Journal of Number Theory 208 (2020) 59–71

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

General Section

A finite analogue of the ring of algebraic numbers

Julian Rosen

University of Maine

ARTICLE INFO

Article history:
Received 12 October 2018
Received in revised form 9 July 2019
Accepted 12 July 2019
Available online 27 August 2019
Communicated by S.J. Miller

Keywords:
Finite periods
Frobenius automorphism
Linear recurrence
Congruence

ABSTRACT

We construct an analogue of the ring of algebraic numbers, living in a quotient of the product of all finite fields of prime order. We use this ring to deduce some results about linear recurrent sequences.

1. Introduction

A period is a complex number given as the integral of an algebraic function over a region defined by algebraic inequalities. The set of all periods is a countable subring of $\mathbb{C}$ containing $\overline{\mathbb{Q}}$ (see [8] for an overview of periods). Several recent works (e.g. [3–5,10,11,13]) consider "finite" analogues of certain periods (finite multiple zeta values, finite multiple polylogarithms, etc.) living in the ring

$$\mathcal{A} := \frac{\prod_p \mathbb{Z}/p\mathbb{Z}}{\bigoplus_p \mathbb{Z}/p\mathbb{Z}},$$

E-mail address: julianrosen@gmail.com.

https://doi.org/10.1016/j.jnt.2019.07.017
0022-314X/

which was introduced by Konstsevich ([7], §2.2). An element of $\mathcal{A}$ is a prime-indexed sequence $(a_p)_p$, with $a_p \in \mathbb{Z}/p\mathbb{Z}$, and two sequences are equal if they agree for all sufficiently large p. Every non-zero integer is invertible modulo p for all sufficiently large p, so there is a diagonal embedding $\mathbb{Q} \hookrightarrow \mathcal{A}$.

1.1. Results

The purpose of this paper is to define a countable $\mathbb{Q}$-subalgebra $\mathcal{P}_{\mathcal{A}}^0 \subset \mathcal{A}$ that is a finite analogue of $\overline{\mathbb{Q}} \subset \mathbb{C}$. This algebra is *not* the integral closure of $\mathbb{Q}$ inside $\mathcal{A}$, which has continuum cardinality.

Our first main result is three equivalent characterizations of $\mathcal{P}_{\mathcal{A}}^0$.

Theorem 1.1. *The following subsets of $\mathcal{A}$ are equal.*

(1) *The set of elements $(a_p \mod p)_p$, where $a_0, a_1, a_2, \ldots \in \mathbb{Q}$ is a recurrent sequence (that is, a sequence satisfying a linear recurrence relation with constant coefficients).*
(2) *The set of elements $\big(g(\phi_p) \mod p\big)_p$, where $L/\mathbb{Q}$ is a finite Galois extension, $g : \mathrm{Gal}(L/\mathbb{Q}) \to L$ satisfies $g(\sigma\tau\sigma^{-1}) = \sigma(g(\tau))$, and ϕ_p is the[1] Frobenius at p.*
(3) *The set of $\mathbb{Q}$-linear combinations of matrix coefficients for the $\mathcal{A}$-valued Frobenius automorphism*

$$F_{\mathcal{A}} : L \otimes \mathcal{A} \to L \otimes \mathcal{A},$$

defined by Definition 4.1, as L ranges over all number fields.

The equivalence of (1) and (2) is Theorem 2.2, and the equivalence of (2) and (3) is Theorem 4.2.

Definition 1.2. We define $\mathcal{P}_{\mathcal{A}}^0 \subset \mathcal{A}$ to be the set given by Theorem 1.1.

The Skolem-Mahler-Lech theorem says that if (a_n) is a recurrent sequence, the set $\{n : a_n = 0\}$ has finite symmetric difference with a finite union of arithmetic progressions. As a consequence of Theorem 1.1, we obtain an analogue of Skolem-Mahler-Lech for the set of primes $\{p : a_p \equiv 0 \bmod p\}$. A set P of primes is called *Frobenian* (cf. [12], §3.3) if there is a finite Galois extension $L/\mathbb{Q}$ and a union of conjugacy classes $C \subset \mathrm{Gal}(L/\mathbb{Q})$ such that P has finite symmetric difference with the set of rational primes whose Frobenius conjugacy class is in C. The Chebotarev density theorem implies that the natural density of a Frobenian set exists and is a rational number.

Corollary 1.3. *A set P of primes is Frobenian if and only if there exists a recurrent sequence (a_n) such that*

[1] This is independent of the representative of the Frobenius conjugacy class (see §2).

$$P = \{p : a_p \equiv 0 \bmod p\}.$$

Unlike the Skolem-Mahler-Lech Theorem, Corollary 1.3 is effective: given the recurrence relation satisfied by (a_n) and a list of initial values, there is a finite algorithm to determine the number field L, union of conjugacy classes $C \subset \mathrm{Gal}(L/\mathbb{Q})$, and the finite exceptional set.

We also prove some results about polynomial equations satisfied by elements of $\mathcal{P}^0_{\mathcal{A}}$. The first of these results implies that $\mathcal{P}^0_{\mathcal{A}}$ is an integral extension of $\mathbb{Q}$.

Theorem 1.4. *Suppose $\alpha \in \mathcal{P}^0_{\mathcal{A}}$. Then there exists a non-zero polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$, and every such $f(x)$ has a rational root.*

Remark 1.5. The Fibonacci sequence F_n is known to satisfy the congruence $F_p \equiv \left(\frac{p}{5}\right) \bmod p$ for every prime p, where $\left(\frac{p}{5}\right)$ is a Legendre symbol. Thus $f(F_p) \equiv 0 \bmod p$ for $p \geq 7$, where $f(x) = x^2 - 1 \in \mathbb{Q}[x]$. Theorem 1.4 implies that every recurrent sequence satisfies an analogous identity for some f, which necessarily has a rational root.

We also prove a result about the density of the set of primes p for which $f(a_p) \equiv 0 \bmod p$, when $(a_p) \in \mathcal{P}^0_{\mathcal{A}}$ and $f(x) \in \mathbb{Q}[x]$.

Theorem 1.6. *For $f(x) \in \mathbb{Q}[x]$, we have*

$$\sup_{(a_p)\in\mathcal{P}^0_{\mathcal{A}}} \delta\Big(\big\{p : f(a_p) \equiv 0 \bmod p\big\}\Big) = \delta\Big(\big\{p : f \textit{ has a root mod } p\big\}\Big),$$

where δ denotes natural density. Moreover if $f(x)$ has no rational roots, then there is no element of $\mathcal{P}^0_{\mathcal{A}}$ realizing the supremum.

In §4 we explain the analogy between $\mathcal{P}^0_{\mathcal{A}} \subset \mathcal{A}$ and $\overline{\mathbb{Q}} \subset \mathbb{C}$, and the relationship with periods.

2. Functions on a Galois group

Let $L/\mathbb{Q}$ be a finite Galois extension, with ring of integers $\mathcal{O}_L$ and Galois group $\Gamma := \mathrm{Gal}(L/\mathbb{Q})$.

Definition 2.1 *([9], §2).* We define $A(L)$ to be the set of functions $g : \Gamma \to L$ satisfying

$$g(\sigma\tau\sigma^{-1}) = \sigma(g(\tau)) \tag{2.1}$$

for all $\sigma, \tau \in \Gamma$, which is a commutative $\mathbb{Q}$-algebra under pointwise addition and multiplication.

For $g \in A(L)$, let p be a rational prime unramified in L that is coprime to the denominators of all values of g. Let $\mathfrak{P}$ be a prime of L over p, with Frobenius element $\phi_{\mathfrak{P}} \in \Gamma$. It follows from (2.1) that the residue class

$$g(\phi_{\mathfrak{P}}) \mod \mathfrak{P} \tag{2.2}$$

is fixed by $\phi_{\mathfrak{P}}$, so (2.2) is an element of $\mathbb{Z}/p\mathbb{Z} \subset \mathcal{O}_L/\mathfrak{P}$. It can be checked that the value of $g(\phi_{\mathfrak{P}})$ mod $\mathfrak{P}$ is independent of the choice of $\mathfrak{P}|p$ (see [9], §4), and we write $g(\phi_p)$ mod p for this residue class in $\mathbb{Z}/p\mathbb{Z}$. We leave $g(\phi_p)$ mod p undefined for the finitely many primes that are either ramified in L or are not coprime to the denominators of g.

The following result gives equivalence of conditions (1) and (2) in the statement of Theorem 1.1.

Theorem 2.2. *An element of $\mathcal{A}$ has the form $(a_p \mod p)_p$ for some recurrent sequence (a_n) if and only if that element of $\mathcal{A}$ can be written $\big(g(\phi_p) \mod p\big)$ for some finite Galois extension $L/\mathbb{Q}$ and some $g \in A(L)$.*

Proof. ($\Longrightarrow$) Let (a_n) be a recurrent sequence. Then there exist column vectors u, v and an invertible matrix M, with entries in $\mathbb{Q}$, such that

$$a_n = u^T M^n v$$

for all $n \in \mathbb{Z}$. There is a Jordan-Chevalley decomposition

$$M = M_{ss} M_u,$$

where M_{ss} is semi-simple, M_u is unipotent, and M_{ss} commutes with M_u. For every prime p larger than the size of M_u that is coprime to all denominators appearing in M_u, the p-th power M_u^p is congruent to the identity matrix modulo p, and if in addition p is coprime to denominators appearing in u and v, then

$$a_p \equiv u^T M_{ss}^p v \mod p. \tag{2.3}$$

Let L be a finite Galois extension of $\mathbb{Q}$ over which M_{ss} diagonalizes, let $\lambda_1, \dots, \lambda_k \in L$ be the eigenvalues of M_{ss}, and write $\Gamma = \mathrm{Gal}(L/\mathbb{Q})$. Using the Jordan normal form of M_{ss}, it follows from (2.3) that there are elements $b_1, \dots, b_k \in L$ such that

$$a_p \equiv \sum_i b_i \lambda_i^p \mod p,$$

and Γ permutes the pairs b_i, λ_i, i.e. the element

$$\alpha := \sum_i b_i \otimes \lambda_i \in L \otimes_{\mathbb{Q}} L$$

is invariant under the diagonal action of Γ. There is a canonical isomorphism

$$\begin{aligned}\varphi : L \otimes_{\mathbb{Q}} L &\to \mathrm{Hom}(\Gamma, L),\\ x \otimes y &\mapsto \Big(\sigma \mapsto x\sigma(y)\Big),\end{aligned}$$

taking the Γ-invariant elements of $L \otimes L$ to $A(L)$, and we let $g = \varphi(\alpha) \in A(L)$. If p is a rational prime unramified in L coprime to every denominator of the values of g, then for every prime $\mathfrak{P}$ of L over p,

$$\begin{aligned}g(\phi_{\mathfrak{P}}) &= \sum_i b_i \phi_{\mathfrak{P}}(\lambda_i)\\ &\equiv \sum_i b_i \lambda_i^p \mod \mathfrak{P}\\ &\equiv a_p \mod \mathfrak{P}.\end{aligned}$$

Thus we have $(a_p \mod p) = (g(\phi_p) \mod p)$.

($\Longleftarrow$) Suppose $g \in A(L)$ is given, and let

$$\varphi^{-1}(g) = \sum b_i \otimes \lambda_i \in (L \otimes L)^{\Gamma},$$

where we may choose b_i, λ_i such that the pairs (b_i, λ_i) are permuted by Γ. Then the sequence

$$a_n := \sum_i b_i \lambda_i^n$$

is recurrent, and takes values in $\mathbb{Q}$ because the pairs (b_i, λ_i) are permuted by Γ. By the computation above, we see that

$$a_p \equiv g(\phi_p) \mod p$$

for all sufficiently large p. This completes the proof. $\square$

Remark 2.3. Let $L/\mathbb{Q}$ be a finite Galois extension. In the language of motives, the ring $A(L)$ defined in §2 is the ring of de Rham motivic periods of $\operatorname{Spec} L$ (see [2], §1.2, and [9], §5). There is a ring homomorphism

$$\begin{aligned}per_{\mathcal{A}} : A(L) &\to \mathcal{A},\\ g &\mapsto \big(g(\phi_p) \mod p\big)_p,\end{aligned}$$

which is an example of an $\mathcal{A}$-*valued period map* (see [10], §5).

3. Proofs of the theorems

In this section we prove Corollary 1.3, and Theorems 1.4 and 1.6.

Proof of Corollary 1.3. Suppose (a_n) is a recurrent sequence. Let $L/\mathbb{Q}$ and $g \in A(L)$ be as in the statement of Theorem 2.2. Then for all primes p unramified in L coprime to the numerators and denominators of all non-zero values of L and all $\mathfrak{P}|p$, we have

$$a_p \equiv 0 \mod p \Leftrightarrow g(\phi_{\mathfrak{P}}) = 0.$$

So we may take $C = \{\sigma \in \mathrm{Gal}(L/\mathbb{Q}) : g(\sigma) = 0\}$, which is a union of conjugacy classes by (2.1).

Conversely, suppose $L/\mathbb{Q}$ and $C \subset \mathrm{Gal}(L/\mathbb{Q})$ are given. Let $g \in A(L)$ be the characteristic function of C, and let a_n be a recurrent sequence such that

$$a_p \equiv g(\phi_p) \mod p$$

for all but finitely many p (which exists by Theorem 2.2). Then $\{p : a_p \equiv 0 \mod p\}$ coincides with $\{p : \phi_p \subset C\}$ up to a finite set. We can multiply the sequence (a_n) through by a constant rational number to modify $\{p : a_p \equiv 0 \mod p\}$ by any finite set. This completes the proof. □

Proof of Theorem 1.4. Suppose $(a_p)_p \in \mathcal{P}^0_{\mathcal{A}}$ is given. By Theorem 2.2, we can find $L/\mathbb{Q}$ and $g \in A(L)$ such that $a_p \equiv g(\phi_p) \mod p$ for all sufficiently large p. Since $A(L)$ is a finite-dimensional $\mathbb{Q}$-algebra, there is a non-zero $f(x) \in \mathbb{Q}[x]$ such that $f(g) = 0$, which implies

$$f(a_p) \equiv f(g(\phi_p)) \equiv 0 \mod p \tag{3.1}$$

for all sufficiently large p. We can scale $f(x)$ by a rational constant to make (3.1) hold for all p.

Now suppose we are given $f(x) \in \mathbb{Q}[x]$ with $f(a_p) \equiv 0 \bmod p$ for all p. There are infinitely many primes p that split completely in L, and for all but finitely many of these p, we have

$$f(a_p) \equiv f(g(1)) \equiv 0 \mod p, \tag{3.2}$$

where $1 \in \mathrm{Gal}(L/\mathbb{Q})$ is the identity element. Since (3.2) holds for arbitrarily large p, it follows that $f(g(1)) = 0$. Finally, (2.1) implies that $g(1) \in \mathbb{Q}$, so we conclude $f(x)$ has a rational root. □

Before proving Theorem 1.6, we need some preliminary results. Suppose $f(x) \in \mathbb{Q}[x]$ is monic, let $L/\mathbb{Q}$ be a finite Galois extension over which $f(x)$ splits into linear factors, and define $\Gamma := \mathrm{Gal}(L/\mathbb{Q})$. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in L, and for $1 \leq i \leq n$ set $\Gamma_i = \mathrm{Gal}(L/\mathbb{Q}(\alpha_i)) \subset \Gamma$.

Lemma 3.1. *Let p be a rational prime unramified in L that is coprime to the denominators of coefficients of f. Then $f(x)$ has a root modulo p if and only if the Frobenius conjugacy class $\phi_p \subset \Gamma$ is contained in*

$$S_1 := \bigcup_i \Gamma_i.$$

Proof. There is a root of $f(x)$ in $\mathbb{Z}/p\mathbb{Z}$ if and only if for some (equivalently, every) prime $\mathfrak{P}$ of L over p, there is some i for which $\alpha_i \mod \mathfrak{P}$ is in $\mathbb{Z}/p\mathbb{Z} \subset \mathcal{O}_L/\mathfrak{P}$. Now, $\alpha_i \mod \mathfrak{P}$ is in $\mathbb{Z}/p\mathbb{Z}$ if and only if $\phi_{\mathfrak{P}}(\alpha_i) = \alpha_i$, which happens if and only if $\phi_{\mathfrak{P}} \in \Gamma_i$. So f has a root in $\mathbb{Z}/p\mathbb{Z}$ if and only if there exists $\mathfrak{P}|p$ with $\phi_{\mathfrak{P}} \in \bigcup \Gamma_i$. Since $\bigcup \Gamma_i$ is closed under conjugation, this is equivalent to the condition that $\phi_p \subset \bigcup \Gamma_i$. $\square$

We also need the following fact.

Lemma 3.2. *Define a set*

$$S_2 := \bigcup_i \{\sigma \in \Gamma : C_\Gamma(\sigma) \subset \Gamma_i\},$$

where $C_\Gamma(\sigma)$ is the centralizer of σ inside Γ. The for every $g \in A(L)$, we have

$$\{\sigma \in \Gamma : f(g(\sigma)) = 0\} \subseteq S_2, \tag{3.3}$$

and there exists $g \in A(L)$ for which (3.3) is an equality of sets.

Proof. If $f(g(\sigma)) = 0$, then $g(\sigma) = \alpha_i$ for some i. By (2.1), $g(\sigma)$ is fixed by $C_\Gamma(\sigma)$, so we must have $C_\Gamma(\sigma) \subset \mathrm{Gal}(L/\mathbb{Q}(\alpha_i)) = H_i$. This proves the containment (3.3). To show that we can choose $g \in A(L)$ for which (3.3) is equality, let $\sigma_1, \ldots, \sigma_k \in \Gamma$ be a system of conjugacy class representatives. For $1 \leq j \leq k$, if there does not exist i for which $C_\Gamma(\sigma_j) \subset H_i$, then define g to be 0 on the conjugacy class of σ_j. If there does exist i, the define g on the conjugacy class of σ_j by

$$g(\tau\sigma_j\tau^{-1}) = \tau(\alpha_i).$$

We have $g \in A(L)$ and $\{\sigma : f(g(\sigma)) = 0\} = S_2$. $\square$

We also need a group-theoretic fact about wreath products.

Lemma 3.3. *Let Γ and A be finite groups, with A abelian, and consider the wreath product*

$$\Gamma' := A^\Gamma \rtimes \Gamma.$$

Let $\pi : \Gamma' \to \Gamma$ be the projection. Then at least

$$\left(1 - \frac{|\Gamma|^2}{|A|}\right) |\Gamma'|$$

elements $\xi \in \Gamma'$ satisfy

$$\pi\big(C_{\Gamma'}(\xi)\big) \subset \langle \pi(\xi) \rangle. \tag{3.4}$$

Proof. We identify elements of Γ' with pairs (φ, σ), where $\varphi : \Gamma \to A$ and $\sigma \in \Gamma$. Under this identification, multiplication in Γ' is given by

$$(\varphi, \sigma) \circ (\psi, \tau) = \big(\varphi + \psi \circ R_\sigma, \sigma\tau\big)$$

(here $R_\sigma : \Gamma \to \Gamma$ is right multiplication by σ). A direct computation shows that (φ, σ), $(\psi, \tau) \in \Gamma'$ commute if and only if σ and τ commute and

$$\varphi - \varphi \circ R_\tau = \psi - \psi \circ R_\sigma. \tag{3.5}$$

For $\eta : \Gamma \to A$, there exists $\psi : \Gamma \to A$ with $\eta = \psi - \psi \circ R_\sigma$ if and only if

$$\sum_{n=0}^{ord(\sigma)-1} \eta \circ R_{\sigma^n} = 0. \tag{3.6}$$

Combining (3.5) and (3.6), we see that, if φ, σ, and τ are fixed, then there exists ψ such that (φ, g) and (ψ, h) commute if and only if

$$\sum_{n=0}^{ord(\sigma)-1} \big(\varphi \circ R_{\sigma^n\tau} - \varphi \circ R_{\sigma^n}\big) = 0. \tag{3.7}$$

For each σ, $\tau \in \Gamma$, define a group homomorphism

$$\begin{aligned} \chi_{\sigma,\tau} &: A^\Gamma \to A, \\ \varphi &\mapsto \sum_{n=0}^{ord(\sigma)-1} \big(\varphi(\sigma^n\tau) - \varphi(\sigma^n)\big). \end{aligned}$$

If $\tau \notin \langle \sigma \rangle$, then the elements σ^n and $\sigma^n\tau$ are all distinct. In this case $\chi_{\sigma,\tau}$ is seen to be surjective, and the kernel of $\chi_{\sigma,\tau}$ has index $|A|$ in A^Γ. It follows from (3.7) that, for fixed τ, σ with $\tau \notin \langle \sigma \rangle$, there are at most $|A|^{|\Gamma|-1}$ functions $\varphi : \Gamma \to A$ for which $\tau \in \pi(C_{\Gamma'}((\sigma, \varphi))$. Taking the union over all σ, $\tau \in \Gamma$ with $\tau \notin \langle \sigma \rangle$, we find that the number of elements $\xi \in \Gamma'$ for which (3.4) does *not* hold is at most

$$|\Gamma|^2|A|^{|\Gamma|-1}.$$

This completes the proof. □

We are now ready to prove Theorem 1.6.

Proof of Theorem 1.6. Suppose $f(x) \in \mathbb{Q}[x]$. It is obvious that

$$\delta\Big(\{p : f(a_p) \equiv 0 \bmod p\}\Big) \leq \delta\Big(\{p : f \text{ has a root mod } p\}\Big) \tag{3.8}$$

for all $(a_p)_p \in \mathcal{P}^0_{\mathcal{A}}$. We need to show that the inequality (3.8) is strict if $f(x)$ has no rational roots, and that we can choose $(a_p)_p \in \mathcal{P}^0_{\mathcal{A}}$ to make (3.8) arbitrarily close to an equality.

Suppose $f(x)$ has no rational roots. For $(a_p)_p \in \mathcal{P}^0_{\mathcal{A}}$, let $L/\mathbb{Q}$ and $g \in A(L)$ be such that $a_p \equiv g(\phi_p) \mod p$, and let $\Gamma \supset S_1 \supset S_2$ be as in the statements of Lemmas 3.1 and 3.2. By the Chebotarev density theorem,

$$\delta\left(\{p : f \text{ has a root modulo } p\}\right) = \frac{\#S_1}{\#\Gamma},$$

$$\max_{g \in A(L)} \delta\left(\{p : f(g(\phi_p)) \equiv 0 \mod p\}\right) = \frac{\#S_2}{\#\Gamma}.$$

We get strictness of (3.8) because the identity element of Γ is in S_1 but not in S_2.

To show that (3.8) is sharp, we pass from L to an extension L'/L with the property that in $\mathrm{Gal}(L'/\mathbb{Q})$, most elements have small centralizers (in a sense to be made precise). For $L'/\mathbb{Q}$ a finite Galois extension containing L, write $\Gamma' = \mathrm{Gal}(L'/\mathbb{Q})$ and $\pi : \Gamma' \twoheadrightarrow \Gamma$ for the restriction map. Let

$$\Gamma'_i = \pi^{-1}(\Gamma_i) = \mathrm{Gal}(L'/\mathbb{Q}(\alpha_i)) \subset \Gamma',$$

for $i = 1, \ldots, n$. If an element $\sigma \in \Gamma'_i$ satisfies

$$\pi\big(C_{\Gamma'}(\sigma)\big) \subset \langle \pi(\sigma) \rangle, \tag{3.9}$$

then $C_{\Gamma'}(\sigma) \subset \Gamma'_i$. We will show that for every $\epsilon > 0$, we can choose the L'/L so that (3.9) holds for at least $(1-\epsilon)|\Gamma'|$ elements σ of Γ'. This will prove the theorem.

Let $\epsilon > 0$ be given, and choose a positive integer r such that

$$\frac{|\Gamma|^2}{2^r} < \epsilon.$$

Let $p_1, \ldots, p_r$ be distinct rational primes that split completely in the Hilbert class field of L. For each i, let $\beta_i \in \mathcal{O}_L$ be a generator for a (necessarily degree 1 and principal) prime of L over p_i. Let L' be the extension of L obtained by adjoining a square root of $\sigma(\beta_i)$ for all $\sigma \in \Gamma$ and $1 \leq i \leq r$. Then Γ' is isomorphic to a wreath product

$$\Gamma' \cong A^\Gamma \rtimes \Gamma,$$

with $A = (\mathbb{Z}/2)^r$. The result now follows from Lemma 3.3. $\square$

4. Periods

In this section we prove the equivalence of conditions (1) and (3) of Theorem 1.1. We also explain why $\mathcal{P}^0_{\mathcal{A}}$ is analogous to $\overline{\mathbb{Q}}$, and we explain how to obtain other analogues of periods inside $\mathcal{A}$.

4.1. Dimension 0

Let $L/\mathbb{Q}$ be a finite Galois extension, with ring of integers $\mathcal{O}_L$. There is an isomorphism of $\mathcal{A}$-algebras

$$L \otimes_{\mathbb{Q}} \mathcal{A} \cong \frac{\prod_p \mathcal{O}_L/p\mathcal{O}_L}{\bigoplus_p \mathcal{O}_L/p\mathcal{O}_L}.$$

For each rational prime p, the p-th power map is a $\mathbb{Z}/p\mathbb{Z}$-algebra endomorphism $F_{p,L}$ of $\mathcal{O}_L/p\mathcal{O}_L$, which is an automorphism if p is unramified in L.

Definition 4.1. The $\mathcal{A}$*-valued Frobenius automorphism* is the $\mathcal{A}$-algebra automorphism $F_{\mathcal{A},L}$ of $L \otimes_{\mathbb{Q}} \mathcal{A}$ induced by $F_{p,L}$ in the p-th factor.

If we choose a basis for L as a $\mathbb{Q}$-vector space, we can represent $F_{\mathcal{A},L}$ by a square matrix with entries in $\mathcal{A}$, and the $\mathbb{Q}$-span of the matrix entries does not depend on the choice of basis.

Theorem 4.2. *For each finite Galois extension $L/\mathbb{Q}$, the $\mathbb{Q}$-span of the matrix entries for $F_{\mathcal{A},L}$ is equal to the set of elements $(g(\phi_p) \mod p)_p \in \mathcal{A}$ for $g \in A(L)$.*

Proof. The $\mathbb{Q}$-span of matrix coefficients for $F_{\mathcal{A},L}$ is the image of the map

$$\begin{aligned} L^\vee \otimes_{\mathbb{Q}} L &\to \mathcal{A}, \\ \varphi \otimes y &\mapsto \big(\varphi(y^p) \mod p\big)_p. \end{aligned} \tag{4.1}$$

Here $L^\vee$ is the $\mathbb{Q}$-linear dual of L. The trace form induces an isomorphism of L with $L^\vee$, so the image of (4.1) is equal to the image of

$$\begin{aligned}
&L \otimes L \to \mathcal{A}, \\
&x \otimes y \mapsto \left(\left(\sum_{\sigma \in \Gamma} \sigma(xy^p) \right) \mod p \right)_p,
\end{aligned}$$

where $\Gamma = \mathrm{Gal}(L/\mathbb{Q})$.

It follows from the proof of Theorem 2.2 that $\{(g(\phi_p) \mod p)_p\}$ is equal to the image of the map

$$\begin{aligned}
&(L \otimes L)^\Gamma \to \mathcal{A}, \\
\sum_i x_i \otimes y_i \mapsto &\left(\left(\sum_i x_i y_i^p \right) \mod \mathfrak{P} \right)_p,
\end{aligned}$$

where for each p we have chosen a prime $\mathfrak{P}$ of L over p. The result now follows from the fact that

$$\begin{aligned}
&L \otimes L \to (L \otimes L)^\Gamma, \\
&x \otimes y \mapsto \sum_\sigma \sigma(x) \otimes \sigma(y)
\end{aligned}$$

is surjective. □

The algebraic de Rham cohomology of $\mathrm{Spec}(L)$ (which we view as a 0-dimensional algebraic variety over $\mathbb{Q}$) is identified with L. Thus $\mathcal{P}^0_{\mathcal{A}}$ is the $\mathbb{Q}$-span of the matrix coefficients for the isomorphism

$$H^0_{dR}(\mathrm{Spec}(L)) \otimes \mathcal{A} \xrightarrow{\sim} H^0_{dR}(\mathrm{Spec}(L)) \otimes \mathcal{A},$$

for L ranging over the finite Galois extensions of $\mathbb{Q}$. If instead we look at de Rham-Betti comparison isomorphism

$$H^0_{dR}(\mathrm{Spec}(L)) \otimes \mathbb{C} \xrightarrow{\sim} H^0_{B}(\mathrm{Spec}(L)) \otimes \mathbb{C}$$

for varying L, the $\mathbb{Q}$-span of the matrix coefficients is $\overline{\mathbb{Q}}$. For this reason $\mathcal{P}^0_{\mathcal{A}} \subset \mathcal{A}$ is analogous to $\overline{\mathbb{Q}} \subset \mathbb{C}$. By contrast, the integral closure of $\mathbb{Q}$ inside $\mathcal{A}$ is uncountable.

4.2. Positive dimension

The characterization of $\mathcal{P}^0_{\mathcal{A}}$ as matrix coefficients of the $\mathcal{A}$-valued Frobenius can be generalized to produce elements of $\mathcal{A}$ from varieties of positive dimension. If X is a variety defined over $\mathbb{Q}$ and $i \geq 0$ is an integer, the algebraic de Rham cohomology $H^i_{dR}(X)$ is finite-dimensional vector space over $\mathbb{Q}$, and for all sufficiently large p there is a distinguished automorphism

$$F_{p,X} : H^i_{dR}(X) \otimes \mathbb{Q}_p \xrightarrow{\sim} H^i_{dR}(X) \otimes \mathbb{Q}_p$$

coming from crystalline cohomology (see [6]). Matrix coefficients for $F_{p,X}$ with respect to a $\mathbb{Q}$-basis are (one type of) p-adic periods of X. Each matrix coefficient for $F_{p,X}$ is p-integral for all sufficiently large p, so reduction modulo p (for all large p at once) gives an element of $\mathcal{A}$. These elements are called $\mathcal{A}$-valued periods in [10]. It is convenient to assemble the maps $F_{p,X}$ to form an $\mathcal{A}$-valued Frobenius map

$$F_{\mathcal{A},X} : H^i_{dR}(X) \otimes \mathcal{A} \to H^i_{dR}(X) \otimes \mathcal{A},$$

whose matrix coefficients are $\mathcal{A}$-valued periods (the map $F_{\mathcal{A},X}$ is no longer an isomorphism). Details can be found in [10], §6.

If we instead use the de Rham-Betti comparison isomorphism

$$comp_X : H^i_{dR}(X) \otimes \mathbb{C} \xrightarrow{\sim} H^i_B(X) \otimes \mathbb{C},$$

matrix coefficients are the ordinary (complex) periods of X. So in this analogy $\mathcal{A}$ corresponds to $\mathbb{C}$, and $F_{\mathcal{A},X}$ corresponds to $comp_X$. Define $\mathcal{P}_{\mathcal{A}} \subset \mathcal{A}$ (resp. $\mathcal{P}_{\mathbb{C}} \subset \mathbb{C}$) to be the $\mathbb{Q}$-span of the matrix coefficients for $F_{\mathcal{A},X}$ (resp. $comp_X$), as X ranges through all varieties over $\mathbb{Q}$. By taking X to have dimension 0 we see that $\mathcal{P}^0_{\mathcal{A}} \subset \mathcal{P}_{\mathcal{A}}$ and $\overline{\mathbb{Q}} \subset \mathcal{P}_{\mathbb{C}}$.

The period conjecture of Grothendieck (see [1], §7.5) would imply that there is a $\mathbb{Q}$-algebra homomorphism

$$\Delta : \mathcal{P}_{\mathbb{C}} \to \mathcal{P}_{\mathbb{C}} \otimes_{\mathbb{Q}} \mathcal{P}_{\mathcal{A}}.$$

Concretely, fix a variety X and bases for $H^i_{dR}(X)$ and $H^i_{dR}(X)$, say of length n. Write $F_{\mathcal{A},X}$ and $comp_X$ as matrices $(\alpha_{i,j}) \in M_n(\mathcal{A})$ and $(\beta_{i,j}) \in M_n(\mathbb{C})$, respectively. The map Δ is then given by

$$\Delta(\beta_{i,j}) = \sum_{k=1}^{n} \beta_{i,k} \otimes \alpha_{k,j} \in \mathcal{P}_{\mathbb{C}} \otimes_{\mathbb{Q}} \mathcal{P}_{\mathcal{A}}. \tag{4.2}$$

A priori the right hand side of (4.2) might depend on X, i, and j, but the period conjecture implies that in fact the right hand side depends only on the value $\beta_{i,j} \in \mathcal{P}_{\mathbb{C}}$.

Every algebraic number occurs as a matrix coefficient for $comp_X$ for some 0-dimensional X. Since the $\mathcal{A}$-valued periods of this X are in $\mathcal{P}^0_{\mathcal{A}}$, this implies Δ takes $\overline{\mathbb{Q}} \subset \mathcal{P}_{\mathbb{C}}$ into $\mathcal{P}^0_{\mathcal{A}} \otimes_{\mathbb{Q}} \mathcal{P}_{\mathbb{C}}$. So the truth of the period conjecture would imply that if we see an algebraic number as a complex period of an arbitrary variety, we will also see elements of $\mathcal{P}^0_{\mathcal{A}}$ in the $\mathcal{A}$-valued periods of that variety.

Acknowledgments

We thank Jeffrey Lagarias for helpful comments. We thank the anonymous referee for helpful suggestions on the structure of the paper.

References

[1] Yves André, Une introduction aux motifs: motifs purs, motifs mixtes, périodes, 2004.
[2] Francis Brown, Single-Valued Motivic Periods and Multiple Zeta Values, Forum of Mathematics, Sigma, vol. 2, Cambridge University Press, 2014.
[3] David Jarossay, An explicit theory of $\pi_1^{\mathrm{un,crys}}(\mathbb{P}^1 - \{0, \mu_N, \infty\})$ – II-3: sequences of multiple harmonic sums viewed as periods, arXiv:1601.01159, 2016.
[4] Masanobu Kaneko, Finite multiple zeta values (in Japanese), RIMS Kôkyûroku Bessatsu B68 (2017) 175–190.
[5] Masanobu Kaneko, Don Zagier, Finite multiple zeta values (in preparation).
[6] Kiran S. Kedlaya, p-Adic cohomology, in: Algebraic Geometry, vol. 2, Seattle 2005: 2005 Summer Research Institute, July 25-August 12, 2005, University of Washington, Seattle, Washington, 2009, p. 667.
[7] Maxim Kontsevich, Holonomic $\mathcal{D}$-modules and positive characteristic, Jpn. J. Math. 4 (1) (2009) 1–25.
[8] Maxim Kontsevich, Don Zagier, Periods, in: Mathematics Unlimited—2001 and Beyond, Springer, 2001, pp. 771–808.
[9] Julian Rosen, A choice-free absolute Galois group and Artin motives, arXiv:1706.06573, 2017.
[10] Julian Rosen, Sequential periods of the crystalline Frobenius, arXiv:1805.01885, 2018.
[11] Kenji Sakugawa, On modified finite polylogarithms, J. Number Theory 201 (2019) 190–205.
[12] Jean-Pierre Serre, Lectures on $N_X(p)$, AK Peters/CRC Press, 2016.
[13] Jianqiang Zhao, Multiple Zeta Functions, Multiple Polylogarithms and Their Special Values, vol. 12, World Scientific, 2016.