Journal of Number Theory 263 (2024) 335–365

Contents lists available at ScienceDirect

Journal of Number Theory

journal homepage: www.elsevier.com/locate/jnt

General Section

The ring of finite algebraic numbers and its application to the law of decomposition of primes

Julian Rosen [a], Yoshihiro Takeyama [b], Koji Tasaka [c,*], Shuji Yamamoto [d]

[a] *Independent author, Bangor, ME, USA*
[b] *Department of Mathematics, Institute of Pure and Applied Sciences, University of Tsukuba, Tsukuba, Ibaraki 305-8571, Japan*
[c] *Department of Mathematics, Kindai University, Higashiosaka-city, Osaka, 577-8502, Japan*
[d] *Department of Mathematics, Faculty of Science and Technology, Keio University, 3-14-1 Hiyoshi, Kouhoku-ku, Yokohama 223-8522, Japan*

ARTICLE INFO

Article history:
Received 5 November 2023
Received in revised form 30 April 2024
Accepted 30 April 2024
Available online 24 May 2024
Communicated by L. Smajlovic

Keywords:
Algebraic numbers
Linear recurrent sequence modulo primes
Mod p congruences of Fibonacci numbers

ABSTRACT

In this paper, we develop an explicit method to express finite algebraic numbers (in particular, certain idempotents among them) in terms of linear recurrent sequences, and give applications to the characterization of the splitting primes in a given finite Galois extension over the rational field.

* Corresponding author.
E-mail addresses: julianrosen@gmail.com (J. Rosen), takeyama@math.tsukuba.ac.jp (Y. Takeyama), tasaka@math.kindai.ac.jp (K. Tasaka), yamashu@math.keio.ac.jp (S. Yamamoto).

https://doi.org/10.1016/j.jnt.2024.04.003

1. Introduction

1.1. Splitting of primes

We denote by $\boldsymbol{P}_{\mathbb{Q}}$ the set of all rational prime numbers. Let L be a finite Galois extension over $\mathbb{Q}$ (contained in a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$) and O_L the ring of integers in L. For $p \in \boldsymbol{P}_{\mathbb{Q}}$, the ideal of O_L generated by p has a unique factorization into prime ideals:

$$pO_L = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}, \tag{1.1}$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are distinct prime ideals of O_L. Since $L/\mathbb{Q}$ is Galois, we have $e_1 = \cdots = e_r =: \mathbf{e}$ and $[O_L/\mathfrak{p}_1 : \mathbb{F}_p] = \cdots = [O_L/\mathfrak{p}_r : \mathbb{F}_p] =: \mathbf{f}$, where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The prime number p is said to *split completely* in L if $\mathbf{e} = 1$ and $\mathbf{f} = 1$. Determining the set

$$\mathrm{Spl}(L) := \{p \in \boldsymbol{P}_{\mathbb{Q}} \mid p \text{ splits completely in } L\}$$

is an important theme in algebraic number theory; in fact, it is known that L is determined uniquely by the set $\mathrm{Spl}(L)$. More precisely, if M is another finite Galois extension over $\mathbb{Q}$ (in the same algebraic closure $\overline{\mathbb{Q}}$) and $\mathrm{Spl}(M)$ is equal to $\mathrm{Spl}(L)$ except for finitely many primes, then $L = M$ holds (see [4, Theorem 8.19]).

In this paper, we give a characterization of primes splitting completely in L through the study of finite algebraic numbers introduced by the first author. The basic question behind our study is as follows.

Question 1.1. *Given a finite Galois extension $L/\mathbb{Q}$, is there a rule which, for every prime p, determines whether p belongs to* $\mathrm{Spl}(L)$*?*

This question is intimately related to the splitting of polynomials modulo primes studied in the context of a reciprocity law (see [25] for the exposition of a reciprocity law). In general, let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial and $K = \mathbb{Q}(\alpha) \cong \mathbb{Q}[x]/(f(x))$ be the number field generated by a root α of f (note that K is not necessarily Galois over $\mathbb{Q}$). Then we have

$$p \in \mathrm{Spl}(K) \Longleftrightarrow N_p(f) = \deg f \tag{1.2}$$

for all but finitely many primes p (cf. [13, Chapter I, Proposition 25] and Remark after that), where we denote by $N_p(f)$ the number of distinct roots in $\mathbb{F}_p$ of the reduction of $f(x)$ modulo p. For example, the quadratic reciprocity law shows that $N_p(x^2 - 5) = 2$ if and only if $p \equiv 1, 4 \bmod 5$, which implies

$$\mathrm{Spl}\left(\mathbb{Q}(\sqrt{5})\right) = \{p \in \boldsymbol{P}_{\mathbb{Q}} \mid p \equiv 1, 4 \bmod 5\}. \tag{1.3}$$

Similarly to the quadratic reciprocity law, the set $\mathrm{Spl}(L)$ is characterized by congruence conditions if the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ is abelian. This is a consequence of the class field theory over $\mathbb{Q}$. If L is not abelian, even though the set $\mathrm{Spl}(L)$ is not characterized by congruence conditions, there are several studies that systematically provide explicit descriptions of $\mathrm{Spl}(L)$. For example, let $L = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi\sqrt{-1}/3})$ be the splitting field of $x^3 - 2$. Its Galois group is isomorphic to the symmetric group $\mathfrak{S}_3$. Then, with finitely many exceptions, we have the following three equivalent conditions (see [6, Theorem 1.1]):

$$\begin{aligned} p \in \mathrm{Spl}(L) &\iff N_p(x^3-2) = 3, \\ &\iff \text{there exists } x, y \in \mathbb{Z} \text{ such that } p = x^2 + 27y^2, \qquad (1.4) \\ &\iff b_p = 2, \end{aligned}$$

where $\sum_{m\geq 0} b_m q^m = q\prod_{n\geq 1}(1-q^{6n})(1-q^{18n}) = \eta(6\tau)\eta(18\tau)$ is a modular form of weight 1. The first equivalence follows from (1.2) and the fact that p splits completely in $K \cong \mathbb{Q}[x]/(x^3-2)$ if and only if p splits completely in the Galois closure L of K (cf. [15, Chapter 1, §8, Exercise 4]). The second one comes from the study of primes of the form $x^2 + ny^2$ ([4, Theorem 9.4 and Proposition 9.5]). The last description of $\mathrm{Spl}(L)$ is a special case of the Langlands program (cf. [6, §5.1.2]): a correspondence between Galois representations and modular forms. For more examples and recent developments on the reciprocity laws, see [24] and references therein.

1.2. Approaches via linear recurrent sequences

Some of the existing research on congruences of linear recurrent sequences has been (often implicitly) linked with the decomposition laws of primes. For example, let $(F_m)_m$ be the Fibonacci sequence, i.e., the sequence of integers satisfying the linear recurrence relation $F_m - F_{m-1} - F_{m-2} = 0$ for $m \geq 2$ with the initial values $(F_0, F_1) = (0, 1)$. It is known (cf. [3, Chap. XVII]) that for any odd prime p we have

$$F_p \equiv 1 \bmod p \iff p \equiv 1, 4 \bmod 5,$$

which, by (1.3), gives another description of $\mathrm{Spl}\left(\mathbb{Q}(\sqrt{5})\right)$:

$$\mathrm{Spl}\left(\mathbb{Q}(\sqrt{5})\right) = \{p \in \boldsymbol{P}_{\mathbb{Q}} \setminus \{2\} \mid F_p \equiv 1 \bmod 5\}.$$

In this example, the quadratic field $\mathbb{Q}(\sqrt{5})$ naturally appears as the splitting field of the characteristic polynomial $x^2 - x - 1$ of the linear recurrent sequence $(F_m)_m$.

In a similar context, there are several studies on a rule determining $N_p(f)$ by a linear recurrent sequence modulo p (cf. [14,20,23] and references therein). As examples of solutions to Question 1.1, let us rephrase Sun's and Saito's results (note that these are not equivalent to the original statements from [14, Theorem 5] and [20, Theorem 1]).

Theorem 1.2.

(1) *(Z.-W. Sun) Let* $f(x) = x^3 + c_1x^2 + c_2x + c_3 \in \mathbb{Z}[x]$ *be a monic irreducible polynomial such that* $c_1^2 \neq 3c_2$ *and* L *its splitting field over* $\mathbb{Q}$*. Define the integer sequence* $(s_m)_m$ *by the linear recurrence* $s_m + c_1s_{m-1} + c_2s_{m-2} + c_3s_{m-3} = 0$ $(\forall m \geq 3)$ *with the initial values* $(s_0, s_1, s_2) = (3, -c_1, c_1^2 - 2c_2)$*. Then,*

$$p \in \mathrm{Spl}(L) \iff s_{p+1} \equiv c_1^2 - 2c_2 \bmod p$$

holds for all but finitely many primes p*.*

(2) *(S. Saito) Let* $f = x^d + c_1x^{d-1} + \cdots + c_d \in \mathbb{Z}[x]$ *be a monic irreducible polynomial of degree* $d \geq 2$ *with non-zero discriminant and* L *its splitting field over* $\mathbb{Q}$*. Define the integer sequence* $(u_m)_m$ *by* $u_m + c_1u_{m-1} + \cdots + c_du_{m-d} = 0$ $(\forall m \geq d)$ *with the initial values* $(u_0, \dots, u_{d-2}, u_{d-1}) = (0, \dots, 0, 1)$*. Then,*

$$p \in \mathrm{Spl}(L) \iff u_{p-2+d} \equiv 1 \bmod p$$

holds for all but finitely many primes p*.*

The condition that $c_1^2 \neq 3c_2$ in Theorem 1.2 (1) is necessary to distinguish the cases $N_p(f) = 1$ and $N_p(f) = 3$. Due to this, Theorem 1.2 (1) can not be applied to the case $f(x) = x^3 - 2$. On the other hand, Theorem 1.2 (2) does cover the case. Namely, we have that

$$p \in \mathrm{Spl}\left(\mathbb{Q}(\sqrt[3]{2}, e^{2\pi\sqrt{-1}/3})\right) \iff u_{p+1} \equiv 1 \bmod p \tag{1.5}$$

holds for all but finitely many primes p, where the integer sequence $(u_m)_m$ is defined by $u_m = 2u_{m-3}$ $(m \geq 3)$ with $(u_0, u_1, u_2) = (0, 0, 1)$. Notice that in [20, Theorem 1], d is assumed to be ≥ 3, but the case $d = 2$ in Theorem 1.2 (2) also holds and covers the case of $f(x) = x^2 - x - 1$, the Fibonacci numbers $(F_m)_m$.

We remark that Theorem 1.2 is weaker than the full statements [14, Theorem 5] and [20, Theorem 1]; they also determined exceptional primes for which the claimed equivalences do not hold. Later, we will come back to the determination problem of exceptional primes.

1.3. Our result

The reason we write Theorem 1.2 in this manner is because it fits the framework of *finite algebraic numbers*. The notion of finite algebraic number is introduced in [18] as an $\mathcal{A}$-analogue of the period interpretation of the algebraic numbers (see Remark 2.14 for more details). Here the symbol $\mathcal{A}$ stands for the ring $\left(\prod_p \mathbb{F}_p\right) / \left(\bigoplus_p \mathbb{F}_p\right)$, where p runs over all primes. This ring was first introduced by Kontsevich [12, §2.2] and recently used in the study of multiple zeta values (see Remark 2.15). In this setting, the sequence $(a_p)_p$ is zero in $\mathcal{A}$ if $a_p = 0$ for all but finitely many primes p.

This framework provides a conceptual explanation as to why the set $\mathrm{Spl}(L)$ can be characterized by the values of a linear recurrent sequence modulo primes. Moreover, using the same machinery, we can give a law of decomposition of primes in L, namely, a classification of primes (which are unramified in $L/\mathbb{Q}$) according to the number of prime factors in (1.1). Recall that p is *unramified* in $L/\mathbb{Q}$ if $\mathbf{e} = 1$ in the decomposition (1.1). In this case, the number $r = [L : \mathbb{Q}]/\mathbf{f}$ of factors is determined by the conjugacy class of $\mathrm{Gal}(L/\mathbb{Q})$ to which the Frobenius automorphism at p belongs. For the precise statement, let

$$\mathrm{Rec}(f;\mathbb{Q}) := \left\{ (a_m)_m \in \prod_{m\geq 0} \mathbb{Q} \;\middle|\; a_m + c_1 a_{m-1} + \cdots + c_d a_{m-d} = 0 \text{ for all } m \geq d \right\} \quad (1.6)$$

be the $\mathbb{Q}$-vector space of sequences satisfying the homogeneous linear recurrence relation with characteristic polynomial $f(x) = x^d + c_1 x^{d-1} + \cdots + c_d \in \mathbb{Z}[x]$ of degree d.

Theorem 1.3. *Let L be a finite Galois extension over $\mathbb{Q}$ and $f \in \mathbb{Q}[x]$ a monic irreducible polynomial such that all roots of f are simple and form a basis of L over $\mathbb{Q}$. Then, for any conjugacy class C in the Galois group* $\mathrm{Gal}(L/\mathbb{Q})$, *there exists a unique sequence* $(a_m)_m = (a_m(C))_m \in \mathrm{Rec}(f;\mathbb{Q})$ *such that*

$$a_p \equiv \begin{cases} 1 \mod p & (\textit{if the Frobenius automorphism at } p \textit{ belongs to } C), \\ 0 \mod p & (\textit{otherwise}) \end{cases} \quad (1.7)$$

holds for all but finitely many primes p. In particular, letting $C = \{\mathrm{id}\}$, we have

$$a_p \equiv \begin{cases} 1 \mod p & (\textit{if } p \in \mathrm{Spl}(L)), \\ 0 \mod p & (\textit{otherwise}) \end{cases} \quad (1.8)$$

for all but finitely many primes p.

The assumption on the polynomial f in Theorem 1.3 means that f is the minimal polynomial of a normal element of L (an element of L is said to be normal if its Galois conjugates form a basis of L over $\mathbb{Q}$). In particular, this implies that $\deg f = [L : \mathbb{Q}]$.

Remark 1.4. Let us compare our Theorem 1.3 with Saito's result [20, Theorem 1] of which Theorem 1.2 (2) is a special case. First, our assumption on the polynomial f to be the minimal polynomial of a normal element is stronger than the one in Saito's result. For example, to apply Theorem 1.3 to the field $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi\sqrt{-1}/3})$, we need some polynomial of degree 6. However, it follows from (1.5) (a special case of Theorem 1.2 (2)) that the sequence $(a_m)_m \in \mathrm{Rec}(x^3 - 2;\mathbb{Q})$ with $(a_0, a_1, a_2) = (0, 1, 0)$ satisfies

$$p \in \mathrm{Spl}\left(\mathbb{Q}(\sqrt[3]{2}, e^{2\pi\sqrt{-1}/3})\right) \iff a_p \equiv 1 \bmod p$$

for all but finitely many primes p. In this sense, Theorem 1.2 (2) is more generally applicable than our Theorem 1.3.

On the other hand, Theorem 1.3 is finer than Saito's result: From the latter, one can read the information about the *order* of the Frobenius automorphisms, while our result also gives the information of *conjugacy classes* of them. We also remark that, with Saito's construction, one cannot control $a_p \bmod p$ for $p \notin \mathrm{Spl}(L)$ as done in (1.8).

An interesting result is obtained when we apply Theorem 1.3 to a characterization of the p-th Fourier coefficients of a modular form of weight 1 corresponding to an irreducible odd Artin representation $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$ (cf. [5,9–11]). If $\sum_{m\geq 1} b_m q^m$ is such a modular form and L is the fixed field by the kernel of ρ, then $b_p = \mathrm{Tr}(\rho(\phi_{\mathfrak{p}}))$ holds for any prime p unramified in $L/\mathbb{Q}$ (note that there are only finitely many primes which are not unramified, i.e., ramify in $L/\mathbb{Q}$), where $\phi_{\mathfrak{p}} \in \mathrm{Gal}(L/\mathbb{Q})$ denotes the Frobenius automorphism at a prime $\mathfrak{p}$ of L above p. Since the trace $\mathrm{Tr}(\rho(\sigma))$ depends only on the conjugacy class of σ in $\mathrm{Gal}(L/\mathbb{Q})$, the following linear combination of the sequences $(a_m(C))_m$ in Theorem 1.3 is well-defined:

$$a_m(\rho) = \sum_{C \subset \mathrm{Gal}(L/\mathbb{Q})\text{: conjugacy class}} \mathrm{Tr}(\rho(\sigma_C))a_m(C) \qquad (\sigma_C \in C).$$

Then we have

$$a_p(\rho) \equiv \mathrm{Tr}(\rho(\phi_{\mathfrak{p}})) \equiv b_p \bmod p$$

for all but finitely many primes p. The following is an example of this construction:

Proposition 1.5. *Let* $f(x) = x^6 + 3x^5 + 12x^4 + 25x^3 + 60x^2 + 51x + 127$*, whose splitting field is* $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi\sqrt{-1}/3})$*. Define the sequence* $(a_m)_m \in \mathrm{Rec}(f;\mathbb{Q})$ *by the initial values* $(a_0, a_1, \ldots, a_5) = (0, 2, -4, -3, 20, -40)$*. Then, the* p*-th Fourier coefficient of* $\eta(6\tau)\eta(18\tau) = \sum_{m\geq 0} b_m q^m$ *as in* (1.4) *satisfies*

$$a_p \equiv b_p \mod p$$

for all but finitely many primes p*.*

Here we list the values of a_p and b_p for small primes p:

p	2	3	5	7	11	13	17	…	31
a_p	−4	−3	−40	−169	8690	−49336	854726	…	−647044186129
b_p	0	0	0	−1	0	−1	0	…	2

Our proof of Theorem 1.3 relies on the theory of finite algebraic numbers; for example, the fact that every finite algebraic number is obtained from a linear recurrent sequence over $\mathbb{Q}$ (see Theorem 2.9). It is possible to generalize this theory to the relative case, i.e., the base field $\mathbb{Q}$ can be replaced by an arbitrary number field K, with no essential difficulty, but we will not develop this point here. The proof provides a method of explicit computation of the sequence describing the decomposition laws.

1.4. Refinement

As we have mentioned in the end of §1.2, there are finitely many exceptional primes for which the congruences in Theorem 1.3 do not hold. To determine these exceptions, we refine the theory of finite algebraic numbers working over the ring of S-integers $\mathbb{Z}_S := \mathbb{Z}\left[p^{-1} \mid p \in S\right]$ for a finite subset S of $\boldsymbol{P}_{\mathbb{Q}}$. In this setting, we introduce the ring of S-integers in finite algebraic numbers and prove that every such S-integer is obtained from a linear recurrent sequence over $\mathbb{Z}_S$ (cf. Theorem 4.7). With this refinement, we can control exceptional primes in Theorem 1.3 as follows.

Theorem 1.6. *Let L, f and $(a_m)_m = (a_m(C))_m \in \mathrm{Rec}(f;\mathbb{Q})$ be as in Theorem 1.3 and denote all distinct roots of f by $\xi_1, \dots, \xi_d$, where $d = [L : \mathbb{Q}]$. Suppose that a finite subset $S \subset \boldsymbol{P}_{\mathbb{Q}}$ of primes satisfies the following conditions:*

(S0) *Each component of the sequence $(a_m)_m$ is an S-integer.*
(S1) *S contains all primes ramifying in $L/\mathbb{Q}$.*
(S2) *f belongs to $\mathbb{Z}_S[x]$ and $\mathrm{disc}(f) := \prod_{i<j}(\xi_i - \xi_j)^2$ is invertible in $\mathbb{Z}_S$.*

Then, the congruence (1.7) holds for all primes $p \notin S$.

Note that, if $f \in \mathbb{Z}_S[x]$, then we can confirm the condition (S0) by checking $a_m \in \mathbb{Z}_S$ for $m = 0, \dots, d-1$.

Let us illustrate an example of the use of Theorem 1.6.

Example 1.7. Set $\omega_1 = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$ and let $L = \mathbb{Q}(\omega_1)$. Then its Galois group is isomorphic to the quaternion group Q_8. The element $\xi = (1+\sqrt{2})(1+\sqrt{3})(1+\omega_1)$ is a normal element of L and its minimal polynomial is

$$f(x) = x^8 - 8x^7 - 736x^6 - 3344x^5 + 5800x^4 + 18272x^3 - 27904x^2 + 9920x - 368.$$

By Theorem 1.3, one can find the sequence $(a_m)_m \in \mathrm{Rec}(f;\mathbb{Q})$ such that (1.8) holds for all but finitely many primes p. Using the method described in §3.2, we obtain the initial values of $(a_m)_m$ as follows:

$$a_0 = \frac{1}{8}, \quad a_1 = 1, \quad a_2 = \frac{1393}{20}, \quad a_3 = \frac{3199}{2},$$

$$a_4 = \frac{2003629}{30}, \quad a_5 = 1936618, \quad a_6 = \frac{1043676173}{15}, \quad a_7 = \frac{10973964638}{5}.$$

Now let us determine exceptional primes. For the first condition (S0), we count prime factors of denominators of the initial values $(a_0, \dots, a_7)$ which are 2, 3 and 5. For (S1), we recall that a prime p ramifies in $L/\mathbb{Q}$ if (and only if) p divides the discriminant $\mathrm{disc}(L)$ of L (see (4.1) for the definition). The prime factorizations of $\mathrm{disc}(L)$ and $\mathrm{disc}(f)$ are given by

$$\begin{aligned}\mathrm{disc}(L) &= 2^{24} \cdot 3^6,\\ \mathrm{disc}(f) &= 2^{72} \cdot 3^6 \cdot 23^2 \cdot 241^2 \cdot 359^2 \cdot 147409^2.\end{aligned}$$

Thus, the set

$$S = \{2, 3, 5, 23, 241, 359, 147409\}$$

satisfies the conditions (S0) to (S2) in Theorem 1.6. Hence, the above sequence $(a_m)_m$ satisfies (1.8) for all prime $p \notin S$.

To complement the list of primes splitting completely in L, we may use a mathematical software. Indeed, we can confirm that every $p \in S$ does not split completely in L of Example 1.7. This can be checked by the following code in SAGEMATH [19]:

```
sage: K.<y> = NumberField(x^8 - 8*x^7 - 736*x^6 - 3344*x^5 + 5800*x^4 + 18272*x^3
- 27904*x^2 + 9920*x - 368)
sage: K.completely_split_primes(147409)
[71, 191, 239, 313, 337, 383, ..., 147311]
```

Remark 1.8. In the same way, we obtain a set S of (possibly) exceptional primes in Proposition 1.5 as follows (note that in this case, we have $\mathrm{disc}(L) = -2^4 \cdot 3^7$ and $\mathrm{disc}(f) = -2^4 \cdot 3^{17} \cdot 5^2 \cdot 11^2$).

$$S = \{2, 3, 5, 11\}.$$

By a direct calculation, one can check that these four primes are actually not exceptional (see the table given after Proposition 1.5). Therefore, in this case, we conclude that the congruence $a_p \equiv b_p \pmod{p}$ holds for *every* prime p.

1.5. Contents

The paper is structured as follows. In §2, we recall the theory of finite algebraic numbers developed by the first author in [18], using a slightly general convention. In §3, we explain the method to find a recurrent sequence $(a_m)_m$ of Theorem 1.3 and illustrate it in the cases of $[L : \mathbb{Q}] = 2$ and 3. At this stage, there is a problem that our method described in §3.2 does not provide any information about the finite set S of exceptional primes. In §4, we settle this problem by showing Theorem 1.6 and give some more examples in which both S and $(a_m)_m$ are explicitly determined.

Notation: Throughout the paper, we let L be a finite Galois extension of $\mathbb{Q}$ and set $G = \mathrm{Gal}(L/\mathbb{Q})$.

2. Finite algebraic numbers

In this section, we review some basic constructions relevant to finite algebraic numbers. Our expositions are rendered as self-contained as possible, whilst the materials and some of results presented here are essentially contained in [18].

2.1. Definition of finite algebraic numbers

For a prime p, let $\mathbb{F}_p$ be the finite field of order p and consider the ring

$$\mathcal{A} := \Big(\prod_{p\in \boldsymbol{P}_{\mathbb{Q}}} \mathbb{F}_p\Big) \Big/ \Big(\bigoplus_{p\in \boldsymbol{P}_{\mathbb{Q}}} \mathbb{F}_p\Big).$$

An element of $\mathcal{A}$ is denoted as $(a_p)_p$ with $a_p \in \mathbb{F}_p$ for each prime p, and two elements $(a_p)_p, (b_p)_p \in \mathcal{A}$ are equal if $a_p = b_p$ in $\mathbb{F}_p$ holds for all but finitely many primes p. Thus, to describe an element $(a_p)_p \in \mathcal{A}$, we can ignore a finite number of primes p.

As an example, let c be a rational number. Since we have $c \in \mathbb{Z}_{(p)}$ except for a finite number of primes p, where $\mathbb{Z}_{(p)}$ denotes the localization of $\mathbb{Z}$ at the prime ideal (p), we can define an element $(c \bmod p)_p \in \mathcal{A}$. Here, by an abuse of notation, we write "$c \bmod p$" for the class of $c \in \mathbb{Z}_{(p)}$ in the residue field $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{F}_p$. Thus we obtain an injective ring homomorphism $\mathbb{Q} \to \mathcal{A}$ given by $c \mapsto (c \bmod p)_p$, through which $\mathcal{A}$ is viewed as a $\mathbb{Q}$-algebra.

Definition 2.1. An element $\alpha \in \mathcal{A}$ is called a *finite algebraic number* if there exists a sequence $(a_m)_m$ of rational numbers satisfying a homogeneous linear recurrence relation such that $\alpha = (a_p \bmod p)_p$. The set of all finite algebraic numbers is denoted by $\mathcal{P}_0^{\mathcal{A}}$.

As in (1.6), let $\mathrm{Rec}(f;\mathbb{Q})$ denote the $\mathbb{Q}$-vector space of rational sequences satisfying a homogeneous linear recurrence relation with characteristic polynomial $f(x) = x^d + c_1x^{d-1} + \cdots + c_d \in \mathbb{Q}[x]$ of degree d. Since elements in $\mathrm{Rec}(f;\mathbb{Q})$ are determined by initial values, it holds that $\dim_{\mathbb{Q}} \mathrm{Rec}(f;\mathbb{Q}) = d$. For any sequence $(a_m)_m \in \mathrm{Rec}(f;\mathbb{Q})$ and a prime p which does not divide the denominators of the initial terms $a_0, \dots, a_{d-1}$ and the denominators of the coefficients $c_1, \dots, c_d$ of f, we see that all terms a_m belong to $\mathbb{Z}_{(p)}$. In particular, $(a_p \bmod p)_p \in \mathcal{A}$ is well defined. Therefore, there is a $\mathbb{Q}$-linear map

$$r_f\colon\ \mathrm{Rec}(f;\mathbb{Q}) \longrightarrow \mathcal{A};\ (a_m)_m \longmapsto (a_p \bmod p)_p. \tag{2.1}$$

By definition, the subset $\mathcal{P}_0^{\mathcal{A}}$ of $\mathcal{A}$ is the union of the images of these maps r_f, where f runs over all monic polynomials over $\mathbb{Q}$.

Example 2.2.

(1) A rational number, viewed as an element of $\mathcal{A}$, is a finite algebraic number. Indeed, for $f(x) = x - 1$, the image of the map $r_f \colon \operatorname{Rec}(f;\mathbb{Q}) \to \mathcal{A}$ is exactly the rational numbers.

(2) Let $f(x) = x^2 - x - 1$. The Fibonacci sequence $(F_m)_m$ given by $F_m = F_{m-1} + F_{m-2}$ with $F_0 = 0, F_1 = 1$ is an element of $\operatorname{Rec}(f;\mathbb{Q})$, so $r_f((F_m)_m)$ is a finite algebraic number. Remark that the Fibonacci numbers satisfy $F_p \equiv \left(\frac{5}{p}\right) \mod p$ for all primes p (see [3, Chap. XVII]), where $\left(\frac{D}{p}\right)$ denotes the Kronecker symbol. Hence,

$$r_f((F_m)_m) = \left(\left(\frac{5}{p}\right)\right)_p.$$

This shows that $\left(\left(\frac{5}{p}\right)\right)_p \in \mathcal{P}_0^{\mathcal{A}}$. In this way, we can also prove that for any square-free integer D, the element $\left(\left(\frac{D}{p}\right)\right)_p \in \mathcal{A}$ is a finite algebraic number (see, for example, [16, p.46]).

The notion of finite algebraic number is first introduced by the first author [18, Theorem 1.1], where three equivalent constructions are made. The first construction is given in Definition 2.1. The second construction is Galois theoretic; we recast this in the following subsections and prove its equivalence with the first construction (see Corollary 2.10). For the third construction, see Remark 2.14.

2.2. The ring $\mathcal{A}_L$

Recall that L denotes a finite Galois extension of $\mathbb{Q}$. Let $\boldsymbol{P}_L$ denote the set of all maximal ideals of O_L, the ring of integers in L. Then we define the ring $\mathcal{A}_L$ associated with L by

$$\mathcal{A}_L := \left(\prod_{\mathfrak{p}\in\boldsymbol{P}_L} O_L/\mathfrak{p}\right) \Big/ \left(\bigoplus_{\mathfrak{p}\in\boldsymbol{P}_L} O_L/\mathfrak{p}\right).$$

In particular, the ring $\mathcal{A}_{\mathbb{Q}}$ coincides with the ring $\mathcal{A} = \left(\prod_p \mathbb{F}_p\right)/\left(\bigoplus_p \mathbb{F}_p\right)$ introduced in the previous subsection, where we identify the set $\boldsymbol{P}_{\mathbb{Q}}$ with the set of rational primes.

As in the case of $\mathcal{A}_{\mathbb{Q}} = \mathcal{A}$, an element $(a_{\mathfrak{p}})_{\mathfrak{p}}$ of $\mathcal{A}_L$ is specified by giving elements $a_{\mathfrak{p}} \in O_L/\mathfrak{p}$ for all but finitely many $\mathfrak{p} \in \boldsymbol{P}_L$. In particular, for any $c \in L$, we have a well-defined element $(c \bmod \mathfrak{p})_{\mathfrak{p}} \in \mathcal{A}_L$ since $c \in O_{L,\mathfrak{p}}$ (the localization of O_L at $\mathfrak{p}$) for all but finitely many $\mathfrak{p} \in \boldsymbol{P}_L$. Thus $\mathcal{A}_L$ admits an injective ring homomorphism $L \to \mathcal{A}_L$ given by $c \mapsto (c \bmod \mathfrak{p})_{\mathfrak{p}}$, through which $\mathcal{A}_L$ is viewed as an L-algebra.

We define an action of the Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$ on the ring $\mathcal{A}_L$ as follows:

$$\sigma\big((a_\mathfrak{p})_\mathfrak{p}\big) = \big(\sigma(a_{\sigma^{-1}(\mathfrak{p})})\big)_\mathfrak{p} \quad \text{for } \sigma \in G.$$

Here the isomorphism $O_L/\sigma^{-1}(\mathfrak{p}) \to O_L/\mathfrak{p}$ induced by $\sigma\colon O_L \to O_L$ is denoted by the same symbol σ. The inclusion $L \hookrightarrow \mathcal{A}_L$ is G-equivariant under this action.

2.3. The Frobenius-Evaluation Map

Let

$$\mathrm{Fun}(G, L) := \{g\colon G \to L\}$$

be the L-algebra of all functions from G to L with pointwise operations, e.g., $(g_1 + g_2)(\tau) = g_1(\tau) + g_2(\tau)$. This ring also has a G-action defined by

$$(\sigma g)(\tau) := \sigma\big(g(\sigma^{-1}\tau\sigma)\big) \quad \text{for } g \in \mathrm{Fun}(G, L) \text{ and } \sigma, \tau \in G,$$

under which the structure map $L \to \mathrm{Fun}(G, L)$ is G-equivariant.

As is well-known in Galois theory, there is an isomorphism of L-algebras

$$\varphi\colon L \otimes_\mathbb{Q} L \longrightarrow \mathrm{Fun}(G, L);\ \xi \otimes \eta \longmapsto \big(\tau \mapsto \xi\tau(\eta)\big),$$

where $L \otimes_\mathbb{Q} L$ is regarded as an L-algebra by the map $\xi \mapsto \xi \otimes 1$. This isomorphism is also G-equivariant if we let G act on $L \otimes_\mathbb{Q} L$ diagonally: indeed,

$$\varphi\big(\sigma(\xi \otimes \eta)\big)(\tau) = \sigma(\xi)\tau\sigma(\eta) = \sigma\big(\xi\,\sigma^{-1}\tau\sigma(\eta)\big) = \big(\sigma\varphi(\xi \otimes \eta)\big)(\tau).$$

If $\mathfrak{p} \in \boldsymbol{P}_L$ is unramified in $L/\mathbb{Q}$, let $\phi_\mathfrak{p} \in G$ be the Frobenius automorphism.

Definition 2.3. We define the L-algebra homomorphism $\mathrm{ev}\colon \mathrm{Fun}(G, L) \to \mathcal{A}_L$ by

$$\mathrm{ev}(g) := \big(g(\phi_\mathfrak{p}) \bmod \mathfrak{p}\big)_\mathfrak{p}.$$

This expression makes sense in $\mathcal{A}_L$ since, for all but finitely many $\mathfrak{p} \in \boldsymbol{P}_L$, $\mathfrak{p}$ is unramified in $L/\mathbb{Q}$ and $g(\tau) \in O_{L,\mathfrak{p}}$ for all $\tau \in G$.

Proposition 2.4. *The map* $\mathrm{ev}\colon \mathrm{Fun}(G, L) \to \mathcal{A}_L$ *is G-equivariant and injective.*

Proof. The G-equivariance is directly verified as

$$\mathrm{ev}\big(\sigma g\big) = \big(\sigma(g(\sigma^{-1}\phi_\mathfrak{p}\sigma))\big)_\mathfrak{p} = \big(\sigma(g(\phi_{\sigma^{-1}(\mathfrak{p})}))\big)_\mathfrak{p} = \sigma\big(\mathrm{ev}(g)\big).$$

To prove the injectivity, suppose that $g \in \mathrm{Fun}(G, L)$ satisfies $\mathrm{ev}(g) = 0$. Then, for any $\tau \in G$ there are infinitely many $\mathfrak{p}$ such that $g(\phi_\mathfrak{p}) \equiv 0 \bmod \mathfrak{p}$ and $\phi_\mathfrak{p} = \tau$ (because of the

Čebotarev density theorem; see e.g. [15, VII (13.4)]). This shows that $g(\tau) = 0$ for all $\tau \in G$, as desired. □

2.4. The space of linear recurrent sequences

Let $f(x) = x^d + c_1 x^{d-1} + \cdots + c_d \in \mathbb{Q}[x]$ be a monic polynomial over $\mathbb{Q}$ of degree d. For any extension field K of $\mathbb{Q}$, we let $\mathrm{Rec}(f;K)$ be the K-vector space of homogeneous linear recurrent sequences with characteristic polynomial f:

$$\mathrm{Rec}(f;K) := \left\{ (a_m)_m \in \prod_{m\geq 0} K \;\middle|\; a_m + c_1 a_{m-1} + \cdots + c_d a_{m-d} = 0 \text{ for } \forall m \geq d \right\}.$$

The map $\mathrm{Rec}(f;K) \to K^d$ given by $(a_m)_m \mapsto (a_0, \ldots, a_{d-1})$ is an isomorphism of K-vector spaces.

In the following, assume that f decomposes into linear factors over L (which is a finite Galois extension over $\mathbb{Q}$, as before). Let $\xi_1, \ldots, \xi_\nu \in L$ be all the distinct roots of f and let μ_j denote the multiplicity of the root ξ_j, namely, $f(x) = \prod_{j=1}^{\nu}(x - \xi_j)^{\mu_j}$. Then the sequences

$$\left(\binom{m}{i}\xi_j^{m-i}\right)_m \quad \text{for } j = 1, \ldots, \nu \text{ and } i = 0, \ldots, \mu_j - 1 \tag{2.2}$$

form a basis of the L-vector space $\mathrm{Rec}(f;L)$ (if $\xi_j = 0$, we replace the above sequence with $(\delta_{m,i})_m$).

Recall that $L \otimes_{\mathbb{Q}} L$ is equipped with an L-algebra (hence L-linear) structure given by $\xi \mapsto \xi \otimes 1$, and the diagonal G-action. On the other hand, the L-vector space $\mathrm{Rec}(f;L)$ also has a G-action defined entrywise: $\sigma\big((a_m)_m\big) := \big(\sigma(a_m)\big)_m$. Note that these G-actions are semilinear over L, i.e., we have $\sigma(\xi v) = \sigma(\xi)\sigma(v)$ for $\sigma \in G$, $\xi \in L$ and $v \in L \otimes_{\mathbb{Q}} L$ or $\mathrm{Rec}(f;L)$.

Proposition 2.5. *Let $\psi_f \colon \mathrm{Rec}(f;L) \to L \otimes_{\mathbb{Q}} L$ be the L-linear map defined on the basis (2.2) by*

$$\psi_f\left(\left(\binom{m}{i}\xi_j^{m-i}\right)_m\right) := \begin{cases} 1 \otimes \xi_j & (i = 0), \\ 0 & (i > 0). \end{cases}$$

Then ψ_f is a G-equivariant map.

Proof. By semilinearity, it suffices to check the equivariance on the basis. For $j = 1, \ldots, \nu$, $i = 0, \ldots, \mu_j - 1$ and $\sigma \in G$, we have

$$\psi_f\left(\sigma\left(\binom{m}{i}\xi_j^m\right)_m\right) = \psi_f\left(\left(\binom{m}{i}\sigma(\xi_j)^m\right)_m\right) = \begin{cases} 1 \otimes \sigma(\xi_j) & (i = 0), \\ 0 & (i > 0) \end{cases}$$

$$= \sigma\Big(\psi_f\Big(\big(\tbinom{m}{i}\xi_j^m\big)_m\Big)\Big),$$

where the second equality follows from that $\sigma(\xi_j) = \xi_{j'}$ for some j' and $\mu_j = \mu_{j'}$. This shows the desired equivariance. □

The map ψ_f is not an isomorphism in general. In fact, we have the following:

Proposition 2.6. *For a monic polynomial $f \in \mathbb{Q}[x]$ which decomposes into linear factors over L, the following conditions are equivalent:*

(1) *The L-linear map $\psi_f \colon \mathrm{Rec}(f;L) \to L \otimes_{\mathbb{Q}} L$ is an isomorphism.*
(2) *All roots of f are simple, and form a basis of L over $\mathbb{Q}$.*
(3) *f is the minimal polynomial of a normal element of L over $\mathbb{Q}$ (recall that $\xi \in L$ is called normal if its Galois conjugates $\sigma(\xi)$ $(\sigma \in G)$ form a basis of L over $\mathbb{Q}$).*

In particular, for any finite Galois extension L over $\mathbb{Q}$, there exists f satisfying these conditions.

Proof. The equivalence of the conditions (1) and (2) is clear from the construction of ψ_f.

The condition (3) obviously implies (2). To show the converse, let us assume the condition (2). Then it is enough to prove that the G-action on the set $\{\xi_1, \dots, \xi_\nu\}$ of all the distinct roots of f is transitive. Note first that the sum of the elements of each G-orbit in $\{\xi_1, \dots, \xi_\nu\}$ is a rational number, which is nonzero because of the linear independence. If there are two (or more) G-orbits, there exist two ways to express the rational numbers as linear combinations of $\xi_1, \dots, \xi_\nu$, which contradicts the linear independence. Thus the set $\{\xi_1, \dots, \xi_\nu\}$ is a single G-orbit, as desired.

The "in particular" part follows from the normal basis theorem. □

2.5. Taking invariant parts

In the previous subsections, for a monic polynomial $f \in \mathbb{Q}[x]$ which decomposes into linear factors over L, we have constructed G-equivariant maps

$$\mathrm{Rec}(f;L) \xrightarrow{\psi_f} L \otimes_{\mathbb{Q}} L \xrightarrow{\varphi} \mathrm{Fun}(G,L) \xrightarrow{\mathrm{ev}} \mathcal{A}_L.$$

Recall that the map φ is bijective and that the map ev is injective (Proposition 2.4). By taking the subspaces of G-invariant elements, we obtain the $\mathbb{Q}$-linear maps

$$\mathrm{Rec}(f;\mathbb{Q}) \xrightarrow{\psi_f} (L \otimes_{\mathbb{Q}} L)^G \xrightarrow{\varphi} A(L) \xrightarrow{\mathrm{ev}} \mathcal{A}_L^G, \tag{2.3}$$

where we set

$$A(L) \coloneqq \mathrm{Fun}(G, L)^G = \{g \colon G \to L \mid \sigma(g(\tau)) = g(\sigma\tau\sigma^{-1}) \text{ for } \forall \sigma, \tau \in G\}.$$

We show that $\mathcal{A}_L^G$ is isomorphic to $\mathcal{A} = \mathcal{A}_{\mathbb{Q}}$. First, we consider the diagonal embedding $\mathbb{F}_p \to \prod_{\mathfrak{p}|p} O_L/\mathfrak{p}$ for each rational prime p, where $\mathfrak{p}$ runs over the primes of L lying above p. Then the product of these embeddings

$$\prod_{p \in \boldsymbol{P}_{\mathbb{Q}}} \mathbb{F}_p \longrightarrow \prod_{p \in \boldsymbol{P}_{\mathbb{Q}}} \left(\prod_{\mathfrak{p}|p} O_L/\mathfrak{p} \right) = \prod_{\mathfrak{p} \in \boldsymbol{P}_L} O_L/\mathfrak{p}$$

defines, by passage to the quotient, a $\mathbb{Q}$-algebra homomorphism $\mathcal{A} \to \mathcal{A}_L$.

Proposition 2.7. *The map $\mathcal{A} \to \mathcal{A}_L$ constructed above induces an isomorphism $\mathcal{A} \cong \mathcal{A}_L^G$ of $\mathbb{Q}$-algebras.*

Proof. The injectivity of the map $\mathcal{A} \to \mathcal{A}_L$ follows from the equality

$$\bigoplus_{p \in \boldsymbol{P}_{\mathbb{Q}}} \left(\prod_{\mathfrak{p}|p} O_L/\mathfrak{p} \right) = \bigoplus_{\mathfrak{p} \in \boldsymbol{P}_L} O_L/\mathfrak{p}.$$

Moreover, its image is obviously contained in $\mathcal{A}_L^G$. Conversely, let $(a_{\mathfrak{p}})_{\mathfrak{p}}$ be an arbitrary element of $\mathcal{A}_L^G$. This means that we have $\sigma(a_{\mathfrak{p}}) = a_{\sigma(\mathfrak{p})}$ for all $\sigma \in G$ and all but finitely many $\mathfrak{p} \in \boldsymbol{P}_L$. By replacing $a_{\mathfrak{p}}$ for finitely many $\mathfrak{p}$, we may assume that the above identity holds for all $\mathfrak{p}$. Then, for each $p \in \boldsymbol{P}_{\mathbb{Q}}$, choose some $\mathfrak{p} \in \boldsymbol{P}_L$ lying above p and set $b_p \coloneqq a_{\mathfrak{p}}$. The G-invariance implies that this element $b_p \in O_L/\mathfrak{p}$ actually belongs to the subfield $\mathbb{F}_p$, and is independent of the choice of $\mathfrak{p}$. Thus we obtain an element $(b_p)_p \in \mathcal{A}$, and by construction, this maps to the given $(a_{\mathfrak{p}})_{\mathfrak{p}} \in \mathcal{A}_L^G$. □

In what follows, we identify $\mathcal{A}_L^G$ with $\mathcal{A}$ via the isomorphism in Proposition 2.7.

Definition 2.8. For each finite Galois extension L over $\mathbb{Q}$, we define a $\mathbb{Q}$-subalgebra $\mathcal{P}_L^{\mathcal{A}}$ of $\mathcal{A}$ by

$$\mathcal{P}_L^{\mathcal{A}} \coloneqq \mathrm{ev}\big(A(L)\big).$$

We now relate $r_f\big(\mathrm{Rec}(f;\mathbb{Q})\big)$ with $\mathcal{P}_L^{\mathcal{A}}$, where the map r_f is defined in (2.1).

Theorem 2.9. *Let $f \in \mathbb{Q}[x]$ be a monic polynomial which decomposes into linear factors over L.*

1. *The map $r_f \colon \mathrm{Rec}(f;\mathbb{Q}) \to \mathcal{A}$ is equal to $\mathrm{ev} \circ \varphi \circ \psi_f$, the composition of the maps in (2.3). In particular, we have $r_f\big(\mathrm{Rec}(f;\mathbb{Q})\big) \subset \mathcal{P}_L^{\mathcal{A}}$.*
2. *The map $r_f : \mathrm{Rec}(f;\mathbb{Q}) \to \mathcal{P}_L^{\mathcal{A}}$ is an isomorphism of $\mathbb{Q}$-vector spaces if f is the minimal polynomial of a normal element of L.*

Proof. (1) Let $\xi_1, \dots, \xi_\nu \in L$ be all the distinct roots of f. For a sequence $(a_m)_m \in \mathrm{Rec}(f;\mathbb{Q})$, if we write $a_m = \sum_{i,j} z_{i,j}\binom{m}{i}\xi_j^{m-i}$ with some $z_{i,j} \in L$ by using the basis (2.2), then for all but finitely many primes p, we have

$$a_p = \sum_{i,j} z_{i,j}\tbinom{p}{i}\xi_j^{p-i} \equiv \sum_j z_{0,j}\xi_j^p \equiv \sum_j z_{0,j}\phi_{\mathfrak{p}}(\xi_j) \mod \mathfrak{p}$$

with $\mathfrak{p} \in \boldsymbol{P}_L$ lying above p. This shows the equality $r_f = \mathrm{ev} \circ \varphi \circ \psi_f$, and hence $r_f\bigl(\mathrm{Rec}(f;\mathbb{Q})\bigr) \subset \mathrm{ev}\bigl(A(L)\bigr) = \mathcal{P}_L^{\mathcal{A}}$.

(2) If f is the minimal polynomial of a normal element of L, then the G-equivariant map ψ_f is an isomorphism by Proposition 2.6. Hence the statement follows from (1). □

Corollary 2.10.

(1) *We have that* $\dim_{\mathbb{Q}} \mathcal{P}_L^{\mathcal{A}} = [L : \mathbb{Q}]$.
(2) *The subset* $\mathcal{P}_0^{\mathcal{A}}$ *of* $\mathcal{A}$ *is equal to the union of* $\mathcal{P}_L^{\mathcal{A}}$*, where* L *runs over all finite Galois extensions of* $\mathbb{Q}$.

Proof. (1) Suppose that f is the minimal polynomial of a normal element of L. Then, by Theorem 2.9 (2), we have $\dim_{\mathbb{Q}} \mathcal{P}_L^{\mathcal{A}} = \dim_{\mathbb{Q}} \mathrm{Rec}(f;\mathbb{Q}) = \deg f = [L : \mathbb{Q}]$.

(2) The set $\mathcal{P}_0^{\mathcal{A}}$ is, by definition, the union of the images of maps r_f. Therefore, the result follows from the "in particular" part of Proposition 2.6 and Theorem 2.9. □

Corollary 2.10 (2) says that an element α of $\mathcal{A}$ is a finite algebraic number if and only if there exists a finite Galois extension $L/\mathbb{Q}$ and $g \in A(L)$ such that $\mathrm{ev}(g) = \alpha$. This was first proved in [18, Theorem 2.2].

2.6. Ring of finite algebraic numbers

Although not necessary for the proof of the main results, we clarify the structure of $A(L)$ in order to highlight the difference with L.

Proposition 2.11. *Let* $R \subset G$ *be a set of representatives from all conjugacy classes of* G *and, for each* $\varrho \in R$*, let* $C_G(\varrho) \coloneqq \{\sigma \in G \mid \sigma\varrho = \varrho\sigma\}$ *be the centralizer of* ϱ *in* G*. Then we have an isomorphism of* $\mathbb{Q}$*-algebras*

$$A(L) \cong \prod_{\varrho \in R} L^{C_G(\varrho)}.$$

In particular, the equality $\dim_{\mathbb{Q}} A(L) = [L : \mathbb{Q}]$ *holds.*

Proof. We define the map $A(L) \to \prod_{\varrho\in R} L^{C_G(\varrho)}$ by sending $g \in A(L)$ to $\bigl(g(\varrho)\bigr)_{\varrho\in R}$. Indeed, for $\varrho \in R$ and $\sigma \in C_G(\varrho)$, the G-invariance of g implies that $\sigma\bigl(g(\varrho)\bigr) = g(\sigma\varrho\sigma^{-1}) =$

$g(\varrho)$, hence $g(\varrho)$ is $C_G(\varrho)$-invariant. Conversely, for $(\xi_\varrho)_\varrho \in \prod_{\varrho\in R} L^{C_G(\varrho)}$, we define $g\colon G \to L$ by

$$g(\sigma\varrho\sigma^{-1}) := \sigma(\xi_\varrho) \quad \text{for } \sigma \in G \text{ and } \varrho \in R.$$

This is well-defined since ξ_ϱ is $C_G(\varrho)$-invariant, and the function g is G-invariant. These two maps are inverse to each other.

The latter part follows from the equality $\dim_{\mathbb{Q}} L^{C_G(\varrho)} = \#G/\#C_G(\varrho) = \#[\varrho]$, where

$$[\varrho] := \{\sigma\varrho\sigma^{-1} \mid \sigma \in G\} \tag{2.4}$$

denotes the conjugacy class of ϱ. □

Remark 2.12. Since $A(L) \cong \mathcal{P}_L^{\mathcal{A}}$, we have obtained an alternative proof of the equality $\dim_{\mathbb{Q}} \mathcal{P}_L^{\mathcal{A}} = [L : \mathbb{Q}]$.

In [18], it is implicitly noted that $\mathcal{P}_0^{\mathcal{A}}$ forms a $\mathbb{Q}$-subalgebra of $\mathcal{A}$. We give a proof of it for the convenience of the reader.

Proposition 2.13. *The subset $\mathcal{P}_0^{\mathcal{A}}$ of $\mathcal{A}$ is a $\mathbb{Q}$-subalgebra, which is isomorphic to the direct limit $\varinjlim_L A(L)$, where L runs over all finite Galois extensions of $\mathbb{Q}$ and the transition maps $A(L) \to A(L')$ are induced from the natural maps $\mathrm{Fun}(G, L) \to \mathrm{Fun}(G', L')$ for inclusions $L \subset L'$, where G' denotes the Galois group of $L'/\mathbb{Q}$.*

Proof. For any inclusion $L \subset L'$ of Galois extensions over $\mathbb{Q}$, we show that there is a commutative diagram

$$\begin{tikzcd}
\mathrm{Fun}(G, L) \arrow[r, "\mathrm{ev}"] \arrow[d] & \mathcal{A}_L \arrow[d] \\
\mathrm{Fun}(G', L') \arrow[r, "\mathrm{ev}"] & \mathcal{A}_{L'}
\end{tikzcd}$$

of G'-equivariant maps. Then the statement follows by taking G'-invariant parts and by passage to the direct limit.

The left vertical map is given by the composition with the natural surjection $G' \twoheadrightarrow G$ and the inclusion $L \hookrightarrow L'$, and the right vertical arrow is defined similarly to the map $\mathcal{A} \to \mathcal{A}_L$ of Proposition 2.7. The commutativity of the above diagram can be verified as follows. Take $g\colon G \to L$ and let g' be the composition $G' \twoheadrightarrow G \xrightarrow{g} L \hookrightarrow L'$. For $\mathfrak{p} \in \boldsymbol{P}_L$ such that "$g(\phi_{\mathfrak{p}}) \bmod \mathfrak{p}$" is defined, let $\mathfrak{p}'$ be an arbitrary prime of L' lying above $\mathfrak{p}$. Then we have $\phi_{\mathfrak{p}'}|_L = \phi_{\mathfrak{p}}$ by the definition of Frobenius automorphisms, and hence $g'(\phi_{\mathfrak{p}'}) = g(\phi_{\mathfrak{p}})$, which shows the desired commutativity. □

It is also easily checked that

$$\varinjlim_{L} A(L) \cong A(\overline{\mathbb{Q}}) := \mathrm{Fun}_{\mathrm{cont}}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \overline{\mathbb{Q}})^{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})},$$

where $\mathrm{Fun}_{\mathrm{cont}}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \overline{\mathbb{Q}})$ denotes the ring of continuous functions $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \overline{\mathbb{Q}}$ with respect to the Krull topology on $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and the discrete topology on $\overline{\mathbb{Q}}$, equipped with a natural action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Remark 2.14. From the theory of motivic periods [2, §5.1], the $\mathbb{Q}$-algebra $\mathcal{P}_0^{\mathcal{A}}$ is obtained as the image of the $\mathbb{Q}$-algebra $\mathcal{P}^{\mathfrak{dr}}_{\mathcal{AM}(\mathbb{Q})}$ of de Rham periods of the Tannakian category $\mathcal{AM}(\mathbb{Q})$ of Artin motives under the $\mathcal{A}$-valued period map (see [17] for further details). This is an analogy of the fact that the $\mathbb{Q}$-algebra $\overline{\mathbb{Q}}$ of algebraic numbers is the image of the $\mathbb{Q}$-algebra $\mathcal{P}^{\mathfrak{m}}_{\mathcal{AM}(\mathbb{Q})}$ of motivic periods of $\mathcal{AM}(\mathbb{Q})$ under the $\mathbb{C}$-valued period map [2]. Although we do not use this construction in this paper, it plays an important role in understanding that the $\mathbb{Q}$-algebra $\mathcal{P}_0^{\mathcal{A}}$ (resp. $\mathcal{P}_L^{\mathcal{A}}$) is the true analogue of $\overline{\mathbb{Q}}$ (resp. L) in $\mathcal{A}$ (see [18, §4] for more details).

Remark 2.15. The ring $\mathcal{A}$ appears in the recent works on finite multiple zeta values introduced by Kaneko and Zagier (cf. [8]); they conjectured a certain explicit correspondence between the finite multiple zeta value, an element in $\mathcal{A}$, and the symmetric multiple zeta value, an element in the $\mathbb{Q}$-algebra generated by multiple zeta values modulo π^2. Similarly to finite algebraic numbers, finite (resp. symmetric) multiple zeta values are obtained as the image of the ring $\mathcal{P}^{\mathfrak{dr}}_{\mathcal{MT}(\mathbb{Z})}$ of de Rham periods (resp. the ring $\mathcal{P}^{\mathfrak{m}}_{\mathcal{MT}(\mathbb{Z})}$ of motivic periods) of the Tannakian category $\mathcal{MT}(\mathbb{Z})$ of mixed Tate motives over $\mathbb{Z}$ under the $\mathcal{A}$-valued (resp. the $\mathbb{C}$-valued) period map; see [17]. In contrast to the fact that there are non-canonical isomorphisms $\mathcal{P}^{\mathfrak{dr}}_{\mathcal{MT}(\mathbb{Z})} \xrightarrow{\sim} \mathcal{P}^{\mathfrak{m}}_{\mathcal{MT}(\mathbb{Z})}$ (see [1, §2.9]), the $\mathbb{Q}$-algebra $\mathcal{P}^{\mathfrak{dr}}_{\mathcal{AM}(\mathbb{Q})}$ $(\cong \mathcal{P}_0^{\mathcal{A}})$ is not isomorphic to the $\mathbb{Q}$-algebra $\mathcal{P}^{\mathfrak{m}}_{\mathcal{AM}(\mathbb{Q})}$ $(\cong \overline{\mathbb{Q}})$. So, for finite algebraic numbers, we can not expect the similar correspondence as in the conjecture of Kaneko and Zagier.

3. Characterization of idempotents by recurrent sequences

In this section, we first prove Theorem 1.3 and then discuss an explicit method to compute the linear recurrent sequence $(a_m(C))_m$ for any conjugacy class C in the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ such that

$$a_p(C) \equiv \begin{cases} 1 \mod p & (\text{if } \phi_{\mathfrak{p}} \in C \text{ for } \mathfrak{p} \mid p), \\ 0 \mod p & (\text{otherwise}) \end{cases} \tag{3.1}$$

holds for all but finitely many primes p. Then we will illustrate it by some examples.

3.1. Proof of Theorem 1.3

Motivated by the right-hand side of (3.1), for $\varrho \in G$ and a prime p which is unramified in $L/\mathbb{Q}$, we define

$$I_\varrho(p) := \begin{cases} 1 & (\text{if } \phi_{\mathfrak{p}} \in [\varrho] \text{ for } \mathfrak{p} \mid p), \\ 0 & (\text{otherwise}), \end{cases}$$

where $[\varrho]$ denotes the conjugacy class of ϱ in G as in (2.4). We also let

$$e_\varrho^{\mathcal{A}} := (I_\varrho(p))_p \in \mathcal{A}.$$

Proof of Theorem 1.3. Define $e_\varrho \colon G \to L$ by

$$e_\varrho(\tau) := \begin{cases} 1 & (\text{if } \tau \in [\varrho]), \\ 0 & (\text{otherwise}). \end{cases} \tag{3.2}$$

One finds that $e_\varrho \in A(L)$. By definition, we have that $\mathrm{ev}(e_\varrho) = e_\varrho^{\mathcal{A}}$, which implies $e_\varrho^{\mathcal{A}} \in \mathcal{P}_L^{\mathcal{A}}$. Therefore, the result follows from Theorem 2.9 (2). □

It should be noted that the above element $e_\varrho \in A(L)$ becomes the idempotent (i.e., $e_\varrho^2 = e_\varrho$) corresponding to the unit element of the component $L^{C_G(\varrho)}$ via the isomorphism $A(L) \cong \prod_{\varrho \in R} L^{C_G(\varrho)}$ given in Proposition 2.11.

3.2. Methodology

We are interested not only in the existence of a sequence $\boldsymbol{a} \in \mathrm{Rec}(f;\mathbb{Q})$ such that $e_\varrho^{\mathcal{A}} = r_f(\boldsymbol{a})$, but also in finding such a sequence explicitly. In the following, we explain our method to compute the sequence $\boldsymbol{a}$.

Proposition 3.1. *Let L be a finite Galois extension over $\mathbb{Q}$ and f a monic polynomial in $\mathbb{Q}[x]$ which decomposes into linear factors over L. Suppose that all roots $\xi_1, \ldots, \xi_d$ of f are simple and that $e_\varrho^{\mathcal{A}} \in r_f\big(\mathrm{Rec}(f;\mathbb{Q})\big)$. Then, there exists a solution $(z_1, \ldots, z_d) \in L^d$ to the linear equations*

$$\sum_{j=1}^{d} z_j \tau(\xi_j) = \begin{cases} 1 & (\tau \in [\varrho]), \\ 0 & (\tau \notin [\varrho]). \end{cases} \tag{3.3}$$

With this solution, letting $a_m = \sum_{j=1}^{d} z_j \xi_j^m$ $(m \geq 0)$, we obtain

$$e_\varrho^{\mathcal{A}} = r_f\big((a_m)_m\big).$$

Proof. Since all roots of f are simple, the set $\{(\xi_j^m)_m \mid j = 1, \dots, d\}$ is a basis of $\mathrm{Rec}(f; L)$ (see (2.2)). Accordingly, for any $\boldsymbol{a} \in \mathrm{Rec}(f; \mathbb{Q})$, we can write $\boldsymbol{a} = \left(\sum_{j=1}^{d} z_j \xi_j^m\right)_m$ for some $z_j \in L$. For such $\boldsymbol{a}$, one has

$$\begin{array}{ccccc} \mathrm{Rec}(f;\mathbb{Q}) & \xrightarrow{\psi_f} & (L \otimes L)^G & \xrightarrow{\varphi} & A(L), \\ \boldsymbol{a} & \longmapsto & \displaystyle\sum_{j=1}^{d} z_j \otimes \xi_j & \longmapsto & \left(\tau \mapsto \displaystyle\sum_{j=1}^{d} z_j \tau(\xi_j)\right). \end{array}$$

Hence the assumption $e_\varrho^{\mathcal{A}} \in r_f\big(\mathrm{Rec}(f; \mathbb{Q})\big)$ shows the existence of solutions to the linear system (3.3) in L^d, and for such a solution, we get $e_\varrho^{\mathcal{A}} = r_f(\boldsymbol{a})$ as desired. □

If all roots of f are simple and form a basis of L over $\mathbb{Q}$ (equivalently, if f is the minimal polynomial of a normal element of L over $\mathbb{Q}$), then by Theorem 2.9 (2), the map $r_f\colon \mathrm{Rec}(f; \mathbb{Q}) \to \mathcal{P}_L^{\mathcal{A}}$ is an isomorphism. In this case, we always have a unique solution to the equation (3.3), which gives rise to a solution to $e_\varrho^{\mathcal{A}} = r_f(\boldsymbol{a})$. In the computation, we do not need to find the above solution $(z_1, \dots, z_d) \in L^d$ explicitly. For example, in the case $\varrho = \mathrm{id}$, let x_m $(m \geq 0)$ be the determinant

$$x_m = \begin{vmatrix} \xi_1^m & \xi_2^m & \cdots & \xi_d^m \\ \tau_2(\xi_1) & \tau_2(\xi_2) & \cdots & \tau_2(\xi_d) \\ \vdots & \vdots & \ddots & \vdots \\ \tau_d(\xi_1) & \tau_d(\xi_2) & \cdots & \tau_d(\xi_d) \end{vmatrix},$$

where we set $\{\tau_1, \dots, \tau_d\} = G$ with $\tau_1 = \mathrm{id}$. Then, by Cramer's rule, we have $e_{\mathrm{id}}^{\mathcal{A}} = r_f\big((a_m)_m\big)$ with $a_m = x_m / x_1$.

3.3. Examples

Let us work out some examples of the solution to the equation $e_\varrho^{\mathcal{A}} = r_f(\boldsymbol{a})$. For simplicity, we write

$$e^{\mathcal{A}} := e_{\mathrm{id}}^{\mathcal{A}}.$$

Note that a sequence $\boldsymbol{a} \in \mathrm{Rec}(f; \mathbb{Q})$ such that $e^{\mathcal{A}} = r_f(\boldsymbol{a})$ satisfies the congruences (1.8) for all but finitely many p, and hence, gives an explicit description of the set $\mathrm{Spl}(L)$ of primes splitting completely in $L/\mathbb{Q}$. We also remark that the argument in the ring $\mathcal{A}$ does not explicitly determine a finite set of exceptional primes. This problem is discussed in the next section.

Example 3.2 *(Quadratic fields).* For a square-free integer D, let $L = \mathbb{Q}(\sqrt{D})$ and write $G = \{\mathrm{id}, \tau\}$. In this case, since p splits completely in L if and only if $\left(\frac{D}{p}\right) = 1$, the idempotents $e_\varrho^{\mathcal{A}} \in \mathcal{P}_L^{\mathcal{A}}$ are simply written as

$$e^{\mathcal{A}} = e^{\mathcal{A}}_{\mathrm{id}} = \frac{1}{2}\left(1 + \left(\frac{D}{p}\right)\right)_p \quad \text{and} \quad e^{\mathcal{A}}_{\tau} = \frac{1}{2}\left(1 - \left(\frac{D}{p}\right)\right)_p .$$

Now suppose that $\xi \in L$ is a normal element of L. Its minimal polynomial $f = (x - \xi)(x - \tau(\xi)) = x^2 - c_1 x + c_2 \in \mathbb{Q}[x]$ satisfies $c_1 \neq 0$. Note that $\xi = \frac{c_1 \pm \sqrt{c_1^2 - 4c_2}}{2}$. With this, it holds that

$$x_0 = \begin{vmatrix} 1 & 1 \\ \tau(\xi) & \xi \end{vmatrix} = \sqrt{c_1^2 - 4c_2}, \quad x_1 = \begin{vmatrix} \xi & \tau(\xi) \\ \tau(\xi) & \xi \end{vmatrix} = c_1\sqrt{c_1^2 - 4c_2}.$$

Then the solution to $e^{\mathcal{A}} = r_f(\boldsymbol{a})$ is given by $\boldsymbol{a} \in \mathrm{Rec}(f;\mathbb{Q})$ with the initial values $a_0 = \frac{1}{c_1},\ a_1 = 1$.

Example 3.3 *(Cyclic cubic fields).* Let L be a cyclic cubic extension over $\mathbb{Q}$ and τ the element of G of order 3, i.e., $G = \{1, \tau, \tau^2\}$. Set $\tau_j = \tau^{j-1}$ for $j = 1, 2, 3$. Suppose that $\xi \in L$ is a normal element of L. Let $f(x) = x^3 - c_1 x^2 + c_2 x - c_3$ be the minimal polynomial of ξ over $\mathbb{Q}$ ($c_1 \neq 0$). Then we see that

$$\begin{aligned} x_0 &= 3c_2 - c_1^2, \\ x_1 &= c_1(3c_2 - c_1^2), \\ x_2 &= 4c_1^2 c_2 - 3c_1 c_3 - 2c_2^2 - c_1^4. \end{aligned}$$

Therefore, the corresponding sequence $(a_m)_m \in \mathrm{Rec}(f;\mathbb{Q})$ to $e^{\mathcal{A}} \in \mathcal{P}_L^{\mathcal{A}}$ is determined by the initial values

$$a_0 = \frac{1}{c_1}, \quad a_1 = 1, \quad a_2 = \frac{4c_1^2 c_2 - 3c_1 c_3 - 2c_2^2 - c_1^4}{c_1(3c_2 - c_1^2)}.$$

Remark 3.4. For every cyclic cubic field $L/\mathbb{Q}$, there is a rational number $t \in \mathbb{Q}$ such that L is the splitting field of Shanks' polynomial [22]

$$f_t(x) = x^3 - tx^2 - (t+3)x - 1.$$

When $t \neq 0$, the above result shows that the sequence $(a_m)_m \in \mathrm{Rec}(f_t;\mathbb{Q})$ with the initial values

$$a_0 = \frac{1}{t}, \quad a_1 = 1, \quad a_2 = \frac{2}{t} + 1 + t$$

satisfies $e^{\mathcal{A}} = r_{f_t}((a_m)_m)$. Note that the splitting field of f_0 coincides with $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$ which is the splitting field of both f_3 and f_{54}; see [7].

As an example of a decomposition law, we prove Proposition 1.5, the case $L = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi\sqrt{-1}/3})$ whose Galois group is the symmetric group $\mathfrak{S}_3$.

Proof of Proposition 1.5. Let $\omega = e^{\frac{2\pi\sqrt{-1}}{3}}$. The element $\xi = \omega + 2^{\frac{1}{3}} + 2^{\frac{2}{3}}\omega$ is a normal element of L and its minimal polynomial coincides with $f(x) = x^6 + 3x^5 + 12x^4 + 25x^3 + 60x^2 + 51x + 127$. By Theorem 2.9, the map $r_f : \mathrm{Rec}(f;\mathbb{Q}) \to \mathcal{P}_L^{\mathcal{A}}$ is an isomorphism.

Define the automorphisms σ_1, σ_2 of the Galois group G for the generators $2^{\frac{1}{3}}$ and ω of L by

$$\sigma_1\big(2^{\frac{1}{3}}\big) = 2^{\frac{1}{3}}\omega,\ \sigma_1(\omega) = \omega \text{ and } \sigma_2\big(2^{\frac{1}{3}}\big) = 2^{\frac{1}{3}},\ \sigma_2(\omega) = \omega^2.$$

These are representatives of conjugacy classes of G: $G = [\mathrm{id}] \cup [\sigma_1] \cup [\sigma_2]$ with $\#[\sigma_1] = 2, \#[\sigma_2] = 3$. All elements of G are $\tau_1 = \mathrm{id},\ \tau_2 = \sigma_1,\ \tau_3 = \sigma_1^2,\ \tau_4 = \sigma_2,\ \tau_5 = \sigma_1\sigma_2,\ \tau_6 = \sigma_1^2\sigma_2$. Let $\xi_j = \tau_j(\xi)$ $(j = 1, 2, \ldots, 6)$, a basis of L. The group homomorphism $\rho : \mathrm{Gal}(L/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$ given by

$$\sigma_1 \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix}, \quad \sigma_2 \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

is an irreducible Artin representation, and hence, for any primes p which is unramified in $L/\mathbb{Q}$ we get

$$b_p = \mathrm{Tr}(\rho(\phi_{\mathfrak{p}})) = \begin{cases} 2 & (\phi_{\mathfrak{p}} \in [\mathrm{id}] \text{ for } \mathfrak{p} \mid p), \\ -1 & (\phi_{\mathfrak{p}} \in [\sigma_1] \text{ for } \mathfrak{p} \mid p), \\ 0 & (\phi_{\mathfrak{p}} \in [\sigma_2] \text{ for } \mathfrak{p} \mid p). \end{cases}$$

Theorem 1.3 shows that $(b_p)_p = 2e_{\mathrm{id}}^{\mathcal{A}} - e_{\sigma_1}^{\mathcal{A}} \in \mathcal{P}_L^{\mathcal{A}}$. By Theorem 2.9 (2), there is a sequence $\boldsymbol{a} = (a_m)_m \in \mathrm{Rec}(f;\mathbb{Q})$ such that $r_f(\boldsymbol{a}) = (b_p)_p$. Similarly to Proposition 3.1, we now consider the system of linear equations

$$\begin{pmatrix} \tau_1(\xi_1) & \cdots & \tau_1(\xi_6) \\ \tau_2(\xi_1) & \cdots & \tau_2(\xi_6) \\ \vdots & \cdots & \vdots \\ \tau_6(\xi_1) & \cdots & \tau_6(\xi_6) \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ \vdots \\ z_6 \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \\ -1 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{3.4}$$

Note that, as a permutation on the set $\{\xi_1, \ldots, \xi_6\}$, the automorphisms σ_1, σ_2 are viewed as

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 5 & 1 & 3 & 2 \end{pmatrix},$$

so the coefficient matrix of (3.4) is

$$\begin{pmatrix} \xi_1 & \xi_2 & \xi_3 & \xi_4 & \xi_5 & \xi_6 \\ \xi_2 & \xi_3 & \xi_1 & \xi_5 & \xi_6 & \xi_4 \\ \xi_3 & \xi_1 & \xi_2 & \xi_6 & \xi_4 & \xi_5 \\ \xi_4 & \xi_6 & \xi_5 & \xi_1 & \xi_3 & \xi_2 \\ \xi_5 & \xi_4 & \xi_6 & \xi_2 & \xi_1 & \xi_3 \\ \xi_6 & \xi_5 & \xi_4 & \xi_3 & \xi_2 & \xi_1 \end{pmatrix}.$$

Let $z = \frac{1}{54}(2\xi_1 - \xi_2 - \xi_3 - 2\xi_4 - 2\xi_5 + 4\xi_6)$. Then one can check that

$$(z_1, z_2, \dots, z_6) = (\tau_1(z), \tau_2(z), \dots, \tau_6(z))$$

is the unique solution to (3.4). With this, we obtain

$$(a_m)_m = \left(\sum_{j=1}^{6} \tau_j(z)\xi_j^m \right)_m \in \mathrm{Rec}(f; \mathbb{Q}),$$

which satisfies $a_p \equiv b_p \bmod p$ for all but finitely many primes p. In particular, we see that the initial values are given by $(a_0, a_1, \dots, a_5) = (0, 2, -4, -3, 20, -40)$, from which the desired result follows. □

Several values of $a_p \bmod p$ for $(a_m)_m$ defined in Proposition 1.5 are listed as follows.

p	23	29	31	37	41	43	47	53	59	61	67	71
$a_p \bmod p$	0	0	2	-1	0	2	0	0	0	-1	-1	0

In fact, one can check that these values agree with b_p. In particular, since $b_{31} = b_{43} = 2$, two primes 31 and 43 split completely. However, due to the existence of a finite set of exceptional primes, we cannot deduce this fact from our argument. This inconvenience will be gotten rid of in the next section by considering the "S-integral refinement" of the theory of finite algebraic numbers.

4. Determination of exceptional primes

In §3.2 we have explained how to compute the solution $\boldsymbol{a} \in \mathrm{Rec}(f; \mathbb{Q})$ to the equation $e_\varrho^{\mathcal{A}} = r_f(\boldsymbol{a})$. However, as we have seen above, this method cannot provide information about a finite set S of exceptional primes. The goal of this section is to control the set S by refining the construction given in §2 over the ring of S-integers.

4.1. The ring $\mathcal{A}_{L,S}$

For a finite set S of prime numbers, let

$$\mathbb{Z}_S \coloneqq \mathbb{Z}\left[p^{-1} \mid p \in S\right]$$

be the ring of S-integers. We set

$$\mathcal{A}_S \coloneqq \prod_{p \in \boldsymbol{P}_{\mathbb{Q}} \setminus S} \mathbb{F}_p \cong \mathbb{Z}_S \otimes_{\mathbb{Z}} \prod_{p \in \boldsymbol{P}_{\mathbb{Q}}} \mathbb{F}_p,$$

which is a $\mathbb{Z}_S$-algebra. One can show that

$$\varinjlim_S \mathbb{Z}_S = \mathbb{Q} \quad \text{and} \quad \mathcal{A} = \varinjlim_S \mathcal{A}_S,$$

where S runs through all finite sets of prime numbers and transition maps are the injections $\mathbb{Z}_S \to \mathbb{Z}_{S'}$ and the projections $\mathcal{A}_S \to \mathcal{A}_{S'}$ for $S \subset S'$, respectively. From the latter equality, we have the canonical surjection $\mathcal{A}_S \to \mathcal{A}$ sending each element to its equivalence class. We also set

$$O_{L,S} \coloneqq O_L \otimes_{\mathbb{Z}} \mathbb{Z}_S, \qquad \mathcal{A}_{L,S} \coloneqq \prod_{\mathfrak{p} \in \boldsymbol{P}_L \setminus S_L} O_L/\mathfrak{p} \cong O_{L,S} \otimes_{O_L} \prod_{\mathfrak{p} \in \boldsymbol{P}_L} O_L/\mathfrak{p},$$

where S_L denotes the set of primes of L lying above elements of S. Then we have

$$\varinjlim_S O_{L,S} = L \quad \text{and} \quad \mathcal{A}_L = \varinjlim_S \mathcal{A}_{L,S}.$$

Note that each $\mathcal{A}_{L,S}$ admits a natural G-action, which induces the G-action on $\mathcal{A}_L$ by passage to the inductive limit.

4.2. Modules and homomorphisms over $O_{L,S}$

In this subsection, we construct the G-equivariant homomorphisms

$$\mathrm{Rec}(f; O_{L,S}) \xrightarrow{\psi_{f,S}} O_{L,S} \otimes O_{L,S} \xrightarrow{\varphi_S} \mathrm{Fun}(G, O_{L,S}) \xrightarrow{\mathrm{ev}_S} \mathcal{A}_{L,S}$$

of $O_{L,S}$-modules, under some assumptions on S and f.

First let us consider the map

$$\varphi_S \colon O_{L,S} \otimes O_{L,S} \longrightarrow \mathrm{Fun}(G, O_{L,S});\ \xi \otimes \eta \longmapsto \big(\tau \mapsto \xi\tau(\eta)\big),$$

which is the S-integral version of the isomorphism $\varphi\colon L \otimes L \to \mathrm{Fun}(G, L)$. This is a homomorphism of $O_{L,S}$-algebras, and is G-equivariant.

Proposition 4.1. *If S contains all primes which ramify in $L/\mathbb{Q}$, then the map φ_S is an isomorphism.*

Proof. Recall that the discriminant of the number field L is defined by

$$\mathrm{disc}(L) = \big(\det\big(\tau(\omega_j)\big)_{\tau,j}\big)^2, \tag{4.1}$$

where $\{\omega_1, \ldots, \omega_n\}$ is a $\mathbb{Z}$-basis of O_L. Here, $\big(\tau(\omega_j)\big)_{\tau,j}$ denotes the $n \times n$ matrix whose (i,j)-entry is $\tau_i(\omega_j)$, with some permutation $\tau_1, \ldots, \tau_n$ of elements of G; its square is independent of the permutation.

By Dedekind's theorem on ramification and the assumption on S, the discriminant $\operatorname{disc}(L)$ is invertible in $\mathbb{Z}_S$, hence in $O_{L,S}$. This means that the functions $\tau \mapsto \tau(\omega_j)$ for $j = 1, \ldots, n$ form an $O_{L,S}$-basis of $\operatorname{Fun}(G, O_{L,S})$. On the other hand, the elements $1 \otimes \omega_j$ form an $O_{L,S}$-basis of $O_{L,S} \otimes O_{L,S}$. Therefore, φ_S maps a basis to a basis, hence is an isomorphism. □

In the following, we always assume that S contains all primes ramifying in $L/\mathbb{Q}$. Then we can also define the homomorphism of $O_{L,S}$-algebras

$$\mathrm{ev}_S \colon \operatorname{Fun}(G, O_{L,S}) \longrightarrow \mathcal{A}_{L,S}$$

by

$$\mathrm{ev}_S(g) := \big(g(\phi_\mathfrak{p}) \bmod \mathfrak{p}\big)_\mathfrak{p}.$$

Note that the L-algebra homomorphism $\mathrm{ev} \colon \operatorname{Fun}(G, L) \to \mathcal{A}_L$ given in Definition 2.3 is obtained from the above maps by passage to the inductive limit $\varinjlim_S$.

Proposition 4.2. *The map* $\mathrm{ev}_S \colon \operatorname{Fun}(G, O_{L,S}) \longrightarrow \mathcal{A}_{L,S}$ *is G-equivariant and injective.*

Proof. This is shown in the proof of Proposition 2.4. □

Finally, let us construct the S-integral version of $\psi_f \colon \operatorname{Rec}(f; L) \to L \otimes L$. Let $f(x) = x^d + c_1 x^{d-1} + \cdots + c_d$ be a monic polynomial with coefficients in $\mathbb{Z}_S$. For any $\mathbb{Z}_S$-algebra R, let $\operatorname{Rec}(f; R)$ denote the R-module of sequences $(a_m)_m$ in R satisfying the linear recurrence relation $a_m + c_1 a_{m-1} + \cdots + c_d a_{m-d} = 0$ for all $m \geq d$.

In the following, we assume that the monic polynomial $f \in \mathbb{Z}_S[x]$ of degree d has d distinct roots $\xi_1, \ldots, \xi_d$, all belonging to L. Note that f is not necessarily irreducible over $\mathbb{Q}$ at this stage.

Proposition 4.3.

(1) *For $j = 1, \ldots, d$, the sequence $(\xi_j^m)_m$ is an element of* $\operatorname{Rec}(f; O_{L,S})$.
(2) *The elements $(\xi_j^m)_m$ for $j = 1, \ldots, d$ form an $O_{L,S}$-basis of* $\operatorname{Rec}(f; O_{L,S})$ *if and only if the discriminant* $\operatorname{disc}(f) = \prod_{i<j}(\xi_i - \xi_j)^2$ *of the polynomial f is invertible in $\mathbb{Z}_S$.*

Proof. (1) Since $O_{L,S}$ is the integral closure of $\mathbb{Z}_S$ in L, we have $\xi_j \in O_{L,S}$. The recurrence relation of $(\xi_j^m)_m$ is obvious.

(2) Note that the map $(a_m)_m \mapsto (a_0, \dots, a_{d-1})$ gives an isomorphism $\mathrm{Rec}(f; R) \to R^d$ of R-modules. Thus $(\xi_j^m)_m$ $(j = 1, \dots, d)$ forms a basis if and only if the Vandermonde determinant

$$\det \begin{pmatrix} 1 & \xi_1 & \dots & \xi_1^{d-1} \\ 1 & \xi_2 & \dots & \xi_2^{d-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \xi_d & \dots & \xi_d^{d-1} \end{pmatrix}$$

is invertible in $O_{L,S}$. Since its square is equal to $\mathrm{disc}(f)$, the statement follows. □

By Proposition 4.3, supposing that $\mathrm{disc}(f) \in \mathbb{Z}_S^\times$, we can define the $O_{L,S}$-linear map

$$\psi_{f,S}\colon\ \mathrm{Rec}(f; O_{L,S}) \longrightarrow O_{L,S} \otimes O_{L,S};\ (\xi_j^m)_m \longmapsto 1 \otimes \xi_j.$$

This is a G-equivariant map.

Proposition 4.4. *The following conditions are equivalent.*

(1) *The map $\psi_{f,S}$ is an isomorphism.*
(2) *All roots $\xi_1, \dots, \xi_d$ of f form a $\mathbb{Z}_S$-basis of $O_{L,S}$.*
(3) *$d = [L : \mathbb{Q}]$ and $\det\big(\mathrm{Tr}(\xi_i \xi_j)\big)_{i,j} \in \mathbb{Z}_S^\times$.*

Proof. It is obvious that (1) and (2) are equivalent.

Let us show the equivalence of (2) and (3). Since each of them includes the condition $d = [L : \mathbb{Q}]$, we may assume it. If we put $X = O_{L,S}$ and $X' = \sum_{j=1}^d \mathbb{Z}_S \cdot \xi_j$, we have $X' \subset X$ and

$$X' = X \iff O_{L,S} \cdot \det\big(\mathrm{Tr}(\xi_i \xi_j)\big)_{i,j} = O_{L,S} \cdot \mathrm{disc}(L) \ \big(= O_{L,S}\big),$$

cf. [21, Chapter III, Corollary to Proposition 5]. Therefore, the condition (2) holds if and only if $d = [L : \mathbb{Q}]$ and $\det\big(\mathrm{Tr}(\xi_i \xi_j)\big)_{i,j}$ is invertible in $O_{L,S}$. Since $\det\big(\mathrm{Tr}(\xi_i \xi_j)\big)_{i,j}$ obviously belongs to $\mathbb{Z}_S$, the latter condition is equivalent to (3). □

Remark 4.5. Given a finite Galois extension $L/\mathbb{Q}$, we have introduced the following conditions on a finite set S of primes and a monic polynomial $f \in \mathbb{Q}[x]$ of degree d with d distinct roots $\xi_1, \dots, \xi_d$ in L:

(S1) S contains all primes ramifying in $L/\mathbb{Q}$.
(S2) f belongs to $\mathbb{Z}_S[x]$ and $\mathrm{disc}(f) \in \mathbb{Z}_S^\times$.
(S3) $d = [L : \mathbb{Q}]$ and $\det\big(\mathrm{Tr}(\xi_i \xi_j)\big)_{i,j} \in \mathbb{Z}_S^\times$.

The conditions (S1) and (S2) already appear in Theorem 1.6. The role of each condition is as follows. (S1) ensures that φ_S is an isomorphism and also is needed to define the map ev_S. (S2) allows us to define the map $\psi_{f,S}$, and then, the new condition (S3) is necessary and sufficient for $\psi_{f,S}$ to be an isomorphism.

For any finite Galois extension L over $\mathbb{Q}$, one can construct a pair (S, f) satisfying all of these conditions as follows. First let f be the minimal polynomial of a normal basis $\xi_1, \ldots, \xi_d$ of $L/\mathbb{Q}$. Then let S be the set of primes which ramify in L, divide the denominator of a coefficient of f, divide the numerator of $\mathrm{disc}(f)$, or divide the numerator of $\det\bigl(\mathrm{Tr}(\xi_i\xi_j)\bigr)_{i,j}$.

4.3. *S-integers in $\mathcal{P}_L^{\mathcal{A}}$*

As in the previous subsection, let S be a finite set of primes containing all ones ramifying in $L/\mathbb{Q}$. By taking the G-invariant part of

$$O_{L,S} \otimes O_{L,S} \xrightarrow{\varphi_S} \mathrm{Fun}(G, O_{L,S}) \xrightarrow{\mathrm{ev}_S} \mathcal{A}_{L,S},$$

we obtain $\mathbb{Z}_S$-algebra homomorphisms

$$(O_{L,S} \otimes O_{L,S})^G \xrightarrow{\varphi_S} A(L,S) := \mathrm{Fun}(G, O_{L,S})^G \xrightarrow{\mathrm{ev}_S} (\mathcal{A}_{L,S})^G \cong \mathcal{A}_S.$$

The last isomorphism $(\mathcal{A}_{L,S})^G \cong \mathcal{A}_S$ is shown in the same way as Proposition 2.7.

Definition 4.6. For a finite Galois extension L over $\mathbb{Q}$ and a finite set S of primes containing all ones ramifying in $L/\mathbb{Q}$, we define a $\mathbb{Z}_S$-subalgebra $\mathcal{P}_{L,S}^{\mathcal{A}}$ of $\mathcal{A}_{L,S}$ by

$$\mathcal{P}_{L,S}^{\mathcal{A}} := \mathrm{ev}_S\bigl(A(L,S)\bigr).$$

From the commutative diagram

$$\begin{tikzcd}
A(L,S) \arrow[r, "\mathrm{ev}_S", "\cong"'] \arrow[d, hook] & \mathcal{P}_{L,S}^{\mathcal{A}} \arrow[r, hook] \arrow[d] & \mathcal{A}_S \arrow[d, two heads] \\
A(L) \arrow[r, "\mathrm{ev}", "\cong"'] & \mathcal{P}_L^{\mathcal{A}} \arrow[r, hook] & \mathcal{A}
\end{tikzcd}$$

we see that the image of $\mathcal{P}_{L,S}^{\mathcal{A}}$ under the projection $\mathcal{A}_S \to \mathcal{A}$ is contained in $\mathcal{P}_L^{\mathcal{A}}$, and the induced map $\mathcal{P}_{L,S}^{\mathcal{A}} \to \mathcal{P}_L^{\mathcal{A}}$ is an injection. Therefore, we may view $\mathcal{P}_{L,S}^{\mathcal{A}}$ as a subring of $\mathcal{P}_L^{\mathcal{A}}$. We call it *the ring of S-integers* in $\mathcal{P}_L^{\mathcal{A}}$.

As in the case of finite algebraic numbers, every S-integer in $\mathcal{P}_L^{\mathcal{A}}$ is obtained from an S-integral sequence in $\mathrm{Rec}(f; \mathbb{Z}_S)$ for some $f \in \mathbb{Z}_S[x]$. To see this, we first notice that, if $f(x) \in \mathbb{Q}[x]$ is a monic polynomial having distinct roots in L and satisfying the condition (S2) in Remark 4.5, we have a map

$$\psi_{f,S} \colon \mathrm{Rec}(f; \mathbb{Z}_S) \longrightarrow (O_{L,S} \otimes O_{L,S})^G,$$

which is the G-invariant part of $\psi_{f,S}\colon \operatorname{Rec}(f; O_{L,S}) \to O_{L,S} \otimes O_{L,S}$. Then, similarly to the case over $\mathbb{Q}$ (cf. Theorem 2.9), one can observe that the composition $\mathrm{ev}_S \circ \varphi_S \circ \psi_{f,S}$ is equal to the map

$$r_{f,S}\colon \operatorname{Rec}(f; \mathbb{Z}_S) \longrightarrow \mathcal{P}^{\mathcal{A}}_{L,S};\ (a_m)_m \longmapsto (a_p \bmod p)_p.$$

Further, if S satisfies the condition (S3) in Remark 4.5, then the above map $r_{f,S}$ is an isomorphism. As a result, we obtain the S-integral refinement of Theorem 2.9.

Theorem 4.7. *Let S be a finite subset of primes and $f \in \mathbb{Q}[x]$ a monic polynomial of degree d with d distinct roots in L.*

(1) *If S and f satisfy the conditions (S1) and (S2) in Remark 4.5, then we have that $r_{f,S} = \mathrm{ev}_S \circ \varphi_S \circ \psi_{f,S}$. In particular, $r_{f,S}\bigl(\operatorname{Rec}(f; \mathbb{Z}_S)\bigr) \subset \mathcal{P}^{\mathcal{A}}_{L,S}$.*
(2) *If S and f satisfy the conditions (S1) to (S3) in Remark 4.5, then the map $r_{f,S}$: $\operatorname{Rec}(f; \mathbb{Z}_S) \to \mathcal{P}^{\mathcal{A}}_{L,S}$ is an isomorphism.*

4.4. Decomposition laws of primes with recurrent sequences

In this subsection, we discuss the determination problems of exceptional primes in our decomposition law of primes in L.

Let us prove Theorem 1.6. We notice that for each $\varrho \in G$, the function e_ϱ defined in (3.2) lies in $A(L, S)$ for any S. Denote its image under the map ev_S by $e^{\mathcal{A}}_{\varrho,S} \in \mathcal{P}^{\mathcal{A}}_{L,S}$. This element $e^{\mathcal{A}}_{\varrho,S}$ coincides with $e^{\mathcal{A}}_{\varrho} = \mathrm{ev}(e_\varrho) \in \mathcal{P}^{\mathcal{A}}_{L}$ studied in §3 under the inclusion $\mathcal{P}^{\mathcal{A}}_{L,S} \subset \mathcal{P}^{\mathcal{A}}_{L}$ mentioned above.

Proof of Theorem 1.6. From the assumption on S and f, we have $r_{f,S}\bigl(\operatorname{Rec}(f; \mathbb{Z}_S)\bigr) \subset \mathcal{P}^{\mathcal{A}}_{L,S}$. Since $\boldsymbol{a} = (a_m)_m \in \operatorname{Rec}(f; \mathbb{Z}_S)$, we obtain the identity $e^{\mathcal{A}}_{\varrho,S} = r_{f,S}(\boldsymbol{a})$ in $\mathcal{P}^{\mathcal{A}}_{L,S}$ for any $\rho \in C$, from which the desired result follows. □

Below, we write $e^{\mathcal{A}} = e^{\mathcal{A}}_{\mathrm{id,S}}$ and consider the equation

$$e^{\mathcal{A}} = r_{f,S}(\boldsymbol{a}) \tag{4.2}$$

with $\boldsymbol{a} \in \operatorname{Rec}(f; \mathbb{Z}_S)$ to get a characterization of the splitting primes in $L/\mathbb{Q}$. In some cases, it is convenient to work with a polynomial f which is *not* the minimal polynomial of a normal element (namely, use Theorem 4.7 (1)). Though ψ_f is not an isomorphism for such f, it is sometimes possible to give an explicit set S satisfying (S1) and (S2) in Remark 4.5 and an explicit solution to (4.2).

As examples of solutions to (4.2), we deal with two families: the cyclotomic field $\mathbb{Q}(\zeta_N)$ and the field $\mathbb{Q}(\zeta_N, \sqrt[N]{M})$, where ζ_N is a primitive N-th root of unity.

Example 4.8 *(Cyclotomic fields $\mathbb{Q}(\zeta_N)$).* Let N be a positive integer and $\mathbb{Q}(\zeta_N)$ be the cyclotomic field. Then

$$S = \{p \in \boldsymbol{P}_{\mathbb{Q}} \mid p \text{ divides } N\}$$

satisfies the condition (S1). Moreover, let $f(x) = x^N - 1$. We have

$$\begin{aligned}\operatorname{disc}(f) &= \prod_{0\le i<j\le N-1} (\zeta_N^i - \zeta_N^j)^2 = (-1)^{N(N-1)/2} \prod_{\substack{0\le i,j\le N-1\\ i\neq j}} (\zeta_N^i - \zeta_N^j)\\ &= (-1)^{N(N-1)/2}\zeta_N^{N(N-1)/2}\left(\prod_{k=1}^{N-1}(1-\zeta_N^k)\right)^N = (-1)^{N(N-1)/2}N^N,\end{aligned}$$

since

$$\prod_{k=1}^{N-1}(1-\zeta_N^k) = \left.\frac{x^N-1}{x-1}\right|_{x=1} = N.$$

Thus the condition (S2) also holds for S and f.

Now let $\boldsymbol{a} = (a_m)_m$ be the sequence given by

$$a_m := \begin{cases} 1 & (m \equiv 1 \mod N),\\ 0 & (m \not\equiv 1 \mod N),\end{cases}$$

which obviously belongs to $\operatorname{Rec}(f; \mathbb{Z}_S)$. As an element of $\operatorname{Rec}(f; O_{L,S})$, it is also written as

$$a_m = \frac{1}{N}\sum_{j=0}^{N-1}\zeta_N^{(m-1)j} = \frac{1}{N}\sum_{j=0}^{N-1}\zeta_N^{-j}(\zeta_N^j)^m.$$

Hence we have

$$\psi_{f,S}(\boldsymbol{a}) = \frac{1}{N}\sum_{j=0}^{N-1}\zeta_N^{-j}\otimes\zeta_N^j, \qquad \varphi_S\circ\psi_{f,S}(\boldsymbol{a})(\tau) = \frac{1}{N}\sum_{j=0}^{N-1}\zeta_N^{-j}\tau(\zeta_N^j) \quad (\tau\in G).$$

Now recall that each $\tau \in G$ is characterized by $\tau(\zeta_N) = \zeta_N^a$ with a unique $a \in (\mathbb{Z}/N\mathbb{Z})^\times$. Then

$$\varphi_S\circ\psi_{f,S}(\boldsymbol{a})(\tau) = \frac{1}{N}\sum_{j=0}^{N-1}\zeta_N^{-j}\zeta_N^{aj} = \frac{1}{N}\sum_{j=0}^{N-1}\zeta_N^{(a-1)j} = \begin{cases} 1 & (a = 1 \text{ in } (\mathbb{Z}/N\mathbb{Z})^\times),\\ 0 & (\text{otherwise}).\end{cases}$$

Since $a = 1$ in $(\mathbb{Z}/N\mathbb{Z})^\times$ means that $\tau = \mathrm{id}$ in G, we see that $\varphi_S\circ\psi_{f,S}(\boldsymbol{a}) = e_{\mathrm{id}}$, and $r_{f,S}(\boldsymbol{a}) = e^{\mathcal{A}}$ in $\mathcal{P}_{L,S}^{\mathcal{A}}$. Therefore, we obtain the equivalence

$$p \text{ splits completely in } \mathbb{Q}(\zeta_N) \iff a_p \equiv 1 \pmod{p} \iff p \equiv 1 \pmod{N}$$

for all primes p not dividing N, which is a well-known result in the theory of cyclotomic fields.

Example 4.9 *(The fields $\mathbb{Q}(\zeta_N, \sqrt[N]{M})$).* Let N be a positive integer and M an integer for which the field $L = \mathbb{Q}(\zeta_N, \sqrt[N]{M})$ has degree N over $\mathbb{Q}(\zeta_N)$. Note that this includes the field considered in Proposition 1.5.

We set

$$\begin{aligned} S &= \{p \in \boldsymbol{P}_{\mathbb{Q}} \mid p \text{ divides } N,\, M \text{ or } M^j - 1 \text{ for some } j = 1, \dots, N-1\}, \\ f(x) &= \prod_{j=0}^{N-1} (x^N - M^j). \end{aligned}$$

The condition (S1) holds since only the prime divisors of NM ramify in L. Moreover, after some computations, we obtain that

$$\operatorname{disc}(f) = N^{N^2} \cdot M^{N(N-1)^2/2} \cdot \prod_{\substack{0 \le j, j' \le N-1 \\ j \ne j'}} (M^j - M^{j'})^N,$$

which implies the condition (S2).

The roots of f are written as $\zeta_N^i M^{j/N}$ with $i, j = 0, \dots, N-1$. The Galois group is given by $G = \{\tau_{a,b} \mid a \in (\mathbb{Z}/N\mathbb{Z})^\times,\, b = 0, \dots, N-1\}$, where

$$\tau_{a,b}(\zeta_N) = \zeta_N^a, \quad \tau_{a,b}(M^{1/N}) = \zeta_N^b M^{1/N}, \text{ so } \tau_{a,b}(\zeta_N^i M^{j/N}) = \zeta_N^{ai+bj} M^{j/N}.$$

Now we define the sequence $\boldsymbol{a} = (a_m)_m$ by

$$\begin{aligned} a_m &= \frac{1}{N^2} \sum_{i,j=0}^{N-1} \zeta_N^{(m-1)i} M^{(m-1)j/N} = \frac{1}{N^2} \sum_{i,j=0}^{N-1} \zeta_N^{-i} M^{-j/N} (\zeta_N^i M^{j/N})^m \\ &= \begin{cases} \frac{1}{N} \sum_{j=0}^{N-1} M^{j(m-1)/N} & (m \equiv 1 \mod N), \\ 0 & (m \not\equiv 1 \mod N). \end{cases} \end{aligned}$$

This belongs to $\operatorname{Rec}(f; \mathbb{Z}_S)$, and satisfies

$$\begin{aligned} \varphi_S \circ \psi_{f,S}(\boldsymbol{a})(\tau_{a,b}) &= \frac{1}{N^2} \sum_{i,j=0}^{N-1} \zeta_N^{-i} M^{-j/N} \tau_{a,b}(\zeta_N^i M^{j/N}) \\ &= \frac{1}{N^2} \sum_{i,j=0}^{N-1} \zeta_N^{-i} M^{-j/N} \cdot \zeta_N^{ai+bj} M^{j/N} \end{aligned}$$

$$= \frac{1}{N^2}\sum_{i,j=0}^{N-1}\zeta_N^{(a-1)i+bj} = \begin{cases} 1 & ((a,b)=(1,0)), \\ 0 & ((a,b)\neq(1,0)). \end{cases}$$

In other words, the identity $e^{\mathcal{A}} = r_{f,S}(\boldsymbol{a})$ holds in $\mathcal{P}^{\mathcal{A}}_{L,S}$. From this, we again reproduce the well-known result

$$p \text{ splits completely in } L \iff p \equiv 1 \bmod N \text{ and } M \text{ is an } N\text{-th power residue modulo } p$$

for $p \notin S$, since

$$a_p = \frac{1}{N}\sum_{j=0}^{N-1}\left(M^{(p-1)/N}\right)^j \equiv \begin{cases} 1 & (M^{(p-1)/N} \equiv 1 \mod p), \\ 0 & (\text{otherwise}) \end{cases}$$

for any prime $p \equiv 1 \mod N$.

Data availability

No data was used for the research described in the article.

Acknowledgments

This work is partially supported by JSPS KAKENHI Grant Number 18K03233, 18H01110, 18H05233, 20K14294 and 21K03185. We are grateful to Prof. Tomokazu Kashio and Ryutaro Sekigawa for answering our questions about cyclic cubic extension.

References

[1] F. Brown, Single-valued motivic periods and multiple zeta values, Forum Math. Sigma 2 (2014) e25.

[2] F. Brown, Notes on motivic periods, Commun. Number Theory Phys. 11 (3) (2017) 557–655.

[3] L.E. Dickson, History of the Theory of Numbers, Volume I: Divisibility and Primality, Stechert, New York, 1934.

[4] D.A. Cox, Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication, Wiley-Interscience, New York, 1970.

[5] P. Deligne, J.P. Serre, Formes modulaires de poids 1 (French), Ann. Sci. Éc. Norm. Supér. (4) 7 (1974) 507–530.

[6] T. Hiramatsu, S. Saito, An Introduction to Non-Abelian Class Field Theory, Series on Number Theory and Its Applications, vol. 13, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2017.

[7] A. Hoshi, On correspondence between solutions of a family of cubic Thue equations and isomorphism classes of the simplest cubic fields, J. Number Theory 131 (11) (2011) 2135–2150.

[8] M. Kaneko, An introduction to classical and finite multiple zeta values, Publ. Math. Univ. Franche-Comté Besançon Algèbr. Theor. Nr. 1 (2019) 103–129.

[9] C. Khare, Remarks on mod p forms of weight one, Int. Math. Res. Not. 3 (1997) 127–133.

[10] C. Khare, J.P. Wintenberger, Serre's modularity conjecture (I), Invent. Math. 178 (2009) 485–504.

[11] C. Khare, J.P. Wintenberger, Serre's modularity conjecture (II), Invent. Math. 178 (2009) 505–586.

[12] M. Kontsevich, Holonomic D-modules and positive characteristic, Jpn. J. Math. 4 (1) (2009) 1–25.

[13] S. Lang, Algebraic Number Theory, 2nd ed., Graduate Text in Mathematics, vol. 110, Springer-Verlag, New York, 1994.

[14] P. Moree, A. Noubissie, Higher reciprocity laws and ternary linear recurrence sequences, arXiv: 2205.06685v1.

[15] J. Neukirch, Algebraic Number Theory, Grundlagen der mathematischen Wissenschaften, vol. 322, Springer-Verlag, Berlin, Heidelberg, New York, 1999.

[16] P. Ribenboim, The Book of Prime Number Records, second ed., Springer, New York, 1989.

[17] J. Rosen, Sequential periods of the crystalline Frobenius, preprint, arXiv:1805.01885.

[18] J. Rosen, A finite analogue of the ring of algebraic numbers, J. Number Theory 208 (2020) 59–71.

[19] SageMath, the Sage Mathematics Software System (Version 9.7), The Sage Developers, 2022, https://www.sagemath.org.

[20] S. Saito, The kth-order Fibonacci-Lucas sequences and their applications to some generalized higher reciprocity law, SUT J. Math. 42 (2) (2006) 207–224.

[21] J.-P. Serre, Local Fields, Graduate Texts in Mathematics, vol. 67, Springer, 1979.

[22] D. Shanks, The simplest cubic fields, Math. Comput. 28 (128) (1974) 1137–1152.

[23] Z.-H. Sun, Cubic and quartic congruences modulo a prime, J. Number Theory 102 (1) (2003) 41–89.

[24] J. Weinstein, Reciprocity laws and Galois representations: recent breakthroughs, Bull. Am. Math. Soc. 53 (1) (2016) 1–39.

[25] B. Wyman, What is a reciprocity law?, Am. Math. Mon. 79 (6) (1972) 571–586.