Inauguraldissertation
zur
Erlangung der Doktorwürde
der
Naturwissenschaftlich-Mathematischen Gesamtfakultät
der
Ruprecht-Karls-Universität
Heidelberg

vorgelegt von
Luis Felipe Müller, M.Sc.
geboren in Bogotá

Tag der mündlichen Prüfung:

Analytic Properties of s-Functions

L. Felipe Müller
Betreuer: Professor Dr. Johannes Walcher

30. April 2021

Eigenständigkeitserklärung

Hiermit versichere ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.
Heidelberg, den 30. April 2021

Luis Felipe Müller

Abstract

Let K be a number field, normal over $\mathbb{Q}$, and p be an unramified prime in $K|\mathbb{Q}$. We study s-sequences and analytic properties of their generating functions (which are s-fold derivatives of s-functions) where s refers to a natural number. The entries of such an s-sequence $(a_n)_{n\in\mathbb{N}}$ are p-adic integral numbers and satisfy certain supercongruence relations that depend on s and involve the Frobenius element at every prime ideal dividing p. While the case $s = 1$ is widely studied in the literature, we are interested in the situation $s \geq 2$. The obstruction of being an s-sequence grows for growing s. The first result in the present work is the statement that if the generating function of a 2-sequence represents a rational function, then the coefficients a_n belong to a cyclotomic field. More precisely, we show that the poles of such functions are poles of order one given by roots of unity and rational residue. In the second part, we analyze an operator on formal power series, called framing, which preserves 2-functions. As a second result, we show that the image of rational 2-functions under the framing can be integrated to 3-functions, at least for almost all primes p. As a trivial consequence of this second theorem, we obtain the Jacobsthal-Kazandzidis congruence.

Zusammenfassung

Sei K ein Zahlkörper, normal über $\mathbb{Q}$, und p eine Primzahl, welche unverzweigt in $K|\mathbb{Q}$ ist. Wir untersuchen s-Folgen und analytische Eigenschaften deren generierenden Funktionen, wobei s eine natürliche Zahl bezeichne. Die Einträge einer solchen s-Folge $(a_n)_{n\in\mathbb{N}}$ sind p-adische ganze Zahlen und erfüllen gewisse Superkongruenzen $\mathrm{Frob}_{\mathfrak{p}}(a_{mp^{r-1}}) \equiv a_{mp^r} \mod \mathfrak{p}^{sr}$, wobei $\mathfrak{p}$ ein Primideal über p ist und $\mathrm{Frob}_{\mathfrak{p}}$ das korrespondierende Frobeniuselement in der Galois Gruppe. Während der Fall $s = 1$ in der Literatur weitestgehend erforscht ist, interessieren wir uns für $s \geq 2$. Die Stärke der definierenden Bedingung einer s-Folge wächst mit steigendem s. Das erste Resultat der vorliegenden Arbeit ist die Aussage, dass falls die generierende Funktion einer 2-Folge eine rationale Funktion darstellt, die Folgenglieder a_n in einem zyklotomischen Körper liegen. Genauer zeigen wir, dass die Polstellen einer solchen Funktion Ordnung 1 haben mit rationalem Residuum und Einheitswurzeln sind. Im zweiten Teil der Arbeit untersuchen wir den sogenannten Framing Operator, der auf formalen Potenzreihen definiert ist und welcher 2-Funktionen auf 2-Funktionen abbildet. Das zweite Resultat ist die Aussage, dass sich das Bild einer rationalen 2-Funktion unter dem Framing Operator zu einer 3-Funktion integrieren lässt, zumindest für fast alle (unverzweigten) Primzahlen p. Als Korollar dieser Aussage erhalten wir die Jacobsthal-Kazandzidis Kongruenz.

Acknowledgements

I would like to thank my supervisor, Johannes Walcher, for his support and sharing his experience with me.

I would also like to thank Mirko Rösner and Ingmar Saberie who provided me with valuable discussions and gave me new inspiration to further my research.

I am grateful to Johanna Berndt. Your wise counsel and sympathetic ears helped me to successfully complete my dissertation.

Also, I would like to thank my mother. You are always there for me.

Finally, I am grateful to my friends, Dominik Wrazidlo, Sebastian Nill, Conrad Knittel, Xenia Gerloff, Nils Rörup, Vera Engels and Florentine Jurisch for their valuable advice as well as happy distractions to rest my mind outside of my research.

Contents

Chapter 1
Introduction

Parts of the content of the chapters 1-4 of this dissertation are uploaded to arXiv, see [32], [33], and are submitted to journals with a review process. In the present chapter, the author will summarize the content of the work and give a survey on the background in physics as the initial motivation for this work. The author does not claim to have full insights of the physics.

Fermat's and Euler's congruences are well-known in number theory and are rich of remarkable consequences. In the following we will give a short survey of these congruences. We start with the famous

Theorem 1.1 (Euler) *The congruence*

$$a^{p^r} \equiv a^{p^{r-1}} \mod p^r \tag{1.1}$$

holds for all integers $a \in \mathbb{Z}$, all primes p, and all natural numbers $r \in \mathbb{N}$.

(Theorem 1.1 is more than a good opener, it plays a very important role in the context of Theorem 1.2 below.) A sequence $(a_k)_{k\in\mathbb{N}}$ of rational numbers is called an *Euler sequence* (or *Gauss sequence* as in [7]) for the prime p, if a_k is a p-adic integer for all $k \in \mathbb{N}$ and

$$a_{mp^r} \equiv a_{mp^{r-1}} \mod p^r \tag{1.2}$$

for all integers $r \geq 1$ and $m \geq 1$. A survey of these congruences has been given in [30] and [48].

Beukers coined the term *supercongruence*: A supercongruence (with respect to a

prime p) refers to a sequence $(a_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p^{\mathbb{N}}$ that satisfies congruences of the type

$$a_{mp^r} \equiv a_{mp^{r-1}} \mod p^{sr}, \tag{1.3}$$

for all $m, r \in \mathbb{N}$ and a fixed $s \in \mathbb{N}$, $s > 1$ (cf. [12]). Such supercongruences are given by the Jacobsthal-Kazandzidis congruence (cf. [10] or Example 4.26 in the present work), Apéry numbers (cf. [3], [6]), generalized Domb numbers (cf. [36]) and Almkvist-Zudilin numbers (cf. [2], [18]) to name a few. The Apéry numbers

$$A_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2, \quad \text{for } n \in \mathbb{N},$$

appear in Apéry's irrationality proof of the values $\zeta(2)$ and $\zeta(3)$, while the Almkvist-Zudilin numbers

$$B_n = \sum_{k=0}^{\lfloor n/3 \rfloor} (-1)^{n-k} \binom{3k}{k} \binom{2k}{k} \binom{n}{3k} \binom{n+k}{k} 3^{n-3k}, \quad \text{for } n \in \mathbb{N}$$

appear as coefficients of a solution of a linear differential equation similar to those occurring in Calabi-Yau theory.

1.1 Analyticity and Basis of s-Functions

Sequences satisfying eq. (1.3) for all primes in $\mathbb{Z}$ are also referred to as *s-realizable sequences* in [2]. For instance, the sequence of coefficients of the Maclaurin expansion of the Yukawa coupling is expected to be 3-realizable. Note that all the above mentioned supercongruences are 2-realizable and 3-realizable for all $p \geq 5$. Taking the Lambert expansion of the generating power series of an s-realizable sequence $(a_n)_{n\in\mathbb{N}}$

$$\sum_{n=1}^{\infty} a_n z^n = \sum_{n=1}^{\infty} b_n n^s \frac{z^n}{1-z^n} \tag{1.4}$$

gives integral coefficients $(b_n)_{n\in\mathbb{N}}$ (and vice versa, given integers $(b_n)_{n\in\mathbb{N}}$ in eq. (1.4), one obtains an s-realizable sequence $(a_n)_{n\in\mathbb{N}}$). In the case of the Yukawa coupling when the moduli space of complex structures is one-dimensional, the coefficients $\{b_n\}_n$ ($s = 3$) are realized by numbers which are referred to as "*instanton numbers*" in mathematical literature, see for instance [26]. Indeed, according to the Mirror Symmetry Conjecture (see [11], [31]) the number b_n in the case of the Yukawa coupling is the number of rational curves of degree n on a generic quintic hypersurface in projective space $\mathbb{P}^4$. In particular, physical dualities predict the numbers b_n, $n \in \mathbb{N}$ to be integers, which is a

highly non-trivial fact and which is equivalent to $(a_n)_{n\in\mathbb{N}}$ being 3-realizable.

Let K be an algebraic number field and $\mathcal{O}$ its ring of algebraic integers. We consider a generalization of s-realizable sequences to sequences of algebraic integers in K. More precisely, for $s \in \mathbb{N}$ an s-sequence is a sequence $(a_n) \in K^{\mathbb{N}}$, such that for any unramified prime ideal $\mathfrak{p} \in \mathcal{O}$ lying above the prime $p \in \mathbb{Z}$, $a_n \in \mathcal{O}_{\mathfrak{p}}$, and for all $m, r \in \mathbb{N}$,

$$\mathrm{Frob}_{\mathfrak{p}}\left(a_{p^{r-1}m}\right) - a_{p^r m} \equiv 0 \mod p^{sr}\mathcal{O}_{\mathfrak{p}}, \tag{1.5}$$

where $\mathcal{O}_{\mathfrak{p}}$ is the ring of $\mathfrak{p}$-adic integers and $\mathrm{Frob}_{\mathfrak{p}}$ is the canonical lift of the standard Frobenius element of $\mathfrak{p}$ in the Galois group of the local field extension $(\mathcal{O}/\mathfrak{p})|(\mathbb{Z}/p)$. The generating function $V(z)$ of an s-sequence then integrates to what is referred to as an s-function in [40] (hence the name). More precisely, the s-sequence $a \in K^{\mathbb{N}}$ corresponds to the s-function $\int^s V(z)$ (see Proposition 2.10 in Section 2) given by the (formal) power series

$$\int^s V(z) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} z^n \in zK[\![z]\!], \tag{1.6}$$

This rises the question whether there exist analytic s-functions. The most elementary case is given by $a_n = 1$ (and $K = \mathbb{Q}$), in which case eq. (1.6) becomes $\int^s V(z) = \mathrm{Li}_s(z)$ the polylogarithm function of order s. In [47], Zagier gave a survey on the dilogarithm function Li_2 and its appearance and significance in number theory, geometry and mathematical physics, and discussed analytic properties of Li_2. It would therefore be interesting to find analogous statements for 2-functions are a (natural) generalization Li_2^K of Li_2 with coefficients in K in terms of 2-sequences satisfying analogous analytic properties. On the other hand, one realization of 2-functions is provided in super symmetry, see [39], [40]. As stated in [40], see Thm. 22 therein, 2-functions appear as the non-singular part of the superpotential function (without the constant term) with algebraic coefficients. In other words, algebraic cycles on Calabi-Yau three-folds provide a source of 2-functions that are analytic and furthermore satisfy a differential equation with algebraic coefficients. Therefore, it is expected that understanding the numerical interpretation of open Gromov-Witten/BPS theory highly depend on delivering some (natural) basis of the class of 2-functions with algebraic coefficients.

It is therefore of main interest to characterize a submodule of s-functions of suitable algebraic or analytic properties, and a class of distinguished generators for this submodule. The contribution of the present work to this problem is to give a characterization of a 2-function $\int^2 V(z)$, where V represents a rational function. We have

Theorem 1.2 *Let $V \in zK[\![z]\!]$, $V(z) \neq 0$, be the generating function of a 2-sequence*

$(a_n)_{n\in\mathbb{N}} \in K^{\mathbb{N}}$, representing the rational function $F(z) \in K(z)$ as its Maclaurin expansion. Then, there is an $N \in \mathbb{N}$ and there are rational coefficients $A_i \in \mathbb{Q}$ for $i = 1, ..., N$ and an appropriate primitive N-th root of unity ζ, such that

$$F(z) = \sum_{i=1}^{N} \frac{A_i \zeta^i z}{1 - \zeta^i z}. \tag{1.7}$$

In particular, the coefficients a_n of $V(z)$ have the form

$$a_n = \sum_{i=1}^{N} A_i \zeta^{in}. \tag{1.8}$$

A consequence of Theorem 1.2 is that for an s-sequence in $\mathbb{Z}$, $(a_n)_{n\in\mathbb{N}} \in \mathbb{Z}^{\mathbb{N}}$, representing a rational function $V(z)$, where $s \geq 2$, the Lambert expansion eq. (1.4) of the generating function $V(z)$ of $\{a_n\}$ terminates,

$$V(z) = \sum_{n=1}^{N} b_n n^s \frac{z^n}{1 - z^n}. \tag{1.9}$$

Of course, as long as $s \geq 2$ and $a_n \in \mathbb{Z}$, eq. (1.9) is equivalent to Theorem 1.2, see Theorem 2.12 and Theorem 3.18. The author is not aware of a direct proof of eq. (1.9) for rational V, yet, without concluding it from Theorem 1.2. Furthermore, for algebraic coefficients $a_n \in K$, the Lambert series expansion eq. (1.9) does not terminate, even if V represents a rational function, see Example 2.11 (2) for a counterexample. The reason for this is that the Lambert expansion of V is a priori a formal expression. This shows, that s-sequences with algebraic coefficients are more complicated than s-realizable sequences (where the coefficients are rational integers).

The initial (mathematical) motivation for the statement of Theorem 1.2 was the question whether or not the subfield $K' \subset K$ generated by the coefficients of V is contained in a cyclotomic field, or equivalently by the Kronecker-Weber Theorem, if the normal closure of K' has abelian Galois group. Theorem 1.2 answers this question indirectly in the affirmative. This result was expected since V encodes information about the Frobenius endomorphism at all (unramified) primes by p-adic estimation given in eq. (1.5). The rationality of V then should imply a lot of regularity among the Frobenius elements at different primes which should only be possible if the underlying Galois elements commute. However, this is not how the proof of Theorem 1.2 works.

The proof of Theorem 1.2 examines the poles of V, which a priori do not need to be roots of unity, see Example 2.11 (1) for a counterexample where $s = 1$. The first reduction is given by Theorem 3.2 which is an adapted version of a theorem due to Minton (cf. [30]).

In its original form, this theorem states that the generating functions of Euler sequences are given by sums of logarithmic derivatives of polynomials with rational coefficients. The analogous statement for an 1-sequence $(a_n)_n$ then implies that V has only poles of order 1 with rational residues. What is left to show is that those (analytic) poles lie in roots of unity using the (algebraic) supercongruence condition eq. (1.5) for $s = 2$.

1.2 Framing of Rational 2-Functions and Wolstenholme Type Congruences

One of the most interesting observations concerning 2-functions in particular is that these functions permit a certain algebraic transformation (of formal power series) called *framing*. Formally, framing to the parameter $\nu \in \mathbb{Z}$ can be characterized by a functional equation. Let $V \in zK[\![z]\!]$ be a power series, then the ν-framing $V^{(-,\nu)} \in zK[\![z]\!]$ (the additional minus sign refers to a sign convention explained later) of V gives a power series satisfying the functional equation

$$\int V^{(-,\nu)}\left(z\left(-\exp(-\int V(z))^{\nu}\right)\right) = \int V(z). \tag{1.10}$$

(Here, the symbol $\int$ refers to a formal integration of power series.) These framing transformations appear in the context of open topological string theory, see [1], where the name has been coined. In [35], it was expected that for an appropriate choice of parametrization, the coefficients of the Lambert expansion eq. (1.4), the coefficients (b_n) are counting dimensions of spaces of BPS states, hence $(b_n)_n \in \mathbb{Z}^{\mathbb{N}}$. In this setting, the superpotential (and its BPS invariants) depend on the integer parameter $\nu \in \mathbb{Z}$, called "*the framing*". Framing therefore results from an ambiguity in the identification of the open string modulus. The main result in [40], due to Schwarz, Vologodsky and Walcher, is the *Integrality of Framing Theorem* that states that the framing operator preserves 2-functions (also for more general algebraic coefficients) and defines a group action of $\mathbb{Z}$ on the set of 2-functions.

Theorem 1.3 (Integrality of Framing Theorem, [40]) *Let $V \in zK[\![z]\!]$ be the generating function of a 2-sequence and let $V^{(-,\nu)} \in zK[\![z]\!]$ its framing to the framing number $\nu \in \mathbb{Z}$. Then the sequence of coefficients $(a_n^-)_{n\in\mathbb{N}}$ of $V^{(-,\nu)}$ is a 2-sequence.*

There seems to be a subclass of 2-functions ($s \geq 2$) whose framings integrate to 3-functions. For instance, this behavior has been observed in [15] by the (extremal) BPS invariants of twist knots and has been referred therein as an "improved integrality". These 3-functions appear as solutions of so-called extremal A-polynomials of these knots, and all their framings are expected to be also 3-functions, or at least can be lifted to

3-functions by multiplying with an appropriate constant ([15, Conj. 1.3]). This improved integrality, however, does not hold in general. It would be interesting to give a physical interpretation of this property.

As a second task of the present work and as an attempt to tackle Conj. 1.3 in [15], the author tried to identify the subclass of those 2-sequences, such that all framings of the corresponding generating functions integrate to 3-functions. The result is given below by Theorem 1.4. Let $V^{(+,\nu)}(z) := V^{(-,\nu)}((-1)^\nu z) \in zK[\![z]\!]$. This sign convention for $V^{(+,\nu)}$ is for simplifying some notations and calculations since it does not affect the congruence condition eq. (1.5) for the coefficients of $V^{(+,\nu)}$, except for $p = 2$.

Theorem 1.4 *Let $V \in zK[\![z]\!] \setminus \{0\}$ be the generating series of a 2-sequence $(a_n)_{n\in\mathbb{N}}$ representing a rational function as its Maclaurin expansion, and let $\nu \in \mathbb{Z}$. Write $a_n^+ = [V^{(+,\nu)}(z)]_n$ be the n-th coefficient of $V^{(+,\nu)}$ for all $n \in \mathbb{N}$. Then, for almost all primes $p \geq 5$, which are unramified in $K|\mathbb{Q}$, and any prime ideal $\mathfrak{p}$ dividing p, we find for all $m, r \in \mathbb{N}$,*

$$\mathrm{Frob}_\mathfrak{p}\left(a^+_{mp^{r-1}}\right) - a^+_{mp^r} \equiv 0 \mod p^{3r}\mathcal{O}_\mathfrak{p}.$$

Note, that this result was only possible after establishing Theorem 1.2. Let us give a summary of the proof for Theorem 1.4 for $\nu = 1$. From the Integrality of Framing Theorem we directly obtain that

$$\frac{2}{p^2n^2} \cdot \left(\mathrm{Frob}_\mathfrak{p}\left(a_n^+\right) - a_{pn}^+\right), \tag{1.11}$$

is a p-adic integer, that is a $\mathfrak{p}$-adic integer for all $\mathfrak{p} \mid (p)$ in $\mathcal{O}$. Assuming rationality of V we then find for all but finitely many p

$$\frac{2}{p^2n^2} \cdot \left(\mathrm{Frob}_\mathfrak{p}\left(a_n^+\right) - a_{pn}^+\right) \equiv \sum_{m=0}^{n} \left(\tilde{y}_{n,m,p} \sum_{\substack{\ell=1 \\ p\nmid\ell}}^{p(n-m)} \frac{a_{p(n-m)-\ell}a_\ell}{\ell^2} \right) \mod p^{\mathrm{ord}_p(pn)-\delta_{3,p}}\mathcal{O}_\mathfrak{p}, \tag{1.12}$$

where $\tilde{y}_{n,m,p}$ are certain p-adic integers in $\mathcal{O}$. The sum appearing in the big bracket of eq. (1.12), namely

$$\sum_{\substack{\ell=1 \\ p\nmid\ell}}^{p(n-m)} \frac{a_{p(n-m)-\ell}a_\ell}{\ell^2}, \tag{1.13}$$

should be interpreted as a weighted harmonic sum, weighted by a convolution of the 2-

sequence $(a_n)_n$ with itself. At the same time, many supercongruences are known among the binomial coefficients, for instance the Jacobsthal-Kazandzidis congruence mentioned above, which is typically proven by using sharp p-adic estimations of harmonic sums. This kind of p-adic estimations are often referred to as Wolstenholme type congruences, see also Wolstenholme's Theorem (for instance [29]). This connection led to the following generalization of Wolstenholme's Theorem, handling the sum (1.13).

Theorem 1.5 *Let p be an unramified prime in $K|\mathbb{Q}$ and $\mathfrak{p} \subset \mathcal{O}$ be a prime ideal dividing (p). Let $(a_k)_{k\in\mathbb{N}} \in \mathcal{O}_{\mathfrak{p}}^{\mathbb{N}}$ be a periodic sequence of periodicity N, i.e. $N \in \mathbb{N}$ is given by*

$$N = \min\{i \in \mathbb{N} \,|\, a_{k+i} = a_k \text{ for all } n \in \mathbb{N}\}.$$

Then, for all $n \in \mathbb{N}$,

$$\sum_{\substack{k=1 \\ p\nmid k}}^{n} \frac{a_{n-k}a_k}{k^2} \equiv 0 \mod p^{\max\{0,\mathrm{ord}_p(n)-\varepsilon_{p,N}\}}\mathcal{O}_{\mathfrak{p}},$$

where

$$\varepsilon_{p,N} = \begin{cases} \max\{\mathrm{ord}_2(N), \mathrm{ord}_2(N+2)\}, & \text{if } p = 2 \text{ and } 2 \mid N, \\ 1 + \mathrm{ord}_2(N+1), & \text{if } p = 2 \text{ and } 2 \nmid N, \\ 1 + \mathrm{ord}_3(N), & \text{if } p = 3, \\ \mathrm{ord}_p(N), & \text{if } p \geq 5. \end{cases}$$

Finally, $\tilde{y}_{n,m,p}$ contributes exactly the remaining p-divisibility to obtain Theorem 1.4. This contribution can be considered as an auxiliary to Dwork's Integrality Lemma, see [27, Ch. 14] for the classical formulation. In the setting of s-functions it is given by the following statement. Let $V \in zK[\![z]\!]$ and let $Y \in 1 + zK[\![z]\!]$ be related by $Y(z) = \exp(\int V(z))$. Then V is the generating series of an 1-sequence if and only if Y has integral coefficients at all unramified prime ideals $\mathfrak{p} \subset \mathcal{O}$. Dwork himself used his lemma (stated for $K = \mathbb{Q}$) as a key step to prove his theorem that for an affine hypersurface H over a finite field $\mathbb{F}_q$ the zeta-function $Z(H;X)$ of H in the variable X is a rational function and its logarithmic derivative $\dfrac{Z'(H;X)}{Z(H;X)}$ is the generating function of the non-negative numbers $(N_n)_{n\in\mathbb{N}}$ of $\mathbb{F}_{q^n}$-points of H, i.e. $N_n = |H(\mathbb{F}_{q^n})|$. To us, however, this estimation is not sufficient. What we need is the following statement.

Proposition 1.6 *Let $V \in zK[\![z]\!]$ be the generating series of an 1-sequence and let p be an unramified prime in $K|\mathbb{Q}$. Then for all $n, m \in \mathbb{N}$ with $\mathrm{ord}_p(n) \geq \mathrm{ord}_p(m)$, we find the*

following $\mathfrak{p}$*-adic estimation for the* m*-th coefficient* $\tilde{y}_m$ *of the function* $\exp\left(n \int V(z)\right)$

$$\tilde{y}_m \equiv 0 \mod p^{\mathrm{ord}_p(n)-\mathrm{ord}_p(m)}\mathcal{O}_{\mathfrak{p}}. \tag{1.14}$$

In simple words, we may now say that Theorem 1.4 follows from

$$\underbrace{\mathrm{ord}_p(m-n)}_{Theorem\ 1.5} + \underbrace{\min\{0, \mathrm{ord}_p(n) - \mathrm{ord}_p(m)\}}_{Proposition\ 1.6} \geq \mathrm{ord}_p(n).$$

Theorem 1.4 is a generalization of the Jacobsthal-Kazandzidis congruence. Also the proof of the latter served as a source of inspiration to the author in the process of finding the proof of Theorem 1.4.

1.3 Integrality Statements for Fractional Framing

The Jacobsthal-Kazandzidis congruence does not follow from Theorem 1.4, yet! For this we give an extension of Theorem 1.4 and also of the Integrality of Framing Theorem, where we allow the framing number ν to be a rational number in the following manner. For a power series $\sum_{n=0}^{\infty} x_n z^n \in K[\![z]\!]$ and a natural number $\ell \in \mathbb{N}$ the *Cartier operator* $\mathscr{C}_\ell$ is given by

$$\mathscr{C}_\ell\left(\sum_{n=0}^{\infty} x_n z^n\right) = \sum_{n=0}^{\infty} x_{\ell n} z^n.$$

Then *fractional framing* refers to power series obtained by $\frac{1}{\sigma}\mathscr{C}_\sigma V^{(+/-,\nu)}$, where $V \in zK[\![z]\!]$, $\nu \in \mathbb{Q}$ and $\sigma \in \mathbb{N}$.

Theorem 1.7 *Let* $\sigma \in \mathbb{N}$ *and* $\nu \in \frac{1}{\sigma}\mathbb{Z}$.

(1) *Integrality of Fractional Framing: Let* $V \in zK[\![z]\!]$ *be the generating series of a 2-sequence. Then*

$$\frac{1}{\sigma}\mathscr{C}_\sigma V^{(-,\nu)}$$

is the generating series of a 2-sequence.

(2) *Improved Integrality of Fractional Framing: Let* $V \in zK[\![z]\!]$ *be the generating series of a 2-sequence representing a rational function as its Maclaurin expansion. Let* $\tilde{a}_n^+$ *denote the* n*-th coefficient of* $\frac{1}{\sigma}\mathscr{C}_\sigma V^{(+,\nu)}(z)$. *Then for almost all unramified* $p \geq 5$

in $K|\mathbb{Q}$*, and all* $m, r \in \mathbb{N}$*,*

$$\mathrm{Frob}_{\mathfrak{p}}\left(\tilde{a}^{+}_{mp^{r-1}}\right) - \tilde{a}^{+}_{mp^{r}} \equiv 0 \mod p^{3r}\mathcal{O}_{\mathfrak{p}}.$$

The proofs of these statements go analogously to the non-fractional case. Since $\mathscr{C}_1$ is the identity, the non-fractional cases follow from Theorem 1.7. The Jacobsthal-Kazandzidis congruence then is a special case of Theorem 1.7 (2) by taking $a_n = 1$ for all $n \in \mathbb{N}$, that is, taking $V(z) = \dfrac{z}{1-z}$, and varying appropriate σ and ν.

1.4 Overview

In Chapter 2, we will give the basic definitions involving s-sequences and s-functions, give some equivalent characterizations of s-functions by their Lambert extension. Then we continue by stating Dwork's Integrality Lemma in the setting of 1-functions and give a proof. This fits nicely in the context, since it has its contribution in the proof of Theorem 1.4 and furthermore, it is needed to prove Proposition 1.6. Finally, we collect some algebraic properties of the set of s-functions.

Chapter 3 is dedicated to prove and discuss Theorem 1.2. We first give a proof of Minton's Theorem in the setting of rational 1-functions, following a proof due to Beukers, Houben and Straub in [7]. Theorem 1.2 then permits us to give a (Hamel) basis of 2-realizable sequences (these are 2-sequences in $\mathbb{Q}^{\mathbb{N}}$), whose generating series are given by rational functions in $\mathbb{Q}(z)$. These are precisely the logarithmic derivatives of cycolotomic polynomials, $\dfrac{nz\Phi_n'(z)}{\Phi_n(z)}$ for $n \in \mathbb{N}$, compare with Proposition 2.14 and Theorem 3.18.

In Chapter 4, we introduce framing of power series by defining it in terms of Bell transformations, which are studied in [9]. Therefore, framing will be introduced independently of the geometric setting. We give the proof of the Integrality of Framing Theorem as a starting point for the proof of Theorem 1.4. Section 4.3 is dedicated to Theorem 1.5 and to give a short survey of Wolstenholme's Theorem (compare Theorem 4.14). We also give a proof of the Jacobsthal-Kazandzidis congruence, which can be considered as some prototype version of the proof of Theorem 1.4.

Notation

Throughout this work, the natural numbers will be meant to be the set of all positive integers, $\mathbb{N} = \{1, 2, ...\}$, while $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. If X is a set, then $X^{\mathbb{N}}$ denotes the set of all sequences indexed by the natural numbers, $(x_n)_{n\in\mathbb{N}} \in X^{\mathbb{N}}$. For a ring R let $R[\![z]\!]$ denote the ring of formal power series in the variable z with coefficients in R.

Chapter 2

Preliminaries

In the present section we introduce the definitions and notational conventions that will be used throughout this work. We mainly follow the conventions given in [40].

2.1 Basics

Let K be a fixed algebraic number field and we assume K to be normal over $\mathbb{Q}$. Denote by $\mathcal{O}$ the ring of integers of K. Let D be the discriminant of $K|\mathbb{Q}$. We say that a prime $p \in \mathbb{Z}$ is unramified in $K|\mathbb{Q}$, if all prime ideals $\mathfrak{p} \mid p\mathcal{O}$ are unramified. Note that an unramified prime p is characterized by the property that $p \nmid D$. For any prime ideal $\mathfrak{p}$, $\mathcal{O}_\mathfrak{p}$ denotes the ring of $\mathfrak{p}$-adic integers. Then $\mathcal{O}_\mathfrak{p}$ is an integral domain and its field of fractions $K_\mathfrak{p} = \mathrm{Quot}(\mathcal{O}_\mathfrak{p})$ is the $\mathfrak{p}$-adic completion of K.

Definition 2.1 (The rings $\mathcal{O}_p$ and K_p) For an unramified prime p, we set $\mathcal{O}_p$ to be given by

$$\mathcal{O}_p = \prod_{\mathfrak{p}|(p)} \mathcal{O}_\mathfrak{p}.$$

Analogously,

$$K_p = \prod_{\mathfrak{p}|(p)} K_\mathfrak{p}.$$

Multiplication is realized by component-wise multiplication, that is, for $(x_\mathfrak{p})_{\mathfrak{p}|(p)}$ and $(y_\mathfrak{p})_{\mathfrak{p}|(p)} \in \mathcal{O}_p$ (resp. K_p) we have $(x_\mathfrak{p})_{\mathfrak{p}|(p)} \cdot (y_\mathfrak{p})_{\mathfrak{p}|(p)} = (x_\mathfrak{p} \cdot y_\mathfrak{p})_{\mathfrak{p}|(p)} \in \mathcal{O}_p$ (K_p resp.). Therefore, K_p is a K-algebra.

Let $\iota_\mathfrak{p} \colon K \hookrightarrow K_\mathfrak{p}$ be the canonical embedding of K into its $\mathfrak{p}$-adic completion, then K

is embedded in K_p by the map $\iota_p\colon K \hookrightarrow K_p$, $x \mapsto (\iota_{\mathfrak{p}}(x))_{\mathfrak{p}|(p)}$. Nonetheless, if it is clear from the context, we will use the same symbol x for $\iota_p(x)$ or $\iota_{\mathfrak{p}}(x)$, whenever $x \in K$. We say that $x \in K$ is a *p-adic integer* (*p-adic unit* resp.), if $x \in \mathcal{O}_{\mathfrak{p}}$ ($x \in \mathcal{O}_{\mathfrak{p}}^{\times}$ resp.) with respect to all prime ideals $\mathfrak{p} \mid (p)$.

$\iota_{\mathfrak{p}}$ (ι_p resp.) can be extended to the ring of formal power series $K_{\mathfrak{p}}[\![z]\!]$ ($K_p[\![z]\!]$ resp.) by setting $\iota_{\mathfrak{p}}(z) = z$ and $\iota_p(z) = z$ and linear extending to maps $\iota_{\mathfrak{p}}\colon K[\![z]\!] \hookrightarrow K_{\mathfrak{p}}[\![z]\!]$ and $\iota_p\colon K[\![z]\!] \hookrightarrow K_p[\![z]\!]$. Again, for $V \in K[\![z]\!]$, we will use the same symbol V to refer to the power series $\iota_{\mathfrak{p}}(V) \in K_{\mathfrak{p}}[\![z]\!]$ and $\iota_p(V) \in K_p[\![z]\!]$. We denote by $\mathrm{ord}_{\mathfrak{p}}\colon \mathcal{O}_{\mathfrak{p}} \to \mathbb{N}_0$ the p-adic order. Furthermore,

$$\mathrm{Ord}_p\colon \mathcal{O}_p \to \mathbb{N}_0, \quad (x_{\mathfrak{p}})_{\mathfrak{p}|(p)} \mapsto \min\{\mathrm{ord}_{\mathfrak{p}}(x_{\mathfrak{p}}) \mid \mathfrak{p} \mid (p)\}.$$

For $\mathfrak{p} \mid (p)$, the *Frobenius element* $\mathrm{Fr}_{\mathfrak{p}}$ at $\mathfrak{p}$ is the unique element satisfying the following two conditions: $\mathrm{Fr}_{\mathfrak{p}}$ is an element in the decomposition group $D(\mathfrak{p}) \subset \mathrm{Gal}(K|\mathbb{Q})$ of $\mathfrak{p}$ and for all $x \in \mathcal{O}$, $\mathrm{Fr}_{\mathfrak{p}}(x) \equiv x^p \mod \mathfrak{p}$. By Hensel's Lemma, $\mathrm{Fr}_{\mathfrak{p}}$ can be lifted to $\mathcal{O}_{\mathfrak{p}}$ and then extended to an automorphism $\mathrm{Frob}_{\mathfrak{p}}\colon K_{\mathfrak{p}} \to K_{\mathfrak{p}}$.

Definition 2.2 (The Frob_p map) Let $p \in \mathbb{Z}$ be a prime, unramified in $K|\mathbb{Q}$. Then $\mathrm{Frob}_p\colon K_p \to K_p$ is defined by

$$K_p \ni \mathbf{x} = (x_{\mathfrak{p}})_{\mathfrak{p}|(p)} \mapsto \mathrm{Frob}_p(\mathbf{x}) := (\mathrm{Frob}_{\mathfrak{p}}(x_{\mathfrak{p}})).$$

By declaring $\mathrm{Frob}_p(z) = z$, Frob_p can be (linearly) extended to an endomorphism $\mathrm{Frob}_p\colon K_p[\![z]\!] \to K_p[\![z]\!]$. Note that in contrast to [40], where $\mathrm{Frob}_p(z) = z^p$, we decided to set $\mathrm{Frob}_p(z) = z$ to have more flexibility using this notation.

In the following, let R be a $\mathbb{Q}$-algebra. Let $R(\!(z)\!)$ denote the ring of formal Laurent series.

Definition 2.3 (Euler derivative, integration, the Cartier operator and ε_ℓ) The *Euler operator* $\delta_R\colon R(\!(z)\!) \to R(\!(z)\!)$ is given by $z\dfrac{\mathrm{d}}{\mathrm{d}z}$, i.e.

$$\delta_R\left[\sum_{n=-\infty}^{\infty} r_n z^n\right] = \sum_{n=-\infty}^{\infty} n r_n z^n.$$

Its (partial) inverse of δ_R is the *logarithmic integration* $\int_R\colon zR[\![z]\!] \oplus z^{-1}R\left[\!\left[z^{-1}\right]\!\right] \to zR[\![z]\!] \oplus z^{-1}R\left[\!\left[z^{-1}\right]\!\right]$ given by

$$\textstyle\int_R\left[\sum_{n=-\infty}^{\infty} r_n z^n\right] = \sum_{n=-\infty}^{\infty} \frac{r_n}{n} z^n \qquad \text{and} \qquad \int_R(0) = 0.$$

For a number $k \in \mathbb{N}$ let $\mathscr{C}_{R,k}$ be the operator $\mathscr{C}_{R,k}\colon R(\!(z)\!) \to R(\!(z)\!)$, called the *Cartier operator*, given by

$$\mathscr{C}_{R,k}\left[\sum_{n=-\infty}^{\infty} r_n z^n\right] = \sum_{n=-\infty}^{\infty} r_{kn} z^n.$$

For a number $\ell \in \mathbb{N}$, let $\varepsilon_{R,\ell}\colon R(\!(z)\!) \to R(\!(z)\!)$ be the R-algebra homomorphism uniquely determined by setting

$$\varepsilon_{R,\ell}(z) = z^\ell.$$

Hereafter, we will omit R from the notation of δ_R, $\int_R$, $\mathscr{C}_{R,k}$ and $\varepsilon_{R,\ell}$.

Definition 2.4 (Extracting coefficients) Let $n \in \mathbb{Z}$ be an integer. Let $[-]_n$ denote the R-functional $[-]_n\colon R(\!(z)\!) \to R$, uniquely determined by

$$\left[z^k\right]_n = \delta_{n,k} = \begin{cases} 0, & \text{if } n = k, \\ 1, & \text{if } n \neq k, \end{cases}$$

where $\delta_{n,k}$ denotes the *Kronecker symbol*. In other words, $[-]_n$ extracts the n-th coefficient of a Laurent series.

Remark 2.5 Obviously, for any $V \in R(\!(z)\!)$ and $n \in \mathbb{Z}$, we have

$$[\delta V(z)]_n = n \cdot [V(z)]_n . \tag{2.1}$$

In particular, for $n = 0$ we obtain a formula for *integrating by parts*: Let $F, G \in R(\!(z)\!)$, then

$$0 = [\delta(F(z) \cdot G(z))]_0 = [G(z) \cdot \delta F(z) + F(z) \cdot \delta G(z)]_0$$

and therefore

$$[G(z) \cdot \delta F(z)]_0 = -[F(z) \cdot \delta G(z)]_0 . \tag{2.2}$$

Analogously, if $[F(z)]_0 = 0$ and $n \neq 0$, then

$$[\textstyle\int F(z)]_n = \frac{1}{n}[F(z)]_n \quad \text{and} \quad [\textstyle\int F(z)]_0 = 0. \tag{2.3}$$

Terminology 2.6 (rational/algebraic/D-finite power series) Let K be a field. We will call a (formal) power series $V(z) \in K[\![z]\!]$:

- *rational*, if V is the Maclaurin expansion of a rational function $F \in K(z)$.
- *algebraic*, if V is the Maclaurin expansion of a function $F \in \mathcal{K}$, where $\mathcal{K}$ is an algebraic extension of $K(z)$, $\mathcal{K}|K(z)$.
- *D-finite*, if all (formal) derivatives of V,

$$\left(\frac{\mathrm{d}}{\mathrm{d}z}\right)^n V(z), \quad \text{for } n \in \mathbb{N},$$

span a finite dimensional vector space over $K(z)$.

We will use the symbols 'rat', 'alg', 'D-fin' as acronyms to rational, algebraic, D-finite, respectively. The following implications hold

$$\text{rational} \Rightarrow \text{algebraic} \Rightarrow \text{D-finite}, \tag{2.4}$$

where the last implication is precisely the statement of a theorem due to Stanley in [42], see also Theorem 3.5.

2.2 s-Functions, s-Sequences and Polylogarithms

In the present section we give the basic definitions of s-sequences, s-functions and give some further characterizations of s-functions (cf. Proposition 2.10).

Definition 2.7 (s-function with algebraic coefficients) In [40], an *s-function with coefficients in K* (for $s \in \mathbb{N}$) is defined to be a formal power series $V \in zK[\![z]\!]$ such that for every unramified prime $p \in \mathbb{Z}$ in $K|\mathbb{Q}$ we have

$$\frac{1}{p^s}\mathrm{Frob}_p V(z^p) - V(z) \in z\mathcal{O}_p[\![z]\!]. \tag{2.5}$$

In the following, we will identify s-functions with s-sequences.

Definition 2.8 (s-sequence) A sequence $(a_n)_{n\in\mathbb{N}} \in K^{\mathbb{N}}$ is said to satisfy the *local s-function property for p*, if $p \in \mathbb{Z}$ is unramified in $K|\mathbb{Q}$, and $a_n \in \mathcal{O}_p$ is a p-adic integer for all $n \in \mathbb{N}$, and

$$\mathrm{Frob}_p\left(a_{mp^{r-1}}\right) \equiv a_{mp^r} \mod p^{sr}\mathcal{O}_p, \tag{2.6}$$

for all $m, r \in \mathbb{N}$. $(a_n)_{n\in\mathbb{N}}$ is called an *s-sequence* if it satisfies the local s-function property for all unramified primes p in $K|\mathbb{Q}$.

From the above definition of an s-sequence $a \in K^{\mathbb{N}}$, it is evident that $a \in \mathcal{O}\left[D^{-1}\right]^{\mathbb{N}}$.

Definition 2.9 ($\mathcal{S}^s(K|\mathbb{Q})$) We denote by $\mathcal{S}^s(K|\mathbb{Q}) \subset z\mathcal{O}\left[D^{-1}\right][\![z]\!]$ the set of all generating functions of s-sequences with coefficients in K

$$\mathcal{S}^s(K|\mathbb{Q}) := \left\{ V \in z\mathcal{O}\left[D^{-1}\right][\![z]\!];\, V = \sum_{n=1}^{\infty} a_n z^n, \text{ where } (a_n)_{n\in\mathbb{N}} \text{ is an } s\text{-sequence} \right\}.$$

Furthermore, $\overline{\mathcal{S}}^s(K|\mathbb{Q}) \subset zK[\![z]\!]$ denote the set of formal power series which differ from being an element in $\mathcal{S}^s(K|\mathbb{Q})$ by a rational constant, i.e.

$$\overline{\mathcal{S}}^s(K|\mathbb{Q}) := \{V \in zK[\![z]\!];\, \text{there is a constant } C \in \mathbb{N}, \text{ such that } CV(z) \in \mathcal{S}^s(K|\mathbb{Q})\}.$$

Originally (compare [40]), an s-function $\int^s V \in zK[\![z]\!]$ was called *algebraic* if $Y(z) := \exp(-\int V)$ is the Maclaurin series expansion of an algebraic function. Consequently, a rational s-function should be an s-function $\int^s V(z)$ such that Y is the Maclaurin expansion of a rational function. However, in the present work, this terminology has been changed as we see immediately. This change becomes clear in the presence of Corollary 3.3, Proposition 3.4 and Theorem 3.7 below.

We denote by $\mathcal{S}^s_{\mathcal{P}}(K|\mathbb{Q})$ ($\overline{\mathcal{S}}^s_{\mathcal{P}}(K|\mathbb{Q})$, resp.) the subset in $\mathcal{S}^s(K|\mathbb{Q})$ ($\overline{\mathcal{S}}^s(K|\mathbb{Q})$, resp.) of elements with the respect property $\mathcal{P}$, where $\mathcal{P} \in \{$'rat', 'alg', 'D-fin'$\}$, compare Terminology 2.6. Let S be a finite set consisting of prime numbers, then

$$\mathcal{S}^s(K|\mathbb{Q})_S := \left\{ V \in z\mathcal{O}\left[D^{-1}, q^{-1}; q \in S\right][\![z]\!];\, V = \sum_{n=1}^{\infty} a_n z^n, \text{ where } (a_n)_{n\in\mathbb{N}} \text{ satisfies the local } s\text{-function property for all unramified } p \notin S \right\}.$$

Also,

$$\mathcal{S}^s(K|\mathbb{Q})_{\text{fin}} = \bigcup_S \mathcal{S}^s(K|\mathbb{Q})_S,$$

where S runs through all finite subsets of rational primes. Analogously, the sets $\overline{\mathcal{S}}^s(K|\mathbb{Q})_S$ and $\overline{\mathcal{S}}^s(K|\mathbb{Q})_{\text{fin}}$ are defined. Naturally, we obtain the sequence

$$\mathcal{S}^1(K|\mathbb{Q}) \supset \mathcal{S}^2(K|\mathbb{Q}) \supset \mathcal{S}^3(K|\mathbb{Q}) \supset \cdots \supset \mathcal{S}^{s-1}(K|\mathbb{Q}) \supset \mathcal{S}^s(K|\mathbb{Q}) \supset \mathcal{S}^{s+1}(K|\mathbb{Q}) \supset \cdots \tag{2.7}$$

Therefore, we may define

$$\mathcal{S}^{\infty}(K|\mathbb{Q}) := \bigcap_{s=1}^{\infty} \mathcal{S}^{s}(K|\mathbb{Q}).$$

Note that $\overline{\mathcal{S}}^{s}(K|\mathbb{Q})$ is a vector space over $\mathbb{Q}$, with $\mathbb{Q}$-subspaces

$$\overline{\mathcal{S}}^{s}_{\mathrm{rat}}(K|\mathbb{Q}) \subset \overline{\mathcal{S}}^{s}_{\mathrm{alg}}(K|\mathbb{Q}) \subset \overline{\mathcal{S}}^{s}_{\text{D-fin}}(K|\mathbb{Q}) \subset \overline{\mathcal{S}}^{s}(K|\mathbb{Q}),$$

by eq. (2.4). Definition 2.7 and Definition 2.8 are equivalent as shown in Lemma 4 in [40]. This equivalence is stated as the equivalence of *(i)* and *(ii)* in the following . Also, *(iii)* and *(iv)* give a characterization of s-functions by formal linear sums of the polylogarithm Li_s, where the sequences $(b_n)_{n\in\mathbb{N}}$ and $(q_n)_{n\in\mathbb{N}}$ satisfy some integrality conditions.

Proposition 2.10 *Let $s \in \mathbb{N}$. Then the following is equivalent:*

(i) $V \in \mathcal{S}^{s}(K|\mathbb{Q})$,

(ii) $\int^{s} V$ *is an s-function,*

(iii) for all unramified primes p in $K|\mathbb{Q}$ and all $r \in \mathbb{N}$,

$$\begin{aligned} \mathscr{C}_p^{r-1}\left(\mathrm{Frob}_p V(z) - \mathscr{C}_p V(z)\right) &\equiv 0 \mod p^{sr}\mathcal{O}_p[\![z]\!], \quad \text{and} \\ V(z) - \varepsilon_p \mathscr{C}_p V(z) &\in z\mathcal{O}_p[\![z]\!]. \end{aligned} \tag{2.8}$$

(iv) There is a sequence $b \in K^{\mathbb{N}}$ satisfying

$$\sum_{i=1}^{\mathrm{ord}_p(n)} \frac{\mathrm{Frob}_p(b_{n/p^i}) - b_{n/p^i}}{p^{si}} - b_n \in \mathcal{O}_p$$

for all $n \in \mathbb{N}$ and unramified p in $K|\mathbb{Q}$, such that $\int^{s} V(z)$ can be represented as a formal sum of polylogarithms in the following way

$$\int^{s}(V(z)) = \sum_{n=1}^{\infty} b_n \,\mathrm{Li}_s(z^n). \tag{2.9}$$

(v) There is a sequence $q \in \mathcal{O}\left[D^{-1}\right]^{\mathbb{N}}$ satisfying

$$\sum_{d|n} \frac{\mathrm{Frob}_p\left(q_{n/d}^{d}\right) - q_{n/d}^{pd}}{d} - p\sum_{\substack{d|n \\ p\nmid d}} \frac{q_{n/d}^{d}}{d} \equiv 0 \mod p^{(s-1)\,\mathrm{ord}_p(n)+s}\mathcal{O}_p$$

for all $n \in \mathbb{N}$ and unramified p in $K|\mathbb{Q}$, such that $\int^s V(z)$ can be represented as a formal sum of polylogarithms in the following way

$$\int^s V(z) = \sum_{d=1}^{\infty} \frac{1}{d^{s-1}} \operatorname{Li}_s(q_d z^d) \tag{2.10}$$

Proof. Write $a_n := [V(z)]_n$ for all $n \in \mathbb{N}$.

(i) $\Leftrightarrow$ (ii): Compute

$$\begin{aligned}\frac{1}{p^s}\operatorname{Frob}_p \int^s V(z^p) - \int^s V(z) &= \frac{1}{p^s}\sum_{n=1}^{\infty} \frac{\operatorname{Frob}_p(a_n)}{n^s} z^{pn} - \sum_{n=1}^{\infty} \frac{a_n}{n^s} z^n \\ &= -\sum_{\substack{n=1 \\ p\nmid n}}^{\infty} \frac{a_n}{n^s} z^n + \sum_{n=1}^{\infty} \frac{\operatorname{Frob}_p(a_n) - a_{pn}}{p^s n^s} z^{pn}\end{aligned}$$

Note, that the p-adic integrality of the first sum is not disturbed by the denominators n^s, since their p-adic order is 0. Therefore, the equivalence $V \in \mathcal{S}^s(K|\mathbb{Q})$ if and only if $\int^s V(z)$ follows immediately.

(i) $\Leftrightarrow$ (iii): Let p be unramified in $K|\mathbb{Q}$ and $r \in \mathbb{N}$. Then

$$\begin{aligned}\mathscr{C}_p^{r-1}\left(\operatorname{Frob}_p V(z) - \mathscr{C}_p V(z)\right) &= \mathscr{C}_p^{r-1}\left(\sum_{n=1}^{\infty} (\operatorname{Frob}_p(a_n) - a_{pn}) z^n\right) \\ &= \sum_{n=1}^{\infty} \left(\operatorname{Frob}_p\left(a_{p^{r-1}n}\right) - a_{p^r n}\right) z^n,\end{aligned}$$

and

$$V(z) - \varepsilon_p \mathscr{C}_p V(z) = \sum_{\substack{n=1 \\ p\nmid n}}^{\infty} a_n z^n.$$

The condition that $V - \varepsilon_p \mathscr{C}_p V \in \mathcal{O}_p[\![z]\!]$ is then equivalent to saying that every coefficient whose index is not a multiple of p is a p-adic integer, $a_n \in \mathcal{O}_p$ for all $p \nmid n$. Therefore, for all unramified primes p in $K|\mathbb{Q}$ and $r \in \mathbb{N}$,

$$\begin{gathered}\mathscr{C}_p^{r-1}\left(\operatorname{Frob}_p V(z) - \mathscr{C}_p V(z)\right) \equiv 0 \mod p^{sr} z\mathcal{O}_p[\![z]\!], \quad \text{and} \\ V(z) - \varepsilon_p \mathscr{C}_p V(z) \in z\mathcal{O}_p[\![z]\!]\end{gathered}$$

if and only if $V \in \mathcal{S}^s(K|\mathbb{Q})$.

(iv) $\Rightarrow$ *(i)*: Let $b \in K^{\mathbb{N}}$ such that

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} z^n = \sum_{n=1}^{\infty} b_n \operatorname{Li}_s(z^n).$$

By comparing coefficients, we can write equivalently for all $n \in \mathbb{N}$,

$$a_n = n^s \sum_{d|n} \frac{b_d}{(n/d)^s} = \sum_{d|n} d^s b_d.$$

Let us assume for all $n \in \mathbb{N}$ and all unramified primes p in $K|\mathbb{Q}$ that

$$\sum_{i=1}^{\operatorname{ord}_p(n)} \frac{\operatorname{Frob}_p(b_{n/p^i}) - b_{n/p^i}}{p^{si}} - b_n \in \mathcal{O}_p.$$

Write $n = mp^r$ for $m, r \in \mathbb{N}$ with $\gcd(p, m) = 1$ (i.e. $\operatorname{ord}_p(n) = r$). We then obtain

$$\begin{aligned}
\operatorname{Frob}_p(a_{mp^{r-1}}) - a_{mp^r} &= \sum_{d|n/p} d^s \operatorname{Frob}_p(b_d) - \sum_{d|n} d^s b_d \\
&= \sum_{i=0}^{r-1} \sum_{d|m} (dp^i)^s \operatorname{Frob}_p(b_{dp^i}) - \sum_{i=0}^{r} \sum_{d|m} (dp^i)^s b_{dp^i} \\
&= p^{sr} \sum_{d|m} d^s \left(\sum_{i=0}^{r-1} p^{(i-r)s} \operatorname{Frob}_p(b_{dp^i}) - \sum_{i=0}^{r} p^{(i-r)s} b_{dp^i} \right) \\
&= p^{sr} \sum_{d|m} d^s \left(\sum_{i=0}^{r-1} p^{-i-1} \left(\operatorname{Frob}_p(b_{dp^{r-i-1}} - b_{dp^{r-i-1}} \right) - b_{dp^r} \right) \\
&= p^{sr} \sum_{d|m} d^s \underbrace{\left(\sum_{i=1}^{r} \frac{\operatorname{Frob}_p(b_{dp^{r-i}}) - b_{dp^{r-i}}}{p^{si}} - b_{dp^r} \right)}_{\in \mathcal{O}_p} \\
&\equiv 0 \mod p^{sr}\mathcal{O}_p.
\end{aligned}$$

Furthermore, if $r = 0$, the sum $\displaystyle\sum_{i=1}^{\operatorname{ord}_p(n)} \frac{\operatorname{Frob}_p(b_{n/p^i}) - b_{n/p^i}}{p^{si}}$ is the empty sum, i.e. equals to 0. Therefore, $b_n \in \mathcal{O}_p$ whenever $\operatorname{ord}_p(n) = 0$. Consequently, $a_n = \displaystyle\sum_{d|n} d^s b_d \in \mathcal{O}_p$ in that case.

(i) ⇒ (iv): By the *Möbius inversion formula* we have

$$b_n = \frac{1}{n^s} \sum_{d|n} \mu\left(\frac{n}{d}\right) a_d.$$

First assume $\mathrm{ord}_p(n) = 0$. Then b_n is the sum of p-adic integers and therefore, b_n is itself a p-adic integer. Now we may assume $\mathrm{ord}_p(n) > 0$. Again, write $n = mp^r$ for $m, r \in \mathbb{N}$ with $\gcd(m, p) = 1$ (i.e. $\mathrm{ord}_p(n) = r$). Recall that $\mu(k) \neq 0$ if and only if k is square-free, therefore,

$$b_n = \frac{1}{n^s} \sum_{d|n} \mu\left(\frac{n}{d}\right) a_d = \frac{1}{m^s p^{sr}} \sum_{d|m} \mu\left(\frac{m}{d}\right) (a_{dp^r} - a_{dp^{r-1}}). \tag{2.11}$$

Hence,

$$\begin{aligned}
&\sum_{i=1}^{r} \frac{\mathrm{Frob}_p(b_{n/p^i}) - b_{n/p^i}}{p^{si}} - b_n \\
&\quad = \frac{1}{m^s} \sum_{d|m} \mu\left(\frac{m}{d}\right) \frac{\mathrm{Frob}_p\left(\sum_{i=1}^{r} (a_{dp^{r-i}} - a_{dp^{r-i-1}})\right) - \sum_{i=0}^{r} (a_{dp^{r-i}} - a_{dp^{r-i-1}})}{p^{sr}} \\
&\quad = \frac{1}{m^s} \sum_{d|m} \mu\left(\frac{m}{d}\right) \frac{\mathrm{Frob}_p(a_{dp^{r-1}}) - a_{dp^r}}{p^{sr}}.
\end{aligned}$$

Assuming $V \in \mathcal{S}^s(K|\mathbb{Q})$ therefore implies

$$\sum_{i=1}^{r} \frac{\mathrm{Frob}_p(b_{n/p^i}) - b_{n/p^i}}{p^{si}} - b_n \in \mathcal{O}_p.$$

(i) ⇔ (v): Find a sequence $q \in K^{\mathbb{N}}$, such that

$$a_n = \sum_{d|n} \frac{n}{d} q_{n/d}^d.$$

Indeed, q_n can be defined recursively by

$$q_n = a_n - \sum_{\substack{d|n \\ d>1}} \frac{n}{d} q_{n/d}^d. \tag{2.12}$$

Therefore, $q \in \mathcal{O}\left[D^{-1}\right]^{\mathbb{N}}$ if and only if $a \in \mathcal{O}\left[D^{-1}\right]^{\mathbb{N}}$. We obtain

$$\int^s V(z) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} z^n = \sum_{n=1}^{\infty} \sum_{d|n} \frac{q_{n/d}^d}{n^{s-1} d} z^n.$$

By substitution $n \mapsto dm$ we obtain

$$\begin{aligned}
\int^s V(z) &= \sum_{m=1}^{\infty} \sum_{d=1}^{\infty} \frac{q_m^d}{(dm)^{s-1} d} z^{dm} \\
&= \sum_{m=1}^{\infty} \frac{1}{m^{s-1}} \sum_{d=1}^{\infty} \frac{q_m^d}{d^s} z^{dm} \\
&= \sum_{m=1}^{\infty} \frac{1}{m^{s-1}} \operatorname{Li}_s\left(q_m z^m\right).
\end{aligned}$$

Furthermore,

$$\begin{aligned}
\operatorname{Frob}_p(a_n) - a_{np} &= n \left[\sum_{d|n} \frac{\operatorname{Frob}_p\left(q_{k/d}^d\right)}{d} - p \sum_{d|np} \frac{q_{np/d}^d}{d} \right] \\
&= n \left[\sum_{d|n} \frac{\operatorname{Frob}_p\left(q_{n/d}^d\right) - q_{n/d}^{pd}}{d} - p \sum_{\substack{d|n \\ p \nmid d}} \frac{q_{n/d}^d}{d} \right].
\end{aligned}$$

Hence, $V \in \mathcal{S}^s(K|\mathbb{Q})$ if and only if

$$\sum_{d|n} \frac{\operatorname{Frob}_p\left(q_{n/d}^d\right) - q_{n/d}^{pd}}{d} - p \sum_{\substack{d|n \\ p \nmid d}} \frac{q_{n/d}^d}{d} \equiv 0 \mod p^{(s-1)\operatorname{ord}_p(n)+s} \mathcal{O}_p.$$

This completes the proof. □

Example 2.11 Note however, that the assumption for a power series $V \in \mathcal{S}^s(K|\mathbb{Q})$ being rational does *not* imply that the representations via the formal sums of polylogarithms eq. (2.9) and eq. (2.10) given in Proposition 2.10 *(iv)* and *(v)* are terminating. This is because these equations, eq. (2.9) and eq. (2.10), are only formally valid. However, it turns out that for rational coefficients, eq. (2.9) becomes finite, compare with Theorem 2.12 below. To illustrate this, we give the following examples.

(1) *We give an example of a rational* 1*-function with rational coefficients such that its representing formal sum given by eq.* (2.9) *does not terminate.*

Let $V \in \mathcal{S}^1_{\mathrm{rat}}(\mathbb{Q})$ be given by

$$V(z) = \frac{5z}{1-5z} = \sum_{k=1}^{\infty} 5^k z^k.$$

By Theorem 1.1 (Euler's Thm.) V does indeed satisfy the local 1-function condition for all prime numbers $p \in \mathbb{Z}$. Let us assume that the corresponding formal sum given in eq. (2.9) terminates for V, i.e. suppose there is a natural number $d \in \mathbb{N}$ and suitable integers $b_k \in \mathbb{Z}$, for $k \in \{1, ..., d\}$, such that

$$V(z) = \sum_{k=1}^{d} b_k \frac{z^k}{1-z^k}. \tag{2.13}$$

This would in particular imply that V has an analytic representative whose poles lie on the unit circle in the complex plane. However, V has in fact a pole in $z = \frac{1}{5}$, contradicting the finiteness condition. Indeed, writing $n = p^r$ with a prime p and $r \in \mathbb{N}$, we have by eq. (2.11)

$$b_{p^r} = 5^{p^{r-1}} \left(5^{p^{r-1}(p-1)} - 1\right).$$

In particular, $(b_n)_{n\in\mathbb{N}}$ does not vanish for n large.

(2) *Next, we give an example of a rational 2-function with algebraic coefficients, such that its representing formal sum given by eq.* (2.9) *does not terminate.*
Let $K = \mathbb{Q}(\zeta_7)$, where ζ_7 is a primitive 7-th root of unity, and let $V \in \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$ be given by

$$V(z) = \frac{\zeta_7 z}{1-\zeta_7 z} + \frac{\zeta_7^{-1} z}{1-\zeta_7^{-1} z} = \frac{(\zeta_7 + \zeta_7^{-1})z - 2z^2}{1-(\zeta_7+\zeta_7^{-1})z + z^2} =: \sum_{n=1}^{\infty} a_n z^n.$$

(Indeed, the underlying sequence $a_n = \zeta_7^n + \zeta_7^{-n}$ is a 2-sequence, since a Frobenius element acts on a root of unity by taking the p-power for the underlying prime p.) By Proposition 2.10 *(iv)*, there is a suitable sequence $b \in K^{\mathbb{N}}$, such that

$$b_n = \sum_{d|n} \mu\left(\frac{n}{d}\right) a_d \quad \text{and} \quad V(z) = \sum_{n=1}^{\infty} \frac{b_n z^n}{1-z^n}.$$

For $p \neq 7$ prime and by eq. (2.11) we find for $n = mp^r$, $m, r \in \mathbb{N}$ and $\gcd(m, p) = 1$,

$$b_{mp^r} = \sum_{d|m} \mu\left(\frac{m}{d}\right) \left(\zeta_7^{dp^r} + \zeta_7^{-dp^r} - \zeta_7^{dp^{r-1}} - \zeta_7^{-dp^{r-1}}\right).$$

Now, taking $m = 1$ and $p = 2$, we find for $r \in \mathbb{N}$,

$$b_{2^r} = \mu(1)\left(\zeta_7^{2^r} + \zeta_7^{-2^r} - \zeta_7^{2^{r-1}} - \zeta_7^{-2^{r-1}}\right)$$
$$= \begin{cases} \zeta_7^2 + \zeta_7^{-2} - 2, & \text{if } r \equiv 1 \mod 3, \\ \zeta_7^4 + \zeta_7^{-4} - \zeta_7^2 - \zeta_7^{-2}, & \text{if } r \equiv 2 \mod 3, \text{ and} \\ \zeta_7 + \zeta_7^{-1} - \zeta_7^4 - \zeta_7^{-4}, & \text{if } r \equiv 0 \mod 3. \end{cases}$$

In particular, the sequence $(b_n)_{n\in\mathbb{N}}$ does not vanish for n sufficiently large, although V was given by a rational function.

(3) *Interestingly, for rational* 2*-functions with rational coefficients, the corresponding representation via the formal sum given by eq.* (2.9) *does indeed terminate.*
The following statement was proposed by Wadim Zudilin, [49]. However, the proof relies on Theorem 1.2.

Theorem 2.12 *The power series $V \in z\mathbb{Z}[\![z]\!]$ is an element in $\mathcal{S}^2_{\mathrm{rat}}(\mathbb{Q})$ if and only if it can be represented as the finite sum*

$$V(z) = \sum_{k=1}^{N} k^2 b_k \frac{z^k}{1 - z^k},$$

with integral coefficients $b_k \in \mathbb{Z}$ for all $k \in \{1, ..., N\}$.

Proof. This is a direct consequence of Proposition 2.10, Proposition 2.14 and Theorem 3.18 below. □

The author is not aware of a direct proof of Theorem 2.12. Instead, it seems to be a consequence of Theorem 1.2. Also, since the finiteness depends on whether s is equal to 1 or greater than 1 (recall Example 2.11 (1)), it seems fairly necessary to examine the analytic singularities of such a rational 2-function. This was the initial idea for the proof of Theorem 1.2.

One (very natural) consequence of Theorem 1.2 is the following theorem, which we will prove in Chapter 3, Theorem 3.18 therein. For $d \in \mathbb{N}$ we denote by $\Phi_d(z) \in \mathbb{Z}[z]$ the d-th cyclotomic polynomial.

Theorem 2.13 *$\overline{\mathcal{S}}^2_{\mathrm{rat}}(\mathbb{Q})_{\mathrm{fin}}$ is an infinite dimensional vector space over $\mathbb{Q}$ with Hamel basis given by the set $\{\delta \log(\Phi_n) \,|\, n \in \mathbb{N}\}$ of logarithmic derivatives of all cyclotomic polynomials. However, for $R = \mathbb{Q}[\varepsilon_k;\, k \in \mathbb{N}]$, $\overline{\mathcal{S}}^2_{\mathrm{rat}}(\mathbb{Q})_{\mathrm{fin}}$ is an R-module of rank* 1.

Knowing the basis of $\overline{\mathcal{S}}^2_{\mathrm{rat}}(\mathbb{Q})_{\mathrm{fin}}$, the proof of Theorem 2.12 then reduces to proving the following proposition. Note, that the proof of Proposition 2.14 is independent of Theorem 2.13.

Proposition 2.14 *We have*

$$V(z) := N\frac{z\Phi'_N(z)}{\Phi_N(z)} \in \mathcal{S}^2_{\mathrm{rat}}(\mathbb{Q}),$$

and V admits a finite extension

$$\int^2 V(z) = \sum_{k=1}^{N} b_k \operatorname{Li}_2\left(z^k\right),$$

with $b_k \in \mathbb{Z}$ for $k \in \{1, ..., N\}$.

Proof. We need to show the existence of integers $b_1, ..., b_N \in \mathbb{Z}$, such that

$$V(z) = \sum_{k=1}^{N} b_k k^2 \frac{z^k}{1-z^k}.$$

For $N = 1$, we immediately find $b_1 = -1$ and $b_k = 0$ for all $k \geq 2$. Let $N \in \mathbb{N}$, $N > 1$, be arbitrary and suppose that the assertion is correct for all $d < N$. As a starting point, recall the formula

$$z^N - 1 = \prod_{d|N} \Phi_d(z).$$

Then by using logarithmic derivatives,

$$N\frac{z^N}{z^N-1} = \sum_{d|N} \frac{z\Phi'_N(z)}{\Phi_N(z)}.$$

Equivalently,

$$\begin{aligned} N\frac{\Phi'_N(z)}{\Phi_N(z)} &= -N^2\frac{z^N}{1-z^N} - N\sum_{\substack{d|N\\ d<N}} \frac{z\Phi'_d(z)}{\Phi_d(z)} \\ &= -N^2\frac{z^N}{1-z^N} - \sum_{\substack{d|N\\ d<N}} \frac{N}{d}\cdot d\frac{z\Phi'_d(z)}{\Phi_d(z)}. \end{aligned}$$

Then $b_N = -1$. Furthermore, applying the induction hypothesis to $d\dfrac{z\Phi'_d(z)}{\Phi_d(z)}$, we

obtain $b_n \in \mathbb{Z}$ and $b_n = 0$ for all $n > N$. By the equivalence Proposition 2.10 $(i) \Leftrightarrow (iv)$ we then ensured $V \in \mathcal{S}^2(\mathbb{Q})$, since in the present case, the Frobenius element over an arbitrary prime $p \in \mathbb{Z}$ is given by the identity. □

(4) *We give an example of a rational 2-function with rational coefficients, such that its representing formal sum given by eq.* (2.10) *does not terminate.* Let $V \in \mathcal{S}^2_{\mathrm{rat}}(\mathbb{Q})_{\{2\}}$ be given by

$$V(z) = \frac{z}{1-z} + \frac{z}{1+z} =: \sum_{n=1}^{\infty} a_n z^n,$$

where

$$a_n = 1 + (-1)^n = \begin{cases} 2 & \text{for } n \equiv 0 \mod 2 \\ 0 & \text{for } n \equiv 1 \mod 2. \end{cases}$$

By Proposition 2.10 *(v)*, there is a suitable sequence $q \in \mathbb{Z}\left[2^{-1}\right]^{\mathbb{N}}$, such that

$$\int^2 V(z) = \sum_{d=1}^{\infty} \frac{1}{d} \operatorname{Li}_2(q_d z^d).$$

By eq. (2.12) q_n is given by

$$q_n = a_n - \sum_{\substack{d|n \\ d>1}} \frac{n}{d} q_{n/d}^d.$$

We immediately observe $q_1 = a_1 = 0$. Hence, for any prime $p \in \mathbb{Z}$,

$$q_p = a_p - q_1^p = \begin{cases} 2, & \text{for } p = 2, \text{ and} \\ 0, & \text{for } p > 2. \end{cases}$$

But, for $n = 2p$, where p runs through all prime numbers in $\mathbb{Z}$ greater than 2, we have

$$q_{2p} = a_{2p} - pq_p^2 - 2q_2^p = 2 - 2^{p+1} \neq 0.$$

In particular, the sequence $(q_n)_{n\in\mathbb{N}}$ does not vanish for n sufficiently large, although V was given by a rational function.

2.3 Dwork's Integrality Lemma

Next we will rephrase *Dwork's Integrality Lemma* in the setting of 1-functions as has been done in [40]. Dwork's Lemma is actually given by the equivalence *(iii)* $\Leftrightarrow$ *(iv)*, a proof of the classical statement is given in [27, Ch. 14].

Theorem 2.15 (cf. Prop. 7 in [40], Dwork's Integrality Lemma) *Let $V \in zK[\![z]\!]$ and $Y \in 1+zK[\![z]\!]$ be related by $V = \log Y$, $Y = \exp(V)$. Then the following is equivalent*

(i) *V is an 1-function.*

(ii) *There is a sequence $q \in \mathcal{O}\left[D^{-1}\right]^{\mathbb{N}}$ such that*

$$\int V(z) = -\sum_{n=1}^{\infty} \log(1 - q_n z^n)$$

(iii) *For every unramified prime p in $K|\mathbb{Q}$,*

$$\frac{\mathrm{Frob}_p(Y)(z^p)}{Y(z)^p} \in 1 + zp\mathcal{O}_p[\![z]\!],$$

(iv) *$Y \in 1 + z\mathcal{O}\left[D^{-1}\right][\![z]\!]$.*

Proof. Let p be a prime unramified in $K \mid \mathbb{Q}$.

(i) $\Leftrightarrow$ *(ii)*: Using the equivalence Proposition 2.10 *(ii)* $\Leftrightarrow$ *(v)* for $s = 1$, the statement follows from

$$\sum_{d|n} \frac{\mathrm{Frob}_p\left(q_{n/d}^d\right) - q_{n/d}^{pd}}{d} - p\sum_{\substack{d|n \\ p\nmid d}} \frac{q_{n/d}^d}{d} \equiv 0 \mod p\mathcal{O}_p. \tag{2.14}$$

If $p \nmid d$, then $p\dfrac{q_{n/d}^d}{d} \in p\mathcal{O}_p$. Therefore, eq. (2.14) follows from Euler's Theorem, for all $q_{n/d} \in \mathcal{O}\left[D^{-1}\right]$,

$$\mathrm{Frob}_p\left(q_{n/d}^d\right) - q_{n/d}^{pd} \equiv 0 \mod p^{\mathrm{ord}_p(d)+1}\mathcal{O}_p.$$

(ii) $\Rightarrow$ *(iv)*: Given *(ii)*, we have

$$Y(z) = \exp(V(z)) = \prod_{d=1}^{\infty}(1 - q_d z^d)^{-1} \in 1 + z\mathcal{O}\left[D^{-1}\right][\![z]\!].$$

(iv) $\Rightarrow$ *(iii)*: Let $y \in \mathcal{O}\left[D^{-1}\right]^{\mathbb{N}}$ be given by the sequence

$$y := ([Y(z)]_{n-1})_{n\in\mathbb{N}}.$$

(The shift $n-1$ in the index above is due to the fact that $Y(z)$ has leading constant (zeroth) coefficient.) Then $Y(z)^p$ can be expressed in terms of (partial) Bell polynomials which we will introduce in Definition 4.3. Using the convention $!y = (n!y_n)_{n\in\mathbb{N}}$, we obtain (by Definition 4.3)

$$Y(z)^p = \frac{1}{z^p}\left(\sum_{n=1}^{\infty} y_n z^n\right)^p = \sum_{n=p}^{\infty} \frac{p!}{n!} B_{n,p}(!y) z^{n-p}.$$

Furthermore,

$$\frac{p!}{n!} B_{n,p}(!y) = \sum_{\alpha\in\pi(n,p)} \binom{p}{\alpha_1, ..., \alpha_{n-p+1}} \prod_{i=1}^{n-p+1} y_i^{\alpha_i},$$

where $\alpha \in \pi(n,p) \subset \mathbb{N}_0^{n-p+1}$ if and only if

$$\sum_{i=1}^{n-p+1} \alpha_i = p \qquad \text{and} \qquad \sum_{i=1}^{n-p+1} i\alpha_i = n.$$

If there is a $1 \le j \le n-p+1$ such that $\alpha_j < p$, then

$$\binom{p}{\alpha_1, ..., \alpha_{n-p+1}} = \frac{p}{\alpha_j}\binom{p-1}{\alpha_1, ..., \alpha_j - 1, ..., \alpha_{n-p+1}} \equiv 0 \mod p\mathcal{O}_p.$$

If $\alpha_j = p$, then $\alpha_i = 0$ for all $1 \le i \le n-p+1$, $i \ne j$. (Indeed, this follows from the condition $\sum_{i=1}^{n-p+1} \alpha_i = p$). Hence

$$n = \sum_{i=1}^{n-p+1} i\alpha_i = jp.$$

In particular, if $p \nmid n$, then $\frac{p!}{n!} B_{n,p}(!y) \equiv 0 \mod p\mathcal{O}_p$. We obtain for $p \mid n$,

$$\frac{p!}{n!} B_{n,p}(!y) \equiv y_{n/p}^p \mod p\mathcal{O}_p.$$

Therefore, since Frob_p is given by taking component-wise the p-th power modulo

$\mathfrak{p}$ for all prime ideals $\mathfrak{p} \mid (p)$, we have

$$\begin{aligned} Y(z)^p &= \sum_{n=p}^{\infty} \frac{p!}{n!} B_{n,p}(!y) z^{n-p} \equiv \sum_{\substack{n=p \\ p \mid n}}^{\infty} y_{n/p}^p z^{n-p} \mod p\mathcal{O}_p[\![z]\!] \\ &= \sum_{n=1}^{\infty} y_n^p z^{p(n-1)} \equiv \sum_{n=1}^{\infty} \mathrm{Frob}_p(y_n) z^{p(n-1)} \mod p\mathcal{O}_p[\![z]\!] \\ &= \mathrm{Frob}_p \left[\sum_{n=1}^{\infty} [Y(z)]_{n-1} z^{p(n-1)} \right] = \mathrm{Frob}_p\, Y(z^p). \end{aligned}$$

Consequently, there is a $g(z) \in z\mathcal{O}_p[\![z]\!]$, such that

$$\mathrm{Frob}_p\, Y(z^p) = Y(z)^p + pg(z).$$

Hence,

$$\frac{\mathrm{Frob}_p\, Y(z^p)}{Y(z)^p} = 1 + p\frac{g(z)}{Y(z)^p}.$$

Since $Y \in 1 + z\mathcal{O}\left[D^{-1}\right][\![z]\!]$, Y is invertible in $\mathcal{O}_p[\![z]\!]$ and therefore

$$\frac{g(z)}{Y(z)^p} \in z\mathcal{O}_p[\![z]\!],$$

from which *(iii)* follows.

(iii) $\Rightarrow$ *(i)*: Given *(iii)*, we have an element $g(z) \in z\mathcal{O}_p[\![z]\!]$, such that $\dfrac{\mathrm{Frob}_p\, Y(z^p)}{Y(z)^p} = 1 + pg(z)$. Taking the logarithm then gives

$$p\left[\frac{1}{p}\,\mathrm{Frob}_p\, V(z^p) - V(z)\right] = \log(1 + pg(z)) = \sum_{n=1}^{\infty} \frac{(-pg(z))^n}{n} \in pz\mathcal{O}_p[\![z]\!].$$

In particular, V is an 1-function.

This completes the proof. □

Dwork himself used his lemma (stated for $K = \mathbb{Q}$) as a key step to prove his theorem

Theorem 2.16 (Dwork [13]) *Let H be an affine hypersurface defined over a finite field $\mathbb{F}_q$, then the zeta-function*

$$Z(H/\mathbb{F}_q; X) = \exp\left(\sum_{k=1}^{\infty} \frac{N_k X^k}{k}\right)$$

of H is a rational function in X, where N_k denotes the number of $\mathbb{F}_{q^k}$-points of H, that is, $N_k = |H(\mathbb{F}_{q^k})|$.

We will prove an auxiliary to Theorem 2.15 (iii) in Section 4.4, namely

Theorem 2.17 *Let $V \in \mathcal{S}^1(K|\mathbb{Q})$ and $Y \in 1 + zK[\![z]\!]$ be related by $V = \delta \log Y$, $Y = \exp(\int V)$ and let p be unramified in $K|\mathbb{Q}$. Then*

$$[Y(z)^n]_m \equiv 0 \mod p^{\max\{0, \mathrm{ord}_p(n) - \mathrm{ord}_p(m)\}}\mathcal{O}_p.$$

Theorem 2.17 will be a key element to show that the framing of rational 2-functions can be integrated to 3-functions, i.e. Theorem 4.1. A proof of Theorem 2.17 is given in Section 4.4.

2.4 Algebraic Structures of $\mathcal{S}^s(K|\mathbb{Q})$ and $\overline{\mathcal{S}}^s(K|\mathbb{Q})$

Recall Definition 2.3. Let $V \in \mathcal{S}^s(K|\mathbb{Q})$ and $k \in \mathbb{N}$. Obviously, ε_k preserves the integrality property eq. (2.5) of the s-function $\int^s V(z)$, that is, $\varepsilon_k \int^s V(z)$ remains an s-function. Therefore, we may define $\varepsilon_k^{(s)} \colon \mathcal{S}^s(K|\mathbb{Q}) \to \mathcal{S}^s(K|\mathbb{Q})$ by the composition

$$\varepsilon_k^{(s)} \colon \mathcal{S}^s(K|\mathbb{Q}) \xrightarrow{\int^s} zK[\![z]\!] \xrightarrow{\varepsilon_k} zK[\![z]\!] \xrightarrow{\delta^s} \mathcal{S}^s(K|\mathbb{Q}). \tag{2.15}$$

Equivalently, $\varepsilon_k^{(s)}$ is given by $z \mapsto k^s z^k$, i.e. $\varepsilon_k^{(s)} = k^s \varepsilon_k$. In particular,

$$\varepsilon_k \colon \overline{\mathcal{S}}^s(K|\mathbb{Q}) \to \overline{\mathcal{S}}^s(K|\mathbb{Q}),$$

i.e. the multiplication by k^s can be omitted. It is also obvious, that the Cartier operator $\mathscr{C}_\ell$ for an integer $\ell \in \mathbb{N}$ gives a map $\mathscr{C}_\ell \colon \mathcal{S}^s(K|\mathbb{Q}) \to \mathcal{S}^s(K|\mathbb{Q})$, compare with Proposition 2.10 *(i) $\Leftrightarrow$ (iii)*. Analogously to above, we find an s-function preserving map by setting $\mathscr{C}_\ell^{(s)} := \ell^s \mathscr{C}_\ell$. Note that $\varepsilon_k^{(s)}$ and $\mathscr{C}_\ell$ preserve rationality, i.e.

$$\varepsilon_k, \mathscr{C}_\ell \colon \overline{\mathcal{S}}^s_{\mathrm{rat}}(K|\mathbb{Q}) \to \overline{\mathcal{S}}^s_{\mathrm{rat}}(K|\mathbb{Q}). \tag{2.16}$$

This is obvious for $\varepsilon_k^{(s)}$. To see that $\mathscr{C}_\ell$ preserves rationality, we may take $\zeta_\ell = \exp\left(\frac{2\pi i}{\ell}\right)$ and immediately observe that

$$\frac{1}{\ell} \sum_{r=1}^{\ell} V\left(\zeta_\ell^r z^{1/\ell}\right).$$

is – as a sum of rational functions – a rational function in the variable $z^{1/\ell}$. Recall, for $k \in \mathbb{Z}$, the identity

$$\frac{1}{\ell}\sum_{r=1}^{\ell}\zeta_\ell^{kr} = \delta_{\ell,k \bmod \ell} = \begin{cases} 1, & \text{if } \ell \mid k, \\ 0, & \text{if } \ell \nmid k. \end{cases}$$

Then

$$\begin{aligned}\frac{1}{\ell}\sum_{r=1}^{\ell} V\left(\zeta_\ell^r z^{1/\ell}\right) &= \frac{1}{\ell}\sum_{r=1}^{\ell}\sum_{n=1}^{\infty} a_n \zeta_\ell^{nr} z^{n/\ell} = \sum_{n=1}^{\infty} a_n z^{n/\ell}\frac{1}{\ell}\sum_{r=1}^{\ell}\zeta_\ell^{nr} \\ &= \sum_{n=1}^{\infty} a_n z^{n/\ell}\delta_{0,n \bmod \ell} \overset{n\mapsto \ell n}{=} \sum_{n=1}^{\infty} a_{\ell n} z^n = \mathscr{C}_\ell V.\end{aligned}$$

Therefore, $\mathscr{C}_\ell(V)$ is indeed a rational function in the variable z. More generally, the Cartier Operator $\mathscr{C}_\ell \colon K[\![z]\!] \to K[\![z]\!]$ can be represented as

$$\mathscr{C}_\ell W(z) = \frac{1}{\ell}\sum_{r=1}^{\ell} W\left(\zeta_\ell^r z^{1/\ell}\right), \tag{2.17}$$

where ζ_ℓ is a primitive ℓ-th root of unity and $W \in K[\![z]\!]$ is a formal power series.

Let $[\mathscr{C}_\ell, \varepsilon_k]$ denote the commutator bracket,

$$[\mathscr{C}_\ell, \varepsilon_k] = \mathscr{C}_\ell\varepsilon_k - \varepsilon_k\mathscr{C}_\ell.$$

We obtain

Proposition 2.18 *Let R be the ring given by $R = \mathbb{Q}[\varepsilon_k, \mathscr{C}_\ell \mid k, \ell \in \mathbb{N}]$. Then $\overline{\mathcal{S}}^s(K|\mathbb{Q})$ is an R-module. Also, $\overline{\mathcal{S}}^2_{\mathrm{rat}}(K|\mathbb{Q})$ is a R-submodule of $\overline{\mathcal{S}}^s(K|\mathbb{Q})$ for all $s \geq 2$. Furthermore, ε_k and $\mathscr{C}_\ell$ are not commutative in general. Instead, for $\tilde{\ell} = \dfrac{\ell}{\gcd(k,\ell)}$ and $\tilde{k} = \dfrac{k}{\gcd(k,\ell)}$,*

$$[\mathscr{C}_\ell, \varepsilon_k]\left(\sum_{n=1}^{\infty} a_n z^n\right) = \sum_{\substack{n=1 \\ \gcd(k,\ell)\nmid n}}^{\infty} a_{\tilde{\ell}n} z^{\tilde{k}n}.$$

Proof. The first part of the proposition is clear by eq. (2.16). The second part for $s = 2$ follows immediately, since ε_k and $\mathscr{C}_\ell$ preserve rationality. Let $k, \ell \in \mathbb{N}$ and write

$\tilde{k} = \dfrac{k}{\gcd(k,\ell)}$ and $\tilde{\ell} = \dfrac{\ell}{\gcd(k,\ell)}$. Then

$$\begin{aligned}\mathscr{C}_\ell\left(\varepsilon_k\left(\sum_{n=1}^{\infty} a_n z^n\right)\right) = \mathscr{C}_\ell\left(\sum_{n=1}^{\infty} a_n z^{kn}\right) &= \frac{1}{\ell}\sum_{n=1}^{\infty} a_n \sum_{i=1}^{\ell} \zeta_\ell^{ikn} z^{kn/\ell} \\ &= \frac{1}{\ell}\sum_{n=1}^{\infty} a_n z^{kn/\ell} \gcd(k,\ell) \sum_{i=1}^{\tilde{\ell}} \zeta_{\tilde{\ell}}^{i\tilde{k}n} \\ &= \frac{1}{\ell}\sum_{n=1}^{\infty} a_n z^{kn/\ell} \gcd(k,\ell)\tilde{\ell}\delta_{0,n \mod \tilde{\ell}} \\ &= \sum_{n=1}^{\infty} a_{\tilde{\ell}n} z^{\tilde{k}n}.\end{aligned}$$

On the other hand,

$$\begin{aligned}\varepsilon_k\left(\mathscr{C}_\ell\left(\sum_{n=1}^{\infty} a_n z^n\right)\right) &= \frac{1}{\ell}\sum_{i=1}^{\ell}\sum_{n=1}^{\infty} a_n \zeta_\ell^{in} z^{kn/\ell} \\ &= \sum_{n=1}^{\infty} a_n \delta_{n,0 \mod \ell} z^{kn/\ell} = \sum_{n=1}^{\infty} a_{\ell n} z^{kn}.\end{aligned}$$

Therefore,

$$[\mathscr{C}_\ell, \varepsilon_k]\left(\sum_{n=1}^{\infty} a_n z^n\right) = \sum_{n=1}^{\infty} a_{\tilde{\ell}n} z^{\tilde{k}n} - \sum_{n=1}^{\infty} a_{\ell n} z^{kn} = \sum_{\substack{n=1 \\ \gcd(k,\ell)\nmid n}}^{\infty} a_{\tilde{\ell}n} z^{\tilde{k}n},$$

as stated. □

It is clear that the s-function property eq. (2.5) is not respected by regular multiplication of power series. However, we find that $\mathcal{S}^s(K|\mathbb{Q})$ is closed under the *Hadamard product* of power series.

Definition 2.19 (Hadamard product) The *Hadamard product* of power series is defined by multiplying the coefficients component-wise. Let $V, W \in K[\![z]\!]$, $V(z) = \sum_{n=0}^{\infty} a_n z^n$ and $W(z) = \sum_{n=0}^{\infty} b_n z^n$. Then the Hadamard product $V \odot W$ of V and W is given by the power series

$$V \odot W(z) = \sum_{n=0}^{\infty} a_n b_n z^n.$$

Proposition 2.20 *$(\mathcal{S}^s(K|\mathbb{Q}), +, \odot)$ is a $\mathbb{Z}\left[D^{-1}\right]$-algebra.*

Proof. We only need to show that $V \odot W \in \mathcal{S}^s(K|\mathbb{Q})$, whenever $V, W \in \mathcal{S}^s(K|\mathbb{Q})$. Let therefore $V(z) = \sum_{n=1}^{\infty} a_n z^n$ and $W(z) = \sum_{n=1}^{\infty} b_n z^n$, then

$$\mathrm{Frob}_p(a_n b_n) - a_{pn} b_{pn} \equiv a_{pn} \left(\mathrm{Frob}_p(b_n) - b_{pn}\right) \equiv 0 \mod p^{s(\mathrm{ord}_p(n)+1)}\mathcal{O}_p,$$

as stated. □

Let us recall the more general but classical result in the theory of analytic functions (in one variable), see [22], [41].

Theorem 2.21 (Jungen, [22]) *Let V and $W \in K[\![z]\!]$ represent a rational and an algebraic function, respectively, then the Hadamard product $V \odot W$ represents an algebraic function. If, further, W is rational, so is $V \odot W$.*

What is more, we have the following result due to Stanley.

Theorem 2.22 (Thm. 2.10, [42]) *Let $V, W \in K[\![z]\!]$ be D-finite, so is $V \odot W$.*

As a conclusion, we have the following statement.

Corollary 2.23 *$(\mathcal{S}^s(K|\mathbb{Q}), +, \odot)$ is an $\mathcal{S}^s_{\mathrm{rat}}(K|\mathbb{Q})$-algebra. Furthermore, $\mathcal{S}^s_{\text{D-fin}}(K|\mathbb{Q})$ is an $\mathcal{S}^s_{\mathrm{rat}}(K|\mathbb{Q})$-subalgebra and $\mathcal{S}^s_{\mathrm{alg}}(K|\mathbb{Q})$ is an $\mathcal{S}^s_{\mathrm{rat}}(K|\mathbb{Q})$-submodule of $\mathcal{S}^s(K|\mathbb{Q})$.*

Proof. Follows directly from Proposition 2.20, Theorem 2.21 and Theorem 2.22. □

Remark 2.24 (Unity with respect to $\odot$) The unit element in $\mathcal{S}^s(K|\mathbb{Q})$with respect to the Hadamard product $\odot$ has a unit element, namely the harmonic series $z \sum_{n=0}^{\infty} z^n$.

Theorem 2.25 (Bézivin, [8]) *Let K be a field of characteristic zero and let $F(z) \in K[\![z]\!]$ be a D-finite power series such that $[F(z)]_n \in G \cup \{0\}$ for every $n \in \mathbb{N}_0$, where $G \subset K^\times$ is a finitely generated subgroup. Then $F(z)$ is the Maclaurin expansion of a rational function.*

Proposition 2.26 *Let $V \in z\mathcal{O}\left[D^{-1}\right][\![z]\!]$ be D-finite with coefficients in $\mathcal{O}\left[D^{-1}\right]$, such that V is invertible with respect to the Hadamard product. Then V is the Maclaurin expansion of a rational function.*

Proof. Since V is invertible with respect to the Hadamard product, we have $[V(z)]_n \in \left(\mathcal{O}\left[D^{-1}\right]\right)^\times$ for all $n \in \mathbb{N}$. By *Dirichlet's Unit Theorem* (see for instance, Thm. 7.4 in [34]), $\mathcal{O}\left[D^{-1}\right]^\times \subset K^\times$ is finitely generated. Using the D-finiteness of V, the statement then follows from Theorem 2.25. □

Chapter 3

Rational 2-Functions are Abelian

The author published Section 3.1 and Section 3.2 in the preprint [32].

The present chapter is dedicated to the proof of Theorem 1.2. Moreover, the following statement is a precise summary of the main results of this chapter.

Theorem 3.1 *Let $V \in \overline{\mathcal{S}}^2_{\mathrm{rat}}(K|\mathbb{Q})_{\mathrm{fin}}$, $V(z) \neq 0$, representing the rational function $F(z) \in K(z)$ as its Maclaurin expansion and write $a_n = [V(z)]_n$, for all $n \in \mathbb{N}$. Then V is periodic, i.e. there is an $N \in \mathbb{N}$ such that*

$$N = \min\{k \in \mathbb{N} \,|\, a_n = a_{n+k} \text{ for all } n \in \mathbb{N}\}.$$

Furthermore, there are rational coefficients $A_i \in \mathbb{Q}$ for $i = 1, ..., N$ and an appropriate primitive N-th root of unity ζ, such that

$$F(z) = \sum_{i=1}^{N} \frac{A_i \zeta^i z}{1 - \zeta^i z}, \quad \text{and } A_1 \neq 0. \tag{3.1}$$

In particular, the coefficients a_n of $V(z)$ have the form

$$a_n = \sum_{i=1}^{N} A_i \zeta^{in}. \tag{3.2}$$

Moreover, the map $\pi \colon \overline{\mathcal{S}}^2_{\mathrm{rat}}(K|\mathbb{Q})_{\mathrm{fin}} \to \mathbb{N}_0$, taking $V \mapsto N$ and $0 \mapsto 0$, is surjective.

Theorem 3.1 gives a full characterization of those 2-functions, whose second derivative is rational. Originally, the task was to give some description of the 2-function $\int^2 V(z)$ with coefficients in an algebraic field extension under the assumption that $Y(z) = \exp(\int V(z))$

is rational. However, the rationality of V follows immediately if we assume $Y(z)$ to be rational, compare Corollary 3.3. Also, it is more simple to draw consequences for the coefficients of V (as has been done in Theorem 3.1) then for the coefficients of Y by assuming rationality of Y. The message of Theorem 3.1 is that if $Y(z) = \exp(-\int V(z))$ is rational for an s-function $\int^s V(z)$ (with $s \geq 2$ and algebraic coefficients), then the number field generated by the coefficients of the s-function must be an abelian extension over $\mathbb{Q}$. This result is not unexpected: The s-function encodes information about the Frobenius endomorphism at all the (unramified) primes, modulo p^s. Y being rational then implies that there is a lot of regularity among the Frobenius elements at different primes. Such regularity is only expected for an abelian extension.

3.1 Rational 1-Functions and a Theorem due to Minton

The next Theorem 3.2 is a modified version of Theorem 7.1 in [7], which on the other hand is a re-proven statement from [30]. It is the starting point for the proof of Theorem 1.2. In its original formulation it states, that the generating functions of Euler sequences (which are rational 1-sequences, compare with eq. (1.2)) are given by sums of logarithmic derivatives of polynomials with integral coefficients. Since the original theorem is formulated for rational integers, we re-prove the statement for algebraic integers, that is, for 1-sequences, for the sake of completeness The crucial point is, that a rational 1-function only admits poles of order 1. In the course of this, we follow the ideas given in [7].

Theorem 3.2 (compare with [7], [30]) *Let $V \in \mathcal{S}^1_{\mathrm{rat}}(K|\mathbb{Q})$ representing the rational function $F(z) \in K(z)$ as its Maclaurin expansion. Then there is an integer $r \in \mathbb{N}$, distinct algebraic numbers $\alpha_i \in \overline{\mathbb{Q}}^\times$, and $A_i \in \mathbb{Q}^\times$, for $i = 1, ..., r$, such that F can be written as*

$$F(z) = \sum_{i=1}^{r} \frac{A_i \alpha_i z}{1 - \alpha_i z}.$$

Proof. Let F be given by the fraction of $P, Q \in K[z]$, $Q \not\equiv 0$, i.e. $F = \dfrac{P}{Q}$. We may assume that $Q(0) \neq 0$ and $P(0) = 0$. By [7, Prop. 3.5], we have $\deg(P) \leq \deg(Q)$. By adding a constant $C \in K$ to F it does not affect the 1-function condition but we may assume $\deg(P) < \deg(Q)$. Then, by the *Partial Fraction Decomposition* $\widetilde{F} = \dfrac{P}{Q} + C$ has the form

$$\widetilde{F} = \sum_{i=1}^{r} \sum_{j=1}^{m_i} \frac{A_{i,j}}{(1 - \alpha_i z)^j},$$

where the $\alpha_i \in \overline{\mathbb{Q}}^\times$, $i \in \{1,...,r\}$ are distinct algebraic numbers, $m_i \in \mathbb{N}$ and $A_{i,j} \in \overline{\mathbb{Q}}$ for all $(i,j) \in \{1,...,r\} \times \{1,...,m_i\}$. Now, let p be a sufficiently large prime, unramified in $K|\mathbb{Q}$, such that the following conditions are simultaneously satisfied:

(i) α_i and its Frob_p-conjugate are p-adic units for all $i \in \{1,...,r\}$,

(ii) $\alpha_i - \alpha_j$ and its Frob_p-conjugate are p-adic units for all $i,j \in \{1,...,r\}$, $i \neq j$, and

(iii) $p > m_i$ for all $i \in \{1,...,r\}$.

What we need to show is $m_i = 1$ for all $i \in \{1,...,r\}$. We have

$$\frac{1}{(1-\alpha_i z)^j} = \sum_{k=0}^{\infty} \binom{k+j-1}{j-1} \alpha_i^k z^k.$$

Therefore, if $\widetilde{V}(z) = V(z) + C$ is the Maclaurin series expansion of $\widetilde{F}$, we have

$$\mathscr{C}_p \widetilde{V} = \sum_{k=0}^{\infty} \left[\sum_{i=1}^{r} \sum_{j=1}^{m_i} A_{i,j} \binom{pk+j-1}{j-1} \alpha_i^{pk} \right] z^k.$$

Since $p > m_i$, we find $\binom{pk+\nu}{\nu} \equiv 1 \mod p$ for all $0 \leq \nu < m_i$ (in particular, $\nu < p$) by the following calculation

$$\binom{pk+\nu}{\nu} = \prod_{\ell=1}^{\nu} \left(1 + \frac{pk}{\ell}\right) \equiv 1 \mod p.$$

Consequently,

$$\begin{aligned} \mathscr{C}_p \widetilde{V} &\equiv \sum_{k=0}^{\infty} \left[\sum_{i=1}^{r} \sum_{j=1}^{m_i} A_{i,j} \alpha^{pk} \right] z^k \mod p \\ &= \sum_{i=1}^{r} \sum_{j=1}^{m_i} \frac{A_{i,j}}{1-\alpha_i^p z} \\ &= \sum_{i=1}^{r} \frac{A_i}{1-\alpha_i^p z}, \end{aligned}$$

where $A_i = \sum_{j=1}^{m_i} A_{i,j}$. Hence, $\mathscr{C}_p \widetilde{V}$ represents a rational function with exclusively simple poles modulo p. Thus, the 1-function property

$$\mathscr{C}_p(\widetilde{V}) - \mathrm{Frob}_{\mathfrak{p}} \widetilde{V} \equiv 0 \mod p\mathcal{O}_p[\![z]\!]$$

ensures that $\tilde{F}$ has only simple poles as well. Therefore, we write from now on

$$\widetilde{F} = \sum_{i=1}^{r} \frac{A_i}{1-\alpha_i z},$$

where $A_i, \alpha_i \in \overline{\mathbb{Q}}^{\times}$ and $\alpha_i \neq \alpha_j$ for $i \neq j$. Evaluating $\widetilde{F}$ at $z = 0$ we conclude that $C = \sum_{i=1}^{r} A_i$. Therefore,

$$\begin{aligned} F = \widetilde{F} - C &= \sum_{i=1}^{r} \frac{A_i}{1-\alpha_i z} - \sum_{i=1}^{r} A_i \\ &= \sum_{i=1}^{r} \frac{A_i \alpha_i z}{1-\alpha_i z}. \end{aligned}$$

In particular, we have

$$a_n = \sum_{i=1}^{r} A_i \alpha_i^n \qquad \text{for all } n \in \mathbb{N}.$$

The local 1-function property for p then gives

$$0 \equiv \mathrm{Frob}_p(a_m) - a_{mp} = \sum_{i=1}^{r} (\mathrm{Frob}_p(A_i)\mathrm{Frob}_p(\alpha_i^m) - A_i \alpha_i^{mp}) \mod p\mathcal{O}_p,$$

for all $m \in \mathbb{N}$. Since Frob_p is given by taking component-wise the p-th power modulo $\mathfrak{p}$ for all $\mathfrak{p} \mid (p)$, we conclude

$$0 \equiv \sum_{i=1}^{r} (A_i^p - A_i)\, \alpha_i^{mp} \mod p\mathcal{O}_p,$$

for all $m \in \mathbb{N}$. The Vandermonde type matrix M

$$M = \begin{pmatrix} \alpha_1^p & \alpha_1^{2p} & \dots & \alpha_1^{rp} \\ \alpha_2^p & \alpha_2^{2p} & \dots & \alpha_2^{rp} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_r^p & \alpha_r^{2p} & \dots & \alpha_r^{rp} \end{pmatrix}.$$

is invertible modulo $p\mathcal{O}_p$. Indeed, its determinant is given by

$$\begin{aligned}\det(M) &= \Big(\prod_{i=1}^{r}\alpha_i^p\Big)\times\prod_{1\le i<j\le r}\big(\alpha_j^p-\alpha_i^p\big)\\ &\equiv \Big(\prod_{i=1}^{r}\alpha_i^p\Big)\times\prod_{1\le i<j\le r}(\alpha_j-\alpha_i)^p \mod p\mathcal{O}_p\\ &\equiv \mathrm{Frob}_p\left(\prod_{i=1}^{r}\alpha_i\times\prod_{1\le i<j\le r}(\alpha_j-\alpha_i)\right) \mod p\mathcal{O}_p.\end{aligned}$$

By assumption (i) and (ii) above, we obtain $\det(M)\in\mathcal{O}_p^\times$. Hence, $A_i^p\equiv A_i \mod p$ for all $i\in\{1,...,r\}$. From *Frobenius's Densitiy Theorem*, see for instance [21], it follows that $A_i\in\mathbb{Q}$ for all $i\in\mathbb{N}$. □

Corollary 3.3 *Let $V\in\mathcal{S}^1(K|\mathbb{Q})$ and $Y=\exp(-\int V)$. Then V is the series expansion of a rational function if Y is the series expansion of a rational function. Conversely, if V represents a rational function, then there is an $M\in\mathbb{N}$ such that Y^M is the series expansion of a rational function.*

Proof. Let Y be the series expansion of a rational function, then so is δY. Hence, $\dfrac{\delta Y}{Y}$ is the series expansion of a rational function. Consequently, $V=-\dfrac{\delta Y}{Y}$ represents a rational function. Note that this holds even for arbitrary $V\in zK[\![z]\!]$. Conversely, let V represent a rational function at zero. By Theorem 3.2 (here we use $V\in\mathcal{S}^1(K|\mathbb{Q})$) there exists a natural number $r\in\mathbb{N}$, and distinct $\alpha_i\in\overline{\mathbb{Q}}^\times$, $A_i\in\mathbb{Q}^\times$, for $i=1,...,r$, such that

$$\begin{aligned}V&=\sum_{i=1}^{r}\frac{A_i\alpha_i z}{1-\alpha_i z}=\sum_{i=1}^{r}A_i\sum_{n=1}^{\infty}\alpha_i^n z^n\\ &=\sum_{i=1}^{r}A_i\delta\sum_{n=1}^{\infty}\frac{\alpha_i^n}{n}z^n=-\sum_{i=1}^{r}A_i\delta\log(1-\alpha_i z).\end{aligned}$$

Therefore,

$$Y=\exp(-\textstyle\int V)=\exp\left(\sum_{i=1}^{r}A_i\log(1-\alpha_i z)\right)=\prod_{i=1}^{r}(1-\alpha_i z)^{A_i}.$$

Taking $M\in\mathbb{N}$ to be the least common multiple of the denominators of A_i we find that Y^M is a rational function. □

Proving Corollary 3.3 does not go without mentioning the following more general facts. More precisely, we have the following generalizations of Corollary 3.3 given in

Proposition 3.4 and Theorem 3.7. The author could not find a direct reference for Proposition 3.4. At the same time, Proposition 3.4 seems to be common knowledge to some authors (at least to [15]). This might be based therein that Proposition 3.4 follows from more general theorems. For instance, it should be a direct consequence of the combined work of Stanley (see [42], 1980) and Harris and Sibuya (see [19], 1985) as we will demonstrate immediately.

Proposition 3.4 *Let $V \in K[\![z]\!]$ and $Y = \exp(-\int V) \in 1 + zK[\![z]\!]$. If Y is the series expansion of an algebraic function, then V is the series expansion of an algebraic function.*

Proof. Assume that Y represents an algebraic function, i.e. an algebraic element over the field of rational functions $K(z)$. Then $\frac{1}{Y}$ is also an algebraic function. By the following theorem due to Stanley, Y and $\frac{1}{Y}$ are D-finite.

Theorem 3.5 (Thm. 2.1 in [42]) *If $Y \in K[\![z]\!]$ is algebraic, then Y is D-finite.*

Additionally, in [19], Harris and Sibuya established the following theorem:

Theorem 3.6 (Cor. 1 in [19]) *Let $Y \in K[\![z]\!]$, $Y \neq 0$, be a power series such that Y and $\frac{1}{Y}$ are D-finite. Then the logarithmic derivative $\frac{\delta Y}{Y}$ of Y is algebraic over $K(z)$.*

The statement then follows by recognizing that $V = -\frac{\delta Y}{Y}$. □

As pointed out in [15] (and also in [23]), the converse of Proposition 3.4 is not true: Take for Y the exponential function $\exp(z)$, which is a transcendental formal power series, then $\frac{\delta Y}{Y} = z$, which is even a rational function. However, under an additional assumption on the integrality of the coefficients of Y, Kassel and Reuntenauer wrote down a proof of the following theorem in [23], 2014, by using the solution to the *Grothendieck-Katz conjecture*.

Theorem 3.7 (Thm. 4.4 in [23]) *If $Y \in \mathbb{Z}[\![z]\!]$ is a formal power series with integral coefficients such that $\frac{\delta Y}{Y}$ is algebraic, then Y is algebraic.*

Recall from Dwork's Integrality Lemma (cf. Theorem 2.15) that the integrality condition on the coefficients of Y in the case where $Y \in 1 + z\mathbb{Z}[\![z]\!]$ is equivalent to saying that $V = (\pm)\frac{\delta Y}{Y} \in \mathcal{S}^1(\mathbb{Q})$. This observation coincides with the proof of Corollary 3.3.

3.2 Proof of Theorem 3.1

In the present section we will give a proof of Theorem 3.1 which implies Theorem 1.2. By multiplication with an integral constant, we may assume $V \in \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})_{\mathrm{fin}}$ and write

$a_n = [V(z)]_n$ for all $n \in \mathbb{N}$. Let S be the finite set of those primes, which ramify in $K|\mathbb{Q}$ and at which V does not satisfy the local 2-function property. We might also assume $V \in \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$, since we might substitute K by $K(\zeta_q | q \in S)$. By doing that, we ensure that all primes in S ramify in K. Therefore, let $V \in \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$. In particular, $V \in \mathcal{S}^1(K|\mathbb{Q})$ by eq. (2.7), and by Theorem 3.2, there is an $r \in \mathbb{N}$, $A_i \in \mathbb{Q}^\times$ and distinct $\alpha_i \in \overline{\mathbb{Q}}^\times$ for $i \in \{1, ..., r\}$ such that

$$a_n = \sum_{i=1}^{r} A_i \alpha_i^n \text{ for all } n \in \mathbb{N}.$$

In the following, let us assume $\alpha_i \in K$, since we might otherwise substitute K by a normal closure of $K(\alpha_1, ..., \alpha_r)$. As pointed out by Minton in [30] the *Chebotarëv Density Theorem* implies

Theorem 3.8 (Thm. 3.3. in [30]) *Let K be a Galois number field. For any $\sigma \in \mathrm{Gal}(K|\mathbb{Q})$, there exists infinitely many primes $\mathfrak{p}$ of K such that $\mathrm{Fr}_\mathfrak{p} = \sigma$.*

Let $p \in \mathbb{Z}$ be an unramified prime in $K|\mathbb{Q}$, splitting completely in K, i.e. $\mathrm{Fr}_\mathfrak{p} = \mathrm{id}_K$ for all $\mathfrak{p} \mid (p)$. By the density theorem of Chebotarëv there are infinitely many such primes p. Let $m, n \in \mathbb{N}$ be integers then the local 2-function property reads

$$\begin{aligned} a_{p^n m} - \mathrm{Frob}_p(a_{p^{n-1}m}) &= a_{p^n m} - a_{p^{n-1}m} \\ &= \sum_{i=1}^{r} A_i \left(\alpha_i^{p^n m} - \alpha_i^{p^{n-1}m} \right) \equiv 0 \mod p^{2n}\mathcal{O}_p. \end{aligned} \tag{3.3}$$

Before we dive into the proof, we give an intuition of why Theorem 1.2 is correct. Since the congruence given in eq. (3.3) is valid for infinitely many primes and all $m, n \in \mathbb{N}$, it should be true that these congruences already hold for each summand individually. In other words, we expect

$$\alpha_i^{p^n m} - \alpha_i^{p^{n-1}m} \equiv 0 \mod p^{2n}\mathcal{O}_p,$$

for all $i \in \{1, ..., r\}$ and all $m, n \in \mathbb{N}$ and all primes p that split completely in $K|\mathbb{Q}$. Therefore, we should be able to reduce eq. (3.3) to the case $r = 1$. The case $r = 1$ is subject of Lemma 3.9 Indeed, the speed of convergence of eq. (3.3) is the crucial obstruction.

Lemma 3.9 *Let $x \in K^\times$ and $p \in \mathbb{Z}$ be a prime, which is unramified in $K|\mathbb{Q}$ and splits completely, such that $\iota_p(x)$ is a p-adic unit. Suppose that*

$$\iota_p(x)^{p^n} - \iota_p(x)^{p^{n-1}} \equiv 0 \mod p^{2n}\mathcal{O}_p,$$

for all $n \in \mathbb{N}$. Then x is a root of unity in K.

Proof. If p splits completely in $K|\mathbb{Q}$, then for all prime ideals $\mathfrak{p} \subset \mathcal{O}$ dividing (p) we have $K_\mathfrak{p} \cong \mathbb{Q}_p$ and $\mathcal{O}_\mathfrak{p} \cong \mathbb{Z}_p$. Let $\overline{x} \in \mathbb{Q}_p$ denote the image of $\iota_\mathfrak{p}(x)$ under this identification. Then we have in particular $\overline{x} \in \mathbb{Z}_p$ and the congruence assumption reformulates to

$$\overline{x}^{p^n} - \overline{x}^{p^{n-1}} \equiv 0 \mod p^{2n}\mathbb{Z}_p \quad \text{for all } n \in \mathbb{N}.$$

Equivalently,

$$\overline{x}^{p^{n-1}(p-1)} \equiv 1 \mod p^{2n}\mathbb{Z}_p \quad \text{for all } n \in \mathbb{N}.$$

Recall that the Iwasawa logarithm preserves the p-adic order, therefore

$$p^{n-1} \log_p(\overline{x}^{p-1}) \equiv 0 \mod p^{2n}\mathbb{Z}_p \quad \text{for all } n \in \mathbb{N}.$$

Hence, $\log_p(\overline{x}^{p-1}) \equiv 0 \mod p^{n+1}$ for all $n \in \mathbb{N}$, implying $\overline{x} \in \ker \log_p$. Since $\iota_p(x)$ is a p-adic unit, $\overline{x}$ is a root of unity in $\mathbb{Z}_p$ and consequently, x needs to be a root of unity in K. □

The obvious problem is that, *a priori*, one may not make any conclusions on the p-divisibility of the sumands in eq. (3.3) by only knowing the p-divisibility of the whole sum. This is reflected by the fact that $\log_p$ is not additive. That makes it unlikely to generalize the procedure in the proof of Lemma 3.9 to eq. (3.3) for $r > 1$. Hence, there does not seem to exist a true reduction of eq. (3.3) to the case $r = 1$. At the other hand, Lemma 3.9 surprisingly suggests that it should be sufficient to investigate the 2-function property eq. (3.3) for only one suitably chosen prime p (which is only possible since there are infinitely many such primes by Chebotarëv Density Theorem). Therefore, the strategy we will pursue is a proof by contradiction: We will assume that there is no root of unity among α_i, for $i = 1, ..., r$. By Lemma 3.9, this amounts in saying, that the individual sumands $\alpha_i^{mp^n} - \alpha_i^{mp^{n-1}}$, for $i = 1, ..., r$, are converging *slowly* towards zero (they are converging after all by Euler's Theorem 1.1). For a suitable chosen prime (such that all relevant quantities are p-adic units), the p-adic estimations of the error functions $\rho_{i,n}(m) = \dfrac{\alpha_i^{mp^n} - \alpha_i^{mp^{n-1}}}{p^n}$ given by Proposition 3.10 and Proposition 3.11 in combination with the assumption given by eq. (3.3) will then lead to a contradiction. The resulting statement is given by Theorem 3.12.

Let $x \in \mathbb{Z}_p^\times$ and $m \in \mathbb{N}$. By Euler's Theorem 1.1 there is a sequence $(\rho_n(m))_{n\in\mathbb{N}} \in \mathbb{Z}_p^\mathbb{N}$

such that

$$x^{mp^n} - x^{mp^{n-1}} = p^n \rho_n(m).$$

We also write $\kappa_n(m) := \mathrm{ord}_p(\rho_n(m)) \in \mathbb{N}_0 \cup \{\infty\}$. As we will successively discover in Proposition 3.10 and Proposition 3.11, $\kappa_n(m)$ is independent of $n, m \in \mathbb{N}$ for $\gcd(p, m) = 1$.

Proposition 3.10 *Let $p > 2$ and $x \in \mathbb{Z}_p^\times$. Then the sequence $\kappa_n(m) \in \mathbb{N}_0 \cup \{\infty\}$ is independent of n, i.e. $\kappa_1(m) = \kappa_n(m)$ for all $n \in \mathbb{N}$. If $\kappa(m) := \kappa_1(m) \neq \infty$, then*

$$\rho_{n+1}(m) \equiv \rho_n(m) \mod p^{n+2\kappa(m)}\mathbb{Z}_p$$

for all $n \in \mathbb{N}$.

Proof. To simplify the notation, let $\rho_n := \rho_n(m)$, $x = x^m$ and $\kappa_n = \kappa_n(m)$. Suppose $\rho_{n_0} = 0$ for some $n_0 \in \mathbb{N}_0$. But then, the equation $x^{p^{n_0-1}(p-1)} = 1$ implies that x is a root of unity in $\mathbb{Z}_p$ and therefore $x^{p^{n-1}(p-1)} = 1$ for all $n \in \mathbb{N}$, i.e. $\rho_n = 0$ for all $n \in \mathbb{N}$. Recall that the set of torsion elements of $\mathbb{Z}_p$ (i.e. the set of roots of unity in $\mathbb{Q}_p$) are given by μ_{p-1}, the set of $(p-1)$-th roots of unity. Conversely, if x is a root of unity, we therefore have $\rho_n = 0$ for all $n \in \mathbb{N}$. Suppose therefore, that $\rho_n \neq 0$ for all $n \in \mathbb{N}$, i.e. x is not a root of unity in $\mathbb{Z}_p$. Then the statement follows by using the *Binomial Theorem*. We have

$$\begin{aligned}
x^{p^n} &= \left(x^{p^{n-1}}\right)^p = \left(x^{p^n} - p^n\rho_n\right)^p \\
&= \sum_{k=0}^{p} \binom{p}{k} x^{kp^n} (-1)^{p-k} p^{n(p-k)} \rho_n^{p-k} \\
&= x^{p^{n+1}} + \sum_{k=1}^{p-1} \binom{p}{k} x^{kp^n} (-1)^{p-k} p^{n(p-k)} \rho_n^{p-k} + (-1)^p p^{np} \rho_n^p. \\
&= x^{p^{n+1}} + \sum_{k=1}^{p-1} \binom{p-1}{k} x^{kp^n} \frac{(-1)^{p-k}}{p-k} \rho_n^{p-k} p^{n(p-k)+1} + (-1)^p \rho_n^p p^{np}.
\end{aligned}$$

Therefore, by using the definition $\rho_{n+1} = \dfrac{1}{p^{n+1}}\left(x^{p^{n+1}} - x^{p^n}\right)$, we obtain

$$\begin{aligned}
p^{n+1}\rho_{n+1} &= \sum_{k=1}^{p-1} \binom{p-1}{k} x^{kp^n} \frac{(-1)^{p-k+1}}{p-k} \rho_n^{p-k} p^{n(p-k)+1} - (-1)^p \rho_n^p p^{np}, \\
\Leftrightarrow\ \rho_{n+1} &= \sum_{k=1}^{p-1} \binom{p-1}{k} x^{kp^n} \frac{(-1)^{p-k+1}}{p-k} \rho_n^{p-k} p^{n(p-k-1)} - (-1)^p \rho_n^p p^{n(p-1)-1}.
\end{aligned}$$

If $p > 2$, we find modulo $p^{n+2\kappa_n}$,

$$\rho_{n+1} \equiv x^{(p-1)p^n}\rho_n \mod p^{n+2\kappa_n}\mathbb{Z}_p.$$

From this congruence it is evident that $\kappa_{n+1} = \kappa_n$. We therefore write κ for κ_n. Furthermore, using $x^{(p-1)p^n} = 1 + p^{n+1}x^{-p^n}\rho_{n+1}$ once more, this leads to

$$\begin{aligned}\rho_{n+1} &\equiv x^{(p-1)p^n}\rho_n \mod p^{n+2\kappa}\mathbb{Z}_p \\ &= \left(1 + p^{n+1}x^{-p^n}\rho_{n+1}\right)\rho_n \\ &\equiv \rho_n \mod p^{n+2\kappa}\mathbb{Z}_p,\end{aligned}$$

which finishes the proof. □

Proposition 3.11 *Let $x \in \mathbb{Z}_p^\times$ be a p-adic unit and $n, m \in \mathbb{N}$ be integers such that $\gcd(m, p) = 1$. Then $\kappa := \kappa(m) \in \mathbb{N}_0 \cup \{\infty\}$ does not depend on m. Furthermore, if $\kappa < \infty$, then*

$$\rho_n(m) \equiv mx^{(m-1)p^{n-1}}\rho_n(1) \mod p^{n+2\kappa}.$$

Proof. Fix $n \in \mathbb{N}$. If x is a root of unity in $\mathbb{Z}_p$, then $\kappa(m) = \infty$ for all $m \in \mathbb{N}$. Conversely, if $\rho_n(m)$ vanishes for some $m \in \mathbb{N}$, then x is a root of unity in $\mathbb{Z}_p$. Therefore, let x be not a root of unity in $\mathbb{Z}_p$. Since $\rho_n(1) \neq 0$ we have

$$\begin{aligned}x^{-(m-1)p^{n-1}}\frac{\rho_n(m)}{\rho_n(1)} &= \frac{1 - x^{mp^{n-1}(p-1)}}{1 - x^{p^{n-1}(p-1)}} \\ &= \sum_{k=0}^{m-1} x^{kp^{n-1}(p-1)} \\ &= m + p^n \sum_{k=1}^{m-1} x^{-kp^{n-1}}\rho_n(k).\end{aligned}$$

The above computation shows that $\kappa(m) = \operatorname{ord}_p(\rho_n(m))$ is constant in m, since $\gcd(m, p) = 1$. Therefore, write $\kappa := \kappa(m)$ for all $m \in \mathbb{N}$. In particular, the p-adic order of the sum $\sum_{k=1}^{m-1} x^{-kp^{n-1}}\rho_n(k)$ is at least κ (since every single summand has p-adic order greater or equal to κ). Therefore,

$$\rho_n(m) \equiv mx^{(m-1)p^{n-1}}\rho_n(1) \mod p^{n+2\kappa}\mathbb{Z}_p,$$

as stated. □

Theorem 3.12 *Let $p \in \mathbb{Z}$ be an odd prime. Let $r \in \mathbb{N}$ such that $r < p$ and for all $i = 1, ...r$ let $x_i, B_i \in \mathbb{Z}_p^\times$ such that $x_k \neq x_\ell \mod p\mathbb{Z}_p$ for $k \neq \ell$. Suppose the validity of the following family of congruences*

$$\sum_{i=1}^{r} B_i \left(x_i^{mp^n} - x_i^{mp^{n-1}} \right) \equiv 0 \mod p^{2n}\mathbb{Z}_p \quad \text{for all } m, n \in \mathbb{N}. \tag{3.4}$$

Then x_i is a root of unity in $\mathbb{Z}_p$ for all $i = 1, ..., r$.

Proof. Suppose there is a $j \in \{1, ..., r\}$ such that x_j is a root of unity in $\mathbb{Z}_p$. Then $x_j^{p-1} = 1$ and therefore

$$x_j^{mp^n} - x_j^{mp^{n-1}} = x_j^{mp^{n-1}} \left(x_j^{(p-1)m} - 1 \right) = 0.$$

Hence, eq. (3.4) becomes a reduced sum with $r - 1$ summands of the same type, namely,

$$\sum_{i=1}^{r} B_i \left(x_i^{mp^n} - x_i^{mp^{n-1}} \right) = \sum_{\substack{i=1 \\ i \neq j}}^{r} B_i \left(x_i^{mp^n} - x_i^{mp^{n-1}} \right).$$

Therefore, w. l. o. g. we may assume that none of the x_i eq. (3.4) are roots of unity. We will lead this assumption to a contradiction, which then implies that all x_i are roots of unity in $\mathbb{Z}_p$. In the following, we will write

$$\rho_{i,n}(m) := \frac{1}{p^n} \left(x_i^{mp^n} - x_i^{mp^{n-1}} \right), \qquad \text{and} \qquad \sigma_n(m) := \frac{1}{p^n} \sum_{i=1}^{r} B_i \rho_{i,n}(m)$$

for suitable $\rho_{i,n}(m), \sigma_n(m) \in \mathbb{Z}_p$. Note that $\sigma_n(m)$ is indeed in $\mathbb{Z}_p$ by eq. (3.4). In particular, we have $\rho_{i,n}(m) \neq 0$ for all $i, n, m \in \mathbb{N}$ with $\gcd(m, p) = 1$. By Proposition 3.10 and Proposition 3.11 we have for every $i = 1, ..., r$ a $\kappa_i \in \mathbb{N}$ such that $\kappa_i = \mathrm{ord}_p(\rho_{i,n}(m))$ for all $n, m \in \mathbb{N}$ with $\gcd(m, p) = 1$. Define $\kappa := \min\{\kappa_i \mid i = 1, ..., r\}$.

Within this scenario, we will prove the following statement: *For all $n, m \in \mathbb{N}$ with $\gcd(m, p) = 1$ we have*

$$\sum_{i=1}^{r} B_i x_i^{(m-1)p^{n-1}} \rho_{i,n}(1) \equiv 0 \mod p^{n+2\kappa}\mathbb{Z}_p. \tag{3.5}$$

By applying Proposition 3.10 to each $\rho_{i,n+1}$ separately, we obtain

$$p^{n+1}\sigma_{n+1}(m) = \sum_{i=1}^{r} B_i \rho_{i,n+1}(m) \equiv \sum_{i=1}^{r} B_i \rho_{i,n}(m) = p^n \sigma_n \mod p^{n+2\kappa}\mathbb{Z}_p.$$

Dividing the above equation by p^n, we obtain

$$p\sigma_{n+1}(m) \equiv \sigma_n(m) \mod p^{2\kappa}\mathbb{Z}_p, \tag{3.6}$$

for all $n \in \mathbb{N}$. Iteratively,

$$\sigma_n(m) \equiv p^{2\kappa}\sigma_{n+2\kappa}(m) \equiv 0 \mod p^{2\kappa}\mathbb{Z}_p,$$

for all $n \in \mathbb{N}$. Therefore,

$$\sum_{i=1}^{r} B_i \rho_{i,n}(m) \equiv 0 \mod p^{n+2\kappa}\mathbb{Z}_p \qquad \text{for all } n \in \mathbb{N}. \tag{3.7}$$

From eq. (3.7) the assertion eq. (3.5) for $m = 1$ follows immediately. Now, let $m \in \mathbb{N}$ be arbitrary again. Using Proposition 3.11 gives

$$\sum_{i=1}^{r} B_i x_i^{(m-1)p^{n-1}} \rho_{i,n}(1) \equiv \frac{1}{m} \sum_{i=1}^{r} B_i \rho_{i,n}(m) \mod p^{n+2\kappa}\mathbb{Z}_p. \tag{3.8}$$

Since $\gcd(m, p) = 1$, applying eq. (3.7) on the right-hand side of eq. (3.8) yields the formula eq. (3.5).

Inserting $n = 1$ and $m = 1, ..., r$ into eq. (3.5) yields the following system of linear equations, since $r < p$,

$$\begin{pmatrix} B_1 & B_2 & \cdots & B_r \\ B_1 x_1 & B_2 x_2 & \cdots & B_r x_r \\ \vdots & \vdots & \ddots & \vdots \\ B_1 x_1^{r-1} & B_2 x_2^{r-1} & \cdots & B_r x_r^{r-1} \end{pmatrix} \begin{pmatrix} \rho_{1,1}(1) \\ \rho_{2,1}(1) \\ \vdots \\ \rho_{r,1}(1) \end{pmatrix} \equiv 0 \mod p^{1+2\kappa}\mathbb{Z}_p^r.$$

The determinant of the above Vandermonde matrix is given by

$$\det \begin{pmatrix} B_1 & B_2 & \cdots & B_r \\ B_1 x_1 & B_2 x_2 & \cdots & B_r x_r \\ \vdots & \vdots & \ddots & \vdots \\ B_1 x_1^{r-1} & B_2 x_2^{r-1} & \cdots & B_r x_r^{r-1} \end{pmatrix} = \Big(\prod_{i=1}^{r} B_i\Big) \times \prod_{1 \le k < \ell \le r} (x_k - x_\ell) \not\equiv 0 \mod p\mathbb{Z}_p.$$

Hence, the determinant is invertible mod p, since $x_k - x_\ell$ is a p-adic unit for all $k \neq \ell$. Consequently, $(\rho_{i,1}(1))_{i=1,...,r} \equiv 0 \mod p^{1+2\kappa}\mathbb{Z}_p^r$. In other words, $\kappa \geq 1 + 2\kappa$, which is the desired contradiction. We conclude that all $x_1, ..., x_r$ are roots of unity in $\mathbb{Z}_p$. $\square$

The following corollary summarizes our results so far and contains the core statement of Theorem 1.2.

Corollary 3.13 *Let $V \in \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$, $V(z) \neq 0$, be the generating series of the underlying 2-sequence $(a_n)_{n\in\mathbb{N}} = ([V(z)]_n)_{n\in\mathbb{N}}$, representing a rational function $F \in K(z)$. Then there is an integer $N \in \mathbb{N}$ and coefficients $A_i \in \frac{1}{N}\mathbb{Z}\left[D^{-1}\right]$ for $i = 1, ..., N$ such that*

$$F(z) = \sum_{i=1}^{N} \frac{A_i \zeta^i z}{1 - \zeta^i z},$$

where ζ is a appropriate primitive N-th root of unity.

Proof. By Theorem 3.2 the coefficients $a_n = [V(z)]_n$ of V are given by the power sums $a_n = \sum_{i=1}^{r} A_i \alpha_i^n$, for fixed $r \in \mathbb{N}$, where $A_i \in \mathbb{Q}^\times$ and where the $\alpha_i \in \overline{\mathbb{Q}}^\times$ are distinct algebraic numbers. As mentioned at the beginning of this section, we may assume $\alpha_i \in K$ for all i. Now, choose a prime $p \in \mathbb{Z}$ such that

(i) p is unramified in $K|\mathbb{Q}$ and splits completely,

(ii) α_i, A_i and $\alpha_k - \alpha_\ell$ are p-adic units for all $i = 1, ..., r$ and $k \neq \ell$,

(iii) $\max\{r, 2\} < p$.

This choice of p is possible by Theorem 3.8. Therefore, we have $K_\mathfrak{p} \cong \mathbb{Q}_p$ and $\mathcal{O}_\mathfrak{p} \cong \mathbb{Z}_p$ for all prime ideals $\mathfrak{p} \subset \mathcal{O}$ dividing (p). Hence, $\mathcal{O}_p$ may be identified with $\prod_{\mathfrak{p}|(p)} \mathbb{Z}_p$. Since $\mathrm{Fr}_\mathfrak{p} = \mathrm{id}_K$, the local 2-function condition for p then reads

$$\sum_{i=1}^{r} A_i \left(\alpha_i^{mp^n} - \alpha_i^{mp^{n-1}}\right) \equiv 0 \mod p^{2n}\mathcal{O}_p,$$

for all $m, n \in \mathbb{N}$. For $B_i = \iota_\mathfrak{p}(A_i)$ and $x_i = \iota_\mathfrak{p}(\alpha_i)$ for $\mathfrak{p} \mid (p)$, Theorem 3.12 states that α_i are all roots of unity. In particular, the coefficients lie in a Galois subfield of K, which is abelian over $\mathbb{Q}$. Choose an appropriate primitive N-th root of unity ζ and a bijection $\nu\colon \{1, ..., N\} \to \{1, ..., N\}$, such that $\alpha_i = \zeta^{\nu(i)}$ for all $i \in \{1, .., N\}$. W. l. o. g., we may assume $A_i \in \mathbb{Q}$ (zeros are allowed) and

$$a_n = \sum_{i=1}^{N} A_i \zeta^{in}.$$

We observe that the coefficients a_n are in $\mathcal{O}\left[D^{-1}\right] \cap \mathbb{Q}(\zeta)$. By assumption, we have

$$\begin{pmatrix} \zeta & \zeta^2 & \cdots & \zeta^{N-1} & 1 \\ \zeta^2 & \zeta^4 & \cdots & \zeta^{2(N-1)} & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \zeta^{N-1} & \zeta^{(N-1)2} & \cdots & \zeta^{(N-1)^2} & 1 \\ 1 & 1 & \cdots & 1 & 1 \end{pmatrix} \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_{N-1} \\ A_N \end{pmatrix} \in \mathcal{O}\left[D^{-1}\right]^N.$$

The above matrix is invertible in $\mathbb{Q}(\zeta)$ with inverse

$$\left(\zeta^{ij}\right)^{-1}_{\substack{i=1,\dots,N \\ j=1,\dots,N}} = \frac{1}{N} \cdot \left(\zeta^{-ij}\right)_{\substack{i=1,\dots,N \\ j=1,\dots,N}}.$$

Therefore, $A_i \in \frac{1}{N}\mathcal{O}\left[D^{-1}, \zeta\right] \cap \mathbb{Q} = \frac{1}{N}\mathbb{Z}\left[D^{-1}\right]$ for all $i = 1, ..., N$. □

An obvious consequence of Corollary 3.13 is that the coefficients of a given V are *periodic* (as defined below) with the periodicity being a positive integer P_V dividing the number N. What remains to show is the simple fact that a minimal such N is given by P_V. This is the statement of Proposition 3.15.

Definition 3.14 (Periodicity) Let $V \in \overline{\mathcal{S}}^2_{\text{rat}}(K|\mathbb{Q})_{\text{fin}} \setminus \{0\}$. The *periodicity* P_V of V is given by the periodicity of the coefficients of its Maclaurin series. More precisely, $P_V \in \mathbb{N}$ is given by

$$P_V = \min\{N \in \mathbb{N} \,|\, [V(z)]_n = [V(z)]_{n+N} \text{ for all } n \in \mathbb{N}\}.$$

Note that the existence of P_V is ensured by Corollary 3.13. Furthermore, $\pi\colon \overline{\mathcal{S}}^2_{\text{rat}}(K|\mathbb{Q})_{\text{fin}} \to \mathbb{N}_0$ denotes the map given by $\pi(V) = P_V$, if $V \neq 0$, and $\pi(0) = 0$. For $N \in \mathbb{N}_0$, we denote by $\overline{\mathcal{S}}_N$ ($\mathcal{S}_N$, resp.) the preimage of N under π (the intersection of the preimage of N under π and $\mathcal{S}^2_{\text{rat}}(K|\mathbb{Q})_{\text{fin}}$, resp.), i.e.

$$\overline{\mathcal{S}}_N := \pi^{-1}(N) \subset \overline{\mathcal{S}}^2_{\text{rat}}(K|\mathbb{Q})_{\text{fin}} \quad \text{and} \quad \mathcal{S}_N := \pi^{-1}(N) \cap \mathcal{S}^2_{\text{rat}}(K|\mathbb{Q})_{\text{fin}}.$$

Proposition 3.15 *Let $V \in \overline{\mathcal{S}}^2_{\text{rat}}(K|\mathbb{Q})_{\text{fin}} \setminus \{0\}$ and let $P_V = \pi(V)$ be the periodicity of V, i.e. $V \in \overline{S}_{P_V}$. Then $[V(z)]_n \in K \cap \mathbb{Q}(\zeta_{P_V})$ and, for an appropriate P_V-th primitive root of unity ζ_{P_V}, there are $A_j \in \mathbb{Q}$, $1 \leq j \leq P_V$, such that*

$$A_1 \neq 0 \quad \textit{and} \quad V(z) = \frac{z}{1 - z^{P_V}} \sum_{i=0}^{P_V - 1} a_{i+1} z^i, \quad \textit{and} \quad a_i = \sum_{j=1}^{P_V} A_j \zeta^{ij}.$$

Furthermore, the map $\pi\colon \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q}) \to \mathbb{N}_0$ *is surjective.*

Proof. By Theorem 1.2, there is an $N \in \mathbb{N}$ and a primitive N-th root of unity and suitable coefficients A_i, $1 \leq i \leq N$ such that

$$V(z) = \sum_{i=1}^{N} \frac{A_i \zeta^i z}{1 - \zeta^i z}. \tag{3.9}$$

From this representation of V, one immediately sees $P_V \leq N$. Let $\hat{N}$ denote the minimum of the set of all $N \in \mathbb{N}$, such that V permits a representation given by eq. (3.9). In particular, $\hat{N} \leq P_V$. Assume that all A_i (which depend on $\hat{N}$) with $\gcd(i, \hat{N}) = 1$ are vanishing. In that case, V has a representation given by eq. (3.9) with $N \leq \hat{N}$, violating the minimality of $\hat{N}$. Therefore, we may assume that at least one A_i does not vanish for $\gcd(i, \hat{N}) = 1$. This implies by the representation given in eq. (3.9) that V has a pole of order 1 at an $\hat{N}$-th primitive root of unity, say $\zeta_{\hat{N}}$. Therefore, we may assume $A_1 \neq 0$. Since V has periodicity P_V, we can write

$$V(z) = \sum_{i=1}^{\infty} a_i z^i = \sum_{i=1}^{P_V} a_i \sum_{k=0}^{\infty} z^{i+P_V k} = \sum_{i=1}^{P_V} a_i z^i \sum_{k=0}^{\infty} z^{P_V k} = \frac{z}{1 - z^{P_V}} \sum_{i=0}^{P_V - 1} a_{i+1} z^i.$$

This shows all singularities of V to be roots of the polynomial $1 - z^{P_V}$. Therefore, $\zeta_{\hat{N}}$ is a P_V-th root of unity and hence, $\hat{N} \leq P_V$. We conclude $\hat{N} = P_V$. For the surjectivity of π recall the map $\varepsilon_k^{(2)}\colon \mathcal{S}^2(K|\mathbb{Q}) \to \mathcal{S}^2(K|\mathbb{Q})$ for $k \in \mathbb{N}$ from eq. (2.15). Now, take $N \in \mathbb{N}$, and let $V(z) = \dfrac{z}{1-z} = \displaystyle\sum_{k=1}^{\infty} z^k \in \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$. Then, in particular, $\varepsilon_N^{(2)} V \in \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$, and

$$\pi\left(\varepsilon_N^{(2)}\left(V(z)\right)\right) = \pi\left(\frac{N^2 z^N}{1 - z^N}\right) = N.$$

Hence, π is surjective. □

3.3 Algebraic Generators of $\mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$ and Rational Super Congruences

Proposition 3.16 *(i) $V \in \mathcal{S}_N$ if and only if V has only poles at N-th roots of unity and at least one pole at a primitive N-th root of unity.*

(ii) Let $N, M \in \mathbb{N}$ with $\gcd(N, M) = 1$ and $V \in \mathcal{S}_N$, $W \in \mathcal{S}_M$. Then $V \odot W \in \mathcal{S}_{MN}$.

(iii) Let $\ell \in \mathbb{N}$ and $V \in \mathcal{S}_N$, then $\varepsilon_\ell V \in \mathcal{S}_{\ell N}$.

(iv) Let $k, N \in \mathbb{N}$ and $V \in \mathcal{S}_N$ and write $[V(z)]_n = \sum_{i=1}^{N} A_i \zeta_N^{in}$ for suitable coefficients A_i, for $i = 1, ..., N$, and a primitive N-th root of unity ζ_N (as in Proposition 3.15). If there is a $j \in \left\{1, ..., \frac{N}{\gcd(k,N)}\right\}$ with $\gcd\left(j, \frac{N}{\gcd(k,N)}\right) = 1$, such that

$$\sum_{\nu=0}^{\gcd(k,N)-1} A_{j+N\nu/\gcd(k,N)} \neq 0,$$

then $\mathscr{C}_k V \in \mathcal{S}_{N/\gcd(N,k)}$. In particular, if $\gcd(k, N) = 1$, then $\mathscr{C}_k V \in \mathcal{S}_N$.

(v) For $M, N \in \mathbb{N}$ with $M \neq N$ and $V \in \mathcal{S}_M$ and $W \in \mathcal{S}_N$. Then V and W are $\mathbb{Q}$-linear independent. In particular, $\overline{\mathcal{S}}^2_{\mathrm{rat}}(K|\mathbb{Q})$ is an infinite dimensional vector space over $\mathbb{Q}$.

Proof. (i) This has been proven within the proof of Proposition 3.15.

(ii) Write $[V(z)]_n = a_n = \sum_{i=1}^{N} A_i \zeta_N^{in}$ and $[W(z)]_n = b_n = \sum_{j=1}^{M} B_j \zeta_M^{jn}$, where we identify $\zeta_N = \exp\left(\frac{2\pi \mathrm{i}}{N}\right)$ and $\zeta_M = \exp\left(\frac{2\pi \mathrm{i}}{M}\right)$, and let A_i, B_j, $1 \leq i \leq N$ and $1 \leq j \leq M$, suitable rational coefficients (*beware!* $\mathrm{i} \neq i$). Then, for $\zeta_{MN} = \exp\left(\frac{2\pi \mathrm{i}}{MN}\right)$, we obtain

$$[V \odot W]_n = a_n b_n = \sum_{i=1}^{N} \sum_{j=1}^{M} A_i B_j \zeta_{MN}^{(iM+jN)n}.$$

By the same argument as in the proof of Proposition 3.15 there is an $1 \leq \hat{\imath} \leq N$ and a $1 \leq \hat{\jmath} \leq M$ with $\gcd(\hat{\imath}, N) = \gcd(\hat{\jmath}, M) = 1$ and $A_{\hat{\imath}} \neq 0 \neq B_{\hat{\jmath}}$. The assumption $\gcd(M, N) = 1$ implies $\gcd(MN, \hat{\imath}M + \hat{\jmath}N) = 1$. (Indeed, let p be a prime dividing MN. Since $\gcd(M, N) = 1$, this means $p|M$ or $p|N$. Assume w. l. o. g. $p|M$, then $p \nmid \hat{\imath}M + \hat{\jmath}N$, since $p \nmid \hat{\jmath}N$. Hence $\gcd(MN, \hat{\imath}M + \hat{\jmath}N) = 1$). Therefore, by part *(i)*, $\pi(V \odot W) = MN$.

(iii) This is obvious.

(iv) Write $\tilde{k} = \frac{k}{\gcd(k,N)}$ and $\tilde{N} = \frac{N}{\gcd(k,N)}$ and let ζ_k ($\zeta_{\tilde{N}}$, resp.) denote a primitive k-th ($\tilde{N}$-th, resp.) root of unity. Then

$$\mathscr{C}_k V(z) = \sum_{i=1}^{k} V\left(\zeta_k^i z^{1/k}\right) = \sum_{i=1}^{k} \sum_{n=1}^{\infty} a_n \zeta_k^{in} z^{n/k}$$

$$
\begin{aligned}
&= \sum_{n=1}^{\infty} \left[\sum_{i=1}^{k} \sum_{j=1}^{N} A_j \zeta_N^{jn} \zeta_k^{in} \right] z^{n/k} \\
&= \sum_{n=1}^{\infty} z^n \sum_{j=1}^{N} A_j \zeta_N^{jkn} = \sum_{n=1}^{\infty} z^n \sum_{j=1}^{N} A_j \zeta_{\tilde{N}}^{j\tilde{k}n} \\
&= \sum_{n=1}^{\infty} z^n \sum_{j=1}^{\tilde{N}} \sum_{\nu=0}^{\gcd(k,N)-1} A_{j+\tilde{N}\nu} \zeta_{\tilde{N}}^{(j+\tilde{N}\nu)\tilde{k}n} \\
&= \sum_{n=1}^{\infty} z^n \sum_{j=1}^{\tilde{N}} \zeta_{\tilde{N}}^{j\tilde{k}n} \sum_{\nu=0}^{\gcd(k,N)-1} A_{j+\tilde{N}\nu} \\
&= \sum_{n=1}^{\infty} z^n \sum_{j=1}^{\tilde{N}} \tilde{A}_j \zeta_{\tilde{N}}^{j\tilde{k}n}, \quad \text{for } \tilde{A}_j := \sum_{\nu=0}^{\gcd(k,N)-1} A_{j+\tilde{N}\nu}.
\end{aligned}
$$

Now, using part *(i)*, the statement follows.

(v) The functions $V(z)$ and $W(z)$ are $\mathbb{Q}$-linear independent, simply because they can be recognized by their poles, which do not fulfill some $\mathbb{Q}$-linear relation. Since $\pi\colon \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q}) \to \mathbb{N}_0$ is surjective, we have infinitely many $\mathbb{Q}$-linear independent elements in $\mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$. □

For a given $m \in \mathbb{N}$, let ζ_m be a primitive root of unity. Hereafter, we identify $\mathrm{Gal}(\mathbb{Q}(\zeta_m)|\mathbb{Q})$ with $(\mathbb{Z}/m\mathbb{Z})^\times$ via

$$(\mathbb{Z}/m\mathbb{Z})^\times \ni \bar{r} \mapsto (\sigma_r\colon \zeta_m \mapsto \zeta_m^r).$$

Note that the Frobenius conjugacy class $\{\mathrm{Fr}_{\mathfrak{p}} \,|\, \mathfrak{p} \mid (p)\}$ at p consists of one element since the Galois group is abelian. In this case we simply write Fr_p for this element. This Frobenius automorphism Fr_p for an unramified prime $p \in \mathbb{Z}$ in $K|\mathbb{Q}$ is given by $\mathrm{Fr}_p(\zeta) = \zeta^p$.

Since the coefficients of a power series $V \in \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$ are $\mathbb{Q}$-linear combinations of roots of unity, we may assume K to be an abelian number field, therefore, let $K|\mathbb{Q}$ be a number field, such that the Galois group is abelian. Let $V \in S_N = \pi^{-1}(N) \subset \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$. By the *Kronecker-Weber Theorem* (see for instance [25, Thm. 10.1.1]), there is a primitive M-th root of unity, such that K can be embedded in $\mathbb{Q}(\zeta)$. Choose a minimal $M \in \mathbb{N}$ such that $N \mid M$. Then, there is a subgroub $\Gamma \subset \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ such that $K = \mathbb{Q}(\zeta)^\Gamma$ and

$$\mathrm{Gal}(K|\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})/\Gamma.$$

Let $X = \{1, ..., M\}$, then Γ acts on X by $(\sigma_r, \ell) \mapsto \sigma_r(\ell)$ for $(\bar{r}, \ell) \in \Gamma \times X$, where

$\sigma_r(\ell) \equiv r\ell \mod M$. Let X/Γ denote the set of Γ-orbits in X and for $k \in X$ let $\mathrm{Orb}(k) = \{\ell \in X \mid \exists \sigma \in \Gamma : \ell = \sigma k\} \subset X$ denote an element in X/Γ.

Theorem 3.17 *As described above, let $K|\mathbb{Q}$ be an abelian number field, $V \in \mathcal{S}_N$ and $M \in \mathbb{N}$ minimal such that $N \mid M$ and $K \subset \mathbb{Q}(\zeta_M)$, where ζ_M is a primitive M-th root of unity. Then for every $\mathrm{Orb}(k) \in X/\Gamma$ there are unique rational coefficients $A_{\mathrm{Orb}(k)} \in \mathbb{Q}$ such that V can be written as*

$$V(z) = \sum_{\mathrm{Orb}(k) \in X/\Gamma} A_{\mathrm{Orb}(k)} \sum_{i \in \mathrm{Orb}(k)} \frac{\zeta_M^i z}{1 - \zeta_M^i z}. \tag{3.10}$$

Conversely, for given data $K|\mathbb{Q}$ and $M \in \mathbb{N}$, where $K|\mathbb{Q}$ is abelian, such that $K \subset \mathbb{Q}(\zeta_M)$, functions of the form given in eq. (3.10) *are contained in $\overline{\mathcal{S}}^2_{\mathrm{rat}}(K|\mathbb{Q})_{\mathrm{fin}}$ (cf. Definition 2.9).*

Proof. The functions $V_i(z) = \dfrac{\zeta^i z}{1 - \zeta^i z}$, for $i = 1, ..., N$, are $\mathbb{Q}$-linear independent, as explained above. By Theorem 1.2, we have $V(z) = \sum_{i=1}^{N} A_i V_i(z)$ for suitable $A_i \in \mathbb{Q}$. Since $V \in K[\![z]\!]$, we find for all $\sigma_r \in \Gamma$ (set $\sigma_r(z) := z$)

$$\begin{aligned} 0 = V(z) - \sigma_r(V(z)) &= \sum_{i=1}^{N} A_i (V_i(z) - \sigma_r(V_i(z))) \\ &= \sum_{i=1}^{N} A_i (V_i(z) - V_{\sigma_r(i)}(z)) = \sum_{i=1}^{N} \left(A_i - A_{\sigma_r^{-1}(i)} \right) V_i(z). \end{aligned}$$

Since $V_i(z)$ are $\mathbb{Q}$-linearly independent, these coefficients need to satisfy $A_i = A_{\sigma_r^{-1}(i)}$. In other words, for each orbit $\mathrm{Orb}(k) \in X/\Gamma$ we find an $A_{\mathrm{Orb}(k)} \in \mathbb{Q}$ such that $A_i = A_{\mathrm{Orb}(k)}$ for all $i \in \mathrm{Orb}(k)$. Conversely, let $K|\mathbb{Q}$ be an abelian number field with abelian Galois group $\mathrm{Gal}(K|\mathbb{Q})$ and let $M \in \mathbb{N}$ be a natural number such that for an M-th primitive root of unity ζ_M we have $K \subset \mathbb{Q}(\zeta_M)$ (which is possible by the Kronecker-Weber Theorem). Then there is a subgroup $\Gamma \subset \mathrm{Gal}(\mathbb{Q}(\zeta_M)|\mathbb{Q})$ such that $K = \mathbb{Q}(\zeta_M)^\Gamma$. For every orbit $\mathrm{Orb}(k) \in X/\Gamma$, where $X = \{1, ..., M\}$, let $A_{\mathrm{Orb}(k)} \in \mathbb{Q}$ denote a rational number and set

$$V(z) = \sum_{\mathrm{Orb}(k) \in X/\Gamma} A_{\mathrm{Orb}(k)} \sum_{i \in \mathrm{Orb}(k)} \frac{\zeta_M^i z}{1 - \zeta_M^i z}.$$

Since we are allowed to multiply V by an integral constant, we may assume $A_{\mathrm{Orb}(k)} \in \mathbb{Z}$ for all orbits $\mathrm{Orb}(k) \in X/\Gamma$. By the above calculation we immediately obtain $V(z) \in zK[\![z]\!]$. Let $p \in \mathbb{Z}$ be a prime that is unramified in $\mathbb{Q}(\zeta_M)|\mathbb{Q}$. In particular, p is unramified

in $K|\mathbb{Q}$. Let Frob_p denote the Frobenius morphism as defined in Definition 2.2, but with respect to the field extension $\mathbb{Q}(\zeta_M)|\mathbb{Q}$. Then we immediately obtain

$$\mathrm{Frob}_p V(z) - \mathscr{C}_p V(z) = 0 \quad \text{and} \quad V(z) - \varepsilon_p \mathscr{C}_p V(z) \in z\mathcal{O}_p[\![z]\!].$$

Hence, $V \in \overline{\mathcal{S}}^2_{\mathrm{rat}}(K|\mathbb{Q})_{\mathrm{fin}}$. □

Theorem 3.18 *$\overline{\mathcal{S}}^2_{\mathrm{rat}}(\mathbb{Q})_{\mathrm{fin}}$ is an infinite dimensional vector space over $\mathbb{Q}$ with Hamel basis given by the set $\{\delta \log(\Phi_n) \,|\, n \in \mathbb{N}\}$ of logarithmic derivatives of all cyclotomic polynomials. However, for $R = \mathbb{Q}[\varepsilon_k;\, k \in \mathbb{N}]$, $\overline{\mathcal{S}}^2_{\mathrm{rat}}(\mathbb{Q})_{\mathrm{fin}}$ is an R-module of rank 1.*
Note: The calculation in Proposition 2.14 additionally implies

$$\overline{\mathcal{S}}^2_{\mathrm{rat}}(\mathbb{Q})_{\mathrm{fin}} = \overline{\mathcal{S}}^2_{\mathrm{rat}}(\mathbb{Q}).$$

Proof. $\overline{\mathcal{S}}^2_{\mathrm{rat}}(\mathbb{Q})_{\mathrm{fin}}$ is an infinite dimensional vector space over $\mathbb{Q}$ by Proposition 3.16 *(v)*. Let $V \in \overline{\mathcal{S}}^2_{\mathrm{rat}}(\mathbb{Q})_{\mathrm{fin}}$, then there is a constant $C \in \mathbb{N}$ such that $CV \in \mathcal{S}^2_{\mathrm{rat}}(\mathbb{Q})_{\mathrm{fin}}$. Therefore, w. l. o. g. we may assume that $V \in \mathcal{S}_N \subset \mathcal{S}^2_{\mathrm{rat}}(\mathbb{Q})$. For $k \in \{1, ..., N\}$ let $\mathrm{Orb}(k)$ denote the orbit of k in $X = \{1, ..., N\}$ under the group action of $\Gamma = (\mathbb{Z}/N\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$, where ζ denotes a primitive N-th root of unity. Then, by Theorem 3.17, there is for each orbit $\mathrm{Orb}(k) \in X/\Gamma$ a rational number $A_{\mathrm{Orb}(k)} \in \mathbb{Q}$ such that

$$V(z) = \sum_{\mathrm{Orb}(k) \in X/\Gamma} A_{\mathrm{Orb}(k)} \sum_{i \in \mathrm{Orb}(k)} \frac{\zeta^i z}{1 - \zeta^i z}.$$

For given $k \in \{1, ..., N\}$ set $d = \gcd(k, N)$. First we show $\mathrm{Orb}(k) \subset \{1, ..., N\}$ is given by

$$\mathrm{Orb}(k) = \{i \,|\, \gcd(i, N) = d\}. \tag{3.11}$$

The set on the right-hand side of eq. (3.11) is invariant under the action of $(\mathbb{Z}/N\mathbb{Z})^\times$ and is therefore equal to $\mathrm{Orb}(d)$. Conversely, let $k \in \{1, ..., N\}$ and $d = \gcd(k, N)$, and let $x \in \{1, ..., N\}$ such that $\gcd(x, N) = d$. Set $\tilde{k} = \dfrac{k}{d}$, $\tilde{x} = \dfrac{k}{d}$ and $\tilde{N} = \dfrac{N}{d}$, then $\gcd(\tilde{k}, \widetilde{N}) = \gcd(\tilde{x}, \widetilde{N}) = 1$ and therefore, there is an $\tilde{r} \in (\mathbb{Z}/\tilde{N}\mathbb{Z})^\times$ such that

$$\tilde{x} \equiv \tilde{k}\tilde{r} \mod \widetilde{N}. \tag{3.12}$$

Let $r \in \mathbb{Z}/N\mathbb{Z}$ given by

$$r \equiv \tilde{r} + \widetilde{N} \cdot \Pi \mod N, \quad \text{where } \Pi = \prod_{p|N,\, p \nmid \tilde{N}\tilde{r}} p.$$

Then $\gcd(r, N) = 1$: Indeed, suppose there is a prime q dividing $\gcd(r, N)$. If $q \mid \tilde{r}$, it also divides $\widetilde{N}\Pi$. Since $\gcd(\tilde{r}, \widetilde{N}) = 1$, we have $q \mid \Pi$. By definition of Π this implies $q \mid \tilde{r}$, a contradiction. Also, $q \mid \widetilde{N}$ implies $q \mid \tilde{r}$, which is not possible since $\gcd(\tilde{r}, \widetilde{N}) = 1$. Same goes for $q \mid \Pi$, then $q \mid \tilde{r}$ and $q \nmid \tilde{r}$, proving $\gcd(r, N) = 1$. By construction we obtain

$$\begin{aligned} r \cdot k &= (\tilde{r} + \widetilde{N} \cdot \Pi) \cdot \tilde{k} \cdot \gcd(N, k) \\ &\overset{eq.\ (3.12)}{\equiv} \tilde{x} \cdot \gcd(N, k) + \tilde{N} \cdot \gcd(N, k) \cdot \tilde{k} \cdot \Pi \mod N \\ &= x + N \cdot \tilde{k} \cdot \Pi \\ &\equiv x \mod N. \end{aligned}$$

Therefore, $x \in \mathrm{Orb}(k)$. In particular, $\mathrm{Orb}(k) = \mathrm{Orb}(d)$.

Next we compute the basis elements $\displaystyle\sum_{i \in \mathrm{Orb}(d)} \frac{\zeta^i z}{1 - \zeta^i z}$. From eq. (3.11) we then obtain

$$\begin{aligned} \sum_{i \in \mathrm{Orb}(d)} \frac{\zeta^i z}{1 - \zeta^i z} &= \sum_{\substack{i=1,\dots,N \\ \gcd(i,N)=d}} \frac{\zeta^i z}{1 - \zeta^i z} = \sum_{\substack{i=1,\dots,N \\ \gcd(i,N)=d}} -\delta \log(1 - \zeta^i z) \\ &= -\delta \log \prod_{\substack{i=1,\dots,N \\ \gcd(i,N)=d}} (1 - \zeta^i z) = -\delta \log \Phi_d(z) = -\frac{z\Phi_d'(z)}{\Phi_d(z)}. \end{aligned}$$

Note that the basis elements $\dfrac{z\Phi_d'(z)}{\Phi_d(z)}$ do satisfy the local 2-function condition precisely for prime p which do not divide d. We proved in Proposition 2.14 that

$$d\frac{z\Phi_d'}{\Phi_d(z)} \in \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q}),$$

i.e. the factor d is precisely what it takes to lift $\delta \log(\Phi_d(z))$ as an element in $\overline{\mathcal{S}}^2_{\mathrm{rat}}(K|\mathbb{Q})_{\mathrm{fin}}$ to an element in $\mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$. This implies

$$\overline{\mathcal{S}}^2_{\mathrm{rat}}(K|\mathbb{Q})_{\mathrm{fin}} = \overline{\mathcal{S}}^2_{\mathrm{rat}}(K|\mathbb{Q}).$$

Now we show the second part of the assertion, namely, $\overline{\mathcal{S}}^2_{\mathrm{rat}}(K|\mathbb{Q})_{\mathrm{fin}}$ is an R-module of rank 1. Recall $\mathcal{S}_N = \pi^{-1}(N) \subset \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})_{\mathrm{fin}}$. We will show $\mathcal{S}_N \subset R \cdot \dfrac{z}{1-z}$ for all $N \in \mathbb{N}$ by induction. Let $V \in \mathcal{S}_1$, then $[V(z)]_n = [V(z)]_{n+1} \neq 0$ for all $n \in \mathbb{N}$. Therefore, $\dfrac{1}{[V(z)]_1} V(z) = \displaystyle\sum_{n=1}^{\infty} z^n = \frac{z}{1-z}$ and $S_1 \in R \cdot \dfrac{z}{1-z}$. Assume that for $N \in \mathbb{N}$, $N > 1$, we

have $\mathcal{S}_k \subset R \cdot \dfrac{z}{1-z}$ for all $k < N$. Let $V \in \mathcal{S}_N$, then by the first part of the present proof, there are for every divisior d of N, $d|N$, a rational number $A_d \in \mathbb{Q}$ such that

$$V(z) = \sum_{d|N} A_d \frac{z\Phi'_d(z)}{\Phi_d(z)}.$$

Since $\dfrac{z\Phi'_d(z)}{\Phi_d(z)} \in \mathcal{S}_d$ and $\mathcal{S}_k \subset R \cdot \dfrac{z}{1-z}$ for all $k < N$ by the induction hypothesis, we may assume

$$V(z) = \frac{z\Phi'_N(z)}{\Phi_N(z)}.$$

We have

$$\begin{aligned} N\varepsilon_N\left(\frac{z}{1-z}\right) = \frac{Nz^N}{1-z^N} &= -\frac{\delta\left(\prod_{d|N}\Phi_d(z)\right)}{\prod_{d|N}\Phi_d(z)} = -\sum_{d|N}\frac{z\Phi'_d(z)}{\Phi_d(z)} \\ &= -\frac{z\Phi'_N(z)}{\Phi_N(z)} - \sum_{\substack{d|N \\ d<N}} \frac{z\Phi'_d(z)}{\Phi_d(z)}. \end{aligned}$$

Again, by induction hypothesis $\mathcal{S}_k \subset R \cdot \dfrac{z}{1-z}$ for all $k < N$, we therefore find

$$\frac{z\Phi'_N(z)}{\Phi_N(z)} = N\varepsilon_N\left(\frac{z}{z-1}\right) - \sum_{\substack{d|N \\ d<N}} \frac{z\Phi'_d(z)}{\Phi_d(z)} \in R \cdot \frac{z}{1-z}.$$

This completes the proof. □

Corollary 3.19 *We have*

$$\mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q}) \subset \mathcal{S}^\infty(K|\mathbb{Q})_{\mathrm{fin}}.$$

Proof. Let $V \in \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$. We may assume K to be an abelian Galois extension, since all coefficients $a_n = [V(z)]_n$ lie in an abelian Galois extension over $\mathbb{Q}$, as a consequence of Theorem 1.2. By the Kronecker-Weber Theorem, we may also assume $K = \mathbb{Q}(\zeta_d)$, where ζ_d is a primitive d-th root of unity. By Theorem 1.2, there is an $N \in \mathbb{N}$ and a primitive N-th root of unity ζ_N, such that the coefficients a_n is a $\mathbb{Q}$-linear combination of $\{\zeta_N^i \,|\, i \in \{1, ..., N\}\}$, i.e. for suitable $A_i \in \mathbb{Q}$,

$$a_n = \sum_{i=1}^{N} A_i \zeta_N^{in}$$

Then p is an unramified prime over $K|\mathbb{Q}$, if and only if $p \nmid d$. If $p \nmid N$, then p is unramified in $\mathbb{Q}(\zeta_N)$. Therefore, the Frobenius Element $\sigma_p \in \mathrm{Gal}(K|\mathbb{Q})$ of p, inducing Frob_p on K_p, uniquely extends to the Frobenius element $\overline{\sigma}_p \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)|\mathbb{Q})$ of p, which acts on ζ_N by taking the p-th power, i.e. $\overline{\sigma}_p(\zeta_N) = \zeta_N^p$, inducing $\overline{\mathrm{Frob}_p}\colon \mathbb{Q}(\zeta_N)_p \to \mathbb{Q}(\zeta_N)_p$. Therefore,

$$\mathrm{Frob}_p\left(a_n\right) = \mathrm{Frob}_p\left(\sum_{i=1}^{N} A_i \zeta_N^{in}\right) = \sum_{i=1}^{N} A_i \overline{\mathrm{Frob}}_p(\zeta_N)^{in} = \sum_{i=1}^{N} A_i \zeta_N^{ipn} = a_{pn}.$$

In particular, the supercongruence proposed by the s-function property is in fact an equality in this case. For those unramified primes p in $K|\mathbb{Q}$, which divide N (these are finitely many), we have in general $\mathrm{Frob}_p(a_n) \neq a_{pn}$. As an example consider $V(z) = -3\dfrac{z\Phi_3'(z)}{\Phi_3(z)} \in \mathcal{S}^2_{\mathrm{rat}}(\mathbb{Q})$,

$$V(z) = -3\frac{z(1+2z)}{1+z+z^2} = 3\frac{(\zeta_3+\zeta_3^2)z - 2z^2}{1-(\zeta_3+\zeta_3^2)z+z^2} = 3\left(\frac{z\zeta_3}{1-\zeta_3 z} + \frac{z\zeta_3^2}{1-\zeta_3^2 z}\right).$$

Then

$$a_n = 3(\zeta_3^n + \zeta_3^{2n}) = \begin{cases} -3, & \text{if } n \equiv 1 \mod 3, \\ -3, & \text{if } n \equiv 2 \mod 3, \\ 6, & \text{if } n \equiv 0 \mod 3. \end{cases}$$

Therefore, for $3 \nmid n$, $a_{3n} - a_n = 6 + 3 = 9 \equiv 0 \mod 9$, but $9 \neq 0$. □

Chapter 4

Framing of Rational 2-Functions

The results presented in the present chapter are published in [33]. The present is dedicated to prove Theorem 1.4. More precisely, we will prove

Theorem 4.1 *We have*

$$\Phi^+\left(\mathbb{Z}\left[D^{-1}\right]\times\mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})\right)\subset\overline{\mathcal{S}}^3(K|\mathbb{Q})_{\mathrm{fin}},\quad \textit{and}$$
$$\Phi^-\left(\mathbb{Z}\times\mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})\right)\subset\overline{\mathcal{S}}^3(K|\mathbb{Q})_{\mathrm{fin}}.$$

More precisely, let $V\in\mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$ be given by a generating series of a 2-sequence, representing a rational function, of periodicity $N\in\mathbb{N}$ and $\nu\in\mathbb{Z}\left[D^{-1}\right]$ and let $a^+_n=\left[V^{(+,\nu)}(z)\right]_n$ denote the n-th coefficient of $V^{(+,\nu)}(z)$ for all $n\in\mathbb{N}$. Then, for all primes p which are unramified in $K|\mathbb{Q}$ such that $p\nmid N$ and all $n\in\mathbb{N}$ – except for the case in which $p=2$ and $\mathrm{ord}_2(n)=0$ – we have

$$\mathrm{Frob}_p(a^+_n)-a^+_{pn}\equiv 0\mod p^{2(\mathrm{ord}_p(n)+1)-\delta_{2,p}+\max\{0,\mathrm{ord}_p(n)+1-\gamma_p\}}\mathcal{O}_p,$$

where γ_p is given by

$$\gamma_p=\begin{cases}1+\mathrm{ord}_2(N+1), & \textit{if } p=2 \textit{ and } 2\nmid N,\\ 1, & \textit{if } p=3,\\ 0, & \textit{if } p\geq 5.\end{cases}$$

In particular, for all primes $p\geq 5$, which are unramified in $K|\mathbb{Q}$ and do not divide N, we find for all $n\in\mathbb{N}$,

$$\mathrm{Frob}_p(a^+_n)-a^+_{pn}\equiv 0\mod p^{3(\mathrm{ord}_p(n)+1)}\mathcal{O}_p.$$

In Section 4.1, we will define the Framing operator(s) $\Phi^{+/-}$ (cf. Definition 4.9) (Φ^+ and Φ^- differ by a sign convention) in terms of Bell transformations (cf. Definition 4.4), which are introduced by Birmajer, Gil and Weiner in [9], 2018. From the definition it becomes evident that the framing operators $\Phi^{+/-}$ define group actions of the additive group $\mathbb{C}$ on the set of formal power series with coefficients in $\mathbb{C}$ and vanishing constant coefficient. In Section 4.2 we formulate and prove the Integrality of Framing Theorem from [40], which is the statement that $\Phi^{\pm}$ preserve $\mathcal{S}^2(K|\mathbb{Q})$.

In Section 4.3, we give a short survey on the classical Wolstenholme Theorem and prove the generalization Theorem 1.5. As a consequence, we recall the proof of the Jacobsthal-Kazandzidis, which can be considered as a prototype of Theorem 1.4.

In Section 4.5 we give a generalization of the Integrality of Framing Theorem and of Theorem 4.1 with respect to what we call *fractional framing*. We have

Theorem 4.2 *Let $\sigma \in \mathbb{N}$.*

(1) *Integrality of Fractional Framing: Then,*

$$\left(\frac{1}{\sigma}\mathscr{C}_\sigma \circ \Phi^-\right)\left(\left(\frac{1}{\sigma}\mathbb{Z}\right) \times \mathcal{S}^2(K|\mathbb{Q})\right) \subset \mathcal{S}^2(K|\mathbb{Q})$$

and

$$\left(\frac{1}{\sigma}\mathscr{C}_\sigma \circ \Phi^+\right)\left(\left(\frac{1}{\sigma}\mathbb{Z}\left[D^{-1}\right]\right) \times \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})\right) \subset \left(\mathcal{S}^2(K|\mathbb{Q})_{\{2\}} \cap \overline{\mathcal{S}}^2(K|\mathbb{Q})\right).$$

(2) *Improved Integrality of Fractional Framing: Then*

$$\left(\frac{1}{\sigma}\mathscr{C}_\sigma \circ \Phi^{+/-}\right)\left(\left(\frac{1}{\sigma}\mathbb{Z}\right) \times \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})\right) \subset \mathcal{S}^3(K|\mathbb{Q})_{\mathrm{fin}}.$$

More precisely, for a rational 2-function $V \in \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$ of periodicity N and $\nu \in \frac{1}{\sigma}\mathbb{Z}$ and $S = \{p \text{ prim with } p \mid N\} \cup \{2, 3\}$,

$$\widetilde{V}(z) := \frac{1}{\sigma}\left(\mathscr{C}_\sigma\left(\Phi^+(\nu, V)\right)\right) \in \mathcal{S}^3(K|\mathbb{Q})_S.$$

For $\tilde{a}^+_n = \left[\widetilde{V}(z)\right]_n$, $n \in \mathbb{N}$ we have

$$\mathrm{Frob}_p\left(\tilde{a}^+_n\right) - \tilde{a}^+_{pn} \equiv 0 \mod p^{2\,\mathrm{ord}_p(pn)-\delta_{2,p}+\max\{0,\mathrm{ord}_p(pn)-\gamma_p\}}\mathcal{O}_p,$$

where γ_p is equal to $1+\mathrm{ord}_2(N+1)$, 1 and 0, if p is equal to 2, 3 and greater than 3,

respectively. In particular, for unramified $p \geq 5$ in $K|\mathbb{Q}$ with $p \nmid N$, and all $m, r \in \mathbb{N}$,

$$\mathrm{Frob}_p\left(\tilde{a}^+_{mp^{r-1}}\right) - \tilde{a}^+_{mp^r} \equiv 0 \mod p^{3r}\mathcal{O}_p.$$

The proofs of the statements in Theorem 4.2 are analogously to the original proofs.

4.1 Partial Bell Polynomials and Bell Transformations

Let $\mathbb{Q}[\mathfrak{X}]$ be the ring of polynomials in a countable number of indeterminates $\mathfrak{X} = \{X_1, X_2, ...\}$ over $\mathbb{Q}$. The complete exponential Bell polynomials $\{B_n | n \in \mathbb{N}\}$ (named in honor of the mathematician and science fiction writer Eric Temple Bell) are defined by the generating coefficients of $\exp\left(\sum_{n=1}^{\infty} \frac{X_i}{i!} z^i\right)$,

$$\exp\left(\sum_{n=1}^{\infty} \frac{X_i}{i!} z^i\right) =: \sum_{n=1}^{\infty} B_n(\mathfrak{X}) \frac{z^n}{n!}.$$

The (n,k)-th *partial Bell polynomial* (see Definition 4.3) can be implicitly defined as the homogeneous part of degree k of the n-th complete exponential Bell polynomial $B_n \in \mathbb{Q}[\mathfrak{X}]$. For a sequence $x = (x_n)_{n\in\mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$ we write

$$!x = (n! x_n)_{n\in\mathbb{N}}.$$

For a multi-index $\alpha \in \mathbb{C}^r$ ($r \in \mathbb{N}$), the *absolute value of* α is defined by the sum of components of α, i.e. $|\alpha| = \sum_{i=1}^{r} \alpha_i$.

Definition 4.3 (partial Bell polynomials) For $k, n \in \mathbb{N}$, $k \leq n$ let $B_{n,k} \in \mathbb{Q}[\mathfrak{X}]$ be the *(n,k)-th partial Bell polynomial*. $B_{n,k}$ may be defined through the series expansion

$$\frac{1}{k!}\left(\sum_{j=1}^{\infty} X_j \frac{z^j}{j!}\right)^k = \sum_{n=k}^{\infty} B_{n,k}(\mathfrak{X}) \frac{z^n}{n!}.$$

The polynomial $B_{n,k}$ can be written as

$$B_{n,k}(\mathfrak{X}) = n! \sum_{\alpha\in\pi(n,k)} \left(\prod_{i=1}^{n-k+1} \frac{1}{\alpha_i!}\left(\frac{X_i}{i!}\right)^{\alpha_i}\right),$$

where $\pi(n,k)$ denotes the set of multi-indices $\alpha \in \mathbb{N}_0^{n-k+1}$ such that

$$|\alpha| = \sum_{i=1}^{n-k+1} \alpha_i = k \quad \text{and} \quad \sum_{i=1}^{n-k+1} i\alpha_i = n.$$

Note that $B_{n,k}(\mathfrak{X})$ is in fact a polynomial in the variables $X_1, ..., X_{n-k+1}$ for all $n, k \in \mathbb{N}$, $k \leq n$.

It follows immediately from the definition that the (n,k)-th partial Bell polynomial is homogeneous of degree k and of weight n. Let $\lambda \in \mathbb{C}$ be a (complex) scalar. Then homogeneity and weight follows respectively,

$$\begin{aligned} B_{n,k}(\lambda\mathfrak{X}) &= n! \sum_{\alpha\in\pi(n,k)} \left(\prod_{i=1}^{n-k+1} \frac{1}{\alpha_i!} \left(\frac{\lambda X_i}{i!} \right)^{\alpha_i} \right) \\ &= n! \sum_{\alpha\in\pi(n,k)} \left(\lambda^{|\alpha|} \prod_{i=1}^{n-k+1} \frac{1}{\alpha_i!} \left(\frac{X_i}{i!} \right)^{\alpha_i} \right) = \lambda^k B_{n,k}(\mathfrak{X}) \quad \text{(homogeneity)}, \end{aligned} \tag{4.1}$$

and

$$\begin{aligned} B_{n,k}\left(\left(\lambda^i X_i\right)_{i\in\mathbb{N}} \right) &= n! \sum_{\alpha\in\pi(n,k)} \left(\prod_{i=1}^{n-k+1} \frac{1}{\alpha_i!} \left(\frac{\lambda^i X_i}{i!} \right)^{\alpha_i} \right) \\ &= n! \sum_{\alpha\in\pi(n,k)} \left(\lambda^{\sum_{i=1}^{n-k+1} i\alpha_i} \prod_{i=1}^{n-k+1} \frac{1}{\alpha_i!} \left(\frac{X_i}{i!} \right)^{\alpha_i} \right) = \lambda^n B_{n,k}\left(\mathfrak{X}\right) \quad \text{(weight)}. \end{aligned} \tag{4.2}$$

In [9], *Bell transformations of sequences* were introduced to tackle a wide variety of problems in enumerative combinatorics. These transformations come along with functional equations satisfied by the corresponding generating power series. To us, Bell transformations come in handy to define the framing operators $\Phi^{+/-}$ and use the corresponding functional equations.

Definition 4.4 (Bell transformation) Let $a, b, c, d \in \mathbb{C}$ be fixed. Then the *Bell transformation* associated to (a, b, c, d) is a map $\mathscr{Y}_{a,b,c,d}\colon \mathbb{C}^{\mathbb{N}} \to \mathbb{C}^{\mathbb{N}}$: For a sequence $x = (x_n)_{n\in\mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$ then $y = (y_n)_{n\in\mathbb{N}} = \mathscr{Y}_{a,b,c,d}(x)$ is given by

$$y_n = \frac{1}{n!} \sum_{k=1}^{n} \left[\prod_{j=1}^{k-1} (an + bk + cj + d) \right] B_{n,k}(!x) \quad \text{for all } n \geq 1.$$

The following results (Theorem 4.5, Corollary 4.6, Theorem 4.7) on Bell transforma-

tions are from [9].

Theorem 4.5 (cf. Theorem 2.1 in [9]) *Let $x, y \in \mathbb{C}^{\mathbb{N}}$ such that $y = \mathscr{Y}_{a,b,c,d}(x)$. Assume $c \neq 0$. Then, for every $n \in \mathbb{N}$ and for any $\lambda \in \mathbb{C}$, we have*

$$\sum_{k=1}^{n} \left[\prod_{j=1}^{k-1} (\lambda - dj + d) \right] B_{n,k}(!y) = \sum_{k=1}^{n} \left[\prod_{j=1}^{k-1} (an + bk + cj + d + \lambda) \right] B_{n,k}(!x).$$

Corollary 4.6 (cf. Corollary 2.3 in [9]) *Let $x, y \in \mathbb{C}^{\mathbb{N}}$ be sequences such that $y = \mathscr{Y}_{a,b,c,d}(x)$.*

(i) If $c \neq 0$, then

$$\mathscr{Y}^{-1}_{a,b,c,d} = \frac{b+c}{c} \mathscr{Y}_{-a,0,-d,-b-c} - \frac{b}{c} \mathscr{Y}_{-a,0,-d,-b}.$$

In particular,

$$\mathscr{Y}^{-1}_{a,0,c,d} = \mathscr{Y}_{-a,0,-d,-c} \quad \text{and} \quad \mathscr{Y}^{-1}_{a,-c,c,d} = \mathscr{Y}_{-a,0,-d,c}.$$

(ii) If $c = 0$, then

$$\mathscr{Y}^{-1}_{a,0,0,d} = \mathscr{Y}_{-a,0,-d,0}.$$

Theorem 4.7 (cf. Corollary 3.6 in [9]) *Let $x, y \in \mathbb{C}^{\mathbb{N}}$ be sequences such that $y = \mathscr{Y}_{a,b,c,d}(x)$ and let $X(z) = \mathcal{G}(x) = \sum_{n=1}^{\infty} x_n z^n$ and $Y(z) = \mathcal{G}(y) = \sum_{n=1}^{\infty} y_n z^n$ denote the generating power series of the sequences x and y. Then:*

(i) If $c \neq 0$ and $d \neq 0$, $X\left(z(1 + dY(z))^{a/d}\right) = \frac{1}{c}\left[1 - (1 + dY(z))^{-c/d}\right](1 + dY(z))^{-b/d}$.

(ii) If $c = 0$ and $d \neq 0$, $X\left(z(1 + dY(z))^{a/d}\right) = \log\left((1 + dY(z))^{1/d}\right)(1 + dY(z))^{-b/d}$.

(iii) If $c \neq 0$ and $d = 0$, $X\left(ze^{aY(z)}\right) = \frac{1}{c}\left[1 - e^{-cY(z)}\right]e^{-bY(z)}$.

(iv) If $c = d = 0$, $X\left(ze^{aY(z)}\right) = Y(z)e^{-bY(z)}$.

Corollary 4.8 is not stated in [9], although it follows from Theorem 4.5.

Corollary 4.8 (Composition of Bell Transformations) *Let $a, b, c, d, e, f \in \mathbb{C}$ such that either $c \neq 0$ or $b = c = 0$. Then*

$$\mathscr{Y}_{e,0,-d,f} \circ \mathscr{Y}_{a,b,c,d} = \mathscr{Y}_{a+e,b,c,f}.$$

Proof. Let $c \neq 0$ and let $x, y, \hat{y} \in \mathbb{C}^{\mathbb{N}}$ be sequences related by

$$y = \mathscr{Y}_{a,b,c,d}(x) \quad \text{and} \quad \hat{y} = \mathscr{Y}_{e,0,-d,f}(y).$$

In particular, we have

$$n!\hat{y}_n = \sum_{k=1}^{n} \left[\prod_{j=1}^{k-1} (en - dj + f) \right] B_{n,k}(!y).$$

By Theorem 4.5 we therefore find for $\lambda = en - d + f$

$$\hat{y}_n = \frac{1}{n!} \sum_{k=1}^{n} \left[\prod_{j=1}^{k-1} ((a+e)n + bk + cj + f) \right] B_{n,k}(!x).$$

This is the desired formula $\mathscr{Y}_{e,0,-d,f} \circ \mathscr{Y}_{a,b,c,d} = \mathscr{Y}_{a+e,b,c,f}$.
Let $b = c = 0$. Then we have $\mathscr{Y}_{a,0,0,d}^{-1} = \mathscr{Y}_{-a,0,-d,0}$ by Corollary 4.6 *(ii)*. Hence, by the previous case, we may compute

$$\mathscr{Y}_{a+e,0,0,f} \circ \mathscr{Y}_{a,0,0,d}^{-1} = \mathscr{Y}_{a+e,0,0,f} \circ \mathscr{Y}_{-a,0,-d,0} = \mathscr{Y}_{e,0,-d,f}.$$

Equivalently, $\mathscr{Y}_{e,0,-d,f} \circ \mathscr{Y}_{a,0,0,d} = \mathscr{Y}_{a+e,0,0,f}$. □

Next, we will define *framing* as a map of power series.

Definition 4.9 (Framing operators $\Phi^{+/-}$) Define the framing operator $\Phi^{+}\colon \mathbb{C} \times z\mathbb{C}[\![z]\!] \to \mathbb{C}[\![z]\!]$, $(\nu, V) \mapsto V^{(\nu,+)}(z)$ by the following composition

$$\Phi^{+}(\nu, -)\colon z\mathbb{C}[\![z]\!] \xrightarrow{\int} z\mathbb{C}[\![z]\!] \xrightarrow{([-]_n)_{n\in\mathbb{N}}} \mathbb{C}^{\mathbb{N}} \xrightarrow{\mathscr{Y}_{\nu,0,0,0}} \mathbb{C}^{\mathbb{N}} \xrightarrow{\mathcal{G}} z\mathbb{C}[\![z]\!] \xrightarrow{\delta} z\mathbb{C}[\![z]\!].$$

Also, define $\Phi^{-}\colon \mathbb{C} \times z\mathbb{C}[\![z]\!] \to z\mathbb{C}[\![z]\!]$, $(\nu, V) \mapsto \Phi^{-}(\nu, V)$ by twisting sign convolution $z \mapsto (-1)^{\nu} z$, i.e.

$$\Phi^{-}(\nu, V) = V^{(+,\nu)}\left((-1)^{\nu} z\right).$$

Proposition 4.10 *Let $V \in z\mathbb{C}[\![z]\!]$ and write $V^{(\nu,+)} := \Phi^{+}(\nu, V)$ and $V^{(\nu,-)} := \Phi^{-}(\nu, V)$. Furthermore, write $a_n^{+} := \left[V^{(+,\nu)}(z)\right]_n$ and $a_n^{-} := \left[V^{(-,\nu)}(z)\right]_n$. Then*

(i) Φ^{+} and Φ^{-} define group actions of the additive group $(\mathbb{C}, +)$ on the set $z\mathbb{C}[\![z]\!]$ of formal power series with vanishing zeroth coefficient. In particular, we have

$$\Phi^{+/-}(0, -) = \mathrm{id} \quad \textit{and} \quad \Phi^{+/-}(\nu, -) \circ \Phi^{+}(\mu, -) = \Phi^{+/-}(\nu + \mu, -).$$

(*ii*) *The following functional equations are satisfied*

$$\int V^{(\nu,+)}\left(z\exp(-\nu\int V(z))\right)=\int V(z), \tag{4.3}$$

and

$$\int V^{(\nu,-)}\left(z\left(-\exp(-\int V(z))^{\nu}\right)\right)=\int V(z). \tag{4.4}$$

(*iii*) *For the coefficients* a_n^+ *and* a_n^- *we have for all* $n\in\mathbb{N}$,

$$a_n^+=\frac{1}{\nu}\left[\frac{\exp(\nu n\int V(z))}{z^n}\right]_0, \tag{4.5}$$

and consequently by definition,

$$a_n^-=(-1)^{\nu n}a_n^+=\frac{(-1)^{\nu n}}{\nu}\left[\frac{\exp(\nu n\int V(z))}{z^n}\right]_0. \tag{4.6}$$

Proof. The group action property for Φ^+ follows immediately from Corollary 4.8 by setting $a=\nu$, $e=\mu$ and $b=c=d=f=0$. Since the partial Bell polynomials $B_{n,k}(\mathfrak{X})$, $k\leq n$, have weight n , it is obvious that the additional sign change does not effect the group action property of Φ^+, i.e. Φ^+ passes its group action property on to Φ^-. This proves (i).

The functional equation eq. (4.3) is given by [9, Cor. 4 (iv)]. By using the *Lagrange Inversion Formula* (LIF) given below, we find the formulas given in eq. (4.5) and eq. (4.6). For further reference of the LIF, see for instance [17], [28].

Theorem 4.11 (LIF) *Let* $F,H\in z\mathbb{C}[\![z]\!]$ *and* $G\in z\mathbb{C}[\![z]\!]$ *the compositional inverse to* F*, i.e.* $F(G(z))=G(F(z))=z$*. Then*

$$[H(G(z))]_n=\frac{1}{n}\left[\frac{\delta H(z)}{F(z)^n}\right]_0. \tag{4.7}$$

Of course, eq. (4.6) follows from eq. (4.5) by definition. Therefore, it is sufficient to proof eq. (4.5). For

$$F(z)=z\exp(-\nu\int V(z))$$

let $G\in z\mathbb{C}[\![z]\!]$ be the compositional inverse to F, $F(G(z))=G(F(z))=z$. Hence,

$$\int V^{(\nu,+)}(z)=\int V(G(z))$$

Using eq. (2.3), we have

$$a_n^+ = \left[V^{(+,\nu)}(z)\right]_n = n\left[\int V^{(+,\nu)}(z)\right]_n .$$

Then, Theorem 4.11 gives

$$a_n^+ = \left[\frac{V(z)}{z^n}\exp(\nu n \int V(z))\right]_0 .$$

Since $[-]_0 \circ \delta \equiv 0$ (compare with eq. (2.1)) we obtain

$$0 = \left[\delta\left(\frac{\exp(\nu n \int V(z))}{z^n}\right)\right]_0 = n \cdot \left[\frac{\nu V(z) - 1}{z^n}\exp(\nu n \int V(z))\right]_0 . \tag{4.8}$$

Therefore,

$$a_n^+ = \left[\frac{V(z)}{z^n}\exp(\nu n \int V(z))\right]_0 = \frac{1}{\nu}\left[\frac{\exp(\nu n \int V(z))}{z^n}\right]_0 ,$$

proving (*iii*).

Let $\widetilde{V}(z) \in z\mathbb{C}[\![z]\!]$ be the power series satisfying the functional equation eq. (4.4), i.e.

$$\int \widetilde{V}\left(z\left(-\exp(-\int V(z))^\nu\right)\right) = \int V(z),$$

and write $\tilde{a}_n := \left[\widetilde{V}(z)\right]_n$ for all $n \in \mathbb{N}$. Then, by an analogue calculation as for a_n^+ we find

$$\tilde{a}_n = \frac{(-1)^{\nu n}}{\nu}\left[\frac{\exp(\nu n \int V(z))}{z^n}\right]_0 = a_n^-, \quad \text{for all } n \in \mathbb{N}.$$

Hence, $\widetilde{V} = V^{(-,\nu)}$, proving (*ii*). □

As mentioned above, the original framing transformation of power series can be considered as the mirror of the framing of knots in 3-manifolds on local open string mirror symmetry. The framing operator given in [40] was defined by the functional equation for eq. (4.4), induced by Φ^-. The proof of the *Integrality of Framing* – that is Theorem 4.12 for Φ^- – is given in [40, Thm. 8]. The point is, Φ^- satisfies the local 2-function property even at $p = 2$ due to the sign convention, which is not preserved by Φ^+. However, Φ^- does not seem to preserve 3-integrality at $p = 2$ even for $V \in \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$. Recall, the coefficients of such a rational $V \in \mathcal{S}^2$ are periodic, as a consequence of Theorem 3.1. Furthermore, 3-integrality also fails for $p = 3$ by a 3-order of 1 and for all primes p that ramify in $K|\mathbb{Q}$ and which divide the periodicity of V. There are several reasons listed

here:

(1) For a given rational function $V \in \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$ let N denote the periodicity of V and let S be the set of primes dividing N. As stated in Corollary 3.19, we obtain that V is also an element in $\mathcal{S}^\infty(K|\mathbb{Q})_S$. Therefore, for an unramified prime p in $K|\mathbb{Q}$, which does not divide N, we have the equality $\mathrm{Frob}_p\left([V(z)]_n\right) = [V(z)]_{pn}$, while generally, $\mathrm{Frob}_q\left([V(z)]_n\right) \neq [V(z)]_{qn}$ for all primes $q \mid N$.

(2) The Wolstenholme type congruences Theorem 4.15 does only permit weaker p-adic estimations for $p = 2, 3$, than for $p \geq 5$. Also, it depends on a periodic sequence $(a_n)_{n\in\mathbb{N}} \in K^{\mathbb{N}}$ of periodicity, say, $N \in \mathbb{N}$ (effectively, this is the same N as above and $a_n = [V(z)]_n$). Because of that, these congruences are additionally weaker for those p dividing N by a p-order of $\max\{\mathrm{ord}_2(N), \mathrm{ord}_2(N+2)\}$, or $\mathrm{ord}_p(N)$ if p equals to 2, or greater than 2, respectively.

(3) The p-adic approximation of e^p up to the p-power of 3 gives an additional summand for the primes 2 and 3.

$$e^p \equiv \begin{cases} 1 + p + \dfrac{p^2}{2} \mod p^3, & \text{for } p \geq 5, \\ 1 + p + \dfrac{p^2}{2} + \dfrac{p^3}{6} \mod p^3, & \text{for } p \in \{2, 3\}. \end{cases}$$

Since $\Phi^{+/-}$ are implicitly defined by concatenation with the exponential power series exp, illustrated by the functional equations eq. (4.3) and eq. (4.4), this contributes to the failure of the 3-itegrality at $p \in \{2, 3\}$.

4.2 Integrality of Framing for 2-Functions

In this section we will proof that the Framing operator Φ^- preserves integrality and defines a group action of the group $(\mathbb{Z}, +)$ on $\mathcal{S}^2(K|\mathbb{Q})$. Fix an embedding $K \hookrightarrow \mathbb{C}$.

Theorem 4.12 (Integrality of Framing Theorem) *The two maps*

$$\Phi^+ \colon \mathbb{Z}\left[D^{-1}\right] \times \mathcal{S}^2(K|\mathbb{Q})_{\{2\}} \to \mathcal{S}^2(K|\mathbb{Q})_{\{2\}}, \quad (\nu, V(z)) \mapsto V^{(+,\nu)}(z), \tag{4.9}$$

and

$$\Phi^- \colon \mathbb{Z} \times \mathcal{S}^2(K|\mathbb{Q}) \to \mathcal{S}^2(K|\mathbb{Q}), \quad (\nu, V(z)) \mapsto V^{(-,\nu)}(z) \tag{4.10}$$

are well defined. Furthermore, Φ^+ defines a faithful group action of the additive group $\left(\mathbb{Z}\left[D^{-1}\right], +\right)$ on $\mathcal{S}^2(K|\mathbb{Q})_{\{2\}}$, while Φ^- defines a faithful group action of the additive

group $(\mathbb{Z},+)$ *on* $\mathcal{S}^2(K|\mathbb{Q})$.

Proof. The proof is due to the work of A. Schwarz, V. Vologodsky and J. Walcher in [40]. An analogue statement for *fractional framing* is given by Theorem 4.23, from which Theorem 4.12 follows by setting $\sigma = \rho = 1$ therein. Nonetheless, for the sake of completeness, we recall the proof. Eq. (4.9) follows from *Case 1* below. *Case 2* and *Case 3* are dedicated to $p = 2$.

Case 1: $p \geq 3$. Let p be a prime number unramified in $K|\mathbb{Q}$ greater than 3. In particular, $p \equiv 1 \mod 2$. Therefore, the statement for Φ^- follows from the statement for Φ^+ by definition of the coefficients of $V^{(+/-,\nu)}$ and $(-1)^{\nu n} = (-1)^{\nu pn}$, for all $n \in \mathbb{N}$ and $\nu \in \mathbb{Z}$, we have $a_n^+ = a_n^-$.
Let $\nu \in \mathbb{Z}\left[D^{-1}\right]$ and let $a_n^+ = \left[V^{(+,\nu)}(z)\right]_n$ for all $n \in \mathbb{N}$. Then we have

$$\begin{aligned}
&\mathrm{Frob}_p(a_n^+) - a_{pn}^+ \\
&\quad = \frac{1}{\nu}\left[\frac{\exp(\nu np \int V(z)}{z^{pn}}\left(\exp\left(\nu np\left(\frac{1}{p}\left(\mathrm{Frob}_p \int V\right)(z^p) - \int V(z)\right)\right) - 1\right)\right]_0 \\
&\quad = \frac{1}{\nu}\left[\frac{\exp(\nu np \int V(z))}{z^{pn}}\left(\exp\left(\nu np \int \left(\mathrm{Frob}_p V\left(z^p\right) - V(z)\right)\right) - 1\right)\right]_0 .
\end{aligned}$$

Recall $\exp(\int V(z)) \in 1 + z\mathcal{O}_p[\![z]\!]$, from Theorem 2.15. By Proposition 2.10 *(i)*, V satisfies the local 2-function property at p if and only if

$$\int^2 \left(\mathrm{Frob}_p V\left(z^p\right) - V(z)\right) =: \int^2 X(z) \in z\mathcal{O}_p[\![z]\!]. \tag{4.11}$$

Note, X depends on p, which is omitted from the notation. Therefore,

$$\mathrm{Frob}_p(a_n^+) - a_{pn}^+ = \frac{1}{\nu}\left[\frac{\exp(\nu np \int V(z))}{z^{pn}}\left(\sum_{k=1}^{\infty}\frac{(\nu np \int X(z))^k}{k!}\right)\right]_0 \tag{4.12}$$

The formula for the p-adic order of $k!$ is given by

$$\mathrm{ord}_p(k!) = \frac{k - S_p(k)}{p-1} \leq \frac{k-1}{p-1} \leq \frac{k-1}{2},$$

where $S_p(k)$ denotes the sum of the digits of k in base p. Therefore, we obtain for $k \geq 2$

$$\begin{aligned}
\mathrm{ord}_p\left(\frac{(pn)^k}{k!}\right) &\geq k(\mathrm{ord}_p(n) + 1) - \frac{k-1}{2} \\
&= k\left(\mathrm{ord}_p(n) + \frac{1}{2}\right) + \frac{1}{2}
\end{aligned}$$

$$\geq 2\mathrm{ord}_p(n) + 1 + \frac{1}{2}.$$

Since p-adic order has integral values, we conclude

$$\mathrm{ord}_p\left(\frac{(pn)^k}{k!}\right) \geq 2(\mathrm{ord}_p(n)+1) \quad \text{for all } k \geq 2.$$

Therefore,

$$\begin{aligned}\exp(\nu np \int X(z)) - 1 &= \sum_{k=1}^{\infty} \frac{(\nu np)^k (\int X(z))^k}{k!} \\ &\equiv \nu np \int X(z) \mod p^{2(\mathrm{ord}_p(n)+1)}\mathcal{O}_p[\![z]\!].\end{aligned}$$

Hence, eq. (4.12) becomes

$$\mathrm{Frob}_p(a_n^+) - a_{pn}^+ = np\left[\frac{\exp(\nu np \int V(z))}{z^{pn}} \int X(z)\right]_0 \mod p^{2(\mathrm{ord}_p(n)+1)}\mathcal{O}_p.$$

Using eq. (4.8) once more leads to

$$\begin{aligned}\mathrm{Frob}_p(a_n^+) - a_{pn}^+ &\equiv -np\left[\int^2 X(z)\delta\left(\frac{\exp(\nu np \int V(z))}{z^{pn}}\right)\right]_0 \mod p^{2(\mathrm{ord}_p(n)+1)}\mathcal{O}_p \\ &= (np)^2\left[\int^2 X(z)\cdot\exp(\nu np\int V(z))\cdot\frac{1-\nu V(z)}{z^{pn}}\right]_0 \\ &\equiv 0 \mod p^{2(\mathrm{ord}_p(n)+1)}\mathcal{O}_p,\end{aligned}$$

since all involved power series have coefficients in $\mathcal{O}_p$. This completes the proof for eq. (4.9). The remaining two cases are dedicated to eq. (4.10).

Case 2: $p = 2$ and $\mathrm{ord}_2(n\nu) \geq 1$. Now we show that Φ^- preserves the local 2-function property for $p = 2$. Note, the computation in this case also applies to Φ^+. Therefore, we will still assume $\nu \in \mathbb{Z}$. Then

$$\mathrm{ord}_2\left(\frac{(2n)^k}{k!}\right) = k(\mathrm{ord}_2(n)+1) - k + S_2(k).$$

Since $S_2(k) \geq 1$ for $k \geq 1$ we find

$$\mathrm{ord}_2\left(\frac{(2n)^k}{k!}\right) \geq k\,\mathrm{ord}_2(n) + 1.$$

For $k \geq 3$ we therefore have

$$\operatorname{ord}_2\left(\frac{(2n)^k}{k!}\right) \geq 2(\operatorname{ord}_2(n)+1).$$

Hence, we obtain analogously to eq. (4.12) for $\nu \in \mathbb{Z}$

$$\begin{aligned}
&\operatorname{Frob}_2(a_n^-) - a_{2n}^- = (-1)^{\nu n}\operatorname{Frob}_2(a_n^+) - (-1)^{2\nu n}a_{2n}^+ \\
&= \operatorname{Frob}_2(a_n^+) - a_{2n}^+ \\
&\equiv \frac{1}{\nu}\left[\frac{\exp(2\nu n\int V(z))}{z^{2n}}\left(2\nu n\int X(z) + 2(\nu n)^2(\int X(z))^2\right)\right]_0 \mod 2^{2(\operatorname{ord}_2(n)+1)}\mathcal{O}_2.
\end{aligned} \tag{4.13}$$

Note however, for $\nu \in \mathbb{Z}\left[D^{-1}\right]$ we still have

$$\begin{aligned}
&\operatorname{Frob}_2(a_n^+) - a_{2n}^+ \\
&\equiv \frac{1}{\nu}\left[\frac{\exp(2\nu n\int V(z))}{z^{2n}}\left(2\nu n\int X(z) + 2(\nu n)^2(\int X(z))^2\right)\right]_0 \mod 2^{2(\operatorname{ord}_2(n)+1)}\mathcal{O}_2.
\end{aligned}$$

For the following calculation we may therefore assume $\nu \in \mathbb{Z}\left[D^{-1}\right]$. The first summand in the above calculation vanishes by the same calculation as in the previous case, i.e. by using eq. (4.8). Therefore, in this case, the assertion follows from

$$0 \equiv \nu\left[\frac{\exp(2\nu n\int V(z))}{z^{2n}}(\int X(z))^2\right]_0 \mod 2\mathcal{O}_2.$$

Let $x_i := [X(z)]_i \in \mathcal{O}_2$. Then by definition eq. (4.11), we have $x_i \in 2^{2\operatorname{ord}_2(i)}\mathcal{O}_2$ and therefore,

$$\begin{aligned}
(\int X(z))^2 = \sum_{i,j=1}^{\infty}\frac{x_ix_j}{ij}z^{i+j} &= 2\sum_{\substack{i,j=1\\ i<j}}^{\infty}\frac{x_ix_j}{ij}z^{i+j} + \sum_{i=1}^{\infty}\frac{x_i^2}{i^2}z^{2i} \\
&\equiv \sum_{\substack{i=1\\ i\text{ odd}}}^{\infty}\frac{x_i^2}{i^2}z^{2i} \equiv \sum_{\substack{i=1\\ i\text{ odd}}}^{\infty}x_i^2z^{2i} \mod 2z\mathcal{O}_2[\![z]\!].
\end{aligned} \tag{4.14}$$

Consider for odd $i \in \mathbb{N}$,

$$\begin{aligned}
\left[\exp(2\nu n\int V(z))z^{2(i-n)}\right]_0 &= -\frac{1}{2i}\left[\delta\left(\frac{\exp(2n\nu\int V(z))}{z^{2n}}\right)z^{2i}\right]_0 \\
&= -\frac{n}{i}\left[(1-\nu V(z))z^{2(i-n)}\exp(2n\nu\int V(z))\right]_0
\end{aligned}$$

$$\equiv 0 \mod 2\mathcal{O}_2, \tag{4.15}$$

in which the congruence follows from $\mathrm{ord}_2(n) \geq 1$. A more general argument for the calculation eq. (4.15) is given by Proposition 4.22. Therefore,

$$\left[\frac{\exp(2\nu n \int V(z))}{z^{2n}}(\int X(z))^2\right]_0 = \sum_{\substack{i=1\\ i \text{ odd}}}^{\infty} x_i^2 \left[\exp(2\nu n \int V(z)) z^{2(i-n)}\right]_0 \equiv 0 \mod 2\mathcal{O}_2.$$

Case 3: Let $p = 2$, and $\mathrm{ord}_2(n\nu) = 0$. We obtain

$$(-1)^{\nu n}\left(\mathrm{Frob}_2(a_n^-) - a_{2n}^-\right) = \mathrm{Frob}_2(a_n^+) + a_{2n}^+.$$

Since

$$\mathrm{ord}_2\left(\frac{2^k}{k!}\right) = k - k + S_2(k) = S_2(k),$$

we observe that $\mathrm{ord}_2\left(\frac{2^k}{k!}\right) \geq 2$ if and only if k is not a non-negative integer power of 2. Indeed, $S_2(k) = 1$ if and only if $k = 2^\ell$ for some $\ell \in \mathbb{N}_0$. Therefore, eq. (4.12) becomes modulo $2^{2(\mathrm{ord}_2(n)+1)} = 4$

$$\begin{aligned}\mathrm{Frob}_2(a_n^+) + a_{2n}^+ &\equiv \frac{1}{\nu}\left[\frac{\exp(2\nu n \int V(z))}{z^{2n}}\left(\exp\left(2\nu n \int X(z)\right) + 1\right)\right]_0 \\ &\equiv \frac{1}{\nu}\left[\frac{\exp(2\nu n \int V(z))}{z^{2n}}\left(2 + \sum_{\ell=0}^{\infty}\frac{(2\nu n \int X(z))^{2^\ell}}{(2^\ell)!}\right)\right]_0 \mod 4\mathcal{O}_2.\end{aligned}$$

Since $\mathrm{ord}_2\left(\frac{2^{2^\ell}}{(2^\ell)!}\right) = 1$ for all $\ell \in \mathbb{N}$ – and therefore $\frac{2^{2^\ell}}{2(2^\ell)!} \equiv 1 \mod 2$ – the assertion follows, by excluding the factor 2, from

$$0 \equiv \left[\frac{\exp(2\nu n \int V(z))}{z^{2n}}\left(1 + \sum_{\ell=0}^{\infty}(\int X(z))^{2^\ell}\right)\right]_0 \mod 2\mathcal{O}_2 \quad \text{(note: } \mathrm{ord}_2(\nu) = 0\text{)}.$$

As in the calculation given in eq. (4.14), we find for all $\ell \in \mathbb{N}_0$

$$(\int X(z))^{2^\ell} \equiv \sum_{\substack{i=1\\ i \text{ odd}}}^{\infty} x_i^{2^\ell} z^{2^\ell i} \mod 2z\mathcal{O}_2[\![z]\!].$$

Note that for odd $i \in \mathbb{N}$ (and for $a_{i/2} := 0$ in this case) and since V is in particular

an element in $\mathcal{S}^1(K|\mathbb{Q})$, we have

$$x_i^{2^\ell} = (\mathrm{Frob}_2(a_{i/2}) - a_i)^{2^\ell} = a_i^{2^\ell} \equiv \mathrm{Frob}_2^\ell(a_i) \equiv a_{2^\ell i} \mod 2\mathcal{O}_2.$$

Therefore, we have

$$\begin{aligned}
\sum_{\ell=0}^{\infty} (\int X(z))^{2^\ell} &\equiv \sum_{\ell=0}^{\infty} \sum_{\substack{i=1 \\ i \text{ odd}}}^{\infty} x_i^{2^\ell} z^{2^\ell i} \mod 2\mathcal{O}_2[\![z]\!] \\
&\equiv \sum_{\ell=0}^{\infty} \sum_{\substack{i=1 \\ i \text{ odd}}}^{\infty} a_{2^\ell i} z^{2^\ell i} \mod 2\mathcal{O}_2[\![z]\!] \\
&\equiv \sum_{k=1}^{\infty} a_k z^k \mod 2\mathcal{O}_2[\![z]\!] \\
&= V(z). \qquad (4.16)
\end{aligned}$$

Hence, again by eq. (4.8),

$$\begin{aligned}
&\left[\frac{1 + \exp(2\nu n \int V(z))}{z^{2n}} \left(1 + \sum_{\ell=0}^{\infty} (\int X(z))^{2^\ell} \right) \right]_0 \\
&\qquad \equiv \left[\frac{\exp(2\nu n \int V(z))}{z^{2n}} \cdot (1 + V(z)) \right]_0 \mod 2\mathcal{O}_2 \\
&\qquad \equiv \left[\frac{\exp(2\nu n \int V(z))}{z^{2n}} \cdot (1 - V(z)) \right]_0 \mod 2\mathcal{O}_2 \\
&\qquad \equiv 0 \mod 2\mathcal{O}_2.
\end{aligned}$$

For the faithfulness it is sufficient to show that for $\nu, \mu \in \mathbb{Z}\left[D^{-1}\right]$ and $V(z) = -\dfrac{z}{1-z} \in \mathcal{S}^2(K|\mathbb{Q})$, we have $V^{(+,\nu)} \neq V^{(+,\mu)}$. This is immediately clear by eq. (4.5). □

Remark 4.13 Although Φ^+ fails to preserve the local 2-function property for $p = 2$ precisely if $\mathrm{ord}_2(n) = \mathrm{ord}_2(\nu) = 0$. However, in that case we still have

$$\mathrm{Frob}_2(a_n^+) - a_{2n}^+ \equiv 0 \mod 2\mathcal{O}_2.$$

Therefore, we may preserve 2-integrality for Φ^+ by multiplying with 2,

$$2 \cdot \Phi^+ \left(\mathbb{Z}\left[D^{-1}\right] \times \mathcal{S}^2(K|\mathbb{Q}) \right) \subset \mathcal{S}^2(K|\mathbb{Q}).$$

4.3 Wolstenholme's Theorem: Harmonic Sums, Binomials and a new Generalization

The goal of the present section is to prove a generalization of Wolstenholme's Theorem given by Theorem 4.15, which turns out to be crucial to the proof of Theorem 4.1 presented in Section 4.4. For a survey on Wolstenholme's Theorem see [29].

In 1862, J. Wolstenholme proved that for all primes $p \geq 5$ we have

$$\binom{2p-1}{p-1} \equiv 1 \mod p^3. \tag{4.17}$$

This result is originally known as Wolstenholme's theorem, see [46] for the original work. As pointed out by Rosen in [37], the related congruence on harmonic numbers $H_n := \sum_{k=1}^{n} \frac{1}{k}$, stating that for all primes $p \geq 5$,

$$H_{p-1} = \sum_{k=1}^{p-1} \frac{1}{k} \equiv 0 \mod p^2 \tag{4.18}$$

(which was discovered 80 years earlier by E. Waring in 1782 (see [45]) and later by C. Babbage in 1819 (see [4])), is in fact equivalent to Wolstenholme's original result. In modern literature, eq. (4.18) is referred to as *Wolstenholme's Theorem*. More generally, we have

Theorem 4.14 ("Wolstenholme's Theorem", Waring-Babbage, cf. [16]) *Let p be a prime and let ϵ_p be 2, 1, or 0 according to whether p is 2, 3 or ≥ 5, respectively. Then, for all $n \in \mathbb{N}$,*

$$\sum_{\substack{k=1 \\ p \nmid k}}^{pn} \frac{1}{k} \equiv 0 \mod p^{2(\mathrm{ord}_p(n)+1)-\varepsilon_p}\mathbb{Z}_p. \tag{4.19}$$

Proof. First check the identity for $1 \leq k \leq n$

$$\frac{1}{k} + \frac{1}{n-k} = -\frac{n}{k^2} + \frac{n^2}{k^2(n-k)}.$$

Note, the sum given in eq. (4.19) is trivially a p-adic integer. Therefore, w. l. o. g., we

assume $2\,\mathrm{ord}_p(n) - \varepsilon \geq 0$. Then,

$$2\sum_{\substack{k=1\\ p\nmid k}}^{n} \frac{1}{k} = \sum_{\substack{k=1\\ p\nmid k}}^{n} \left(\frac{1}{k} + \frac{1}{n-k}\right) = \sum_{\substack{k=1\\ p\nmid k}}^{n} \left(-\frac{n}{k^2} + \frac{n^2}{k^2(n-k)}\right)$$
$$= -n\sum_{\substack{k=1\\ p\nmid k}}^{n} \frac{1}{k^2} + n^2 \sum_{\substack{k=1\\ p\nmid k}}^{n} \frac{1}{k^2(n-k)} \equiv -n\sum_{\substack{k=1\\ p\nmid k}}^{n} \frac{1}{k^2} \mod p^{2\,\mathrm{ord}_p(n)}\mathbb{Z}_p.$$

Now, we immediately observe the assertion eq. (4.19) to be equivalent to the validity of the following congruence,

$$\sum_{\substack{k=1\\ p\nmid k}}^{n} \frac{1}{k^2} \equiv 0 \mod p^{\mathrm{ord}_p(n)-\varepsilon_p+\delta_{p,2}}\mathbb{Z}_p. \tag{4.20}$$

A proof of eq. (4.20) is given in [16, Lemma 1]. What is more, we will prove Theorem 4.15, which is a generalization of eq. (4.20) involving algebraic coefficients related to (rational) 2-functions. In particular, eq. (4.20) follows from Theorem 4.15 for $V(z) = \dfrac{z}{1-z}$ for $p \geq 3$ and from Remark 4.17 for $p = 2$. □

There are a number of generalizations and extensions of Wolstenholme's Theorem in terms of multiple harmonic sums and congruences among binomial coefficients. The next theorem gives a generalization in yet another direction. We will allow the nominator each summand be the folding of a periodic sequence with algebraic coefficients. The motivation for this has its origin in the proof of Theorem 4.1.

Theorem 4.15 *Let p be an unramified prime in $K|\mathbb{Q}$. Let $(a_k)_{k\in\mathbb{N}} \in \mathcal{O}_p^{\mathbb{N}}$ be a periodic sequence of periodicity N, i.e. $N \in \mathbb{N}$ is given by*

$$N = \min\{i \in \mathbb{N} \,|\, a_{k+i} = a_k \text{ for all } n \in \mathbb{N}\}.$$

Then, for all $n \in \mathbb{N}$,

$$\sum_{\substack{k=1\\ p\nmid k}}^{n} \frac{a_{n-k}a_k}{k^2} \equiv 0 \mod p^{\max\{0,\mathrm{ord}_p(n)-\varepsilon_{p,N}\}}\mathcal{O}_p,$$

where

$$\varepsilon_{p,N} = \begin{cases} \max\{\mathrm{ord}_2(N), \mathrm{ord}_2(N+2)\}, & \text{if } p = 2 \text{ and } 2 \mid N, \\ 1 + \mathrm{ord}_2(N+1), & \text{if } p = 2 \text{ and } 2 \nmid N, \\ 1 + \mathrm{ord}_3(N), & \text{if } p = 3, \\ \mathrm{ord}_p(N), & \text{if } p \geq 5. \end{cases}$$

Proof. Write $n = mp^r$ for $r = \mathrm{ord}_p(n)$ and suitable $m \in \mathbb{N}$ such that $\gcd(m,p) = 1$. Then, by using the geometric series $(1-xp)^{-1} = \sum_{k=0}^{\infty}(xp)^k$ for $x \in \mathbb{Z}_p$, we obtain

$$\sum_{\substack{k=0 \\ p\nmid k}}^{n} \frac{a_{n-k}a_k}{k^2} \overset{k\mapsto \mu p^r+\ell}{=} \sum_{\mu=0}^{m-1}\sum_{\substack{\ell=0 \\ p\nmid \ell}}^{p^r} \frac{a_{(m-\mu)p^r-\ell}a_{\mu p^r+\ell}}{(\mu p^r+\ell)^2} = \sum_{\mu=0}^{m-1}\sum_{\substack{\ell=0 \\ p\nmid \ell}}^{p^r} \frac{a_{(m-\mu)p^r-\ell}a_{\mu p^r+\ell}}{\ell^2(1+\frac{\mu}{\ell}p^r)^2}$$

$$\equiv \sum_{\mu=0}^{m-1}\sum_{\substack{\ell=0 \\ p\nmid \ell}}^{p^r} \frac{a_{(m-\mu)p^r-\ell}a_{\mu p^r+\ell}}{\ell^2} \mod p^r\mathcal{O}_p. \tag{4.21}$$

Note, the sum in eq. (4.21) is trivially an element in $\mathcal{O}_p$. First, find $q \in \mathbb{N}$ such that $p \nmid q$, $N \mid q-1$, and – whenever possible – $p \nmid q+1$. We have

Case 1: If $p \nmid N+1$ and $p \nmid N+2$, choose $q = N+1$. Trivially, $N \mid q-1$. In that case,

$$p \nmid q, \quad \text{by definition, and}$$
$$q^2 - 1 = (q-1)(q+1) = N(N+2),$$

and therefore,

$$\mathrm{ord}_p(q^2-1) = \mathrm{ord}_p(N).$$

Case 2: Let $p > 2$. If $p \mid N+1$ and $p \nmid N+2$, then choose $q = 3N+1$. Note that $p \mid N+1$ implies $p \nmid N$. Indeed, $N \mid q-1$ and

$$q = 3N+1 \equiv 2N \not\equiv 0 \mod p, \quad \text{and}$$
$$q+1 = 3N+2 \equiv N \not\equiv 0 \mod p, \quad \text{since } p \nmid N \text{ and } p \neq 2.$$

Also, $p \nmid q$, since $3N+1 = N-1+2(N+1)$ and $p \neq 2$. Finally, $p \nmid q+1$, since

$3N + 2 = N + 2(N + 1)$ and $p \nmid N$. In this case,

$$q^2 - 1 = 3N(3N + 2).$$

Hence,

$$\mathrm{ord}_p(q^2 - 1) = \mathrm{ord}_p(N) + \delta_{p,3}.$$

Case 3: Let $p = 2$ and $p \mid N + 1$, $p \nmid N + 2$. Then choose $q = 2N + 1$. Observe, that $N \mid q - 1$ and

$$q = 2N + 1 \equiv N \neq 0 \mod 2, \quad \text{since } p \nmid N.$$

At the same time,

$$\mathrm{ord}_2(q^2 - 1) = \mathrm{ord}_2((q - 1)(q + 1)) = \mathrm{ord}_2(4N(N + 1)) = 2 + \mathrm{ord}_2(N + 1).$$

Case 4: Let $p \notin \{2, 3\}$ and $p \nmid N + 1$ and $p \mid N + 2$, then choose $q = 2N + 1$. Trivially, $N \mid q - 1$ and we have

$$\begin{aligned} q = 2N + 1 \equiv -3 \not\equiv 0 \mod p, \quad \text{since } p \neq 3 \text{ and,} \\ q + 1 = 2N + 2 \equiv N \not\equiv 0 \mod p, \quad \text{since } p \neq 2. \end{aligned}$$

In that case,

$$q^2 - 1 = 4N(N + 1).$$

Hence,

$$\mathrm{ord}_p(q^2 - 1) = \mathrm{ord}_p(N).$$

Case 5: Let $p = 3$, $3 \nmid N + 1$ and $3 \mid N + 2$, then choose $q = 3N + 1$. Note that $p = 3$ implies $3 \nmid N$. Hence, $N \mid q - 1$ and we have

$$q = 3N + 1 \equiv N - 3 \equiv N \not\equiv 0 \mod 3.$$

Furthermore,

$$q^2 - 1 = 3N(3N + 2)$$

and therefore,

$$\operatorname{ord}_3(q^2-1)=1.$$

Case 6: Let $p=2$, $2\nmid N+1$ and $2\mid N+2$ (i.e. $2\mid N$), then choose $q=N+1$. We have

$$q=N+1\not\equiv 0 \mod 2.$$

Then

$$q^2-1=N^2+2N=N(N+2)$$

and therefore

$$\operatorname{ord}_2(q^2-1)=\operatorname{ord}_2(N)+\operatorname{ord}_2(N+2)=1+\max\{\operatorname{ord}_2(N),\operatorname{ord}_2(N+2)\}.$$

Since we may find q such that $q\equiv 1 \mod N$ in every case, we have $a_{m+q\ell}=a_{m+\ell}$ for all $m\in\mathbb{N}_0$ and $\ell\in\mathbb{N}$. Since $p\nmid q$, we see that multiplication by $q \bmod p^r$ gives a bijection on $(\mathbb{Z}/p^r\mathbb{Z})^\times$ and hence, we may also permute the sumands in eq. (4.21) by the transformation $\ell\mapsto q\ell$. Therefore,

$$\begin{aligned}\sum_{\substack{k=0\\p\nmid k}}^{n}\frac{a_{n-k}a_k}{k^2}&\equiv\sum_{\mu=0}^{m-1}\sum_{\substack{\ell=0\\p\nmid\ell}}^{p^r}\frac{a_{(m-\mu)p^r-\ell}a_{\mu p^r+\ell}}{\ell^2} \mod p^r\mathcal{O}_p\\&\equiv\sum_{\mu=0}^{m-1}\sum_{\substack{\ell=0\\p\nmid\ell}}^{p^r}\frac{a_{(m-\mu)p^r-q\ell}a_{\mu p^r+q\ell}}{(q\ell)^2} \mod p^r\mathcal{O}_p\\&=\frac{1}{q^2}\sum_{\mu=0}^{m-1}\sum_{\substack{\ell=0\\p\nmid\ell}}^{p^r}\frac{a_{(m-\mu)p^r-\ell}a_{\mu p^r+\ell}}{\ell^2}\equiv\frac{1}{q^2}\sum_{\substack{k=0\\p\nmid k}}^{n}\frac{a_{n-k}a_k}{k^2} \mod p^r\mathcal{O}_p.\end{aligned}$$

Equivalently,

$$\frac{q^2-1}{q^2}\cdot\sum_{\substack{k=0\\p\nmid k}}^{n}\frac{a_ka_{n-k}}{k^2}\equiv 0 \mod p^r\mathcal{O}_p.$$

By the above choice of q and recalling $q^2-1 \equiv 0 \mod p^{\varepsilon_{p,N}+\delta_{p,2}}\mathbb{Z}$, we therefore conclude

$$\sum_{\substack{k=0\\ p\nmid k}}^{n} \frac{a_k a_{n-k}}{k^2} \equiv 0 \mod p^{r-\varepsilon_{p,N}-\delta_{2,p}}\mathcal{O}_p.$$

For $p>2$, we are finished. For $p=2$ we may in particular assume $\mathrm{ord}_2(n)=r\geq 1$. By using the symmetry (i.e. the invariance of $k\mapsto n-k$) of the coefficients $a_k a_{n-k}$, we have

$$\sum_{\substack{k=0\\ k \text{ odd}}}^{n} \frac{a_{n-k}a_k}{k^2} \equiv 2\cdot \sum_{\substack{k=0\\ k \text{ odd}}}^{n/2} \frac{a_{n-k}a_k}{k^2} \mod 2^r\mathcal{O}_2.$$

Then by the same calculation as for general p, and the same choice of $q\in\mathbb{Z}$, we find

$$\sum_{\substack{k=0\\ k \text{ odd}}}^{n/2} \frac{a_{n-k}a_k}{k^2} \equiv \frac{1}{q^2} \sum_{\substack{k=0\\ k \text{ odd}}}^{n/2} \frac{a_{n-k}a_k}{k^2} \mod 2^r\mathcal{O}_2.$$

Equivalently,

$$\frac{q^2-1}{q^2} \sum_{\substack{k=0\\ k \text{ odd}}}^{n/2} \frac{a_{n-k}a_k}{k^2} \equiv 0 \mod 2^r\mathcal{O}_2.$$

Therefore,

$$\sum_{\substack{k=0\\ k \text{ odd}}}^{n} \frac{a_{n-k}a_k}{k^2} \equiv 0 \mod 2^{r-\varepsilon_{p,N}}\mathcal{O}_2,$$

as stated. □

Example 4.16 Let $V\in\mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$ of periodicity N and $a=([V(z)]_n)_{n\in\mathbb{N}}\in\mathcal{O}\left[D^{-1}\right]^{\mathbb{N}}$. By Theorem 1.2, the sequence a is *periodic* in the sense of Theorem 4.15, of periodicity N. Therefore, for all unramified primes p in $K|\mathbb{Q}$ and all $n\in\mathbb{N}$,

$$\sum_{\substack{k=1\\ p\nmid k}}^{n} \frac{a_{n-k}a_k}{k^2} \equiv 0 \mod p^{\max\{0,\mathrm{ord}_p(n)-\varepsilon_{p,N}\}}\mathcal{O}_p,$$

for $\varepsilon_{p,N}$ as in Theorem 4.15. Trivially, multiplying the function V with an integral

constant improves the congruence relation. For instance, let

$$C = 2^{\left\lceil \frac{\mathrm{ord}_2(N+1)}{2} \right\rceil + \left\lceil \frac{\max\{\mathrm{ord}_2(N), \mathrm{ord}_2(N+2)\}}{2} \right\rceil} \cdot \prod_{\substack{p \in \mathbb{N} \text{ prime} \\ p>2}} p^{\left\lceil \frac{\mathrm{ord}_p(N)}{2} \right\rceil}.$$

Then $\tilde{V} := C \cdot V \in \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$, and $\tilde{a}_n = C \cdot a_n$. Then

$$\sum_{\substack{k=1 \\ p \nmid k}}^{n} \frac{\tilde{a}_{n-k}\tilde{a}_k}{k^2} \equiv 0 \mod p^{\max\{0, \mathrm{ord}_p(n) - \tilde{\varepsilon}_p\}} \mathcal{O}_p,$$

where

$$\tilde{\varepsilon}_p = \begin{cases} 1, & \text{if } p = 2, \\ 1, & \text{if } p = 3, \\ 0, & \text{if } p \geq 5. \end{cases}$$

Remark 4.17 ($p = 2$) In the special case of eq. (4.20), for $p = 2$ and $V(z) = \dfrac{z}{1-z}$ (i.e. $a_n = 1$ for all $n \in \mathbb{N}$) one can improve the 2-adic estimation. In that case, we find

$$\sum_{\substack{k=1 \\ k \text{ odd}}}^{n} \frac{1}{k^2} \equiv 0 \mod 2^{\mathrm{ord}_2(n)-1}\mathbb{Z}_2, \tag{4.22}$$

which is sharper than what Theorem 4.15 permits. The reason for this is given by eq. (4.23) below. We prove eq. (4.22) for the sake of completeness. Write $n = 2^r m$ for $r = \mathrm{ord}_2(n)$ and $m \in \mathbb{N}$, $\gcd(2, m) = 1$. Since

$$\begin{aligned} \sum_{\substack{k=1 \\ k \text{ odd}}}^{n} \frac{1}{k^2} &= \sum_{\mu=0}^{m-1} \sum_{\substack{\ell=0 \\ \ell \text{ odd}}}^{2^r} \frac{1}{(\mu \cdot 2^r + \ell)^2} \equiv \sum_{\mu=0}^{m-1} \sum_{\substack{\ell=0 \\ \ell \text{ odd}}}^{2^r} \frac{1}{\ell^2} \mod 2^r\mathbb{Z}_2 \\ &= m \cdot \sum_{\substack{k=0 \\ k \text{ odd}}}^{2^r} \frac{1}{k^2}, \end{aligned}$$

we may assume w.l.o.g. $n = 2^r$. For $r = 1$ and $r = 2$ the assertion is trivial. Therefore, we may also assume $r \geq 3$. In that case, every odd square k^2 has four square roots

modulo 2^r, namely, $\pm k$ and $2^{r-1} \pm k$. Therefore,

$$\sum_{\substack{k=0 \\ k \text{ odd}}}^{2^r} \frac{1}{k^2} \equiv 4 \cdot \sum_{\substack{k=0 \\ k \text{ odd}}}^{2^{r-2}} \frac{1}{k^2} \mod 2^r. \tag{4.23}$$

Furthermore, the multiplication $k \mapsto 3k$ gives a bijection on $(\mathbb{Z}/2^r\mathbb{Z})^\times$ and

$$\begin{aligned} \sum_{\substack{k=0 \\ k \text{ odd}}}^{2^{r-2}} \frac{1}{k^2} &\equiv \sum_{\substack{k=0 \\ k \text{ odd}}}^{2^{r-2}} \frac{1}{(3k)^2} \mod 2^r \\ &= \frac{1}{9} \cdot \sum_{\substack{k=0 \\ k \text{ odd}}}^{2^{r-2}} \frac{1}{k^2}. \end{aligned}$$

Equivalently,

$$\frac{8}{9} \cdot \sum_{\substack{k=0 \\ k \text{ odd}}}^{2^{r-2}} \frac{1}{k^2} \equiv 0 \mod 2^r.$$

Hence,

$$\sum_{\substack{k=0 \\ k \text{ odd}}}^{2^{r-2}} \frac{1}{k^2} \equiv 0 \mod 2^{r-3}. \tag{4.24}$$

Inserting eq. (4.24) in eq. (4.23) leads to eq. (4.22).

We will now state the so-called *Jacobsthal-Kazandzidis congruence* (Theorem 4.18), which was first discovered by Jacobsthal as a corollary to his work [10] in 1949 and later in a more general formulation by Kazandzidis in 1969 (see [24]) and Trakhtman in 1974 (see [43]). Nonetheless, the proof of Theorem 4.18 as given in [16] makes use of the congruence relations of harmonic sums as stated by Theorem 4.14, Theorem 4.15 and Remark 4.17. The Jacobsthal-Kazandzidis congruence also follows from Theorem 4.1 as we will discuss in Section 4.5. Moreover, the proof of Theorem 4.1 may be considered as a generalization of the proof of Theorem 4.18 in a similar way as Theorem 4.15 generalizes Wolstenholme's Theorem, in particular because Theorem 4.15 is essential to Theorem 4.1, as the classical Wolsentholme's Theorem is to the Jacobsthal-Kazandzidis congruence. In this sense, the proof of Theorem 4.18 served the author as a source of inspiration in the process of proving Theorem 4.1.

Theorem 4.18 (Jacobsthal-Kazandzidis) *Let $a, b \in \mathbb{N}_0$ be non-negative integers, $r \in \mathbb{N}$ a positive integer, and let p be a prime. Then we have*

$$\binom{ap^r}{bp^r} \equiv \binom{ap^{r-1}}{bp^{r-1}} \mod p^{3r-\varepsilon_p},$$

where ϵ_p is (as in Theorem 4.14) 2, 1, or 0, whether p is 2, 3, or greater than 3, respectively.

Proof. We begin with

$$\binom{ap^r}{bp^r}\Big/\binom{ap^{r-1}}{bp^{r-1}} = \prod_{k=1}^{bp^r} \frac{(a-b)p^r+k}{k} \cdot \prod_{k=1}^{bp^{r-1}} \frac{k}{(a-b)p^{r-1}+k} = \prod_{\substack{k=1\\ p\nmid k}}^{bp^r} \left(1 + p^r \frac{a-b}{k}\right)$$

$$\equiv 1 + p^r(a-b)F_1 + p^{2r}(a-b)^2 F_2 \mod p^{3r}, \tag{4.25}$$

where F_1 and F_2 are given by the harmonic sums $F_1 = \sum_{\substack{k=0\\ p\nmid p}}^{bp^r} \frac{1}{k}$ and $F_2 = \sum_{\substack{i,j=0, i<j\\ p\nmid ij}}^{bp^r} \frac{1}{ij}$. We have

$$2F_2 = \sum_{\substack{i\neq j\\ p\nmid ij}}^{bp^r} \frac{1}{ij} = \left[\sum_{i=1,\, p\nmid i}^{bp^r} \frac{1}{i}\right]^2 - \sum_{\substack{i=1\\ p\nmid i}}^{bp^r} \frac{1}{i^2}.$$

By Theorem 4.14, Theorem 4.15 and Remark 4.17, this implies

$$F_2 \equiv 0 \mod p^{r-\epsilon_p},$$

and finally,

$$\binom{ap^r}{bp^r}\Big/\binom{ap^{r-1}}{bp^{r-1}} \equiv 1 \mod p^{3r-\epsilon_p}.$$

This finishes the proof. □

4.4 Proof of Theorem 4.1

The present section is dedicated to the proof of Theorem 4.1. Before we dive into the proof, we give an overview of the main steps. During this illustration, we assume $\nu = 1$ for simplification.

The first step consists of Lemma 4.19 and Corollary 4.20. From Theorem 4.12, we

know that for all unramified primes p, the expression

$$\frac{2}{p^2n^2} \cdot \left(\mathrm{Frob}_p\left(a_n^+\right) - a_{pn}^+\right), \tag{4.26}$$

is a p-adic integer for all $n \in \mathbb{N}$, i.e. is an element in $\mathcal{O}_p$. Lemma 4.19 gives an estimation of the expression given in (4.26), assuming at least 3-integrality of V (i.e. $V \in \mathcal{S}^3(K|\mathbb{Q})$). By also assuming $V \in \mathcal{S}^\infty(K|\mathbb{Q})$, this estimation can be further simplified. This assumption of '∞-integrality' then allows us to perform partial integration eq. (2.2) as often as needed without destroying p-adic integrality of the terms appearing. The statement of Corollary 4.20 then reduces the proof of Theorem 4.1 to showing the validity of the congruence

$$0 \equiv \left[V(z) \cdot \left(\frac{Y(z)}{z}\right)^{pn} \cdot \int^2 \left(\mathrm{Frob}_p\, V(z^p) - V(z)\right)\right]_0 \mod p^{\mathrm{ord}_p(pn)-\gamma_p}\mathcal{O}_p, \tag{4.27}$$

for all $n \in \mathbb{N}$, where $Y(z) = \exp(\int V)$. The assumption "$V \in \mathcal{S}^\infty$" may seem poorly justified at this point. However, in retrospect, to apply Theorem 4.15 we even need V to have periodic coefficients, implying its rationality and therefore $V \in \mathcal{S}^\infty(K|\mathbb{Q})_S$, where $S = \{p \text{ prime};\, p \mid N\}$, as described in Corollary 3.19.

The next step is to evaluate the right hand side of eq. (4.27) up to the p-power of $\mathrm{ord}_p(n) + 1 - \delta_{3,p}$ (see eq. (4.38))

$$\begin{aligned}&\left[V(z)\left(\frac{Y(z)}{z}\right)^{pn} \int^2 \left(\mathrm{Frob}_p\, V(z^p) - V(z)\right)\right]_0 \\ &\quad\overset{\text{Lemma 4.21}}{\equiv} \sum_{m=0}^{n}\left(\left[\left(\varepsilon_p\widetilde{Y}(z)\right)^n\right]_m \sum_{\substack{\ell=1\\ p\nmid\ell}}^{p(n-m)} \frac{a_{p(n-m)-\ell}a_\ell}{\ell^2}\right) \mod p^{\mathrm{ord}_p(pn)-\delta_{3,p}}\mathcal{O}_p,\end{aligned} \tag{4.28}$$

where $\widetilde{Y}(z) = \exp\left(\int \mathscr{C}_p V(z)\right)$. The building blocks of this sum are

$$\underbrace{\left[\left(\varepsilon_p\widetilde{Y}(z)\right)^n\right]_m}_{(\dagger)} \quad \text{and} \quad \underbrace{\sum_{\ell=1,\, p\nmid\ell}^{p(n-m)} \frac{a_{p(n-m)-\ell}a_\ell}{\ell^2}}_{(\ddagger)} \quad \text{for } m = 0, ..., n,$$

see also eq. (4.38). While (†) seems arbitrary, (‡) reminds one of the congruences amongst harmonic sums given by Wolstenholme's Theorem 4.14 and has therefore been the motivation for proving Theorem 4.15. Also, the sum given in eq. (4.28) can be considered

as a generalization of eq. (4.25) in the proof of the Jacobsthal-Kazandzidis congruence Theorem 4.18.

Once Theorem 4.15 is proven, one may expect

$$(\dagger) \equiv 0 \mod p^{\max\{0,\mathrm{ord}_p(n)-\mathrm{ord}_p(m)\}}\mathcal{O}_p$$

should be true. Of course, by Dwork's Integrality Lemma, (†) has non-negative p-adic order. The sharper estimation needed is provided by Proposition 4.22.

All what is left is putting the pieces of the puzzle together. From Theorem 4.15, Proposition 4.22 and eq. (4.28) the congruence eq. (4.27) follows directly and therefore, Theorem 4.1.

Lemma 4.19 *Let $V \in \mathcal{S}^3(K|\mathbb{Q})$ and $\nu \in \mathbb{Z}[D^{-1}]$. Denote by $a_n = [V(z)]_n$ and $a_n^+ = \left[V^{(+,\nu)}(z)\right]_n$ the n-th coefficient of $V(z)$ and $V^{(+,\nu)}(z)$, respectively. Then we have for all (unramified) primes p and for all $n \in \mathbb{N}$ – except for the case where $p = 2$ and $\mathrm{ord}_2(n) = 0$ – the congruence*

$$\frac{2}{p^2n^2}\cdot\left(\mathrm{Frob}_p(a_n^+) - a_{pn}^+\right) \equiv \nu\left[\delta\left(\mathrm{Frob}_p V(z^p) + V(z)\right)\cdot\left(\frac{\exp(\nu\int V(z))}{z}\right)^{pn}\times\cdots\right.$$
$$\left.\cdots\times\int^3\left(\mathrm{Frob}_p V(z^p) - V(z)\right)\right]_0 \mod p^{\mathrm{ord}_p(n)+1-\delta_{3,p}}\mathcal{O}_p. \tag{4.29}$$

Note, for the exceptional case $p = 2$ and $\mathrm{ord}_2(n) = 0$, by Theorem 4.12 we only have $\mathrm{Frob}_2\left(a_n^+\right) - a_{2n}^+ \equiv 0 \mod 2\mathcal{O}_2$.

Proof. We will consequently exclude the case $p = 2$ and $\mathrm{ord}_2(n) = 0$ in the following without necessarily mentioning it. Let p be an unramified prime in K. As in the proof of Theorem 4.12 we will write

$$X(z) := \mathrm{Frob}_p V\left(z^p\right) - V(z).$$

Then we obtain

$$\begin{aligned}\mathrm{Frob}_p(a_n^+) - a_{pn}^+ &= \frac{1}{\nu}\left[\frac{\exp(\nu np\int V(z))}{z^{pn}}\left(\exp\left(\nu np\int X(z)\right)-1\right)\right]_0\\ &= \frac{1}{\nu}\left[\frac{\exp(\nu np\int V(z))}{z^{pn}}\sum_{k=1}^{\infty}\frac{(\nu np)^k}{k!}(\int X(z))^k\right]_0.\end{aligned}$$

We find for $k \geq 4$ and $p \geq 3$

$$\begin{aligned}\mathbb{Z} \ni \operatorname{ord}_p\left(\frac{(pn)^k}{k!}\right) &\geq k(\operatorname{ord}_p(n)+1) - \frac{k-1}{2} \\ &= k\left(\operatorname{ord}_p(n)+\frac{1}{2}\right)+\frac{1}{2} \geq 4\operatorname{ord}_p(n)+\frac{5}{2} > 3(\operatorname{ord}_p(n)+1)-1.\end{aligned}$$

And therefore, $\operatorname{ord}_p\left(\frac{(pn)^k}{k!}\right) \geq 3(\operatorname{ord}_p(n)+1)$. For $p=2$ we assume $\operatorname{ord}_2(n) \geq 1$, then for $k \geq 4$

$$\operatorname{ord}_2\left(\frac{(2n)^k}{k!}\right) = k\operatorname{ord}_2(n) + S_2(k) \geq 3\operatorname{ord}_2(n)+2 = 3(\operatorname{ord}_2(n)+1)-1.$$

For $k=3$ we still have

$$\operatorname{ord}_p\left(\frac{(pn)^3}{3!}\right) = \begin{cases} 3(\operatorname{ord}_p(n)+1), & \text{if } p \geq 5, \\ 3(\operatorname{ord}_p(n)+1)-1, & \text{if } p \in \{2,3\}. \end{cases}$$

Therefore, we obtain for $p \geq 5$,

$$\begin{aligned}&\operatorname{Frob}_p(a_n^+) - a_{pn}^+ \\ &\quad\equiv np\left[\frac{\exp(\nu np\int V(z))}{z^{pn}}\left(\int X(z) + \frac{\nu np}{2}(\int X(z))^2\right)\right]_0 \mod p^{3(\operatorname{ord}_p(n)+1)}\mathcal{O}_p,\end{aligned} \tag{4.30}$$

and for $p \in \{2,3\}$, (again, except for the case where $p=2$ and $\operatorname{ord}_2(n)=0$)

$$\begin{aligned}\operatorname{Frob}_p(a_n^+) - a_{pn}^+ \equiv \Bigg[&\frac{\exp(\nu np\int V(z))}{z^{pn}} \times \cdots \\ &\cdots \times \left(np\int X(z) + \frac{\nu}{2}(np)^2(\int X(z))^2\right)\Bigg]_0 \mod p^{3\operatorname{ord}_p(n)+2}\mathcal{O}_p.\end{aligned} \tag{4.31}$$

We will compute the expressions given in (4.32) and (4.33) separately.

$$\left[\frac{\exp(\nu np\int V(z))}{z^{pn}}\int X(z)\right]_0 \mod p^{2(\operatorname{ord}_p(n)+1)}\mathcal{O}_p, \qquad \text{for all primes } p, \tag{4.32}$$

$$\left[\frac{\exp(\nu np\int V(z))}{z^{pn}}(\int X(z))^2\right]_0 \mod p^{\operatorname{ord}_p(n)+1}\mathcal{O}_p, \qquad \text{for all primes } p. \tag{4.33}$$

In the following, we will write $F(z) = \dfrac{\exp(\nu np \int V(z))}{z^{pn}}$. We have for all primes p

$$\begin{aligned}
\delta^2 F(z) &= \delta^2 \left(z^{-pn} \exp(\nu pn \textstyle\int V(z)) \right) \\
&= \delta \left(-pn z^{-pn} \exp(\nu pn \textstyle\int V(z)) + \nu pn V(z) z^{-pn} \exp(\nu pn \textstyle\int V(z)) \right) \\
&= pn \cdot \delta \left((\nu V(z) - 1) F(z) \right) \\
&= pn\nu \cdot \delta V(z) \cdot F(z) + pn(\nu V(z) - 1) \cdot \delta F(z) \\
&= pn\nu \cdot \delta V(z) \cdot F(z) + (pn)^2 (\nu V(z) - 1)^2 F(z) \\
&\equiv pn\nu \cdot \delta V(z) \cdot F(z) \mod p^{2(\mathrm{ord}_p(n)+1)} \mathcal{O}_p[\![z]\!].
\end{aligned}$$

Therefore, by using the fact that $\int^3 X(z) \in z\mathcal{O}_p[\![z]\!]$ (for all p, which is equivalent to saying $V \in \mathcal{S}^3(K|\mathbb{Q})$), partial integration (see eq. (2.2)) applied to (4.32) gives us

$$\begin{aligned}
[F(z) \cdot \textstyle\int X(z)]_0 &= \left[\delta^2 F(z) \cdot \int^3 X(z) \right]_0 \\
&\equiv pn\nu \left[\delta V(z) \cdot F(z) \cdot \int^3 X(z) \right]_0 \mod p^{2(\mathrm{ord}_p(n)+1)} \mathcal{O}_p.
\end{aligned}$$

Furthermore, (4.33) for $p > 2$ becomes

$$\begin{aligned}
\left[F(z) (\textstyle\int X(z))^2 \right]_0 &= \left[\delta^2 (F(z) \cdot \textstyle\int X(z)) \cdot \int^3 X(z) \right]_0 \\
&= \left[(\delta^2 F(z) \cdot \textstyle\int X(z) + 2 \cdot \delta F(z) \cdot X(z) + F(z) \cdot \delta X(z)) \cdot \int^3 X(z) \right]_0 \\
&\equiv \left[(pn\nu \cdot \delta V(z) \cdot \textstyle\int X(z) + \delta X(z)) \cdot F(z) \cdot \int^3 X(z) \right]_0 \mod p^{\mathrm{ord}_p(n)+1} \mathcal{O}_p \\
&\equiv \left[\delta X(z) \cdot F(z) \cdot \int^3 X(z) \right]_0 \mod p^{\mathrm{ord}_p(n)+1} \mathcal{O}_p.
\end{aligned}$$

Therefore, inserting (4.32) and (4.33), for $p \geq 5$, into eq. (4.30), we obtain

$$\begin{aligned}
&\mathrm{Frob}_p(a_n^+) - a_{pn}^+ \\
&\quad \equiv \nu (np)^2 \left[\delta V(z) \cdot F(z) \cdot \int^3 X(z) \right]_0 + \\
&\qquad\qquad + \frac{\nu}{2} (np)^2 \left[\delta X(z) \cdot F(z) \cdot \int^3 X(z) \right]_0 \mod p^{3(\mathrm{ord}_p(n)+1)} \mathcal{O}_p \\
&\quad = \frac{\nu}{2} (np)^2 \left[\delta \left(2V(z) + X(z) \right) \cdot F(z) \cdot \int^3 X(z) \right]_0 \mod p^{3(\mathrm{ord}_p(n)+1)} \mathcal{O}_p \\
&\quad = \frac{\nu}{2} (np)^2 \left[\delta (\mathrm{Frob}_p V(z^p) + V(z)) \cdot F(z) \cdot \int^3 X(z) \right]_0 \mod p^{3(\mathrm{ord}_p(n)+1)} \mathcal{O}_p,
\end{aligned}$$

which proves eq. (4.29) for $p \geq 5$. For $p \in \{2, 3\}$, eq. (4.31) becomes

$$\begin{aligned}
&\mathrm{Frob}_p(a_n^+) - a_{pn}^+ \\
&\quad \equiv \frac{\nu}{2} (np)^2 \left[\delta (\mathrm{Frob}_p V(z^p) + V(z)) \cdot F(z) \cdot \int^3 X(z) \right]_0 \mod p^{3\,\mathrm{ord}_p(n)+2} \mathcal{O}_p.
\end{aligned}$$

As stated in eq. (4.29) for $p \in \{2,3\}$. □

It is very tedious to check whether $V^{(+/-,\nu)}(z)$ satisfies the local 3-function property for a given prime p by using eq. (4.29) explicitly. However, for $V \in \bigcap_{s=1}^{\infty} \mathcal{S}^s(K|\mathbb{Q}) = \mathcal{S}^\infty(K|\mathbb{Q})$ we may simplify eq. (4.29). This is the statement of the following Corollary 4.20.

Corollary 4.20 *Let $V(z) \in \mathcal{S}^\infty(K|\mathbb{Q})$ and $\nu \in \mathbb{Z}\left[D^{-1}\right]$. Denote by a_n^+ the n-th coefficient of $V^{(\nu,+)}(z)$ for all $n \in \mathbb{N}$. Then for all (unramified) primes p and all $n \in \mathbb{N}$ we have – except for the case where $p = 2$ and $\mathrm{ord}_2(n) = 0$ – the congruence*

$$\frac{2}{p^2n^2} \cdot \left(\mathrm{Frob}_p(a_n^+) - a_{pn}^+\right) \equiv \nu\left[V(z) \cdot \left(\frac{\exp(\nu \int V(z))}{z}\right)^{pn} \cdot \int^2 \left(\mathrm{Frob}_p V(z^p) - V(z)\right)\right]_0 \mod p^{\mathrm{ord}_p(n)+1-\delta_{3,p}}\mathcal{O}_p.$$

Proof. Let p be an unramfied prime in $K|\mathbb{Q}$ and fix $n \in \mathbb{N}$. As in the proof of Theorem 4.12 we will write

$$X(z) := \mathrm{Frob}_p V\left(z^p\right) - V(z) \quad \text{and} \quad F(z) := z^{-pn} \exp(\nu pn \int V(z)).$$

By assumption, $\int^s X(z) \in z\mathcal{O}_p[\![z]\!]$ for all $s \in \mathbb{N}$. Equivalently, $[X(z)]_{pn} = 0$ for all $n \in \mathbb{N}$. Let $s = \mathrm{ord}_p(n) + 3$. Then

$$\begin{aligned}\Big[\delta\left(\mathrm{Frob}_p V(z^p) + V(z)\right) \cdot F(z) \cdot \delta^{\mathrm{ord}_p(n)} \textstyle\int^{\mathrm{ord}_p(n)+3} X(z)\Big]_0 \\ = (-1)^{\mathrm{ord}_p(n)} \left[\delta^{\mathrm{ord}_p(n)}\left(\delta\left(\mathrm{Frob}_p V(z^p) + V(z)\right) \cdot F(z)\right) \cdot \textstyle\int^{\mathrm{ord}_p(n)+3} X(z)\right]_0.\end{aligned}$$

Note that $\delta F(z) \equiv 0 \mod p^{\mathrm{ord}_p(n)+1}$, therefore

$$\begin{aligned}\delta^{\mathrm{ord}_p(n)}&\left(\delta\left(\mathrm{Frob}_p V(z^p) + V(z)\right) \cdot F(z)\right) \\ &\equiv \delta^{\mathrm{ord}_p(n)+1}\left(\mathrm{Frob}_p V(z^p) + V(z)\right) \cdot F(z) \mod p^{\mathrm{ord}_p(n)+1} z\mathcal{O}_p[\![z]\!] \\ &\equiv \delta^{\mathrm{ord}_p(n)+1} V(z) \cdot F(z) \mod p^{\mathrm{ord}_p(n)+1} z\mathcal{O}_p[\![z]\!] \\ &\equiv \delta^{\mathrm{ord}_p(n)+1}(V(z)F(z)) \mod p^{\mathrm{ord}_p(n)+1} z\mathcal{O}_p[\![z]\!].\end{aligned}$$

Therefore, by Lemma 4.19, we have

$$-\frac{2}{p^2n^2} \cdot \left(\mathrm{Frob}_p(a_n^+) - a_{pn}^+\right) \equiv \nu\left[V(z) \cdot F(z) \cdot \int^2 X(z)\right]_0 \mod p^{\mathrm{ord}_p(n)+1-\delta_{3,p}}\mathcal{O}_p,$$

as stated. □

Lemma 4.21 *For all $V \in \mathcal{S}^1(K|\mathbb{Q})$ and $r \in \mathbb{N}$ and unramified primes p in $K|\mathbb{Q}$ we have*

$$\exp\left(p^r \int (\mathrm{Frob}_p V(z^p) - V(z))\right) \in 1 + p^r z \mathcal{O}_p[\![z]\!].$$

Proof. Write $X(z) = \mathrm{Frob}_p V(z^p) - V(z)$. Since $V \in \mathcal{S}^1(K|\mathbb{Q})$ we have $\int X(z) \in z\mathcal{O}_p[\![z]\!]$ for all unramified primes p in $K|\mathbb{Q}$. In particular, the statement follows if

$$\exp\left(p^r \widetilde{X}(z)\right) \in 1 + p^r z \mathcal{O}_p[\![z]\!]$$

for any $\widetilde{X} \in \mathcal{O}_p[\![z]\!]$. We have

$$\exp\left(p^r \widetilde{X}(z)\right) = 1 + \sum_{k=1}^{\infty} \frac{p^{rk}}{k!} \widetilde{X}(z)^k.$$

Then

$$\mathrm{ord}_p\left(\frac{p^{rk}}{k!}\right) = rk - \frac{k - S_p(k)}{p-1} \overset{p\geq 2}{\geq} rk - k + S_p(k) \overset{S_p(k)\geq 1}{\geq} (r-1)k + 1 \overset{k\geq 1}{\geq} r,$$

from which the statement follows. □

The next Proposition 4.22 can be seen as some auxiliary to Dwork's Lemma (cf. Theorem 2.15). For the proof of Theorem 4.1 we will see that Dwork's Lemma does not suffice. Instead, the p-adic estimation of the coefficients given in eq. (4.34) precisely ensures the 3-integrality of framing of rational 2-functions.

Proposition 4.22 *Let $V \in \mathcal{S}^1(K|\mathbb{Q})$ and let p be an unramified prime in $K|\mathbb{Q}$. Then for all $n, m \in \mathbb{N}$ with $\mathrm{ord}_p(n) \geq \mathrm{ord}_p(m)$,*

$$\left[\exp\left(n \int V(z)\right)\right]_m \equiv 0 \mod p^{\mathrm{ord}_p(n) - \mathrm{ord}_p(m)} \mathcal{O}_p. \tag{4.34}$$

Proof. Write

$$\exp(\textstyle\int V(z)) = 1 + \displaystyle\sum_{m=1}^{\infty} y_m z^m \quad \text{and} \quad \exp(n \textstyle\int V(z)) = 1 + \displaystyle\sum_{m=1}^{\infty} \tilde{y}_m z^m.$$

In particular, we have $\left(\dfrac{\tilde{y}_m}{n}\right)_{m\in\mathbb{N}} = \mathscr{Y}_{0,0,-1,n}\left((y_m)_{m\in\mathbb{N}}\right)$. Of course, by Dwork's Integrality Theorem 2.15 $\tilde{y}_m$ and y_m are elements $\mathcal{O}_p$ for all $m \in \mathbb{N}$. We have

$$\tilde{y}_m = n \sum_{k=1}^{m} \frac{1}{k} \binom{n-1}{k-1} \frac{k!}{m!} B_{m,k}(!y). \tag{4.35}$$

Note, that $\binom{n-1}{k-1} \in \mathbb{N}_0$ and $\frac{k!}{m!}B_{m,k}(!y) \in \mathcal{O}_p$, since $y \in \mathcal{O}_p^{\mathbb{N}}$. Therefore, we have for all $1 \leq k \leq m$ with $\mathrm{ord}_p(k) \leq \mathrm{ord}_p(m)$

$$\begin{aligned}\frac{n}{k}\binom{n-1}{k-1}\frac{k!}{m!}B_{m,k}(!y) &\equiv 0 \mod p^{\mathrm{ord}_p(n)-\mathrm{ord}_p(k)} \\ &\equiv 0 \mod p^{\mathrm{ord}_p(n)-\mathrm{ord}_p(m)}.\end{aligned}$$

Hence, mod $p^{\mathrm{ord}_p(n)-\mathrm{ord}_p(m)}$, we can ignore those sumands in eq. (4.35) where $\mathrm{ord}_p(k) \leq \mathrm{ord}_p(m)$. Let $1 \leq k \leq m$ with $\mathrm{ord}_p(k) > \mathrm{ord}_p(m)$. In that case, we will show that

$$\frac{k!}{m!}B_{m,k}(!y) \equiv 0 \mod p^{\mathrm{ord}_p(k)-\mathrm{ord}_p(m)}, \tag{4.36}$$

which implies eq. (4.34). We have

$$\frac{k!}{m!}B_{m,k}(!y) = \sum_{\alpha\in\pi(m,k)} \binom{k}{\alpha_1,\ldots,\alpha_{m-k+1}} \prod_{i=1}^{m-k+1} y_i^{\alpha_i}, \tag{4.37}$$

where $\pi(m,k) \subset \mathbb{N}_0^{m-k+1}$ such that $\alpha \in \pi(m,k)$ if and only if

$$\sum_{i=1}^{m-k+1} \alpha_i = k \quad \text{and} \quad \sum_{i=1}^{m-k+1} i\alpha_i = m.$$

Let $\alpha \in \pi(m,k)$. Assume there is an $1 \leq j \leq m-k+1$ such that $\mathrm{ord}_p(\alpha_j) \leq \mathrm{ord}_p(m)$. Then

$$\begin{aligned}\binom{k}{\alpha_1,\ldots,\alpha_{m-k+1}} &= \frac{k}{\alpha_j}\binom{k-1}{\alpha_1,\ldots,\alpha_j-1,\ldots,\alpha_{m-k+1}} \\ &\equiv 0 \mod p^{\mathrm{ord}_p(k)-\mathrm{ord}_p(\alpha_j)} \\ &\equiv 0 \mod p^{\mathrm{ord}_p(k)-\mathrm{ord}_p(m)}.\end{aligned}$$

Hence, mod $p^{\mathrm{ord}_p(n)-\mathrm{ord}_p(k)}$, we can ignore these sumands in eq. (4.37). Suppose, there exists an $\alpha \in \pi(m,k)$ such that for all $1 \leq i \leq m-k+1$ we have $\mathrm{ord}_p(\alpha_i) > \mathrm{ord}_p(m)$. Then

$$\mathrm{ord}_p(m) = \mathrm{ord}_p\left(\sum_{i=1}^{m-k+1} i\alpha_i\right) \geq \min_{i=1,\ldots,m-k+1} \mathrm{ord}_p(i\alpha_i) > \mathrm{ord}_p(m),$$

which is a contradiction. We conclude $\tilde{y}_m \equiv 0 \mod p^{\mathrm{ord}_p(n)-\mathrm{ord}_p(m)}$ in every case. □

Finally, we put the pieces together:

Proof. (of Theorem 4.1) Let $V \in \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$ and $\nu \in \mathbb{Z}\left[D^{-1}\right]$ and N the periodicity of V. Furthermore, let S be the set of primes dividing N. Fix an unramified prime p in $K|\mathbb{Q}$ and $n \in \mathbb{N}$, such that $p \notin S$. Let $a_m := [V(z)]_m$ and write $X(z) = \mathrm{Frob}_p V(z^p) - V(z)$. Hence, since $\mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q}) \subset \mathcal{S}^\infty(K|\mathbb{Q})_S$ (see proof of Corollary 3.19),

$$X(z) = -\sum_{\substack{k=1 \\ p\nmid k}}^{\infty} a_k z^k.$$

By Lemma 4.21 and since $\dfrac{\nu n}{p^{\mathrm{ord}_p(n)}} V \in \mathcal{S}^1(K|\mathbb{Q})$, we obtain

$$\begin{aligned}
\exp(\nu n p \int V(z)) &= \exp(-\nu n p \int X(z)) \exp(\nu n p \int (\mathrm{Frob}_p V(z^p))) \\
&\equiv \exp(\nu n p \int (\mathrm{Frob}_p V(z^p))) \mod p^{\mathrm{ord}_p(n)+1} \\
&= \exp\left(\nu n \sum_{k=1}^{\infty} \frac{a_{pk}}{k} z^{pk}\right).
\end{aligned}$$

Let us denote $\exp\left(\sum_{k=1}^{\infty} \dfrac{a_{pk}}{k} z^k\right) = 1 + \sum_{k=1}^{\infty} y_k z^k = Y(z)$ and

$$Y(z)^{\nu n} = \exp\left(\nu n \sum_{k=1}^{\infty} \frac{a_{pk}}{k} z^k\right) = \widetilde{Y}(z).$$

By Dwork's Integrality Theorem 2.15, we have

$$\widetilde{Y}(z), Y(z) \in \mathcal{O}_p[\![z]\!].$$

Set $\tilde{y}_m = \left[\widetilde{Y}(z)\right]_m$ for all $m \in \mathbb{N}_0$. Note that by Proposition 4.22,

$$\tilde{y}_m \equiv 0 \mod p^{\max\{0, \mathrm{ord}_p(\nu n) - \mathrm{ord}_p(m)\}}.$$

Then we compute the expression given in Corollary 4.20 explicitly

$$\begin{aligned}
&\frac{2}{p^2 n^2}(\mathrm{Frob}_p(a_n^+) - a_{pn}^+) \\
&\equiv -\nu \left[V(z) \cdot \left(\frac{\exp(\nu \int V(z))}{z}\right)^{pn} \cdot \int^2 (\mathrm{Frob}_p V(z^p) - V(z))\right]_0 \mod p^{\mathrm{ord}_p(n)+1-\delta_{p,3}} \mathcal{O}_p \\
&\equiv -\nu \left[\frac{V(z)}{z^{pn}} \widetilde{Y}(z^p) \int^2 X(z)\right]_0 \mod p^{\mathrm{ord}_p(n)+1-\delta_{p,3}} \mathcal{O}_p
\end{aligned}$$

$$= \nu \sum_{k=1}^{\infty} \sum_{\substack{\ell=1 \\ p\nmid\ell}}^{\infty} \sum_{m=0}^{\infty} \tilde{y}_m \frac{a_k a_\ell}{\ell^2} \left[z^{p(m-n)+k+\ell} \right]_0$$

$$= \nu \sum_{m=0}^{n} \tilde{y}_m \sum_{\substack{\ell=1 \\ p\nmid\ell}}^{p(n-m)} \frac{a_{p(n-m)-\ell} a_\ell}{\ell^2}, \tag{4.38}$$

where for the last step, we used $\left[z^{p(m-n)+k+\ell} \right]_0 = \delta_{k,p(n-m)-\ell}$. We need to compute

$$x(m) = \mathrm{Ord}_p \left(\nu \tilde{y}_m \sum_{\substack{\ell=1 \\ p\nmid\ell}}^{p(n-m)} \frac{a_{p(n-m)-\ell} a_\ell}{\ell^2} \right). \tag{4.39}$$

By Theorem 4.15 and Proposition 4.22 and respecting the p-adic estimation used in the calculation given in eq. (4.38), we obtain

$$x(m) \geq \min \left\{ \mathrm{ord}_p(n) + 1 - \delta_{p,3}, \max\{0, \mathrm{ord}_p(n) - \mathrm{ord}_p(m)\} + \max\{0, \mathrm{ord}_p(n-m) + 1 - \gamma_p\} \right\},$$

where γ_p is given as in Theorem 4.15.

- For $\mathrm{ord}_p(n) \geq \mathrm{ord}_p(m)$ and $\gamma_p \leq \mathrm{ord}_p(n-m) + 1$ we have

$$\begin{aligned} x(m) &\geq \min \left\{ \mathrm{ord}_p(n) + 1 - \delta_{p,3}, \mathrm{ord}_p(n) - \mathrm{ord}_p(m) + \mathrm{ord}_p(m) + 1 - \gamma_p \right\} \\ &= \mathrm{ord}_p(n) + 1 - \gamma_p \geq 0. \end{aligned}$$

- For $\mathrm{ord}_p(n) \geq \mathrm{ord}_p(m)$ and $\gamma_p > \mathrm{ord}_p(n-m) + 1$, then $-\mathrm{ord}_p(m) > 1 - \gamma_p$ and therefore

$$\begin{aligned} x(m) &\geq \min \left\{ \mathrm{ord}_p(n) + 1 - \delta_{p,N}, \mathrm{ord}_p(n) - \mathrm{ord}_p(m) + \mathrm{ord}_p(m) + 1 - \gamma_p \right\} \\ &= \mathrm{ord}_p(n) + 1 - \gamma_p \geq 0. \end{aligned}$$

- For $\mathrm{ord}_p(n) < \mathrm{ord}_p(m)$ and $\gamma_p \leq \mathrm{ord}_p(n-m) + 1$, we have

$$\begin{aligned} x(m) &\geq \min \left\{ \mathrm{ord}_p(n) + 1 - \delta_{p,N}, \mathrm{ord}_p(n) + 1 - \gamma_p \right\} \\ &= \mathrm{ord}_p(n) + 1 - \gamma_p \geq 0. \end{aligned}$$

- For $\mathrm{ord}_p(n) < \mathrm{ord}_p(m)$ and $\gamma_p > \mathrm{ord}_p(n-m)+1$, we have

$$\begin{aligned} x(m) &\geq \min\{\mathrm{ord}_p(n)+1-\delta_{p,N}, 0\} \\ &= 0 > \mathrm{ord}_p(n-m)+1-\gamma_p = \mathrm{ord}_p(n)+1-\gamma_p. \end{aligned}$$

Therefore, for $x := \min\{x(m) \mid m \in \{0,...,n\}\}$, we have

$$x \geq \max\{0, \mathrm{ord}_p(n)+1-\gamma_p\}.$$

Hence,

$$\mathrm{Frob}_p(a_n^+) - a_{pn}^+ \equiv 0 \mod p^{2(\mathrm{ord}_p(n)+1)-\delta_{2,p}+\max\{0,\mathrm{ord}_p(n)+1-\gamma_p\}}\mathcal{O}_p,$$

as stated. In particular, for $p \geq 5$ unramified in $K|\mathbb{Q}$, that does not divide N, we have (in this case, $\gamma_p = 0$)

$$\mathrm{Frob}_p(a_n^+) - a_{pn}^+ \equiv 0 \mod p^{3(\mathrm{ord}_p(n)+1)}\mathcal{O}_p.$$

Nonetheless, for

$$C = 2 \cdot \prod_{p \text{ prim}} p^{\gamma_p},$$

we have $C \cdot V^{(\nu,+)(z)} \in \mathcal{S}^3(K|\mathbb{Q})$, and therefore, $V^{(\nu,+)}(z) \in \overline{\mathcal{S}}^3(K|\mathbb{Q})$. □

4.5 Improved Integrality for Fractional Framing

In this section we will introduce the notion of fractional framing. For $\nu \in \mathbb{Q}$ and $V \in \mathcal{S}^2(K|\mathbb{Q})$, $V^{(-,\nu)}$ fails to fulfill the local 2-function property precisely at those p such that $\mathrm{ord}_p(\nu) < 0$. This can be fixed by applying the Cartier operator $\mathscr{C}_\sigma$ to $V^{(-,\nu)}$ with the obstruction $\mathrm{ord}_p(\sigma\nu) \geq 0$. This is referred to as *fractional framing*.

Theorem 4.23 (Integrality of Fractional Framing) *Let $V \in \mathcal{S}^2(K|\mathbb{Q})$ and $\nu \in \mathbb{Q}$ and $\rho, \sigma \in \mathbb{N}$, such that $\gcd(\rho,\sigma) = 1$ and $\nu\frac{\sigma}{\rho} \in \mathbb{Z}\left[D^{-1}\right]$. Then*

$$\frac{1}{\sigma}\varepsilon_\rho^{(2)}\left(\mathscr{C}_\sigma\left(\Phi^-(\nu,V)\right)\right) \in \mathcal{S}^2(K|\mathbb{Q})$$

and

$$\frac{1}{\sigma}\varepsilon_\rho^{(2)}\left(\mathscr{C}_\sigma\left(\Phi^+(\nu,V)\right)\right) \in \left(\mathcal{S}^2(K|\mathbb{Q})_{\{2\}} \cap \overline{\mathcal{S}}^2(K|\mathbb{Q})\right).$$

Proof. The proof we are presenting here follows the same arguments and steps as the proof of Theorem 4.12. As above, we assume $\nu \neq 0$.

We write $\widetilde{V} = \frac{1}{\sigma}\varepsilon_\rho^{(2)}\left(\mathscr{C}_\sigma\left(\Phi^-(\nu, V)\right)\right)$ and $\tilde{a}_n^- := \left[\widetilde{V}(z)\right]_n$ for all $n \in \mathbb{N}$. We have

$$\tilde{a}_n^- = \frac{\rho^2}{\sigma}\left[\mathscr{C}_\sigma V^{(\nu,-)}(z)\right]_{n/\rho} = \frac{\rho^2}{\sigma} a^-_{\sigma n/\rho},$$

with the understanding that $\tilde{a}_n^- = 0$, whenever $\rho \nmid n$. Then

$$\mathrm{Frob}_p(\tilde{a}_n^-) - \tilde{a}_{pn}^- = \begin{cases} 0, & \text{if } \rho \nmid pn, \\ -\frac{\rho^2}{\sigma} a^-_{\sigma pn/\rho}, & \text{if } \rho \mid pn, \text{ but } \rho \nmid n, \\ \frac{\rho^2}{\sigma}\left(\mathrm{Frob}_p\left(a^-_{\sigma n/\rho}\right) - a^-_{\sigma pn/\rho}\right), & \text{if } \rho \mid n. \end{cases}$$

In the first two cases, the local 2-function property at the prime p is trivially satisfied. For $\rho \mid n$, we still need to check

$$\mathrm{Frob}_p\left(a^-_{\sigma n/\rho}\right) - a^-_{\sigma pn/\rho} \equiv 0 \mod p^{2(\mathrm{ord}_p(n)+1-\mathrm{ord}_p(\rho))+\mathrm{ord}_p(\sigma)}\mathcal{O}_p.$$

In the following, we will assume $\mathrm{ord}_p(\rho) \leq \mathrm{ord}_p(n)$, which is an implementation of the condition $\rho \mid n$.

Case 1: $p \geq 3$. Let p be a prime number unramified in $K|\mathbb{Q}$ greater than 3. Recall that $a^-_{\sigma n/\rho} = (-1)^{\nu\frac{\sigma n}{\rho}} a^+_{\sigma n/\rho}$. As before, we write $\int^2 X(z) = \int^2 \left(\mathrm{Frob}_p V\left(z^p\right) - V(z)\right)$. Then by the same p-adic estimation as given in *Case 1* of the proof of Theorem 4.12, we have

$$\begin{aligned} \mathrm{Frob}_p\left(a^+_{\sigma n/\rho}\right) - a^+_{\sigma pn/\rho} &= \frac{1}{\nu}\left[\frac{\exp(\nu\frac{\sigma}{\rho} np \int V(z))}{z^{\sigma pn/\rho}} \cdot \left(\sum_{k=1}^{\infty} \frac{(\nu\frac{\sigma}{\rho} np \int X(z))^k}{k!}\right)\right]_0 \\ &= \left[\frac{\exp\left(\nu\frac{\sigma}{\rho} np \int V(z)\right)}{z^{\sigma pn/\rho}} \sum_{k=1}^{\infty} (\sigma\nu)^{k-1} \frac{\sigma}{k!}\left(\frac{np}{\rho}\right)^k \left(\int X(z)\right)^k\right]_0. \end{aligned}$$

Using $\mathrm{ord}_p(\sigma\nu) \geq 0$ and $\rho \mid n$ we obtain for $k \geq 2$

$$\begin{aligned} \mathrm{ord}_p\left((\sigma\nu)^{k-1}\frac{\sigma}{k!}\left(\frac{np}{\rho}\right)^k\right) &= k\,\mathrm{ord}_p\left(\frac{n}{\rho}p\right) + \mathrm{ord}_p(\sigma) + (k-1)\,\mathrm{ord}_p(\sigma\nu) \\ &\geq 2\,\mathrm{ord}_p\left(\frac{n}{\rho}p\right) + \mathrm{ord}_p(\sigma). \end{aligned}$$

Therefore,

$$\begin{aligned}
&\mathrm{Frob}_p(a^+_{\sigma n/\rho}) - a^+_{\sigma pn/\rho} \\
&\quad\equiv \frac{\sigma}{\rho} pn \left[\frac{\exp\left(\nu\frac{\sigma}{\rho} pn \int V(z)\right)}{z^{pn\sigma/\rho}} \cdot \int X(z) \right]_0 \mod p^{2(\mathrm{ord}_p(n)+1-\mathrm{ord}_p(\rho))+\mathrm{ord}_p(\sigma)}\mathcal{O}_p \\
&\quad= -\frac{\sigma}{\rho} pn \left[\delta\left(\frac{\exp(\nu\frac{\sigma}{\rho} pn \int V(z))}{z^{pn\sigma/\rho}} \right) \cdot \int^2 X(z) \right]_0 \\
&\quad= -\sigma \left(\frac{pn}{\rho}\right)^2 \cdot \left[(\sigma\nu V(z) - \sigma) \cdot \left(\frac{\exp(\nu \int V(z))}{z} \right)^{pn\sigma/\rho} \cdot \int^2 X(z) \right]_0 .
\end{aligned}$$

Since $\mathrm{ord}_p(\nu\sigma) \geq 0$, the expression in $[-]_0$ is a p-adic integer. Therefore,

$$\mathrm{Frob}_p\left(a^+_{\sigma n/\rho}\right) - a^+_{\sigma pn/\rho} = 0 \mod p^{2(\mathrm{ord}_p(n)+1-\mathrm{ord}_p(\rho))+\mathrm{ord}_p(\sigma)}\mathcal{O}_p.$$

Case 2: $p = 2$, *and* $\mathrm{ord}_2\left(\frac{\sigma n}{\rho}\nu\right) \geq 1$. Then, if $\frac{\sigma n}{\rho} \in \mathbb{Z}$,

$$\begin{aligned}
\mathrm{Frob}_2\left(a^-_{\sigma n/\rho}\right) - a^-_{2\sigma n/\rho} &= (-1)^{\nu\sigma n/\rho}\mathrm{Frob}_2\left(a^+_{\sigma n/\rho}\right) - (-1)^{2\nu\sigma n/\rho} a^+_{2\sigma n/\rho} \\
&= (-1)^{\nu\sigma n/\rho}\left(\mathrm{Frob}_2\left(a^+_{\sigma n/\rho}\right) - (-1)^{\nu\sigma n/\rho} a^+_{2\sigma n/\rho}\right) \\
&= (-1)^{\nu\sigma n/\rho}\left(\mathrm{Frob}_2\left(a^+_{\sigma n/\rho}\right) - a^+_{2\sigma n/\rho}\right)
\end{aligned}$$

Therefore, it suffices to check the congruence for $\mathrm{Frob}_2\left(a^+_{\sigma n/\rho}\right) - a^+_{2\sigma n/\rho}$ and we may assume $\frac{\sigma n}{\rho} \in \mathbb{Z}\left[D^{-1}\right]$. We have

$$\begin{aligned}
&\mathrm{Frob}_2\left(a^+_{\sigma n/\rho}\right) - a^+_{2\sigma n/\rho} \\
&\qquad = \left[\frac{\exp\left(2\nu\frac{\sigma}{\rho} n \int V(z)\right)}{z^{2\sigma n/\rho}} \left(\sum_{k=1}^{\infty} (\sigma\nu)^{k-1} \frac{\sigma}{k!} \left(\frac{2n}{\rho}\right)^k \left(\int X(z)\right)^k \right) \right]_0 .
\end{aligned}$$

For $k \geq 3$ we have

$$\begin{aligned}
&\mathrm{ord}_2\left((\sigma\nu)^{k-1} \frac{\sigma}{k!} \left(\frac{2n}{\rho}\right)^k \right) \\
&\qquad = k\,\mathrm{ord}_2\left(\frac{2n}{\rho}\right) + \mathrm{ord}_2(\sigma) + 1 + (k-1)\,\mathrm{ord}_2(\nu\sigma) - \mathrm{ord}_2(k!) - k + S_2(k)
\end{aligned}$$

$$= k \operatorname{ord}_2\left(\frac{n}{\rho}\right) + \operatorname{ord}_2(\sigma) + 1 + (k-1)\operatorname{ord}_2(\nu\sigma) - \operatorname{ord}_2(k!) + S_2(k).$$

Recall that $S_2(k)$ denotes the sum of the digits of k in base 2. Using $S_2(k) \geq 1$ for all $k \in \mathbb{N}$, $\operatorname{ord}_2\left(\frac{\sigma n}{\rho}\nu\right) \geq 1$, and $\operatorname{ord}_2(\nu\sigma) \geq 0$, we obtain

$$\begin{aligned}\operatorname{ord}_2\left((\sigma\nu)^{k-1}\frac{\sigma}{k!}\left(\frac{2n}{\rho}\right)^k\right) &\geq k\operatorname{ord}_2\left(\frac{n}{\rho}\right) + \operatorname{ord}_2(\sigma) + 1 + (k-1)\operatorname{ord}_2(\nu\sigma)\\ &\geq (k-1)\operatorname{ord}_2\left(\frac{n}{\rho}\right) + 2 + \operatorname{ord}_2(\sigma) + (k-2)\operatorname{ord}_2(\nu\sigma)\\ &\overset{k\geq 3}{\geq} 2\left(\operatorname{ord}_2\left(\frac{n}{\rho}\right) + 1\right) + \operatorname{ord}_2(\sigma).\end{aligned}$$

Therefore,

$$\begin{aligned}\operatorname{Frob}_2\left(a^+_{\sigma n/\rho}\right) - a^+_{2\sigma n/\rho} \equiv \frac{2\sigma n}{\rho}\Bigg[&\frac{\exp\left(2\nu\frac{\sigma}{\rho}n\int V(z)\right)}{z^{2\sigma n/\rho}}\times\\ &\times\left(\int X(z) + \nu\frac{\sigma}{\rho}n\left(\int X(z)\right)^2\right)\Bigg]_0 \mod 2^{2\left(\operatorname{ord}_2\left(\frac{n}{\rho}\right)+1\right)+\operatorname{ord}_2(\sigma)}\mathcal{O}_2.\end{aligned}$$

What remains to show is

$$\left[\frac{\exp\left(2\nu\frac{\sigma}{\rho}n\int V(z)\right)}{z^{2\sigma n/\rho}}\int X(z)\right]_0 \equiv 0 \mod 2^{\operatorname{ord}_2(n)-\operatorname{ord}_2(\rho)+1}\mathcal{O}_2 \tag{4.40}$$

and

$$\nu\sigma\left[\frac{\exp\left(2\nu\frac{\sigma}{\rho}n\int V(z)\right)}{z^{2\sigma n/\rho}}\left(\int X(z)\right)^2\right]_0 \equiv 0 \mod 2\mathcal{O}_2. \tag{4.41}$$

The first summand (a.k.a. eq. (4.40)) vanishes by the same calculation as in the previous case. Therefore, it remains to show eq. (4.41). By eq. (4.14), we have

$$\left(\int X(z)\right)^2 \equiv \sum_{\substack{i=1\\ i \text{ odd}}}^{\infty} x_i^2 z^{2i} \mod 2\mathcal{O}_2.$$

Hence,

$$\left[\frac{\exp\left(2\nu\frac{\sigma}{\rho}n\int V(z)\right)}{z^{2\sigma n/\rho}}\left(\int X(z)\right)^2\right]_0 \equiv \sum_{\substack{i=1\\ i \text{ odd}}}^{\infty} x_i^2\left[\exp\left(2\nu\frac{\sigma}{\rho}n\int V(z)\right)\right]_{2\left(\frac{\sigma n}{\rho}-i\right)} \mod 2\mathcal{O}_2.$$

Using Proposition 4.22, we find for all odd $i \in \mathbb{N}$, $i \leq \frac{\sigma}{\rho}n$,

$$\nu\sigma\left[\exp\left(2\nu\frac{\sigma}{\rho}n\int V(z)\right)\right]_{2\left(\frac{\sigma}{\rho}n-i\right)} \equiv 0 \mod 2\mathcal{O}_2, \tag{4.42}$$

since:

- if $\operatorname{ord}_2\left(\frac{\sigma n}{\rho}\right) \geq 1$, then $\operatorname{ord}_2\left(\frac{\sigma n}{\rho}-i\right) = \operatorname{ord}_2(i) = 0$ and therefore

$$\operatorname{ord}_2\left(2\nu\frac{\sigma}{\rho}n\right) - \operatorname{ord}_2\left(2\left(\frac{\sigma n}{\rho}-i\right)\right) \geq 2-1 = 1.$$

- if $\operatorname{ord}_2\left(\frac{\sigma n}{\rho}\right) = 0$, then $\operatorname{ord}_2(\nu) \geq 1$ (and therefore, $\operatorname{ord}_2(\nu\sigma) \geq 1$). In that case, the congruence eq. (4.42) is immediately satisfied, since the power series in the brackets $[-]_0$ has 2-adic integral coefficients by Dwork's Integrality Lemma.

Finally, we have

$$\operatorname{Frob}_2\left(a^+_{\sigma n/\rho}\right) - a^+_{2\sigma n/\rho} \equiv 0 \mod 2^{2(\operatorname{ord}_2(n)+1-\operatorname{ord}_2(\rho))+\operatorname{ord}_2(\sigma)}\mathcal{O}_2.$$

Case 3: Let $p = 2$, $\operatorname{ord}_2\left(\nu\frac{\sigma}{\rho}n\right) = 0$ and $\nu\frac{\sigma}{\rho} \in \mathbb{Z}$. First recall that $\gcd(\sigma,\rho) = 1$ by definition, $\operatorname{ord}_2(\rho) \leq \operatorname{ord}_2(n)$, since $\rho \mid n$ by assumption, and $\operatorname{ord}_2(\nu\sigma) \geq 0$. Therefore, we immediately see that $\operatorname{ord}_2\left(\frac{n}{\rho}\right) = \operatorname{ord}_2(\nu\sigma) = 0$. Indeed, since we assume $\operatorname{ord}_2\left(\nu\frac{\sigma}{\rho}n\right) = 0$, we have

$$0 \leq \operatorname{ord}_2\left(\frac{n}{\rho}\right) = -\operatorname{ord}_2(\nu\sigma) \leq 0.$$

Note that

$$(-1)^{\nu\sigma n/\rho}\left(\mathrm{Frob}_2\left(a^-_{n\sigma/\rho}\right)-a^-_{2n\sigma/\rho}\right)=\mathrm{Frob}_2\left(a^+_{n\sigma/\rho}\right)+a^+_{2n\sigma/\rho}.$$

Therefore, we need to show

$$\mathrm{Frob}_2\left(a^+_{n\sigma/\rho}\right)+a^+_{2n\sigma/\rho}\equiv 0 \mod 2^{2+\mathrm{ord}_2(\sigma)}\mathcal{O}_2.$$

We have

$$\begin{aligned}&\mathrm{Frob}_2\left(a^+_{n\sigma/\rho}\right)+a^+_{2n\sigma/\rho}\\ &\qquad\equiv\left[\frac{\exp\left(2\nu\frac{\sigma}{\rho}n\int V(z)\right)}{z^{2\sigma n/\rho}}\left(\frac{2}{\nu}+\sum_{k=1}^{\infty}(\nu\sigma)^{k-1}\frac{\sigma}{k!}\left(\frac{2n}{\rho}\right)^k(\int X(z))^k\right)\right]_0.\end{aligned}$$

For all $k\in\mathbb{N}$ such that $k\neq 2^\ell$ for some $\ell\in\mathbb{N}$, we have $\mathrm{ord}_2(k)\geq 2$ and therefore, for such k,

$$\begin{aligned}\mathrm{ord}_2\left((\nu\sigma)^{k-1}\frac{\sigma}{k!}\left(\frac{2n}{\rho}\right)^k\right)&=\mathrm{ord}_2(\sigma)+k-k+S_2(k)=\mathrm{ord}_2(\sigma)+S_2(k)\\ &\geq 2+\mathrm{ord}_2(\sigma).\end{aligned}$$

Also, note that $\mathrm{ord}_2\left(\frac{2^{2^\ell}}{(2^\ell)!}\right)=2^\ell-2^\ell+1=1$ for all $\ell\in\mathbb{N}$ – and hence $\frac{2^{2\ell}}{2(2^\ell)!}\equiv 1 \mod 2$ – we obtain

$$\begin{aligned}\mathrm{Frob}_2\left(a^+_{n\sigma/\rho}\right)+a^+_{2n\sigma/\rho}\equiv 2\sigma\Bigg[&\frac{\exp\left(2\nu\frac{\sigma}{\rho}n\int V(z)\right)}{z^{2\sigma n/\rho}}\times\cdots\\ &\cdots\times\left(\frac{1}{\nu\sigma}+\sum_{\ell=0}^{\infty}\frac{(\nu\sigma)^{2^\ell-1}}{2(2^\ell)!}\left(\frac{2n}{\rho}\right)^{2^\ell}(\int X(z))^{2^\ell}\right)\Bigg]_0 \mod 2^{2+\mathrm{ord}_2(\sigma)}\mathcal{O}_2.\end{aligned}$$

Note that $\frac{1}{\nu\sigma}\equiv\frac{n}{\rho}\equiv\frac{2^{2^\ell}}{2(2^\ell)!}\equiv 1 \mod 2\mathbb{Z}_2$, it remains to prove

$$\left[\frac{\exp\left(2\nu\frac{\sigma}{\rho}n\int V(z)\right)}{z^{2\sigma n/\rho}}\left(1+\sum_{\ell=0}^{\infty}(\int X(z))^{2^\ell}\right)\right]_0\equiv 0 \mod 2\mathcal{O}_2.$$

This follows by eq. (4.16) and eq. (4.8) as follows

$$\begin{aligned}
&\left[\frac{\exp\left(2\nu\frac{\sigma}{\rho}n\int V(z)\right)}{z^{2\sigma n/\rho}}\left(1+\sum_{\ell=0}^{\infty}\left(\int X(z)\right)^{2^\ell}\right)\right]_0 \\
&\qquad \overset{eq.\ (4.16)}{\equiv} \left[\frac{\exp\left(2\nu\frac{\sigma}{\rho}n\int V(z)\right)}{z^{2\sigma n/\rho}}\left(1+V(z)\right)\right]_0 \mod 2\mathcal{O}_2 \\
&\qquad \equiv \left[\frac{\exp\left(2\nu\frac{\sigma}{\rho}n\int V(z)\right)}{z^{2\sigma n/\rho}}\left(1-V(z)\right)\right]_0 \mod 2\mathcal{O}_2 \\
&\qquad \overset{eq.\ (4.8)}{\equiv} 0 \mod 2\mathcal{O}_2
\end{aligned}$$

This finishes the proof. □

Remark 4.24 As in Remark 4.13, we like to point out that we have an analogue statement of Theorem 4.23 for Φ^+. Let $V \in \mathcal{S}^2(K|\mathbb{Q})$, $\sigma, \rho \in \mathbb{N}$, and $\nu \in \mathbb{Q}$, such that $\nu\frac{\sigma}{\rho} \in \mathbb{Z}\left[D^{-1}\right]$, $\gcd(\sigma,\rho)=1$ and $\mathrm{ord}_2\left(\nu\frac{\sigma}{\rho}n\right)=0$ (which is the setting of *Case 3* in the above proof). We then still find

$$\mathrm{Frob}_2\left(a^+_{\sigma n/\rho}\right) - a^+_{2\sigma n/\rho} \equiv 0 \mod 2\mathcal{O}_2.$$

Therefore, we may preserve 2-integrality for fractional framing of by multiplying with 2,

$$2\cdot\varepsilon^{(2)}_\rho\left(\mathscr{C}_\sigma\left(\Phi^+(\nu,V)\right)\right) \in \mathcal{S}^2(K|\mathbb{Q}).$$

Theorem 4.25 (Improved Integrality for Fractional Framing) *Let $\rho,\sigma\in\mathbb{N}$ with $\gcd(\rho,\sigma)=1$. Then*

$$\left(\frac{1}{\sigma}\varepsilon^{(3)}_\rho\circ\mathscr{C}_\sigma\circ\Phi^{+/-}\right)\left(\left(\frac{\rho}{\sigma}\mathbb{Z}\right)\times\mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})\right)\subset\overline{\mathcal{S}}^3(K|\mathbb{Q})_{\mathrm{fin}}.$$

More precisely, for a rational 2-function $V\in\mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$ of periodicity N and $\nu\in\frac{\rho}{\sigma}\mathbb{Z}$ and $S=\{p \text{ prim with } p\mid N\}\cup\{2,3\}$,

$$\widetilde{V}(z) := \frac{1}{\sigma}\varepsilon^{(3)}_\rho\left(\mathscr{C}_\sigma\left(\Phi^+(\nu,V)\right)\right)\in\mathcal{S}^3(K|\mathbb{Q})_S.$$

For $\tilde{a}_n^+ = \left[\widetilde{V}(z)\right]_n$, $n \in \mathbb{N}$ *we have*

$$\mathrm{Frob}_p\left(\tilde{a}_n^+\right) - \tilde{a}_{pn}^+ \equiv 0 \mod p^{2\,\mathrm{ord}_p(pn)+\mathrm{ord}_p(\rho)-\delta_{2,p}+\max\{0,\mathrm{ord}_p\left(\frac{pn}{\rho}\right)-\gamma_p\}}\mathcal{O}_p,$$

where γ_p *is equal to* $1+\mathrm{ord}_2(N+1)$, 1 *and* 0 *if* p *is equal to* 2, 3 *and greater than* 3, *respectively. In particular, for unramified* $p \geq 5$ *in* $K|\mathbb{Q}$ *with* $p \nmid N$,

$$\mathrm{Frob}_p\left(\tilde{a}_n^+\right) - \tilde{a}_{pn}^+ \equiv 0 \mod p^{3(\mathrm{ord}_p(n)+1)}\mathcal{O}_p.$$

Proof. The proof we are presenting here follows the same arguments and steps as the proof of Theorem 4.12. In the following we assume $\nu \neq 0$.
We write $\widetilde{V}(z) = \frac{1}{\sigma}\varepsilon_\rho^{(3)}\left(\mathscr{C}_\sigma\left(\Phi^+(\nu,V)\right)\right)$ and $\tilde{a}_n^+ := \left[\widetilde{V}(z)\right]_n$ for all $n \in \mathbb{N}$. We have

$$\tilde{a}_n^+ = \frac{1}{\sigma}\left[\varepsilon_\rho^{(3)}\left(\mathscr{C}_\sigma\left(\Phi^+(\nu,V)\right)\right)\right]_n = \frac{\rho^3}{\sigma}\left[\mathscr{C}_\sigma V^{(\nu,+)}(z)\right]_{n/\rho} = \frac{\rho^3}{\sigma}a_{\sigma n/\rho}^+,$$

with the understanding that $a_{\sigma n/\rho}^+ = 0$, whenever $\rho \nmid n$. Then

$$\mathrm{Frob}_p(\tilde{a}_n^+) - \tilde{a}_{pn}^+ = \begin{cases} 0, & \text{if } \rho \nmid pn, \\ -\dfrac{\rho^3}{\sigma}a_{\sigma pn/\rho}^+, & \text{if } \rho \mid pn, \text{ but } \rho \nmid n, \\ \dfrac{\rho^3}{\sigma}\left(\mathrm{Frob}_p\left(a_{\sigma n/\rho}^+\right) - a_{\sigma pn/\rho}^+\right), & \text{if } \rho \mid n. \end{cases}$$

For $\rho \nmid pn$, and $\rho \mid pn$ but $\rho \nmid n$, the local 3-function property at the prime p for the coefficients a_n^+ is trivially satisfied. For $\rho \mid n$, we still need to check

$$\mathrm{Frob}_p\left(a_{n\sigma/\rho}^+\right) - a_{pn\sigma/\rho}^+ \equiv 0 \mod p^{2\,\mathrm{ord}_p\left(\frac{pn}{\rho}\right)-\delta_{2,p}+\mathrm{ord}_p(\sigma)+\max\left\{0,\mathrm{ord}_p\left(\frac{pn}{\rho}\right)-\gamma_p\right\}}\mathcal{O}_p.$$

In the following, we will assume $\mathrm{ord}_p(\rho) \leq \mathrm{ord}_p(n)$.

Step 1: Analogue to Lemma 4.19. Here, we only assume $V \in \mathcal{S}^3(K|\mathbb{Q})$ and set $X(z) = \mathrm{Frob}_p V(z^p) - V(z)$. We have

$$\mathrm{Frob}_p\left(a_{\sigma n/\rho}^+\right) - a_{p\sigma n/\rho}^+ = \left[\frac{\exp\left(\nu\frac{\sigma n}{\rho}p\int V(z)\right)}{z^{p\sigma n/\rho}} \cdot \sum_{k=1}^{\infty}(\nu\sigma)^{k-1}\frac{\sigma}{k!}\left(\frac{np}{\rho}\right)^k\left(\int X(z)\right)^k\right]_0.$$

For $p \geq 3$ and $k \geq 4$

$$\mathrm{ord}_p\left(\frac{\sigma}{k!}\left(\frac{np}{\rho}\right)^k\right) \overset{k\geq 4}{\geq} 4\,\mathrm{ord}_p\left(\frac{n}{\rho}\right) + 2 + \mathrm{ord}_p(\sigma) + \frac{1}{2}$$

$$> 3\,\mathrm{ord}_p\left(\frac{n}{\rho}\right) + 2 + \mathrm{ord}_p(\sigma),$$

$$\Rightarrow \mathrm{ord}_p\left(\frac{\sigma}{k!}\left(\frac{np}{\rho}\right)^k\right) \geq 3\left(\mathrm{ord}_p\left(\frac{n}{\rho}\right)+1\right) + \mathrm{ord}_p(\sigma).$$

For $p=2$, $k\geq 4$ and $\mathrm{ord}_2\left(\nu\frac{\sigma}{\rho}n\right) > 0$, we have

$$\begin{aligned}
\mathrm{ord}_2\left((\nu\sigma)^{k-1}\frac{\sigma}{k!}\left(\frac{2n}{\rho}\right)^k\right) &= (k-1)\,\mathrm{ord}_2(\nu\sigma) + k\,\mathrm{ord}_2\left(\frac{n}{\rho}\right) + \mathrm{ord}_2(\sigma) + 1 \\
&\geq 3\,\mathrm{ord}_2(\nu\sigma) + 4\,\mathrm{ord}_2\left(\frac{n}{\rho}\right) + \mathrm{ord}_2(\sigma) + 1 \\
&= 2\,\mathrm{ord}_2(\nu\sigma) + 3\,\mathrm{ord}_2\left(\frac{n}{\rho}\right) + \mathrm{ord}_2(\sigma) + 1 + \mathrm{ord}_2\left(\nu\frac{\sigma}{\rho}n\right) \\
&> 3\,\mathrm{ord}_2\left(\frac{n}{\rho}\right) + 2 + \mathrm{ord}_2(\sigma).
\end{aligned}$$

For $k=3$ we still have

$$\mathrm{ord}_p\left((\nu\sigma)^2\frac{\sigma}{3!}\left(\frac{pn}{\rho}\right)^3\right) = \begin{cases} 3(\mathrm{ord}_p\left(\frac{n}{\rho}\right)+1) + \mathrm{ord}_p(\sigma), & \text{for } p\geq 5, \text{ and} \\ 3\left(\mathrm{ord}_p\left(\frac{n}{\rho}\right)+1\right) + \mathrm{ord}_p(\sigma) - 1, & \text{for } p\in\{2,3\}. \end{cases}$$

Therefore, analogously to eq. (4.30) and eq. (4.31), we obtain

$$\begin{aligned}
&\frac{\rho}{np\sigma}\cdot\left(\mathrm{Frob}_p\left(a^+_{\sigma n/\rho}\right) - a^+_{p\sigma n/\rho}\right) \equiv \\
&\left[\frac{\exp\left(\nu\frac{\sigma}{\rho}np\int V(z)\right)}{z^{p\sigma n/\rho}}\left(\int X(z) + \frac{\nu np\sigma}{2\rho}(\int X(z))^2\right)\right]_0 \mod p^{2\left(\mathrm{ord}_p\left(\frac{n}{\rho}\right)+1\right)-\epsilon_p}\mathcal{O}_p,
\end{aligned}$$

where $\epsilon_p = 0$ for all $p\geq 5$, and $\epsilon_p = 1$ for $p\in\{2,3\}$. By the same calculation as in the proof of Lemma 4.19 we obtain

$$\begin{aligned}
&\frac{2\rho^2}{p^2n^2\sigma}\cdot\left(\mathrm{Frob}_p\left(a^+_{\sigma n/\rho}\right) - a^+_{pn\sigma/\rho}\right) \equiv \nu\sigma\left[\delta\left(\mathrm{Frob}_p V(z^p) + V(z)\right)\times\cdots\right. \\
&\left.\cdots\times\left(\frac{\exp(\nu\int V(z))}{z}\right)^{pn\sigma/\rho}\cdot\int^3\left(\mathrm{Frob}_p V(z^p) - V(z)\right)\right]_0 \mod p^{\mathrm{ord}_p\left(\frac{n}{\rho}\right)+1-\delta_{3,p}}\mathcal{O}_p.
\end{aligned}$$

Step 2: Analogue to Corollary 4.20. From now on, we will additionally assume $V\in\mathcal{S}^\infty(K|\mathbb{Q})$. Then the same calculation (i.e. by the partial integration principle

eq. (2.2)) as in the proof of Corollary 4.20 leads directly the p-adic estimation

$$\frac{2\rho^2}{p^2n^2\sigma}\cdot\left(\mathrm{Frob}_p\left(a^+_{n\sigma/\rho}\right)-a^+_{pn\sigma/\rho}\right)\equiv\nu\sigma\left[V(z)\cdot\left(\frac{\exp(\nu\int V(z))}{z}\right)^{pn\sigma/\rho}\times\cdots\right.$$
$$\left.\cdots\times\int^2\left(\mathrm{Frob}_pV(z^p)-V(z)\right)\right]_0\mod p^{\mathrm{ord}_p\left(\frac{n}{\rho}\right)+1-\delta_{3,p}}\mathcal{O}_p.$$

Step 3: We now assume $V\in\mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})\subset\mathcal{S}^\infty(K|\mathbb{Q})_{\mathrm{fin}}$. More precisely, we have $V\in\mathcal{S}^\infty(K|\mathbb{Q})_S$. In the following we assume $p\nmid N$. By Lemma 4.21, we immediately notice

$$\exp\left(\nu\frac{pn\sigma}{\rho}\int V(z)\right)\equiv\exp\left(\nu\frac{n\sigma}{\rho}\sum_{k=1}^{\infty}\frac{a_{pk}}{k}z^{pk}\right)\mod p^{\mathrm{ord}_p\left(\nu\frac{\sigma}{\rho}n\right)+1}\mathcal{O}_p.$$

For $\widetilde{Y}(z):=\exp\left(\nu\frac{n\sigma}{\rho}\sum_{k=1}^{\infty}\frac{a_{pk}}{k}z^{pk}\right)$ we have by Proposition 4.22, and since $\mathrm{ord}_p\left(\nu\frac{\sigma}{\rho}\right)\geq 0$,

$$\tilde{y}_m:=\left[\widetilde{Y}(z)\right]_m\equiv 0\mod p^{\max\left\{0,\mathrm{ord}_p\left(\nu\frac{\sigma}{\rho}n\right)-\mathrm{ord}_p(m)\right\}}\mathcal{O}_p.$$

By the previous two steps and some calculation

$$\frac{2\rho^2}{p^2n^2\sigma}\cdot\left(\mathrm{Frob}_p\left(a^+_{n\sigma/\rho}\right)-a^+_{pn\sigma/\rho}\right)$$
$$\equiv\nu\sigma\sum_{m=0}^{\sigma n/\rho}\tilde{y}_m\sum_{\substack{\ell=1\\ p\nmid\ell}}^{p\left(\frac{\sigma n}{\rho}-m\right)}\frac{a_{p\left(\frac{\sigma n}{\rho}-m\right)-\ell}a_\ell}{\ell^2}\mod p^{\mathrm{ord}_p\left(\frac{n}{\rho}\right)+1-\delta_{3,p}}\mathcal{O}_p. \tag{4.43}$$

We need to give an estimation for $x(m)$, $m=0,...,\frac{\sigma n}{\rho}$, defined by

$$x(m)=\mathrm{Ord}_p\left(\nu\sigma\tilde{y}_m\sum_{\substack{\ell=1\\ p\nmid\ell}}^{p\left(\frac{\sigma n}{\rho}-m\right)}\frac{a_{p\left(\frac{\sigma n}{\rho}-m\right)-\ell}a_\ell}{\ell^2}\right). \tag{4.44}$$

For $m=0$ we have $\tilde{y}_0=1$ and by Theorem 4.15,

$$x(0)\geq\min\left\{\mathrm{ord}_p(n)-\mathrm{ord}_p(\rho)+1-\delta_{3,p},\max\{0,\mathrm{ord}_p(n)-\mathrm{ord}_p(\rho)+1-\gamma_p\}\right\}$$

$$= \max\left\{0, \operatorname{ord}_p\left(\frac{n}{\rho}\right) + 1 - \gamma_p\right\}.$$

Therefore, we may assume $m > 0$ in the following. By Theorem 4.15 and Proposition 4.22 we obtain (for $m > 0$)

$$x(m) \geq \min\left\{\operatorname{ord}_p\left(\frac{pn}{\rho}\right) - \delta_{3,p}, \operatorname{ord}_p(\nu\sigma) + \max\left\{0, \operatorname{ord}_p\left(\frac{\nu n\sigma}{\rho m}\right)\right\} + \max\left\{0, \operatorname{ord}_p\left(\frac{\sigma n}{\rho} - m\right) + 1 - \gamma_p\right\}\right\},$$

Taking into account, that $\operatorname{ord}_p(\nu\sigma) \geq 0$ for all unramified primes p, we immediately get

$$x = x(m) \geq \min\left\{\operatorname{ord}_p\left(\frac{pn}{\rho}\right) - \delta_{3,p}, \max\left\{0, \operatorname{ord}_p\left(\frac{n}{\rho m}\right)\right\} + \max\left\{0, \operatorname{ord}_p\left(\frac{\sigma n}{\rho} - m\right) + 1 - \gamma_p\right\}\right\}.$$

Recall that we assume $\rho \mid n$ and $\gcd(\sigma, \rho) = 1$. In particular this means $\operatorname{ord}_p(\rho) \leq \operatorname{ord}_p(n)$ for all primes p.

- If $\operatorname{ord}_p\left(\frac{n}{\rho m}\right) \geq 0$ and $\operatorname{ord}_p\left(\frac{\sigma n}{\rho} - m\right) + 1 \geq \gamma_p$, then $\operatorname{ord}_p\left(\frac{\sigma n}{\rho} - m\right) = \operatorname{ord}_p(m)$ and hence

$$\begin{aligned} x &\geq \min\left\{\operatorname{ord}_p\left(\frac{pn}{\rho}\right) - \delta_{3,p}, \operatorname{ord}_p\left(\frac{n}{\rho m}\right) + \operatorname{ord}_p(m) + 1 - \gamma_p\right\} \\ &= \operatorname{ord}_p\left(\frac{pn}{\rho}\right) - \gamma_p \geq 0. \end{aligned}$$

- If $\operatorname{ord}_p\left(\frac{n}{\rho m}\right) \geq 0$ and $\operatorname{ord}_p\left(\frac{\sigma n}{\rho} - m\right) + 1 < \varepsilon_{p,N}$, then $\operatorname{ord}_p\left(\frac{\sigma n}{\rho} - m\right) = \operatorname{ord}_p(m)$ and $-\operatorname{ord}_p(m) > 1 - \gamma_p$. Hence

$$\begin{aligned} x &\geq \min\left\{\operatorname{ord}_p\left(\frac{pn}{\rho}\right) - \delta_{3,p}, \operatorname{ord}_p\left(\frac{n}{\rho}\right) - \operatorname{ord}_p(m)\right\} \\ &\geq \max\left\{0, \min\left\{\operatorname{ord}_p\left(\frac{pn}{\rho}\right) - \delta_{3,p}, \operatorname{ord}_p\left(\frac{n}{\rho}\right) + 1 - \gamma_p\right\}\right\} \\ &= \max\left\{0, \operatorname{ord}_p\left(\frac{pn}{\rho}\right) - \gamma_p\right\}. \end{aligned}$$

- If $\operatorname{ord}_p\left(\frac{n}{\rho m}\right) < 0$ and $\operatorname{ord}_p\left(\frac{\sigma n}{\rho} - m\right) + 1 \geq \gamma_p$, then, in particular,

$$\min\left\{\operatorname{ord}_p\left(\frac{\sigma n}{\rho}\right), \operatorname{ord}_p(m)\right\} \geq \operatorname{ord}_p\left(\frac{n}{\rho}\right).$$

  Hence,

$$\begin{aligned} x &\geq \min\left\{\operatorname{ord}_p\left(\frac{pn}{\rho}\right) - \delta_{3,p}, \operatorname{ord}_p\left(\frac{n}{\rho m}\right) + 1 - \gamma_p\right\} \\ &\geq \max\left\{0, \min\left\{\operatorname{ord}_p\left(\frac{pn}{\rho}\right) - \delta_{3,p}, \right.\right. \\ &\qquad\qquad \left.\left. \min\left\{\operatorname{ord}_p\left(\frac{\sigma n}{\rho}\right), \operatorname{ord}_p(m)\right\} + 1 - \gamma_p\right\}\right\} \\ &\geq \max\left\{0, \min\left\{\operatorname{ord}_p\left(\frac{pn}{\rho}\right) - \delta_{3,p}, \operatorname{ord}_p\left(\frac{n}{\rho}\right) + 1 - \gamma_p\right\}\right\} \\ &\geq \max\left\{0, \operatorname{ord}_p\left(\frac{pn}{\rho}\right) - \gamma_p\right\}. \end{aligned}$$

- If $\operatorname{ord}_p\left(\frac{n}{\rho m}\right) < 0$ and $\operatorname{ord}_p\left(\frac{\sigma n}{\rho} - m\right) + 1 < \gamma_p$, then $x \geq 0$. On the other hand,

$$\begin{aligned} \operatorname{ord}_p\left(\frac{pn}{\rho}\right) - \gamma_p &\leq \min\left\{\operatorname{ord}_p\left(\frac{\sigma n}{\rho}\right), \operatorname{ord}_p(m)\right\} + 1 - \gamma_p \\ &\leq \operatorname{ord}_p\left(\frac{\sigma n}{\rho} - m\right) + 1 - \gamma_p < 0. \end{aligned}$$

Summarizing the above considerations, we obtain

$$\min_{m \in \{0,\ldots,\sigma n/\rho\}} x(m) \geq \max\left\{0, \operatorname{ord}_p\left(\frac{pn}{\rho}\right) - \gamma_p\right\}.$$

Therefore,

$$\nu\sigma \sum_{m=0}^{\sigma n/\rho} \tilde{y}_m \sum_{\substack{\ell=1 \\ p \nmid \ell}}^{p\left(\frac{\sigma n}{\rho} - m\right)} \frac{a_{p\left(\frac{\sigma n}{\rho} - m\right) - \ell} a_\ell}{\ell^2} \equiv 0 \mod p^{\max\left\{0, \operatorname{ord}_p\left(\frac{pn}{\rho}\right) - \gamma_p\right\}} \mathcal{O}_p.$$

Consequently, by eq. (4.43), we obtain – except for the case $p = 2$ and $\operatorname{ord}_2\left(\nu\frac{\sigma}{\rho}n\right) = 0$ –

$$\operatorname{Frob}_p\left(a^+_{n\sigma/\rho}\right) - a^+_{pn\sigma/\rho} \equiv 0 \mod p^{2\operatorname{ord}_p\left(\frac{pn}{\rho}\right) - \delta_{2,p} + \operatorname{ord}_p(\sigma) + \max\left\{0, \operatorname{ord}_p\left(\frac{pn}{\rho}\right) - \gamma_p\right\}} \mathcal{O}_p.$$

This finishes the proof. □

Example 4.26 (Jacobsthal-Kazandzidis) Let $V(z) = \dfrac{z}{1-z} \in \mathcal{S}^2_{\mathrm{rat}}(\mathbb{Q})$ and $\nu = \dfrac{\rho}{\sigma}$ with $\rho, \sigma \in \mathbb{N}$, $\gcd(\rho, \sigma) = 1$. V has periodicity $N = 1$ and

$$\int V(z) = \int \left(\frac{z}{1-z}\right) = \sum_{k=1}^{\infty} \frac{z^k}{k} = -\log(1-z).$$

As always, $a_n^+ := \left[\Phi^+(\nu, V)\right]_n$ Recall from eq. (4.5)

$$a_n^+ = \frac{1}{\nu}\left[\frac{\exp(\nu n \int V(z))}{z^n}\right]_0, \quad \text{for all } n \in \mathbb{N}.$$

Then

$$a_n^+ = \frac{1}{\nu}\left[\frac{1}{z^n}(1-z)^{-\nu n}\right]_0.$$

By the *generalized Binomial Theorem* we have

$$(1-z)^{-\nu n} = \sum_{k=0}^{\infty} \binom{-\nu n}{k} (-1)^k z^k.$$

Note, in this case the binomial coefficient is defined by

$$\binom{-\nu n}{k} = \frac{1}{k!} \prod_{j=0}^{k-1} (-\nu n - j). \tag{4.45}$$

Rewriting the binomial coefficient, we obtain

$$\begin{aligned}
\binom{-\nu n}{k} &= \frac{1}{k!} \prod_{j=0}^{k-1} (\nu n + k - 1 - j) \\
&= \frac{(-1)^k}{k!} \prod_{j=1}^{k} (\nu n + k - j) \\
&= \frac{(-1)^k}{k!} \frac{\nu n}{\nu n + k} \prod_{j=0}^{k-1} (\nu n + k - j) \\
&= (-1)^k \frac{\nu n}{\nu n + k} \binom{\nu n + k}{k}.
\end{aligned}$$

Therefore,

$$\begin{aligned} a_n^+ &= \frac{1}{\nu}\left[\frac{1}{z^n}\sum_{k=0}^{\infty}\frac{\nu n}{\nu n+k}\binom{\nu n+k}{k}z^k\right]_0 \\ &= \frac{1}{\nu+1}\binom{(\nu+1)n}{n}. \end{aligned}$$

In particular, for $\widetilde{V}(z) = \frac{1}{\sigma}\mathscr{C}_\sigma\left(\Phi^+(\nu, V)\right)$,

$$a_{\sigma n}^+ = \left[\widetilde{V}(z)\right]_n = \frac{1}{\rho+\sigma}\binom{(\rho+\sigma)n}{\sigma n}.$$

Applying Theorem 4.25 to $\widetilde{V}(z)$ gives for all primes $p \geq 3$

$$a_{\sigma n}^+ - a_{\sigma pn}^+ \equiv 0 \mod p^{3(\mathrm{ord}_p(n)+1)-\delta_{p,3}}\mathbb{Z}_p.$$

On the other hand for $p \geq 3$

$$a_{\sigma n}^+ - a_{\sigma pn}^+ = \frac{1}{\rho+\sigma}\left[\binom{(\rho+\sigma)n}{\sigma n} - \binom{(\rho+\sigma)pn}{\sigma pn}\right].$$

Therefore,

$$\begin{aligned} \binom{(\rho+\sigma)n}{\sigma n} - \binom{(\rho+\sigma)pn}{\sigma pn} &= (\rho+\sigma)\left(a_{\sigma n}^+ - a_{\sigma pn}^+\right) \\ &\equiv 0 \mod p^{3(\mathrm{ord}_p(n)+1)-\delta_{p,3}+\mathrm{ord}_p(\rho+\sigma)}. \end{aligned}$$

Hence,

$$\binom{(\rho+\sigma)pn}{\sigma pn} \equiv \binom{(\rho+\sigma)n}{\sigma n} \mod p^{3(\mathrm{ord}_p(n)+1)-\delta_{p,3}+\mathrm{ord}_p(\rho+\sigma)}. \tag{4.46}$$

Now we will prove the Theorem of Jacobsthal-Kazandzidis (see Theorem 4.18) for $p \geq 3$ as a consequence of Theorem 4.25. Fix a prime $p \geq 3$, let $a, b \in \mathbb{N}_0$ be non-negative integers and let $r \in \mathbb{N}$ be an integer. W. l. o. g., let $b \leq a$ and $\gamma = \min\{\mathrm{ord}_p(a), \mathrm{ord}_p(b)\}$. Then either $bp^{-\gamma}$ or $(a-b)p^{-\gamma}$ is a p-adic unit. Since the binomial coefficient is symmetric (that is, $\binom{a}{b}$ invariant under the exchange $b \leftrightarrow a-b$), we may assume that $bp^{-\gamma}$ is a p-adic integer. Then Theorem 4.18 follows from eq. (4.46) by setting $\sigma = p^{-\gamma}b$, $\rho = p^{-\gamma}(a-b)$

and $n = p^{\gamma+r-1}$, i.e.

$$\binom{ap^r}{bp^r} \equiv \binom{ap^{r-1}}{bp^{r-1}} \mod p^{3(r+\gamma)-\delta_{p,3}}.$$

Chapter 5
Conclusion and Outlook

This work was dedicated to understand algebraic and analytic properties of s-functions with algebraic coefficients. In the present chapter, we conclude with an outlook on future directions on research.

5.1 Algebraic s-Functions

As a next step beyond rational 2-functions, one should work on a description of algebraic 2-functions. As in the rational case, we may instead consider an element $V \in \mathcal{S}^2_{\mathrm{alg}}(K|\mathbb{Q})$. Of course, this reduction is supported by Proposition 3.4. Algebraicity of V should still accommodate many regularities among the Frobenius endomorphisms at all (unramified) primes and their local s-function properties, which should only be possible, if the Frobenius elements commute. We may find a similar result as in the rational case. This leads to

Conjecture 5.1 *Let $V \in \mathcal{S}^2_{\mathrm{alg}}(K|\mathbb{Q})$ be the generating function of a 2-sequence representing an algebraic function. Then the coefficients $[V(z)]_n$, $n \in \mathbb{N}$, of V lie in a cyclotomic field.*

Generally, the following formula describes the coefficients of the Maclaurin expansion of an algebraic function.

Theorem 5.2 (Flajolet-Soria, [5], [20]) *Let $P \in K[z, y]$ be a polynomial in two variables (z, y), such that $P(0, 0) = 0$, $\dfrac{\partial}{\partial y}P(0, 0) = 0$ and $P(z, 0) \neq 0$. Let $f(z)$ be the algebraic function implicitly defined by $P(z, f(z)) = 0$. Then, the Maclaurin coefficients f_n of $f(z)$ are given by the finite sum*

$$f_n = \sum_{m \geq 1} \frac{1}{m} [z^n y^{m-1}] P^m(z, y).$$

By applying the Multinomial Theorem we may rewrite

$$f_n = \sum_{m\geq 1} \frac{1}{m} \sum_{\substack{m_1+\cdots+m_d=m \\ b_1m_1+\cdots+b_dm_d=n \\ c_1m_1+\cdots+c_dm_d=m-1}} \binom{m}{m_1,\ldots,m_d} a_1^{m_1}\cdots a_d^{m_d}.$$

This Flajolet–Soria formula (FSF) was first published in the habilitation thesis of Michèle Soria in 1990. So the straight forward idea is to combine the FSF with the local 2-function congruence condition eq. (2.6) at every unramified prime.

Another approach to tackle Conjecture 5.1 might be a detour over s-functions of several variables. Let $\mathbf{z} := (z_1, ..., z_n)$ be the n-tupel of the n variables $z_1, ..., z_n$. For a multiindex $\mathbf{k} \in \mathbb{Z}^n$ we use the notation $\mathbf{z}^{\mathbf{k}} = z_1^{k_1} z_2^{k_2} ... z_n^{k_n}$.

Definition 5.3 Let $s \in \mathbb{N}$. We say that a Laurent series in several variables

$$V(z) = \sum_{\mathbf{k}\in\mathbb{Z}^n} a_{\mathbf{k}}\mathbf{z}^{\mathbf{k}} \in \mathcal{O}\left[D^{-1}\right]\left[\!\left[\mathbf{z}^{\pm 1}\right]\!\right]$$

satisfies the local s-function property with respect to the prime p, unramified in $K|\mathbb{Q}$, if

$$\mathrm{Frob}_p(a_{\mathbf{m}p^{r-1}}) \equiv a_{\mathbf{m}p^r} \mod p^{sr}\mathcal{O}_p.$$

for all $\mathbf{m} \in \mathbb{Z}^n$ and $r \in \mathbb{N}$. We also say that f satisfies the s-function property if it satisfies the local s-function property for all $p \nmid D$.

For a formal power series $f \in K[\![z_1, z_2]\!]$

$$f(z_1, z_2) = \sum_{n_1,n_2=1}^{\infty} a_{n_1,n_2} z_1^{n_1} z_2^{n_2}$$

its *diagonal* $\mathscr{D}f(z)$ is defined as the element in $K[\![z]\!]$ given by

$$\mathscr{D}f(z) = \sum_{n=1}^{\infty} a_{n,n} z^n.$$

It is a well-known fact that the diagonal $\mathscr{D}f$ of a power series $f \in K[\![z_1, z_2]\!]$ represents an algebraic function. Conversely, Furstenberg proved in [14] that algebraic functions appear as diagonals of rational functions in two variables:

Theorem 5.4 (Furstenberg, [14]) *Let $P(z, y)$ be a polynomial in the variables y, z and let $\varphi(z) \in K[\![z]\!]$ a formal power series in satisfying $P(z, \varphi(z)) = 0$. If $(\partial P/\partial y)(0, 0) \neq$*

0, *then*

$$\varphi = \mathscr{D}\left(y^2 \frac{\frac{\partial P}{\partial y}(zy, y)}{P(zy, y)}\right) \tag{5.1}$$

Of course, it is not clear if every element $V \in \mathcal{S}^2_{\mathrm{alg}}(K|\mathbb{Q})$ can be embedded as the diagonal in a rational 2-function in the variables z_1, z_2, but we reach a subclass of these functions. In fact, the main result in [7], Thm. 1.1 therein, can be formulated for rational 1-functions in several variables as follows

Theorem 5.5 *Let $m \leq n$ and let $f_1, ..., f_m \in \mathcal{O}(\mathbf{z})$ be nonzero. Then the rational function*

$$\frac{z_1 \cdots z_m}{f_1 \cdots f_m} \det\left(\frac{\partial f_j}{\partial x_i}\right)_{i,j=1,\ldots,m}$$

has the 1*-function property.*

Also, Prop. 3.4, Prop. 3.5, Cor. 3.7, Cor 3.8 and Thm. 5.4 in [7] can be translated verbatim to the setting of s-functions (mainly by substituting the term *"Gauß property"* in [7] by 1-function property) to obtain the following statement.

Theorem 5.6 *Let $P, Q \in \mathcal{O}[z, \mathbf{x}]$ such that Q is linear in the variables $x_1, ..., x_n$. Write $P = \sum_{\mathbf{k}} p_{\mathbf{k}}(z)\mathbf{x}^{\mathbf{k}}$ and $Q = \sum_{\mathbf{k}} q_{\mathbf{k}}(z)\mathbf{x}^{\mathbf{k}}$ with $p_{\mathbf{k}}, q_{\mathbf{k}} \in \mathcal{O}[z]$. Then the Maclaurin expansion V of $\frac{P}{Q}$ satisfies the 2-function property if and only if $p_{\mathbf{k}} \neq 0$ implies $q_{\mathbf{k}} \neq 0$ and $\frac{p_{\mathbf{k}}}{q_{\mathbf{k}}} \in \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q})$ for all $\mathbf{k}$ with $q_{\mathbf{k}} \neq 0$.*

Combining Theorem 5.6 with Theorem 1.2 confirms Conjecture 5.1, at least in the case where the algebraic function $V \in \mathcal{S}^2_{\mathrm{alg}}(K|\mathbb{Q})$ is the diagonal of $\frac{P}{Q}$ and Q is linear in the variables $x_1, ..., x_n$.

5.2 Framing

The second result of this work is given by Theorem 4.1 and Theorem 4.25. What remains, is a full description of the preimage of $\mathcal{S}^3(K|\mathbb{Q})$ under the framing operators $(\Phi^{+/-})^{-1}\left(\mathcal{S}^3(K|\mathbb{Q})\right)$. The author's impression is that

$$(\Phi^{+/-})^{-1}\left(\mathcal{S}^3(K|\mathbb{Q})\right) \setminus \mathcal{S}^2_{\mathrm{rat}}(K|\mathbb{Q}) = \varnothing,$$

since the periodicity of the coefficients of rational 2-functions played a crucial role in the proof of Theorem 4.1 and the generalized Wolstenholme Theorem 4.15. The author was not able to prove it.

5.3 MISCELLANEOUS

One may develop the theory of s-functions in the setting of a relative field extension $L|K$, or in the case, where $L|K$ is a field extension of function fields.

Bibliography

[1] M. Aganagic, A. Klemm, C. Vafa, *Disk instantons, mirror symmetry and the duality web*, Z. Naturforsch. A **57**, 1, (2002).

[2] G. Almkvist and W. Zudilin, *Differential equations, mirror maps and zeta values*, Mirror symmetry. V, volume **38** of AMS/IP Stud. Adv. Math. (2006), pp. 481–515.

[3] R. Apéry, *Irrationalité de* $\zeta(2)$ *et* $\zeta(3)$, Astérisque no. **61** (1979), pp. 11–13.

[4] C. Babbage, *Demonstration of a theorem relating to prime numbers*, The Edinburgh Philosophical Journal **1**, 1819, pp. 46–49.

[5] C. Banderier, M. Drmota, *Coeffizients of algebraic functions: formulae and asymptotics*, DMTCS Proc. AS, 25th International Conference on Formal Power Series and Algebraic Combinatoris (FPSAC 2013), 2013, pp. 1065–1076.

[6] F. Beukers, *Some Congruences for the Apery Numbers*, Journal of Number Theory, volume **21** (1985), issue 2, pp. 141–155.

[7] F. Beukers, M. Houben, and A. Straub, *Gauss congruences for rational functions in several variables*, Acta Arithmetica, volume **184**, issue 4 (2018), pp. 341–362.

[8] J.-P. Bézivin, *Sur un théorème de G. Pólya*, J. Reine Angew. Math. **364**, pp. 60–68, (1986).

[9] D. Birmajer, J. Gil, and M. Weiner, *A family of Bell transformations*, Journal of Discrete Mathematics, volume **342**, nr. 1, pp. 38–54, (2019), doi: https://doi.org/10.1016/j.disc.2018.09.011.

[10] V. Brun, J.O. Stubban, J.E. Fjedlstad, R. Tambs Lyche, K.E. Aubert, W. Ljunggren, E. Jacobsthal, *On the divisibility of the difference between two binomial coefficients*, Den 11te Skandinaviske Matematikerkongress, Trondheim (1949), pp. 42–54.

[11] P. Candelas, X. de la Ossa, P. Green, L. Parkes, *A pair of Calabi-Yau manifolds as an exactly soluble superconformal theory*, Essays on Mirror Manifolds, S.-T. Yau (ed.), International Press, Hong Kong, 1992, pp. 31-95.

[12] M.J. Coster, *Supercongruences*, [Thesis] Univ. of Leiden, the Netherlands (1988).

[13] B. Dwork, *On the Rationality of the Zeta Function of an Algebraic Variety*, American Journal of Mathematics **82.3**, (1960), pp. 631–648.

[14] H. Furstenberg, *Algebraic Functions over Finite Fields*, J. Algebra **7** (1967), pp. 271–277.

[15] S. Garoufalidis, P. Kucharski, P. Sułkowski, *Knots, BPS states, and algebraic curves*, Commun. Math. Phys. **346**, 2016, pp.75–113, https://doi.org/10.1007/s00220-016-2682-z.

[16] I. Gessel, *Some Congruences for generalized Euler numbers*, Canadian Journal of Mathematics **14** (1983), pp. 687-709. doi:10.4153/CJM-1983-039-5.

[17] I. Gessel, *Lagrange Inversion*, Journal of Combinatorial Theory, Series A, volume **144** (2016), pp. 212–249.

[18] O. Gorodetsky, *q-Congruences, with Applications to Supercongruences and the Cyclic Sieving Phenomenon*, Int. J. Number Theory **15** (2019), no. 9, pp. 1919-1968.

[19] W.A. Harris, Y. Sibuya, *The reciprocals of solutions of linear ordinary differential equations*, Adv. in Math. **85** (1985), no. 2, pp. 119–132.

[20] M. Hickel, M. Matusinski, *On the algebraicity of Puiseux series*, Rev. Ma. Complut., Volume **30**, issue 3, pp. 589–620, 2017.

[21] G.J. Janusz, *Algebraic Number Fields*, Academic Press, New York, 1973.

[22] R. Jungen, *Sur les series de Taylor n'ayant que des singularités algébrico-logarithmiques sur lear cercle de convergence*, Comment. Math. Helv. **3** (1931), pp. 226–306.

[23] C. Kassel, C. Reutenauer, *Algebraicity of the zeta function associated to a matrix over a free group algebra*, Algebra Number Theory, **8(2)**, pp. 497–511, 2014.

[24] G.S. Kazandzidis, *On congruences in number-theory*, Bull. Soc. Math. Grèce (N. S.), **10**, 1969, pp. 35–40.

[25] H. Koch, *Number Theory: Algebraic numbers and functions*, (Amer. Math. Soc, Providence, RI, 2000).

[26] M. Kontsevich, A. Schwarz, V. Vologodsky, *Integrality of instanton numbers and p-adic B-model*, Phys. Lett. B **637**, 97 (2006); [arXiv:hep-th/0603106].

[27] S. Lang, *Cyclotomic Fields 1 and 2*, Springer New York Berlin Heidelberg (1990), isbn: 0387966714.

[28] D. Merlini, R. Sprugnoli, and M. Cecilia Verri, *Lagrange Inversion: When and How*, Acta Applicandae Mathematica, volume **94** (2006), no. 3, pp. 233–249, https://doi.org/10.1007/s10440-006-9077-7.

[29] R. Meštrović, *Wolstenholme's Theorem: Its generalizations and extensions in the last hundred and fifty years (1862-2012)*, eprint: arXiv:1111.3057v2.

[30] G.T. Minton, *Linear recurrence sequences satisfying congruence conditions*, Proceedings of the American Mathematical Society, Volume **142**, nr. 7, July 2014, pp. 2337–2352.

[31] D. Morrison, *Mirror Symmetry and rational curves on quintic threefolds: A Guide for mathematicians*, J. of the Amer. Math. Soc. **6** (1993), pp. 223–247.

[32] L.F. Müller, *Rational 2-Functions are Abelian*, https://arxiv.org/abs/2006.06388, (2020).

[33] L.F. Müller, *Wolstenholme Type Congruences and the Framing of Rational 2-Functions*, https://arxiv.org/abs/2104.10754, (2021).

[34] J. Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag Berlin Heidelberg, (1992).

[35] H. Ooguri, C. Vafa, *Knot invariants and topological strings*, Nucl. Phys. B **577**, 419, (2000).

[36] R. Osburn and B. Sahu, *A supercongruence for generalized Domb numbers*, Funct. Approx. Comment. Math., Volume **48**, Number 1 (2013), pp. 29–36.

[37] J. Rosen, *Multiple harmonic sums and Wolstenholme's theorem*, Int. J. Number Theory 9, 2013, pp. 2033–2052.

[38] A. Schwarz, V. Vologodsky, *Integrality theorems in the theory of topological strings*, Nucl. Phys.B **821**, 506, 2009.

[39] A. Schwarz, V. Vologodsky, and J. Walcher, *Framing the Di-logarithm (over $\mathbb{Z}$)*, Contribution to Proceedings of String-Math 2012, Bonn, https://arxiv.org/abs/1306.4298.

[40] A. Schwarz, V. Vologodsky, and J. Walcher, *Integrality of Framing and geometric origin of 2-functions (with algebraic coefficients)*, (2016), arXiv: https://arxiv.org/abs/1702.07135

[41] M.P. Schützenberger, *On a theorem of R. Jungen*, Proc. Amer. Math. Soc. **13**, pp. 885–889, 1962.

[42] R.P. Stanley, *Differentiably finite power series*, European J. Combin. **1**, pp. 175–188, 1980.

[43] Yu. A. Trakhtman, *On the divisibility of certain differences formed from binomial coefficients* (Russian), Doklady Akad. Nauk Arm. S. S. R. **59**, 1974, pp. 10–16.

[44] J. Walcher, *On the arithmetic of D-branes superpotentials*, Comm. Num. Th. Phys. **6**, no. 2, pp. 279–337, 2012.

[45] E. Waring, *Meditationes Algebraicae*, Editio tertia recensita et aucta, Cambridge: J. Nicholson, 1782.

[46] J. Wolstenholme, *On certain properties of prime numbers*, The Quarterly Journal of Pure and Applied Mathematics, **5**, pp. 35–39, 1862.

[47] D. Zagier, *The Dilogarithm Function*, Frontiers in number theory, physics, and geometry, II., pp. 3–65, Springer, Berlin, 2007.

[48] A.V. Zarelua, *On Congruences for the Traces of Powers of Some Matrices*, Proceedings of the Steklov Institute of Mathematics (2008), vol. **263**, pp. 78–98.

[49] W. Zudilin, *personal communication*, (2021).