THE SEQUENCE OF PRIME COEFFICIENTS OF AN ALGEBRAIC POWER SERIES

JULIAN ROSEN

Abstract. We describe a family of elements of $\mathcal{A}$ coming from algebraic power series. We prove a family of relations among these elements coming from algebraic change of variables.

1. Introduction

The commutative $\mathbb{Q}$-algebra $\mathcal{A}$ is defined by

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

An element of $\mathcal{A}$ is a prime-indexed sequence $(a_p)_p$, with $a_p \in \mathbb{Z}/p\mathbb{Z}$, and $(a_p)_p = (b_p)_p$ if $a_p = b_p$ for all but finitely many primes p (this is a special case of a more general construction due to Kontsevich [4], §2.2). Kaneko and Zagier introduced the *finite multiple zeta values* [3][2], which are are defined for positive integers $k_1, \dots, k_r$ by

$$\zeta_{\mathcal{A}}(k_1, \dots, k_r) := \left(\sum_{p > n_1 > \dots > n_r > 0} \frac{1}{n_1^{k_1} \cdots n_r^{k_r}} \mod p \right)_p.$$

Here, we consider a family of elements of $\mathcal{A}$ coming from formal power series. For $f(x) \in \mathbb{Q}[[x]]$, we say $f(x)$ is *algebraic* if there exist polynomials $b_0(x), \dots, b_n(x) \in \mathbb{Q}[x]$, not all 0, such that

$$\sum_{k=0}^{n} b_k(x) f(x)^k = 0. \tag{1}$$

The set of all algebraic power series is a countable $\mathbb{Q}$-subalgebra of $\mathbb{Q}[[x]]$, which we denote by $\mathbb{Q}[[x]]^{alg}$. For $f(x) \in \mathbb{Q}[[x]]$ and $n \geq 0$, we write $f(x)[x^n]$ for the coefficient of x^n in $f(x)$. If $f(x) \in \mathbb{Q}[[x]]^{alg}$, then Corollary 2.2 below implies $f(x)[x^p]$ is p-integral for every sufficiently large prime p, so it makes sense to reduce $f(x)[x^p]$ modulo p.

Definition 1.1. For $f(x) \in \mathbb{Q}[[x]]^{alg}$, we define

$$f(x)_{\mathcal{A}} := \big(f(x)[x^p] \mod p\big)_p \in \mathcal{A}.$$

It is not difficult to see that the set $\{f(x)_{\mathcal{A}} : f(x) \in \mathbb{Q}[[x]]^{alg}\} \subset \mathcal{A}$ is a countable $\mathbb{Q}$-subspace. However, since the Hadamard product (i.e. coefficient-wise product) of algebraic power series is not algebraic in general, the set of elements $f(x)_{\mathcal{A}}$ is not closed under multiplication.

The main result of this short paper is gives an equality $f_1(x)_{\mathcal{A}} = f_2(x)_{\mathcal{A}}$, coming from algebraic change of variables.

Theorem. *If $f(x)$, $g(x) \in \mathbb{Q}[[x]]^{alg}$ satisfy $f(0) = g(0) = 0$ and $g'(0) \neq 0$, then*

$$\left(xf(g(x)) \frac{g'(x)}{g(x)} \right)_{\mathcal{A}} = g'(0) f(x)_{\mathcal{A}}.$$

This is proved as Theorem 3.2 below. As an application, we give a short proof of a congruence for binomial coefficients.

Remark 1.2. If $f(x) \in \mathbb{Q}[[x]]$ is the (power series expansion of) a rational function, then the sequence of coefficients satisfies a linear recurrence relation. Since the product of two such sequences again satisfies a recurrence relation, the space of elements of $\mathcal{A}$ obtained from rational functions is a subalgebra. A complete description of the algebraic structure of this subalgebra is given in [5].

2. Preliminaries

In this section, we collect some general results about algebraic power series. Our first result is that only finitely many primes divide the denominators of the terms in an algebraic series.

Proposition 2.1. *Suppose $f(x) \in \mathbb{Q}[[x]]^{alg}$. Then there exists an integer $N \geq 1$ such that $f(x)[x^n] \in \mathbb{Z}[N^{-1}]$ for all $n \geq 0$.*

Proof. Let $g(T) \in \mathbb{Z}[x][T]$ be an irreducible polynomial in T, with coefficients in $\mathbb{Z}[x]$, such that $g(f(x)) = 0$ (we can obtain g from (1) by clearing denominators). For $k \in \mathbb{N}$, define $f^{[k]} := \sum_{n=0}^{k} f[x^n] x^n \in \mathbb{Q}[x]$, the truncation of f at degree k. Since $g(T)$ is irreducible, we have $g'(f) \neq 0$ (here g' is the derivative with respect to T). So for all sufficiently large k, we have $v_x(g(f^{[k]})) > 2v_x(g'(f^{[k]}))$, where v_x is the x-adic valuation on $\mathbb{Q}[[x]]$.

Define a sequence $f_1, f_2, \ldots \in \mathbb{Q}[[x]]$ by $f_1 = f^{[k]}$ and

$$f_{n+1} = f_n - \frac{g(f_n)}{g'(f_n)} \in \mathbb{Q}[x].$$

It follows from Hensel's Lemma that (f_n) is a Cauchy sequence for the x-adic topology on $\mathbb{Q}[x]$, and that $f_n \to f$ as $n \to \infty$. Let N be a positive integer divisible by the denominators of all coefficients of f_1, and also divisible by the coefficient of term of least degree appearing in $g(f_1)$. Then we see by induction that $f_1, f_2, \ldots \in \mathbb{Z}[N^{-1}][[x]]$, and therefore since $f_n \to f$, we get $f \in \mathbb{Z}[N^{-1}][[x]]$. □

As an immediate consequence, we see that $f(x)_{\mathcal{A}}$ is well-defined.

Corollary 2.2. *If $f(x) \in \mathbb{Q}[[x]]^{alg}$, then $f(x)[x^p] \in \mathbb{Z}_{(p)}$ for every sufficiently large prime p.*

Next, we show that the composition of two algebraic series, when it is defined, is algebraic. The composition of algebraic series appears in one of our relations in §3.

Proposition 2.3. *Suppose that* $f(x),\ g(x) \in \mathbb{Q}[[x]]^{alg}$. *If* $g(0) = 0$, *then* $f(g(x)) \in \mathbb{Q}[[x]]^{alg}$.

Proof. Because $f(x)$ is algebraic over $\mathbb{Q}(x)$, we know $f(g(x))$ is algebraic over $\mathbb{Q}(g(x))$. Additionally, since $g(x) \in \mathbb{Q}[[x]]^{alg}$, we know $\mathbb{Q}(g(x))$ is an algebraic extension of $\mathbb{Q}(x)$. The result now follows from the fact that the composition of algebraic extensions is algebraic. □

Finally, we show that extracting the terms in an arithmetic progression from an algebraic power series yields another algebraic series.

Proposition 2.4. *Suppose* $\sum_{n\geq 0} a_n x^n \in \mathbb{Q}[[x]]^{alg}$. *Then for every* $m, r \in \mathbb{Z}$, $m > 0$, *the series* $\sum_{n\geq 0} a_{mn+r} x^n$ *is in* $\mathbb{Q}[[x]]^{alg}$ *(by convention, we set* $a_n = 0$ *for* $n < 0$*).*

Proof. Write $f(x) = \sum_{n\geq 0} a_n x^n \in \mathbb{Q}[[x]]^{alg}$, and define $f_{m,r}(x) := \sum_{n\geq 0} a_{mn+r} x^n$. One sees directly that

$$f_{m,r}(x) = \sum_{j=0}^{m-1} \zeta_m^{jr} f(\zeta_m^j x^{1/m}) \in \mathbb{Q}(\zeta_m)((x^{1/m})),$$

where ζ_m is a primitive m-th root of unity. For $0 \leq j \leq m-1$, we see $f(\zeta_m^j x^{1/m})$ is algebraic over $\mathbb{Q}(\zeta_m, x^{1/m})$, so we conclude $f_{m,r}(x)$ is algebraic over $\mathbb{Q}(\zeta_m, x^{1/m})$. Finally, $\mathbb{Q}(\zeta_m, x^{1/m})$ is an algebraic extension of $\mathbb{Q}(x)$, and the result follows from the fact that the composition of algebraic extensions is algebraic. □

Corollary 2.5. *Suppose* $f(x) \in \mathbb{Q}[[x]]^{alg}$, $m, r \in \mathbb{Z}$, $m > 0$. *Then there exists* $g(x) \in \mathbb{Q}[[x]]^{alg}$ *such that*

$$\big(f(x)[x^{mp+r}] \mod p\big)_p = g(x)_{\mathcal{A}}.$$

3. Relations

In this section, we prove some equalities among elements $f(x)_{\mathcal{A}}$. The following proposition gives two easy equalities.

Proposition 3.1. *(1) If* $f(x) \in \mathbb{Q}[x]$, *then* $f(x)_{\mathcal{A}} = 0$.
(2) If $f(x) \in \mathbb{Q}[[x]]^{alg}$, *then* $\big(xf'(x)\big)_{\mathcal{A}} = 0$.

Proof. For statement (1), if $f(x) \in \mathbb{Q}[x]$, then $f[x^p] = 0$ for all sufficiently large p. For statement (2), if $f(x) \in \mathbb{Q}[[x]]^{alg}$, then

$$\big(xf'(x)\big)[x^p] = p \cdot f(x)[x^p] \equiv 0 \mod p.$$

□

Our next equality comes from change of variables.

Theorem 3.2. *Suppose* $f(x),\ g(x) \in \mathbb{Q}[[x]]^{alg}$ *satisfy* $f(0) = g(0) = 0$ *and* $g'(0) \neq 0$. *Then*

$$\left(xf(g(x))\frac{g'(x)}{g(x)}\right)_{\mathcal{A}} = g'(0) f(x)_{\mathcal{A}}. \tag{2}$$

Proof. As $f(x)$ and $g(x)$ are algebraic, we can find a smooth projective curve X defined over $\mathbb{Q}$, a rational points $x \in X(\mathbb{Q})$, and a local parameter $t_1 \in \mathcal{O}_{X,x}$ such that $f(t_1)$, $g(t_1)$, and $f(g(t_1))$ are rational functions on X. Define $t_2 = g(t_1)$, which is another local parameter at x. We consider the 1-form

$$\omega := f(t_2)\,\frac{dt_2}{t_2} = t_1 f(g(t_1))\frac{g'(t_1)}{g(t_1)}\frac{dt_1}{t_1} \in \Omega^1_{X,x}.$$

Define sequence a_n, $b_n \in \mathbb{Q}$ by

$$a_n = \left(xf(g(x))\frac{g'(x)}{g(x)}\right)[x^n], \qquad b_n = f(x)[x^n]. \tag{3}$$

Then the rational 1-form ω_f can be expanded as a series in t_1, and as a series in t_2:

$$\omega = \sum_{n\geq 1} a_n t_1^n \frac{dt_1}{t_1} = \sum_{n\geq 1} b_n t_2^n \frac{dt_2}{t_2}.$$

For all sufficiently large p, we write ω_p for the reduction of ω modulo p, which is a rational 1-form on the reduction of X modulo p. We will derive (2) by applying the Cartier operator C_p to ω_p. It follows from [1], Lemma 1.3.6, that $C_p(\omega_p)$ has an expression in local coordinates

$$C_p(\omega_p) \equiv \sum_{n\geq 1} a_{pn} t_1^n \frac{dt_1}{t_1} \equiv \sum_{n\geq 1} b_{pn} t_2^n \frac{dt_2}{t_2} \mod p. \tag{4}$$

Now we use $t_2 = g(t_1)$ to express the right hand side of (4) as a power series in t_1, and we extract the coefficient of dt_1 from both sides of (4) to obtain

$$a_p \equiv g'(0) b_p \mod p.$$

Combining this with (3) completes the proof of the theorem. □

4. A binomial coefficient congruence

We use Theorem 3.2 to prove the following congruence for binomial coefficients.

Proposition 4.1. *Let m be a positive integer. Then for every sufficiently large prime p congruent to 1 modulo $2m$, we have*

$$\binom{(p-1)/m}{(p-1)/(2m)} \equiv (-4)^{(p-1)/(2m)} \binom{(p-1)/2}{(p-1)/(2m)} \mod p.$$

Proof. Define $f_1(x)$, $f_2(x) \in \mathbb{Q}[[x]]^{alg}$ by

$$f_1(x) = \frac{x}{\sqrt{1-4x^{2m}}},$$
$$f_2(x) = \frac{x}{\sqrt[m]{1+x^{2m}}}.$$

Then, for $p \equiv 1 \mod 2m$, we have

$$\begin{aligned} f_1(x)[x^p] &= (-4)^{(p-1)/(2m)} \binom{-1/2}{(p-1)/(2m)} \\ &\equiv (-4)^{(p-1)/(2m)} \binom{(p-1)/2}{(p-1)/(2m)} \mod p, \\ f_2(x)[x^p] &= \binom{-1/m}{(p-1)/(2m)} \equiv \binom{(p-1)/m}{(p-1)/(2m)} \mod p, \end{aligned}$$

and for $p \not\equiv 1 \mod 2m$, we have $f_1(x)[x^p] = f_2(x)[x^p] = 0$. So the proposition is equivalent to the equality $f_1(x)_{\mathcal{A}} = f_2(x)_{\mathcal{A}}$.

Define $g(x) = f_2(x)$. Then we compute

$$\begin{aligned} x f_1(g(x)) \frac{g'(x)}{g(x)} &= x \frac{\frac{x}{\sqrt[m]{1+x^{2m}}}}{\sqrt{1 - 4\frac{x^{2m}}{(1+x^{2m})^2}}} \left(\frac{1}{x} - \frac{2x^{2m-1}}{1+x^{2m}} \right) \\ &= x \frac{1+x^{2m}}{1-x^{2m}} \frac{1}{\sqrt[m]{1+x^{2m}}} \frac{1-x^{2m}}{1+x^{2m}}, \\ &= \frac{x}{\sqrt[m]{1+x^{2m}}} = f_2(x). \end{aligned}$$

Since $g'(0) = 1$, the equality $f_1(x)_{\mathcal{A}} = f_2(x)_{\mathcal{A}}$ now follows from Theorem 3.2. □

References

[1] Michel Brion and Shrawan Kumar. *Frobenius splitting methods in geometry and representation theory*, volume 231. Springer Science & Business Media, 2007.

[2] Masanobu Kaneko. Finite multiple zeta values (in Japanese). *RIMS Kkyroku Bessatsu B68 (to appear)*.

[3] Masanobu Kaneko and Don Zagier. Finite multiple zeta values. *in preparation*.

[4] Maxim Kontsevich. Holonomic $\mathcal{D}$-modules and positive characteristic. *Japanese Journal of Mathematics*, 4(1):1–25, 2009.

[5] Julian Rosen. A finite analogue of the ring of algebraic numbers. *Journal of Number Theory*, 208:59–71, 2020.

Department of Mathematics & Statistics, University of Maine, Orono, ME 04469-5752

Email address: julianrosen@gmail.com