Algebra & Number Theory

Volume 4
2010
No. 7

On exponentials of exponential generating series

Roland Bacher

mathematical sciences publishers

ALGEBRA AND NUMBER THEORY 4:7(2010)

msp

On exponentials of exponential generating series

Roland Bacher

After identification of the algebra of exponential generating series with the shuffle algebra of ordinary formal power series, the exponential map

$$\exp_{!} : X\mathbb{K}[[X]] \longrightarrow 1 + X\mathbb{K}[[X]]$$

for the associated Lie group with multiplication given by the shuffle product is well-defined over an arbitrary field $\mathbb{K}$ by a result going back to Hurwitz. The main result of this paper states that $\exp_{!}$ and its reciprocal map $\log_{!}$ induce a group isomorphism between the subgroup of rational, respectively algebraic series of the additive group $X\mathbb{K}[[X]]$ and the subgroup of rational, respectively algebraic series in the group $1 + X\mathbb{K}[[X]]$ endowed with the shuffle product, if the field $\mathbb{K}$ is a subfield of the algebraically closed field $\overline{\mathbb{F}}_p$ of characteristic p.

1. Introduction

The equality

$$\left(\sum_{n=0}^{\infty} \alpha_n \frac{X^n}{n!}\right)\left(\sum_{n=0}^{\infty} \beta_n \frac{X^n}{n!}\right) = \sum_{n=0}^{\infty}\sum_{m=0}^{n} \binom{n+m}{n} \alpha_n \beta_m \frac{X^{n+m}}{(n+m)!} \tag{1}$$

shows that we can define an algebra structure on the vector space

$$\mathscr{E}(\mathbb{K}) = \left\{ \sum_{n=0}^{\infty} \alpha_n \frac{X^n}{n!} \,\middle|\, \alpha_0, \alpha_1, \ldots \in \mathbb{K} \right\}$$

of formal exponential generating series with coefficients $\alpha_0, \alpha_1, \ldots$ in an arbitrary field or ring $\mathbb{K}$. For the sake of simplicity, we will work only over fields. The expression $\alpha_n/n!$ should be considered formally, since the numerical value of $n!$ is zero over a field of positive characteristic $p \leq n$.

MSC2000: primary 11B85; secondary 11B73, 11E08, 11E76, 22E65.

Keywords: Bell numbers, exponential function, shuffle product, formal power series, divided powers, rational series, algebraic series, homogeneous form, automaton sequence.

Motivation for this work is given by the fact that the formula (1) allows us to define the shuffle product

$$\sum_{n=0}^{\infty} \gamma_n X^n = \left(\sum_{n=0}^{\infty} \alpha_n X^n \right) \sqcup\!\sqcup \left(\sum_{n=0}^{\infty} \beta_n X^n \right)$$

of two formal power series $\sum_{n=0}^{\infty} \alpha_n X^n$ and $\sum_{n=0}^{\infty} \beta_n X^n$ by setting

$$\gamma_n = \sum_{k=0}^{n} \binom{n}{k} \alpha_k \beta_{n-k}. \tag{2}$$

The definition of the shuffle product arises in the theory of divided powers; see, for example, [Berthelot and Ogus 1978, Definition 3.1]. The main properties needed in this paper are already in [Hurwitz 1899]. I have the impression that the main results of the present paper, given by Theorems 1.1 and 1.3, do not fit very well into the theory of divided powers: they are based on an interplay between ordinary power series (used for defining rationality and algebraicity) and exponential power series (used for defining an analogue of the exponential map in positive characteristic). A special instance of this exponential map is a standard ingredient for divided powers [Berthelot and Ogus 1978, Appendix A, Proposition A1], but ordinary formal power series do not seem to play a significant role there.

Definition (2) is also a particular case of a shuffle product defined more generally for formal power series in several noncommuting variables. The associated shuffle algebras arise, for example, in the study of free Lie algebras [Reutenauer 1993], Hopf algebras and polyzetas [Zagier 1994; Cartier 2002], formal languages [Berstel and Reutenauer 1988], etc.

I became interested in this subject through the study of the properties of the algebra of recurrence matrices, a subset of sequences of matrices displaying a kind of self-similarity structure used in [Bacher 2006; 2008] for studying reductions of the Pascal triangle modulo suitable Dirichlet characters. Such recurrence matrices are closely related to automata groups and complex dynamical systems; see, for example, [Nekrashevych 2005] for details. Over a finite field, they can be identified with rational formal power series in several noncommuting variables (the underlying algebras are however very different) and it is thus natural to investigate properties of other possible products preserving these sets. The main results of this paper, Theorems 1.1 and 1.3 (and their effective analogues, Theorems 1.5 and 1.6), deal with properties of the shuffle product for formal power series in one variable that have gone unnoticed in the existing literature, as far as I am aware.

We denote by

$$\mathfrak{m}_{\mathscr{E}} = \left\{ \sum_{n=1}^{\infty} \alpha_n \frac{X^n}{n!} \,\middle|\, \alpha_1, \alpha_2, \dots \in \mathbb{K} \right\} \subset \mathscr{E}(\mathbb{K})$$

the maximal ideal of the local algebra $\mathscr{C}(\mathbb{K})$. A straightforward computation, already known to Hurwitz [1899], shows that $a^n/n!$ is always well-defined for $a \in \mathfrak{m}_{\mathscr{C}}$. Endowing $\mathbb{K}$ with the discrete topology and $\mathscr{C}(\mathbb{K})$ with the topology given by coefficientwise convergence, the functions

$$\exp(a) = \sum_{n=0}^{\infty} \frac{a^n}{n!} \quad \text{and} \quad \log(1+a) = -\sum_{n=1}^{\infty} \frac{(-a)^n}{n}$$

are always defined for $a \in \mathfrak{m}_{\mathscr{C}}$.

Switching back to ordinary generating series

$$A = \sum_{n=1}^{\infty} \alpha_n X^n, \quad B = \sum_{n=1}^{\infty} \beta_n X^n \in \mathfrak{m},$$

contained in the maximal ideal $\mathfrak{m} = X\mathbb{K}[[X]]$, of (ordinary) formal power series, we write

$$\exp_! A = 1 + B$$

if

$$\exp\left(\sum_{n=1}^{\infty} \alpha_n \frac{X^n}{n!}\right) = 1 + \sum_{n=1}^{\infty} \beta_n \frac{X^n}{n!}.$$

It is easy to see that $\exp_!$ defines a one-to-one map between $\mathfrak{m}$ and $1+\mathfrak{m}$ with reciprocal map

$$1 + B \mapsto A = \log_!(1+B).$$

It satisfies

$$\exp_!(A+B) = \exp_! A \sqcup\!\sqcup \exp_! B$$

for all $A, B \in \mathfrak{m}$, where the shuffle product

$$\left(\sum_{n=0}^{\infty} \alpha_n X^n\right) \sqcup\!\sqcup \left(\sum_{n=0}^{\infty} \beta_n X^n\right) = \sum_{n,m=0}^{\infty} \binom{n+m}{n} \alpha_n \beta_m X^{n+m}$$

corresponds to the ordinary product of the associated exponential generating series. The map $\exp_!$ defines thus an isomorphism between the additive group $(\mathfrak{m}, +)$ and the *special shuffle group* $(1+\mathfrak{m}, \sqcup\!\sqcup)$ with group-law given by the shuffle product. It coincides with the familiar exponential map from the Lie algebra $\mathfrak{m}$ into the special shuffle group, considered as an infinite-dimensional Lie group.

It follows from [Fliess 1974] that rational, respectively algebraic elements form a subgroup in $(1+\mathfrak{m}, \sqcup\!\sqcup)$ if one works over a subfield of $\overline{\mathbb{F}}_p$. It is thus natural to consider the corresponding subgroups (under the reciprocal map $\log_!$ of the Lie exponential $\exp_! : \mathfrak{m} \mapsto 1+\mathfrak{m}$) in the isomorphic additive group $(\mathfrak{m}, +)$ forming the Lie algebra of $(1+\mathfrak{m}, \sqcup\!\sqcup)$. The answer, which is the main result of this paper,

is surprisingly simple: the corresponding subgroup is exactly the subgroup of all rational, respectively algebraic elements in the additive group $\mathfrak{m}$. We have thus:

Theorem 1.1. *Let $\mathbb{K}$ be a subfield of the algebraically closed field $\overline{\mathbb{F}}_p$ of positive characteristic p. Given a series $A \in \mathfrak{m} = X\mathbb{K}[[X]]$, the following two assertions are equivalent*:

- *A is rational.*
- *$\exp_!\, A$ is rational.*

Theorem 1.1 fails in characteristic zero: the series

$$\log_!(1-X) = -\sum_{n=1}^{\infty}(n-1)!\,X^n$$

is obviously transcendental. (This series also shows that Theorem 1.3 does not hold in characteristic zero.)

Example 1.2. The Bell numbers $B_0, B_1, B_2, \ldots$ (see [Comtet 1970, pp. 45–46] or [Stanley 1999, Example 5.2.4]) are the natural integers defined by

$$\sum_{n=0}^{\infty} B_n \frac{x^n}{n!} = e^{e^x-1},$$

and have combinatorial interpretations.

Since $e^x - 1$ is the exponential generating series of the sequence $0, 1, 1, \ldots$, we have $\sum_{n=0}^{\infty} B_n x^n = \exp_!(x/(1-x))$ for the ordinary generating series

$$\sum_{n=0}^{\infty} B_n x^n = 1 + x + 2x^2 + 5x^3 + 15x^4 + 52x^5 + 203x^6 + 877x^7 + 4140x^8 + \cdots$$

of the Bell numbers.

The reduction of $\sum_{n=0}^{\infty} B_n x^n$ modulo a prime p is thus always a rational element of $\mathbb{F}_p[[x]]$. A few such reductions are

$$\frac{1}{1+x+x^2} \pmod 2, \quad \frac{1+x+x^2}{1-x^2-x^3} \pmod 3, \quad \frac{1+x+2x^2-x^4}{1-x^4-x^5} \pmod 5.$$

Theorem 1.3. *Let $\mathbb{K}$ be a subfield of the algebraically closed field $\overline{\mathbb{F}}_p$ of positive characteristic p. Given a series $A \in \mathfrak{m} = X\mathbb{K}[[X]]$, the following two assertions are equivalent*:

- *A is algebraic.*
- *$\exp_!\, A$ is algebraic.*

Theorems 1.1 and 1.3 are the main results of this paper and can be restated as follows.

Corollary 1.4. *Over a subfield $\mathbb{K} \subset \overline{\mathbb{F}}_p$, the group isomorphism*

$$\exp_! : (\mathfrak{m}, +) \longrightarrow (1 + \mathfrak{m}, \sqcup\!\sqcup)$$

restricts to an isomorphism between the subgroups of rational elements in $(\mathfrak{m}, +)$ *and in* $(1 + \mathfrak{m}, \sqcup\!\sqcup)$.

It restricts also to an isomorphism between the subgroups of algebraic elements in $(\mathfrak{m}, +)$ *and in* $(1 + \mathfrak{m}, \sqcup\!\sqcup)$.

In particular, the subgroup of rational, respectively algebraic elements in the shuffle group $(1 + \mathfrak{m}, \sqcup\!\sqcup)$ *is a Lie-group whose Lie algebra (over* $\mathbb{K} \subset \overline{\mathbb{F}}_p$*) is given by the additive subgroup of all rational, respectively algebraic elements in* $(\mathfrak{m}, +)$.

Theorems 1.1 and 1.3 can be made more precise as follows.

Given a rational series $A \in \mathbb{K}[[X]]$ represented by a reduced fraction f/g, where f, g with $g \neq 0$ are two coprime polynomials of degrees $\deg f$ and $\deg g$, we set $\|A\| = \max(1 + \deg f, \deg g)$; see also Proposition 2.1 for a well-known equivalent description of $\|A\|$.

Theorem 1.5. *We have*

$$\|\exp_! A\| \leq p^{q^{\|A\|}} \quad \textit{and} \quad \|\log_!(1+A)\| \leq 1 + \|1+A\|^p$$

for a rational series A in $\mathfrak{m} \subset \overline{\mathbb{F}}_p[[X]]$ having all its coefficients in a finite subfield $\mathbb{F}_q \subset \overline{\mathbb{F}}_p$ containing $q = p^e$ elements.

The bounds for $\log_!$ (and the analogous bounds in the algebraic case) can be improved; see Proposition 7.1.

Theorem 1.5 could be called an effective version of Theorem 1.1: given a rational series represented by $f/g \in \mathfrak{m}$ with $f, g \in \overline{\mathbb{F}}_p[X]$, Theorem 1.1 ensures the existence of polynomials u, v such that $\exp_!(f/g) = u/v$. Theorem 1.5 shows that u and v are of degree at most $p^{q^{\|f/g\|}}$. They can thus be recovered as suitable Padé approximants from the series development of $\exp_!(f/g)$ up to order $2p^{q^{\|f/g\|}}$. Experimentally, the number $\|\exp_! A\|$ is generally much smaller.

Since the bounds for $\log_!$ are better than for $\exp_!$, the determination of the rational series $B = \exp_! A$ with $A \in \mathfrak{m}$ rational is best done as follows: start by "guessing" the rational series B and check (or improve the guess for B in case of failure) that $A = \log_!(B)$ using the bounds for $\log_!$.

Given a prime p and a formal power series $C = \sum_{n=0}^{\infty} \gamma_n X^n$ in $\mathbb{K}[[X]]$ with coefficients in a subfield $\mathbb{K}$ of $\overline{\mathbb{F}}_p$, we define for $f \in \mathbb{N}$, $k \in \mathbb{N}$, $k < p^f$ the series

$$C_{k,f} = \sum_{n=0}^{\infty} \gamma_{k+np^f} X^n.$$

The vector space $\mathcal{H}(C) = \mathbb{K}C + \sum_{k,f} \mathbb{K}C_{k,f}$ spanned by C and by all series of the form $C_{k,f}$, $k \in \{0, \dots, p^f - 1\}$, $f \in \{1, 2, \dots\}$ is called the *p-kernel* of C. We denote its dimension by $\kappa(C) = \dim \mathcal{H}(C)$.

Algebraic series in $\mathbb{K}[[X]]$ for $\mathbb{K}$ a subfield of $\overline{\mathbb{F}}_p$ are characterized by a theorem of Christol [Allouche and Shallit 2003, Theorem 12.2.5] stating that a series C in $\overline{\mathbb{F}}_p[[X]]$ is algebraic if and only if its p-kernel $\mathcal{H}(C)$ is of finite dimension $\kappa(C) < \infty$. We have $\kappa(A+B) \leq \kappa(A) + \kappa(B)$, and an algebraic series $A \in \overline{\mathbb{F}}_p[[X]]$ has a minimal polynomial of degree at most $p^{\kappa(A)}$ with respect to A.

Theorem 1.6. *We have*

$$\kappa(\exp_! A) \leq q^{\kappa(A)-1} p^{q^{\kappa(A)}} \quad \text{and} \quad \kappa(\log_!(1+A)) \leq 1 + 4(\kappa(1+A))^p$$

for a nonzero algebraic series A in $\mathfrak{m} \subset \overline{\mathbb{F}}_p[[X]]$ having all its coefficients in a finite subfield $\mathbb{F}_q \subset \overline{\mathbb{F}}_p$ containing $q = p^e$ elements.

Considerations similar to those made after Theorem 1.5 are valid and Theorem 1.6 can be turned into an algorithmically effective version of Theorem 1.3.

A map $\mu : \mathcal{V} \longrightarrow \mathcal{W}$ between two $\mathbb{K}$-vector spaces is a homogeneous form of degree d if $l \circ \mu : \mathcal{V} \longrightarrow \mathbb{K}$ is homogeneous of degree d (given by a homogeneous polynomial of degree d with respect to coordinates) for all linear forms $l : \mathcal{W} \longrightarrow \mathbb{K}$.

A useful ingredient for proving Theorems 1.1, 1.3 and their effective versions is the following characterization of $\log_!$:

Proposition 1.7. *Over a field $\mathbb{K} \subset \overline{\mathbb{F}}_p$, the application $\log_! : 1 + \mathfrak{m} \longrightarrow \mathfrak{m}$ extends to a homogeneous form of degree p from $\mathbb{K}[[X]]$ into $\mathfrak{m}$.*

Example 1.8. In characteristic 2, we have

$$\log_!\left(\sum_{n=0}^{\infty} \alpha_n X^n\right) = \sum_{n=0}^{\infty} \alpha_{2^n}^2 X^{2^{n+1}} + \sum_{0 \leq i < j} \binom{i+j}{i} \alpha_i \alpha_j X^{i+j},$$

for $\sum_{n=0}^{\infty} \alpha_n X^n$ in $1 + X\overline{\mathbb{F}}_2[[X]]$.

Remark 1.9. Defining $f_!$ as

$$f_!\left(\sum_{n=1}^{\infty} \alpha_n X^n\right) = \sum_{n=1}^{\infty} \beta_n X^n$$

if

$$f\left(\sum_{n=1}^{\infty} \alpha_n \frac{X^n}{n!}\right) = \sum_{n=1}^{\infty} \beta_n \frac{X^n}{n!},$$

Theorems 1.1, 1.3, 1.5 and 1.6 have analogues for the functions $\sin_!$ and $\tan_!$ (and for their reciprocal functions $\arcsin_!$ and $\arctan_!$).

The rest of the paper is organized as follows. In Sections 2–6, we recall a few definitions and well-known facts that are essentially standard knowledge in the theory of divided powers; see [Berthelot and Ogus 1978] or the original work [Roby 1963; 1965]. Section 7 contains the proofs for all results mentioned above.

In a second part, starting at Section 8, we generalize Theorems 1.1 and 1.5 to formal power series in several noncommuting variables.

2. Rational and algebraic elements in $\mathbb{K}[[X]]$

This section recalls a few well-known facts concerning rational and algebraic elements in the algebra $\mathbb{K}[[X]]$ of formal power series.

We denote by $\tau : \mathbb{K}[[X]] \longrightarrow \mathbb{K}[[X]]$ the shift operator

$$\tau\left(\sum_{n=0}^{\infty} \alpha_n X^n\right) = \sum_{n=0}^{\infty} \alpha_{n+1} X^n$$

acting on formal power series. The following well-known result characterizes rational series:

Proposition 2.1. *A formal power series $A = \sum_{n=0}^{\infty} \alpha_n X^n$ of $\mathbb{K}[[X]]$ is rational if and only if the series $A, \tau(A), \tau^2(A), \ldots, \tau^k(A) = \sum_{n=0}^{\infty} \alpha_{n+k} X^n, \ldots$ span a finite-dimensional vector space in $\mathbb{K}[[X]]$.*

More precisely, the vector space spanned by $A, \tau(A), \tau^2(A), \ldots, \tau^i(A), \ldots$ has dimension $\|A\| = \max(1 + \deg f, \deg g)$ if f/g, with $f, g \in \mathbb{K}[X]$, is a reduced expression of a rational series A.

The function $A \mapsto \|A\|$ satisfies the inequality

$$\|A + B\| \le \|A\| + \|B\|$$

for rational series A, B in $\mathbb{K}[[X]]$. As a particular case, we have

$$\|A\| - 1 \le \|1 + A\| \le \|A\| + 1.$$

Given a prime p and a formal power series $C = \sum_{n=0}^{\infty} \gamma_n X^n$ in $\overline{\mathbb{F}}_p[[X]]$, we denote by $\kappa(C) \in \mathbb{N} \cup \{\infty\}$ the dimension of its p-kernel

$$\mathcal{K}(C) = \mathbb{K}C + \sum_{f,k} \overline{\mathbb{F}}_p C_{k,f},$$

spanned by C and all series of the form

$$C_{k,f} = \sum_{n=0}^{\infty} \gamma_{k+np^f} X^n,$$

with $k \in \mathbb{N}$ such that $k < p^f$ for $f \in \{1, 2, \ldots\}$.

Algebraic series of $\mathbb{K}[[X]]$, for $\mathbb{K}$ a subfield of the algebraic closure $\overline{\mathbb{F}}_p$ of finite prime characteristic p, are characterized by the following theorem of Christol [1979] (see also [Allouche and Shallit 2003, Theorem 12.2.5]):

Theorem 2.2. *A formal power series $C = \sum_{n=0}^{\infty} \gamma_n X^n$ of $\overline{\mathbb{F}}_p[[X]]$ is algebraic if and only if the dimension $\kappa(C) = \dim \mathcal{K}(C)$ of its p-kernel $\mathcal{K}(C)$ is finite.*

Finiteness of $\kappa(C)$ amounts to recognizability of C, which has the following well-known consequence.

Corollary 2.3. *An algebraic series of $\overline{\mathbb{F}}_p[[X]]$ has all its coefficients in a finite subfield of $\overline{\mathbb{F}}_p$.*

Proposition 2.4. *Let $C = \sum_{n=0}^{\infty} \gamma_n X^n$ be an algebraic series with coefficients in a subfield $\mathbb{K} \subset \overline{\mathbb{F}}_p$.*

(i) $\mathcal{K}(\tau(C)) \subset \mathcal{K}(C) + \tau(\mathcal{K}(C))$, *which implies* $\kappa(\tau(C)) \leq 2\kappa(C)$.

(ii) $\mathcal{K}(C) \subset \mathbb{K} + \mathcal{K}(\tau(C)) + X\mathcal{K}(\tau(C))$, *which implies* $\kappa(C) \leq 1 + 2\kappa(\tau(C))$.

Proof. Assertion (i) follows from an iterated application of the easy computations

$$(\tau(C))_{k,1} = C_{k+1,1},$$

if $0 \leq k < p-1$ and

$$(\tau(C))_{p-1,1} = \tau(C_{0,1}).$$

The proof of assertion (ii) is similar. □

3. The shuffle algebra

This section recalls mostly well-known results concerning shuffle products of elements in the set $\mathbb{K}[[X]]$ of formal power series over a commutative field $\mathbb{K}$, which is arbitrary unless specified otherwise.

The *shuffle product*

$$A \sqcup\!\sqcup B = C = \sum_{n=0}^{\infty} \gamma_n X^n$$

of $A = \sum_{n=0}^{\infty} \alpha_n X^n$ and $B = \sum_{n=0}^{\infty} \beta_n X^n$ is defined by

$$\gamma_n = \sum_{k=0}^{n} \binom{n}{k} \alpha_k \beta_{n-k},$$

and corresponds to the usual product $ab = c$ of the associated exponential generating series

$$a = \sum_{n=0}^{\infty} \alpha_n \frac{X^n}{n!}, \quad b = \sum_{n=0}^{\infty} \beta_n \frac{X^n}{n!}, \quad c = \sum_{n=0}^{\infty} \gamma_n \frac{X^n}{n!}.$$

The *shuffle algebra* is the algebra $(\mathbb{K}[[X]], \sqcup\!\sqcup)$ obtained by endowing the vector space $\mathbb{K}[[X]]$ of ordinary generating series with the shuffle product. By construction, the shuffle algebra is isomorphic to the algebra $\mathscr{E}(\mathbb{K})$ of exponential generating series. In characteristic zero, the trivial identity

$$\sum_{n=0}^{\infty} \alpha_n X^n = \sum_{n=0}^{\infty} (n!\alpha_n) \frac{X^n}{n!}$$

gives an isomorphism between the usual algebra $\mathbb{K}[[X]]$ of ordinary generating series and the shuffle algebra $(\mathbb{K}[[X]], \sqcup\!\sqcup)$.

The identity

$$\left(\sum_{n\geq 0} \lambda^n X^n\right) \sqcup\!\sqcup \left(\sum_{n\geq 0} \mu^n X^n\right) = \sum_{n\geq 0} (\lambda+\mu)^n X^n,$$

equivalent to $e^{\lambda X} e^{\mu X} = e^{(\lambda+\mu)X}$, implies that the convergence radius of the shuffle product of two complex series with strictly positive convergence radii ρ_1, ρ_2 is at least the harmonic mean $1/(1/\rho_1 + 1/\rho_2)$ of ρ_1 and ρ_2.

Proposition 3.1. *The shift operator*

$$\tau\left(\sum_{n=0}^{\infty} \alpha_n X^n\right) = \sum_{n=0}^{\infty} \alpha_{n+1} X^n$$

acts as a derivation on the shuffle algebra.

Proof. The map τ is clearly linear. The computation

$$\begin{aligned}\tau\left(\sum_{i,j\geq 0} \binom{i+j}{i} \alpha_i \beta_j X^{i+j}\right) &= \sum_{\substack{i,j\geq 0\\ i+j\geq 1}} \binom{i+j}{i} \alpha_i \beta_j X^{i+j-1} \\ &= \sum_{\substack{i,j\geq 0\\ i+j\geq 1}} \left(\binom{i+j-1}{i-1} + \binom{i+j-1}{j-1}\right) \alpha_i \beta_j X^{i+j-1}\end{aligned}$$

shows that τ satisfies the Leibniz rule $\tau(A \sqcup\!\sqcup B) = \tau(A) \sqcup\!\sqcup B + A \sqcup\!\sqcup \tau(B)$. □

Proposition 3.1 is trivial and well-known in characteristic zero: the usual derivation d/dX acts obviously as the shift operator on the algebra $\mathscr{E}(\mathbb{K})$ of exponential generating series over a field of characteristic zero.

The following two results seem to be due to Fliess [1974, Proposition 6].

Proposition 3.2. *Shuffle products of rational power series are rational.*

More precisely, we have

$$\|A \sqcup\!\sqcup B\| \leq \|A\| \, \|B\|,$$

for two rational series A, B in $\mathbb{K}[[X]]$.

Proof. Proposition 3.1 implies $\tau^n(A \sqcup\!\sqcup B) = \sum_{k=0}^{n} \binom{n}{k} \tau^k(A) \sqcup\!\sqcup \tau^{n-k}(B)$. The series $\tau^n(A \sqcup\!\sqcup B)$ belongs thus to the vector space spanned by shuffle products with factors in the vector spaces $\sum_{n\geq 0} \mathbb{K}\tau^n(A)$ and $\sum_{n\geq 0} \mathbb{K}\tau^n(B)$. This implies the inequality. Proposition 2.1 ends the proof. □

Proposition 3.3. *Shuffle products of algebraic series in $\overline{\mathbb{F}}_p[[X]]$ are algebraic.*
More precisely, we have

$$\kappa(A \sqcup\!\sqcup B) \leq \kappa(A)\kappa(B).$$

Proof. Denoting by $C_{k,f}$ the series

$$C_{k,f} = \sum_{n=0}^{\infty} \gamma_{k+np^f} X^n$$

associated to a series $C = \sum_{n=0}^{\infty} \gamma_n X^n$, as in Section 2, and by $\kappa(C)$ the dimension of the vector space $\mathcal{H}(C) = \mathbb{K}C + \sum_{k,f} \overline{\mathbb{F}}_p C_{k,f}$, Lucas's identity [1878]

$$\binom{n}{k} \equiv \prod_{i\geq 0} \binom{\nu_i}{\kappa_i} \pmod{p},$$

for $n = \sum_{i\geq 0} \nu_i p^i$ and $k = \sum_{i\geq 0} \kappa_i p^i$ with $\nu_i, \kappa_i \in \{0, \ldots, p-1\}$, implies

$$(A \sqcup\!\sqcup B)_{k,1} = \sum_{i=0}^{k} \binom{k}{i} A_{i,1} \sqcup\!\sqcup B_{k-i,1},$$

for $k = 0, \ldots, p-1$. Iteration of this formula shows that $(A \sqcup\!\sqcup B)_{k,f}$ (for arbitrary $k, f \in \mathbb{N}$ such that $k < p^f$) belongs to the vector space spanned by shuffle products with factors in the vector spaces $\mathcal{H}(A)$ and $\mathcal{H}(B)$ of dimension $\kappa(A)$ and $\kappa(B)$.

Christol's Theorem (Theorem 2.2) ends the proof. □

Remark 3.4. Given a subfield $\mathbb{K}$ of $\overline{\mathbb{F}}_p$, let $\mathcal{A} \subset \mathbb{K}[[X]]$ denote a vector space of finite dimension $a = \dim \mathcal{A}$ containing the p-kernel $\mathcal{H}(A)$ of every element $A \in \mathcal{A}$.

We consider an element $B = A_1 \sqcup\!\sqcup A_2 \sqcup\!\sqcup \cdots \sqcup\!\sqcup A_k$ given by the shuffle product of k series $A_1, \ldots, A_k \in \mathcal{A}$. Expressing all elements $A_1, A_2, \ldots$ as linear combinations of elements in a fixed basis of $\mathcal{A}$ and using commutativity of the shuffle product, the proof of Proposition 3.3 shows that the inequality $\kappa(B) \leq \kappa(A_1)\kappa(A_2)\cdots \leq a^k = (\dim \mathcal{A})^k$ can be improved to

$$\kappa(B) \leq \binom{k+a-1}{a-1},$$

where the binomial coefficient gives the dimension of the vector space of homogeneous polynomials of degree k in a (commuting) variables $X_1, X_2, \ldots, X_a$.

4. The special shuffle group

We call the group of units of the shuffle algebra $(\mathbb{K}[[X]], \sqcup\!\sqcup)$ the *shuffle group*. Its elements are given by the set $\mathbb{K}^* + X\mathbb{K}[[X]]$ underlying the multiplicative unit group. The shuffle group is the direct product of the unit group $\mathbb{K}^*$ of $\mathbb{K}$ with the *special shuffle group* $(1 + X\mathbb{K}[[X]], \sqcup\!\sqcup)$.

The inverse in the shuffle group of $1 - A \in (1 + X\mathbb{K}[[X]], \sqcup\!\sqcup)$ is given by

$$\sum_{n=0}^{\infty} A^{\sqcup\!\sqcup^n} = 1 + A + A \sqcup\!\sqcup A + A \sqcup\!\sqcup A \sqcup\!\sqcup A + \cdots ,$$

where $A^{\sqcup\!\sqcup^0} = 1$ and $A^{\sqcup\!\sqcup^{n+1}} = A \sqcup\!\sqcup A^{\sqcup\!\sqcup^n}$ for $n \geq 1$.

The trivial identity $X \sqcup\!\sqcup X^n = \binom{n+1}{1} X^{n+1} = (n+1)X^{n+1} \in \mathbb{K}[[X]]$ implies $(1 - X) \sqcup\!\sqcup \left(\sum_{n=0}^{\infty} n! X^n\right) = 1$. Invertible rational (analytical) power series have thus generally a transcendental (nonanalytical) shuffle inverse over the complex numbers.

Proposition 4.1. *The special shuffle group* $(1 + X\mathbb{K}[[X]], \sqcup\!\sqcup)$ *is isomorphic to an infinite-dimensional* $\mathbb{F}_p$*-vector space if the field* $\mathbb{K}$ *is of positive characteristic* p.

Proposition 4.1 shows that $(1 + X\mathbb{K}[[X]], \sqcup\!\sqcup)$ is not isomorphic to the multiplicative group structure on $1 + X\mathbb{K}[[X]]$ if $\mathbb{K}$ is of positive characteristic.

Proof of Proposition 4.1. It follows from the fact that $\exp_!$ is a group isomorphism between the $\mathbb{F}_p$-vector space $\mathfrak{m}$ and the special shuffle group. □

Proposition 4.1 follows also as a special case from Proposition 8.1. This yields a different proof, which is not based on properties of $\exp_!$.

Remark 4.2. One can show that a rational fraction $A \in 1 + X\mathbb{C}[[X]]$ has a rational inverse for the shuffle product if and only if $A = 1/(1 - \lambda X)$ with $\lambda \in \mathbb{C}$. (Compute $A \sqcup\!\sqcup B = 1$ using the decomposition into simple fractions of the rational series A, B.)

5. The exponential and the logarithm for exponential generating functions

Hurwitz showed that $1/(k!)a^k$ is well-defined for $a \in \mathfrak{m}_{\mathscr{C}}$ with coefficients in an arbitrary field or commutative ring [Hurwitz 1899, Satz 1]. We give a different proof of this fact, that implies that $\exp_!$ and $\log_!$ are well-defined over fields of positive characteristic.

Proposition 5.1. *For all natural numbers* $j, k \geq 1$, *the set* $\{1, \ldots, jk\}$ *can be partitioned in exactly*

$$\frac{(jk)!}{(j!)^k k!} \tag{3}$$

different ways into k unordered disjoint subsets of j elements. In particular, the rational number in (3) is an integer for all natural numbers j, k such that $j \geq 1$.

Proof. The multinomial coefficient $(jk)!/(j!)^k$ counts the number of ways of partitioning $\{1, \ldots, jk\}$ into an ordered sequence of k disjoint subsets containing all j elements. Dividing by $k!$ removes the order on these k subsets.

This proves that the formula defines an integer for all $j, k \geq 1$, and integrality obviously also holds for $k = 0$ and $j \geq 1$. □

Remark 5.2. A slightly different proof of Proposition 5.1 follows from the observation that $(jk)!/((j!)^k k!)$ is the index in the symmetric group over jk elements of the subgroup formed by all permutations stabilizing a partition of the set $\{1, \ldots, jk\}$ into k disjoint subsets of j elements.

A different proof is given by the formula

$$\frac{(jk)!}{(j!)^k k!} = \prod_{n=1}^{k} \binom{nj-1}{j-1},$$

easily shown using induction on k; see [Berthelot and Ogus 1978, Section 3] (which contains a small misprint).

Proposition 5.3. *For any natural integer $k \in \mathbb{N}$, there exist polynomials $P_{k,n} \in \mathbb{N}[\alpha_1, \ldots, \alpha_n]$ such that*

$$\frac{1}{k!}\left(\sum_{n=1}^{\infty} \alpha_n \frac{X^n}{n!}\right)^k = \sum_{n=0}^{\infty} P_{k,n}(\alpha_1, \alpha_2, \ldots, \alpha_n)\frac{X^n}{n!}.$$

Proof. The contribution of a monomial

$$\alpha_1^{j_1}\alpha_2^{j_2}\ldots\alpha_s^{j_s}\frac{X^{\sum_{i=1}^s ij_i}}{(\sum_{i=1}^s ij_i)!},$$

with $j_1 + j_2 + \cdots + j_s = k$, to $\frac{1}{k!}\left(\sum_{n=1}^{\infty} \alpha_n X^n/n!\right)^k$ is given by

$$\frac{1}{k!}\,\frac{k!}{(j_1)!(j_2)!\ldots(j_s)!}\,\frac{(\sum_{i=1}^s ij_i)!}{\prod_{i=1}^s (i!)^{j_i}} = \left(\prod_{i=1}^{s}\frac{(ij_i)!}{(i!)^{j_i}(j_i)!}\right)\frac{(\sum_{i=1}^s ij_i)!}{\prod_{i=1}^s (ij_i)!},$$

where the last expression is a product of a natural integer by Proposition 5.1 and of a multinomial coefficient. It is thus a natural integer. □

Corollary 5.4. *For $a = \sum_{n=1}^{\infty} \alpha_n X^n/n!$, the formulae*

$$\exp\left(\sum_{n=1}^{\infty} \alpha_n \frac{X^n}{n!}\right) = \sum_{k=0}^{\infty}\sum_{n=0}^{\infty} P_{k,n}(\alpha_1, \ldots, \alpha_n)\frac{X^n}{n!}$$

and

$$\log\left(1+\sum_{n=1}^{\infty}\alpha_n\frac{X^n}{n!}\right)=\sum_{k=1}^{\infty}\sum_{n=0}^{\infty}(-1)^{k+1}(k-1)!\,P_{k,n}(\alpha_1,\ldots,\alpha_n)\frac{X^n}{n!}$$

define the exponential function and the logarithm of an exponential generating series in $a\in\mathfrak{m}_{\mathscr{E}}$ *and* $1+a\in 1+\mathfrak{m}_{\mathscr{E}}$, *respectively, over an arbitrary field* $\mathbb{K}$. *These functions are one-to-one and mutually reciprocal.*

The following result shows that the functions $\exp_{!}$ and $\log_{!}$ behave as expected under the derivation $\tau:\sum_{n=0}^{\infty}\alpha_n X^n\mapsto\sum_{n=0}^{\infty}\alpha_{n+1}X^n$ of the shuffle algebra.

Proposition 5.5. *For all* $A\in\mathfrak{m}=X\mathbb{K}[[X]]$ *over an arbitrary field* $\mathbb{K}$, *we have*

$$\tau(\exp_{!}A)=(\exp_{!}A)\sqcup\!\sqcup\tau(A)$$

and

$$\tau(\log_{!}(1+A))=(1+A)^{\sqcup\!\sqcup^{-1}}\sqcup\!\sqcup\tau(A),$$

where $(1+A)^{\sqcup\!\sqcup^{-1}}$ *denotes the shuffle inverse of* $(1+A)$.

Proof. Proposition 3.1 implies the formal identities

$$\tau\left(\sum_{n=0}^{\infty}\frac{A^{\sqcup\!\sqcup^n}}{n!}\right)=\sum_{n=0}^{\infty}n\frac{A^{\sqcup\!\sqcup^{n-1}}}{n!}\sqcup\!\sqcup\tau(A)=\left(\sum_{n=0}^{\infty}\frac{A^{\sqcup\!\sqcup^n}}{n!}\right)\sqcup\!\sqcup\tau(A),$$

for $A\in\mathfrak{m}$. By Proposition 5.1, this identity holds over the ring $\mathbb{Z}$ and thus over an arbitrary commutative field. This establishes the formula for $\exp_{!}$.

For $\log_{!}$ we get similarly

$$\tau\left(-\sum_{n=1}^{\infty}\frac{(-A)^{\sqcup\!\sqcup^n}}{n}\right)=\sum_{n=1}^{\infty}n\frac{(-A)^{\sqcup\!\sqcup^{n-1}}}{n}\sqcup\!\sqcup\tau(A)=\left(\sum_{n=0}^{\infty}(-A)^{\sqcup\!\sqcup^n}\right)\sqcup\!\sqcup\tau(A),$$

which implies the result, by Proposition 5.1 and by the trivial identity

$$(1+A)^{\sqcup\!\sqcup^{-1}}=\sum_{n=0}^{\infty}(-A)^{\sqcup\!\sqcup^n},$$

for the shuffle inverse $(1+A)^{\sqcup\!\sqcup^{-1}}$ of $1+A\in 1+\mathfrak{m}$. □

6. The logarithm as a p-homogeneous form over $\overline{\mathbb{F}}_p[[x]]$

Given a fixed prime number p, Proposition 4.1 implies that there exist polynomials $Q_{p,n}\in\mathbb{N}[\alpha_0,\ldots,\alpha_n]$ for $n\geq 1$ such that

$$\left(\sum_{n=0}^{\infty}\alpha_n X^n\right)^{\sqcup\!\sqcup^p}=\alpha_0^p+p\sum_{n=1}^{\infty}Q_{p,n}(\alpha_0,\ldots,\alpha_n)X^n.$$

The polynomials $Q_{p,n}$ are homogeneous of degree p with respect to the variables $\alpha_0, \dots, \alpha_n$, and we denote by

$$\mu_p\Big(\sum_{n=0}^{\infty}\alpha_n X^n\Big)=\sum_{n=1}^{\infty}Q_{p,n}(\alpha_0,\dots,\alpha_n)X^n$$

the p-homogeneous form defined by the ordinary generating series of the polynomials $Q_{p,1}, Q_{p,2}, \dots$.

Proposition 6.1. *The restriction of μ_p to $1+\mathfrak{m}\subset\overline{\mathbb{F}}_p[[X]]$ coincides with the function* $\log_!$.

Proof. We have

$$\tau(\mu_p(1+A))=(1+A)^{\sqcup\!\sqcup^{p-1}}\sqcup\!\sqcup\,\tau(1+A)$$

for A in $\mathfrak{m}$, where $\tau\big(\sum_{n=0}^{\infty}\alpha_n X^n\big)=\sum_{n=0}^{\infty}\alpha_{n+1}X^n$ is the shift operator of Proposition 3.1. This identity defines the restriction of the p-homogeneous form μ_p to $1+\mathfrak{m}$. Proposition 5.5 and the identity

$$(1+A)^{\sqcup\!\sqcup^{p-1}}\sqcup\!\sqcup\,(1+A)=1$$

show that the function $\log_!$ satisfies the same equation

$$\tau(\log_!(1+A))=(1+A)^{\sqcup\!\sqcup^{p-1}}\sqcup\!\sqcup\,\tau(1+A).$$

Since both series $\mu_p(1+A)$ and $\log_!(1+A)$ are without constant term, the equality $\tau(\mu_p(1+A))=\tau(\log_!(1+A))$ implies $\mu_p(1+A)=\log_!(1+A)$. □

7. Proofs

Proposition 7.1. *If A in $X\overline{\mathbb{F}}_p[[X]]$ is rational (respectively algebraic), then the formal power series* $\log_!(1+A)$ *is rational (respectively algebraic).*

More precisely,

$$\|\log_!(1+A)\|\le 1+\binom{p+\|1+A\|-1}{p}\le 1+\|1+A\|^p$$

for A rational in $\mathfrak{m}=X\overline{\mathbb{F}}_p[[X]]$, and

$$\kappa(\log_!(1+A))\le 1+4\kappa(A)\binom{p+\kappa(1+A)-2}{p-1}\le 1+4(\kappa(1+A))^p$$

for A algebraic in $\mathfrak{m}$.

Proposition 7.2. *If A in $X\overline{\mathbb{F}}_p[[X]]$ is rational (respectively algebraic), then* $\exp_!A$ *is rational (respectively algebraic).*

More precisely, denoting by $q=p^e$ the cardinality of a finite field $\mathbb{F}_q\subset\overline{\mathbb{F}}_p$ containing all coefficients of A,

$$\|\exp_!A\|\le p^{q^{\|A\|}}$$

for A rational in $\mathfrak{m}$*, and*

$$\kappa(\exp_!\, A) \le q^{\kappa(A)-1} p^{q^{\kappa(A)}}$$

for A algebraic and nonzero in $\mathfrak{m}$.

Theorems 1.1, 1.3, 1.5 and 1.6 are now simple reformulations of Propositions 7.1 and 7.2.

Proof of Proposition 7.1. Apply the identity $(1+A)^{\sqcup\!\sqcup^p} = 1$, which follows from Proposition 4.1, to

$$\tau(\log_!(1+A)) = (1+A)^{\sqcup\!\sqcup^{-1}} \sqcup\!\sqcup \tau(A)$$

of Proposition 5.5, to establish

$$\tau(\log_!(1+A)) = (1+A)^{\sqcup\!\sqcup^{p-1}} \sqcup\!\sqcup \tau(A),$$

already encountered in the proof of Proposition 6.1. This shows

$$\|\tau(\log_!(1+A)\| \le \|1+A\|^{p-1}\|\tau(A)\| \le \|1+A\|^p$$

and implies

$$\|\log_!(1+A)\| \le 1 + \|1+A\|^p.$$

This proves the cruder inequality in the rational case. The finer inequality follows from the fact that all p factors of

$$(1+A)^{\sqcup\!\sqcup^{p-1}} \sqcup\!\sqcup \tau(A) = \tau(\log_!(1+A))$$

belong to a common vector space of dimension $\|1+A\|$ that is closed for the shift map. The details are the same as for Remark 3.4.

For algebraic A we have similarly

$$\begin{aligned}\kappa(\tau(\log_!(1+A))) &\le (\kappa(1+A))^{p-1}\, \kappa(\tau(A)) = (\kappa(1+A))^{p-1}\, \kappa(\tau(1+A)) \\ &\le (\kappa(1+A))^{p-1} 2\kappa(1+A) \le 2(\kappa(1+A))^p,\end{aligned}$$

using Proposition 2.4(i). This shows

$$\kappa(\log_!(1+A)) \le 1 + 2\kappa(\tau(\log_!(1+A))) \le 1 + 4(\kappa(1+A))^p,$$

by Proposition 2.4(ii), and ends the proof for the cruder inequality.

The finer inequality follows from Proposition 2.4 and Remark 3.4. □

Given a vector space $\mathcal{V} \subset \mathbb{K}[[X]]$ containing $\mathbb{K}$, we denote by $\Gamma(\mathcal{V})$ the shuffle subgroup generated by all elements of $\mathcal{V} \cap (1 + X\mathbb{K}[[X]])$.

Lemma 7.3. *Every element of a vector space* $\mathcal{V} \subset \mathbb{K}[[X]]$ *containing the field* $\mathbb{K}$ *of constants can be written as a linear combination of elements in* $\Gamma(\mathcal{V})$.

Proof. We have the identity

$$A = (1 - \epsilon(A) + A) + (\epsilon(A) - 1),$$

where $\epsilon\left(\sum_{n=0}^{\infty} \alpha_n X^n\right) = \alpha_0$ is the augmentation map and where $(1 - \epsilon(A) + A)$ and the constant $(\epsilon(A) - 1)$ are both in $\mathbb{K}\Gamma(\mathcal{V})$ for $A \in \mathcal{V}$. □

Proof of Proposition 7.2 for A rational. Corollary 2.3 shows that we can work over a finite subfield $\mathbb{K} = \mathbb{F}_q$ of $\overline{\mathbb{F}}_p$ consisting of $q = p^e$ elements.

Given a rational series A in $\mathfrak{m} = X\mathbb{K}[[X]]$, we denote by Γ_A the shuffle subgroup generated by all elements of the set

$$\left\{ \bigcup_{n=0}^{\infty} \left(\tau^n(A) + \mathbb{K}\right) \right\} \cap \{1 + X\mathbb{K}[[X]]\}.$$

This generating set of Γ_A contains at most $q^{\|A\|}$ elements. Proposition 4.1 implies thus that Γ_A is a finite group having at most $p^{q^{\|A\|}}$ elements. The subalgebra $\mathbb{K}[\Gamma_A] \subset \mathbb{K}[[X]]$ spanned by all elements of Γ_A is thus of dimension $\leq p^{q^{\|A\|}}$. The identity

$$\tau(\exp_!\, A) = \exp_!\, A \sqcup\!\sqcup \tau(A)$$

of Proposition 5.5 and the fact that the derivation τ of $\mathbb{K}[[X]]$ restricts to a derivation of the subalgebra $\mathbb{K}[\Gamma_A]$ show the inclusion

$$\tau^n(\exp_!\, A) \in \exp_!\, A \sqcup\!\sqcup \mathbb{K}[\Gamma_A]$$

for all $n \in \mathbb{N}$ by Lemma 7.3. This ends the proof, since the right side is a $\mathbb{K}$-vector space of dimension at most $p^{q^{\|A\|}}$. □

Proposition 7.4. *We have, for every prime number p and for all natural integers j, k such that $j \geq 1$, the identity*

$$\frac{(jk)!}{(j!)^k k!} \equiv \frac{(pjk)!}{((pj)!)^k k!} \pmod{p}.$$

Proof. The fraction on the right side yields the cardinality of the set $\mathcal{E}$ of all partitions of $\{1, \ldots, pjk\}$ into k subsets of pj elements. Consider the group G generated by the jk cycles of length p of the form $(i, i+jk, i+2jk, \ldots, i+(p-1)jk)$ for $i = 1, \ldots, jk$. The group G has p^{jk} elements and acts on the set of partitions by preserving their type defined as the multiset of cardinalities of all involved parts. In particular, it acts by permutation on the set $\mathcal{E}$. A partition $P \in \mathcal{E}$ is a fixpoint for G if and only if every part of P is a union of G-orbits. Choosing a bijection between $\{1, \ldots, jk\}$ and G-orbits of $\{1, \ldots, pjk\}$, fixpoints of $\mathcal{E}$ are in bijection with partitions of the set $\{1, \ldots, jk\}$ into k subsets of j elements. The number of fixpoints of the G-action on $\mathcal{E}$ equals thus $(jk)!/((j!)^k k!)$. Since G is a p-group,

the cardinalities of all nontrivial G-orbits of $\mathscr{C}$ are strictly positive powers of p. This ends the proof. □

Corollary 7.5. $\exp_!$ *and* $\log_!$ *commute with the "Frobenius substitution"*

$$\varphi\left(\sum_{n=0}^{\infty}\alpha_n X^n\right)=\sum_{n=0}^{\infty}\alpha_n X^{pn}$$

for series in $X\overline{\mathbb{F}}_p[[X]]$ *and* $1+X\overline{\mathbb{F}}_p[[X]]$, *respectively.*

This implies $(\exp_! A)_{0,f}=\exp_! A_{0,f}$, where $C_{k,f}=\sum_{n=0}^{\infty}\gamma_{k+np^f}X^n$ for $C=\sum_{n=0}^{\infty}\gamma_n X^n$.

Lemma 7.6. $(B \sqcup\!\sqcup C)_{0,1}=B_{0,1}\sqcup\!\sqcup C_{0,1}$.

Proof. Follows from the identity $\binom{pn}{k}\equiv 0 \pmod p$ if $k\not\equiv 0 \pmod p$. □

Proof of Proposition 7.2 for A algebraic. We work again over a finite subfield $\mathbb{K}=\mathbb{F}_q\subset\overline{\mathbb{F}}_p$ containing all coefficients of A. Let Γ_A denote the shuffle subgroup generated by all elements in

$$(\mathcal{H}(A)+\mathbb{K})\cap(1+X\mathbb{K}[[X]]),$$

where

$$\mathcal{H}(A)=\mathbb{K}A+\sum_{k,f}\mathbb{K}A_{k,f}$$

denotes the p-kernel of A. We denote by $\mathbb{K}[\Gamma_A]\subset(\mathbb{K}[[X]],\sqcup\!\sqcup)$ the shuffle subalgebra of dimension at most $p^{q^{\kappa(A)}}$ spanned by all elements of the group $\Gamma_A\subset(1+X\mathbb{K}[[X]],\sqcup\!\sqcup)$.

Using the convention $A_{0,0}=A$, we have, for $B\in\mathbb{K}[\Gamma(A)]$ and for k such that $0\le k<p$,

$$\begin{aligned}(\exp_!(A_{0,f})\sqcup\!\sqcup B)_{k,1}&=(\tau^k(\exp_!(A_{0,f})\sqcup\!\sqcup B))_{0,1}\\&=\left(\sum_{j=0}^{k}\binom{k}{j}\tau^j(\exp_! A_{0,f})\sqcup\!\sqcup\tau^{k-j}(B)\right)_{0,1}\\&=\sum_{j=0}^{k}\binom{k}{j}(\tau^j(\exp_! A_{0,f}))_{0,1}\sqcup\!\sqcup B_{k-j,1},\end{aligned}$$

where the last equality is due to Lemma 7.6 (and to the equality $(\tau^k(C))_{0,1}=C_{k,1}$ for $0\le k<p$).

Proposition 5.5 gives $\tau(\exp_! A_{0,f})=(\exp_! A_{0,f})\sqcup\!\sqcup\tau(A_{0,f})$; iterating this identity shows that $\tau^j(\exp_! A_{0,f})$ is of the form $(\exp_! A_{0,f})\sqcup\!\sqcup F$, where F is

a linear combination of shuffle products involving at most j factors of the set $\{\tau(A_{0,f}), \tau^2(A_{0,f}), \dots, \tau^j(A_{0,f})\}$. Applying Lemma 7.6, we get

$$(\tau^j(\exp_! A_{0,f}))_{0,1} = (\exp_{0,f+1}(A)) \sqcup\!\sqcup F_{0,1}.$$

An iterated application of Lemma 7.6 now shows that $F_{0,1}$ is a linear combination of shuffle products involving at most j factors in $\{A_{1,f+1}, \dots, A_{j,f+1}\}$. We thus have $F_{0,1} \in \mathbb{K}[\Gamma_A]$, by Lemma 7.3, and we get the inclusion

$$(\exp_!(A_{0,f}) \sqcup\!\sqcup \mathbb{K}[\Gamma_A])_{k,1} \subset \exp_!(A_{0,f+1}) \sqcup\!\sqcup \mathbb{K}[\Gamma_A]$$

for all $f \in \mathbb{N}$ and for all $k \in \{0, \dots, p-1\}$.

Setting

$$E_A = \{\exp_! B \mid B \in \mathcal{H}(A) \cap X\mathbb{K}[[X]]\},$$

we have the inclusion

$$\mathcal{H}(\exp_! A) \subset E_A \sqcup\!\sqcup \mathbb{K}[\Gamma_A] \subset \mathbb{K}[E_A] \sqcup\!\sqcup \mathbb{K}[\Gamma_A],$$

where $\mathcal{H}(\exp_! A)$ denotes the p-kernel of $\exp_! A$. This implies

$$\kappa(\exp_! A) \leq \dim \mathbb{K}[E_A] \dim \mathbb{K}[\Gamma_A].$$

We suppose now A that is nonzero. The vector space $\mathcal{H}(A) \cap X\mathbb{K}[[X]]$ is thus of codimension 1 in $\mathcal{H}(A)$. The image E_A of $\mathcal{H}(A) \cap X\mathbb{K}[[X]]$ under the group isomorphism $\exp_! : (X\mathbb{K}[[X]], +) \mapsto (1 + X\mathbb{K}[[X]], \sqcup\!\sqcup)$ is hence a subgroup of cardinality $q^{\kappa(A)-1}$ in $(1 + X\mathbb{K}[[X]], \sqcup\!\sqcup)$. We have thus

$$\kappa(\exp_! A) \leq \dim \mathbb{K}[E_A] \dim \mathbb{K}[\Gamma_A] \leq q^{\kappa(A)-1} p^{q^{\kappa(A)}},$$

which ends the proof. □

8. Power series in free noncommuting variables

This and the next section recall a few basic and well-known facts concerning (rational) power series in free noncommuting variables; see, for instance, [Stanley 1999] or [Berstel and Reutenauer 1988]. Sometimes, however, we use a different terminology, motivated by [Bacher 2008].

We denote by $\mathcal{X}^*$ the free monoid on a finite set $\mathcal{X} = \{X_1, \dots, X_k\}$. We write 1 for the identity element and we use a boldface capital $\boldsymbol{X}$ for a noncommutative monomial $\boldsymbol{X} = X_{i_1} X_{i_2} \dots X_{i_l} \in \mathcal{X}^*$. We denote by

$$A = \sum_{\boldsymbol{X} \in \mathcal{X}^*} (A, \boldsymbol{X}) \boldsymbol{X} \in \mathbb{K}\langle\langle X_1, \dots, X_k \rangle\rangle$$

a noncommutative formal power series, where $\mathcal{X}^* \ni \boldsymbol{X} \mapsto (A, \boldsymbol{X}) \in \mathbb{K}$ stands for the coefficient function.

We denote by $\mathfrak{m} \subset \mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$ the maximal ideal consisting of formal power series without constant coefficient, and by $\mathbb{K}^* + \mathfrak{m} = \mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle \setminus \mathfrak{m}$ the unit group of the algebra $\mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$ consisting of all (multiplicatively) invertible elements in $\mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$. The unit group is isomorphic to the direct product $\mathbb{K}^* \times (1 + \mathfrak{m})$, where $\mathbb{K}^*$ is the central subgroup consisting of nonzero constants and where $1 + \mathfrak{m}$ denotes the multiplicative subgroup given by the affine subspace formed by power series with constant coefficient 1. We have $(1-A)^{-1} = 1 + \sum_{n=1}^{\infty} A^n$ for the multiplicative inverse $(1-A)^{-1}$ of an element $1 - A \in 1 + \mathfrak{m}$.

The shuffle algebra. The *shuffle product* $\boldsymbol{X} \sqcup\!\sqcup \boldsymbol{X}'$ of two noncommutative monomials $\boldsymbol{X}, \boldsymbol{X}' \in \mathscr{X}^*$ of degrees $a = \deg \boldsymbol{X}$ and $b = \deg \boldsymbol{X}'$ (for the obvious grading given by $\deg X_1 = \cdots = \deg X_k = 1$) is the sum of all $\binom{a+b}{a}$ monomials of degree $a + b$ obtained by shuffling in all possible ways the linear factors (elements of $\mathscr{X}$) involved in $\boldsymbol{X}$ with the linear factors of $\boldsymbol{X}'$. A monomial involved in $\boldsymbol{X} \sqcup\!\sqcup \boldsymbol{X}'$ can be thought of as a monomial of degree $a + b$ whose linear factors are colored by two colors with $\boldsymbol{X}$ corresponding to the product of all linear factors of the first color and $\boldsymbol{X}'$ corresponding to the product of the remaining linear factors. The shuffle product $\boldsymbol{X} \sqcup\!\sqcup \boldsymbol{X}'$ can also be recursively defined by $\boldsymbol{X} \sqcup\!\sqcup 1 = 1 \sqcup\!\sqcup \boldsymbol{X} = \boldsymbol{X}$ and

$$(\boldsymbol{X}X_s) \sqcup\!\sqcup (\boldsymbol{X}'X_t) = (\boldsymbol{X} \sqcup\!\sqcup (\boldsymbol{X}'X_t))X_s + ((\boldsymbol{X}X_s) \sqcup\!\sqcup \boldsymbol{X}')X_t,$$

where $X_s, X_t \in \mathscr{X} = \{X_1, \ldots, X_k\}$ are monomials of degree 1.

Extending the shuffle product in the obvious way to formal power series endows the vector space $\mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$ with an associative and commutative algebra structure called the *shuffle algebra*. In the case of one variable $X = X_1$, we recover the definition of Section 3.

The group $\mathrm{GL}_k(\mathbb{K})$ acts on the vector space $\mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$ by linear substitutions. This action induces an automorphism of the multiplicative (noncommutative) algebra-structure or of the (commutative) shuffle algebra-structure underlying the vector space $\mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$.

Substitution of all variables X_j of formal power series in $\mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$ by X (or more generally by arbitrary not necessarily equal formal power series without constant term) yields a homomorphism of (shuffle) algebras into the commutative (shuffle) algebra $\mathbb{K}[\![X]\!]$.

The commutative unit group (set of invertible elements for the shuffle product) of the shuffle algebra, given by the set $\mathbb{K}^* + \mathfrak{m}$, is isomorphic to the direct product $\mathbb{K}^* \times (1 + \mathfrak{m})$, where $1 + \mathfrak{m}$ is endowed with the shuffle product. The inverse of an element $1 - A \in (1 + \mathfrak{m}, \sqcup\!\sqcup)$ is given by

$$\sum_{n=0}^{\infty} A^{\sqcup\!\sqcup^n} = 1 + A + A \sqcup\!\sqcup A + A \sqcup\!\sqcup A \sqcup\!\sqcup A + \cdots .$$

The following result generalizes Proposition 4.1:

Proposition 8.1. *Over a field of positive characteristic p, the subgroup $1+\mathfrak{m}$ of the shuffle group is an infinite-dimensional $\mathbb{F}_p$-vector space.*

Proof. Contributions to a p-fold shuffle product $A_1 \sqcup\!\sqcup A_2 \sqcup\!\sqcup \cdots \sqcup\!\sqcup A_p$ are given by monomials with linear factors colored by p colors $\{1,\dots,p\}$ keeping track of their "origin" with coefficients given by the product of the corresponding "monochromatic" coefficients in $A_1,\dots,A_p$. A permutation of the colors $\{1,\dots,p\}$ (and in particular, a cyclic permutation of all colors) leaves such a contribution invariant if $A_1=\cdots=A_p$. Coefficients of strictly positive degree in $A^{\sqcup\!\sqcup^p}$ are thus zero in characteristic p. □

As in the one-variable case, one can prove that

$$\frac{1}{k!}A^{\sqcup\!\sqcup^k}$$

is defined over an arbitrary field $\mathbb{K}$ for $A\in\mathfrak{m}$. Monomials contributing to $A^{\sqcup\!\sqcup^k}$ can be considered as colored by k colors and the $k!$ possible color-permutations yield identical contributions.

For $A\in\mathfrak{m}$, we denote by

$$\exp_!\, A=\sum_{n=0}^{\infty}\frac{1}{n!}A^{\sqcup\!\sqcup^n}$$

the resulting exponential map from the Lie algebra $\mathfrak{m}$ into the infinite-dimensional commutative Lie group $(1+\mathfrak{m},\sqcup\!\sqcup)$. As expected, its reciprocal function is

$$\log_!(1+A)=\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}A^{\sqcup\!\sqcup^n}.$$

In the case of a field $\mathbb{K}$ of positive characteristic p, the function $\log_!$ is again given by the restriction to $1+\mathfrak{m}$ of a p-homogeneous form μ_p.

The form μ_p has all its coefficients in $\mathbb{N}$ and is again defined by the equality

$$A^{\sqcup\!\sqcup^p}=(A,1)^p+p\mu_p(A)$$

over $\mathbb{Z}$. It can thus be defined over an arbitrary field.

9. Rational series

We say that a formal power series A is *rational* if it belongs to the smallest subalgebra in $\mathbb{K}\langle\langle X_1,\dots,X_k\rangle\rangle$ that contains the free associative algebra $\mathbb{K}\langle X_1,\dots,X_k\rangle$ of noncommutative polynomials and intersects the group of multiplicative units of $\mathbb{K}\langle\langle X_1,\dots,X_k\rangle\rangle$ in a subgroup.

Given a monomial $\boldsymbol{T} \in \mathscr{X}^*$, we denote by

$$\rho(\boldsymbol{T}) : \mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle \longrightarrow \mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$$

the linear application defined by

$$\rho(\boldsymbol{T})A = \sum_{\boldsymbol{X}\in\mathscr{X}^*} (A, \boldsymbol{XT})\boldsymbol{X}$$

for $A = \sum_{\boldsymbol{X}\in\mathscr{X}^*}(A, \boldsymbol{X})\boldsymbol{X}$ in $\mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$. The identity

$$\rho(\boldsymbol{T})(\rho(\boldsymbol{T}')A) = \rho(\boldsymbol{TT}')A$$

shows that we have a representation

$$\rho : \mathscr{X}^* \longrightarrow \mathrm{End}(\mathbb{K}\langle\langle\mathscr{X}\rangle\rangle)$$

of the free monoid $\mathscr{X}^*$ on $\mathscr{X}$. The *recursive closure* $\overline{A}$ of a power series A is the vector space spanned by its orbit $\rho(\mathscr{X}^*)A$ under $\rho(\mathscr{X}^*)$. We call the dimension $\dim \overline{A}$ of $\overline{A}$ the *complexity* of A.

We call a subspace $\mathscr{A} \subset \mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$ *recursively closed* if it contains the recursive closure of all its elements.

Rational series coincide with series of finite complexity by a theorem of Schützenberger [Berstel and Reutenauer 1988, Theorem 1].

Remark 9.1. In the case of one variable, the complexity $\dim \overline{A}$ of a reduced nonzero rational fraction $A = f/g$ with $f \in \mathbb{K}[X]$ and $g \in 1 + X\mathbb{K}[X]$ equals $\dim \overline{A} = \max(1 + \deg f, \deg g)$.

Remark 9.2. The (generalized) *Hankel matrix* $H = H(A)$ of

$$A = \sum_{\boldsymbol{X}\in\mathscr{X}^*} (A, \boldsymbol{X})\boldsymbol{X} \in \mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$$

is the infinite matrix with rows and columns indexed by the free monoid $\mathscr{X}^*$ of monomials and entries $H_{\boldsymbol{XX}'} = (A, \boldsymbol{XX}')$. The rank of H is given by the complexity $\dim \overline{A}$ of A, and $\overline{A}$ corresponds to the column-span of H.

Given subspaces $\mathscr{A}, \mathscr{B}$ of $\mathbb{K}\langle\langle\mathscr{X}\rangle\rangle$, we denote by $\mathscr{A} \sqcup\!\sqcup \mathscr{B}$ the vector space spanned by all products $A \sqcup\!\sqcup B$ with $A \in \mathscr{A}$ and $B \in \mathscr{B}$.

Proposition 9.3. *We have the inclusion* $\overline{A \sqcup\!\sqcup B} \subset \overline{A} \sqcup\!\sqcup \overline{B}$ *for the shuffle product* $A \sqcup\!\sqcup B$ *of* $A, B \in \mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$.

Corollary 9.4 [Fliess 1974, Proposition 4]. *We have*

$$\dim(\overline{A \sqcup\!\sqcup B}) \leq \dim \overline{A}\ \dim \overline{B}$$

for the shuffle product $A \sqcup\!\sqcup B$ *of* $A, B \in \mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$. *In particular, shuffle products of rational elements in* $\mathbb{K}\langle\langle X_1, \ldots, X_k\rangle\rangle$ *are rational.*

Proof of Proposition 9.3. For $Y \in \bar{A}$, $Z \in \bar{B}$ and X in $\{X_1, \dots, X_k\}$, the recursive definition of the shuffle product given in Section 8 shows

$$\rho(X)(Y \sqcup\!\sqcup Z) = (\rho(X)Y) \sqcup\!\sqcup Z + Y \sqcup\!\sqcup (\rho(X)Z).$$

We thus have the inclusions $\rho(X)(Y \sqcup\!\sqcup Z) \in \bar{A} \sqcup\!\sqcup Z + Y \sqcup\!\sqcup \bar{B} \subset \bar{A} \sqcup\!\sqcup \bar{B}$, which show that the vector space $\bar{A} \sqcup\!\sqcup \bar{B}$ is recursively closed. Proposition 9.3 follows now from the inclusion $A \sqcup\!\sqcup B \in \bar{A} \sqcup\!\sqcup \bar{B}$. □

Remark 9.5. Similar arguments show that the set of rational elements in $\mathbb{K}\langle\langle X_1, \dots, X_k\rangle\rangle$ is also closed under the ordinary product (and multiplicative inversion of invertible series), Hadamard product and composition (where one considers $A \circ (B_1, \dots, B_k)$ with $A \in \mathbb{K}\langle\langle X_1, \dots, X_k\rangle\rangle$ and $B_1, \dots, B_k \in \mathfrak{m} \subset \mathbb{K}\langle\langle X_1, \dots, X_k\rangle\rangle$).

Remark 9.6. The shuffle inverse of a rational element in $\mathbb{K}^* + \mathfrak{m}$ is in general not rational in characteristic 0. An exception is given by geometric progressions

$$\left(1 - \sum_{j=1}^{k} \lambda_j X_j\right)^{-1} = \sum_{n=0}^{\infty} \left(\sum_{j=1}^{k} \lambda_j X_j\right)^n,$$

since we have

$$\frac{1}{1-\sum_{j=1}^{k} \lambda_j X_j} \sqcup\!\sqcup \frac{1}{1-\sum_{j=1}^{k} \mu_j X_j} = \frac{1}{1-\sum_{j=1}^{k} (\lambda_j+\mu_j) X_j}$$

corresponding to $e^{\lambda X} e^{\mu X} = e^{(\lambda+\mu)X}$ in the one-variable case.

There are no other such elements in $1 + \mathfrak{m} \subset \mathbb{K}[[X]]$; see Remark 4.2. I do not know whether the maximal rational shuffle subgroup of $1 + \mathfrak{m} \subset \mathbb{C}\langle\langle X_1, \dots, X_k\rangle\rangle$ (defined as the set of all rational elements in $1 + \mathfrak{m}$ with rational inverse for the shuffle product) contains other elements if $k \geq 2$.

Remark 9.7. Any finite set of rational elements in $\mathbb{K}\langle\langle X_1, \dots, X_k\rangle\rangle$ over a field $\mathbb{K}$ of positive characteristic is included in a unique minimal finite-dimensional recursively closed subspace of $\mathbb{K}\langle\langle X_1, \dots, X_k\rangle\rangle$ that intersects the shuffle group $(\mathbb{K}^* + \mathfrak{m}, \sqcup\!\sqcup)$ in a subgroup.

10. Main result for generating series in noncommuting variables

The following statement is our main result in a noncommutative framework.

Theorem 10.1. *Let $\mathbb{K}$ be a subfield of $\overline{\mathbb{F}}_p$. Given a noncommutative formal power series $A \in \mathfrak{m} \subset \mathbb{K}\langle\langle \mathcal{X}\rangle\rangle$, the following two assertions are equivalent*:

- *A is rational.*
- $\exp_!$ *A is rational.*

More precisely, we have for a rational series A in $\mathfrak{m}$ the inequalities

$$\dim \overline{\log_!(1+A)} \leq 1 + \left(\dim \overline{1+A}\right)^p$$

and

$$\dim \overline{\exp_! A} \leq p^{q^{\dim \bar{A}}},$$

where $q = p^e$ is the cardinality of a finite field $\mathbb{F}_q$ containing all coefficients of A.

Proof. The identity

$$\log_!(1+A) = \sum_{X \in \mathcal{X}} \left((1+A)^{\sqcup\!\sqcup^{p-1}} \sqcup\!\sqcup \rho(X)A \right) X$$

and Corollary 9.4 show

$$\dim \overline{\log_!(1+A)} \leq 1 + \left(\dim \overline{1+A}\right)^p.$$

For the opposite direction we denote by $\mathbb{K} = \mathbb{F}_q$ a finite subfield of $\overline{\mathbb{F}}_p$ containing all coefficients of A. We have

$$\overline{\exp_! A} \subset \exp_! A \sqcup\!\sqcup \mathbb{K}[\Gamma(A)],$$

where $\mathbb{K}[\Gamma(A)]$ is the shuffle subalgebra of dimension at most $p^{q^{\dim \bar{A}}}$ spanned by all elements of the group Γ generated by all elements of the form

$$(\bar{A} + \mathbb{K}) \cap (1 + \mathfrak{m}).$$

This implies the inequality $\dim \overline{\exp_! A} \leq p^{q^{\dim \bar{A}}}$, which ends the proof. □

Acknowledgements

I thank Jean-Paul Allouche, Michel Brion, Alexei Panchishkin, Tanguy Rivoal, Boris Venkov and an anonymous referee for their interest and helpful remarks.

References

[Allouche and Shallit 2003] J.-P. Allouche and J. Shallit, *Automatic sequences*, Cambridge University Press, 2003. MR 2004k:11028 Zbl 1086.11015

[Bacher 2006] R. Bacher, "La suite de Thue–Morse et la catégorie Rec", *C. R. Math. Acad. Sci. Paris* **342**:3 (2006), 161–164. MR 2006g:11050 Zbl 1148.11012

[Bacher 2008] R. Bacher, "Determinants related to Dirichlet characters modulo 2, 4 and 8 of binomial coefficients and the algebra of recurrence matrices", *Internat. J. Algebra Comput.* **18**:3 (2008), 535–566. MR 2009c:15006 Zbl 1190.15005

[Berstel and Reutenauer 1988] J. Berstel and C. Reutenauer, *Rational series and their languages*, EATCS Monographs on Theoretical Computer Science **12**, Springer, Berlin, 1988. Revised edition available at http://tagh.de/tom/wp-content/uploads/berstelreutenauer2008.pdf. MR 90e:68054 Zbl 0668.68005

[Berthelot and Ogus 1978] P. Berthelot and A. Ogus, *Notes on crystalline cohomology*, Princeton University Press, 1978. MR 58 #10908 Zbl 0383.14010

[Cartier 2002] P. Cartier, "Fonctions polylogarithmes, nombres polyzêtas et groupes pro-unipotents", pp. 137–173 in *Séminaire Bourbaki* 2000/2001 (Exposé 885), Astérisque **282**, Soc. Mat. de France, Paris, 2002. MR 2004i:19005

[Christol 1979] G. Christol, "Ensembles presque periodiques k-reconnaissables", *Theoret. Comput. Sci.* **9**:1 (1979), 141–145. MR 80e:68141 Zbl 0402.68044

[Comtet 1970] L. Comtet, *Analyse combinatoire, II*, Le Mathématicien **5**, Presses Universitaires de France, Paris, 1970. MR 41 #6697 Zbl 0221.05002

[Fliess 1974] M. Fliess, "Sur divers produits de séries formelles", *Bull. Soc. Math. France* **102** (1974), 181–191. MR 50 #7125 Zbl 0313.13021

[Hurwitz 1899] A. Hurwitz, "Über die Entwickelungscoefficienten der lemniskatischen Functionen", *Math. Ann.* **51** (1899), 196–226. JFM 29.0385.02

[Lucas 1878] E. Lucas, "Sur les congruences des nombres eulériens et les coefficients différentiels des fonctions trigonométriques suivant un module premier", *Bull. Soc. Math. France* **6** (1878), 49–54. MR 1503769 JFM 10.0139.04

[Nekrashevych 2005] V. Nekrashevych, *Self-similar groups*, Mathematical Surveys and Monographs **117**, American Mathematical Society, Providence, RI, 2005. MR 2006e:20047 Zbl 1087.20032

[Reutenauer 1993] C. Reutenauer, *Free Lie algebras*, London Mathematical Society Monographs. New Series **7**, Oxford University Press, 1993. MR 94j:17002 Zbl 0798.17001

[Roby 1963] N. Roby, "Lois polynomes et lois formelles en théorie des modules", *Ann. Sci. École Norm. Sup.* (3) **80** (1963), 213–348. MR 28 #5091 Zbl 0117.02302

[Roby 1965] N. Roby, "Les algèbres à puissances divisées", *Bull. Sci. Math.* (2) **89** (1965), 75–91. MR 33 #1348 Zbl 0145.04503

[Stanley 1999] R. P. Stanley, *Enumerative combinatorics, II*, Cambridge Studies in Advanced Mathematics **62**, Cambridge University Press, 1999. MR 2000k:05026 Zbl 0928.05001

[Zagier 1994] D. Zagier, "Values of zeta functions and their applications", pp. 497–512 in *First European Congress of Mathematics* (Paris, 1992), vol. 2, edited by A. Joseph et al., Progr. Math. **120**, Birkhäuser, Basel, 1994. MR 96k:11110 Zbl 0822.11001

Communicated by Hendrik W. Lenstra
Received 2009-08-24 Revised 2010-07-13 Accepted 2010-10-17

Roland.Bacher@ujf-grenoble.fr *Université Grenoble I, CNRS UMR 5582, Institut Fourier, 100, rue des Maths, Boîte Postale 74, 38402 St. Martin d'Hères, France*

Algebra & Number Theory

www.jant.org

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Georgia Benkart	University of Wisconsin, Madison, USA	Susan Montgomery	University of Southern California, USA
Dave Benson	University of Aberdeen, Scotland	Shigefumi Mori	RIMS, Kyoto University, Japan
Richard E. Borcherds	University of California, Berkeley, USA	Andrei Okounkov	Princeton University, USA
John H. Coates	University of Cambridge, UK	Raman Parimala	Emory University, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Victor Reiner	University of Minnesota, USA
Brian D. Conrad	University of Michigan, USA	Karl Rubin	University of California, Irvine, USA
Hélène Esnault	Universität Duisburg-Essen, Germany	Peter Sarnak	Princeton University, USA
Hubert Flenner	Ruhr-Universität, Germany	Michael Singer	North Carolina State University, USA
Edward Frenkel	University of California, Berkeley, USA	Ronald Solomon	Ohio State University, USA
Andrew Granville	Université de Montréal, Canada	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Joseph Gubeladze	San Francisco State University, USA	J. Toby Stafford	University of Michigan, USA
Ehud Hrushovski	Hebrew University, Israel	Bernd Sturmfels	University of California, Berkeley, USA
Craig Huneke	University of Kansas, USA	Richard Taylor	Harvard University, USA
Mikhail Kapranov	Yale University, USA	Ravi Vakil	Stanford University, USA
Yujiro Kawamata	University of Tokyo, Japan	Michel van den Bergh	Hasselt University, Belgium
János Kollár	Princeton University, USA	Marie-France Vignéras	Université Paris VII, France
Hendrik W. Lenstra	Universiteit Leiden, The Netherlands	Kei-Ichi Watanabe	Nihon University, Japan
Yuri Manin	Northwestern University, USA	Andrei Zelevinsky	Northeastern University, USA
Barry Mazur	Harvard University, USA	Efim Zelmanov	University of California, San Diego, USA

PRODUCTION

ant@mathscipub.org

Silvio Levy, Scientific Editor

Andrew Levy, Production Editor

See inside back cover or www.jant.org for submission instructions.

The subscription price for 2010 is US $140/year for the electronic version, and $200/year (+$30 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA.

Algebra & Number Theory (ISSN 1937-0652) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

http://www.mathscipub.org

A NON-PROFIT CORPORATION

Typeset in LaTeX

Copyright ©2010 by Mathematical Sciences Publishers

Algebra & Number Theory

Volume 4 No. 7 2010