X_n \in \mathbb{B}_n$ . Then we have*

$$\begin{aligned} a_0 &= 1, \\ a_{2k-1} &= 2(1 + X_{n-1})^{-1}, \\ a_{2k} &= 2 \end{aligned}$$

for positive integers  $k$ .

*Proof.* By Remark 2.2.2, it suffices to show that  $\phi_n(0)$  is

- (a) a unique closest point to  $\phi_n(\sqrt{2 + X_{n-1}} - 1)$  and
- (b) a unique closest point to  $\phi_n((\sqrt{2 + X_{n-1}} - 1)^{-1} - 2(1 + X_{n-1})^{-1}) = \phi_n((1 + \sqrt{2 + X_{n-1}})^{-1})$

in  $\phi_n(\mathbb{Z}[X_{n-1}])$ . For (a), since  $\phi_n(\mathcal{B}_{n-1})$  is orthogonal in  $\mathbb{R}^{2^{n-1}}$  and the lengths of  $\phi_n(\beta_k)$  ( $k = 1, \dots, 2^{n-1} - 1$ ) are  $\sqrt{2^n}$  (see [56, Lemma 6.3]), it is enough to show that

$$(a-1) \quad \|\sqrt{2 + X_{n-1}} - 1 - 0\| < \sqrt{2^n}/2 \text{ and}$$

$$(a-2) \quad \|\sqrt{2 + X_{n-1}} - 1 - 0\| < \|\sqrt{2 + X_{n-1}} - 1 - (\pm 1)\|.$$

(a-1). The left-hand side of the inequality is  $\|\sqrt{2 + X_{n-1}} - 1\| = \sqrt{2^n \mathfrak{A}_n / \pi}$ , where

$$\mathfrak{A}_n := \frac{\pi}{2^n} \sum_{k=1}^{2^{n-1}} \left( 2 \cos \left( \frac{2k-1}{2^{n+1}} \pi \right) - 1 \right)^2 < \int_{-\frac{\pi}{2^{n+1}}}^{\frac{\pi}{2} + \frac{\pi}{2^{n+1}}} (2 \cos x - 1)^2 dx =: I_n.$$

Now  $(I_n)_{n \geq 6}$  is decreasing with  $I_6 = 0.762\dots < \pi/4$  and we can check numerically that  $\mathfrak{A}_n < \pi/4$  for the cases  $1 \leq n \leq 5$ .

(a-2). We show that

$$(a-2-i) \quad \|\sqrt{2 + X_{n-1}} - 1\| < \|\sqrt{2 + X_{n-1}} - 1 - (+1)\| \text{ and}$$

$$(a-2-ii) \quad \|\sqrt{2 + X_{n-1}} - 1\| < \|\sqrt{2 + X_{n-1}} - 1 - (-1)\|.$$

(a-2-i). Transform the inequality as following;

$$\begin{aligned} & \sum_{k=1}^{2^{n-1}} \left( 2 \cos \left( \frac{2k-1}{2^{n+1}} \pi \right) - 1 \right)^2 < \sum_{k=1}^{2^{n-1}} \left( 2 \cos \left( \frac{2k-1}{2^{n+1}} \pi \right) - 2 \right)^2 \\ \Leftrightarrow & \frac{\pi}{2^{n-1}} \sum_{k=1}^{2^{n-1}} \cos \left( \frac{2k-1}{2^{n+1}} \pi \right) < \frac{3}{4}\pi. \end{aligned}$$

Since the proof of the inequality is almost the same as in case (a-1), using a comparison series-integral with  $\cos x$ , we omit it.

(a-2-ii). Similarly, we see that it suffices to show that

$$1 < \frac{8}{2^n} \sum_{k=1}^{2^{n-1}} \cos\left(\frac{2k-1}{2^{n+1}}\pi\right)$$

for  $n \geq 1$ . In fact, we prove a more general case

$$1 < S_N := \frac{4}{N} \sum_{k=1}^N \cos\left(\frac{2k-1}{4N}\pi\right) \quad (N \geq 1).$$

For  $N = 1$ , we have  $S_1 = 4 \cos(\pi/4) = 2\sqrt{2} > 1$ . For  $N \geq 2$ , a comparison series-integral gives that

$$S_N \geq I_N := \frac{8}{\pi} \int_{\frac{\pi}{4N}}^{\frac{2N-1}{4N}\pi} \cos x dx.$$

Since  $I_N = 8/\pi(\cos(\pi/(4N)) - \sin(\pi/(4N)))$  and the function  $x \mapsto \cos x - \sin x$  decreases in  $[0, \pi/4]$ , we have that  $S_N \geq I_N > I_2 > 1$ .

Similarly to the proof of (a), we separate the proof of (b) into (b-1) and (b-2).

(b-1). We show that  $\left\| (1 + \sqrt{2 + X_{n-1}})^{-1} \right\| < \sqrt{2^n}/2$ , which means that

$$\frac{\pi}{2^n} \sum_{k=1}^{2^{n-1}} \left( \frac{1}{2 \cos\left(\frac{2k-1}{2^{n+1}}\pi\right) + 1} \right)^2 < \frac{\pi}{4}.$$

However, in the proof of (b-2-ii), we show that

$$\frac{\pi}{2^n} \sum_{k=1}^{2^{n-1}} \frac{1}{2 \cos\left(\frac{2k-1}{2^{n+1}}\pi\right) + 1} < \frac{\pi}{4}$$

and this implies the statement because  $2 \cos\left(\frac{2k-1}{2^{n+1}}\pi\right) + 1 > 1$  for all  $1 \leq k \leq 2^{n-1}$ .

(b-2). Similarly to the proof of (a-2), we separate the proof into two cases.

(b-2-i). We show that

$$\left\| \left(1 + \sqrt{2 + X_{n-1}}\right)^{-1} \right\| < \left\| \left(1 + \sqrt{2 + X_{n-1}}\right)^{-1} - (-1) \right\|.$$

This is easy because

$$\begin{aligned} & \sum_{k=1}^{2^{n-1}} \left( \left( \frac{1}{2 \cos\left(\frac{2k-1}{2^{n+1}}\pi\right) + 1} + 1 \right)^2 - \left( \frac{1}{2 \cos\left(\frac{2k-1}{2^{n+1}}\pi\right) + 1} \right)^2 \right) \\ &= \sum_{k=1}^{2^{n-1}} \left( 1 + \frac{2}{2 \cos\left(\frac{2k-1}{2^{n+1}}\pi\right) + 1} \right) > 0. \end{aligned}$$

(b-2-ii).  $\left\| (1 + \sqrt{2 + X_{n-1}})^{-1} \right\| < \left\| (1 + \sqrt{2 + X_{n-1}})^{-1} - (+1) \right\|$ . Similarly to the proof of (a-2-i), it suffices to show that

$$\frac{\pi}{2^n} \sum_{k=1}^{2^{n-1}} \frac{1}{2 \cos \left( \frac{2k-1}{2^{n+1}} \pi \right) + 1} < \frac{\pi}{4}.$$

Since the proof of the inequality is almost the same as in case (a-1), using a comparison series-integral with  $1/(2 \cos x + 1)$ , we omit it.  $\square$

Proposition 2.2.3 only provides a formal expansion. We see that it does converge.

**Theorem 2.2.4.** *For  $n \geq 1$  and each  $\tau \in \text{Gal}(\mathbb{B}_{n-1}/\mathbb{Q})$ , we have*

$$\sqrt{2 + \tau(X_{n-1})} = [1, \overline{2(1 + \tau(X_{n-1}))^{-1}}, 2].$$

Here,  $[a_0, a_1, \dots]$  denotes  $a_0 + \frac{1}{a_1 + \dots}$  and  $[a_0, \dots, a_r, \overline{a_{r+1}, \dots, a_s}]$  denotes the periodicity of the part  $a_{r+1}, \dots, a_s$ , namely

$$[a_0, \dots, a_r, \overline{a_{r+1}, \dots, a_s}] = [a_0, \dots, a_r, a_{r+1}, \dots, a_s, a_{r+1}, \dots, a_s, \dots].$$

**Remark 2.2.5.** Theorem 2.2.4 states that the above continued fraction converges in Euclidean space  $\mathbb{R}^{2^{n-1}} \xrightarrow{\phi_n} \mathbb{B}_n$ . Namely we get a continued fraction expansion of  $\sqrt{2 + X_{n-1}}$  over  $\mathbb{Z}[X_{n-1}]$  for each metric induced by  $\tau \in \text{Gal}(\mathbb{B}_{n-1}/\mathbb{Q})$ . We could not make sure whether this algorithm gives a continued fraction expansion of any element of  $\mathbb{B}_n$ , and whether this algorithm terminates for any element of  $\mathbb{B}_{n-1}$ .

*Proof.* If the continued fraction  $[1, \overline{2(1 + \tau(X_{n-1}))^{-1}}, 2]$  converges, then we see that the numerical value of it is  $\sqrt{2 + \tau(X_{n-1})}$  by an easy calculation. We show the convergence of  $[1, \overline{2(1 + \tau(X_{n-1}))^{-1}}, 2]$  for each  $\tau \in \text{Gal}(\mathbb{B}_{n-1}/\mathbb{Q})$ . We check the conditions in [15, Theorem 4.3]. For  $a \in \mathbb{C}$ , we define

$$D(a) = \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix}.$$

For a continued fraction  $[a_1, a_2, \dots, a_k]$ , we define

$$M([a_1, a_2, \dots, a_k]) = D(a_1)D(a_2) \cdots D(a_k).$$

We should check the followings for all  $n \geq 1$  and  $\tau \in \text{Gal}(\mathbb{B}_{n-1}/\mathbb{Q})$ ;

(a)  $M([1, 2(1 + \tau(X_{n-1}))^{-1}, 2, 0, -1, 0]) \neq \pm \begin{pmatrix} 1, 0 \\ 0, 1 \end{pmatrix}$

(b)  $|M([2(1 + \tau(X_{n-1}))^{-1}, 2])_{2,2}| \leq 1$



$$(b') \quad |M([2, 2(1 + \tau(X_{n-1}))^{-1}])_{2,2}| \leq 1$$

$$(c) \quad \text{Tr}(M([1, 2(1 + \tau(X_{n-1}))^{-1}, 2, 0, -1, 0]))^2 \geq 4$$

where  $M_{2,2}$  denotes the  $(2, 2)$ -element of a matrix  $M$ . The first three (a), (b), and (b') are trivial. We note that

$$\text{Tr}(M([1, 2(1 + \tau(X_{n-1}))^{-1}, 2, 0, -1, 0]))^2 = 4(2(1 + \tau(X_{n-1}))^{-1} + 1)^2.$$

If  $\tau(X_{n-1}) > -1$ , then we have  $(2(1 + \tau(X_{n-1}))^{-1} + 1)^2 \geq 1$  and (c) holds. Otherwise, we have that  $-2 < \tau(X_{n-1}) < -1$ . So we have  $(1 + \tau(X_{n-1}))^{-1} < -1$  and an easy calculation shows that (c) holds.  $\square$

In the case  $n = 1$ , the above theorem states that  $\sqrt{2} = [1, \overline{2}, 2]$  and this is a classical continued fraction expansion of  $\sqrt{2}$ .

### 2.2.3 $\mathbb{Z}[X_{n-1}]$ -solutions

By imitating the classical method, we formulate a conjecture for the  $\mathbb{Z}[X_{n-1}]$ -solutions of the generalized Pell's equation. Since the period of  $[1, \overline{2(1 + X_{n-1})^{-1}}, 2]$  is 2, we look at the first convergent

$$\frac{p_1}{q_1} = \frac{1 + 2(1 + X_{n-1})^{-1}}{2(1 + X_{n-1})^{-1}}.$$

It is easy to check that

$$p_1^2 - X_n^2 q_1^2 = 1$$

for all  $n \geq 1$ . We set

$$\epsilon_n = p_1 + X_n q_1.$$

We conjecture that the element  $\epsilon_n$  generates the  $\mathbb{Z}[X_{n-1}]$ -solutions as a Galois module.

**Conjecture 2.2.6.** *The  $\mathbb{Z}[X_{n-1}]$ -solutions of the generalized Pell's equation  $x^2 - X_n^2 y^2 = 1$  is a  $\text{Gal}(\mathbb{B}_n/\mathbb{Q})$ -module generated by  $-1$  and  $\epsilon_n$ , namely,*

$$\{a + X_n b \mid a, b \in \mathbb{Z}[X_{n-1}], a^2 - X_n^2 b^2 = 1\} = \langle -1, \epsilon_n \rangle_{\mathbb{Z}[\text{Gal}(\mathbb{B}_n/\mathbb{Q})]}.$$

## 2.3 Weber's class number problem

At the beginning of this section, we summarize the history of Weber's problem again. For each positive integer  $n$ , we note that  $\mathbb{B}_n$  is the  $n$ -th layer of the  $\mathbb{Z}_2$ -extension over  $\mathbb{Q}$ , that is, the unique intermediate field of degree  $2^n$ . In 1886, H. Weber [92, Theorem C] showed that  $h(\mathbb{B}_n)$  are odd for all positive integers  $n$ . He also showed  $h(\mathbb{B}_n) = 1$  for  $n = 1, 2$ , and 3 by hand calculations.

After Weber's study, the development of computers allowed researchers to determine the class number of  $\mathbb{B}_n$  as below.

- $h(\mathbb{B}_4) = 1$  (Bauer [6, Ergebnis], Masley [47, Theorem 3.2])
- $h(\mathbb{B}_5) = 1$  (Linden [86, Theorem 1])
- $h(\mathbb{B}_6) = 1$  (Miller [54, Theorem 2.1])
- $h(\mathbb{B}_7) = 1$  under Generalized Riemann Hypothesis (Miller [54, Theorem 2.2])

Except for Bauer, they first gave an upper bound of the class number  $h(\mathbb{B}_n)$  by using *the root discriminant* for each  $n$  and then showed that  $h(\mathbb{B}_n)$  is not divisible by prime numbers below that upper bound. The techniques and their difficulties are briefly summarized in the introduction of [54]. We count them as the first approach.

The second approach we present here is to determine prime numbers that do not divide  $h(\mathbb{B}_n)$  for all  $n$ . Fukuda beautifully summarized this approach in his book [23, Chapter 14], which is written in Japanese. See also [26] for similar contents shortly written in English. The explanation below is based on his book.

Horie found that there is a strong relation between a prime number dividing  $h(\mathbb{B}_n)$  and a certain unit in  $\mathbb{B}_n$ . We need some preparations to explain Horie's work. We write  $\zeta_{2^n} = \exp(2\pi\sqrt{-1}/2^n)$  for each  $n \geq 1$ . Take a generator  $\sigma$  of  $\text{Gal}(\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}(\zeta_{2^2})) \cong \mathbb{Z}/2^n\mathbb{Z}$ . For  $\alpha = \sum_{i=0}^{2^{n-1}-1} a_i \zeta_{2^n}^i \in \mathbb{Z}[\zeta_{2^n}]$  ( $a_i \in \mathbb{Z}$ ), we define

$$\alpha_\sigma = \sum_{i=0}^{2^{n-1}-1} a_i \sigma^i \in \mathbb{Z}[\text{Gal}(\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}(\zeta_{2^2}))]. \quad (2.5)$$

For a prime number  $l$ , let  $F_l$  be the decomposition field of  $l$  in the extension  $\mathbb{Q}(\zeta_{2^n})/\mathbb{Q}$  and fix an intermediate field  $F$  of  $\mathbb{Q}(\zeta_{2^n})/F_l$ . Define

$$\eta_n = \tan \frac{\pi}{2^{n+2}} \quad (2.6)$$

for each  $n \geq 1$ . The following Horie's lemma plays a key role in this approach.

**Lemma 2.3.1** (cf. [31, Lemma 2]). *A prime number  $l$  divides  $h(\mathbb{B}_n)/h(\mathbb{B}_{n-1})$  if and only if there is a prime ideal  $\mathfrak{L}$  of  $F$  dividing  $l$  such that  $\sqrt[n]{\eta_n^{\alpha_\sigma}} \in \mathbb{B}_n$  for all  $\alpha \in l\mathfrak{L}^{-1}$ .*

By showing that " $l \mid h(\mathbb{B}_n)/h(\mathbb{B}_{n-1})$  implies  $\sqrt[n]{\eta_n^{\alpha_\sigma}} \in \mathbb{B}_n$ " and estimating a particular size of  $\eta_n$ , Horie deduced a contradiction. He obtained the following.

**Theorem 2.3.2** ([32, Theorem 3]). *If a prime number  $l$  satisfies  $l \not\equiv \pm 1 \pmod{8}$ , then we have  $l \nmid h(\mathbb{B}_n)$  for all  $n \geq 1$ .*

Many researchers have improved Horie's result.

On the other hand, Fukuda–Komatsu [24, Theorem 1.2] showed that for each prime number  $l$  there exists an integer  $m_l$  such that  $l \nmid h(\mathbb{B}_{m_l})$  implies  $l \nmid h(\mathbb{B}_n)$  for all  $n \geq 1$ . They also improved their result in [25, Theorem 1.1]. By computing such  $m_l$  and showing  $l \nmid h(\mathbb{B}_{m_l})$  for small  $l$ , they obtained the following.

**Theorem 2.3.3** ([25, Corollary 1.2]). *If a prime number  $l$  satisfies  $l < 10^9$ , then we have  $l \nmid h(\mathbb{B}_n)$  for all  $n \geq 1$ .*

Consolidating the recent results, we can summarize as following.

**Theorem 2.3.4** ([55, Corollary B]). *If a prime number  $l$  satisfies  $l \not\equiv \pm 1 \pmod{64}$ , then we have  $l \nmid h(\mathbb{B}_n)$  for all  $n \geq 1$ .*

The aim of this section is to prove the following equivalence:

**Theorem 2.3.5.** *Conjecture 2.2.6 is true for all  $n \geq 0$  if and only if Weber's conjecture is true for all  $n \geq 0$ .*

### 2.3.1 Some known results

We prepare some known results. Let  $E_n$  be the group of units of  $\mathbb{B}_n$  and

$$C_n := \left\langle -1, \zeta_{2^{n+2}}^{\frac{1-a}{2}} \frac{1 - \zeta_{2^{n+2}}^a}{1 - \zeta_{2^{n+2}}} \mid a : \text{odd integers such that } 1 < a < 2^{n+1} \right\rangle_{\mathbb{Z}}$$

be its subgroup of cyclotomic units. Then  $(E_n : C_n) = h_n$ , by [90, Lemma 8.1 and Theorem 8.2]. Noticing that 3 is a generator of  $(\mathbb{Z}/2^{n+2}\mathbb{Z})^*/\{\pm 1\}$  and that

$$1 + X_n = \zeta_{2^{n+2}}^{\frac{1-3}{2}} \frac{1 - \zeta_{2^{n+2}}^3}{1 - \zeta_{2^{n+2}}},$$

by [90, Proposition 8.11], we have

$$C_n = \langle 1 + X_n \rangle_{\mathbb{Z}[\text{Gal}(\mathbb{B}_n/\mathbb{Q})]}.$$

We set  $G_{n/n-1} = \text{Gal}(\mathbb{B}_n/\mathbb{B}_{n-1})$  and define  $\sigma_{n/n-1}$  to be the non-trivial element of  $G_{n/n-1}$ . We note that  $\sigma_{n/n-1}(X_n) = -X_n$ . We define a relative norm map by

$$\text{Nr}_{n/n-1} : \mathbb{B}_n \longrightarrow \mathbb{B}_{n-1}; x \mapsto x\sigma_{n/n-1}(x).$$

**Lemma 2.3.6.** *The restrictions  $\text{Nr}_{n/n-1}|_{E_n} : E_n \longrightarrow E_{n-1}$  and  $\text{Nr}_{n/n-1}|_{C_n} : C_n \longrightarrow C_{n-1}$  are well-defined and surjective.*

*Proof.* Let  $\hat{H}^r(G_{n/n-1}, E_n)$  be the  $r$ -th Tate cohomology group. It suffices to show that  $\hat{H}^0(G_{n/n-1}, E_n) = \{1\}$  for the surjectivity of  $\text{Nr}_{n/n-1}|_{E_n} : E_n \longrightarrow E_{n-1}$ . Yokoi [94, Lemma 3] showed that

$$Q(E_n) = \frac{|\hat{H}^0(G_{n/n-1}, E_n)|}{|\hat{H}^1(G_{n/n-1}, E_n)|} = \frac{1}{2}.$$

Therefore, it suffices to show that  $|\hat{H}^1(G_{n/n-1}, E_n)| = 2$ . Let  $H_{n-1}$  be the maximal unramified abelian extension of  $\mathbb{B}_{n-1}$ . Then we have  $\mathbb{B}_n \cap H_{n-1} = \mathbb{B}_{n-1}$  because  $\mathbb{B}_n/\mathbb{B}_{n-1}$

ramifies at the prime ideal lying above 2. Furthermore,  $\mathbb{B}_n/\mathbb{B}_{n-1}$  ramifies at only one prime, then  $\mathbb{B}_n/\mathbb{B}_{n-1}$  satisfies the assumption of [94, Theorem 1]. Thus we have  $h_{n-1} = |\text{Cl}_n^{G_{n/n-1}}|$ . Since we have  $2 \nmid h_{n-1}$  by [92, Theorem C], we get  $|\hat{H}^1(G_{n/n-1}, E_n)| = 2$  by the Corollary of [94, Theorem 2]. Thus we see that  $\text{Nr}_{n/n-1} : E_n \rightarrow E_{n-1}$  is surjective.

Next we consider  $\text{Nr}_{n/n-1}|_{C_n}$ . The presentation  $C_n = \langle 1+X_n \rangle_{\mathbb{Z}[\text{Gal}(\mathbb{B}_n/\mathbb{Q})]}$  and the easy calculations  $\text{Nr}_{n/n-1}(1+X_n) = -1 - X_{n-1}$  and  $\text{Nr}_{n/n-1}((1+X_n)\sigma(1+X_n) \cdots \sigma^{2^{n-1}-1}(1+X_n)) = -1$  show that  $\text{Nr}_{n/n-1} : C_n \rightarrow C_{n-1}$  is well-defined and surjective, where  $\sigma$  is a generator of  $\text{Gal}(\mathbb{B}_n/\mathbb{Q})$ .  $\square$

Set  $RE_n^+ = \ker(\text{Nr}_{n/n-1}|_{E_n})$  throughout this paper. Lemma 2.3.6 implies the following exact sequence:

$$0 \rightarrow RE_n^+/A_n \rightarrow E_n/C_n \rightarrow E_{n-1}/C_{n-1} \rightarrow 0, \quad (2.7)$$

where  $A_n := RE_n^+ \cap C_n$ . By the exact sequence (2.7), Weber's conjecture is equivalent to

$$(RE_n^+ : A_n) = 1 \text{ for all } n \geq 1. \quad (2.8)$$

### 2.3.2 Proof of Theorem 2.3.5

For  $\epsilon \in RE_n^+$ , there exist unique  $a, b \in \mathbb{Z}[X_{n-1}]$  such that  $\epsilon = a + bX_n$  and we have  $\text{Nr}_{n/n-1}(\epsilon) = a^2 - b^2X_n^2$ . Thus we have a bijection;

$$\begin{array}{ccc} RE_n^+ & \longleftrightarrow & \{\text{the solutions of } x^2 - X_n^2y^2 = 1\} \\ \Psi & & \Psi \\ \epsilon = a + X_nb & \longleftrightarrow & (a, b) \end{array}$$

We recall that Conjecture 2.2.6 states

$$\{a + X_nb \mid a, b \in \mathbb{Z}[X_{n-1}], a^2 - X_n^2b^2 = 1\} = \langle -1, \epsilon_n \rangle_{\mathbb{Z}[\text{Gal}(\mathbb{B}_n/\mathbb{Q})]}.$$

Therefore, Conjecture 2.2.6 is equivalent to that  $RE_n^+ = \langle -1, \epsilon_n \rangle_{\mathbb{Z}[\text{Gal}(\mathbb{B}_n/\mathbb{Q})]}$  for all  $n$ . Combining this formulation and (2.8), to prove Theorem 2.3.5, it suffices to prove that

$$A_n = \langle -1, \epsilon_n \rangle_{\mathbb{Z}[\text{Gal}(\mathbb{B}_n/\mathbb{Q})]}.$$

By easy calculation, we have that

$$\epsilon_n = \frac{X_n + 1}{X_n - 1}$$

for each  $n \geq 1$ . Since  $C_n = \langle -1, 1 + X_n \rangle_{\mathbb{Z}[\text{Gal}(\mathbb{B}_n/\mathbb{Q})]}$ , we have  $\epsilon_n \in C_n$  and  $\epsilon_n \in C_n \cap RE_n^+ = A_n$ . Thus we have  $\langle -1, \epsilon_n \rangle_{\mathbb{Z}[\text{Gal}(\mathbb{B}_n/\mathbb{Q})]} \subset A_n$ .

We put  $\widetilde{\text{Nr}}_{n/n-1}|_{C_n} : C_n/\{\pm 1\} \rightarrow C_{n-1}/\{\pm 1\}$ . Let  $\sigma$  be a generator of  $\text{Gal}(\mathbb{B}_n/\mathbb{Q})$ . We note that the basis of  $C_n/\{\pm 1\}$  and  $C_{n-1}/\{\pm 1\}$  are  $\{\sigma(1+X_n), \sigma^2(1+X_n), \dots, \sigma^{2^n-1}(1+$

$X_n\}$  and  $\{\sigma(1 + X_{n-1}), \sigma^2(1 + X_{n-1}), \dots, \sigma^{2^{n-1}-1}(1 + X_{n-1})\}$  respectively. By considering the representation matrix of  $\widetilde{\text{Nr}}_{n/n-1}|_{C_n}$ , we see that the basis of the kernel of  $\widetilde{\text{Nr}}_{n/n-1}|_{C_n}$  is

$$\left\{ \sigma^i \left( \frac{1 + X_n}{1 - X_n} \right), \prod_{j=0}^{2^{n-1}-1} \sigma^j(1 + X_n) \mid i = 1, 2, \dots, 2^{n-1} - 1 \right\}.$$

Since  $\sigma^i \left( \frac{1+X_n}{1-X_n} \right) \in \left\langle -1, \frac{X_n+1}{X_n-1} \right\rangle_{\mathbb{Z}[G_n]}$ , the rest of the proof is showing, for any  $e \in \mathbb{Z}$ , that

$$\prod_{j=0}^{2^{n-1}-1} \sigma^j(1 + X_n)^e \in \left\langle -1, \frac{X_n + 1}{X_n - 1} \right\rangle_{\mathbb{Z}[G_n]}$$

if  $\text{Nr}_{n/n-1} \left( \prod_{j=0}^{2^{n-1}-1} \sigma^j(1 + X_n)^e \right) = 1$ . Such  $e$  is even because

$$\begin{aligned} \text{Nr}_{n/n-1} \left( \prod_{j=0}^{2^{n-1}-1} \sigma^j(1 + X_n)^e \right) &= \left( \prod_{j=0}^{2^{n-1}-1} \sigma^j(1 + X_n) \sigma^{j+2^{n-1}}(1 + X_n) \right)^e \\ &= (-1)^e. \end{aligned}$$

Therefore it suffices to show that  $\prod_{j=0}^{2^{n-1}-1} \sigma^j(1 + X_n)^2 \in \left\langle -1, \frac{X_n+1}{X_n-1} \right\rangle_{\mathbb{Z}[G_n]}$ . Since  $\prod_{j=0}^{2^{n-1}-1} \sigma^j(1 + X_n) = -1$ , we have

$$\prod_{j=0}^{2^{n-1}-1} \sigma^j(1 + X_n)^2 = - \prod_{j=0}^{2^{n-1}-1} \sigma^j \left( \frac{1 + X_n}{1 - X_n} \right) \in \left\langle -1, \frac{X_n + 1}{X_n - 1} \right\rangle_{\mathbb{Z}[G_n]}.$$

Then the assertion follows.

## 2.4 Results on the explicit unit $\epsilon_n$

In this section, first we show the ‘‘minimality’’ of our explicit unit  $\epsilon_n$ . Secondly, from the Galois action on relative units and the explicitness of  $\epsilon_n$ , we obtain a congruence relation formula for the ratios of the class numbers.

### 2.4.1 The minimality of $\epsilon_n$ in $RE_n^+$

For  $n = 1$ ,  $\epsilon_1 = 3 + 2\sqrt{2}$  comes from the continued fraction of  $\sqrt{2}$ . By the classical method, we have that  $\epsilon_1$  generates all the  $\mathbb{Z}$ -solutions of Pell’s equation  $x^2 - 2y^2 = 1$ . This means that  $\epsilon_1$  is ‘‘minimal’’, that is,

$$\epsilon_1^{\frac{l}{m}} \notin RE_1^+ \text{ for any reduced fraction } \frac{l}{m} \text{ with } 0 < \left| \frac{l}{m} \right| < 1.$$

It follows that Weber's conjecture for  $n = 1$  holds true. We show that  $\epsilon_n$  is also "minimal" for  $n \geq 2$ .

**Theorem 2.4.1.**  $\epsilon_n^{\frac{1}{m}} \notin RE_n^+$  for any reduced fraction  $\frac{l}{m}$  with  $0 < |\frac{l}{m}| < 1$ .

*Proof.* Let  $n \geq 2$ . It suffices to show the statement in case  $\frac{l}{m} = \frac{1}{p}$  for each prime  $p$ . We separate the proof into two cases  $p = 2$  or an odd prime.

Suppose  $p = 2$ . If  $\epsilon_n^{1/2} \in RE_n^+ \subset \mathbb{B}_n$ , then its conjugates are also included in  $\mathbb{B}_n$ . For  $\tau \in \text{Gal}(\mathbb{B}_n/\mathbb{Q})$ ,  $\tau\left(\sqrt{\frac{X_n+1}{X_n-1}}\right)^2 = \frac{\tau(X_n)+1}{\tau(X_n)-1}$ . On the other hand, there exists  $\tau \in \text{Gal}(\mathbb{B}_n/\mathbb{Q})$  such that  $0 < \tau(X_n) < 1$ . For such  $\tau$ , we have  $\tau\left(\sqrt{\frac{X_n+1}{X_n-1}}\right)^2 < 0$  and this contradicts the fact that  $\mathbb{B}_n$  is a totally real field. Thus we have  $\epsilon_n^{1/2} \notin RE_n^+$ .

Now assume that  $p \geq 3$ . By [56, Proposition 6.6] for  $n \geq 2$  and  $\pm 1 \neq \delta \in RE_n^+$  we have

$$\text{Tr}_n(\delta^2) \geq 2^n \cdot 17 \quad (2.9)$$

where  $\text{Tr}_n : \mathbb{B}_n \rightarrow \mathbb{Q}$  be the trace map of  $\mathbb{B}_n$ .

Suppose that  $\epsilon_n^{1/p} \in RE_n^+$ . For each  $\tau \in \text{Gal}(\mathbb{B}_n/\mathbb{Q})$ , the conjugate of  $\epsilon_n^{1/p}$  is  $\left(\frac{\tau(X_n+1)}{\tau(X_n-1)}\right)^{1/p}$ . Then we have

$$\text{Tr}_n\left(\epsilon_n^{\frac{2}{p}}\right) = \sum_{k=1}^{2^n} f_p\left(\frac{2k-1}{2^{n+1}}\pi\right), \text{ where } f_p(x) := \left|\frac{2\cos x + 1}{2\cos x - 1}\right|^{\frac{2}{p}}.$$

Since  $|2\cos((2k-1)\pi/2^{n+1}) + 1| < |2\cos((2k-1)\pi/2^{n+1}) - 1|$  for  $k = 2^{n-1} + 1, \dots, 2^n$ , we have  $f_p((2k-1)\pi/2^{n+1}) < 1$  for such  $k$ . Therefore, by using (2.9) it suffices to show that  $\sum_{k=1}^{2^{n-1}} f_p((2k-1)\pi/2^{n+1}) < 2^{n-1} \cdot 17$ .

For  $k = 1, \dots, 2^{n-1}$ , we have

$$\left|\frac{2\cos((2k-1)\pi/2^{n+1}) + 1}{2\cos((2k-1)\pi/2^{n+1}) - 1}\right| > 1.$$

Then we have

$$f_p\left(\frac{2k-1}{2^{n+1}}\pi\right) < f_3\left(\frac{2k-1}{2^{n+1}}\pi\right)$$

for  $p > 3$ . Therefore it suffices to show this in case  $p = 3$ . Thus our goal is to show that

$$\frac{1}{2^n} \sum_{k=1}^{2^{n-1}} f_3\left(\frac{2k-1}{2^{n+1}}\pi\right) < \frac{17}{2}$$

for  $n \geq 2$ . Let  $K$  be the integer satisfying  $(2K-1)\pi/2^{n+1} < \pi/3 < (2K+1)\pi/2^{n+1}$ .

We write

$$\begin{aligned} \frac{1}{2^n} \sum_{k=1}^{2^{n-1}} f_3 \left( \frac{2k-1}{2^{n+1}} \pi \right) &= \frac{1}{2^n} \sum_{k=1}^{K-1} f_3 \left( \frac{2k-1}{2^{n+1}} \pi \right) + \frac{1}{2^n} f_3 \left( \frac{2K-1}{2^{n+1}} \pi \right) \\ &+ \frac{1}{2^n} f_3 \left( \frac{2K+1}{2^{n+1}} \pi \right) + \frac{1}{2^n} \sum_{k=K+2}^{2^{n-1}} f_3 \left( \frac{2k-1}{2^{n+1}} \pi \right). \end{aligned} \quad (2.10)$$

A comparison series-integral gives that

$$\begin{aligned} \frac{\pi}{2^n} \sum_{k=1}^{K-1} f_3 \left( \frac{2k-1}{2^{n+1}} \pi \right) + \frac{\pi}{2^n} \sum_{k=K+2}^{2^{n-1}} f_3 \left( \frac{2k-1}{2^{n+1}} \pi \right) \\ < \int_0^{\pi/3} f_3(x) dx + \int_{\pi/3}^{\pi/2} f_3(x) dx = 6.4669\dots \end{aligned} \quad (2.11)$$

We used a computer for the last integral calculations.

Finally, we claim that

$$\frac{1}{2^n} f_3 \left( \frac{2K-1}{2^{n+1}} \pi \right) + \frac{1}{2^n} f_3 \left( \frac{2K+1}{2^{n+1}} \pi \right) < 3.$$

for  $n \geq 2$ . Indeed, the continuous function defined for nonzero  $x$  by  $x \mapsto x \frac{2 \cos(\pi/3+x)+1}{2 \cos(\pi/3+x)-1}$  is increasing from  $-\pi$  to 0 on  $[-\pi/3, \pi/3] \setminus \{0\}$ . So we have  $f_3(\pi/3+x) \leq (\pi/|x|)^{2/3}$  on  $[-\pi/3, \pi/3] \setminus \{0\}$ . Set  $r = 2^{n+1} + 3 - 6K$ . So we see that  $r \in \{1, 5\}$ ,  $\frac{2K-1}{2^{n+1}} \pi = \frac{\pi}{3} - \frac{r}{3 \cdot 2^{n+1}} \pi$  and  $\frac{2K+1}{2^{n+1}} \pi = \frac{\pi}{3} + \frac{6-r}{3 \cdot 2^{n+1}} \pi$ . Since  $\frac{5}{3 \cdot 2^{n+1}} \pi < \frac{\pi}{3}$  for  $n \geq 2$ , we obtain that

$$\begin{aligned} \frac{1}{2^n} f_3 \left( \frac{2K-1}{2^{n+1}} \pi \right) + \frac{1}{2^n} f_3 \left( \frac{2K+1}{2^{n+1}} \pi \right) \\ \leq \frac{1}{2^n} \left( \frac{\pi}{\frac{1}{3 \cdot 2^{n+1}} \pi} \right)^{2/3} + \frac{1}{2^n} \left( \frac{\pi}{\frac{5}{3 \cdot 2^{n+1}} \pi} \right)^{2/3} \\ = 2^{\frac{2-n}{3}} \left( 3^{\frac{2}{3}} + \left( \frac{3}{5} \right)^{\frac{2}{3}} \right) < 3 \end{aligned} \quad (2.12)$$

for  $n \geq 2$ . Thus we have the claim and the assertion holds.  $\square$

**Remark 2.4.2.** For  $n = 2$ , we also show that  $h_2 = 1$  by a similar method used above. Let  $\sigma$  be a generator of  $\text{Gal}(\mathbb{B}_2/\mathbb{Q})$ . Since  $h_1 = 1$ , we have  $h_2 = (RE_2^+ : A_2)$ . We recall that  $A_2 = \langle -1, \epsilon_2 \rangle_{\mathbb{Z}[\text{Gal}(\mathbb{B}_2/\mathbb{Q})]}$  and note that  $(RE_2^+ : A_2) < \infty$ . We should show that  $\epsilon_2^x \cdot \sigma(\epsilon_2)^y \notin RE_2^+$  for any  $x, y \in [-1/2, 1/2] \cap \mathbb{Q}$  except for  $x = y = 0$ . If  $\epsilon_2^x \cdot \sigma(\epsilon_2)^y \in \mathbb{B}_2$ , then we have

$$\text{Tr}_2(\epsilon_2^{2x} \cdot \sigma(\epsilon_2)^{2y}) = \sum_{i=1}^4 \sigma^i(\epsilon_2)^{2x} \cdot \sigma^{i+1}(\epsilon_2)^{2y}.$$

Now we define a function  $f_2(x, y) = \text{Tr}_2(\epsilon_2^{2x} \cdot \sigma(\epsilon_2)^{2y})$  on  $[-1/2, 1/2]^2$ . Since  $\frac{\partial^2 f_2}{\partial x^2}(x, y)$  (resp.  $\frac{\partial^2 f_2}{\partial y^2}(x, y)$ )  $> 0$  for each  $y$  (resp.  $x$ )  $\in [-1/2, 1/2]^2$  and  $f_2(\pm 1/2, 0) = f_2(0, \pm 1/2) < f_2(\pm 1/2, \pm 1/2)$ , the maximum of  $f_2(x, y)$  is taken at the points  $(\pm 1/2, \pm 1/2)$ . We have  $f_2(\pm 1/2, \pm 1/2) = 28 < 2^2 \cdot 17$ . This contradicts (2.9), so we have  $RE_2^+ = A_2$  and  $h_2 = 1$ .

## 2.4.2 Observations on the sizes of $\epsilon_n$

In this section, by imitating the classical Pell's equation, we observe some "sizes" of the explicit unit  $\epsilon_n$  and state the conjecture on the minimality of  $\epsilon_n$ . By assuming the conjecture, we give an upper bound for  $k_n$  for small  $n$ . Let  $\sigma$  be a generator of  $\text{Gal}(\mathbb{B}_n/\mathbb{Q})$ . By embedding  $l_n : RE_n^+ \rightarrow \mathbb{R}^{2^{n-1}}; \epsilon \mapsto (\log |\sigma^i(\epsilon)|)_i$ ,  $l_n(RE_n^+)$  forms a complete lattice in  $\mathbb{R}^{2^{n-1}}$ . For a positive integer  $p$ , let  $\|x\|_p = (\sum_{i=1}^{2^{n-1}} |x_i|^p)^{1/p}$  denote the  $L^p$  norm of  $x$  in  $\mathbb{R}^{2^{n-1}}$ .

**Definition 2.4.3** ( $L^p$ -minimal). Let  $S$  be a subset of  $RE_n^+$ . For  $\epsilon \in S \setminus \{\pm 1\}$ , if  $l_n(\epsilon)$  has a minimal  $L^p$  norm in  $l_n(S \setminus \{\pm 1\})$ , then  $\epsilon$  is said to be  $L^p$ -minimal in  $S$ .

We note that this definition is independent of the choice of a generator  $\sigma$  of  $\text{Gal}(\mathbb{B}_n/\mathbb{Q})$ . In the case of  $n = 1$ , if  $\epsilon \in RE_1^+$  corresponds to a fundamental solution, then  $\epsilon$  is  $L^p$ -minimal in  $RE_1^+$  (cf. (2.2)) for any  $p$ . For  $p = 1, 2$ , we conjecture the  $L^p$ -minimality of  $\epsilon_n$  in  $RE_n^+$  as an analogue of the case  $n = 1$ .

**Conjecture 2.4.4.** For all  $n$ ,  $\epsilon_n$  is  $L^1$  and  $L^2$ -minimal in  $RE_n^+$ .

We observe that our explicit unit  $\epsilon_n$  is  $L^2$ -minimal in  $A_n$  for  $1 \leq n \leq 10$  by using Fincke–Pohst algorithm (qfminim command in PARI/GP). Since  $A_n = RE_n^+$  for  $1 \leq n \leq 6$ , we obtain that  $\epsilon_n$  is  $L^2$ -minimal in  $RE_n^+$  for  $1 \leq n \leq 6$ . For each  $\epsilon \in RE_n^+$ , we see that  $\|l_n(\epsilon)\|_1 = \log(\prod_{i=1}^{2^n} \max\{1, |\sigma^i(\epsilon)|\})$ , and the value in log is called the Mahler measure of algebraic numbers. Morisawa and Okazaki [56] investigate  $RE_n^+$  by using the Mahler measure, and obtained a lower bound for  $l_n(RE_n^+ \setminus \{\pm 1\})$  in  $L^1$  norm as  $2^{n-1} \log(2 + \sqrt{5})$  (cf. [56, Lemma 3.2 and Theorem 5.3]). They also obtained a lower bound in  $L^2$  norm as  $\sqrt{2^{n-1}} \log(2 + \sqrt{5})$  (cf. [55, Lemma 2.5 (1)]). Note that these two lower bounds are processed into forms that fit our definitions. We compare  $\|l_n(\epsilon_n)\|_p$  and lower bounds for small  $n$  in Table 2.1.

In the following, by assuming that Conjecture 2.4.4 holds, we give upper bounds of  $h_n/h_{n-1}$  for small  $n$ . Let  $m$  be a positive integer. For a Lebesgue measurable set  $S$  in  $\mathbb{R}^m$ ,  $\text{vol}(S)$  denote the volume of  $S$  in Lebesgue measure on  $\mathbb{R}^m$ . For a complete lattice  $L \subset \mathbb{R}^m$  with a basis  $\mathbf{b} = \{b_1, \dots, b_m\}$ , we define the volume of  $L$  by the volume of the fundamental parallel body of  $\mathbf{b}$ , namely,  $\text{vol}(L) = |\det([b_1 \dots b_m])|$ . Then we have

$$(RE_n^+ : A_n) = \text{vol}(l_n(A_n)) / \text{vol}(l_n(RE_n^+)). \quad (2.13)$$

We use the following Blichfeldt's theorem. Note that the following statement is processed into our settings.



$n$	$\ l_n(\epsilon_n)\ _1$	$2^{n-1} \log(2 + \sqrt{5})$	$\ l_n(\epsilon_n)\ _2$	$\sqrt{2^{n-1}} \log(2 + \sqrt{5})$
1	1.76...	1.44...	1.76...	1.44...
2	3.22...	2.88...	2.35...	2.04...
3	6.28...	5.77...	3.54...	2.88...
4	12.47...	11.54...	5.04...	4.08...
5	24.89...	23.09...	7.20...	5.77...
6	49.76...	46.19...	10.22...	8.16...
7	99.52...	92.39...	14.48...	11.54...

Table 2.1: Comparison of  $\|l_n(\epsilon_n)\|_p$  and lower bounds

**Theorem 2.4.5** (cf. [13, Theorem II, III]). *There exist  $\epsilon, \delta \in RE_n^+ \setminus \{\pm 1\}$  such that*

$$\|l_n(\epsilon)\|_2 \leq \sqrt{\frac{2}{\pi}} \Gamma(2 + 2^{n-2})^{1/2^{n-1}} \text{vol}(l_n(RE_n^+))^{1/2^{n-1}}$$

and

$$\|l_n(\delta)\|_1 \leq \sqrt{\frac{2^n}{\pi}} \Gamma(2 + 2^{n-2})^{1/2^{n-1}} \text{vol}(l_n(RE_n^+))^{1/2^{n-1}},$$

where  $\Gamma$  is the gamma function.

Conjecture 2.4.4 implies that  $\epsilon_n$  satisfies these inequalities. Thus we have

$$\frac{\text{vol}(l_n(A_n))}{\text{vol}(l_n(RE_n^+))} \leq \frac{\text{vol}(l_n(A_n)) \sqrt{2^n/\pi}^{2^{n-1}} \Gamma(2 + 2^{n-2})}{\|l_n(\epsilon_n)\|_1^{2^{n-1}}} \quad (2.14)$$

and

$$\frac{\text{vol}(l_n(A_n))}{\text{vol}(l_n(RE_n^+))} \leq \frac{\text{vol}(l_n(A_n)) \sqrt{2/\pi}^{2^{n-1}} \Gamma(2 + 2^{n-2})}{\|l_n(\epsilon_n)\|_2^{2^{n-1}}}. \quad (2.15)$$

We compute the numerical values of the right-hand sides of (2.14) and (2.15) for each  $n \leq 7$  in Table 2.2. Combining the table at  $p = 2$  and the fact that each prime factor

$n \setminus p$	1	2
1	1.06...	1.06...
2	1.35...	1.27...
3	2.51...	1.55...
4	14.44...	4.89...
5	4345.05...	417.77...
6	17992212754.52...	147730099.26...
7	14822653597271460343569281399.70...	876387598588509574855259.98...

Table 2.2: Upper bounds for  $h_n/h_{n-1}$  assuming Conjecture 2.4.4

of  $h_n$  is greater than  $10^9$  for all  $n$  (cf. [25, Corollary 1.2]), we obtain  $h_n/h_{n-1} = 1$  for  $1 \leq n \leq 6$ .

**Remark 2.4.6.** By using Minkowski's convex body theorem for the  $L^p$  norm open ball of the radius  $\|l_n(\epsilon_n)\|_p$ , we also obtain upper bounds of  $h_n/h_{n-1}$ . In contrast to the discussion above, in this setting, the  $L^1$ -minimality of  $\epsilon_n$  gives a more precise bound than the  $L^2$ -minimality.

By these arguments, the resolution of Conjecture 2.4.4 contributes to Weber's conjecture and Conjecture 2.2.6. However, determining the shortest vector in a lattice is generally a very difficult problem. If we propose to approach Conjecture 2.4.4 by imitating the classical method in Section 2.1, then we should establish “*the best approximation to  $X_n$  at  $\mathbb{Q}(X_{n-1})$* ”.

## 2.5 The ratios of the class numbers

Set

$$h_{n/n-1} = \frac{h_n}{h_{n-1}}$$

for each  $n > 1$ . In this section, we obtain a congruence relation formula for  $h_{n/n-1}$ .

By (2.7) in Section 4, we have

$$h_{n/n-1} = (RE_n^+ : A_n).$$

For each prime  $l$ , let  $(RE_n^+/A_n)_l$  denotes the Sylow  $l$ -subgroup of  $RE_n^+/A_n$ , that is the subgroup consisting of elements of  $l$ -power order. Let  $(h_{n/n-1})_l = |(RE_n^+/A_n)_l|$ . The next theorem is our second main theorem.

**Theorem 2.5.1.** *For all prime  $l$  and all positive integer  $n$ , we have*

$$(h_{n/n-1})_l \equiv 1 \pmod{2^n}.$$

This theorem shows that the sequence  $\{h_n\}$  is a Cauchy sequence in 2-adic topology. Thus the sequence  $\{h_n\}$  converges in  $\mathbb{Z}_2$ .

**Remark 2.5.2.** Kisilevsky also obtained the  $p$ -adic convergence of the class numbers for more general setting in [40, Corollary 2] (see Section 2.6 and Section 2.7 for details). We give an extensive numerical study of the  $p$ -adic limits for elliptic curves and knots in the remaining sections of this chapter.

We prepare two lemmas. We note that  $\text{Gal}(\mathbb{B}_n/\mathbb{Q})$  acts on  $RE_n^+/A_n$  and also on  $(RE_n^+/A_n)_l$ .

**Lemma 2.5.3.** *For  $\delta \in RE_n^+/A_n$ , let  $O(\delta)$  be the  $\text{Gal}(\mathbb{B}_n/\mathbb{Q})$ -orbit of  $\delta$  in  $RE_n^+/A_n$ . If  $|O(\delta)| < 2^n$ , then  $\delta^2 = 1$  in  $RE_n^+/A_n$ .*

*Proof.* We recall that  $\sigma$  is a generator of  $\text{Gal}(\mathbb{B}_n/\mathbb{Q})$ .  $|O(\delta)| < 2^n$  means  $\sigma^{2^{n-1}}(\delta) = \delta$  in  $RE_n^+/A_n$ . Therefore, we have  $\text{Nr}_{n/n-1}(\delta) = \delta\sigma^{2^{n-1}}(\delta) = \delta^2$  in  $RE_n^+/A_n$ . On the other hand, since  $\delta \in RE_n^+$ , we have  $\text{Nr}_{n/n-1}(\delta) = 1$  in  $RE_n^+/A_n$ . Then we have  $\delta^2 = 1$  in  $RE_n^+/A_n$ .  $\square$

**Lemma 2.5.4.** *Let  $\delta \in RE_n^+/A_n$ . If  $|O(\delta)| = 1$ , then  $\delta = 1$  in  $RE_n^+/A_n$ .*

*Proof.* Set  $\epsilon = (X_n + 1)/(X_n - 1)$  (abbreviate “ $n$ ”). Suppose that there exists  $\delta \in RE_n^+/A_n$  with  $\delta \neq 1$  in  $RE_n^+/A_n$  and  $|O(\delta)| = 1$ . By Lemma 2.5.3, we have  $\delta^2 \in A_n$ . Since  $A_n = \langle -1, \epsilon \rangle_{\mathbb{Z}[\text{Gal}(\mathbb{B}_n/\mathbb{Q})]}$ ,  $\delta^2$  can be represented as

$$\pm \epsilon^{e_0} \sigma(\epsilon)^{e_1} \dots \sigma^{2^{n-1}-1}(\epsilon)^{e_{2^{n-1}-1}}$$

by certain integers  $e_i$ . Therefore, we have

$$\delta = \pm \sqrt{|\epsilon^{e_0} \sigma(\epsilon)^{e_1} \dots \sigma^{2^{n-1}-1}(\epsilon)^{e_{2^{n-1}-1}}|}.$$

On the other hand,  $|O(\delta)| = 1$  implies  $\sigma(\delta) = \delta$  in  $(RE_n^+/A_n)_2$ . Therefore, we have

$$\begin{aligned} & \sqrt{|\epsilon^{e_0} \sigma(\epsilon)^{e_1} \dots \sigma^{2^{n-1}-1}(\epsilon)^{e_{2^{n-1}-1}}|} \\ &= \sqrt{|\sigma(\epsilon)^{e_0} \sigma^2(\epsilon)^{e_1} \dots \sigma^{2^{n-1}}(\epsilon)^{e_{2^{n-1}-1}}|} \\ &= \sqrt{|\epsilon^{-e_{2^{n-1}-1}} \sigma(\epsilon)^{e_0} \dots \sigma^{2^{n-1}-1}(\epsilon)^{e_{2^{n-1}-2}}|} \text{ in } (RE_n^+/A_n)_2. \end{aligned}$$

Note that  $\sigma^{2^{n-1}}(\epsilon) = \epsilon^{-1}$ . Since  $\{\epsilon, \sigma(\epsilon), \dots, \sigma^{2^{n-1}-1}(\epsilon)\}$  are linearly independent over  $\mathbb{Z}$  in  $RE_n^+$ , we have

$$-e_{2^{n-1}-1} \equiv e_0 \equiv e_1 \equiv \dots \equiv e_{2^{n-1}-2} \equiv e_{2^{n-1}-1} \pmod{2}.$$

This implies that  $e_i \equiv 0 \pmod{2}$  for all  $i$  or  $e_i \equiv 1 \pmod{2}$  for all  $i$ . Since  $\delta \neq 1$ , we have  $e_i = 1$  for all  $i$ . Then we have  $\sqrt{|\epsilon \sigma(\epsilon) \dots \sigma^{2^{n-1}-1}(\epsilon)|} \in RE_n^+$ .

By easy calculation, we have

$$\left| \prod_{k=0}^{2^{n-1}-1} \sigma^k((X_n + 1)(X_n - 1)) \right| = 1.$$

It follows that

$$|\epsilon \sigma(\epsilon) \dots \sigma^{2^{n-1}-1}(\epsilon)| = \left( \frac{1}{(X_n - 1) \dots \sigma^{2^{n-1}-1}(X_n - 1)} \right)^2.$$

Thus we have

$$\sqrt{|\epsilon \sigma(\epsilon) \dots \sigma^{2^{n-1}-1}(\epsilon)|} = \left| \frac{1}{(X_n - 1) \dots \sigma^{2^{n-1}-1}(X_n - 1)} \right|.$$

Since  $\text{Nr}_{n/n-1}((X_n - 1) \dots \sigma^{2^{n-1}-1}(X_n - 1)) = -1$  and  $\text{Nr}_{n/n-1}(-1) = 1$ , we have  $\text{Nr}_{n/n-1}\left(\left|\frac{1}{(X_n - 1) \dots \sigma^{2^{n-1}-1}(X_n - 1)}\right|\right) = -1$ . This contradicts

$$\sqrt{|\epsilon \sigma(\epsilon) \dots \sigma^{2^{n-1}-1}(\epsilon)|} \in \ker \text{Nr}_{n/n-1}.$$

□

*Proof of Theorem 2.5.1.* First, we prove this for an odd prime  $l$ . Suppose that there exists an element  $\delta \neq 1$  in  $(RE_n^+/A_n)_l$  such that  $|O(\delta)| < 2^n$ . By Lemma 2.5.3, the order of  $\delta$  is 2. This contradicts  $2 \nmid |(RE_n^+/A_n)_l|$ . Therefore, all elements except 1 in  $(RE_n^+/A_n)_l$  have  $2^n$  distinct conjugates. This implies the statement.

Next, we consider the case  $l = 2$ , independently of Weber's proof. Suppose that there exists an element  $\delta \neq 1$  in  $(RE_n^+/A_n)_2$  such that  $|O(\delta)| < 2^n$  and we see that  $|O(\delta)| > 1$  by Lemma 2.5.4. Let  $\delta$  be an element with the smallest size of  $|O(\delta)| = 2^m$ . We note that  $\delta$  satisfies  $\sigma^{2^m}(\delta) = \delta$  and  $\sigma^{2^{m-1}}(\delta) \neq \delta$  in  $(RE_n^+/A_n)_2$ . Since  $\sigma^{2^{m-1}}(\delta\sigma^{2^{m-1}}(\delta)) = \sigma^{2^{m-1}}(\delta)\sigma^{2^m}(\delta) = \sigma^{2^{m-1}}(\delta)\delta$  in  $(RE_n^+/A_n)_2$ , we have  $|O(\delta\sigma^{2^{m-1}}(\delta))| \leq 2^{m-1}$ . By the assumption, we have that  $\delta\sigma^{2^{m-1}}(\delta) = 1$  and  $\delta = \sigma^{2^{m-1}}(\delta)^{-1}$  in  $(RE_n^+/A_n)_2$ . By Lemma 2.5.3, we have  $\sigma^{2^{m-1}}(\delta)^{-1} = \sigma^{2^{m-1}}(\delta)$  in  $(RE_n^+/A_n)_2$ . Thus we have  $\delta = \sigma^{2^{m-1}}(\delta)$  in  $(RE_n^+/A_n)_2$  and this is a contradiction.  $\square$

**Remark 2.5.5.** By Theorem 2.5.1, we have  $2 \nmid h_n$  for all  $n \geq 1$ . This result was first proved by Weber [92, Theorem C], but the proof we have now given is independent of the one by Weber. In the proof of Theorem 2.5.1, we use the fact that  $\text{Nr}_{n/n-1} : E_n/C_n \rightarrow E_{n-1}/C_{n-1}$  is surjective and it comes from  $2 \nmid h_{n-1}$  (see the proof of Lemma 2.3.6). Therefore it may seem like a tautology, but if we admit  $h_0 = h(\mathbb{Q}) = 1$ , the proof goes well by induction without using Weber's result. Moreover, our result is a much more refined version of Weber's result.

**Remark 2.5.6.** Recall that  $h_6 = 1$ , then we have  $(h_{7/6})_l = (h_7)_l$ . By Theorem 2.5.1, we have

$$(h_n)_l \equiv 1 \pmod{2^7}$$

for all odd primes  $l$  and positive integers  $n$ .

## 2.6 The $p$ -adic limits of class numbers in $\mathbb{Z}_p$ -towers

From this section to the end of this chapter, we study the  $p$ -adic convergence of the class numbers for several areas. This section summarizes the story.

W. Sinnott announced in 1985 the  $p$ -adic convergence of the class numbers for a cyclotomic  $\mathbb{Z}_p$ -extension of a CM field and for the “minus” class numbers, and Sang-G. Han established an explicit formula [28, Theorem 4] by using an analytic argument. Their results are specific cases of H. Kisilevsky's theorem over any global field, that is, a finite extension of  $\mathbb{Q}$  or  $\mathbb{F}_{p'}(x)$ ,  $p'$  being a prime number. For a  $\mathbb{Z}_p$ -extension  $k_{p^\infty}$  of a global field, let  $k_{p^n}$  denote the  $n$ -th layer of  $k_{p^\infty}$  for each positive integer  $n$ .

**Theorem 1** (Theorem 2.7.1, [40, Corollary 2]). *Let  $k_{p^\infty}$  be a  $\mathbb{Z}_p$ -extension of a global field  $k$ . Then, the sizes of the class groups  $C(k_{p^n})$ , those of the non- $p$ -subgroups  $C(k_{p^n})_{\text{non-}p}$ , and those of the  $l$ -torsion subgroups  $C(k_{p^n})_{(l)}$  for each prime number  $l$  converge in  $\mathbb{Z}_p$ .*

The growth of  $p$ -torsions has been extensively studied in the context of Iwasawa theory. This theorem defines a numerical invariant, say, *the  $p$ -adic class number*  $\lim_{n \rightarrow \infty} |C(k_{p^n})_{\text{non-}p}|$  of a  $\mathbb{Z}_p$ -extension with any  $p$ -torsion growth.

It is said that Gauss's proof of the quadratic reciprocity law using Gauss sums is based on his insight on the analogy between knots and prime numbers. In addition, the analogy between the Alexander–Fox theory for  $\mathbb{Z}$ -covers and the Iwasawa theory for  $\mathbb{Z}_p$ -extensions has played an important role since the 1960s (cf. [50, 57]). A  $p$ -adic refinement of Alexander–Fox's theory is of its self-interests, as well as applies to the study of profinite rigidity (cf. [79, 83, 45]). In this view, we establish an analogue of Theorem 2.7.1 for 3-manifolds.

**Theorem 2** (Theorem 2.8.1). *Let  $(M_{p^n} \rightarrow M)_n$  be a  $\mathbb{Z}_p$ -cover of a compact 3-manifold  $M$ . Then, the sizes of the torsion subgroups  $H_1(M_{p^n})_{\text{tor}}$ , those of the non- $p$  torsion subgroups  $H_1(M_{p^n})_{\text{non-}p}$ , and those of the  $l$ -torsion subgroups  $H_1(M_{p^n})_{(l)}$  for each prime number  $l$ , of the 1st homology groups converge in  $\mathbb{Z}_p$ .*

By S. Kionke's theorem [39, Theorem 1.1 (ii)] and the Poincaré duality, the  $p$ -adic limit value  $\lim_{n \rightarrow \infty} |H_1(M_{p^n})_{\text{non-}p}|$  coincides with Kionke's  $p$ -adic torsion. In Section 2.7 and Section 2.8, we stick to the homological argument and give proofs to these theorems in a parallel manner. Afterward, in Section 2.9, we state a general proposition and discuss alternative proofs.

In several contexts, the size of the  $n$ -th layer is calculated by the  $n$ -th cyclic resultant  $\text{Res}(t^n - 1, f(t)) = \prod_{\zeta^n=1} f(\zeta)$  of a certain polynomial  $0 \neq f(t) \in \mathbb{Z}[t]$ . In order to pursue numerical studies, we establish the following theorems on the  $p$ -adic limits of cyclic resultants, which are detailed versions of [40, Proposition 2]. In the proof, we invoke an elementary  $p$ -adic number theory and the class field theory with modulus. Let  $\mathbb{C}_p$  denote the  $p$ -adic completion of an algebraic closure of the  $p$ -adic numbers  $\mathbb{Q}_p$  and fix an embedding  $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ .

**Theorem 3** (Theorem 2.10.3). *Let  $0 \neq f(t) \in \mathbb{Z}[t]$ . Then, the  $p$ -power-th cyclic resultants  $\text{Res}(t^{p^n} - 1, f(t))$  converge in  $\mathbb{Z}_p$ . The limit value is zero if and only if  $p \mid f(1)$ . In any case, if  $\text{Res}(t^{p^n} - 1, f(t)) \neq 0$  for any  $n$ , then the non- $p$ -parts of  $\text{Res}(t^{p^n} - 1, f(t))$  converge to a non-zero value in  $\mathbb{Z}_p$ . For each prime number  $l$ , similar assertions for the  $l$ -parts of  $\text{Res}(t^{p^n} - 1, f(t))$  hold.*

**Theorem 4** (Theorem 2.10.7, a short version). *Suppose  $p \nmid f(t)$ . Write  $f(t) = a_0 \prod_i (t - \alpha_i)$  in  $\overline{\mathbb{Q}}[t]$  and note that  $|a_0 \prod_{|\alpha_i|_p > 1} \alpha_i|_p = 1$ . Let  $\xi$  and  $\zeta_i$  denote the unique roots of unity of order prime to  $p$  satisfying  $|a_0 \prod_{|\alpha_j|_p > 1} \alpha_j - \xi|_p < 1$  and  $|\alpha_i - \zeta_i|_p < 1$  for each  $i$  with  $|\alpha_i|_p = 1$ . Then*

$$\lim_{n \rightarrow \infty} \text{Res}(t^{p^n} - 1, f(t)) = (-1)^{p \deg f + \#\{i \mid |\alpha_i|_p < 1\}} \xi \prod_{i; |\alpha_i|_p = 1} (\zeta_i - 1)$$

holds in  $\mathbb{Z}_p$ . In addition, the non- $p$  part of  $\text{Res}(t^{p^n} - 1, f(t))$  converges to

$$(-1)^{p \deg f + \#\{i \mid |\alpha_i|_p < 1\}} \xi \left( \prod_{\substack{i; |\alpha_i|_p = 1, \\ |\alpha_i - 1|_p = 1}} (\zeta_i - 1) \right) p^{-\nu} \prod_{\substack{i; |\alpha_i|_p = 1, \\ |\alpha_i - 1|_p < 1}} \log \alpha_i$$

in  $\mathbb{Z}_p$ , where  $\log$  denotes the  $p$ -adic logarithm and  $\nu$  is Iwasawa's invariant defined by  $p^{-\nu} = \prod_{i:|\alpha_i-1|_p < 1} |\log \alpha_i|_p$ . If all  $\alpha_i$ 's with  $|\alpha_i - 1|_p < 1$  are sufficiently close to 1, then  $p^\nu = |f(1)|_p^{-1}$  holds.

In the cases of  $\mathbb{Z}_p$ -covers of knots, Fox–Weber's formula asserts that the cyclic resultants of the Alexander polynomials coincide with the sizes of torsion subgroups of the 1st homology groups. We calculate the  $p$ -adic limits of  $|H_1(M_{p^n})_{\text{tor}}|$  for the  $\mathbb{Z}_p$ -covers of torus knots  $T_{a,b}$  and twist knots  $J(2, 2m)$  to establish Propositions 2.11.3, 2.11.8, 2.11.10, *completing the table of the cases with the  $p$ -adic limits being in  $\mathbb{Z}$* . Moreover, we give a systematic study of the Iwasawa  $\nu$ -invariants and answer the following question (Propositions 2.11.12, 2.11.16): *Find  $\mathbb{Z}_p$ -covers  $(M_{ep^n} \rightarrow M_e)_n$  with  $e \in \mathbb{Z}_{>0}$  of twist knots  $J(2, 2n)$  such that the base  $p$ -class numbers  $|H_1(X_e)_{(p)}|$  are small and  $\nu$ 's are arbitrarily large*. In Subsection 2.11.4, we discuss several possible analogues of Weber's problem for knots; we remark Livingston's results in [46] and point out further problems in view of the Sato–Tate conjecture.

In the cases of constant  $\mathbb{Z}_p$ -extensions of function fields, the cyclic resultants of the Frobenius polynomials coincide with the sizes of the degree zero divisor class groups. In Section 2.12, we recollect basic facts of function fields, state an analogue of Fox–Weber's formula for constant extensions of function fields (Proposition 2.12.2), and study elliptic curves over finite fields. We point out conditions for the  $p$ -adic limit value being 0 or 1 using the notions of supersingular primes and anomalous primes, as well as *complete the list of the cases with the  $p$ -adic limits being in  $\mathbb{Z}$*  (Proposition 2.12.8, 2.12.10). We also give a systematic study of the Iwasawa  $\nu$ -invariant and answer the following question (Propositions 2.12.12, 2.12.13): *Find constant  $\mathbb{Z}_p$ -extensions  $(k_{ep^n}/k_e)_n$  with  $e \in \mathbb{Z}_{>0}$  of the function fields of elliptic curves over  $\mathbb{F}_l$  such that the base  $p$ -class numbers  $|\text{Cl}^0(k_e)_{(p)}|$  are small and  $\nu$ 's are arbitrarily large*.

Note that we have intensionally kept our materials to the very basic, such as torus knots, twist knots, and elliptic curves, to raise questions in a broad scope. This chapter contains a detailed revisiting of Kisilevsky's short article [40]. Our numerical study of the  $p$ -adic limits gives explicit examples of Kionke's  $p$ -adic torsions introduced in [39]. Recent related works are due to G. Asvin [3] and M. Ozaki [62] (See Remarks 2.10.4 and 2.9.2). In addition, C. Deninger points out that there would exist a common generalization of our work and his [18].

## 2.7 Global fields

A number field is a finite extension of  $\mathbb{Q}$ . A function field is a finite extension of the rational function field  $\mathbb{F}_{p'}(x)$  of one variable over a finite field  $\mathbb{F}_{p'}$ ,  $p'$  being a prime number. A global field is a number field or a function field. For a global field  $k$ , let  $C(k)$  denote the ideal class group  $\text{Cl}(k)$  if  $k$  is a number field, and the degree-zero divisor class group  $\text{Cl}^0(k)$  if  $k$  is a function field. Note that  $C(k)$  is always a finite group. We regard  $C(k)$  as a multiplicative group. For any finite abelian group  $G$  and a prime number  $l$ , let  $G_{(l)}$  and  $G_{\text{non-}p}$  denote the  $l$ -torsion subgroup and non- $p$  torsion

subgroup of  $G$  respectively. The size of a finite set  $X$  is written as  $|X|$ . A  $\mathbb{Z}_p$ -extension  $k_{p^\infty}$  of a global field  $k$  is a direct system  $(k_{p^n})_n$  of  $\mathbb{Z}/p^n\mathbb{Z}$ -extensions or its union  $\bigcup_n k_{p^n}$ . The following theorem was initially proved by Kisilevsky [40, Corollary 2]. We note that although Kisilevsky's proof is short and clear, we here give our original proof with a purpose.

**Theorem 2.7.1.** *Let  $k_{p^\infty}$  be a  $\mathbb{Z}_p$ -extension of a global field  $k$ . Then, the sizes of the class groups  $C(k_{p^n})$ , those of the non- $p$ -subgroups  $C(k_{p^n})_{\text{non-}p}$ , and those of the  $l$ -torsion subgroups  $C(k_{p^n})_{(l)}$  for each prime number  $l$  converge in  $\mathbb{Z}_p$ .*

*Proof.* It is well-known (see Remark 2.7.2 below) that for any  $n \gg 0$ , the class field theory yields that  $|C(k_{p^{n-1}})|$  divides  $|C(k_{p^n})|$ . Hence the sequence  $|C(k_{p^n})_{(p)}|$  is a constant for  $n \gg 0$  or it converges to 0 in  $\mathbb{Z}_p$ . Thus, it suffices to prove for each prime number  $l \neq p$  and  $n \in \mathbb{Z}_{>0}$  the congruence formula of relative class numbers

$$|C(k_{p^n})_{(l)}|/|C(k_{p^{n-1}})_{(l)}| \equiv 1 \pmod{p^n}. \quad (2.16)$$

Define the relative norm map  $\text{Nr}_{n/n-1} : C(k_{p^n}) \rightarrow C(k_{p^{n-1}}) : [\mathfrak{a}] \mapsto \prod_{i=0}^{p-1} \mathfrak{a}^{\tau^i}$ , where  $\tau$  is a generator of  $\text{Gal}(k_{p^n}/k_{p^{n-1}}) \cong \mathbb{Z}/p\mathbb{Z}$ .

The map  $\text{Nr}_{n/n-1} : C(k_{p^n})_{(l)} \rightarrow C(k_{p^{n-1}})_{(l)}$  on the  $l$ -parts is surjective. Indeed, there is a natural homomorphism  $\iota : C(k_{p^{n-1}})_{(l)} \rightarrow C(k_{p^n})_{(l)}$  and the composition map  $\text{Nr}_{n/n-1} \circ \iota : C(k_{p^{n-1}})_{(l)} \rightarrow C(k_{p^{n-1}})_{(l)}$  is given by  $x \mapsto x^p$ . Since  $l \neq p$ , this map  $\text{Nr}_{n/n-1} \circ \iota$  is an isomorphism and hence  $\text{Nr}_{n/n-1}$  is surjective.

Note that  $|(\text{KerNr}_{n/n-1})_{(l)}| = |C(k_{p^n})_{(l)}|/|C(k_{p^{n-1}})_{(l)}|$ . We study the Galois module structure of  $(\text{KerNr}_{n/n-1})_{(l)}$  to obtain the assertion. Put  $G = \text{Gal}(k_{p^n}/k) \cong \mathbb{Z}/p^n\mathbb{Z}$  and let  $\sigma$  be a generator of  $G$ . For each  $[\mathfrak{a}] \in (\text{KerNr}_{n/n-1})_{(l)}$ , let  $G[\mathfrak{a}]$  denote the  $G$ -orbit of  $[\mathfrak{a}]$ . If  $[\mathfrak{a}] \neq 1$ , then  $|G[\mathfrak{a}]| = p^n$ . Indeed, suppose that  $|G[\mathfrak{a}]| < p^n$ . Then  $|G[\mathfrak{a}]|$  divides  $p^{n-1}$  and we have that  $[\mathfrak{a}] = [\mathfrak{a}^{\sigma^{p^{n-1}}}]$ . Note that  $\sigma^{p^{n-1}}$  generates the group  $p^{n-1}\mathbb{Z}/p^n\mathbb{Z} \cong \text{Gal}(k_{p^n}/k_{p^{n-1}}) < G$  and put  $\tau = \sigma^{p^{n-1}}$ . Since  $[\mathfrak{a}] \in (\text{KerNr}_{n/n-1})_{(l)}$ , we have  $[\mathfrak{a}]^p = [\prod_{i=0}^{p-1} \mathfrak{a}^{\tau^i}] = 1$ . Since  $l \neq p$ , we obtain  $[\mathfrak{a}] = 1$ .

Now the  $G$ -orbital decomposition yields that  $(\text{KerNr}_{n/n-1})_{(l)} \equiv 1 \pmod{p^n}$ , hence the claimed formula Eq. (2.16). Therefore, both  $(|C(k_{p^n})_{(l)}|)_n$  and  $(|C(k_{p^n})_{\text{non-}p}|)_n$  are  $p$ -adic Cauchy sequences and converge in the completed ring  $\mathbb{Z}_p$ , and so does  $(|C(k_{p^n})|)_n$ .  $\square$

**Remark 2.7.2.** The following well-known argument completes the first paragraph of the proof.

(1) For each number field  $k$ , let  $\tilde{k}$  denote the Hilbert class field, that is, the maximal unramified abelian extension of  $k$ . Then the class field theory asserts that  $\text{Cl}(k) \cong \text{Gal}(\tilde{k}/k)$ . If  $k'/k$  is a ramified extension of degree  $p$ , then we have  $\tilde{k} \cap k' = k$  and that  $\tilde{k}k'/k'$  is an unramified extension of degree  $|\text{Cl}(k)|$ , and hence  $|\text{Cl}(k)|$  divides  $|\text{Cl}(k')| = \text{deg}(\tilde{k}'/k')$ .

If  $k_{p^\infty}/k$  is a  $\mathbb{Z}_p$ -extension, then the inertia group of a ramified prime is an open subgroup of  $\mathbb{Z}_p = \text{Gal}(k_{p^\infty}/k)$ , and hence  $k_{p^n}/k_{p^{n-1}}$  is a ramified  $p$ -extension for any  $n \gg 0$ .

(2) For a function field  $k$ , let  $\tilde{k}$  denote the maximal unramified abelian extension of  $k$ . Let  $\overline{\mathbb{F}}_{p'}$  denote the algebraic closure of  $\mathbb{F}_{p'}$ , so that we have  $\text{Gal}(\overline{\mathbb{F}}_{p'}/\mathbb{F}_{p'}) \cong \widehat{\mathbb{Z}} = \varprojlim_r \mathbb{Z}/r\mathbb{Z}$ . Then an analogue of the class field theory asserts that  $\text{Cl}^0(k) \cong \text{Gal}(\tilde{k}/k\overline{\mathbb{F}}_{p'})$ .

(i) If  $k'/k$  is a constant extension of degree  $p$ , then by  $k'\overline{\mathbb{F}}_{p'} = k\overline{\mathbb{F}}_{p'}$ ,  $\tilde{k}/k\overline{\mathbb{F}}_{p'}$  is a subextension of  $\tilde{k}'/k'\overline{\mathbb{F}}_{p'}$ , and hence  $|\text{Cl}(k)|$  divides  $|\text{Cl}(k')|$ .

(ii) If  $k'/k$  is a geometric ramified extension of degree  $p$ , then a similar argument to (1) yields that  $|\text{Cl}(k)|$  divides  $|\text{Cl}(k')|$ .

For a  $\mathbb{Z}_p$ -extension  $k_{p^\infty}/k$  of a function field,  $k_{p^n}/k_{p^{n-1}}$  is a constant extension for all  $n \in \mathbb{Z}_{>0}$  and (i) applies, or  $k_{p^n}/k_{p^{n-1}}$  is a geometric ramified extension for all  $n \gg 0$  and (ii) applies. In the latter case, we always have  $p = p'$ .

**Remark 2.7.3.** In a view of the analogy between number fields and function fields, Iwasawa pointed out so-called Iwasawa's class number formula (cf. [34],[90, Section 7.2]), which asserts that if  $k_{p^\infty}$  is a  $\mathbb{Z}_p$ -extension of a number field  $k$ , then there exist some  $\lambda, \mu, \nu \in \mathbb{Z}_{\geq 0}$  such that for any  $n \gg 0$ ,

$$|\text{C}(k_{p^n})_{(p)}| = p^{\lambda n + \mu p^n + \nu}$$

holds. A similar formula with  $\mu = 0$  holds for a constant  $\mathbb{Z}_p$ -extension of a function field [66, Theorem 11.5] and  $\lambda$  is related to the genus of an algebraic curve in several senses.

In many literature of number theory, the suffix is shifted as  $k'_n = k_{p^{n-1}}$ . Note that  $\lambda'n + \mu'p^n + \nu' = \lambda(n-1) + \mu p^{n-1} + \nu$  implies  $\mu = p\mu'$ ,  $\lambda = \lambda'$ ,  $\nu = \nu' + \lambda$ .

Gold–Kisilevsky [27] pointed out that in a geometric  $\mathbb{Z}_p$ -extension the  $p$ -parts can grow arbitrarily fast. Even in such a case, Theorem 2.7.1 persists.

**Remark 2.7.4.** Let  $l \neq p$  be a prime number. Washington [89] proved that in a cyclotomic  $\mathbb{Z}_p$ -extension of a number field abelian over  $k$ , for each prime number  $l \neq p$ , the  $l$ -part of the class numbers are bounded, and hence the sequence is constant for  $n \gg 0$ . The assertion on the  $l$ -part in our Theorem 2.7.1 is a weak generalization of Washington's one.

**Remark 2.7.5.** Weber's class number problem for function fields over finite fields is solved; Shen–Shi [70] completed the list of the only existing 8 exceptional cases.

## 2.8 3-manifolds

In this section, we establish a theorem of  $p$ -adic convergence in the context of 3-dimensional topology. A  $\mathbb{Z}_p$ -cover of a compact 3-manifold  $M$  is a compatible system  $(M_{p^n} \rightarrow M)_n$  of  $\mathbb{Z}/p^n\mathbb{Z}$ -covers. The following is an analogue of Theorem 2.7.1.

**Theorem 2.8.1.** *Let  $(M_{p^n} \rightarrow M)_n$  be a  $\mathbb{Z}_p$ -cover of a compact 3-manifold  $M$ . Then, the sizes of the torsion subgroups  $H_1(M_{p^n})_{\text{tor}}$ , those of the non- $p$  torsion subgroups  $H_1(M_{p^n})_{\text{non-}p}$ , and those of the  $l$ -torsion subgroups  $H_1(M_{p^n})_{(l)}$  for each prime number  $l$ , of the 1st homology groups converge in  $\mathbb{Z}_p$ .*



The following lemma helps to prove the assertion in a parallel manner to Theorem 2.7.1.

**Lemma 2.8.2.** *Let  $(M_{p^n} \rightarrow M)_n$  be a  $\mathbb{Z}_p$ -cover of a compact 3-manifold. Then,  $(H_1(M_{p^n})_{\text{tor}})_n$  is a surjective system for  $n \gg 0$ .*

*Proof of Lemma 2.8.2.* Since a  $\mathbb{Z}_p$ -cover corresponds to a surjective homomorphism  $\widehat{\pi}_1(M) \rightarrow \mathbb{Z}_p$  from the profinite completion of  $\pi_1(M)$  to the ring of  $p$ -adic integers, we see that a fixed layer  $M_{p^{n+1}} \rightarrow M$  is a subcover of some  $\mathbb{Z}$ -cover  $M_\infty \rightarrow M$ . So, it suffices to consider the  $\mathbb{Z}_p$ -cover obtained from a  $\mathbb{Z}$ -cover.

For each  $n \in \mathbb{Z}_{>0}$ , the Wang exact sequence yields the short exact sequence

$$0 \rightarrow H_1(M_\infty)/(t^n - 1)H_1(M_\infty) \rightarrow H_1(M_n) \rightarrow \mathbb{Z} \rightarrow 0$$

of finitely generated abelian groups. We may take a compatible system of sections  $s_n : \mathbb{Z} \rightarrow H_1(X_n)$ , so that

$$H_1(M_\infty)/(t^n - 1)H_1(M_\infty) \cong H_1(M_n)/s_n(\mathbb{Z})$$

forms a compatible surjective system. Note that  $H_1(M_n)/s_n(\mathbb{Z})_{\text{tor}} \cong H_1(M_n)_{\text{tor}}$ . Since

$$H_1(M_\infty)/(t^{p^{n+1}} - 1)H_1(M_\infty) \cong H_1(M_\infty)/(t^{p^n} - 1)H_1(M_\infty) \oplus H_1(M_\infty)/\frac{t^{p^{n+1}} - 1}{t^{p^n} - 1}H_1(M_\infty),$$

their torsion subgroups also form a surjective system for  $n \gg 0$ , and so does  $H_1(M_{p^n})_{\text{tor}}$ .  $\square$

**Remark 2.8.3.** (1) In general, a  $\mathbb{Z}_p$ -cover is not obtained from a  $\mathbb{Z}$ -cover. Even in that case, if we put  $\mathcal{H} = \varprojlim H_1(M_{p^n})/s_{p^n}(\mathbb{Z})$ , then we still have an exact sequence

$$0 \rightarrow \mathcal{H}/(t^n - 1)\mathcal{H} \rightarrow H_1(M_{p^n}) \rightarrow \mathbb{Z} \rightarrow 0.$$

If  $f(t) = \prod_i f_i(t)$  is the characteristic polynomial of an approximating  $\mathbb{Z}$ -cover, then the characteristic ideal of  $\mathcal{H}$  is given by  $(f(t^v))$  with some  $v \in \mathbb{Z}_p^*$ . An example is obtained from a 2-component link  $L = K_1 \cup K_2$  in  $S^3$  with meridians  $\mu_1$  and  $\mu_2$ ; consider the surjective homomorphism  $\widehat{\pi}_1(S^3 - L) \rightarrow \mathbb{Z}_5$  defined by  $\mu_1 \mapsto 1$  and  $\mu_2 \mapsto \sqrt{-1}$ .

(2) Theorem 2.8.1 applies to  $\mathbb{Z}_p$ -cover of the exterior of a finite link in  $S^3$ . In addition, for a link  $\mathcal{L} = \bigcup_{i \in \mathbb{Z}_{>0}} K_j$  with countably infinite disjoint component in  $S^3$ , if we define a surjective homomorphism  $\tau : \widehat{\pi}_1(M - \mathcal{L}) \rightarrow \mathbb{Z}_p; \mu_i \mapsto p^i$  from the profinite completion,  $\mu_i$  being a meridian of  $K_i$ , then we obtain a branched  $\mathbb{Z}_p$ -cover branched along an infinite link. By considering  $\tau_n : \widehat{\pi}_1(M - \bigcup_{i \leq n} K_i) \rightarrow \mathbb{Z}_p; \mu_i \mapsto p^i$  on each layer, Theorem 2.8.1 applies.

*Proof of Theorem 2.8.1.* As we observed in the proof of Lemma 2.8.2,  $H_1(M_{p^n})_{\text{tor}}$  forms a surjective system, and hence  $|H_1(M_{p^{n-1}})_{\text{tor}}|$  divides  $|H_1(M_{p^n})_{\text{tor}}|$  for any  $n$ . Therefore  $|H_1(M_{p^n})_{(p)}|$  is a constant for  $n \gg 0$  or converges to zero in  $\mathbb{Z}_p$ .

It suffices to show for each prime number  $l \neq p$  and  $n \in \mathbb{Z}_{>0}$  the congruence formula

$$|H_1(M_{p^n})_{(l)}|/|H_1(M_{p^{n-1}})_{(l)}| \equiv 1 \pmod{p^n}. \quad (2.17)$$

Write  $h : M_{p^n} \rightarrow M_{p^{n-1}}$  and  $h_* : H_1(M_{p^n}) \rightarrow H_1(M_{p^{n-1}})$ . Consider the transfer map  $h^! : H_1(M_{p^{n-1}}) \rightarrow H_1(M_{p^n})$  defined by  $[c] \mapsto [\sum_{\sigma \in \text{Gal}(h)} \sigma c_1]$ , where  $c$  is an open chain and  $c_1$  is a lift of  $c$ . Then the composition map is  $h_* \circ h^! : H_1(M_{p^{n-1}}) \rightarrow H_1(M_{p^{n-1}}); [c] \mapsto p[c]$ . By Lemma 2.8.2, these maps  $h_*$  and  $h^!$  restrict to  $H_1(M_{p^{n-1}})_{(l)}$  and  $H_1(M_{p^n})_{(l)}$ .

Put  $G = \text{Gal}(M_{p^n} \rightarrow M) \cong \mathbb{Z}/p^n\mathbb{Z}$  and let  $\sigma$  be a generator of  $G$ . For each  $[c] \in (\text{Ker } h_*)_{(l)}$ , let  $G[c]$  denote the  $G$ -orbit of  $[c]$ . If  $[c] \neq 1$ , then  $|G[c]| = p^n$ . Indeed, suppose that  $|G[c]| < p^n$ . Then  $|G[c]|$  divides  $p^{n-1}$  and we have that  $[c] = [\sigma^{p^{n-1}} c]$ . Note that  $\sigma^{p^{n-1}}$  generates the group  $p^{n-1}\mathbb{Z}/p^n\mathbb{Z} \cong \text{Gal}(h) < G$  and put  $\tau = \sigma^{p^{n-1}}$ . Since  $[c] \in (\text{Ker } h_*)_{(l)}$ , we have  $[c]^p = \prod_{i=0}^{p-1} \tau^i [c] = 1$ . Since  $l \neq p$ , we obtain  $[c] = 1$ .

Now the  $G$ -orbital decomposition yields that  $\text{Ker } h_{*(l)} \equiv 1 \pmod{p^n}$ , hence the claimed formula Eq. (2.17). Therefore, both  $(|H_1(M_{p^n})_{(l)}|)_n$  and  $(|H_1(M_{p^n})_{\text{non-}p}|)_n$  are  $p$ -adic Cauchy sequences and converge in the completed ring  $\mathbb{Z}_p$ , and so does  $(|H_1(M_{p^n})_{\text{tor}}|)_n$ .  $\square$

**Remark 2.8.4.** In the situation of Theorem 2.8.1, we have an analogue of the Iwasawa class number formula; Let  $M_{p^n} \rightarrow M$  be a  $\mathbb{Z}_p$ -cover. Then there exists some  $\lambda, \mu, \nu \in \mathbb{Z}_{\geq 0}$  such that for any  $n \gg 0$ ,

$$|H_1(M_{p^n})_{(p)}| = p^{\lambda n + \mu p^n + \nu}$$

holds (cf. [29, 35, 78]). For a  $\mathbb{Z}_p$ -cover of a knot exterior in  $S^3$ , by [77, Theorem 7], we always have  $|H_1(M_{p^n})_{(p)}| = 1$ .

## 2.9 Alternative proofs

Here we state a general proposition to discuss alternative proofs of the  $p$ -adic convergence theorems (Theorems 2.7.1, 2.8.1).

**Proposition 2.9.1.** *Let  $p$  be a prime number. Let  $\Gamma$  be a multiplicative group isomorphic to the additive group  $\mathbb{Z}_p$  of  $p$ -adic integers. For each  $n \in \mathbb{Z}_{>0}$ , put  $\Gamma_n = \Gamma^{p^n}$  and  $G_n = \Gamma/\Gamma_n$ .*

(1) [40, Proposition 1] *Let  $A$  be a discrete  $\Gamma$ -module such that the  $\Gamma_n$ -invariant subgroup  $A_n = A^{\Gamma_n} = \{a \in A \mid \gamma(a) = a \text{ for all } \gamma \in \Gamma_n\}$  is a finite group for every  $n$ . Then we have*

$$|A_n| \equiv |A_{n-1}| \pmod{p^n}.$$

(2) *Let  $H$  be a compact  $\Gamma$ -module such that the  $\Gamma_n$ -coinvariant quotient group  $H_n = H_{\Gamma_n} = H/\{(1-g)a \mid g \in \Gamma_n, a \in H\}$  is a finite group for every  $n$ . Then for any prime number  $l \neq p$ , the sizes of the  $l$ -parts satisfy*

$$|H_{n(l)}| \equiv |H_{n-1(l)}| \pmod{p^n}.$$

*Proof.* (1) Let  $B = \{a \in A_n \mid \gamma(a) \neq a \text{ for all } \gamma \in G_n\}$  and write  $A_n = B \sqcup C$ . Since  $G_n$  is a cyclic group, every  $c \in C$  is fixed by the unique subgroup of  $G_n$  of order  $p$ , so we have  $C \subset A^{\Gamma_{n-1}} = A_{n-1}$ . Since  $A_{n-1} \cap B = \emptyset$ , we have  $A_{n-1} \subset C$ . Thus we have  $C = A_{n-1}$ . Since  $B$  is the disjoint union of orbits of size  $p^n$ , we have  $|A_n| = |B| + |A_{n-1}| \equiv |A_{n-1}| \pmod{p^n}$ .

(2) [Proof 1] We omit “(1)”. It suffices to show that  $|H_n|/|H_{n-1}| = |\text{Ker}(H_n \twoheadrightarrow H_{n-1})| \equiv 1 \pmod{p^n}$ . Let us prove that if  $0 \neq [a] \in \text{Ker}(H_n \twoheadrightarrow H_{n-1})$ , then  $G_n = \langle t \rangle = \Gamma/\Gamma_n \cong \mathbb{Z}/p^n\mathbb{Z}$  acts on  $[a]$  freely. Let  $[a] \in \text{Ker}(H_n \twoheadrightarrow H_{n-1})$  and suppose  $|G_n[a]| < p^n$ , so that we have  $[a] = t^{p^{n-1}}[a]$ . Put  $\sigma = t^{p^{n-1}}$ . Note that we have a standard direct decomposition  $H_n = (\sum_{i=0}^{p-1} \sigma^i)H_n \oplus (1 - \sigma)H_n$  with an isomorphism  $H_{n-1} \cong (\sum_{i=0}^{p-1} \sigma^i)H_n$  and that the natural surjection  $H_n \twoheadrightarrow H_{n-1} \cong (\sum_{i=0}^{p-1} \sigma^i)H_n$  is given by  $a \mapsto (\sum_{i=0}^{p-1} \sigma^i)a$ . Since  $[a] \in \text{Ker}(H_n \twoheadrightarrow H_{n-1})$ , we have  $p[a] = (\sum_{i=0}^{p-1} \sigma^i)[a] = 0$  in  $H_n$ . Since  $l \neq p$ , we have  $[a] = 0$ .

[Proof 2] By the natural injections  $H_{n-1} \cong (\sum_{i=0}^{p-1} \sigma^i)H_n \subset H_n$ , we obtain an injective system  $(H_n)_n$ . If we put  $A = \varinjlim H_n$ , then the assertion (1) applies.  $\square$

The common argument in our proofs in the previous sections may be generalized to the first proof of (2). Kisilevsky [40] applied the assertion (1) to the direct limit of the class groups in a  $\mathbb{Z}_p$ -extension to obtain his result. In the topology side, we may also consider the direct limit  $A = \varinjlim H_1(M_n)_{\text{tor}}$  via the transfer maps  $h^! : H_1(M_{n-1}) \rightarrow H_1(M_n) : [c] \mapsto [\sum_{\sigma \in \text{Gal}(h)} \sigma c_1]$  and apply (1) to obtain the result. Kionke’s general framework [39] for the  $p$ -adic limits of topological invariants instead considers the injective system of the cohomology groups  $H^i(X_n; \mathbb{Z})$ . The proof of Theorem 2.5.1 is very different from those in the above and uses the unit groups. We wonder if it extends to general cases and may be translated into analogous contexts. In fact, an analogue of the unit group is still in mystery (cf. [85]).

**Remark 2.9.2.** After Sinnott’s announcement in 1972, Han [28, Theorem 4] established an explicit formula for the  $p$ -adic limit of class numbers in a  $\mathbb{Z}_p$ -extension of a CM field by using an analytic argument.

Recently, Ozaki [62] generalized the  $p$ -adic convergence theorem of class numbers to a general extension of a number field with a finitely generated pro- $p$  Galois group by developing an analytic method, to reveal relationships amongst several arithmetic invariants; the class numbers, the ratios of  $p$ -adic regulators, the square roots of discriminants, and the order of algebraic  $K_2$ -groups of the ring of integers. Studying their analogues in the knot theory side would give a new cliff to extend the dictionary of arithmetic topology.

**Remark 2.9.3.** J. Schettler proved that in a  $\mathbb{Z}_p$ -extension of a  $\mathbb{Z}_p$ -field, Iwasawa’s  $\lambda$  converges in  $\mathbb{Z}_p$  [69, Corollary 11]. It would be interesting to establish analogous results for 3-manifolds or function fields and give numerical investigations.

## 2.10 Cyclic resultants

Let  $p$  be a prime number as before. In various situations, in a  $\mathbb{Z}_p$ -tower, the class number or its analogue of the layer of degree  $p^n$  is given by the  $p^n$ -th cyclic resultant of a certain polynomial invariant. In this section, we study the  $p$ -adic limits of  $p$ -power-th cyclic resultants of a polynomial in  $\mathbb{Z}[t]$ .

### 2.10.1 Signatures

For each  $n \in \mathbb{Z}_{>0}$ , the  $n$ -th cyclic resultant of  $0 \neq f(t) \in \mathbb{Z}[t]$  is defined by the determinant of Sylvester matrix, or equivalently, by

$$\text{Res}(t^n - 1, f(t)) = \prod_{\zeta^n=1} f(\zeta),$$

where  $\zeta$  runs through  $n$ -th roots of unity in a fixed algebraic closure  $\overline{\mathbb{Q}}$  of  $\mathbb{Q}$ . If  $f(t) = a_0 \prod_i (t - \alpha_i)$ , then  $\text{Res}(t^n - 1, f(t)) = (-1)^{n \deg f(t)} a_0^n \prod (\alpha_i^n - 1)$  holds. The  $n$ -th cyclotomic polynomial  $\Phi_n(t) \in \mathbb{Z}[t]$  for each  $n \in \mathbb{Z}_{>0}$  is an irreducible polynomial determined by  $t^n - 1 = \prod_{m|n} \Phi_m(t)$  ( $m, n \in \mathbb{Z}_{>0}$ ) recursively. The non- $p$  part of an integer  $x = mp^r$  with  $m \in \mathbb{Z}$  and  $r \in \mathbb{Z}_{\geq 0}$  is defined to be  $m$ . For each prime number  $l$ , the  $l$ -part of an integer  $x$  is defined to be the maximal  $l$ -power dividing  $x$ , that is,  $|x|_l^{-1}$ . The following lemma reduces the calculation of the limits of  $p$ -power-th cyclic resultants to that of the absolute values.

**Lemma 2.10.1.** *Let  $0 \neq f(t) \in \mathbb{Z}[t]$ .*

(1) *If  $\text{Res}(t^n - 1, f(t)) \neq 0$ , then we have  $\text{Res}(t^n - 1, f(t)) > 0$  if and only if (i)  $2 \mid n$  and  $f(1)f(-1) > 0$  or (ii)  $2 \nmid n$  and  $f(1) > 0$ .*

(2) *Suppose that  $n \in \mathbb{Z}_{>0}$ . If  $p \neq 2$ , then we have  $\text{Res}(t^{p^n} - 1, f(t)) > 0$  if and only if  $f(1) > 0$ . If  $p = 2$ , then we have  $\text{Res}(t^{p^n} - 1, f(t)) > 0$  if and only if  $f(1)f(-1) > 0$ .*

*Proof.* For any  $m \in \mathbb{Z}_{>2}$ , we have  $\prod_{\zeta; \Phi_m(\zeta)=0} f(\zeta) = \text{Nr}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}} f(\zeta_m) > 0$ , where  $\zeta_m$  is an arbitrary taken primitive  $m$ -th root of unity. By  $\text{Res}(t^n - 1, f(t)) = \prod_{m|n} \prod_{\zeta; \Phi_m(\zeta)=0} f(\zeta)$ , we obtain the assertion.  $\square$

### 2.10.2 $p$ -adic convergence

The  $p$ -adic convergence theorem (Theorem 2.10.3) for a polynomial may be proved by applying Proposition 2.9.1 to the compact module  $H = \varprojlim \Lambda/(f(t), t^{p^n-1})$ . Here, we give another proof by invoking the global field theory with modulus. For a number field  $k$ , let  $I(k)$  and  $P(k)$  denote the ideal group and the principal ideal group of  $k$  respectively. In addition, for a divisor  $\mathfrak{M} = \prod_i \mathfrak{p}_i^{e_i} \prod_j \infty_j$  of  $k$ , where  $\mathfrak{p}_i$ 's are distinct prime ideals of  $k$  with  $e_i \in \mathbb{Z}_{>0}$  and  $\infty_j$ 's are distinct real places, set  $I_{\mathfrak{M}}(k) = \{\mathfrak{a} \in I(k) \mid (\prod_i \mathfrak{p}_i^{e_i}, \mathfrak{a}) = 1\}$  and  $P_{\mathfrak{M}}(k) = \{\mathfrak{a} \in I_{\mathfrak{M}}(k) \cap P(k) \mid \mathfrak{a} \equiv 1 \pmod{*} \mathfrak{M}\}$ , where  $\mathfrak{a} \equiv 1 \pmod{*} \mathfrak{M}$  means that there exists some  $\alpha \in k$  such that (i)  $\mathfrak{a} = (\alpha)$  and the

multiplicative  $\mathfrak{p}_i$ -adic valuation satisfies  $v_{\mathfrak{p}_i}(\alpha - 1) \geq e_i$  for all  $\mathfrak{p}_i$  and (ii)  $\alpha > 0$  at all  $\infty_j$ . Then we have the following.

**Lemma 2.10.2** (Artin reciprocity law, cf. [90, Appendix §3, Theorem 1(i)]). *Let the notation be as above. Let  $k'/k$  be a finite extension and suppose that the conductor  $\mathfrak{f}$  of  $k'/k$  divides  $\mathfrak{M}$ . Then there is a natural isomorphism called Artin's reciprocity map*

$$I_{\mathfrak{M}}(k)/P_{\mathfrak{M}}(k)\mathrm{Nr}_{k'/k}(I_{\mathfrak{M}}(k')) \xrightarrow{\cong} \mathrm{Gal}(k'/k).$$

The following theorem on  $p$ -adic convergence yields alternative proofs of Theorems 2.7.1 and 2.8.1 for several situations, as we will exhibit later.

**Theorem 2.10.3.** *Let  $0 \neq f(t) \in \mathbb{Z}[t]$ . Then, the  $p$ -power-th cyclic resultants  $\mathrm{Res}(t^{p^n} - 1, f(t))$  converge in  $\mathbb{Z}_p$ . The limit values are zero if and only if  $p \mid f(1)$ . In any case, if  $\mathrm{Res}(t^{p^n} - 1, f(t)) \neq 0$  for any  $n$ , then the non- $p$ -parts of  $\mathrm{Res}(t^{p^n} - 1, f(t))$  converge to a non-zero value in  $\mathbb{Z}_p$ . For each prime number  $l$ , similar assertions for the  $l$ -parts of  $\mathrm{Res}(t^{p^n} - 1, f(t))$  hold.*

*Proof.* If  $\mathrm{Res}(t^{p^n} - 1, f(t)) = 0$  for some  $n$ , so that the limit value is zero, then we have  $\Phi_{p^m}(t) \mid f(t)$  for some  $m \mid n$  and hence  $p \mid f(1)$ .

Assume  $\mathrm{Res}(t^{p^n} - 1, f(t)) \neq 0$ . For each  $n \in \mathbb{Z}_{>0}$ , let  $\zeta_{p^n}$  be an arbitrary taken primitive  $p^n$ -th root of unity. Then we have

$$\frac{\mathrm{Res}(t^{p^n} - 1, f(t))}{\mathrm{Res}(t^{p^{n-1}} - 1, f(t))} = \prod_{0 \leq i < p^n; (i,p)=1} f(\zeta_{p^n}^i) = \mathrm{Nr}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}} f(\zeta_{p^n}).$$

If  $p \mid f(1)$ , then we have  $f(t) \equiv (1-t)g(t) \pmod{p}$  and  $f(t) = (1-t)g(t) + ph(t)$  for some  $g(t), h(t) \in \mathbb{Z}[t]$ . Since  $(1 - \zeta_{p^n})$  is a unique prime ideal of  $\mathbb{Z}[\zeta_{p^n}]$  dividing  $(p)$ , we have  $p \mid \mathrm{Nr}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}} f(\zeta_{p^n})$ , and hence  $\mathrm{Res}(t^{p^n} - 1, f(t))$  converges to zero in  $\mathbb{Z}_p$ .

Suppose instead that  $p \nmid f(1)$ . Let us prove that  $\mathrm{Nr}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}} f(\zeta_{p^n}) \equiv 1 \pmod{p^n}$  for each  $n \in \mathbb{Z}_{>1}$ . Note that we have  $(1 - \zeta_{p^n}) \nmid f(\zeta_{p^n})$  in  $\mathbb{Z}[\zeta_{p^n}]$ . Indeed, if  $(1 - \zeta_{p^n}) \mid f(\zeta_{p^n})$ , then  $f(t) \equiv (1-t)g(t) \pmod{\Phi_{p^n}(t)}$  and hence  $f(t) - (1-t)g(t) = \Phi_{p^n}(t)h(t)$  for some  $g(t), h(t) \in \mathbb{Z}[t]$ . By putting  $t = 1$ , we obtain  $f(1) = ph(1)$ , and hence  $p \mid f(1)$ .

By  $(1 - \zeta_{p^n}) \nmid f(\zeta_{p^n})$  in  $\mathbb{Z}[\zeta_{p^n}]$ , we have  $(f(\zeta_{p^n})) \in I_{p^n}(\mathbb{Q}(\zeta_{p^n}))$ . Applying Lemma 2.10.2 for  $K/k = \mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$  and  $\mathfrak{M} = (p^n)\infty$ , we obtain a natural isomorphism

$$I_{p^n}(\mathbb{Q})/P_{p^n\infty}(\mathbb{Q})\mathrm{Nr}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}}(I_{p^n}(\mathbb{Q}(\zeta_{p^n}))) \xrightarrow{\cong} \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^*$$

sending  $\mathrm{Nr}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}} f(\zeta_{p^n})$  to  $1 \pmod{p^n}$ . This means that  $\mathrm{Nr}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}} f(\zeta_{p^n}) \equiv 1 \pmod{p^n}$ . Hence  $(\mathrm{Res}(t^{p^n} - 1, f(t)))_n$  is a  $p$ -adic Cauchy sequence and converges in the  $p$ -adic completion  $\mathbb{Z}_p$  of  $\mathbb{Z}$ . In this case, the limit value is not zero.

Even if  $p \mid f(1)$ , if we replace  $f(\zeta_{p^n})$  in above by its non- $p$  part  $a_{p^n} = f(\zeta_{p^n})(1 - \zeta_{p^n})^{-v_n} \in I_{p^n}\mathbb{Q}(\zeta_{p^n})$ , where  $v_n = v_{(1-\zeta_{p^n})}(f(\zeta_{p^n}))$ , then a similar argument shows that  $\mathrm{Nr}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}} a_{p^n} \equiv 1 \pmod{p^n}$  and hence the assertion on the non- $p$  parts of  $\mathrm{Res}(t^{p^n} - 1, f(t))$ 's.

For each  $l \neq p$ , if  $p \nmid f(1)$ , then  $|\mathrm{Nr}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}} f(\zeta_{p^n})|_l^{-1} \equiv 1 \pmod{p^n}$  holds. A similar argument proves the assertion for the  $l$ -parts. The assertion for the  $p$ -parts is clear.  $\square$

**Remark 2.10.4.** In a study of  $l$ -adic convergence in Iwasawa towers of varieties over finite fields, G. Asvin recently proved a result close to our heart by using a method different from ours; His result [3, Corollary 5] asserts that if  $f(t)$  and  $g(t)$  are monic in  $\mathbb{Z}_l[t]$ , then  $\text{Res}(f(t), g(t^{l^{n+1}})) \equiv \text{Res}(f(t), g(t^{l^n})) \pmod{l^{n+1}}$ . He derives the assertion from a variant of Fermat's little theorem due to Arnold–Zarelua [97, Theorem 4]; For  $A \in M_r(\mathbb{Z}_l)$ ,  $\text{tr}(A^{l^{n+1}}) \equiv \text{tr}A^{l^n} \pmod{l^{n+1}}$  holds.

### 2.10.3 Explicit formula

Let  $\mathbb{C}_p$  denote the  $p$ -adic completion of an algebraic closure of the  $p$ -adic numbers  $\mathbb{Q}_p$  and fix an embedding  $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$ . Let  $\overline{\mathbb{Z}}_p$  denote the closure of  $p$ -adic integers  $\mathbb{Z}_p$  in  $\mathbb{C}_p$ . Since extensions of  $\mathbb{F}_p$  are cyclotomic extensions of degrees prime to  $p$ , an elementary  $p$ -adic number theory yields the following basic fact.

**Lemma 2.10.5** (cf. [80, Lemma 2.10]). *If  $\alpha \in \mathbb{C}_p$  satisfies  $|\alpha|_p = 1$ , then there exists a unique root of unity  $\zeta$  of order prime to  $p$  satisfying  $|\alpha - \zeta|_p < 1$ .*

The following lemma is also elementary and classically known.

**Lemma 2.10.6.** *Let  $\alpha, \zeta \in \mathbb{C}_p$  with  $|\alpha|_p = |\zeta|_p = 1$ .*

- (1) *If  $|\alpha - \zeta|_p < 1$ , then  $\lim_{n \rightarrow \infty} \alpha^{p^n} - \zeta^{p^n} = 0$  in  $\mathbb{C}_p$ .*
- (2) *If  $|\alpha - 1|_p < 1$ , then  $\lim_{n \rightarrow \infty} \frac{\alpha^{p^n} - 1}{p^n} = \log \alpha$  in  $\mathbb{C}_p$ , where  $\log$  denotes the  $p$ -adic logarithm defined by  $\log(1 + x) = \sum_{n=1}^{\infty} \frac{-(-x)^n}{n}$  on  $\overline{\mathbb{Z}}_p$ .*
- (3) *If  $|\alpha - 1|_p < p^{-1/(p-1)}$ , then  $|\log \alpha|_p = |1 - \alpha|_p$ .*

*Proof.* (1) Define a  $(\omega_n)_n$  by  $\omega_1 = \gcd\{p(\alpha - \zeta), (\alpha - \zeta)^p\}$  and  $\omega_{n+1} = \gcd\{p\omega_n, \omega_n^p\}$  for all  $n$ , where  $\gcd$  of a finite subset  $A \subset \overline{\mathbb{Z}}_p$  means the maximal power of a fixed uniformizer dividing all elements of  $A$ . Then we have  $\zeta^{p^n} = (\alpha - (\alpha - \zeta))^{p^n} = (\alpha^p + pg_1(\alpha, \zeta) + (\alpha - \zeta)^p)^{p^{n-1}} = (\alpha^p + \omega_1 h_1(\alpha, \zeta))^{p^{n-1}} = \dots = \alpha^{p^n} + \omega_n h_n(\alpha, \zeta)$  for some  $g_i(\alpha, \zeta), h_i(\alpha, \zeta) \in \mathbb{Z}[\alpha, \zeta]$ . Since  $\lim_{n \rightarrow \infty} \omega_n = 0$  and  $|h_n(\alpha, \zeta)|_p \leq 1$ , we have  $\lim_{n \rightarrow \infty} |\alpha^{p^n} - \zeta^{p^n}|_p = 0$ .

(2) If we put  $\varepsilon = \alpha - 1$ , then by an elementary  $p$ -adic calculus assures that

$$\lim_{n \rightarrow \infty} \frac{\alpha^{p^n} - 1}{p^n} = \lim_{n \rightarrow \infty} \frac{(1 + \varepsilon)^{p^n} - (1 + \varepsilon)^0}{p^n} = \frac{d}{dx} \exp((\log(1 + \varepsilon))x)|_{x=0} = \log(1 + \varepsilon) = \log \alpha.$$

(3) Put  $\varepsilon = \alpha - 1$ . Then the strong triangle inequality yields

$$|\log(1 + \varepsilon)|_p = \left| \sum_{n=1}^{\infty} (-1)^{n-1} \varepsilon^n / n \right|_p \leq \sup\{|\varepsilon^{p^k} / p^k|_p \mid k \in \mathbb{Z}_{\geq 0}\} = |\varepsilon|_p,$$

and the equality holds if the sequence  $|\varepsilon^{p^k} / p^k|_p$  takes distinct values when  $k$  moves. By the assumption, we have  $|\varepsilon|_p > |\varepsilon^p / p|_p$ , hence the equality.  $\square$

The following explicit formula is a key to our numerical study.

**Theorem 2.10.7.** Let  $0 \neq f(t) \in \mathbb{Z}[t]$  and let  $p^\mu$  denote the maximal  $p$ -power dividing  $f(t)$ . Write  $f(t) = a_0 \prod_i (t - \alpha_i)$  in  $\overline{\mathbb{Q}}[t]$  and note that  $|p^{-\mu} a_0 \prod_{|\alpha_i|_p > 1} \alpha_i|_p = 1$ . Let  $\xi$  and  $\zeta_i$  denote the unique roots of unity of orders prime to  $p$  satisfying  $|p^{-\mu} a_0 \prod_{|\alpha_j|_p > 1} \alpha_j - \xi|_p < 1$  and  $|\alpha_i - \zeta_i|_p < 1$  for each  $i$  with  $|\alpha_i|_p = 1$ .

- (1) (i) If  $p \mid f(t)$ , so that  $\mu > 0$ , then  $\lim_{n \rightarrow \infty} \text{Res}(t^{p^n} - 1, f(t)) = 0$  holds in  $\mathbb{Z}_p$ .  
(ii) If  $p \nmid f(t)$ , so that  $\mu = 0$ , then

$$\lim_{n \rightarrow \infty} \text{Res}(t^{p^n} - 1, f(t)) = (-1)^{p \deg f + \#\{i \mid |\alpha_i|_p < 1\}} \xi \prod_{i; |\alpha_i|_p = 1} (\zeta_i - 1)$$

holds in  $\mathbb{Z}_p$ , and the limit value is zero if and only if  $\zeta_i = 1$  for some  $i$ .

(2) In any case, the non- $p$  part  $\text{Res}(t^{p^n} - 1, f(t))_{\text{non-}p} = \text{Res}(t^{p^n} - 1, f(t)) | \text{Res}(t^{p^n} - 1, f(t))|_p$  converges to

$$(-1)^{p \deg f + \#\{i \mid |\alpha_i|_p < 1\}} \xi \left( \prod_{\substack{i; |\alpha_i|_p = 1, \\ |\alpha_i - 1|_p = 1}} (\zeta_i - 1) \right) p^{-\nu} \prod_{\substack{i; |\alpha_i|_p = 1, \\ |\alpha_i - 1|_p < 1}} \log \alpha_i$$

in  $\mathbb{Z}_p$ , where  $\log$  denotes the  $p$ -adic logarithm and  $\nu \in \mathbb{Z}$  is defined by  $p^{-\nu} = \prod_{i; |\alpha_i - 1|_p < 1} |\log \alpha_i|_p$ . If all  $\alpha_i$ 's with  $|\alpha_i - 1|_p < 1$  are sufficiently close to 1, that is, if they all satisfy  $|\alpha_i - 1|_p < p^{-1/(p-1)}$ , then  $p^\nu = |f(1)|_p^{-1}$  holds.

Put  $\lambda = \#\{i \mid |\alpha_i - 1|_p < 1\}$ . Then these  $\lambda, \mu, \nu$  are the Iwasawa invariants of  $f(t)$ , that is,  $|\text{Res}(t^{p^n} - 1, f(t))|_p^{-1} = p^{\lambda n + \mu p^n + \nu}$  holds for any  $n \gg 0$ .

If  $f(t)$  is monic and  $\deg f$  is even, then our theorem recovers [40, Proposition 2]:

$$\text{Res}(t^{p^n} - 1, f(t))_{\text{non-}p} = (-1)^\lambda \left( \prod_{i; |\alpha_i - 1|_p = 1} (1 - \zeta_i) \right) p^{-\nu} \prod_{i; |\alpha_i - 1|_p < 1} \log \alpha_i.$$

*Proof.* It suffices to verify the case with  $\mu = 0$ . By Lemma 2.10.5, if  $\alpha \in \mathbb{C}_p$  satisfies  $|\alpha|_p = 1$ , then there exists a unique root of unity  $\zeta$  of orders prime to  $p$  satisfying  $|\alpha - \zeta|_p < 1$ , and hence Lemma 2.10.6 (1) yields  $\lim_{n \rightarrow \infty} \alpha^{p^n} - \zeta^{p^n} = 0$  in  $\mathbb{C}_p$ . Note that

$$\text{Res}(t^{p^n} - 1, f(t)) = (-1)^{p \deg f} a_0^{p^n} \prod_i (\alpha_i^{p^n} - 1) = (-1)^{p \deg f} a_0^{p^n} \prod_i (\alpha_i^{p^n} - 1)$$

for  $n > 0$ . Since  $p \nmid f(t)$ , the Newton polygon verifies  $|a_0 \prod_{|\alpha_i|_p > 1} \alpha_i|_p = 1$ . Hence we have

$$\begin{aligned} \lim_{n \rightarrow \infty} a_0^{p^n} \prod_i (\alpha_i^{p^n} - 1) &= \lim_{n \rightarrow \infty} a_0^{p^n} \prod_{i; |\alpha_i|_p > 1} (\alpha_i^{p^n} - 1) \prod_{i; |\alpha_i|_p = 1} (\alpha_i^{p^n} - 1) \prod_{i; |\alpha_i|_p < 1} (\alpha_i^{p^n} - 1) \\ &= \lim_{n \rightarrow \infty} \xi^{p^n} \prod_{i; |\alpha_i|_p = 1} (\zeta_i^{p^n} - 1) \prod_{i; |\alpha_i|_p < 1} (-1). \end{aligned}$$

Take  $m \in \mathbb{Z}$  with  $p \nmid m$  and  $\xi^m = \zeta_i^m = 1$  for all  $i$ , and note that  $p^n \equiv 1 \pmod m$  holds if  $n \equiv 0 \pmod \varphi(m)$ . Since the sequence  $(\xi^{p^n} \prod_i (\zeta_i^{p^n} - 1))_n$  is periodic and converges by

Theorem 2.10.3, we have  $\xi^{p^n} \prod_i (\zeta_i^{p^n} - 1) = \xi^{p^{\varphi(m)}} \prod_i (\zeta_i^{p^{\varphi(m)}} - 1) = \xi \prod_i (\zeta_i - 1)$  for any  $n \in \mathbb{Z}_{\geq 0}$ . Therefore, the limit value is  $(-1)^{p \deg f + \#\{i \mid |\alpha_i|_p < 1\}} \xi \prod_{i; |\alpha_i|_p = 1} (\zeta_i - 1)$ .

For each root  $\alpha_i$  with  $|\alpha_i - 1|_p < 1$ , by Lemma 2.10.6 (2), we have  $\lim_{n \rightarrow \infty} (\alpha_i^{p^n} - 1)/p^n = \log \alpha_i$ . If we put  $p^\nu = |\prod_{i; |\alpha_i - 1|_p < 1} \log \alpha_i|_p^{-1}$ , then we obtain the limit value as asserted. In addition, if all  $\alpha_i$ 's with  $|\alpha_i - 1|_p < 1$  are sufficiently close to 1, then by Lemma 2.10.6 (2), we have  $p^\nu = |\prod_{i; |\alpha_i - 1|_p < 1} (\alpha_i - 1)|_p = |f(1)|_p^{-1}$ .

The  $p$ -adic Weierstrass preparation theorem [90, Theorem 7.3] and a standard argument of Iwasawa theory show that there exists some  $\lambda, \mu, \nu \in \mathbb{Z}$  satisfying the equality  $f(1 + T) \doteq p^\mu (T^\lambda + p(\text{lower terms}))$  up to multiplication by units in  $\mathbb{Z}_p[[T]]$  and  $|\text{Res}(t^{p^n} - 1, f(t))|_p^{-1} = p^{\lambda n + \mu p^n + \nu}$  for any  $n \gg 0$ . These  $\lambda, \mu, \nu$  clearly coincide with those in above.  $\square$

**Remark 2.10.8.** In the case of a  $\mathbb{Z}_p$ -extension or a  $\mathbb{Z}_p$ -cover, in general, Iwasawa's  $\nu$  is the sum of several contributions; that of the torsion of the base space, that of the pseudo isomorphism between the Iwasawa/Alexander module and the standard module, and that given in above. We will study examples with large  $\nu$ 's in Subsubsections 2.11.3 and 2.12.2.

**Remark 2.10.9.** The Mahler measure of a polynomial  $f(t)$  is defined by the integral along the unit circle as  $m(f(t)) = \int_{|z|=1} \log |f(z)| \frac{dz}{z}$  and coincides with the limit of the average of the values of  $\log |f(z)|$  at roots of unity. Its  $p$ -adic analogue due to Besser-Deninger is given by Shnirel'man's integral, that is, the  $p$ -adic limit of the average of values at roots of unity of orders prime to  $p$  (cf. [80]). Our  $p$ -adic limits in Theorem 2.10.7 may be seen as  $p$ -adic analogues of the Mahler measures in another direction.

**Corollary 2.10.10.** *Let  $0 \neq f(t) \in \mathbb{Z}[t]$  with leading coefficient 1. If  $f(t) \equiv \Phi_m(t) \pmod{p}$  for  $m \in \mathbb{Z}_{>0}$  with  $p \nmid m$ , then*

$$\lim_{n \rightarrow \infty} \text{Res}(t^{p^n} - 1, f(t)) = \Phi_m(1) = \begin{cases} l & \text{if } m = l^e \text{ for a prime number } l \text{ and } e \in \mathbb{Z}_{>0} \\ 1 & \text{if otherwise} \end{cases} \text{ in } \mathbb{Z}_p.$$

*Proof.* We have  $\lim_{n \rightarrow \infty} \text{Res}(t^{p^n} - 1, f(t)) = (-1)^{p \varphi(m)} \prod_{\zeta; \Phi_m(\zeta)=0} (\zeta - 1) = (-1)^{(p+1)\varphi(m)} \Phi_m(1)$ . If  $m = 2$ , then by  $p \nmid m$ ,  $p$  is odd. If  $m \neq 2$ , then  $\varphi(m)$  is even. In both cases, we have  $(-1)^{(p+1)\varphi(m)} = 1$ , hence the assertion.  $\square$

The following lemma is useful to study  $\mathbb{Z}_p$ -covers in a  $\widehat{\mathbb{Z}} = \varprojlim_{n \in \mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ -cover.

**Lemma 2.10.11.** *Let  $m \in \mathbb{Z}_{>0}$  with  $p \nmid m$  and  $\alpha \in \overline{\mathbb{Q}}$ . Then*

$$\text{Res}(t^{mp^n} - 1, t - \alpha) = \prod_{\zeta^m=1, \xi^{p^n}=1} (\zeta \xi - \alpha) = \prod_{\xi^{p^n}=1} (\xi - \alpha^m) = \text{Res}(t^{p^n} - 1, t - \alpha^m).$$

## 2.11 Knots

In this section, we apply our theorems to  $\mathbb{Z}_p$ -covers of knots to examine concrete examples and point out remarks on analogues of Weber's class number problem.



### 2.11.1 Alexander polynomial and Fox–Weber’s formula

Let  $K$  be a knot in  $S^3$  and let  $M_n \rightarrow S^3$  denote the branched  $\mathbb{Z}/n\mathbb{Z}$ -cover, that is, the Fox completion of the  $\mathbb{Z}/n\mathbb{Z}$ -cover  $X_n \rightarrow M = S^3 - K$ . Let  $\Delta_K(t)$  denote the Alexander polynomial of  $K$  normalized by  $\Delta_K(1) = 1$ . If  $\Delta_K(t)$  does not vanish on  $n$ -th roots of unity, then we have

**Proposition 2.11.1** (Fox–Weber’s formula, cf. [91]).

$$|H_1(M_n)| = |H_1(X_n)_{\text{tor}}| = |\text{Res}(t^n - 1, \Delta_K(t))|.$$

Since  $\Delta_K(1) = 1$ , Lemma 2.10.1 assures that we have  $\text{Res}(t^n - 1, \Delta_K(t)) < 0$  if and only if  $2 \mid n$  and  $\Delta_K(-1) < 0$ . Thus, both our Theorems 2.8.1 and 2.10.7 apply. We will exhibit concrete examples in the succeeding subsections.

We remark that Fox–Weber’s formula has several variants (cf. Sakuma [67, 68], Mayberry–Murasugi [49], and Porti [64] for links and graphs; Tange and Ueki [75, 84] for representations of knot groups). We may replace  $t^{p^n} - 1$  by  $(t^{p^n} - 1)/\text{gcd}(t^{p^n} - 1, f(t))$  in Theorems 2.10.3 and 2.10.7 and apply to these situations.

### 2.11.2 Torus knots

Let  $(a, b)$  be a coprime pair of integers. The Alexander polynomial

$$\Delta_K = \frac{(1-t)(1-t^{ab})}{(1-t^a)(1-t^b)} = \prod_{\substack{m|ab \\ m \nmid a, m \nmid b}} \Phi_m(t)$$

of the  $(a, b)$ -torus knot  $K = T_{a,b}$  is the product of cyclotomic polynomials. For each

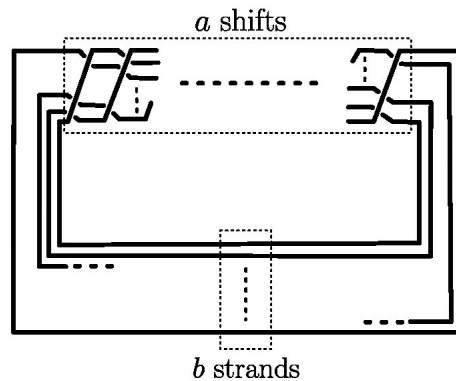


Figure 2.1: Torus knot  $T_{a,b}$

$n \in \mathbb{Z}_{>0}$ , let  $\varphi(n)$  denote Euler’s totient function. We invoke Apostol’s result;

**Lemma 2.11.2** ([1, Theorem 4]). *Suppose that  $m > n > 1$  and  $(m, n) > 1$ . Then,  $\text{Res}(\Phi_m, \Phi_n) = p^{\varphi(n)}$  if  $m/n$  is a power of a prime  $p$ , and  $\text{Res}(\Phi_m, \Phi_n) = 1$  if otherwise.*

**Proposition 2.11.3.** *Let  $p$  be a prime number and let  $(a, b)$  be a coprime pair of positive integers. Assume that  $p \nmid b$  and write  $a = p^r a'$  with  $r, a' \in \mathbb{Z}$ ,  $p \nmid a'$ . Let  $(M_{p^n} \rightarrow M)_n$  denote the  $\mathbb{Z}_p$ -cover of the exterior of the torus knot  $T_{a,b}$  in  $S^3$ . Then  $|H_1(M_{p^n})_{\text{tor}}| = b^{p^{\min\{n,r\}}-1}$  holds for every  $n \in \mathbb{Z}_{\geq 0}$ , and hence*

$$\lim_{n \rightarrow \infty} |H_1(M_{p^n})_{\text{tor}}| = b^{p^r-1} \quad \text{holds in } \mathbb{Z}_p.$$

*In particular, for each pair  $(a, b)$ , we have  $\lim_{n \rightarrow \infty} |H_1(M_{p^n})_{\text{tor}}| = 1$  for almost all  $p$ 's.*

*Proof.* Note that we have  $\Delta_K(-1) = (1+t^a + \cdots + t^{ab})/(1+t + \cdots + t^b)|_{t=-1} = 1$  or  $b > 0$  according as  $2 \nmid a$  or  $2 \mid a$ . By Fox's formula and Lemma 2.10.1, we have

$$\begin{aligned} |H_1(M_{p^n})_{\text{tor}}| &= \text{Res}(t^{p^n} - 1, \Delta_K(t)) \\ &= \text{Res}\left(\prod_{0 \leq i \leq n} \Phi_{p^i}(t), \prod_{\substack{m \mid ab \\ m \nmid a, m \nmid b}} \Phi_m(t)\right) \\ &= \prod_{0 \leq i \leq n} \prod_{\substack{m \mid ab \\ m \nmid a, m \nmid b}} \text{Res}(\Phi_{p^i}(t), \Phi_m(t)). \end{aligned}$$

Since  $(a, b)$  is a coprime pair, Lemma 2.11.2 assures that  $\text{Res}(\Phi_{p^i}(t), \Phi_m(t)) \neq 1$  if and only if  $m = p^i l^j$  for some prime number  $l$  and an integer  $j \in \mathbb{Z}_{>0}$  satisfying  $l^j \mid b$ . Let  $v_l(b)$  denote the standard multiplicative  $l$ -adic valuation of  $b$ . Then, by  $\sum_{0 \leq i \leq n} \varphi(p^i) = p^n - 1$ , we have

$$\begin{aligned} |H_1(M_{p^n})_{\text{tor}}| &= \prod_{0 \leq i \leq \min\{n,r\}} \prod_{l \mid b} \prod_{0 \leq j \leq v_l(b)} \text{Res}(\Phi_{p^i}(t), \Phi_{p^i l^j}(t)) \\ &= \prod_{0 \leq i \leq \min\{n,r\}} \prod_{l \mid b} \prod_{0 \leq j \leq v_l(b)} l^{\varphi(p^i)} \\ &= b^{p^{\min\{n,r\}}-1}. \end{aligned}$$

Hence we obtain the assertion. □

**Example 2.11.4.** Let  $K = T_{2,3} = J(2, 2) = 3_1$  (trefoil). Then we have  $\Delta_K(t) = t^2 - t + 1 = \Phi_6(t)$ . We have  $\text{Res}(t^{2^n} - 1, \Delta_K(t)) = 3 = 3^{2-1}$ ,  $\text{Res}(t^{3^n} - 1, \Delta_K(t)) = 4 = 2^{3-1}$ , and  $\text{Res}(t^{p^n} - 1, \Delta_K(t)) = 1 = 3^{0-1}$  for  $p \neq 2, 3$  for all  $n \in \mathbb{Z}_{>0}$ .

### 2.11.3 Twist knots

For each  $m \in \mathbb{Z}$ , the Alexander polynomial of the twist knot  $K = J(2, 2m)$  is given by  $\Delta_{J(2,2m)}(t) = mt^2 + (1 - 2m)t + m$ . The convention is due to [33], so that we have  $J(2, 2) = 3_1$  and  $J(2, -2) = 4_1$  for instance.

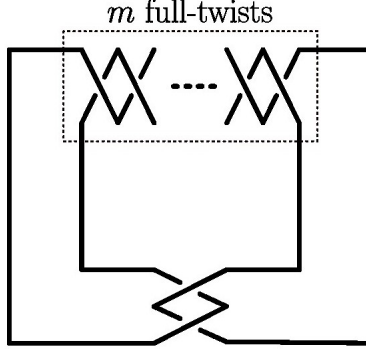


Figure 2.2: Twist knot  $J(2, 2m)$

### Observations for $K = 4_1$

We first examine  $K = 4_1$  to demonstrate the usage of our results and raise questions.

**Example 2.11.5.** Let  $K = J(2, -2) = 4_1$  (the figure-eight knot). Then we have  $\Delta_K(t) = -t^2 + 3t - 1$  and

$p$	2	3	5	7	$\dots$
$\lim_{n \rightarrow \infty}  H_1(M_{p^n})_{\text{tor}} $	-3	-2	-4	$\sqrt{2} - 2$	$\dots$

where  $\alpha = \sqrt{2} \in \mathbb{Z}_7$  denotes the element satisfying  $\alpha^2 = 2$  and  $\alpha \equiv 3 \pmod{7}$ . By using PARI/GP [63], we may verify that

$n$	1	2	3	4	5	6	$\dots$
$\text{Res}(t^{7^n} - 1, \Delta_K(t)) \pmod{7^n}$	1	8	106	2164	4565	38179	$\dots$

We have  $\lim_{n \rightarrow \infty} |H_1(M_{p^n})_{\text{tor}}| \in \mathbb{Z}$  only for  $p = 2, 3, 5$ .

*Proof.* Since  $\Delta_K(-1) = -5 < 0$ , we have  $\lim_{n \rightarrow \infty} |H_1(M_{2^n})_{\text{tor}}| = -\lim_{n \rightarrow \infty} \text{Res}(t^{2^n} - 1, \Delta_K(t))$  in  $\mathbb{Z}_2$  and  $\lim_{n \rightarrow \infty} |H_1(M_{p^n})_{\text{tor}}| = \lim_{n \rightarrow \infty} \text{Res}(t^{p^n} - 1, \Delta_K(t))$  in  $\mathbb{Z}_p$  for  $p \neq 2$  by Lemma 2.10.1.

If  $p = 2$ , then  $\Delta_K(t) \equiv t^2 + t + 1 = \Phi_3(t) \pmod{2}$ . Hence by Theorem 2.10.7, we have  $\lim_{n \rightarrow \infty} \text{Res}(t^{2^n} - 1, \Delta_K(t)) = \text{Res}(t^2 - 1, \Phi_3(t)) = 3$  in  $\mathbb{Z}_2$ .  $\lim_{n \rightarrow \infty} |H_1(M_{2^n})_{\text{tor}}| = -3$  in  $\mathbb{Z}_2$ .

If  $p = 3$ , then  $\Delta_K(t) \equiv -(t^2 + 1) = -\Phi_4(t) \pmod{3}$ , and hence  $\lim_{n \rightarrow \infty} |H_1(M_{3^n})_{\text{tor}}| = \text{Res}(t^3 - 1, -\Phi_4(t)) = -2$  in  $\mathbb{Z}_3$ .

If  $p = 5$ , then  $\Delta_K(t) \equiv -(t+1)^2 = -\Phi_2(t)^2 \pmod{5}$ , and hence  $\lim_{n \rightarrow \infty} |H_1(M_{5^n})_{\text{tor}}| = \text{Res}(t^5 - 1, -(t+1)^2) = -2^2 = -4$  in  $\mathbb{Z}_5$ .

If  $p = 7$ , then  $\Delta_K(t) \equiv -((t+2)^2 - 3) \equiv -\phi_8^+ \pmod{7}$ , where  $\Phi_8 = t^4 + 1 = \phi_8^+ \phi_8^-$ ,  $\phi_8^\pm = t^2 \pm \sqrt{2}t + 1$ . Let  $\zeta$  be a primitive 8th root of unity satisfying  $\zeta + \bar{\zeta} \equiv -4 \equiv 3 \pmod{7}$ . Then  $\lim_{n \rightarrow \infty} |H_1(M_{7^n})_{\text{tor}}| = -(\zeta - 1)(\bar{\zeta} - 1) = -(2 - (\zeta + \bar{\zeta})) = -(2 - (\sqrt{2})) = -2 + \sqrt{2}$ .

Since  $\deg \Phi_m(t) = \varphi(m)$ , the only cyclotomic polynomials of degree  $\leq 2$  are those for  $m = 1, 2, 3, 4, 6$ , and  $t^2 - 3t + 1 \pmod{p}$  for  $p \geq 7$  is not obtained as the product of them. Hence we have  $\lim_{n \rightarrow \infty} |H_1(M_{p^n})_{\text{tor}}| \in \mathbb{Z}$  only for  $p = 2, 3, 5$ .  $\square$

**Example 2.11.6.** Let us examine the  $\mathbb{Z}/3^{12^n}\mathbb{Z}$ -covers of  $K = 4_1$ . Write  $\Delta_K(t) = -t^2 + 3t - 1 = -(t - \alpha)(t - \beta)$ . Put  $\Delta_3(t) = -(t - \alpha^3)(t - \beta^3)$ . Then we have  $\Delta_3(t) = -t^2 + (\alpha^3 + \beta^3)t - \alpha^3\beta^3 = -t^2 + 18t - 1 \equiv -(t - 1)^2 \pmod{2}$ ,  $\Delta_3(1) = 16 > 0$ ,  $\Delta_3(-1) = -20 < 0$ . By Lemmas 2.10.1 and 2.10.11, we have  $|H_1(M_{3 \cdot 2^n})_{\text{tor}}| = -\text{Res}(t^{3 \cdot 2^n} - 1, \Delta_K(t)) = -\text{Res}(t^{2^n} - 1, \Delta_3(t))$  for  $n > 0$ . By  $|a^3 + b^3|_2 = |18|_2 = 1/2$  and  $\alpha^3\beta^3 = 1$ , we have  $|\alpha^3|_2 = |\beta^3|_2 = 1$ . Since  $\alpha^3 - 1$  and  $\beta^3 - 1$  are roots of  $\Delta_K^3(t + 1) = t^2 - 16t - 16$ , we see that  $|\alpha^3 - 1|_2 = |\beta^3 - 1|_2 = 1/4 < 2^{-1/(2-1)} = 1/2$  and hence  $2^{-\nu} = |f(1)|_2 = 2^{-4}$ . The value  $|H_1(M_{3 \cdot 2^n})_{\text{non-2}}| = |H_1(M_{3 \cdot 2^n})_{\text{tor}}| 2^{-(2n+4)} = -\text{Res}(t^{3 \cdot 2^n} - 1, \Delta_K(t)) 2^{-(2n+4)} = -\text{Res}(t^{2^n} - 1, \Delta_3(t)) 2^{-(2n+4)}$  converges to  $-\frac{(\log \alpha^3)(\log \beta^3)}{2^4} = \frac{-9}{16} \log \alpha \log \beta$ , where  $\log$  denotes the 2-adic logarithm extended to  $\mathbb{C}_2$  so that  $\log 2 = 0$ .

$n$	0	1	2	3	4	5	6	7	8	9	10	...
$-\text{Res}(t^{3 \cdot 2^n} - 1, \Delta_K(t)) 2^{-(2n+4)}$	1	5	405	10498005	...							...
$\pmod{2^n}$	1	1	1	5	5	21	21	85	213	213	213	...

Kionke [39] discusses whether the  $p$ -adic Betti number belongs to  $\mathbb{Z}$ , as the  $p$ -adic analogue of Atiyah's conjecture. It also would be interesting to ask when the  $p$ -adic torsion belongs to  $\mathbb{Z}$ . The observations for  $J(2, -2) = 4_1$  raise the following questions, to which we will give answers in the rest of this subsection.

**Question 2.11.7.** Consider the cyclic covers  $X_n \rightarrow M = S^3 - J(2, 2m)$ .

(1) Find all pairs  $(p, m)$  with  $\lim_{n \rightarrow \infty} |H_1(M_{p^n})_{\text{tor}}| \in \mathbb{Z} \subset \mathbb{Z}_p$  and their limit values. Find all pairs  $(p, m)$  with  $\lim_{n \rightarrow \infty} |H_1(M_{p^n})_{\text{tor}}| = 1$ .

(2) Find conditions of  $(e, p)$  with  $p \nmid e$  such that  $\lim_{n \rightarrow \infty} |H_1(M_{ep^n})_{\text{tor}}| = 0$  holds, and study the values of  $\nu$ . Can  $\nu$  be arbitrarily large, with  $|H_1(M_e)_{\text{tor}}|$  being small?

**Cases with  $\lim |H_1(M_{p^n})_{\text{tor}}| \in \mathbb{Z}$**

We discuss both of the cases with  $p \mid m$  and  $p \nmid m$ .

**Proposition 2.11.8.** If  $p \mid m$ , then the  $\mathbb{Z}_p$ -covers of  $K = J(2, 2m)$  satisfies

$$\lim_{n \rightarrow \infty} |H_1(M_{p^n})_{\text{tor}}| = \begin{cases} -\text{sgn}(4m - 1) & \text{if } p = 2, \\ 1 & \text{if } p \neq 2 \end{cases} \quad \text{in } \mathbb{Z}_p.$$

*Proof.* Write  $\Delta_K(t) = m(t - \alpha)(t - \beta)$ . Then by  $|\alpha + \beta|_p = |(2m - 1)/m|_p = |1/m|_p > 1$  and  $\alpha\beta = 1$ , we may assume that  $|\alpha|_p > |\beta|_p$  and hence  $|\alpha|_p = |\alpha + \beta|_p = |1/m|_p$ . Then  $\lim_{n \rightarrow \infty} \text{Res}(t^{p^n} - 1, \Delta_K(t)) = \lim_{n \rightarrow \infty} m^{p^n} (\alpha^{p^n} - 1)(\beta^{p^n} - 1) = \lim_{n \rightarrow \infty} -(m\alpha)^{p^n}$ . The minimal polynomial of  $m\alpha$  is  $(t - m\alpha)(t - m\beta) = t^2 - m(\alpha + \beta) + m^2\alpha\beta = t^2 + (1 - 2m)t + m^2 \equiv t^2 + t = t(t + 1) \pmod{p}$ . Thus  $m\alpha \equiv -1 \pmod{p}$  and hence  $\lim_{n \rightarrow \infty} -(m\alpha)^{p^n} = -1$  if  $p = 2$ ,  $\lim_{n \rightarrow \infty} -(m\alpha)^{p^n} = 1$  if  $p \neq 2$  in  $\mathbb{Z}_p$ . Note that if  $p = 2$ , then we have an additional term  $\text{sgn}\Delta(-1) = \text{sgn}(4m - 1)$  by Lemma 2.10.1.  $\square$

**Example 2.11.9.** Let  $K = J(2, 4) = 5_2$ . Then  $\Delta_K(t) = 2t^2 - 3t + 2$ ,  $\Delta_K(-1) = 7 > 0$ , and

$n$	1	2	3	4	...
$\text{Res}(t^{2^n} - 1, \Delta_K(t))$	7	63	63	60543	...
$\text{mod } 2^n$	1	3	7	15	...

Let  $K = J(2, -4)$ . Then  $\Delta_K(t) = -2t^2 + 5t - 2$ ,  $\Delta_K(-1) = -9 < 0$  and

$n$	1	2	3	4	...
$-\text{Res}(t^{2^n} - 1, \Delta_K(t))$	-9	-225	-65025	-4294836225	...
$\text{mod } 2^n$	1	1	1	1	...

Let  $K = J(2, 6)$ . Then  $\Delta_K(t) = 3t^2 - 5t + 3$  and

$n$	1	2	3	4	...
$\text{Res}(t^{3^n} - 1, \Delta_K(t))$	64	18496	30417519283264	1729618048727305550814328969659247936576	...
$\text{mod } 3^n$	1	1	1	1	...

**Proposition 2.11.10.** *Suppose  $p \nmid m$ . Then the  $\mathbb{Z}_p$ -cover of  $K = J(2, 2m)$  satisfies  $\lim = \lim_{n \rightarrow \infty} |H_1(M_{p^n})_{\text{tor}}| \in \mathbb{Z}$  in  $\mathbb{Z}_p$  if and only if one of the following holds.*

- $p = 2$ ;  $\lim = \text{sgn}(4m - 1) \cdot 3 = \pm 3$ .
- $p = 3$ ;  $3 \mid m - 1$ ,  $\lim = 4$  or  $3 \mid m + 1$ ,  $\lim = -2$ .
- $p = 5$ ;  $5 \mid m + 1$ ,  $\lim = -4$ .
- $p \neq 2, 3$ ;  $p \mid m - 1$ ,  $\lim = 1$ .

*Proof.* In what follows,  $x \equiv y$  stands for  $x \equiv y \pmod{p}$  if otherwise mentioned. Let  $\xi$  and  $\zeta$  denote the unique root of unity of order prime to  $p$  with  $|m - \xi|_p < 1$  and  $\Delta_K(t) \equiv \xi(t - \zeta)(t - \zeta^{-1}) \pmod{p}$ . Note that if  $\lim \text{Res}(t^{p^n} - 1, \Delta_K(t)) = \xi(1 - \zeta)(1 - \zeta^{-1}) \in \mathbb{Z}$ , then we have  $\xi = \pm 1$  and  $\zeta^6 = 1$ , so  $\Delta_K(t)/m \equiv (t - 1)^2, (t + 1)^2, t^2 + t + 1, t^2 + 1, \text{ or } t^2 - t + 1$ . Note that  $\xi \equiv \pm 1$  is equivalent to that  $p \mid m^2 - 1$ .

Since  $\text{Res}(\Delta_K(t), (t + 1)^2) = (4m - 1)^2$ ,  $\text{Res}(\Delta_K(t), t^2 + t + 1) = (3m - 1)^2$ ,  $\text{Res}(\Delta_K(t), t^2 + 1) = (2m - 1)^2$ , and  $\text{Res}(\Delta_K(t), t^2 - t + 1) = (m - 1)^2$ , we have  $\Delta_K(t) \equiv m(t + 1)^2$  if  $p \mid 4m - 1$ ,  $\Delta_K(t) \equiv m(t^2 + t + 1)$  if  $p \mid 3m - 1$ ,  $\Delta_K(t) \equiv m(t^2 + 1)$  if  $p \mid 2m - 1$ , and  $\Delta_K(t) \equiv m(t^2 - t + 1)$  if  $p \mid m - 1$ , while  $\Delta_K(t) \equiv m(t - 1)^2$  is not the case.

Suppose  $p \mid m - 1$ , so that  $m \equiv 1$ . If  $\Delta_K(t) \equiv (t + 1)^2$ , then by  $0 \equiv (4m - 1)^2 \equiv 3^2$ , we have  $p = 3$ . If  $\Delta_K(t) \equiv t^2 + t + 1$ , then by  $0 \equiv (3m - 1)^2 \equiv 2^2$ , we have  $p = 2$ . If  $\Delta_K(t) \equiv t^2 + 1$ , then  $0 \equiv (2m - 1)^2 \equiv 1$ , which is not the case. If  $\Delta_K(t) \equiv t^2 - t + 1$ , then by  $0 \equiv (m - 1)^2$ , we just have  $p \mid m - 1$ . (In this case, we need  $p \neq 2, 3$ .)

Suppose instead  $p \mid m + 1$ , so that  $m \equiv -1$ . If  $-\Delta_K(t) \equiv (t + 1)^2$ , then by  $0 \equiv (4m - 1)^2 \equiv 5^2$ , we have  $p = 5$ . If  $-\Delta_K(t) \equiv t^2 + t + 1$ , then by  $0 \equiv (3m - 1)^2 \equiv 2^4$ , we have  $p = 2$ . If  $-\Delta_K(t) \equiv t^2 + 1$ , then by  $0 \equiv (2m - 1)^2 \equiv 3^2$ , we have  $p = 3$ . If

$-\Delta_K(t) \equiv t^2 - t + 1$ , then by  $0 \equiv (m-1)^2 \equiv 2^2$ , we have  $p = 2$ . (In this case, by  $2 \mid 6$ , Corollary 2.10.10 does not apply, while  $-\Delta_K(t) \equiv t^2 + t + 1$  also holds.)

If  $p = 2$ , then  $\Delta_K(t) \equiv t^2 - t + 1$ . Lemma 2.10.1 yields  $|H_1(M_{2^n})_{\text{tor}}| = \text{sgn}(\Delta_K(-1))\text{Res}(t^{2^n} - 1, \Delta_K(t)) = \text{sgn}(4m - 1)\text{Res}(t^{2^n} - 1, \Delta_K(t))$  and hence  $\lim = \text{sgn}(4m - 1) \cdot 3$ . If  $p = 3$  and  $3 \mid m - 1$ , then  $\lim = \text{Res}(t - 1, (t + 1)^2) = 2^2 = 4$ . If  $p = 3$  and  $3 \nmid m - 1$ , then  $\lim = \text{Res}(t - 1, -(t + 1)^2) = -2$ . If  $p = 5$  and  $5 \mid m + 1$ , then  $\lim = \text{Res}(t - 1, -(t + 1)^2) = -4$ . If  $p \neq 2, 3$  and  $p \mid m - 1$ , then  $\lim = \text{Res}(t - 1, t^2 - t + 1) = 1$ . Combining these above, we obtain the assertion and complete the table.  $\square$

By Propositions 2.11.8 and 2.11.10, we may conclude the following.

**Corollary 2.11.11.** *We have  $\lim_{n \rightarrow \infty} |H_1(M_{p^n})_{\text{tor}}| = 1$  if and only if one of the following holds.*

- $p = 2$ ,  $m$  is even, and  $4m - 1 < 0$ .
- $p \neq 2$  and  $p \mid m$ .
- $p \neq 2, 3$  and  $p \mid (m - 1)$ .

Particularly, for each  $m \neq 0$ , we have  $\lim_{n \rightarrow \infty} |H_1(M_{p^n})_{\text{tor}}| = 1$  for only finitely many  $p$ 's.

We discuss further problems about the cases with  $\lim = 1$  in Subsection 2.11.4.

### Can $\nu$ be large with $r_e$ being small?

We next investigate the Iwasawa  $\nu$ -invariants of  $\mathbb{Z}_p$ -covers  $(M_{ep^n} \rightarrow X_e)_n$  of  $K = J(2, 2m)$  with  $e \in \mathbb{Z}_{>0}$ , whilst essential cases would be those with  $p \nmid e$ . Put  $r_n = \text{Res}(t^n - 1, \Delta_K(t))$ . We have  $\nu > 0$  if  $\lim_{n \rightarrow \infty} |H_1(M_{ep^n})_{\text{tor}}| = 0$  in  $\mathbb{Z}_p$ . More precisely, we have the following. Note that  $r_{ep^n} = 0$  for some  $n$  is equivalent to  $m = 1$  and  $6 \mid ep$ .

**Proposition 2.11.12.** *For the  $\mathbb{Z}_p$ -cover  $(M_{ep^n} \rightarrow X_e)_n$  of  $K = J(2, 2m)$  and  $r_{ep^n} \neq 0$ , the following conditions are equivalent.*

- $\lim |H_1(M_{ep^n})_{\text{tor}}| = 0$  in  $\mathbb{Z}_p$ .
- $\lim |H_1(M_{ep^n})_{\text{non-}p}| \notin \overline{\mathbb{Q}}$ .
- $|H_1(M_e)_{\text{tor}}| \equiv 0 \pmod{p}$ .
- $(M_{ep^n} \rightarrow X_e)_n$  has  $\nu > 0$ .

Furthermore, except for the following special cases, we have  $p^{-\nu} = |H_1(M_e)_{\text{tor}}|_p$ .

- $p = 3$ ,  $2 \mid e$ ,  $|r_2|_3 = |r_e|_3 = 1/3$ .
- $p = 2$ ,  $|r_e|_2 = 1/4$ .

*Proof.* Write  $\Delta_K(t) = m(t - \alpha)(t - \beta)$  and put  $\Delta_e(t) = m^e(t - \alpha^e)(t - \beta^e)$ , so that we have  $r_e = m^e(1 - \alpha^e)(1 - \beta^e) = m^e(2 - (\alpha^e + \beta^e))$ ,  $\Delta_e(t) = m^e t^2 + (r_e - 2m^e)t + m^e$ , and  $\Delta_e(t + 1) = m^e(t - (\alpha^e - 1))(t - (\beta^e - 1)) = m^e t^2 + r_e t + r_e$ .

Suppose that  $p \mid r_e$ . Then we have  $|\alpha^e - 1|_p = |\beta^e - 1|_p = |r_e|_p^{1/2}$ . If  $p > 3$ , then  $|r_e|_p^{1/2} \leq p^{-1/2} < p^{-1/(p-1)}$ , and hence  $|\log \alpha^e|_p = |\log \beta^e|_p = |r_e|_p^{1/2}$  and  $p^{-\nu} = |H_1(M_e)_{\text{tor}}|_p$ . If instead  $p = 3$  and  $3^2 \mid r_e$ , then by  $|r_e|_p^{1/2} \leq p^{-1} < p^{-1/(p-1)}$ , we obtain a similar result. If instead  $p = 2$  and  $2^4 \mid r_e$ , then by  $|r_e|_p^{1/2} \leq 2^{-2} < 2^{-1} = p^{-1/(p-1)}$ , we obtain a similar result. Thus, we obtain the assertion.  $\square$

**Example 2.11.13.** Let  $K = J(2, 2) = 3_1$  with  $\Delta_K(t) = t^2 - t + 1$ . For  $e \leq 10$ , we have

$$\frac{e}{\text{Res}(t^e - 1, \Delta_K(t))} \parallel \begin{array}{c|c|c|c|c|c|c|c|c|c} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \hline 1 & 3 & 2^2 & 3 & 1 & 0 & 1 & 3 & 2^2 & 3 \end{array},$$

- $\nu = 1$  for  $(e, p) = (2, 3), (4, 3), (6, 3), (8, 3)$ ,
- $\nu = 2$  for  $(e, p) = (3, 2), (9, 2)$ .

Let  $K = J(2, -2) = 4_1$  with  $\Delta_K(t) = -t^2 + 3t - 1$ . For  $e \leq 10$ , we have

$$\frac{e}{\text{Res}(t^e - 1, \Delta_K(t))} \parallel \begin{array}{c|c|c|c|c|c|c|c|c|c} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \hline 1 & -5 & 2^4 & -3^2 5 & 11^2 & -2^8 5 & 29^2 & -3^2 5^1 7^2 & 2^4 19^2 & -5^3 11^2 \end{array},$$

- $\nu = 1$  for  $(e, p) = (2, 5), (4, 5), (6, 5), (8, 5)$ ,
- $\nu = 2$  for  $(e, p) = (4, 3), (5, 11), (7, 29), (8, 3), (8, 7), (9, 19), (10, 11)$ ,
- $\nu = 4$  for  $(e, p) = (3, 2), (9, 2)$ .

Let  $K = J(2, 4) = 5_2$  with  $\Delta_K(t) = 2t^2 - 3t + 2$ . For  $e \leq 10$ , we have

$$\frac{e}{\text{Res}(t^e - 1, \Delta_K(t))} \parallel \begin{array}{c|c|c|c|c|c|c|c|c|c} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \hline 1 & 7 & 5^2 & 3^2 7 & 11^2 & 5^2 7 & 13^2 & 3^2 7 & 5^2 & 7^1 11^2 \end{array},$$

- $\nu = 1$  for  $(e, p) = (2, 7), (4, 7), (6, 7), (8, 7)$ ,
- $\nu = 2$  for  $(e, p) = (3, 5), (4, 3), (5, 11), (6, 5), (7, 13), (8, 3), (9, 5), (10, 11)$ .

**Example 2.11.14** (Large base  $p$ -class number). For  $K = J(2, 2m)$ , we have  $r_2 = 4m - 1$ ,  $r_3 = 9m^2 - 6m + 1 = (3m - 1)^2$ , and  $r_4 = (2m - 1)^2(4m - 1)$ . Under the assumption of Proposition 2.11.12, if  $p \mid 4m - 1$  with exponent 1, then we have  $\nu = 1$  for even  $e$ . If instead  $p \nmid 4m - 1$  and  $p \mid r_e$ , then  $\nu$  is even.

For any  $p > 3$  and  $a \in \mathbb{Z}_{\geq 0}$ , if we put  $m = (p^a + 1)/2$ , then we have  $p^a = 2m - 1$  and  $|r_4|_p = p^{-2a}$ . Hence for  $e = 4$ , we have  $\nu = 2a$ .

For any  $p$  with  $p \equiv 3 \pmod{4}$  and  $a \in \mathbb{Z}_{\geq 0}$ , if we put  $m = (3^{2a+1} + 1)/4$ , then we have  $r_2 = 4m - 1 = p^{2a+1}$ . Hence for  $e = 2$ , we have  $\nu \geq 2a + 1$ .

For  $p = 2$  and  $a \in \mathbb{Z}_{\geq 0}$ , if we put  $m = (2^{2c+1} + 1)/3$ , then we have  $r_3 = (3m - 1)^2 = 2^{2+2b} = 2^{2+4c}$ . Hence for  $e = 3$ , we have  $\nu \geq 2 + 4c$ .

**Example 2.11.15** (Small base  $p$ -class number and large  $\nu$ ). Let us examine the two exceptional cases in Proposition 2.11.12. In these cases,  $|r_e|_p = 1/p$  holds and  $\nu$  becomes arbitrarily large.

(1) Suppose  $p = 3$  and  $|r_2|_3 = 1/3$ . Then, since  $r_2 = 4m - 1$ , we have  $m = 3a + 1$  with  $a = 3b$  or  $3b + 1$ , and hence  $m = 9b + 1$  or  $9b + 4$ ,  $b \in \mathbb{Z}$ . (i) If  $m = 9b + 1$ , then  $r_6 = 3^5 b^2 (12b + 1)(27b + 2)^2$ ,  $|r_6|_3 = |3^5 b^2|_3$ . By Proposition 2.11.12 and  $\lambda = 2$ , we have  $\nu = v_3(r_6) - 2 = 5 + 2v_3(b) - 2 = 3 + 2v_3(b)$ . For instance, if we put  $b = 3^c$  with  $c \in \mathbb{Z}$ , then we obtain  $m = 3^{c+2} + 1$  and  $\nu = 3 + 2c$  for  $(p, e) = (3, 2)$ . More concretely, if we put  $c = 8$ , then we see that the  $\mathbb{Z}_3$ -cover  $(M_{2^{13^n}} \rightarrow X_3)_n$  of  $K = J(2, 2(3^{10} + 1)) = J(2, 118100)$  with  $e = 2$  has  $\nu = 19$ . (ii) If instead  $m = 9b + 4$ , then by  $|r_6|_3 = 1/3^3$ ,  $(M_{2^{13^n}} \rightarrow X_3)_n$  has  $\nu = 1$ .

(2) Suppose  $p = 2$  and  $|r_3|_2 = 1/4$ . Then by  $r_3 = (3m - 1)^2$ , we have  $3m - 1 = 2(2a + 1)$ ,  $a = 3b$ ,  $m = 4b + 1$ ,  $b \in \mathbb{Z}$ . Since  $r_6 = 2^6 b^2 (6b + 1)^2 (16b + 3)$  and  $\lambda = 2$ , Proposition 2.11.12 yields that  $\nu = v_2(r_6) - 2 = 6 + 2v_2(b) - 2 = 4 + 2v_2(b)$ . For instance, if we put  $b = 2^c$  with  $c \in \mathbb{Z}$ , then we have  $m = 2^{c+2} + 1$  and  $\nu = 4 + 2c$ . More concretely, if we put  $c = 48$ , then the  $\mathbb{Z}_2$ -cover  $(M_{2^{31^n}} \rightarrow X_3)_n$  of  $K = J(2, 2(2^{50} + 1))$  with  $e = 3$  has  $\nu = 100$ .

By Examples 2.11.14 and 2.11.15, we may conclude the following.

**Proposition 2.11.16.** *For any  $p$  and arbitrary large  $N > 0$ , we may find  $K = J(2, 2m)$  and  $p \nmid e$  such that the  $\mathbb{Z}_p$ -cover  $(M_{ep^n} \rightarrow X_e)_n$  has  $\nu > N$ . Furthermore, for  $(p, e) = (2, 3), (3, 2)$ , we may find such  $\mathbb{Z}_p$ -covers with the base  $p$ -class number  $|H_1(X_e)_{(p)}| = 4, 3$  respectively.*

For a general knot  $K$  and a small  $p$ , we may have a slightly large  $\nu$ , namely,  $p^{-\nu} < |H_1(X_e)_{\text{tor}}|_p$  holds. Nevertheless, such  $p$  is bounded by the degree of  $\Delta_K(t)$ , and hence a fixed  $K$  has bounded  $\nu$ 's when  $(p, e)$  moves.

**Remark 2.11.17.** For any  $\mathbb{Z}_p$ -cover  $(M_{ep^n} \rightarrow X_e)_n$  of a knot  $K$  in  $S^3$ , we always have  $\nu \geq 0$ . This is not the case for a general link in  $S^3$ . Indeed, let  $L_m = K_1 \cup K_2$  be the  $m$ -twisted Whitehead link in  $S^3$  with the Alexander polynomial  $\Delta(t_1, t_2) = m(1 - t_1)(1 - t_2)$  and let  $M_n \rightarrow M = S^3 - L_m$  denote the ‘‘total linking number’’  $\mathbb{Z}/n\mathbb{Z}$ -cover, that is, the cover corresponding to the kernel of the surjective homomorphism  $\pi_1(M) \rightarrow \mathbb{Z}/n\mathbb{Z}$  sending all meridians of  $L_m$  to 1. If we put  $m = p^\mu$  with  $\mu \in \mathbb{Z}_{\geq 0}$ , then a formula of Mayberry–Murasugi [49] or Porti [64] yields that  $|H_1(M_{p^n})_{\text{tor}}| = p^n \prod_{\zeta; \zeta^{p^n}=1, \zeta \neq 1} \Delta(\zeta, \zeta) = p^{3n+\mu p^n-\mu}$  and hence  $\nu = -\mu$  may take any non-positive integer if  $\mu$  moves. The cases of links with multivariable Alexander polynomials will be extensively discussed in [76].

## 2.11.4 Livingston’s results

In the knot theory side, we may choose the extension degree  $p$  and the branch locus  $K$  independently, so we may consider several analogues of Weber’s class number problem.



Livingston’s result in the following considers the set of all prime numbers. We may also verify this assertion by using Lemma 2.11.2.

**Proposition 2.11.18** (Livingston [46, Theorem 1.2]). *Let  $K$  be a knot in  $S^3$ . Then, the equality  $|H_1(M_{p^n})_{\text{tor}}| = 1$  holds for every prime number  $p$  and positive integer  $n$  if and only if every non-trivial factor of the Alexander polynomial  $\Delta_K(t)$  is the  $m$ -th cyclotomic polynomial with  $m$  being divisible by at least three distinct prime numbers.*

**Example 2.11.19.** Note that a knot with any prescribed Alexander polynomial may be constructed by Rolfsen’s method in [65]. Namely, if we have  $\Delta(t) \in \mathbb{Z}[t]$  with  $\Delta(1) = 1$  and  $\Delta(t) = t^{\deg \Delta(t)} \Delta(1/t)$ , then we have a knot  $K$  with  $\Delta_K(t) = \Delta(t)$ .

There are many knots with  $\Delta_K(t) = 1$ . A knot  $K$  with  $\Delta_K(t) = \Phi_{30}(t) = t^8 + t^7 - t^5 - t^4 - t^3 + t + 1$  would be the initial example with  $\Delta_K(t) \neq 1$  satisfying  $|H_1(M_{p^n})_{\text{tor}}| = 1$  for all  $p$  and  $n$ . A systematic study of such knots would be of further interest.

If  $p$  is a fixed prime number, then a knot  $K$  with  $\Delta_K(t) = \Phi_{30}(t) + p(t^6 - t^5 - t^3 + t^2)$  satisfies  $\lim_{n \rightarrow \infty} |H_1(M_{p^n})_{\text{tor}}| = 1$  and  $(|H_1(M_{p^n})|)_n \neq (1)$ . We wonder if there exists a knot with  $\lim_{n \rightarrow \infty} |H_1(M_{p^n})_{\text{tor}}| = 1$  and  $(|H_1(M_{p^n})_{\text{tor}}|)_n \neq (1)$  for infinitely many  $p$ ’s.

A subtle question from a viewpoint of the Sato–Tate conjecture in number theory (cf. Subsubsection 2.12.2) is to ask *whether there exist a knot  $K$  such that the set  $P(K)$  of  $p$ ’s with  $\lim_{n \rightarrow \infty} |H_1(M_{p^n})_{\text{tor}}| = 1$  is an infinite set but the density of  $P(K)$  in the set of all prime numbers is zero*. As we have seen in Proposition 2.11.3 and Corollary 2.11.11, torus knots  $T_{a,b}$  and twist knots  $J(2, 2m) \neq 0_1$  are two extreme cases on the opposite sides; they satisfy  $\lim_{n \rightarrow \infty} |H_1(M_{p^n})_{\text{tor}}| = 1$  and  $\neq 1$  for almost all  $p$ , respectively. We wonder if there is a class with an intermediate behavior.

Another approach to formulating an analogue of the Sato–Tate conjecture is to consider an infinite family  $(K_i)_{i \in \mathbb{Z}_{>0}}$  of disjoint knots in  $S^3$  satisfying some equidistribution theorem, such as the Chebotarev law (cf. [52, 53, 81, 82]). It would be interesting to study the density of knots with the  $p$ -adic torsion being 1 for each fixed  $p$ . A possible clue is Dehornoy’s study on the Lorenz knots ( $\equiv$  modular knots) in [17], which is an analogue of the Riemann/Weil conjecture in a view of Noguchi [60].

For a branched  $\mathbb{Z}_p$ -cover  $(M_{p^n} \rightarrow M_1)_n$ , to ask whether all  $M_{p^n}$ ’s are QHS<sup>3</sup>’s, or equivalently, to whether every  $H_1(M_{p^n})$  is a finite group, is also a weak analogue of Weber’s problem. By  $\Delta_K(1) = 1$ , we have the following.

**Proposition 2.11.20** ([46, Corollary 3.2]). *The branched  $\mathbb{Z}/p^n\mathbb{Z}$ -cover of a knot in  $S^3$  is always a QHS<sup>3</sup>.*

This proposition means that Kionke’s  $p$ -adic Betti number is zero. It would be also interesting to study  $p$ -adic refinements of [46, Theorem 1.1] and [38] on concordance.

## 2.12 Algebraic curves

Theorems on the  $p$ -adic limit of cyclic resultants are applicable to algebraic curves (function fields) as well. We examine the cases of elliptic curves as examples and point out conditions for the  $p$ -adic limit value being zero and one.

### 2.12.1 A formula for function fields

Let us recollect some properties of function fields to obtain an analogue of Fox–Weber’s formula. Basic references are due to Rosen [66] and Stichtenoth [72].

Let  $k$  be a finite extension of  $\mathbb{F}_l(x)$ ,  $l$  being a prime number. (We use  $l$  instead of  $p'$ .) Let  $\mathbb{F}(k)$  denote the constant field of  $k$  and put  $q = l^e = |\mathbb{F}(k)|$ . Let  $\mathcal{D}_k$ ,  $\mathcal{P}_k$ , and  $\mathcal{E}_k$  denote the set of divisors, that of principal divisors, and that of effective divisors of  $k$  respectively. Put  $\mathcal{D}_k^n = \{A \in \mathcal{D}_k \mid \deg A = n\}$  and  $\mathcal{E}_k^n = \{A \in \mathcal{E}_k \mid \deg A = n\}$  for each  $n \in \mathbb{Z}_{\geq 0}$ . Let  $g(k)$  denote the genus of  $k$ . The congruent zeta function of  $k$  is defined by

$$\zeta_k(s) = \sum_{A \in \mathcal{E}_k} \frac{1}{(q^{\deg A})^s}$$

and satisfies

$$\zeta_k(s) = \sum_{n=0}^{\infty} \frac{|\mathcal{E}_k^n|}{(q^n)^s} = \prod_{P \in \mathcal{P}_k} \left(1 - \frac{1}{(q^{\deg P})^s}\right)^{-1}.$$

This Dirichlet series is known to absolutely converges to a holomorphic function on  $\operatorname{Re}(s) > 1$ . Moreover, we have the following.

**Proposition 2.12.1** (Hasse–Weil, cf. [93], [66, Theorem 5.9]). *There exists  $L_k(t) \in \mathbb{Z}[t]$  of degree  $2g(k)$  satisfying*

$$\zeta_k(s) = \frac{L_k(q^{-s})}{(1 - q^{-s})(1 - q^{1-s})}$$

on  $\operatorname{Re}(s) > 1$ .

This  $L_k(t)$  is called *the  $L$ -polynomial of  $k$* . The right-hand side is an analytic continuation of  $\zeta_k(s)$  to  $\mathbb{C}$  as a meromorphic function. In addition, we have the following.

- $L_k(0) = 1$ ,  $L_k(1) = |\operatorname{Cl}^0(k)|$ ,
- $L_k(t) = q^{g(k)} t^{2g(k)} L_k\left(\frac{1}{qt}\right)$ ,
- $L_k(t) = \prod_{i=1}^{2g(k)} (1 - \alpha_i t)$  for some algebraic integers  $\alpha_i$  with  $|\alpha_i| = \sqrt{q}$ .

If we write  $L_k(t) = a_{2g(k)} t^{2g(k)} + \cdots + a_1 t + a_0$ , then we have  $a_0 = 1$ ,  $a_1 = |\mathcal{E}_k^1| - (q + 1)$ ,  $a_{2g(k)} = q^{g(k)}$ , and  $a_{2g(k)-i} = q^{g(k)-i} a_i$  for  $0 \leq i \leq 2g(k)$ . If  $k_n/k$  be a constant extension of degree  $n$ , then we have  $k_n = k \mathbb{F}(k_n)$ ,  $g(k_n) = g(k)$ ,  $L_{k_n}(t) = \prod_{i=1}^{2g(k)} (1 - \alpha_i^n t)$ , and hence

$$|\operatorname{Cl}^0(k_n)| = L_{k_n}(1) = \prod_{i=1}^{2g(k)} (1 - \alpha_i^n) = \operatorname{Res}(t^n - 1, t^{2g(k)} L_k(1/t)).$$

For any prime number  $l' \neq l$ , *the Frobenius polynomial  $F_k(t)$  of  $k$*  is defined as the characteristic polynomial of the geometric Frobenius action on the  $l'$ -adic étale cohomology of the algebraic curve corresponding to  $k$  and satisfies  $F_k(t) = t^{2g(k)} L_k(1/t)$  (cf. [4]). Hence we obtain the following (See also [40, Section 2]).

**Proposition 2.12.2.** *Let  $k$  be a function field and  $k_n/k$  a constant extension of degree  $n$ . Then*

$$|\mathrm{Cl}^0(k_n)| = |\mathrm{Res}(t^n - 1, F_k(t))|.$$

This formula may be seen as an analogue of Fox–Weber’s formula (Proposition 2.11.1) for a constant extension of a function field.

In a geometric extension of a function field, the genera may grow (cf. [41]). In the cases of knots, if we remove the assumption that  $\Delta_K(t)$  does not vanish on roots of unity, then the 1st Betti numbers grow. We may expect further analogies there.

## 2.12.2 Elliptic curves

We observe the cases of elliptic curves as examples. Basic literatures are Silverman [71] and Diamond–Shurman [19]. Let  $E$  be an elliptic curve over a finite field  $\mathbb{F}$  and let  $k$  denote the function field of  $E$ , that is, we have  $k_E = \mathrm{Frac}(\mathbb{F}[x, y]/(E(x, y)))$ . In addition, let  $E(\mathbb{F})$  denote the Mordell–Weil group, that is, the union of the set of  $\mathbb{F}$ -rational points of  $E$  and  $\{\infty\}$ . Write  $F_E(t) = F_k(t)$ . Then, we have  $|\mathrm{Cl}^0(k_E)| = F_E(1) = |E(\mathbb{F})|$ . Let  $\mathbb{F}'/\mathbb{F}$  be a finite extension and let  $E_{\mathbb{F}'}$  denote the same elliptic curve with the coefficient field replaced by  $\mathbb{F}'$ . Then we have  $k_{E_{\mathbb{F}'}} = \mathbb{F}'k_E$  and  $|\mathrm{Cl}^0(k_{E_{\mathbb{F}'}})| = F_{E_{\mathbb{F}'}}(1) = |E(\mathbb{F}')|$ . If  $\mathbb{F} = \mathbb{F}_l$ , then the Frobenius polynomial of  $E$  is given by

$$F_E(t) = t^2 - (l + 1 - |E(\mathbb{F}_l)|)t + l.$$

Write  $F_E(t) = (t - \alpha)(t - \beta)$ . For each  $e \in \mathbb{Z}_{>0}$  and  $n \in \mathbb{Z}_{\geq 0}$ , write  $E_{\mathbb{F}_{l^{ep^n}}} = E_{l^{ep^n}}$ . Then,

$$F_{E_{l^{ep^n}}}(t) = (t - \alpha^{ep^n})(t - \beta^{ep^n})$$

coincides with the Frobenius polynomial of the constant  $\mathbb{Z}/p^n\mathbb{Z}$ -extension  $k_{E_{l^{ep^n}}}$  of  $k_{E_{l^e}}$ .

In what follows, we first examine a fixed elliptic curve over  $\mathbb{F}_5$  for  $p = 2, 3, 5$  and  $e = 1, 3$  and raise a question. Secondly, we study conditions for  $\lim_{n \rightarrow \infty} |\mathrm{Cl}^0(k_{E_{l^{pn}}})| \in \mathbb{Z}$  with focus on the cases with  $p = l$ . Finally, we discuss the Iwasawa  $\nu$ -invariants for the cases with  $\lim_{n \rightarrow \infty} |\mathrm{Cl}^0(k_{E_{l^{pn}}})| = 0$ .

### Observations

We examine the cases of  $E : y^2 = x^3 + 3x + 3$ ,  $l = 5$ ,  $e = 1, 3$ ,  $p = 2, 3, 5$ .

**Example 2.12.3.** Let  $l = 5$  and  $E : y^2 = x^3 + 3x + 3$ . Then  $|E(\mathbb{F}_5)| = F_{E_5}(1) = 5$  and  $F_{E_5}(t) = t^2 - (5 + 1 - 5)t + 5 = t^2 - t + 5$ .

If  $p = 2$ , then by  $t^2 - t + 5 \equiv (t^2 + t + 1) = \Phi_3(t) \pmod{2}$  and  $F_{E_5}(-1) = 5 > 0$ , we have  $\lim_{n \rightarrow \infty} |\mathrm{Cl}^0(E_{5^{2^n}})| = \Phi_3(1) = 3$ .

If  $p = 3$ , then by  $t^2 - t + 5 \equiv t^2 + 2t + 2 \pmod{3}$ , we have  $\lim_{n \rightarrow \infty} |\mathrm{Cl}^0(E_{5^{3^n}})| = 1 - \frac{-1 + \sqrt{-1}}{2} = \frac{3 - \sqrt{-1}}{2}$ , where  $\zeta = \frac{-1 + \sqrt{-1}}{2}$  is a primitive 8-th root of unity with  $\zeta + \bar{\zeta} \equiv -2$ ,  $\zeta\bar{\zeta} \equiv 2 \pmod{3}$ .

If  $p = 5$ , then by  $F_{E_5}(1) = 5$ , we have  $\lim_{n \rightarrow \infty} |\text{Cl}^0(E_{5^{5^n}})| = 0$  in  $\mathbb{Z}_5$ . Let  $\alpha = \frac{1+\sqrt{-19}}{2}$  denote the larger root of  $F_E(t) = t^2 - t + 5$ , so that  $|\alpha|_l$  holds. Since  $\alpha - 1$  is the smaller root of  $E_F(1+t) = t^2 + t + 5$ , we see  $|\alpha - 1|_5 = 5^{-1} < 5^{-1/4}$ . Thus, we have  $\lambda = \nu = 1$  and the value  $|\text{Cl}^0(E_{5^{5^n}})_{\text{non-5}}| = |\text{Cl}^0(E_{5^{5^n}})| 5^{-(n+1)}$  converges to a non-zero value  $\lim_{n \rightarrow \infty} \text{Res}(t^{5^n} - 1, t^2 - t + 5) 5^{-(n+1)} = \lim_{n \rightarrow \infty} \frac{1 - \alpha^{5^n}}{5^{n+1}} = \frac{-\log \alpha}{5} = \frac{-1}{5} \log \frac{1+\sqrt{-19}}{2}$ ;

$n$	1	2	3	4	5	6	...
$\text{Res}(t^{5^n} - 1, F_{E_5}(t)) 5^{-(n+1)}$	$11^2$	$11^2 \times 19704014845201$	...				...
mod $5^n$	1	21	71	321	1571	14071	...

**Example 2.12.4.** Let the notation be as in Example 2.12.3 and put  $q = 5^3$  for instance. Then  $F_{E_{5^3}}(t) = (t - \alpha^3)(t - \beta^3) = t^2 + 14t + 125$ ,  $F_{E_{5^3 p^n}}(t) = (t - \alpha^{3p^n})(t - \beta^{3p^n})$ , and hence  $|\text{Cl}^0(E_{5^3 p^n})| = F_{E_{5^3 p^n}}(1) = \text{Res}(t^{p^n} - 1, t^2 + 14t + 125)$ . Note that  $F_{E_{5^3}}(1) = 140$ .

If  $p = 2$ , then by  $2 \mid 140$ , we have  $\lim_{n \rightarrow \infty} |\text{Cl}^0(E_{5^3 \cdot 2^n})| = 0$  in  $\mathbb{Z}_2$ . Since  $t^2 + 14t + 125 \equiv t^2 + 1 = (t - 1)^2 \pmod{2}$ , we have  $\lambda = 2$  and  $|\text{Cl}^0(E_{5^3 \cdot 2^n})| 2^{-2n}$  converges to a non-zero value in  $\mathbb{Z}_2$ . Since  $|\alpha^3 - 1|_2 < 1$ ,  $|\beta^3 - 1|_2 < 1$ , and  $|(\alpha^3 - 1)(\beta^3 - 1)|_2 = |140|_2 = 2^{-2} \geq (2^{-1})^2$ , we may have  $\nu > 2$ . In fact, we have  $\nu = 4$ ; If we put  $\varepsilon = \alpha^3 - 1$  or  $\beta^3 - 1$ , then a direct calculation shows that  $|\varepsilon|_2 = |\varepsilon^2/2|_2 = 1/2$ ,  $|\varepsilon - \varepsilon^2/2|_2 = |\varepsilon^4/4|_2 = 1/4$ ,  $|\varepsilon - \varepsilon^2/2 - \varepsilon^4/4|_2 = 1/4$ , while other terms satisfy  $|\varepsilon^n/n|_2 < 1/4$ . Thus, we have  $|\log \alpha^3|_2 = |\log \beta^3|_2 = 2^{-2}$ ,  $\nu = 4$ , and  $\lim_{n \rightarrow \infty} |\text{Cl}^0(E_{5^3 \cdot 2^n})_{\text{non-2}}| = 2^{-4} (\log \alpha^3)(\log \beta^3) = \frac{9}{16} (\log \alpha)(\log \beta)$ , where  $\log$  denotes the 2-adic logarithm extended to  $\mathbb{C}_2$  so that  $\log 2 = 0$ ;

$n$	0	1	2	3	4	5	6	7	8	9	10	...
$\text{Res}(t^{2^n} - 1, F_{E_{5^3}}(t)) 2^{-2n-4}$	$35/4$	7	245	953785	...							...
mod $2^n$		1	1	1	1	17	17	17	145	401	401	...

If  $p = 3$ , then by  $3 \nmid 140$  and  $t^2 + 14t + 125 \equiv t^2 + 2t + 2 \pmod{3}$ , the limit is the same as the case with  $q = 5$ .

If  $p = 5$ , then by  $5 \mid 140$ , we have  $\lim_{n \rightarrow \infty} |\text{Cl}^0(E_{5^3 \cdot 5^n})| = 0$ . By  $|\alpha^3 - 1|_5 = |F_{E_{5^3}}(1)| = 5^{-1} < 5^{-1/4}$  and  $|\beta^3 - 1|_5 = 1$ , we have  $\lambda = \nu = 1$ , and the value  $|\text{Cl}^0(E_{5^3 \cdot 5^n})_{\text{non-5}}| = |\text{Cl}^0(E_{5^3 \cdot 5^n})| 5^{-(n+1)}$  converges to a non-zero value  $\frac{-\log \alpha^3}{5} = \frac{-3 \log \alpha}{5} = \frac{-3}{5} \log \frac{1+\sqrt{-19}}{2}$ .

The following question is an analogue of Question 2.11.7 for elliptic curves;

**Question 2.12.5.** Consider the constant  $\mathbb{Z}/n\mathbb{Z}$ -extensions of the function field of an elliptic curve over  $\mathbb{F}_l$ .

(1) Find all cases with  $\text{lim} = \lim_{n \rightarrow \infty} |\text{Cl}^0(k_{E_{l p^n}})| \in \mathbb{Z}$ . Find conditions for the limits being specific values, especially for the case with  $\text{lim} = 1$ .

(2) Find conditions of  $(e, p)$  with  $p \nmid e$  such that  $\lim_{n \rightarrow \infty} |\text{Cl}^0(k_{E_{l e p^n}})| = 0$  holds, and study the values of  $\nu$ . Can  $\nu$  be arbitrarily large, while  $|\text{Cl}^0(k_{E_{l e}})|$  being small?

**Cases with  $\lim |Cl^0(k_{E_{l^n}})| \in \mathbb{Z}$**

First, we focus on the cases with  $p = l$ .

**Example 2.12.6.** Let  $E : y^2 = x^3 - 1$  with good reduction at  $l \neq 2, 3$ . Let us investigate the  $\mathbb{Z}_l$ -extension of  $k_E$ . We have  $F_E(t) = t^2 - (l + 1 - |E(\mathbb{F}_l)|)t + l$ . By Hasse's bound  $|E(\mathbb{F}_l)| - (l + 1) \leq 2\sqrt{l}$ , we have  $l \mid (l + 1 - |E(\mathbb{F}_l)|)$  if and only if  $l + 1 - |E(\mathbb{F}_l)| = 0$ . By [19, Exercise 8.3.6], we have  $|E(\mathbb{F}_l)| \equiv 1$  if and only if  $l \equiv 2 \pmod{3}$ . Thus, if  $l \equiv 2 \pmod{3}$ , then both roots of  $F_E(t) = t^2 + l$  are smaller than 1, and hence  $\lim_{n \rightarrow \infty} |Cl^0(k_{E_{l^n}})| = 1$ . If instead  $l \equiv 1 \pmod{3}$ , then the larger root  $\alpha$  of  $F_E(t)$  satisfies  $|\alpha|_l = 1$  and  $\lim_{n \rightarrow \infty} |Cl^0(k_{E_{l^n}})| = 1 - \zeta$  holds for the  $l$ -prime-th root of  $\zeta$  with  $|\alpha - \zeta|_l < 1$ . We have  $\zeta = 1$  if and only if  $|E(\mathbb{F}_l)| \equiv 1 - (-1)^{(l-1)/6} \binom{(l-1)/3}{(l-1)/2} \equiv 0 \pmod{l}$ , which is in fact not the case by [61].

**Definition 2.12.7** (cf.[51, 43, 19]). Let  $E$  be an elliptic curve over  $\mathbb{Q}$  with good reduction at  $\mathbb{F}_l$ . If  $|E(\mathbb{F}_l)| \equiv 1 \pmod{l}$ , then  $l$  is called a *supersingular prime* of  $E$ . If  $|E(\mathbb{F}_l)| \equiv 0 \pmod{l}$ , then  $l$  is called an *anomalous prime* of  $E$ . We say that  $E$  has *complex multiplication (CM)* over  $\mathbb{Q}(\sqrt{D})$  with  $D < 0$  if  $\text{End}(E)$  is isomorphic to an order of the ring of integers of  $\mathbb{Q}(\sqrt{D})$ .

Put  $a = 1 + l - |E(\mathbb{F}_l)|$ . Since  $F_E(t) = t^2 - at + l \equiv t(t - a) \pmod{l}$ , we have  $\lim_{n \rightarrow \infty} \text{Res}(t^{l^n} - 1, F_E(t)) \in \mathbb{Z}$ , then we have  $\lim_{n \rightarrow \infty} \text{Res}(t^{l^n} - 1, F_E(t)) = 0, 1, 2$  in  $\mathbb{Z}_l$  according as  $t - a \equiv t - 1, t, t + 1 \pmod{l}$  and  $|E(\mathbb{F}_l)| \equiv 0, -1, 1$  respectively. By Hasse's bound  $|a| \leq 2\sqrt{l}$ , we always have  $F_E(1) \geq 0$  and  $F_E(-1) \geq 0$ . Hence these limits coincide with  $\lim_{n \rightarrow \infty} |Cl^0(k_{E_{l^n}})|$  for any  $l$ . Thus, we obtain the following.

**Proposition 2.12.8.** *Let  $E$  be an elliptic curve over  $\mathbb{Q}$  with good reduction at  $\mathbb{F}_l$ . If the limit  $\lim_{n \rightarrow \infty} |Cl^0(k_{E_{l^n}})|$  in  $\mathbb{Z}_p$  is a rational integer, then  $\lim_{n \rightarrow \infty} |Cl^0(k_{E_{l^n}})| = 0, 1, 2$ . Moreover,*

- *We have  $\lim_{n \rightarrow \infty} |Cl^0(k_{E_{l^n}})| = 0$  in  $\mathbb{Z}_l$  if and only if  $l$  is an anomalous prime, that is,  $|E(\mathbb{F}_l)| \equiv 0 \pmod{l}$  holds. We mostly have  $\nu = 1$  and the only exceptional cases are those with  $l = 2$ ,  $|E(\mathbb{F}_l)|_2 = 1/2$ , and  $\nu = 2$  (see Propositions 2.12.13 and Example 2.12.14).*

- *We have  $\lim_{n \rightarrow \infty} |Cl^0(k_{E_{l^n}})| = 1$  in  $\mathbb{Z}_l$  if and only if  $l$  is a supersingular prime of  $E$ , that is,  $|E(\mathbb{F}_l)| \equiv 1 \pmod{l}$  holds. If in addition  $E$  has CM over  $\mathbb{Q}(\sqrt{D})$  with  $D < 0$ , then  $\lim_{n \rightarrow \infty} |Cl^0(k_{E_{l^n}})| = 1$  in  $\mathbb{Z}_l$  if and only if the Legendre symbol satisfies  $(\frac{D}{l}) \neq -1$ .*

- *We have  $\lim_{n \rightarrow \infty} |Cl^0(k_{E_{l^n}})| = 2$  if and only if  $|E(\mathbb{F}_l)| \equiv 2 \pmod{l}$  holds.*

Let  $E$  be an elliptic curve over  $\mathbb{Q}$  and put  $a_l = 1 + l - |E(\mathbb{F}_l)|$ . If  $l \geq 5$ , then the Hasse bound  $|a_l| \leq 2\sqrt{l}$  yields the following table of  $\lim = \lim_{n \rightarrow \infty} |Cl^0(k_{E_{l^n}})|$ .

$ E(\mathbb{F}_l) $	$a_l$	lim	$l$
$l$	1	0	anomalous
$l + 1$	0	1	supersingular
$l + 2$	-1	2	-

Elkies [22] proved that every  $E$  has infinitely many supersingular primes. Mazur asked in [51, Section 1, b)] whether there are infinitely many anomalous primes, which is now proved in the affirmative for most cases [5, Corollary 4.3]. Primes with  $a_l \equiv -1$  also appears in [5, Remark 2.6]. In addition, Namba–Sato and Serre–Tate’s conjecture in the 1960s and Lang–Trotter’s refinement expect the following: Let  $N_E$  denote the conductor of  $E$ , let  $r \in \mathbb{Z}$ , and assume additionally  $r \neq 0$  if  $E$  is CM. Then,  $\pi_{E,r}(x) = \{l \mid l < x, a_l = r, l \nmid N_E\} \sim C_{E,r} \sqrt{x} / \log x$  for a constant  $C_{E,r} \geq 0$  (cf. [43, 88]). Hence, by the prime number theorem  $\pi(x) = \{l \mid l < x\} \sim x / \log x$  and the Hasse bound, the density of each of such primes in the set of all primes is expected to be zero, assuming  $r \neq 0$  if  $E$  is CM.

**Example 2.12.9.** Let  $E : y^2 = x^3 - 5$ . Then  $l = 37$  is known to be an anomalous prime of  $E$ . We have  $F_E(t) = t^2 - t + 37 \equiv t(t-1) \pmod{37}$  and hence  $\lim_{n \rightarrow \infty} |\text{Cl}^0(k_{E_{l^n}})| = 0$ . Put  $\alpha = \frac{1+\sqrt{-147}}{2}$  and  $\beta = \frac{1-\sqrt{-147}}{2}$  so that we have  $F_E(t) = (t - \alpha)(t - \beta)$  with  $1/l = |\beta|_l < |\alpha|_l = 1$ . Since  $\alpha - 1$  is the smaller root of  $F_E(1+t) = t^2 + t + 37$ , we have  $|\alpha - 1|_l = 1/l < l^{-1/(l-1)}$  and hence  $|\log \alpha|_l = 1/l$ . By Proposition 2.12.2 and Theorem 2.10.7, we have  $\lambda = \nu = 1$  and the value  $|\text{Cl}^0(k_{E_{l^n}})_{\text{non-}l}| = |\text{Cl}^0(k_{E_{l^n}})| l^{-(n+1)}$  converges to a non-zero value  $\lim_{n \rightarrow \infty} \text{Res}(t^{l^n} - 1, F_E(t)) l^{-(n+1)} = \lim_{n \rightarrow \infty} \frac{1 - \alpha^{l^n}}{l^{n+1}} = \frac{-\log \alpha}{l} = \frac{-1}{37} \log \frac{1 + \sqrt{-147}}{2}$ ;

$$\frac{n}{\text{Res}(t^{37^n} - 1, F_E(t)) 37^{-(n+1)} \pmod{37^n}} \begin{array}{c|cccc} 0 & 1 & 2 & 3 & \dots \\ \hline 1 & 1 & 741 & 13062 & \dots \end{array}.$$

Next, let us briefly examine the cases with  $p \neq l$ . Since  $F_E(t)$  is monic, the argument becomes much easier than the case of twist knots in Proposition 2.11.10, yielding the following.

**Proposition 2.12.10.** *If  $\lim = \lim |\text{Cl}^0(k_{E_{l^{ep^n}}})| \in \mathbb{Z}$ , then according as  $F_E(t) = t^2 - at + l \equiv (t+1)^2, (t-1)^2, (t+1)(t-1), t^2 + t + 1, t^2 + 1, t^2 - t + 1 \pmod{p}$ , we have  $\lim = 4, 0, 0, 3, 2, 1$  respectively. Especially,  $\lim = 1$  if and only if  $l \equiv 1$  and  $a = 2 - |E(\mathbb{F}_l)| \equiv -1 \pmod{p}$ .*

Propositions 2.12.8, 2.12.10 complete the list of the cases with the  $p$ -adic limit being in  $\mathbb{Z}$ . The cases with  $\lim = 0$  will be further discussed in below.

### Can $\nu$ be large with $r_e$ being small?

For an elliptic curve  $E$  over  $\mathbb{F}_l$  with the function field  $k$ , let  $k_n/k$  denote the constant  $\mathbb{Z}/n\mathbb{Z}$ -extension. Here we give a slightly systematic study of the Iwasawa  $\nu$ -invariants and answer the following question.

**Question 2.12.11** (A paraphrase of Question 2.12.5 (2)). *For any  $N > 0$ , find a  $\mathbb{Z}_p$ -extension  $k_{ep^n}/k_e$  with  $p \nmid e$ ,  $|\text{C}(k_e)_{(p)}| < p^\nu$ ,  $\nu > N$ .*

Put  $F(t) = t^2 - (l+1 - |E(\mathbb{F}_l)|)t + l$ ,  $a = l+1 - |E(\mathbb{F}_l)|$ . By Hasse’s bound, we have  $|a| \leq 2\sqrt{l}$ . Put  $r_n = \text{Res}(t^n - 1, F(t))$ , so that we have  $|r_1| = |E(\mathbb{F}_l)|$ ,  $|r_n| = |\text{C}(k_n)|$ . If we write  $F(t) = (t - \alpha)(t - \beta)$ , then we have  $r_n = 1 + l^n - (\alpha^n + \beta^n)$ . A similar argument to Proposition 2.11.12 yields the following.

**Proposition 2.12.12.** *For any  $e \in \mathbb{Z}_{>0}$ , the following conditions are equivalent.*

- $\lim_{n \rightarrow \infty} |\mathbb{C}(k_{ep^n})| = 0$  in  $\mathbb{Z}_p$
- $\lim_{n \rightarrow \infty} |\mathbb{C}(k_{ep^n})_{non-p}| \notin \overline{\mathbb{Q}}$
- $|\mathbb{C}(k_e)| \equiv 0 \pmod{p}$
- $(k_{ep^n}/k_e)_n$  has  $\nu > 0$ .

Furthermore, except for the following special cases, we have  $p^\nu = |\mathbb{C}(k_e)_{(p)}|$ .

- $p = 3, |r_e|_3 = 1/3$ .
- $p = 2, |r_e|_2 = 1/2, 1/4$ .

Since  $F(t)$  has less symmetricity than the  $\Delta_K(t)$  of twist knots, we have slightly more exceptional cases than in Proposition 2.11.12. More precisely, we have the following.

**Proposition 2.12.13.** (1) *If  $p \nmid l^e - 1$ , then  $F_e(t)$  has just one root which is close to 1, and the only exceptional cases are  $p = l = 2, |r_e|_2 = 1/2, \nu = 2$ .*

(2) *If  $p \mid l^e - 1$ , then  $F_e(t)$  has two roots  $\alpha^e, \beta^e$  close to 1. The only exceptional cases are  $p = 2, |r_e|_2 = 1/2, 1/4$  and  $p = 3, |r_e|_3 = 1/3$ .*

(i) *If in addition  $|r_e + (l^e - 1)|_p \leq |r_e|_p^{1/2}$ , then we have  $|\alpha^e - 1|_p = |\beta^e - 1|_p$ .*

(ii) *If instead  $|r_e + (l^e - 1)|_p > |r_e|_p^{1/2}$ , then then we have  $|\alpha^e - 1|_p \neq |\beta^e - 1|_p$ .*

*Proof.* If we put  $F_n(t) = (t - \alpha^n)(t - \beta^n)$ , then we have  $r_n = F_n(1)$ ,  $F_n(t) = t^2 - (\alpha^n + \beta^n)t + l^n = t^2 - (l^n + 1 - r_n)t + l^n$ ,  $F_n(t+1) = (t - (\alpha^n - 1))(t - (\beta^n - 1)) = t^2 + (2 - \alpha^n - \beta^n)t + (\alpha^n - 1)(\beta^n - 1) = t^2 + (r_n - (l^n - 1))t + r_n$ . Thus, whether  $p \mid l^n - 1$  or not determines the number of roots of  $F_m(t)$  that are close to 1.

Suppose  $p \mid l^e - 1$ , so that  $|1 - \alpha^e|_p < 1$  and  $|1 - \beta^e|_p < 1$ . If  $|1 - \alpha^e|_p = |1 - \beta^e|_p$ , then  $|r_e - (l^e - 1)|_p = |(1 - \alpha^e) + (1 - \beta^e)|_p \leq |1 - \alpha^e|_p = |r_e|_p^{1/2}$ . If instead  $|1 - \alpha^e|_p > |1 - \beta^e|_p$ , then by  $r_n = (1 - \alpha^n)(1 - \beta^n)$ , we have  $|r_e - (l^e - 1)|_p = |(1 - \alpha^e) + (1 - \beta^e)|_p = |1 - \alpha^e|_p > |r_e|_p^{1/2}$ .

Most part of the assertion is proved by a similar argument to Proposition 2.11.12. Example 2.12.14 completes the assertion (1). Example 2.12.15 completes the assertion (2).  $\square$

Let us study the exceptional cases in Proposition 2.12.13 (1).

**Example 2.12.14.** Suppose  $p = l$  (so that  $p \nmid l^e - 1$ ). If  $p = 2$  and  $|r_1|_2 = 1/2$ , then we have  $\nu = 2$ . If otherwise, we have  $\nu = 1$ .

*Proof.* By  $F_e(t+1) \equiv t^2 - (l^n + 1)t \not\equiv t^2 - t$ ,  $F_e(t)$  has just one root  $\alpha^e$  such that  $|r_1| = |\alpha^e - 1|_p < 1$ . If  $p > 3$ , then by  $|r_e|_p \leq 1/p < 1/p^{1/(p-1)}$ , we have  $|r_e|_p = |\alpha^e - 1|_p = |\log \alpha|_p = p^{-\nu}$ . If  $p = 2$  and  $4 \mid r_e$ , then by  $|r_e|_2 \leq 1/4 < 1/2$ , we have the same. Note that if  $2 \nmid e$ , then  $r_e/r_1$  is the square of an integer. Hence if  $p = 2$

and  $|r_e|_2 = 1/2$ , then we have  $|r_e|_2 = |r_1|_2 = 1/2$ . If  $p = l = 2$  and  $e = 1$ , then by Hasse's bound  $|a| \leq 2\sqrt{2}$  and that  $r_1 = F(1) = 3 - a$ , we have  $|3 - a|_1 = 1/2$ , and hence  $a = 1$ . In this case we have  $F(t) = t^2 - t + 2$  and  $\nu = 2 > 1$ . For instance,  $E : y^2 + xy - x^3 - x = 0$  is such a case. In addition, we have  $F_3(t) = t^2 + 5t + 8$  and  $(r_{3^{12^n}})_n$  also have  $\nu = 2$ .  $\square$

We next study exceptional cases in Proposition 2.12.13 (2) (i) with  $e = 1$ . Note that  $\lambda = 2$ .

**Example 2.12.15.** Let  $p = 2$  and  $2 \mid l - 1$ .

- Let  $|r_1|_2 = |l + 1 - a|_2 = 1/2$ . For instance, let  $l = b2^{1+c} + 1$ ,  $2 \nmid b$ ,  $b, c \in \mathbb{Z}_{\geq 0}$ . Note that such a prime number exists for arbitrary large  $c$  by Dirichlet's theorem on arithmetic progressions. If  $a = 0$ , then we have  $r_1 = F(1) = 2(b2^c + 1)$ ,  $r_4 = 2^{2c+4}b^2(b2^c + 1)^2$ ,  $v_2(r_4) = 2c + 4$ . By  $\lambda = 2$ , Proposition 2.12.12 yields  $\nu = v_2(r_4) - 2 \cdot 2 = 2c$ , while  $|r_1|_2 = 1/2$ .

- Let  $|r_1|_2 = |l + 1 - a|_2 = 1/4$ . For instance, if  $l = b2^{c+2} + 1$ ,  $2 \nmid b$ ,  $b, c \in \mathbb{Z}_{\geq 0}$ ,  $a = -2$ , then  $v_2(r_1) = 2$ ,  $v_2(r_4) = 2c + 6$ ,  $\nu = 2c + 6 - 4 = 2c + 2$ .

- If  $|r_1|_2 = 1/2^d$  with  $d > 2$ , then  $\nu$  is determined by  $r_1$ .

**Example 2.12.16.** Let  $p = 3$ . If  $3 \mid l - 1$ , then we have  $|r_1|_3 = |l + 1 - a|_3 = 1/3$ . For instance, if  $l = b3^{2+c} + 1$  with  $3 \nmid b$ ,  $b, c \in \mathbb{Z}_{\geq 0}$  and  $a = 2$ , then  $v_3(r_{3^3}) = c + 8$ ,  $\nu = c + 8 - 6 = c + 2$ .

Examples 2.12.15 and 2.12.16 answer Question 2.12.11. Cases in (2) (ii) may be treated similarly.

**Remark 2.12.17.** For any elliptic curves over  $\mathbb{F}_l$ , we have  $\nu \geq 0$ , as in the cases of knots. We wonder if there is an analogous situation to the cases of links with arbitrary negative  $\nu$  (cf. Remark 2.11.17). A systematic study of the Iwasawa  $\nu$ -invariants of number fields may be found in Sumida-Takahashi's works [73, 74].

**Remark 2.12.18.** We may study  $\mathbb{Z}_p$ -covers of a 3-manifold and constant  $\mathbb{Z}_p$ -extensions of a function field as subcovers or subextensions of the  $\widehat{\mathbb{Z}}$ -cover or the  $\widehat{\mathbb{Z}}$ -extension in a parallel manner. We expect further interactions between these objects.



# Chapter 3

## Bijjective enumerations for symmetrized poly-Bernoulli polynomials

First we recall the definition of the symmetrized poly-Bernoulli polynomial. For non-negative integers  $n, k \geq 0$ , the (normalized) symmetrized poly-Bernoulli polynomial  $\widehat{\mathcal{B}}_n^k(x)$  is defined by

$$\widehat{\mathcal{B}}_n^k(x) = \sum_{j=0}^{\min(n,k)} j!(x+1)^{\bar{j}} \left\{ \begin{matrix} n+1 \\ j+1 \end{matrix} \right\} \left\{ \begin{matrix} k+1 \\ j+1 \end{matrix} \right\} \in \mathbb{Z}[x]. \quad (3.1)$$

Here,  $\left\{ \cdot \right\}$  is the Stirling number of the second kind (see [2, Section 2.1]), and  $(x+1)^{\bar{j}} = (x+1)(x+2)\cdots(x+j)$  is the rising factorial. We study this polynomial from a combinatorial perspective in this chapter.

### 3.1 A bijection between two combinatorial models

Bényi and Matsusaka [11] introduced combinatorial models for symmetrized poly-Bernoulli polynomial  $\widehat{\mathcal{B}}_n^k(x)$ . In this section, we first recall these models, and then provide a bijection between these models.

#### 3.1.1 Double Callan permutations

Throughout this chapter, let  $n$  and  $k$  be non-negative integers.

**Definition 3.1.1.** A *double Callan permutation* of size  $n \times k$  is a pair of (possible empty) strings  $S_1 = a_1 \cdots a_r$  and  $S_2 = b_1 \cdots b_s$  with  $r + s = n + k$  such that

- (1) the terms satisfy  $\{a_1, \dots, a_r\} \sqcup \{b_1, \dots, b_s\} = \{1, \dots, n, 1, \dots, k\}$  with  $r, s \geq 0$ ,

- (2)  $a_1$  is blue, and  $b_1$  is red, and
- (3) consecutive elements of the same color are decreasing.

We let  $\mathcal{C}_n^k$  denote the set of all double Callan permutations of size  $n \times k$ .

**Example 3.1.2.** The following is an example of double Callan permutations of size  $7 \times 6$ :

$$S_1 = 676513132 \quad \text{and} \quad S_2 = 4452.$$

The double Callan permutations are essentially the same as the barred Callan sequences studied in [11]. Indeed, we can express a pair of strings as

$$S_1 = B_1 R_1 \cdots B_\ell R_\ell B_{\ell+1} \quad \text{and} \quad S_2 = R'_1 B'_1 \cdots R'_m B'_m R'_{m+1}, \quad (3.2)$$

where  $R$  and  $B$  are substrings consisting of red and blue elements, respectively. Here,  $\ell, m \geq 0$  and the substrings  $B_{\ell+1}$  and  $R'_{m+1}$  could be empty. This expression defines a barred Callan sequence  $(B_1; R_1) \cdots (B_\ell; R_\ell) | (B'_m; R'_m) \cdots (B'_1; R'_1) (B_{\ell+1}, *; R'_{m+1}, *)$ . Therefore, by reusing the terminology for barred Callan sequences, we refer to  $B_{\ell+1}, R'_{m+1}$  as *extra blocks* and refer to other substrings  $R, B$  as *ordinary blocks*. Moreover, we refer to a pair of red and blue blocks having the same sub-(super-)script as a *Callan pair*. Note that if  $\ell = 0$  (resp.  $m = 0$ ), then the block  $B_1$  (resp.  $R'_1$ ) is the extra block.

**Definition 3.1.3.** For each double Callan permutation  $\lambda = (S_1, S_2) \in \mathcal{C}_n^k$  given as in (3.2), we define its weight  $w_{\mathcal{C}}^{\text{lr}}(\lambda) \in \mathbb{Z}_{\geq 0}$  using the left-to-right minimum as follows:

- (1) Consider the minimum of each blue substring  $B_1, \dots, B_\ell$  in  $S_1$  to obtain a sequence  $\pi = \pi_1 \pi_2 \cdots \pi_\ell$ . Here, we ignore the last blue substring  $B_{\ell+1}$ .
- (2) Count the number of  $1 \leq i \leq \ell$  such that if  $j < i$  then  $\pi_i < \pi_j$ .

For the above example, we obtain the sequence  $\pi = 613$ . Then, the weight is given by  $w_{\mathcal{C}}^{\text{lr}}(\lambda) = 2$ .

**Definition 3.1.4.** For any  $n, k \geq 0$ , we define the *Callan polynomial* by

$$\mathcal{C}_n^k(x) = \mathcal{C}_n^k(x; w_{\mathcal{C}}^{\text{lr}}) = \sum_{\lambda \in \mathcal{C}_n^k} x^{w_{\mathcal{C}}^{\text{lr}}(\lambda)}.$$

The following explicit properties of the Callan polynomials are known.

**Theorem 3.1.5** ([11]). *The Callan polynomials satisfy the explicit formula*

$$\mathcal{C}_n^k(x) = \sum_{j=0}^{\min(n,k)} j! (x+1)^{\bar{j}} \left\{ \begin{matrix} n+1 \\ j+1 \end{matrix} \right\} \left\{ \begin{matrix} k+1 \\ j+1 \end{matrix} \right\}, \quad (3.3)$$

and the generating function

$$\sum_{n=0}^{\infty} \sum_{k=0}^{\infty} \mathcal{C}_n^k(x) \frac{X^n Y^k}{n! k!} = \frac{e^{X+Y}}{(e^X + e^Y - e^{X+Y})^{x+1}}.$$

In particular, by (3.1), we have  $\mathcal{C}_n^k(x) = \widehat{\mathcal{B}}_n^k(x)$ .

**Remark 3.1.6.** For positive integers  $n$  and  $k$ , the Stirling number of the second kind  $\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$  counts the number of ways to divide a set of  $n$  elements into  $k$  nonempty sets. The Stirling numbers satisfy the recurrence formula

$$\left\{ \begin{smallmatrix} n+1 \\ k \end{smallmatrix} \right\} = \left\{ \begin{smallmatrix} n \\ k-1 \end{smallmatrix} \right\} + k \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$$

with the initial values  $\left\{ \begin{smallmatrix} 0 \\ 0 \end{smallmatrix} \right\} = 1$  and  $\left\{ \begin{smallmatrix} n \\ 0 \end{smallmatrix} \right\} = \left\{ \begin{smallmatrix} 0 \\ k \end{smallmatrix} \right\} = 0$  ( $n, k \neq 0$ ). From this definition, the above explicit formula (3.3) immediately follows (see [11, Section 3]).

### 3.1.2 Alternative tableaux

The second combinatorial model for  $\widehat{\mathcal{B}}_n^k(x)$  is given by alternative tableaux of rectangular shape. An alternative tableau of general shape was introduced by Viennot [87] and studied by Nadeau [58]. Here, we recall its definition and the weight function  $w_{\mathcal{T}}^{\text{st}} : \mathcal{T}_n^k \rightarrow \mathbb{Z}_{\geq 0}$  introduced in [11].

**Definition 3.1.7.** Let  $n, k$  be positive integers. An *alternative tableau* of rectangular shape of size  $n \times k$  is a rectangle with a partial filling of the cells with left arrows  $\leftarrow$  and down arrows  $\downarrow$ , such that all cells pointed by an arrow are empty. We let  $\mathcal{T}_n^k$  denote the set of all alternative tableaux with a rectangular shape and a size of  $n \times k$ .

For each  $\lambda \in \mathcal{T}_n^k$ ,

- (1) consider the first from the top consecutive rows that contain left arrows  $\leftarrow$ , and
- (2) count the number of left arrows  $\leftarrow$  such that all  $\leftarrow$  in the upper rows are located further to the right.

We let  $w_{\mathcal{T}}^{\text{st}}(\lambda)$  denote the number of such left arrows, (the superscript “st” of which is an abbreviation of “stair”).

**Example 3.1.8.** The following alternative tableau  $\lambda \in \mathcal{T}_7^6$  has a weight  $w_{\mathcal{T}}^{\text{st}}(\lambda) = 2$ .

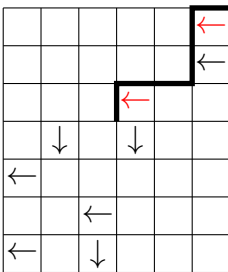


Figure 3.1: An alternative tableau of size  $7 \times 6$  with an indication of its weight.

In a similar manner as above, we define the polynomial  $\mathcal{T}_n^k(x)$  as

$$\mathcal{T}_n^k(x) = \mathcal{T}_n^k(x; w_{\mathcal{T}}^{\text{st}}) = \sum_{\lambda \in \mathcal{T}_n^k} x^{w_{\mathcal{T}}^{\text{st}}(\lambda)}.$$

**Theorem 3.1.9** ([11]). Let  $\mathcal{T}_n^0(x) = \mathcal{T}_0^k(x) = 1$ . For any integers  $n, k \geq 0$ , the polynomial  $\mathcal{T}_n^k(x)$  coincides with  $\mathcal{C}_n^k(x)$ , i.e.,  $\mathcal{T}_n^k(x) = \widehat{\mathcal{B}}_n^k(x)$ .

This theorem was proven by showing that both polynomials  $\mathcal{C}_n^k(x)$  and  $\mathcal{T}_n^k(x)$  satisfy the same recursion

$$\widehat{\mathcal{B}}_n^k(x) = (n+1)\widehat{\mathcal{B}}_n^{k-1}(x) + x \sum_{j=0}^{n-1} \binom{n}{j} \widehat{\mathcal{B}}_j^{k-1}(x) + \sum_{j=1}^{n-1} \binom{n}{j-1} \widehat{\mathcal{B}}_j^{k-1}(x). \quad (3.4)$$

### 3.1.3 A combinatorial bijection

In this subsection, we construct a bijection between these two models.

Both combinatorial models have their own advantages and disadvantages. On one hand, although it is quite easy to show that the polynomial  $\mathcal{T}_n^k(x)$  satisfies the recursion in (3.4), it is difficult to check the explicit formula (Theorem 3.1.5) for  $\mathcal{T}_n^k(x)$ . On the other hand, as we mentioned in Remark 3.1.6, the explicit formula immediately follows from the definition of  $\mathcal{C}_n^k(x)$  by simply enumerating the objects. However, it is slightly complicated to show that the Callan polynomials  $\mathcal{C}_n^k(x)$  satisfy the recursion.

Indeed, the authors [11, Theorem 14] used the following auxiliary map  $\varphi$  to show the recursion for the Callan polynomials. Here, we recall this map.

**Definition 3.1.10.** For any integers  $n \geq 0$  and  $k > 0$ , we define a map  $\varphi : \mathcal{C}_n^k \rightarrow \mathcal{C}_{\leq n}^{k-1} := \bigcup_{i=0}^n \mathcal{C}_i^{k-1}$  as follows. Let  $(S_1, S_2) \in \mathcal{C}_n^k$  be expressed as in (3.2).

- (1) If  $k$  is in the extra block  $B_{\ell+1}$ , then remove  $k$ .
- (2) If  $k$  is alone in the first ordinary block  $B_1$ , then remove the first Callan pair  $B_1 R_1$ .
- (3) Otherwise, let  $R$  be the ordinary red block that forms a Callan pair with the blue block containing  $k$ . Then, remove  $k$  and replace  $R$  with the red element  $0$ . Finally, rearrange the position of  $0$  in decreasing order if needed.

After that, we rearrange red elements from 1.

**Example 3.1.11.** For a double Callan permutation  $(S_1, S_2) = (621445, 7632531) \in \mathcal{C}_7^6$ , we have

$$\begin{aligned} \varphi : (621445, 7632531) &\mapsto (445, 7632531) \mapsto (425, 5432311), & \dots (2) \\ \varphi : (425, 5432311) &\mapsto (42, 5432311), & \dots (1) \\ \varphi : (42, 5432311) &\mapsto (\emptyset, 5432311) \mapsto (\emptyset, 4332211), & \dots (2) \\ \varphi : (\emptyset, 4332211) &\mapsto (\emptyset, 02211) \mapsto (\emptyset, 12321), & \dots (3) \\ \varphi : (\emptyset, 12321) &\mapsto (\emptyset, 0321) \mapsto (\emptyset, 3201) \mapsto (\emptyset, 3211), & \dots (3) \\ \varphi : (\emptyset, 3211) &\mapsto (\emptyset, 0) \mapsto (\emptyset, 1). & \dots (3) \end{aligned}$$

As mentioned above, the polynomials  $\mathcal{C}_n^k(x)$  and  $\mathcal{T}_n^k(x)$  satisfy the same recursion (3.4). This tells us that two models  $(\mathcal{C}_n^k, w_{\mathcal{C}}^{\text{lr}})$  and  $(\mathcal{T}_n^k, w_{\mathcal{T}}^{\text{st}})$  have the same recursive structure. Using the map  $\varphi$ , we construct a bijection from  $\mathcal{C}_n^k$  to  $\mathcal{T}_n^k$  in a stepwise manner on  $k$ . We first define the map from  $\mathcal{C}_n^k$  to  $\mathcal{T}_n^1$ .

**Definition 3.1.12.** For a given double Callan permutation  $\lambda \in \mathcal{C}_n^k$ , we create an alternative tableau  $\lambda_k \in \mathcal{T}_n^1$  by following the steps below. If  $k$  is not in the extra block, let  $R$  be as described in Definition 3.1.10 (3).

- (1) If  $k$  is in the extra block, then  $\lambda_k = \emptyset$ .
- (2) If  $k$  is alone in the first ordinary block  $B_1$ , then the  $(1,1)$ -entry is  $\leftarrow$ . Moreover,
  - (a) if  $1 \in R$ , then the  $(\ell, 1)$ -entry is  $\leftarrow$  for  $\ell \in R$ , and
  - (b) if  $1 \notin R$ , then the  $(m, 1)$ -entry is  $\downarrow$  for  $m = \max R$ , and the  $(\ell, 1)$ -entry is  $\leftarrow$  for  $\ell \in R \setminus \{m\}$ .
- (3) Otherwise,
  - (a) if  $|R| = 1$ , then the  $(\ell, 1)$ -entry is  $\downarrow$  for  $\ell \in R$ ,
  - (b) if  $|R| > 1$  and  $1 \in R$ , then the  $(\ell, 1)$ -entry is  $\leftarrow$  for  $\ell \in R \setminus \{1\}$ , and
  - (c) if  $|R| > 1$  and  $1 \notin R$ , then the  $(m, 1)$ -entry is  $\downarrow$  for  $m = \max R$ , and  $(\ell, 1)$ -entry is  $\leftarrow$  for  $\ell \in R \setminus \{m\}$ .

We next define the desired map  $\mathcal{C}_n^k \rightarrow \mathcal{T}_n^k$  inductively. By Definition 3.1.12, we have  $\lambda_k \in \mathcal{T}_n^1$ . If  $\lambda_k$  contains  $\ell$  left arrows, then  $\varphi(\lambda) \in \mathcal{C}_{n-\ell}^{k-1}$ . By applying the map in Definition 3.1.12 again to  $\varphi(\lambda) \in \mathcal{C}_{n-\ell}^{k-1}$ , we obtain  $\lambda_{k-1} \in \mathcal{T}_{n-\ell}^1$ . By repeating the steps, we have a sequence  $\lambda_1 \lambda_2 \cdots \lambda_k$ . The concatenation gives an alternative tableau in  $\mathcal{T}_n^k$  with the same weight as  $w_{\mathcal{C}}^{\text{lr}}(\lambda)$ .

The bijectiveness can be checked inductively. We sketch the idea of the proof. For any  $n$  and  $k = 1$ , the map  $\mathcal{C}_n^1 \rightarrow \mathcal{T}_n^1$  defined in Definition 3.1.12 is a bijection preserving the weight. We let  $\mathcal{T}_{n,\ell}^1$  denote the subset of  $\mathcal{T}_n^1$  such that  $\lambda \in \mathcal{T}_{n,\ell}^1$  contains  $\ell$  left arrows. Then, our maps induce a bijection  $\mathcal{C}_n^k \rightarrow \bigcup_{\ell=0}^n (\mathcal{C}_{n-\ell}^{k-1} \times \mathcal{T}_{n,\ell}^1) : \lambda \mapsto (\varphi(\lambda), \lambda_k)$ . By the inductive assumption,  $\mathcal{C}_{n-\ell}^{k-1}$  is isomorphic to  $\mathcal{T}_{n-\ell}^{k-1}$ . Thus,  $\mathcal{C}_n^k \rightarrow \mathcal{T}_n^k$  is bijective. Note that Case (2) in Definition 3.1.10 and Case (2) in Definition 3.1.12 affect the weight. In particular, we can check that the bijective map preserves the weight.

In conclusion, we have the following:

**Theorem 3.1.13.** *The above map gives a bijection  $(\mathcal{C}_n^k, w_{\mathcal{C}}^{\text{lr}}) \rightarrow (\mathcal{T}_n^k, w_{\mathcal{T}}^{\text{st}})$ .*

**Example 3.1.14.** For a double Callan permutation  $\lambda = (621445, 7632531) \in \mathcal{C}_7^6$ , we already computed the images under  $\varphi$  in Example 3.1.11. The corresponding sequence  $\lambda_1 \lambda_2 \cdots \lambda_6$  of the alternative tableaux and their concatenation are as follows. This is the alternative tableau given in Example 3.1.8.

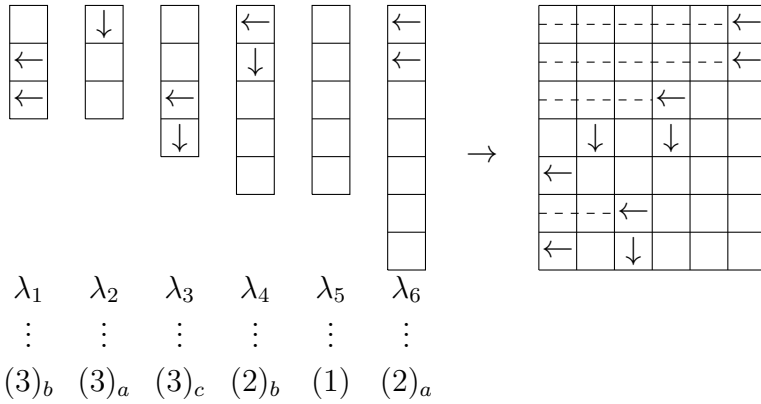


Figure 3.2: The sequence  $\lambda_1 \cdots \lambda_6$  and their concatenation.

## 3.2 A sequence of bijections

In the previous section, we studied two combinatorial polynomials  $\mathcal{C}_n^k(x)$  and  $\mathcal{T}_n^k(x)$ , both of which have definitions of the form

$$\mathcal{P}(x) = \mathcal{P}(x; w) = \sum_{\lambda \in \mathcal{P}} x^{w(\lambda)}$$

for a pair  $(\mathcal{P}, w)$ , where  $\mathcal{P}$  is a set of combinatorial objects and  $w : \mathcal{P} \rightarrow \mathbb{Z}_{\geq 0}$  is a suitable weight function. In this section, we introduce two additional combinatorial polynomials,  $\tilde{\mathcal{T}}_n^k(x)$  and  $\mathcal{S}_n^k(x)$ , and show that all polynomials coincide. In particular, we construct a sequence of bijections  $\mathcal{T}_n^k \rightarrow \tilde{\mathcal{T}}_n^k \rightarrow \mathcal{S}_n^k \rightarrow \mathcal{C}_n^k$  preserving the weight.

### 3.2.1 Packed alternative tableaux

Let  $\mathcal{T}_n^k$  be the set of alternative tableaux of rectangular shape of size  $n \times k$  as in Definition 3.1.7. We consider another weight  $w_{\mathcal{T}}^{\leftarrow} : \mathcal{T}_n^k \rightarrow \mathbb{Z}_{\geq 0}$  defined by the number of columns that contain  $\leftarrow$  but does not contain  $\downarrow$ .

**Theorem 3.2.1.** *The polynomial  $\mathcal{T}_n^k(x; w_{\mathcal{T}}^{\leftarrow}) = \sum_{\lambda \in \mathcal{T}_n^k} x^{w_{\mathcal{T}}^{\leftarrow}(\lambda)}$  coincides with  $\widehat{\mathcal{B}}_n^k(x)$ .*

*Proof.* We can check that the polynomials  $\mathcal{T}_n^k(x; w_{\mathcal{T}}^{\leftarrow})$  satisfy the recursion in (3.4) by cutting out the rightmost column and the rows that contain  $\leftarrow$  in the rightmost cell.  $\square$

The packed alternative tableaux introduced by Nadeau [58] complement alternative tableaux by adding lacking arrows.

**Definition 3.2.2.** A *packed alternative tableau* of rectangular shape of size  $n \times k$  is a rectangle of size  $(n + 1) \times (k + 1)$  with a partial filling of the cells with left arrows and down arrows, such that

- (1) all cells pointed by an arrow are empty,
- (2) each row (resp. column) except for the bottom row (resp. the leftmost column) contains exactly one left arrow  $\leftarrow$  (resp. exactly one down arrow  $\downarrow$ ), and
- (3) the bottom row (resp. the leftmost column) does not contain  $\leftarrow$  (resp.  $\downarrow$ ).

We let  $\tilde{\mathcal{T}}_n^k$  denote the set of all packed alternative tableaux of rectangular shape of size  $n \times k$ . For each  $\lambda \in \tilde{\mathcal{T}}_n^k$ , the weight  $w_{\tilde{\mathcal{T}}}^{\leftarrow, \downarrow}(\lambda)$  counts the number of columns that contain a  $\downarrow$  in its bottom cell, and at least one  $\leftarrow$  elsewhere.

By cutting out the bottom row and the leftmost column of a packed alternative tableau of size  $n \times k$ , we obtain an alternative tableau of size  $n \times k$ . It is clear that the operation defines a bijection  $(\tilde{\mathcal{T}}_n^k, w_{\tilde{\mathcal{T}}}^{\leftarrow, \downarrow}) \rightarrow (\mathcal{T}_n^k, w_{\mathcal{T}}^{\leftarrow, \downarrow})$ . Thus, the polynomial

$$\tilde{\mathcal{T}}_n^k(x) = \tilde{\mathcal{T}}_n^k(x; w_{\tilde{\mathcal{T}}}^{\leftarrow, \downarrow}) = \sum_{\lambda \in \tilde{\mathcal{T}}_n^k} x^{w_{\tilde{\mathcal{T}}}^{\leftarrow, \downarrow}(\lambda)} \quad (3.5)$$

coincides with  $\mathcal{T}_n^k(x; w_{\mathcal{T}}^{\leftarrow, \downarrow})$ , i.e.,  $\tilde{\mathcal{T}}_n^k(x) = \hat{\mathcal{B}}_n^k(x)$ .

**Example 3.2.3.** The  $\lambda \in \mathcal{T}_7^6$  given in Example 3.1.8 corresponds to the following packed alternative tableau and has a weight of  $w_{\tilde{\mathcal{T}}}^{\leftarrow, \downarrow}(\lambda) = 2$ .

						$\leftarrow$
						$\leftarrow$
				$\leftarrow$		
$\leftarrow$		$\downarrow$		$\downarrow$		
	$\leftarrow$					
			$\leftarrow$			
	$\leftarrow$		$\downarrow$			
	$\downarrow$				$\downarrow$	$\downarrow$

Figure 3.3: Packed alternative tableau of size  $7 \times 6$ .

### 3.2.2 Double alternative trees

Alternative trees and forests were studied by Nadeau [58]. Based on this idea, we consider a pair of alternative trees and introduce a suitable weight to the trees.

**Definition 3.2.4.** A *double alternative tree* of size  $n \times k$  is a pair of labeled rooted trees  $(T_1, T_2)$ , such that

- (1) the vertex set satisfies  $V(T_1) \sqcup V(T_2) = \{0, 1, \dots, n, 0, 1, \dots, k\}$ ,
- (2) the roots of the trees  $T_1$  and  $T_2$  are  $0$  and  $0$ , respectively,

- (3) all children of each red (resp. blue) vertex are blue (resp. red), and
- (4) for each vertex, its descendants have a different color or are larger than the vertex.

We let  $\mathcal{T}_n^k$  denote the set of all double alternative trees of size  $n \times k$ .

**Example 3.2.5.** This is an example of double alternative trees.

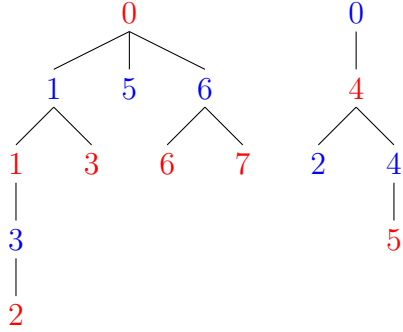
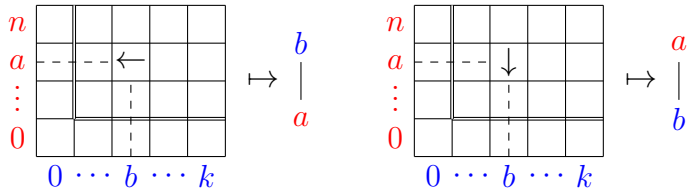


Figure 3.4: Double alternative tree of size  $7 \times 6$ .

For each double alternative tree  $\lambda \in \mathcal{T}_n^k$ , we define its weight  $w_{\mathcal{T}}^{\text{ch}}(\lambda)$  by the number of non-leaf (blue) children of  $0$ . Here, a vertex is called a *leaf* if it does not have any child. For instance, the weight of the above  $\lambda \in \mathcal{T}_7^6$  is  $w_{\mathcal{T}}^{\text{ch}}(\lambda) = \#\{1, 6\} = 2$ .

**Theorem 3.2.6.** *The polynomial  $\mathcal{T}_n^k(x) = \mathcal{T}_n^k(x; w_{\mathcal{T}}^{\text{ch}})$  coincides with the polynomial  $\tilde{\mathcal{T}}_n^k(x)$  defined in (3.5), i.e.,  $\mathcal{T}_n^k(x) = \hat{\mathcal{B}}_n^k(x)$ .*

*Proof.* We can easily check that the map  $\tilde{\mathcal{T}}_n^k \rightarrow \mathcal{T}_n^k$  defined by



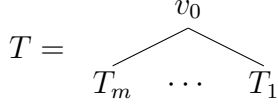
is a bijection  $(\tilde{\mathcal{T}}_n^k, w_{\tilde{\mathcal{T}}}^{\leftarrow}) \rightarrow (\mathcal{T}_n^k, w_{\mathcal{T}}^{\text{ch}})$ . □

Under the above bijection, the packed alternative tableau given in Fig. 3.3 corresponds to the double alternative tree in Fig. 3.4.

**Theorem 3.2.7.** *There is a bijection  $(\mathcal{T}_n^k, w_{\mathcal{T}}^{\text{ch}}) \rightarrow (\mathcal{C}_n^k, w_{\mathcal{C}}^{\text{lr}})$ , i.e., the polynomial  $\mathcal{T}_n^k(x)$  coincides with the polynomial  $\mathcal{C}_n^k(x)$  defined in Definition 3.1.4.*



*Proof.* We define a bijection  $\phi$  from the set of labeled rooted trees to the set of strings inductively. For a singleton  $T = v$ , we put  $\phi(T) = v$ . Let  $T$  be the following rooted tree:



In this expression, assume that  $T_1, \dots, T_m$  are rooted trees, the roots  $R(T_1), \dots, R(T_m)$  of which satisfy the condition  $R(T_m) < \dots < R(T_1)$ . We define  $\phi(T) = \phi(v_0)\phi(T_1) \cdots \phi(T_m)$ . The desired bijection is given by  $\mathbf{0}S_1 = \phi(T_1)$  and  $\mathbf{0}S_2 = \phi(T_2)$ , which preserves the weight.  $\square$

**Example 3.2.8.** Under the above bijection, the example given in Fig. 3.4 corresponds to  $(S_1, S_2) = (676513132, 4452)$ .

In conclusion, we obtain another bijection between  $\mathcal{C}_n^k$  and  $\mathcal{T}_n^k$  by a sequence of bijections

$$(\mathcal{T}_n^k, w_{\mathcal{T}}^{\leftarrow}) \rightarrow (\tilde{\mathcal{T}}_n^k, w_{\tilde{\mathcal{T}}}^{\leftarrow}) \rightarrow (\mathcal{I}_n^k, w_{\mathcal{I}}^{\text{ch}}) \rightarrow (\mathcal{C}_n^k, w_{\mathcal{C}}^{\text{lr}}). \quad (3.6)$$

By the bijection in Theorem 3.1.13, the alternative tableau in Example 3.1.8 corresponds to the double Callan permutation  $(621445, 7632531)$  as explained in Example 3.1.14. On the other hand, by the bijection in (3.6), the alternative tableau corresponds to  $(676513132, 4452)$  as in Example 3.2.8. The difference arises from the existence of two weight functions  $w_{\mathcal{T}}^{\text{st}}$  and  $w_{\mathcal{T}}^{\leftarrow}$  for the set of alternative tableaux  $\mathcal{T}_n^k$ .

By translating the weight  $w_{\mathcal{T}}^{\text{st}}$  via the bijections  $\mathcal{T}_n^k \rightarrow \tilde{\mathcal{T}}_n^k \rightarrow \mathcal{I}_n^k \rightarrow \mathcal{C}_n^k$ , we can obtain new weight functions for  $\tilde{\mathcal{T}}_n^k$ ,  $\mathcal{I}_n^k$ , and  $\mathcal{C}_n^k$ . For example, the new weight  $w_{\mathcal{C}}^{\text{br}} : \mathcal{C}_n^k \rightarrow \mathbb{Z}_{\geq 0}$  is defined as follows:

**Definition 3.2.9.** For each double Callan permutation  $\lambda = (S_1, S_2) \in \mathcal{C}_n^k$ ,

- (1) if the string  $S_2$  does not start from  $n$ , then mark the blue element just before  $n$ , and if  $S_2$  starts from  $n$ , then we stop the steps,
- (2) consider the next largest red element,
  - (i) if the element is the leading element of  $S_2$ , then we stop the steps,
  - (ii) if the element is after a blue element and the blue element is smaller than the last marked element, then we mark the blue element,
  - (iii) otherwise, we do nothing, and
- (3) repeat Step (2) until we reach  $\mathbf{1}$  or until the step stops.

Then, we define  $w_{\mathcal{C}}^{\text{br}}(\lambda)$  by the number of marked blue elements.

**Example 3.2.10.** Let  $\lambda_0 \in \mathcal{T}_7^6$  be as in Example 3.1.8. By the bijections of (3.6),  $\lambda_0$  corresponds to the double Callan permutation  $\lambda = (676513132, 4452)$ , as in Example 3.2.8.

We first mark 6. Since the next largest red element 6 is located after 7, we ignore this element. The next 5 is after a blue element. Since 4 is smaller than the last marked 6, we mark 4. The next 4 is the leading element of  $S_2$ . Thus, we stop the steps here. The weight is given by  $w_{\mathcal{C}}^{\text{br}}(\lambda) = \#\{6, 4\} = 2$ , which coincides with  $w_{\mathcal{T}}^{\text{st}}(\lambda_0)$ . In particular, the indicated left arrows in Example 3.1.8 are in 4th and 6th columns.

**Corollary 3.2.11.** *We have a bijection  $(\mathcal{T}_n^k, w_{\mathcal{T}}^{\text{st}}) \rightarrow (\mathcal{C}_n^k, w_{\mathcal{C}}^{\text{br}})$ , i.e.,  $\mathcal{C}_n^k(x; w_{\mathcal{C}}^{\text{br}}) = \mathcal{T}_n^k(x; w_{\mathcal{T}}^{\text{st}}) = \widehat{\mathcal{B}}_n^k(x)$ .*

### 3.3 Further combinatorial models and weights

In this section, we provide another combinatorial model  $(\mathcal{E}_n^k, w_{\mathcal{E}}^{\text{lr}})$  and prove that the polynomial  $\mathcal{E}_n^k(x; w_{\mathcal{E}}^{\text{lr}})$  is equal to  $\widehat{\mathcal{B}}_n^k(x)$ . We here explain two types of proofs. One type is by checking the recursion (3.4), and the other type is by constructing a bijection  $(\mathcal{C}_n^k, w_{\mathcal{C}}^{\text{RL}}) \rightarrow (\mathcal{E}_n^k, w_{\mathcal{E}}^{\text{lr}})$  with a new weight  $w_{\mathcal{C}}^{\text{RL}} : \mathcal{C}_n^k \rightarrow \mathbb{Z}_{\geq 0}$ .

#### 3.3.1 Excedance set of permutations

We introduce the fifth combinatorial set for the symmetrized poly-Bernoulli polynomial  $\widehat{\mathcal{B}}_n^k(x)$  using an excedance set of a permutation, which was studied by Ehrenborg–Steingrímsson [21].

**Definition 3.3.1.** Let  $[n] = \{1, 2, \dots, n\}$ . An *excedance set* of a permutation  $\lambda : [n] \rightarrow [n]$  is defined by  $E(\lambda) = \{i \in [n] \mid \lambda(i) > i\}$ . For non-negative integers  $n, k \geq 0$ , we set  $\mathcal{E}_n^k = \{\lambda : [n+k+1] \rightarrow [n+k+1] \mid E(\lambda) = [n]\}$ .

**Example 3.3.2.** The following lists all elements  $\lambda = \left( \begin{smallmatrix} 1 & 2 & 3 & 4 \\ \lambda(1) & \lambda(2) & \lambda(3) & \lambda(4) \end{smallmatrix} \right)$  in  $\mathcal{E}_2^1$ .

$$\begin{aligned} & \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{array} \right), \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{array} \right), \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{array} \right), \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{array} \right), \\ & \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{array} \right), \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{array} \right), \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{array} \right) \end{aligned}$$

We define the weight function  $w_{\mathcal{E}}^{\text{lr}} : \mathcal{E}_n^k \rightarrow \mathbb{Z}_{\geq 0}$  by the left-to-right minimum.

**Definition 3.3.3.** We define the weight function  $w_{\mathcal{E}}^{\text{lr}} : \mathcal{E}_n^k \rightarrow \mathbb{Z}_{\geq 0}$  by

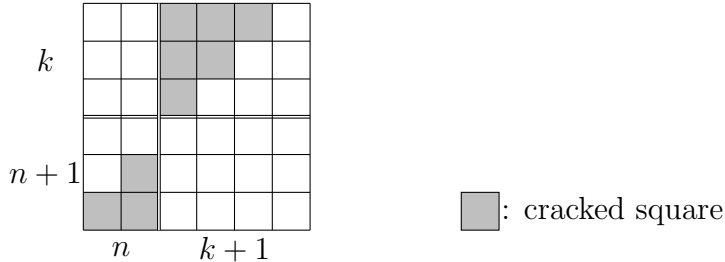
$$w_{\mathcal{E}}^{\text{lr}}(\lambda) = \#\{n+1 < i \leq n+k+1 \mid \lambda(i) < \lambda(j) \text{ for any } n < j < i\}.$$

For instance, the permutation

$$\lambda = \left( \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 3 & 2 & 4 & 6 & 1 \end{array} \right) \in \mathcal{E}_2^4 \tag{3.7}$$

has the weight  $w_{\mathcal{E}}^{\text{lr}}(\lambda) = \#\{4, 7\} = 2$ .

We can express elements in  $\mathcal{E}_n^k$  using the following chessboard of size  $n + k + 1$  with cracked squares, (see Clark–Ehrenborg [16]).



Then, the ways of placing  $n + k + 1$  non-attacking rooks on a cracked chessboard correspond to the elements of  $\mathcal{E}_n^k$ . For instance, the element  $\lambda \in \mathcal{E}_7^6$  given in (3.7) is expressed as follows:

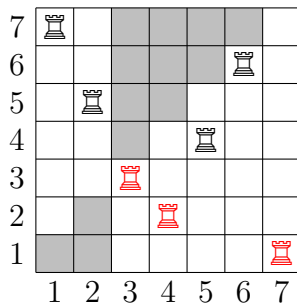


Figure 3.5: The expression of  $\lambda = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 3 & 2 & 4 & 6 & 1 \end{pmatrix} \in \mathcal{E}_2^4$  with the indication of its weight.

**Theorem 3.3.4.** *Let  $\mathcal{E}_n^0(x) = \mathcal{E}_0^k(x) = 1$ . For any integers  $n, k \geq 0$ , the polynomial*

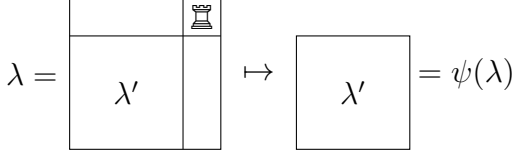
$$\mathcal{E}_n^k(x) = \mathcal{E}_n^k(x; w_{\mathcal{E}}^{\text{lr}}) = \sum_{\lambda \in \mathcal{E}_n^k} x^{w_{\mathcal{E}}^{\text{lr}}(\lambda)}$$

*coincides with the polynomial  $\widehat{\mathcal{B}}_n^k(x)$ .*

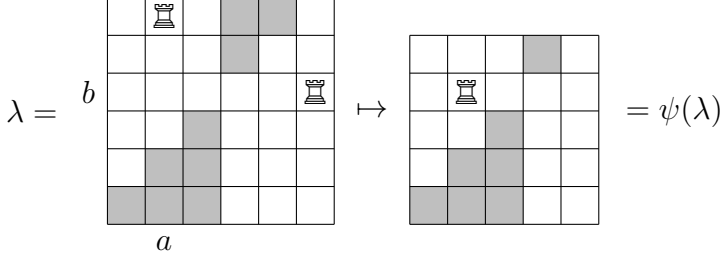
To prove this theorem, we define the auxiliary map  $\psi : \mathcal{E}_n^k \rightarrow \mathcal{E}_{\leq n}^{k-1} := \bigcup_{i=0}^n \mathcal{E}_i^{k-1}$  as follows.

**Definition 3.3.5.** For  $\lambda \in \mathcal{E}_n^k$ ,

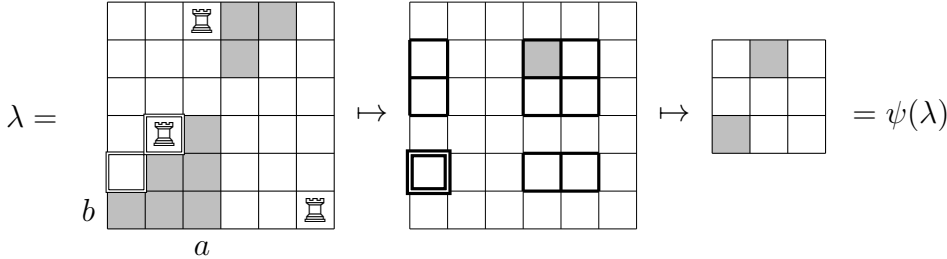
- (1) If  $\lambda(n + k + 1) = n + k + 1$ , then  $\psi(\lambda) \in \mathcal{E}_n^{k-1}$  with  $\psi(\lambda)(i) = \lambda(i)$  for any  $1 \leq i \leq n + k$ .



- (2) If  $\lambda(a) = n + k + 1$ ,  $\lambda(n + k + 1) = b$ , and  $b > a$ , then  $\psi(\lambda) \in \mathcal{E}_n^{k-1}$  with  $\psi(\lambda)(a) = b$  and  $\psi(\lambda)(i) = \lambda(i)$  otherwise.



- (3) If  $\lambda(a) = n + k + 1$ ,  $\lambda(n + k + 1) = b$ , and  $b \leq a \leq n$ , then we set  $D = \{b \leq i < a \mid \lambda(i) = i + 1\} \subset [n - 1]$ . Then, we define  $\psi'(\lambda)$  by  $\psi'(\lambda) = \lambda$  on  $[n + k] - (D \cup \{a\})$ . From  $\psi'(\lambda)$ , we construct  $\psi(\lambda) \in \mathcal{E}_{n-|D|-1}^{k-1}$  by rearranging numbers from 1.



*Proof of Theorem 3.3.4.* We split the set  $\mathcal{E}_n^k$  into disjoint subsets by the above conditions (1), (2), and (3).

(1) The function  $\psi$  gives a bijection from  $\{\lambda \in \mathcal{E}_n^k \mid \lambda(n + k + 1) = n + k + 1\}$  to  $\mathcal{E}_n^{k-1}$ , which preserves the weight. Thus, we have

$$\sum_{\lambda \in \mathcal{E}_n^k | (1)} x^{w_{\mathcal{E}}^{\text{lr}}(\lambda)} = \mathcal{E}_n^{k-1}(x).$$

(2) In this case, the function  $\psi : \{\lambda \in \mathcal{E}_n^k \mid (2)\} \rightarrow \mathcal{E}_n^{k-1}$  is  $n$ -to-1, which preserves the weight, i.e.,

$$\sum_{\lambda \in \mathcal{E}_n^k | (2)} x^{w_{\mathcal{E}}^{\text{lr}}(\lambda)} = n \mathcal{E}_n^{k-1}(x).$$

(3) If  $b = 1$ , the function  $\psi$  reduces the weight by one. In this case, we obtain

$$\sum_{\substack{\lambda \in \mathcal{E}_n^k |_{(3)} \\ b=1}} x^{w_{\mathcal{E}}^{\text{lf}}(\lambda)} = x \sum_{a=1}^n \sum_{|D|=0}^{a-1} \binom{a-1}{|D|} \mathcal{E}_{n-|D|-1}^{k-1}(x) = x \sum_{d=0}^{n-1} \binom{n}{d+1} \mathcal{E}_{n-d-1}^{k-1}(x).$$

If  $b > 1$ ,  $\psi$  does not affect the weight. In a similar manner, we have

$$\sum_{\substack{\lambda \in \mathcal{E}_n^k |_{(3)} \\ b>1}} x^{w_{\mathcal{E}}^{\text{lf}}(\lambda)} = \sum_{2 \leq b \leq a \leq n} \sum_{|D|=0}^{a-b} \binom{a-b}{|D|} \mathcal{E}_{n-|D|-1}^{k-1}(x) = \sum_{d=0}^{n-2} \binom{n}{d+2} \mathcal{E}_{n-d-1}^{k-1}(x).$$

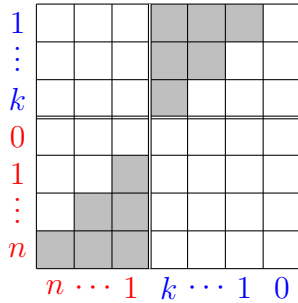
By summation, we have the recurrence formula

$$\mathcal{E}_n^k(x) = (n+1)\mathcal{E}_n^{k-1}(x) + x \sum_{d=0}^{n-1} \binom{n}{d} \mathcal{E}_d^{k-1}(x) + \sum_{d=1}^{n-1} \binom{n}{d-1} \mathcal{E}_d^{k-1}(x),$$

which coincides with that in (3.4). □

### 3.3.2 Another proof by a combinatorial bijection








First, we label the cracked chessboard as follows:



For each double Callan permutation  $(S_1, S_2) \in \mathcal{C}_n^k$ , the placement of  $n+k+1$  rooks on the chessboard are as follows: We set  $S = S_1 0 S_2 0$ .

- (1) For each adjacent same colored pair  $xy$  (resp.  $xy$ ) in  $S$ , place a rook on  $y$ -row,  $x$ -column (resp.  $x$ -row,  $y$ -column).
- (2) Let  $S = x_1 x_2 \dots x_{n+k+2}$ . We perform the following operations in the order  $i = 1, 2, \dots, n+k+1$ :
  - (i) If there is already a rook in the  $x_i$ -column, then we do nothing.
  - (ii) If there is no rook in the  $x_i$ -column, then we place a rook at the  $x_i$ -column and the topmost row among the rows of a different color from  $x_i$  without rooks.

**Example 3.3.6.** From the double Callan permutation  $(S_1, S_2) = (213, 231)$ , we obtain the string  $S = 21302310$ . The corresponding placement of rooks is as follows:

1							
2							
3							
0							
1							
2							
3							
	3	2	1	3	2	1	0

**Theorem 3.3.7.** *The correspondence is well-defined and is a bijection  $\mathcal{C}_n^k \rightarrow \mathcal{E}_n^k$ .*

*Proof.* If there are  $r$  adjacent red pairs and  $b$  adjacent blue pairs in the string  $S$ , then there are  $n + 1 - r$  red substrings and  $k + 1 - b$  blue substrings. By the definition of double Callan permutations, the equation  $n + 1 - r = k + 1 - b$  holds.

By the definition of Step (1), rooks are located on non-cracking squares. The equation  $n - r = k - b$  guarantees the well-definedness of the map. Since we can define the inverse map, this map is bijective.  $\square$

Throughout the above bijection, the weight  $w_{\mathcal{E}}^{\text{lr}}$  allows us to define a new weight  $w_{\mathcal{C}}^{\text{RL}}$  for  $\mathcal{C}_n^k$ .

**Definition 3.3.8.** For each  $\lambda = (S_1, S_2) \in \mathcal{C}_n^k$ , we consider the string  $S = S_1 0 S_2 0$  as before. Let  $\ell$  be the number of blue substrings in  $S$ . We define the weight  $w_{\mathcal{C}}^{\text{RL}}(\lambda)$  using the right-to-left maximum as follows:

- (1) Consider the maximum of each blue substring in  $S$  to obtain a sequence  $\pi = \pi_1 \cdots \pi_{\ell}$ .
- (2) Count the number of  $1 \leq i \leq \ell$  such that, if  $i < j$ , then  $\pi_j < \pi_i$ .
- (3) Subtract 1 from the number.

**Example 3.3.9.** For  $\lambda = (621445, 7632531)$ , we have  $S = 621445076325310$  and  $\pi = 64531$ . The weight of  $\lambda$  is given by  $w_{\mathcal{C}}^{\text{RL}}(\lambda) = \#\{6, 5, 3, 1\} - 1 = 3$ . Similarly, we have  $w_{\mathcal{C}}^{\text{RL}}((213, 231)) = \#\{3\} - 1 = 0$ .

**Corollary 3.3.10.** *The above map defines a bijection  $(\mathcal{C}_n^k, w_{\mathcal{C}}^{\text{RL}}) \rightarrow (\mathcal{E}_n^k, w_{\mathcal{E}}^{\text{lr}})$ , i.e.,  $\mathcal{C}_n^k(x; w_{\mathcal{C}}^{\text{RL}}) = \mathcal{E}_n^k(x; w_{\mathcal{E}}^{\text{lr}})$ .*

By direct enumeration of  $\mathcal{C}_n^k$  with the weight  $w_{\mathcal{C}}^{\text{RL}}$ , we can see that  $\mathcal{C}_n^k(x; w_{\mathcal{C}}^{\text{RL}})$  satisfies (3.1). Thus, again, we have  $\mathcal{E}_n^k(x; w_{\mathcal{E}}^{\text{lr}}) = \widehat{\mathcal{B}}_n^k(x)$ .

### 3.4 An application and remarks

Now, we have various pairs of combinatorial models,  $(\mathcal{C}_n^k, w_{\mathcal{C}}^{\text{lr}})$ ,  $(\mathcal{T}_n^k, w_{\mathcal{T}}^{\text{st}})$ ,  $(\tilde{\mathcal{T}}_n^k, w_{\tilde{\mathcal{T}}}^{\leftarrow})$ ,  $(\mathcal{T}_n^k, w_{\mathcal{T}}^{\text{ch}})$ ,  $(\mathcal{E}_n^k, w_{\mathcal{E}}^{\text{lr}})$ , etc. These models all provide the same polynomial  $\widehat{\mathcal{B}}_n^k(x)$  and have their own characteristics. In this last section, we provide an application of the model  $(\tilde{\mathcal{T}}_n^k, w_{\tilde{\mathcal{T}}}^{\leftarrow})$ .

#### 3.4.1 Combinatorial explanation of the duality

Although the definition of the symmetrized poly-Bernoulli polynomial (3.1) clearly implies the duality  $\widehat{\mathcal{B}}_n^k(x) = \widehat{\mathcal{B}}_k^n(x)$ , it is unclear from the definitions of our combinatorial polynomials. To explain the duality combinatorially, we introduce another weight function for the packed alternative tableau. For each  $\lambda \in \tilde{\mathcal{T}}_n^k$ , the weight  $w_{\tilde{\mathcal{T}}}^{\leftarrow}(\lambda)$  counts the number of rows that contain a  $\leftarrow$  in its leftmost cell, and at least one  $\downarrow$  elsewhere.

**Theorem 3.4.1.** *For any  $n, k \geq 0$ , we have  $\tilde{\mathcal{T}}_n^k(x; w_{\tilde{\mathcal{T}}}^{\leftarrow}) = \tilde{\mathcal{T}}_n^k(x; w_{\tilde{\mathcal{T}}}^{\downarrow})$ .*

*Proof.* We construct a bijection (involution)  $f : (\tilde{\mathcal{T}}_n^k, w_{\tilde{\mathcal{T}}}^{\leftarrow}) \rightarrow (\tilde{\mathcal{T}}_n^k, w_{\tilde{\mathcal{T}}}^{\downarrow})$ . For  $\lambda \in \tilde{\mathcal{T}}_n^k$ , we define  $f(\lambda)$  by the following operations simultaneously:

- (1) Consider all columns that contain a  $\downarrow$  in its bottom cell, and at least one  $\leftarrow$  elsewhere. For each such column, we slide up the  $\downarrow$  to the location of the lowest  $\leftarrow$  in the column, and slide left the lowest  $\leftarrow$  to the leftmost cell in the same row.
- (2) Consider all rows that contain a  $\leftarrow$  in its leftmost cell, and at least one  $\downarrow$  elsewhere. For each such row, we slide right the  $\leftarrow$  to the location of the most-left  $\downarrow$  in the row, and slide down the most-left  $\downarrow$  to the bottom cell in the same column.

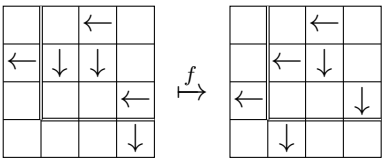


Figure 3.6: Example of the mapping.

The map is a well-defined involution. Moreover, we have  $w_{\tilde{\mathcal{T}}}^{\leftarrow}(\lambda) = w_{\tilde{\mathcal{T}}}^{\downarrow}(f(\lambda))$  for all  $\lambda \in \tilde{\mathcal{T}}_n^k$ .  $\square$

By reflecting packed alternative tableaux, we have  $\tilde{\mathcal{T}}_n^k(x; w_{\tilde{\mathcal{T}}}^{\leftarrow}) = \tilde{\mathcal{T}}_k^n(x; w_{\tilde{\mathcal{T}}}^{\downarrow})$ . Thus, we obtain the duality

$$\tilde{\mathcal{T}}_n^k(x; w_{\tilde{\mathcal{T}}}^{\leftarrow}) = \tilde{\mathcal{T}}_k^n(x; w_{\tilde{\mathcal{T}}}^{\downarrow}).$$

This provides a combinatorial interpretation of the duality formula.

As the above argument suggests, it seems natural to consider a two-variable polynomial defined by the weight function and its “suitable” dual weight function. Here, we will only introduce a few considerations. For instance, the pair of weights  $(w_{\tilde{\mathcal{T}}}^{\leftarrow}, w_{\tilde{\mathcal{T}}}^{\downarrow})$  defines the polynomial

$$\tilde{\mathcal{T}}_n^k(x, y; w_{\tilde{\mathcal{T}}}^{\leftarrow}, w_{\tilde{\mathcal{T}}}^{\downarrow}) := \sum_{\lambda \in \tilde{\mathcal{T}}_n^k} x^{w_{\tilde{\mathcal{T}}}^{\leftarrow}(\lambda)} y^{w_{\tilde{\mathcal{T}}}^{\downarrow}(\lambda)}.$$

The two-variable polynomial clearly satisfies  $\tilde{\mathcal{T}}_n^k(x, y; w_{\tilde{\mathcal{T}}}^{\leftarrow}, w_{\tilde{\mathcal{T}}}^{\downarrow}) = \tilde{\mathcal{T}}_k^n(y, x; w_{\tilde{\mathcal{T}}}^{\leftarrow}, w_{\tilde{\mathcal{T}}}^{\downarrow})$  by reflecting packed alternative tableaux.

Similarly, Bényi–Matsusaka [11] considered a dual weight of  $w_{\mathcal{T}}^{\text{st}} : \mathcal{T}_n^k \rightarrow \mathbb{Z}_{\geq 0}$  by reflecting alternative tableaux and all notions. Of course, the same duality formula in two variables holds, but the resulting polynomials are different generally. In fact, their two-variable polynomial defined in [11, Section 6] for  $n = k = 2$  is given by

$$T_2^2(x, y) = x^2y + xy^2 + x^2 + 7xy + y^2 + 7x + 7y + 6.$$

On the other hand, ours is given by  $\tilde{\mathcal{T}}_2^2(x, y; w_{\tilde{\mathcal{T}}}^{\leftarrow}, w_{\tilde{\mathcal{T}}}^{\downarrow}) = 2x^2 + 4xy + 2y^2 + 11x + 11y + 1$ .

In connection with this topic, Bényi–Matsusaka [10] introduced  $(r, s)$ -extended Callan sequences, and showed a relation to Bayad–Hamahata’s two-variable poly-Bernoulli polynomials (see also [7]).

### 3.4.2 Concluding remarks

Recently, Bényi and Matsusaka [10] and Bényi–Ramírez [12] introduced combinatorial models for (non-symmetrized) poly-Bernoulli polynomials, poly-Euler numbers, and poly-Cauchy numbers based on the idea of Callan sequences. Using the interpretations, they provided combinatorial proofs for a large variety of known or new equations. It would be interesting to understand these polynomials and numbers using our various combinatorial models. As explained in this chapter, our combinatorial objects and weights have their own advantages. Do our models provide new aspects of these polynomials and numbers?

For each combinatorial set  $\mathcal{P}$ , there are many possibilities for weight functions. In this chapter, we defined three weights,  $w_{\mathcal{C}}^{\text{lr}}$ ,  $w_{\mathcal{C}}^{\text{br}}$ , and  $w_{\mathcal{C}}^{\text{RL}}$ , for the set of double Callan permutations. As a similar phenomenon, for instance, Dumont–Foata [20] introduced three weights for the set of (surjective) pistols. The corresponding three polynomials define the same polynomial, namely, the Gandhi polynomial. Furthermore, it is known that the Gandhi polynomial coincides with the anti-diagonal alternating sum of the symmetrized poly-Bernoulli polynomials [48]. This result was shown indirectly by using the recurrence relations. Is it possible to provide its combinatorial proof? (See also Bényi–Josuat-Vergès [9]).



## Acknowledgements

The author would like to thank Tomokazu Kashio for his dedicated guidance and meaningful discussions. It is thanks to him that the author was able to complete this thesis. Hiroki Aoki, Yoshiyuki Fukumoto, Susumu Hirose, Hiroyuki Ito and Masanari Kida also provided many useful suggestions for this thesis throughout the dissertation defense. The author would like to thank them. The author also would like to thank his joint researchers Minoru Hirose, Toshiki Matsusaka, Ryutaro Sekigawa, and Jun Ueki. Yoshinosuke Hirawaka gave the author many useful advice throughout the doctoral course. Finally, the author expresses his greatest gratitude to his mother Yukari Yoshizaki, and two beloved dogs, Valon and Andy. A later half of Chapter 2 (from Section 2.6) is reproduced with permission from Springer Nature.

# Bibliography

- [1] Tom M. Apostol. Resultants of cyclotomic polynomials. *Proc. Amer. Math. Soc.*, Vol. 24, pp. 457–462, 1970.
- [2] Tsuneo Arakawa, Tomoyoshi Ibukiyama, and Masanobu Kaneko. *Bernoulli numbers and zeta functions*. Springer Monographs in Mathematics. Springer, Tokyo, 2014. With an appendix by Don Zagier.
- [3] G. Asvin. On the variation of Frobenius eigenvalues in a skew-abelian Iwasawa tower. preprint. arXiv:2203.16774, March 2022.
- [4] Yves Aubry and Marc Perret. On the characteristic polynomials of the Frobenius endomorphism for projective curves over finite fields. *Finite Fields Appl.*, Vol. 10, No. 3, pp. 412–431, 2004.
- [5] L. Babinkostova, J. C. Bahr, Y. H. Kim, E. Neyman, and G. K. Taylor. Anomalous primes and the elliptic Korselt criterion. *J. Number Theory*, Vol. 201, pp. 108–123, 2019.
- [6] Helmut Bauer. Numerische Bestimmung von Klassenzahlen reeller zyklischer Zahlkörper. *Journal of Number Theory*, Vol. 1, No. 2, pp. 161–162, 1969.
- [7] A. Bayad and Y. Hamahata. Polylogarithms and poly-Bernoulli polynomials. *Kyushu J. Math.*, Vol. 65, No. 1, pp. 15–24, 2011.
- [8] Beáta Bényi and Péter Hajnal. Combinatorics of poly-Bernoulli numbers. *Studia Sci. Math. Hungar.*, Vol. 52, No. 4, pp. 537–558, 2015.
- [9] Beáta Bényi and Matthieu Josuat-Vergès. Combinatorial proof of an identity on Genocchi numbers. *Journal of Integer Sequences*, Vol. 24, , 2021.
- [10] Beáta Bényi and Toshiki Matsusaka. Combinatorial aspects of poly-Bernoulli polynomials and poly-Euler numbers. to appear, *Journal de Théorie des Nombres de Bordeaux*.
- [11] Beáta Bényi and Toshiki Matsusaka. On the combinatorics of symmetrized poly-Bernoulli numbers. *Electron. J. Combin.*, Vol. 28, No. 1, pp. Paper No. 1.47, 20, 2021.

- [12] Beáta Bényi and José Luis Ramírez. Poly-Cauchy numbers – the combinatorics behind. *Enumerative Combinatorics and Applications*, p. Article #S2R1, 2022.
- [13] Hans F. Blichfeldt. A new principle in the geometry of numbers, with some applications. *Transactions of the American Mathematical Society*, Vol. 15, No. 3, pp. 227–235, 1914.
- [14] Chad Brewbaker. A combinatorial interpretation of the poly-Bernoulli numbers and two Fermat analogues. *Integers*, Vol. 8, pp. A02, 9, 2008.
- [15] Bradley W. Brock, Noam D. Elkies, and Bruce W. Jordan. Periodic continued fractions over  $S$ -integers in number fields and Skolem’s  $p$ -adic method. *Acta Arithmetica*, Vol. 197, No. 4, pp. 379–420, 2021.
- [16] Eric Clark and Richard Ehrenborg. Explicit expressions for the extremal exceedance set statistics. *European J. Combin.*, Vol. 31, No. 1, pp. 270–279, 2010.
- [17] Pierre Dehornoy. On the zeroes of the Alexander polynomial of a Lorenz knot. *Ann. Inst. Fourier (Grenoble)*, Vol. 65, No. 2, pp. 509–548, 2015.
- [18] Christopher Deninger.  $p$ -adic limits of renormalized logarithmic Euler characteristics. *Groups Geom. Dyn.*, Vol. 14, No. 2, pp. 427–467, 2020.
- [19] Fred Diamond and Jerry Shurman. *A first course in modular forms*, Vol. 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.
- [20] Dominique Dumont and Dominique Foata. Une propriété de symétrie des nombres de Genocchi. *Bull. Soc. Math. France*, Vol. 104, No. 4, pp. 433–451, 1976.
- [21] Richard Ehrenborg and Einar Steingrímsson. The exceedance set of a permutation. *Adv. in Appl. Math.*, Vol. 24, No. 3, pp. 284–299, 2000.
- [22] Noam D. Elkies. The existence of infinitely many supersingular primes for every elliptic curve over  $\mathbf{Q}$ . *Invent. Math.*, Vol. 89, No. 3, pp. 561–567, 1987.
- [23] Takashi Fukuda. *Exposition of the Iwasawa Theory; from theories to calculations, Juuten kaisetsu Iwasawa riron: riron kara keisan made (in Japanese)*. No. 145 in SGC Library. SAIENSU - SHA, 2019.
- [24] Takashi Fukuda and Keiichi Komatsu. Weber’s Class Number Problem in the Cyclotomic  $\mathbb{Z}_2$ -Extension of  $\mathbb{Q}$ . *Experimental Mathematics*, Vol. 18, No. 2, pp. 213–222, 2009.
- [25] Takashi Fukuda and Keiichi Komatsu. Weber’s class number problem in the cyclotomic  $\mathbb{Z}_2$ -extension of  $\mathbb{Q}$ , iii. *International Journal of Number Theory*, Vol. 07, No. 06, pp. 1627–1635, 2011.

- [26] Takashi Fukuda, Keiichi Komatsu, and Takayuki Morisawa. Weber’s class number one problem. In *Iwasawa theory 2012*, Vol. 7 of *Contrib. Math. Comput. Sci.*, pp. 221–226. Springer, Heidelberg, 2014.
- [27] R. Gold and H. Kisilevsky. On geometric  $\mathbf{Z}_p$ -extensions of function fields. *Manuscripta Math.*, Vol. 62, No. 2, pp. 145–161, 1988.
- [28] Sang-G. Han. On  $p$ -adic  $L$ -functions and the Riemann-Hurwitz genus formula. *Acta Arith.*, Vol. 60, No. 2, pp. 97–104, 1991.
- [29] Jonathan Hillman, Daniel Matei, and Masanori Morishita. Pro- $p$  link groups and  $p$ -homology groups. In *Primes and knots*, Vol. 416 of *Contemp. Math.*, pp. 121–136. Amer. Math. Soc., Providence, RI, 2006.
- [30] Minoru Hirose, Toshiki Matsusaka, Ryutaro Sekigawa, and Hyuga Yoshizaki. Bijective enumerations for symmetrized poly-bernoulli polynomials. *The Electronic Journal of Combinatorics*, Vol. 29, No. 3, 2022.
- [31] Kuniaki Horie. The ideal class group of the basic  $\mathbf{Z}(P)$ -extension over an imaginary quadratic field. *Tohoku Mathematical Journal*, Vol. 57, , 09 2005.
- [32] Kuniaki Horie. Certain primary components of the ideal class group of the  $\mathbf{Z}_p$ -extension over the rationals. *Tohoku Mathematical Journal*, Vol. 59, No. 2, pp. 259 – 291, 2007.
- [33] Jim Hoste and Patrick D. Shanahan. A formula for the A-polynomial of twist knots. *J. Knot Theory Ramifications*, Vol. 13, No. 2, pp. 193–209, 2004.
- [34] Kenkichi Iwasawa. On  $\Gamma$ -extensions of algebraic number fields. *Bull. Amer. Math. Soc.*, Vol. 65, pp. 183–226, 1959.
- [35] Teruhisa Kadokami and Yasushi Mizusawa. Iwasawa type formula for covers of a link in a rational homology sphere. *J. Knot Theory Ramifications*, Vol. 17, No. 10, pp. 1199–1221, 2008.
- [36] Masanobu Kaneko. Poly-Bernoulli numbers. *J. Théor. Nombres Bordeaux*, Vol. 9, No. 1, pp. 221–228, 1997.
- [37] Masanobu Kaneko, Fumi Sakurai, and Hirofumi Tsumura. On a duality formula for certain sums of values of poly-Bernoulli polynomials and its application. *J. Théor. Nombres Bordeaux*, Vol. 30, No. 1, pp. 203–218, 2018.
- [38] Se-Goo Kim. Alexander polynomials and orders of homology groups of branched covers of knots. *J. Knot Theory Ramifications*, Vol. 18, No. 7, pp. 973–984, 2009.
- [39] Steffen Kionke. On  $p$ -adic limits of topological invariants. *J. Lond. Math. Soc. (2)*, Vol. 102, No. 2, pp. 498–534, 2020.

- [40] H. Kisilevsky. A generalization of a result of Sinnott. *Pacific J. Math.*, No. Special Issue, pp. 225–229, 1997. Olga Taussky-Todd: in memoriam.
- [41] Michiel Kusters and Daqing Wan. Genus growth in  $\mathbb{Z}_p$ -towers of function fields. *Proc. Amer. Math. Soc.*, Vol. 146, No. 4, pp. 1481–1494, 2018.
- [42] Serge Lang. *Introduction to Diophantine Approximations, New Expanded Edition*. Springer New York, NY, 1995.
- [43] Serge Lang and Hale Trotter. *Frobenius distributions in  $GL_2$ -extensions*. Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin-New York, 1976. Distribution of Frobenius automorphisms in  $GL_2$ -extensions of the rational numbers.
- [44] Stéphane Launois. Rank  $t$   $\mathcal{H}$ -primes in quantum matrices. *Comm. Algebra*, Vol. 33, No. 3, pp. 837–854, 2005.
- [45] Yi Liu. Finite-volume hyperbolic 3-manifolds are almost determined by their finite quotient groups. *Invent. Math.*, p. 64 pages, September 2022.
- [46] Charles Livingston. Seifert forms and concordance. *Geom. Topol.*, Vol. 6, pp. 403–408, 2002.
- [47] John Myron Masley. Class numbers of real cyclic number fields with small conductor. *Compositio Mathematica*, Vol. 37, No. 3, pp. 297–319, 1978.
- [48] Toshiki Matsusaka. Symmetrized poly-Bernoulli numbers and combinatorics. *J. Integer Seq.*, Vol. 23, No. 9, pp. Art. 20.9.2, 8, 2020.
- [49] John P. Mayberry and Kunio Murasugi. Torsion-groups of abelian coverings of links. *Trans. Amer. Math. Soc.*, Vol. 271, No. 1, pp. 143–173, 1982.
- [50] Barry Mazur. Remarks on the Alexander polynomial. [http://www.math.harvard.edu/~mazur/papers/alexander\\_polynomial.pdf](http://www.math.harvard.edu/~mazur/papers/alexander_polynomial.pdf), 1963–64.
- [51] Barry Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.*, Vol. 18, pp. 183–266, 1972.
- [52] Barry Mazur. Primes, Knots and Po. Lecture notes for the conference “Geometry, Topology and Group Theory” in honor of the 80th birthday of Valentin Poenaru, July 2012.
- [53] Curtis T. McMullen. Knots which behave like the prime numbers. *Compos. Math.*, Vol. 149, No. 8, pp. 1235–1244, 2013.
- [54] John C. Miller. Class numbers of totally real fields and applications to the Weber class number problem. *Acta Arithmetica*, Vol. 164, No. 4, pp. 381–397, 2014.

- [55] Takayuki Morisawa and Ryotaro Okazaki. Height and Weber’s Class Number Problem. *Journal de Théorie des Nombres de Bordeaux*, Vol. Tome 28, No. 3, pp. 811–828, 2016.
- [56] Takayuki Morisawa and Ryotaro Okazaki. Filtrations of units of Viète field. *International Journal of Number Theory*, Vol. 16, No. 05, pp. 1067–1079, 2020.
- [57] Masanori Morishita. *Knots and primes*. Universitext. Springer, London, 2012. An introduction to arithmetic topology.
- [58] Philippe Nadeau. The structure of alternative tableaux. *J. Combin. Theory Ser. A*, Vol. 118, No. 5, pp. 1638–1660, 2011.
- [59] Iven Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. Wiley, 5 edition, 1991.
- [60] Akio Noguchi. A functional equation for the Lefschetz zeta functions of infinite cyclic coverings with an application to knot theory. *Topology Proc.*, Vol. 29, No. 1, pp. 277–291, 2005. Spring Topology and Dynamical Systems Conference.
- [61] Loren D. Olson. Hasse invariants and anomalous primes for elliptic curves with complex multiplication. *J. Number Theory*, Vol. 8, No. 4, pp. 397–414, 1976.
- [62] Manabu Ozaki. On the  $p$ -adic limit of class numbers along a pro- $p$ -extension. preprint., 2022.
- [63] PARI Group, The, Univ. Bordeaux. *PARI/GP version 2.15.0*, 2022. available at <http://pari.math.u-bordeaux.fr/>.
- [64] Joan Porti. Mayberry-Murasugi’s formula for links in homology 3-spheres. *Proc. Amer. Math. Soc.*, Vol. 132, No. 11, pp. 3423–3431 (electronic), 2004.
- [65] Dale Rolfsen. *Knots and links*. Publish or Perish, Inc., Berkeley, Calif., 1976. Mathematics Lecture Series, No. 7.
- [66] Michael Rosen. *Number theory in function fields*, Vol. 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.
- [67] Makoto Sakuma. The homology groups of abelian coverings of links. *Math. Sem. Notes Kobe Univ.*, Vol. 7, No. 3, pp. 515–530, 1979.
- [68] Makoto Sakuma. On the polynomials of periodic links. *Math. Ann.*, Vol. 257, No. 4, pp. 487–494, 1981.
- [69] Jordan Schettler. Generalizations of Iwasawa’s “Riemann-Hurwitz” formula for cyclic  $p$ -extensions of number fields. *Int. J. Number Theory*, Vol. 10, No. 1, pp. 219–233, 2014.

- [70] Qibin Shen and Shuhui Shi. Function fields of class number one. *J. Number Theory*, Vol. 154, pp. 375–379, 2015.
- [71] Joseph H. Silverman. *The arithmetic of elliptic curves*, Vol. 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.
- [72] Henning Stichtenoth. *Algebraic function fields and codes*, Vol. 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.
- [73] Hiroki Sumida-Takahashi. Computation of the Iwasawa invariants of certain real abelian fields. *J. Number Theory*, Vol. 105, No. 2, pp. 235–250, 2004.
- [74] Hiroki Sumida-Takahashi. Computation of the  $p$ -part of the ideal class group of certain real abelian fields. *Math. Comp.*, Vol. 76, No. 258, pp. 1059–1071, 2007.
- [75] Ryoto Tange. Fox formulas for twisted Alexander invariants associated to representations of knot groups over rings of  $S$ -integers. *J. Knot Theory Ramifications*, Vol. 27, No. 5, pp. 1850033, 15, 2018.
- [76] Sohei Tateno and Jun Ueki. The Iwasawa invariants of  $\mathbb{Z}_p^d$ -covers of links. preprint, 2023.
- [77] Jun Ueki. On the homology of branched coverings of 3-manifolds. *Nagoya Math. J.*, Vol. 213, pp. 21–39, 2014.
- [78] Jun Ueki. On the Iwasawa invariants for links and Kida’s formula. *Internat. J. Math.*, Vol. 28, No. 6, pp. 1750035, 30, 2017.
- [79] Jun Ueki. The profinite completions of knot groups determine the Alexander polynomials. *Algebr. Geom. Topol.*, Vol. 18, No. 5, pp. 3013–3030, 2018.
- [80] Jun Ueki.  $p$ -adic Mahler measure and  $\mathbb{Z}$ -covers of links. *Ergodic Theory Dynam. Systems*, Vol. 40, No. 1, pp. 272–288, 2020.
- [81] Jun Ueki. Chebotarev links are stably generic. *Bull. Lond. Math. Soc.*, Vol. 53, No. 1, pp. 82–91, February 2021.
- [82] Jun Ueki. Modular knots obey the chebotarev law. preprint. arXiv:2105.10745, May 2021.
- [83] Jun Ueki. Profinite rigidity for twisted Alexander polynomials. *J. Reine Angew. Math.*, Vol. 771, pp. 171–192, 2021.
- [84] Jun Ueki. Erratum to: Profinite rigidity for twisted Alexander polynomials. *J. Reine Angew. Math.*, Vol. 783, pp. 275–278, February 2022.
- [85] Jun Ueki and Akane Yasuda. A note on units and surfaces. preprint. submitted to Proc. Low dimensional topology and number theory XII, 2022.

- [86] F. J. van der Linden. Class Number Computations of Real Abelian Number Fields. *Mathematics of Computation*, Vol. 39, No. 160, pp. 693–707, 1982.
- [87] Xavier Viennot. Alternative tableaux, permutations and partially asymmetric exclusion process. Isaac Newton Institute, [http://www.xavierviennot.org/xavier/videos\\_files/AT\\_Cambridge\\_web.pdf](http://www.xavierviennot.org/xavier/videos_files/AT_Cambridge_web.pdf), 2008.
- [88] Daqing Wan and Ping Xi. Lang–trotter conjecture for CM elliptic curves. preprint. arXiv:2109.14256, 2021.
- [89] Lawrence C. Washington. The non- $p$ -part of the class number in a cyclotomic  $\mathbf{Z}_p$ -extension. *Invent. Math.*, Vol. 49, No. 1, pp. 87–97, 1978.
- [90] Lawrence C. Washington. *Introduction to cyclotomic fields*, Vol. 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.
- [91] Claude Weber. Sur une formule de R. H. Fox concernant l’homologie des revêtements cycliques. *Enseign. Math. (2)*, Vol. 25, No. 3-4, pp. 261–272 (1980), 1979.
- [92] Heinrich Weber. Theorie der Abel’schen Zahlkörper. *Acta Math.*, Vol. 8, No. 1, pp. 193–263, 1886.
- [93] André Weil. *Sur les courbes algébriques et les variétés qui s’en déduisent*, Vol. 7 of *Publ. Inst. Math. Univ. Strasbourg*. Hermann & Cie, Paris, 1948.
- [94] Hideo Yokoi. On the class number of a relatively cyclic number field. *Nagoya Mathematical Journal*, Vol. 29, pp. 31 – 44, 1967.
- [95] Hyuga Yoshizaki. Generalized Pell’s equations and Weber’s class number problem. *Journal de Théorie des Nombres de Bordeaux*, Vol. 35, No. 2, pp. 373–391, 2023.
- [96] Hyuga Yoshizaki. Weber’s class number problem and its variants. In *Low dimensional topology and Number theory*, Springer Proceedings in Mathematics & Statistics. Springer, 2023.
- [97] A. V. Zarelua. On congruences for the traces of powers of some matrices. *Tr. Mat. Inst. Steklova*, Vol. 263, No. Geometriya, Topologiya i Matematicheskaya Fizika. I, pp. 85–105, 2008.