A POLYNOMIAL BASIS FOR THE STUFFLE ALGEBRA AND ITS APPLICATIONS

TUAN NGO DAC, GIA VUONG NGUYEN CHU, AND LAN HUONG PHAM

Abstract. In this paper we construct a polynomial basis for the stuffle algebra over a field of characteristic $p > 0$. As an application we derive the transcendence degree for multiple zeta values in positive characteristic of small weights. To our knowledge, the only known result is the case of weight 2 which was proved by Mishiba using a completely different approach.

Contents

1. Introduction

1.1. Motivation.

Classically multiple zeta values were introduced and studied by Euler [12] two centuries ago. After the seminal paper of Zagier [38], these objects have been actively studied in various areas of mathematics and physics such as arithmetic geometry, knot invariants, quantum field theory and Witten's zeta functions (see [6, 38] for further details and references). Surprisingly, there are several connections with the well-known shuffle algebra and the stuffle algebra as explained in [15, 17], leading to the influential conjecture of Ihara-Kaneko-Zagier [17] (see for example [16, 30] for further developments). The algebraic structure of these algebras were well understood by the work of Chen-Fox-Lyndon [9], Hoffman [16], Radford [31] among others. In particular, Lyndon words appearing in [9, 31] are the key term in the study of MZV's (e.g., [2, 4, 10]).

According to Weil [37], Iwasawa [22] and Mazur-Wiles [25] there is a well established analogy between number fields and function fields. From now on we will switch to the function field setting. The above story has an analog in this setting:

Date: March 9, 2024.
2010 *Mathematics Subject Classification.* Primary 11M32; Secondary 16T30, 11J93, 11M38.
Key words and phrases. the stuffle algebra, the shuffle algebra, multiple zeta values, transcendence degree.

if $A = \mathbb{F}_q[\theta]$ denotes the ring of regular functions over the affine line over a finite field $\mathbb{F}_q$ of positive characteristic $p > 0$ and K its fraction field, then Carlitz [7] and Thakur [34] introduced the notion of zeta values and MZV's attached to A. Although the connection with an analog of the shuffle algebra was known, to our knowledge, the connection with the stuffle algebra was recently discovered in [18] based on the work of the first author [28]. The study of the shuffle algebra in positive characteristic was done by Radford [31]. We note that the structure of the algebra is quite different from that in characteristic zero (see Theorem 3.2.1 of *loc. cit.* for more details).

Theorem 1.1 (Radford)**.** *The shuffle algebra over a field of characteristic $p > 0$ is a truncated polynomial ring.*

1.2. **Main results and plan of the paper.**

In this paper we complete the work of Radford and study the stuffle algebra in positive characteristic. In contrast to Radford's result, we prove (see Theorem 4.1):

Theorem 1.2. *The stuffle algebra over a field of characteristic $p > 0$ is a polynomial algebra over the $p-$adic prime-to-p Lyndon words.*

The proof relies on two key ingredients. The first one is an identity for the pth power of the stuffle product. We mention that this identity is proved in a more general context in [21]. The second ingredient is the study of variants of Lyndon words in positive characteristic. In our approach the connection between $p-$adic prime-to-p Lyndon words and Lyndon words is indirect since we have to use $p-$adic Lyndon words as an intermediate bridge. A crucial point is that we use a non-trivial connection between the stuffle algebra and the shuffle algebra in Proposition 4.2.

Combining the previous theorem with [28, Theorem B and Corollary C] we derive some results for the transcendence degree of MZV's of small weights (see Theorem 5.5):

Theorem 1.3. *We recall that $K = \mathbb{F}_q[\theta]$. Then for all $w < q$ the transcendence degree of the K-algebra generated by MZV's of weight at most w equals $\sum_{i=1}^{w} |\mathcal{D}_i|$ where $|\mathcal{D}_i|$ is given as in Proposition 3.12.*

To our knowledge, the only known result where one can determine the transcendence degree of MZV's of fixed weight w is $w = 2$, derived from the work of Mishiba [26] using the powerful result of Papanikolas [29] and completely different tools from algebraic geometry.

We note that in the classical setting there are no transcendence results for MZV's except for the even zeta values due to Euler and Lindemann (see [6] for more details).

This paper is structured as follows. In Section 2 we introduce the notation, the notion of the stuffle algebra in positive characteristic and prove the main identity in Proposition 4.2. In Section 4.2 we define different variants of Lyndon words and prove the connections between these variants in Proposition 3.10. In Section 4 we prove the main theorem of this paper in Theorem 4.1 which gives an explicit polynomial basis for the stuffle algebra. In Section 5 we derive several applications to the theory of MZV's in positive characteristic.

1.3. **Acknowledgments.**

This project started when the authors participated in the school and workshop "Hopf algebras and applications" held at the Institute of Mathematics in Hanoi (Vietnam) in October 2023. We would like to thank the organizers and the participants for helpful discussions.

2. The stuffle algebra

2.1. Alphabet.

Throughout this paper $\mathbb{N}$ denotes the set of positive integers $\{1, 2, \dots\}$ and $\mathbb{Z}^{\geq 0}$ denotes the set of non-negative integers $\{0, 1, 2, \dots\}$.

Let K be a field of characteristic $p > 0$. Let I be a countable set and $A = \{x_n\}_{n\in I}$ be a set of variables indexed by I, equipped with weights $w(x_n) \in \mathbb{N}$. The set A will be called an alphabet and its elements are called letters. A word over the alphabet A is a finite string of letters. In particular, the empty word is denoted by 1. Let $\mathfrak{a} = x_{a_1} \dots x_{a_k}$ be a word. Then the depth of $\mathfrak{a}$ denoted by $\mathrm{depth}(\mathfrak{a})$ is k and by convention $\mathrm{depth}(1) = 0$. The weight of $\mathfrak{a}$ denoted by $w(\mathfrak{a})$ equals $a_1 + \dots + a_k$ and we set $w(1) = 0$. Let $\langle A\rangle$ denote the set of all words over A. We endow $\langle A\rangle$ with the concatenation product defined by the following formula:

$$x_{i_1} \dots x_{i_n} \cdot x_{j_1} \dots x_{j_m} = x_{i_1} \dots x_{i_n} x_{j_1} \dots x_{j_m}.$$

Let $K\langle A\rangle$ be the free K-vector space with basis $\langle A\rangle$. The concatenation product extends to $K\langle A\rangle$ by linearity. For a letter $x_a \in A$ and an element $\mathfrak{a} \in K\langle A\rangle$, we simply write $x_a\mathfrak{a}$ instead of $x_a \cdot \mathfrak{a}$. For each non-empty word $\mathfrak{a} \in \langle A\rangle$, we can write $\mathfrak{a} = x_a\mathfrak{a}_-$ where x_a is the first letter of $\mathfrak{a}$ and $\mathfrak{a}_-$ is the word obtained from $\mathfrak{a}$ by removing x_a.

2.2. The stuffle algebra.

From now on the set I will be $\mathbb{N}$ and we denote by $A = \{x_n\}_{n\in\mathbb{N}}$ with weight $w(x_n) = n$ the alphabet attached to the MZV's. We set $\mathfrak{A} = K\langle A\rangle$ which is the free K-vector space with basis $\langle A\rangle$.

We recursively define two products on $\mathfrak{A}$ as K-bilinear maps

$$\diamond\colon \mathfrak{A} \times \mathfrak{A} \longrightarrow \mathfrak{A} \quad \text{and} \quad *\colon \mathfrak{A} \times \mathfrak{A} \longrightarrow \mathfrak{A}$$

by setting $1 \diamond \mathfrak{a} = \mathfrak{a} \diamond 1 = \mathfrak{a}, 1 * \mathfrak{a} = \mathfrak{a} * 1 = \mathfrak{a}$ and

$$\begin{aligned} \mathfrak{a} \diamond \mathfrak{b} &= x_{a+b}(\mathfrak{a}_- * \mathfrak{b}_-), \\ \mathfrak{a} * \mathfrak{b} &= \mathfrak{a} \diamond \mathfrak{b} + x_a(\mathfrak{a}_- * \mathfrak{b}) + x_b(\mathfrak{a} * \mathfrak{b}_-) \end{aligned}$$

for any non-empty words $\mathfrak{a}, \mathfrak{b} \in \langle A\rangle$. We call $\diamond$ the diamond product and $*$ the stuffle product. The unit $u : K \to \mathfrak{A}$ is given by sending 1 to the empty word. We can show that the spaces $(\mathfrak{A}, \diamond)$ and $(\mathfrak{A}, *)$ are commutative K-algebras (see for example [6, 15]).

2.3. Powers of the stuffle product.

In this section we prove some identities for powers of the stuffle product. We borrow these results from [21] where they still hold in a more general setting. We introduce the triangle product as follows: for any non-empty word $\mathfrak{a}$ and any word $\mathfrak{b}$ we write

$$\mathfrak{a} \triangleright \mathfrak{b} = x_a(\mathfrak{a}_- * \mathfrak{b}).$$

With this notation we can easily see that

$$\mathfrak{a} * \mathfrak{b} = \mathfrak{a} \diamond \mathfrak{b} + \mathfrak{a} \triangleright \mathfrak{b} + \mathfrak{b} \triangleright \mathfrak{a}.$$

We recall some properties of the different products $\triangleright$, $\diamond$ and $*$ by the following lemma.

Lemma 2.1. *Let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \in \mathfrak{A}$ be non-empty words, then*

1) $(\mathfrak{a} \triangleright \mathfrak{b}) \triangleright \mathfrak{c} = (\mathfrak{a} \triangleright \mathfrak{c}) \triangleright \mathfrak{b} = \mathfrak{a} \triangleright (\mathfrak{b} * \mathfrak{c})$.
2) $(\mathfrak{a} \diamond \mathfrak{b}) \triangleright \mathfrak{c} = \mathfrak{a} \diamond (\mathfrak{b} \triangleright \mathfrak{c}) = (\mathfrak{a} \triangleright \mathfrak{c}) \diamond \mathfrak{b}$.

Proof. We use the associativity of $(\mathfrak{A}, \diamond)$ and $(\mathfrak{A}, *)$. For Part 1 we have

$$(\mathfrak{a} \triangleright \mathfrak{b}) \triangleright \mathfrak{c} = (x_a(\mathfrak{a}_- * \mathfrak{b})) \triangleright \mathfrak{c} = x_a((\mathfrak{a}_- * \mathfrak{b}) * \mathfrak{c}) = x_a(\mathfrak{a}_- * \mathfrak{b} * \mathfrak{c}).$$

Similarly, $(\mathfrak{a} \triangleright \mathfrak{c}) \triangleright \mathfrak{b} = \mathfrak{a} \triangleright (\mathfrak{b} * \mathfrak{c}) = x_a(\mathfrak{a}_- * \mathfrak{b} * \mathfrak{c})$. This completes Part 1.

For Part 2 we write

$$(\mathfrak{a} \diamond \mathfrak{b}) \triangleright \mathfrak{c} = ((x_a \diamond x_b)(\mathfrak{a}_- * \mathfrak{b}_-)) \triangleright \mathfrak{c} = (x_a \diamond x_b)(\mathfrak{a}_- * \mathfrak{b}_- * \mathfrak{c}).$$

Similarly, $\mathfrak{a} \diamond (\mathfrak{b} \triangleright \mathfrak{c}) = (\mathfrak{a} \triangleright \mathfrak{c}) \diamond \mathfrak{b} = (x_a \diamond x_b)(\mathfrak{a}_- * \mathfrak{b}_- * \mathfrak{c})$. Part 2 follows. □

Let $\mathfrak{a}$ be a word, $n \in \mathbb{N}$. We write two nth powers of $\mathfrak{a}$ as follows:

$$\mathfrak{a}^{*n} = \mathfrak{a} * \cdots * \mathfrak{a}, \quad \mathfrak{a}^{\diamond n} = \mathfrak{a} \diamond \cdots \diamond \mathfrak{a} \quad (n \text{ times}).$$

The next lemma will be useful in the sequel.

Lemma 2.2. *For $a_1, a_2, \ldots, a_n \in \mathbb{N}$ and $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n \in \langle A \rangle$, we have*

$$x_{a_1}\mathfrak{a}_1 \diamond x_{a_2}\mathfrak{a}_2 \diamond \cdots \diamond x_{a_n}\mathfrak{a}_n = (x_{a_1} \diamond x_{a_2} \diamond \cdots \diamond x_{a_n}) \triangleright (\mathfrak{a}_1 * \mathfrak{a}_2 * \cdots * \mathfrak{a}_n).$$

Proof. We proceed the proof by induction on n. The case $n = 1$ is trivial. We assume that the lemma holds for $n \in \mathbb{N}$. We need to show that Lemma 2.2 holds for $n + 1$. It follows from the induction hypothesis that

$$\begin{aligned} x_{a_1}\mathfrak{a}_1 \diamond \cdots \diamond x_{a_{n+1}}\mathfrak{a}_{n+1} &= (x_{a_1} \diamond \cdots \diamond x_{a_n})(\mathfrak{a}_1 * \cdots * \mathfrak{a}_n) \diamond x_{a_{n+1}}\mathfrak{a}_{n+1} \\ &= (x_{a_1} \diamond \cdots \diamond x_{a_n} \diamond x_{a_{n+1}}) \triangleright (\mathfrak{a}_1 * \cdots * \mathfrak{a}_n * \mathfrak{a}_{n+1}). \end{aligned}$$

This proves the lemma. □

We will introduce some new notations. Let $\mathfrak{a} \in \langle A \rangle$ be a non-empty word and let $n_1, n_2, \ldots, n_k \in \mathbb{N}$. We define recursively

$$\mathfrak{a}_{(n_1)} = \mathfrak{a}^{\diamond n_1} = \underbrace{\mathfrak{a} \diamond \mathfrak{a} \cdots \diamond \mathfrak{a}}_{n_1 \text{ times}},$$

$$\mathfrak{a}_{(n_1, n_2, \ldots, n_k)} = \mathfrak{a}_{(n_1)} \triangleright \mathfrak{a}_{(n_2, \ldots, n_k)}.$$

We note that $\mathfrak{a}_{(1)} = \mathfrak{a}$.

In what follows for $s \in \mathbb{N}$ and $m \in \mathbb{N}$, we denote by $s^{\{m\}}$ the sequence of length m with all terms equal to s. We agree by convention that $s^{\{0\}}$ is the empty sequence.

Lemma 2.3. *Let $\mathfrak{a} \in \langle A \rangle$ be a non-empty word. For $n_1, n_2, \ldots, n_k \in \mathbb{N}$, we have*

$$\begin{aligned} \mathfrak{a}_{(n_1, n_2, \ldots, n_k)} * \mathfrak{a}_{(1)} &= \mathfrak{a}_{(1, n_1, n_2, \ldots, n_k)} + \mathfrak{a}_{(n_1+1, n_2, \ldots, n_k)} \\ &+ \sum_{i=1}^{k} \mathfrak{a}_{(n_1, \ldots, n_i, 1, n_{i+1}, \ldots, n_k)} + \sum_{i=2}^{k} \mathfrak{a}_{(n_1, \ldots, n_{i-1}, n_i+1, n_{i+1}, \ldots, n_k)}. \end{aligned}$$

Proof. We proceed the proof by induction on $k \in \mathbb{N}$. It follows from the definition that

$$\begin{aligned}\mathfrak{a}_{(n_1)} * \mathfrak{a}_{(1)} &= \mathfrak{a}_{(n_1)} \diamond \mathfrak{a}_{(1)} + \mathfrak{a}_{(n_1)} \triangleright \mathfrak{a}_{(1)} + \mathfrak{a}_{(1)} \triangleright \mathfrak{a}_{(n_1)} \\ &= \mathfrak{a}_{(n_1+1)} + \mathfrak{a}_{(n_1)}\mathfrak{a}_{(1)} + \mathfrak{a}_{(1)}\mathfrak{a}_{(n_1)}.\end{aligned}$$

Hence the lemma holds for $k = 1$.

We assume that Lemma 2.3 holds for $k \geq 1$. We need to show that the lemma holds for $k+1$. In fact, we have

$$\begin{aligned}&\mathfrak{a}_{(n_1,n_2,\ldots,n_{k+1})} * \mathfrak{a}_{(1)} \\ &= \mathfrak{a}_{(n_1,n_2,\ldots,n_{k+1})} \diamond \mathfrak{a}_{(1)} + \mathfrak{a}_{(1)} \triangleright \mathfrak{a}_{(n_1,n_2,\ldots,n_{k+1})} + \mathfrak{a}_{(n_1,n_2,\ldots,n_{k+1})} \triangleright \mathfrak{a}_{(1)} \\ &= \mathfrak{a}_{(n_1,n_2,\ldots,n_{k+1})} \diamond \mathfrak{a}_{(1)} + \mathfrak{a}_{(1,n_1,n_2,\ldots,n_{k+1})} + \mathfrak{a}_{(n_1,n_2,\ldots,n_{k+1})} \triangleright \mathfrak{a}_{(1)}.\end{aligned}$$

It follows from Lemma 2.1 that

$$\begin{aligned}\mathfrak{a}_{(n_1,n_2,\ldots,n_{k+1})} \triangleright \mathfrak{a}_{(1)} &= \big(\mathfrak{a}_{(n_1)} \triangleright \mathfrak{a}_{(n_2,\ldots,n_{k+1})}\big) \triangleright \mathfrak{a}_{(1)} \\ &= \mathfrak{a}_{(n_1)} \triangleright \big(\mathfrak{a}_{(n_2,\ldots,n_{k+1})} * \mathfrak{a}_{(1)}\big).\end{aligned}$$

Again by Lemma 2.1,

$$\begin{aligned}\mathfrak{a}_{(n_1,n_2,\ldots,n_{k+1})} \diamond \mathfrak{a}_{(1)} &= \big(\mathfrak{a}_{(n_1)} \triangleright \mathfrak{a}_{(n_2,\ldots,n_{k+1})}\big) \diamond \mathfrak{a}_{(1)} \\ &= \big(\mathfrak{a}_{(n_1)} \diamond \mathfrak{a}_{(1)}\big) \triangleright \mathfrak{a}_{(n_2,\ldots,n_{k+1})} \\ &= \mathfrak{a}_{(n_1+1)} \triangleright \mathfrak{a}_{(n_2,\ldots,n_{k+1})} \\ &= \mathfrak{a}_{(n_1+1,n_2,\ldots,n_{k+1})}.\end{aligned}$$

It follows from the induction hypothesis that

$$\begin{aligned}\mathfrak{a}_{(n_2,\ldots,n_{k+1})} * \mathfrak{a}_{(1)} &= \mathfrak{a}_{(1,n_2,\ldots,n_{k+1})} + \mathfrak{a}_{(n_2+1,n_3,\ldots,n_{k+1})} \\ &+ \sum_{i=2}^{k+1} \mathfrak{a}_{(n_2,\ldots,n_i,1,n_{i+1},\ldots,n_{k+1})} + \sum_{i=3}^{k+1} \mathfrak{a}_{(n_2,\ldots,n_{i-1},n_i+1,n_{i+1},\ldots,n_{k+1})}.\end{aligned}$$

Putting it all together gives the lemma. □

Proposition 2.4. *For any word $\mathfrak{a} \in \langle A \rangle$, we have*

$$\mathfrak{a}^{*n} = \underbrace{\mathfrak{a} * \mathfrak{a} * \cdots * \mathfrak{a}}_{n \text{ times}} = \sum_{(n_1,n_2,\ldots,n_k) \in A_n} \binom{n}{n_1,\ldots,n_k} \mathfrak{a}_{(n_1,n_2,\ldots,n_k)}$$

where

$$A_n = \{(n_1,\ldots,n_k) \in \mathbb{N}^k \mid k \in \mathbb{N},\ n_1 + \cdots + n_k = n\}.$$

Proof. We proceed the proof by induction on $n \in \mathbb{N}$. We see that the lemma holds for $n = 1$. We assume that Lemma 2.4 holds for $n \in \mathbb{N}$. We need to show that the lemma holds for $n+1$. In fact, we let $k \in \mathbb{N}$ and $(s_1,\ldots,s_k) \in A_{n+1}$ and set

$$\begin{aligned}J' &= \{j \in \{1,2,\ldots,k\} \mid s_j > 1\}, \\ J &= \{1,2,\ldots,k\} \setminus J'.\end{aligned}$$

If $J' = \emptyset$, then $k = n+1$ and $(s_1, s_2, \dots, s_k) = (\underbrace{1, 1, \dots, 1}_{n+1 \text{ times}}) = 1^{\{n+1\}}$. It follows from Lemma 2.3 that

$$\mathfrak{a}_{1^{\{n\}}} * \mathfrak{a}_{(1)} = (n+1)\mathfrak{a}_{1^{\{n+1\}}} + \mathfrak{a}_{2,1^{\{n-1\}}} + \sum_{j=1}^{n} \mathfrak{a}_{(1^{\{j\}},2,1^{\{n-j\}})}.$$

Thus $\mathfrak{a}_{1^{\{n+1\}}}$ appears in the expression of the stuffle product $\mathfrak{a}^{*(n+1)}$ with the coefficient $c_{1^{\{n+1\}}} = (n+1).n! = (n+1)!$.

If $J' \neq \emptyset$, then we assume that $J' = \{j_1, j_2, \dots, j_m\}$ for some $m \in \mathbb{N}$. It follows from the definition that $(s_1, s_2, \dots, s_{j_1-1}, s_{j_1} - 1, s_{j_1+1}, \dots, s_k) \in A_n$ and by using Lemma 2.3 again we obtain

$$\mathfrak{a}_{(s_1,s_2,\dots,s_{j_1-1},s_{j_1}-1,s_{j_1+1},\dots,s_k)} * \mathfrak{a}_{(1)} = \mathfrak{a}_{(s_1,s_2,\dots,s_{j_1-1},s_{j_1},s_{j_1+1},\dots,s_k)} + \text{ other terms.}$$

Thus $\mathfrak{a}_{(s_1,\dots,s_{j_1-1},s_{j_1},s_{j_1+1},\dots,s_k)}$ appears in the expansion of $\mathfrak{a}_{(s_1,\dots,s_{j_1-1},s_{j_1}-1,s_{j_1+1},\dots,s_k)} * \mathfrak{a}_{(1)}$. Similarly, we see that $\mathfrak{a}_{(s_1,\dots,s_{j_i-1},s_{j_i},s_{j_i+1},\dots,s_k)}$ appears in $\mathfrak{a}_{(s_1,\dots,s_{j_i-1},s_{j_i}-1,s_{j_i+1},\dots,s_k)} * \mathfrak{a}_{(1)}$ for all i. From the induction hypothesis and Lemma 2.3, we derive the coefficient

$$\begin{aligned} c_{s_1,s_2,\dots,s_k} &= \binom{n}{s_1, s_2, \dots, s_{j_1-1}, s_{j_1} - 1, s_{j_1+1}, \dots, s_k} + \cdots + \\ &\quad + \binom{n}{s_1, s_2, \dots, s_{j_m-1}, s_{j_m} - 1, s_{j_m+1}, \dots, s_k} + \binom{n}{s_1, s_2, \dots, s_k} |J| \\ &= \binom{n+1}{s_1, s_2, \dots, s_k}. \end{aligned}$$

The last equality follows from the fact that $s_1 + \cdots + s_k = n+1$. This completes the proof. □

As a corollary we get

Corollary 2.5. *For all words $\mathfrak{a} \in \langle A \rangle$, we have*

$$\mathfrak{a}^{*p} = \mathfrak{a}_{(p)} = \mathfrak{a}^{\diamond p}.$$

Proof. We apply Lemma 2.3 for $n = p$. As we are working over the field K of characteristic p, all the coefficients except c_p vanish. Thus the corollary follows. □

Definition 2.6. Let $\mathfrak{a} = x_{a_1} \dots x_{a_n}$ be a word. We define $\mathfrak{a} \star p$ as the word $x_{pa_1} \dots x_{pa_n}$.

The main result of this sections is as follows.

Proposition 2.7. *For all words $\mathfrak{a} \in \langle A \rangle$, we have*

$$\mathfrak{a}^{*p} = \mathfrak{a} \star p.$$

Proof. The proof is by induction on the weight $w = w(\mathfrak{a})$.

For $w = 1$, we see that Proposition 2.7 holds by using Corollary 2.5 and the definition of the diamond product

$$x_1^{*p} = x_1^{\diamond p} = x_1 \star p.$$

For the induction step let w be an integer strictly greater than 1. We suppose that for all $\mathfrak{a} \in \langle A \rangle$ such that $w(\mathfrak{a}) < w$, we have

$$\mathfrak{a}^{*p} = \mathfrak{a} \star p.$$

We now show that for all $\mathfrak{a} \in \langle A \rangle$ with $w(\mathfrak{a}) = w$,

$$\mathfrak{a}^{*p} = \mathfrak{a} \star p.$$

The proof is divided into two cases.

Case 1: If $\mathfrak{a} = x_w$, then Corollary 2.5 and Lemma 2.2 imply

$$x_w^{*p} = x_w^{\diamond p} = x_w \star p.$$

Case 2: If $\mathfrak{a} = x_u \mathfrak{a}_-$ where $u \in \mathbb{N}$ and $\mathfrak{a}_- \in \langle A \rangle$, then by Corollary 2.5 and Lemma 2.2, we have

$$\mathfrak{a}^{*p} = \mathfrak{a}^{\diamond p} = (x_u \mathfrak{a}_-)^{\diamond p} = x_u^{\diamond p} \triangleright \mathfrak{a}_-^{\diamond p} = x_u^{*p} \triangleright \mathfrak{a}_-^{*p}.$$

We clearly see that $u < w$ and $w(\mathfrak{a}_-) < w$. It follows from the induction hypothesis that $x_u^{*p} = x_{pu} = x_u \star p$ and $\mathfrak{a}_-^{*p} = \mathfrak{a}_- \star p$. So we get

$$\mathfrak{a}^{*p} = (x_u \star p)(\mathfrak{a}_- \star p) = (x_u \star p)(\mathfrak{a}_- \star p) = (x_u \mathfrak{a}_-) \star p = \mathfrak{a} \star p.$$

The proof is finished. □

3. Lyndon words and variants

In this section we will introduce the notion of Lyndon words. We will study several variants that are useful in positive characteristic.

3.1. **Lyndon words.**

From now on we consider the total order

$$x_1 \succ x_2 \succ x_3 \succ \dots$$

We use the lexicographic order for words with letters in A. For $\mathfrak{a}, \mathfrak{b} \in A$ we also write $\mathfrak{a} \prec \mathfrak{b}$ if $\mathfrak{b} \succ \mathfrak{a}$.

Definition 3.1. We say that a nontrivial word $\mathfrak{s}$ is a Lyndon word if $\mathfrak{s} \prec \mathfrak{s}_1$ for any nontrivial factorization $\mathfrak{s} = \mathfrak{s}_0 \mathfrak{s}_1$.

We denote by $\mathcal{D}$ the set of all Lyndon words.

The famous theorem of Chen-Fox-Lyndon [9] reads

Theorem 3.2. *Every word $\mathfrak{s}$ has a unique factorization into Lyndon words:*

$$\mathfrak{s} = \mathfrak{s}_1 \dots \mathfrak{s}_n$$

where $\mathfrak{s}_1 \succeq \dots \succeq \mathfrak{s}_n$ is a decreasing sequence of Lyndon words.

Henceforth, for any word $\mathfrak{s}$, this factorization is called the Chen-Fox-Lyndon (CFL) factorization of $\mathfrak{s}$.

3.2. **Variants of Lyndon words.**

Definition 3.3. 1) A non-negative integer p-power of a Lyndon word is called a $p-$adic Lyndon word; denote by $\mathcal{D}'$ the set of such words.

2) We say that a non-empty word $\mathfrak{s} = x_{i_1} \dots x_{i_k}$ is prime-to-p if for some $1 \leq j \leq k$ we have $p \nmid x_{i_j}$. We denote by $\mathcal{D}''$ the set of prime-to-p, $p-$adic Lyndon words.

We now define two maps, the $p-$index map and the $p-$reduction map on the set of non-empty words as follows. For any non-empty word $\mathfrak{s} = x_{i_1} x_{i_2} \dots x_{i_n}$, let $\mathrm{ind}_p(\mathfrak{s})$ denote the largest non-negative integer r such that p^r divides each index $i_1, i_2, \dots, i_n$. The $p-$reduction of the word $\mathfrak{s}$ is the word $\mathrm{red}(\mathfrak{s})$ obtained from $\mathfrak{s} = x_{i_1} x_{i_2} \dots x_{i_n}$ by replacing each letter x_{i_k}, $1 \leq k \leq n$, by $x_{i'_k}$ where $i'_k = \frac{i_k}{p^{\mathrm{ind}_p(\mathfrak{s})}}$. We see that the $p-$reduction of a word is a prime-to-p word.

Lemma 3.4. *1) For any non-empty word $\mathfrak{s}$ and positive integer n,* $\mathrm{ind}_p(\mathfrak{s}^n) = \mathrm{ind}_p(\mathfrak{s})$ *and* $\mathrm{red}(\mathfrak{s}^n) = \mathrm{red}(\mathfrak{s})^n$.

2) A word $\mathfrak{s}$ is Lyndon if and only if $\mathrm{red}(\mathfrak{s})$ *is Lyndon.*

3) A word $\mathfrak{s}$ is $p-$adic Lyndon if and only if $\mathrm{red}(\mathfrak{s})$ *is $p-$adic Lyndon.*

Proof. 1) For a non-empty word $\mathfrak{s} = x_{i_1} x_{i_2} \dots x_{i_k}$ and a positive integer n, we have $\mathfrak{s}^n = \underbrace{x_{i_1} x_{i_2} \dots x_{i_k} \dots x_{i_1} x_{i_2} \dots x_{i_k}}_{n \text{ times}}$. By definition, $\mathrm{ind}_p(\mathfrak{s})$ and $\mathrm{ind}_p(\mathfrak{s})^n$ are the exponents of p in the greatest common divisors of $i_1, \dots, i_k$ and $\underbrace{i_1, \dots, i_k, \dots, i_1, \dots, i_k}_{n \text{ times}}$ respectively. But these greatest common divisors are obviously equal, so $\mathrm{ind}_p(\mathfrak{s}^n) = \mathrm{ind}_p(\mathfrak{s})$.

Similarly, if $r = \mathrm{ind}_p(\mathfrak{s}^n) = \mathrm{ind}_p(\mathfrak{s})$ then $\mathrm{red}(\mathfrak{s})$ and $\mathrm{red}(\mathfrak{s}^n)$ are the words obtained from $x_{i_1} x_{i_2} \dots x_{i_k}$ and $\underbrace{x_{i_1} x_{i_2} \dots x_{i_k} \dots x_{i_1} x_{i_2} \dots x_{i_k}}_{n \text{ times}}$ by replacing each letter x_{i_s} by $x_{i'_s}$, where $i'_s = \frac{i_s}{p^r}$. So $\mathrm{red}(\mathfrak{s}^n) = \underbrace{x_{i'_1} x_{i'_2} \dots x_{i'_k} \dots x_{i'_1} x_{i'_2} \dots x_{i'_k}}_{n \text{ times}} = \mathrm{red}(\mathfrak{s})^n$.

2) Let $\mathfrak{s} = x_{i_1} x_{i_2} \dots x_{i_k}$ be a non-empty word with $p-$adic index s; $\mathrm{red}(\mathfrak{s}) = x_{i'_1} x_{i'_2} \dots x_{i'_k}$, where $i'_j = \frac{i_j}{p^s}$ for $1 \leq j \leq k$.

Any nontrivial factorization $\mathfrak{s} = (x_{i_1} \dots x_{i_l})(x_{i_{l+1}} \dots x_k)$, $1 < l < k$, corresponds to a nontrivial factorization $\mathrm{red}(\mathfrak{s}) = (x_{i'_1} x_{i'_2} \dots x_{i'_l})(x_{i'_{l+1}} \dots x_{i'_k})$. Since $i_j = p^s i'_j$ for all $1 \leq j \leq l$, we have $x_{i_{s_1}} \prec x_{i_{s_2}}$ if and only if $x_{i'_{s_1}} \prec x_{i'_{s_2}}$. It follows that $x_{i_1} \dots x_{i_k} \prec x_{i_{l+1}} \dots x_k$ if and only if $x_{i'_1} \dots x_{i'_k} \prec x_{i'_{l+1}} \dots x'_k$. This shows that $\mathfrak{s}$ is Lyndon if and only if $\mathrm{red}(\mathfrak{s})$ is Lyndon.

3) Suppose that $\mathfrak{t}$ is Lyndon and m is a non-negative integer. By Part 1, $\mathrm{red}\left(\mathfrak{t}^{p^m}\right) = (\mathrm{red}(\mathfrak{t}))^{p^m}$ is Lyndon since $\mathrm{red}(\mathfrak{t})$ is Lyndon. Conversely, suppose that $\mathfrak{s}$ is a non-empty word such that $\mathrm{red}(\mathfrak{s}) = \mathfrak{a}^{p^m}$ where $\mathfrak{a}$ is Lyndon and m is a non-negative integer. Set $\mathfrak{b} = \mathfrak{a} \star p^s$, where $s = \mathrm{ind}_p(\mathfrak{s})$. Then we have $\mathrm{red}(\mathfrak{b}) = \mathfrak{a}$, $\mathfrak{s} = \mathfrak{b}^{p^m}$. Since $\mathfrak{a}$ is Lyndon, so is $\mathfrak{b}$. This shows that $\mathfrak{s}$ is $p-$adic Lyndon. □

Remark 3.5. Note that since the $p-$reduction of a non-empty word is a prime-to-p word, the previous lemma implies that the $p-$reduction of a Lyndon word is a prime-to-p Lyndon word. Similarly, the $p-$reduction of a $p-$adic Lyndon word is a prime-to-p, p-adic Lyndon word.

Note that the CFL factorization has the following $p-$adic variant:

Lemma 3.6. *Any non-empty $\mathfrak{s}$ word can be uniquely written as $\mathfrak{s} = \mathfrak{s}_1^{m_1}\mathfrak{s}_2^{m_2}\cdots\mathfrak{s}_n^{m_n}$, where $\mathfrak{s}_1 \succ \mathfrak{s}_2 \succ \cdots \succ \mathfrak{s}_n$ are p-adic Lyndon words and $m_1, m_2, \ldots, m_n$ are positive integers smaller than p.*

This factorization is called the p-adic Chen-Fox-Lyndon factorization of $\mathfrak{s}$.

Proof. Let $\mathfrak{t}$ be a Lyndon word and $m \in \mathbb{N}$. We write the p-adic expansion of m:

$$m = m_0 + m_1 p + \cdots + m_n p^n$$

where $0 \leq m_i < p$ for all i and $m_n \neq 0$. Then the p-adic Chen-Fox-Lyndon factorization of $\mathfrak{t}^m$ is given by

$$\mathfrak{t}^m = (\mathfrak{t}^{p^n})^{m_n} \ldots (\mathfrak{t}^p)^{m_1}\mathfrak{t}^{m_0}.$$

Now for any word $\mathfrak{s}$ we write the Chen-Fox-Lyndon factorization of $\mathfrak{s}$:

$$\mathfrak{s} = \mathfrak{s}_1^{m_1} \ldots \mathfrak{s}_n^{m_n}$$

where $m_i \in \mathbb{N}$ for all i and $\mathfrak{s}_1 \succ \cdots \succ \mathfrak{s}_n$ is a strictly decreasing sequence of Lyndon words. Then the product of the p-adic Chen-Fox-Lyndon factorizations of $\mathfrak{s}_i^{m_i}$ is the p-adic Chen-Fox-Lyndon factorization of $\mathfrak{s}$. □

3.3. **A key bijection.**

In the sequence, we will work with multisets over the sets $\mathcal{D}, \mathcal{D}', \mathcal{D}''$.

Definition 3.7. 1) A multiset over a set S is a function $m\colon S \to \mathbb{Z}^{\geq 0}$ such that its support $\{s \in S \mid m(s) \neq 0\}$ is a finite subset of S. For $s \in S$, $m(s)$ is called the multiplicity of s.

2) A multiset is called $M-$bounbed, where M is a fixed positive integer, if $m(s) < M$ for all s. We denote the sets of multisets and M-bounded multisets over a fixed set S by $\mathrm{Mult}(S)$ and $\mathrm{Mult}_{<M}(S)$ respectively.

The addition of two multisets is the defined in a natural way. For two multisets m_1, m_2 over the same set S, their sum $m_1 + m_2$ is the multiset over S defined by $(m_1 + m_2)(s) = m_1(s) + m_2(s)$ for all $s \in S$. More generally, we can form the sum any finite number of multisets over S. It's obvious that $\mathrm{Mult}(S)$, equipped with this addition law, is a free commutative monoid with basis S.

Usually, a multiset will be written as $\{m_1 \cdot s_1, \ldots, m_n \cdot s_n\}$ where $s_1, s_2, \ldots, s_n$ are elements of its support with the corresponding multiplicities $m_1, m_2, \ldots, m_n$. Sometimes we also use the additive notation for a multiset where $m_1 \cdot s_1 + m_2 \cdot s_2 + \cdots + m_n \cdot s_n$ denotes the sum of the multisets $m_1 \cdot s_1$, $m_2 \cdot s_2$, …, $m_n \cdot s_n$ where $m_i \cdot s_i$, $1 \leq i \leq n$, is the multiset whose the support is the singleton $\{s_i\}$ and the multiplicity of s_i is m_i. More specifically, we use the notation $\{m_1 \cdot s_1, \ldots, m_n \cdot s_n\}$ to emphasize that $s_1, s_2, \ldots, s_n$ are distinct, whereas in the additive notation $m_1 \cdot s_1 + m_2 \cdot s_2 + \cdots + m_n \cdot s_n$ the elements $s_1, s_2, \ldots, s_n$ need not be distinct.

Let $\mathfrak{s} = \mathfrak{s}_1^{m_1}\mathfrak{s}_2^{m_2}\cdots\mathfrak{s}_n^{m_n}$ be the $p-$adic CFL factorization of a non-empty word $\mathfrak{s} \in \langle A \rangle$. We define the multiset $f(\mathfrak{s})$ by

$$f(\mathfrak{s}) = \{m_1 \cdot \mathfrak{s}_1, \ldots, m_n \cdot \mathfrak{s}_n\}.$$

Then $f(\mathfrak{s}) \in \mathrm{Mult}_{<p}(\mathcal{D}')$.

Conversely, for a $p-$bounded multiset m in $\mathrm{Mult}_{<p}(\mathcal{D}')$, we define the word $g(m)$ as follows. We first arrange its elements in decreasing order as $m = \{m_1 \cdot \mathfrak{s}_1, \dots, m_n \cdot \mathfrak{s}_n\}$ so that $1 \leq m_i < p$ for all $i = 1, 2, \dots, n$, and $\mathfrak{s}_1 \succ \mathfrak{s}_2 \succ \cdots \succ \mathfrak{s}_n$, then we set

$$g(m) = \mathfrak{s}_1^{m_1} \mathfrak{s}_2^{m_2} \cdots \mathfrak{s}_n^{m_n}.$$

Obviously $g(m) \in \langle A \rangle$.

We can restate Lemma 3.6 in the following terms.

Corollary 3.8. *The maps $f\colon \langle A \rangle \to \mathrm{Mult}_{<p}(\mathcal{D}')$ and $g\colon \mathrm{Mult}_{<p}(\mathcal{D}') \to \langle A \rangle$ are inverses of each other.*

For a multiset $m = \{m_1 \cdot \mathfrak{s}_1, \dots, m_n \cdot \mathfrak{s}_n\} \in \mathrm{Mult}_{<p}(\mathcal{D}')$, we set

$$F(m) = m_1 p^{\mathrm{ind}_p(\mathfrak{s}_1)} \cdot \mathrm{red}(\mathfrak{s}_1) + \cdots + m_n p^{\mathrm{ind}_p(\mathfrak{s}_n)} \mathrm{red}(\mathfrak{s}_n).$$

Since each $\mathrm{red}(\mathfrak{s}_i)$ belongs to $\mathcal{D}''$, the right hand side defines an element of $\mathrm{Mult}(\mathcal{D}'')$.

Conversely, for a multiset $n = \{n_1 \cdot \mathfrak{t}_1, \dots, n_k \cdot \mathfrak{t}_k\}$ in $\mathrm{Mult}(\mathcal{D}'')$, we define a multiset $G(n)$ in $\mathrm{Mult}_{<p}(\mathcal{D}')$ as follows. For each i, let $n_i = \sum_{j=0}^{+\infty} n_{i,j} p^j$ be the $p-$adic expansion of n_i where $0 \leq n_{i,j} \leq p-1$ and $n_{i,j} = 0$ for all but finitely many j. We then set

$$G(n) = \sum_{i=1}^{k} \sum_{j=0}^{+\infty} n_{i,j} \cdot (\mathfrak{t}_i \star p^j).$$

Note that according to our convention for notating of the multiset $\{n_1 \cdot \mathfrak{t}_1, \dots, n_k \cdot \mathfrak{t}_k\}$, the words $\mathfrak{t}_1, \mathfrak{t}_2, \dots, \mathfrak{t}_k$ are pairwise distinct in $\mathcal{D}''$. It follows that the words $\mathfrak{t}_i \star p^j$ are also pairwise distinct elements of $\mathcal{D}'$ and $0 \leq n_{i,j} < p$, the expression on the right hand side defines a multiset in $\mathrm{Mult}_{<p}(\mathcal{D}')$.

Lemma 3.9. *The maps $F\colon \mathrm{Mult}_{<p}(\mathcal{D}') \to \mathrm{Mult}(\mathcal{D}'')$ and $G\colon \mathrm{Mult}(\mathcal{D}'') \to \mathrm{Mult}_{<p}(\mathcal{D}')$ are inverses of each other.*

Proof. It follows from the definitions of F and G. □

Let us summarize the previous results in the following proposition:

Proposition 3.10. *There are natural bijections between:*

1) *The set of words $\langle A \rangle$;*
2) *The set of $p-$bounded multisets of $p-$adic Lyndon words $\mathrm{Mult}_{<p}(\mathcal{D}')$;*
3) *The set of multisets of prime-to-p, $p-$adic Lyndon words $\mathrm{Mult}(\mathcal{D}'')$.*

Proof. The bijections between $\langle A \rangle$ and $\mathrm{Mult}_{<p}(\mathcal{D}')$ are given by f and g. The bijections between $\mathrm{Mult}_{<p}(\mathcal{D}')$ and $\mathrm{Mult}(\mathcal{D}'')$ are given by F and G. Finally, the bijections between $\langle A \rangle$ and $\mathrm{Mult}(\mathcal{D}'')$ are given by $F \circ f$ and $g \circ G$. □

As a corollary, we get

Corollary 3.11. *For all w we denote by $\mathcal{D}_w$ (resp. $\mathcal{D}'_w, \mathcal{D}''_w$) the set of elements of weight w in $\mathcal{D}$ (resp. $\mathcal{D}', \mathcal{D}''$). Then $|\mathcal{D}_w| = |\mathcal{D}''_w|$.*

3.4. **Number of generators.**

We end this section by recalling the cardinality of $|\mathcal{D}_w|$ for all w. We follow closely the presentation given as in [6, §1.4]. Since $\mathfrak{A}$ is a graded K-algebra with $\mathfrak{A}_0 = K$, we consider its Hilbert-Poincaré series given by

$$H_{\mathfrak{A}}(t) = \sum_{w\geq 0} \dim \mathfrak{A}_w \, t^w.$$

We see that

$$\dim \mathfrak{A}_w = \begin{cases} 1 & \text{if } w = 0, \\ 2^{w-1} & \text{if } w > 0. \end{cases}$$

So

$$H_{\mathfrak{A}}(t) = \frac{1-t}{1-2t}.$$

Next we express the logarithm of $H_{\mathfrak{A}}(t)$ as follows:

$$\log H_{\mathfrak{A}}(t) = \sum_{w\geq 1} h_w t^w.$$

Recall that the Môbius function μ takes the value 1 (resp. -1) on square-free integers with an even (resp. odd) number of prime factors, and 0 for non-square-free integers. In particular, $\mu(1) = 1$. Then Theorem 3.2 and the Möbius inversion formula imply that

Proposition 3.12. *For all w we have*

$$|\mathcal{D}_w| = \sum_{d|w} \mu(d)\, h_{w/d}.$$

Proof. Since $\mathfrak{A}$ is a graded K-algebra with $\mathfrak{A}_0 = K$, we consider its Hilbert-Poincaré series given by

$$H_{\mathfrak{A}}(t) = \sum_{w\geq 0} \dim \mathfrak{A}_w \, t^w.$$

By definition, $\dim \mathfrak{A}_w$ is the number of words with weight w. A word $\mathfrak{s} = x_{i_1} \dots x_{i_k}$ of weight w corresponds to a decomposition of w into a sum of positive integers $w = i_1 + \ldots + i_k$, that is, a composition of w. It is known that the number of compositions of an integer $w > 1$ is 2^{w-1}. Thus

$$\dim \mathfrak{A}_w = \begin{cases} 1 & \text{if } w = 0, \\ 2^{w-1} & \text{if } w > 0. \end{cases}$$

It follows that

$$H_{\mathfrak{A}}(t) = 1 + t + 2t + 2^2 t^3 + \cdots$$

Consider the following power series for the $*-$product:

$$\begin{aligned} S &= \prod_{\mathfrak{s}\in D''} (1 + \mathfrak{s} + \mathfrak{s}^{*2} + \cdots) \\ &= \prod_{w\geq 1} \prod_{\mathfrak{s}\in D''_w} (1 + \mathfrak{s} + \mathfrak{s}^{*2} + \cdots). \end{aligned}$$

After the expansion, the expression S contains every $*-$monomial, each with coefficient 1. By Theorem 4.1, $\mathcal{D}''$ is a polynomial basis of $\mathfrak{A}$. This implies that the expression S, when evaluated at $\mathfrak{s} = t^w$, for all $\mathfrak{s} \in \mathcal{D}_w$, agrees with $H_{\mathfrak{A}}(t)$:

$$\begin{aligned} H_{\mathfrak{A}}(t) &= \prod_{w\geq 1} \prod_{\mathfrak{s}\in D''_w} (1 + t^w + t^{2w} + \cdots) \\ &= \prod_{w\geq 1} (1 + t^w + t^{2w} + \cdots)^{d''_w} \\ &= \prod_{w\geq 1} (1 + t^w + t^{2w} + \cdots)^{d''_w} \\ &= \prod_{w\geq 1} \frac{1}{(1-t^w)^{d''_w}}. \end{aligned}$$

Now, by differentiating both sides, then multiplying both sides by t we get

$$\begin{aligned} td \log H_{\mathfrak{A}}(t) &= \sum_{w\geq 1} w d''_w \frac{t^w}{1-t^w} \\ &= \sum_{w\geq 1} w d''_w (t^w + t^{2w} + \cdots) \\ &= \sum_{n\geq 1} \left(\sum_{w|n} w d''_w \right) t^n. \end{aligned}$$

Note that if $\log H_{\mathfrak{A}}(t) = \sum_{n\geq 0} h_n t^n$ then $td \log H_{\mathfrak{A}}(t) = \sum_{n\geq 1} n h_n t^n$. Therefore, the previous identity shows that, for all positive integers n,

$$\sum_{w|n} w d''_w = n h_n.$$

This recursive formula allows us to compute d_w using the coefficients of the series $\log H_{\mathfrak{A}}(t)$.

It follows from the Mobius inversion formula that, for all positive integers n,

$$d''_w = \sum_{d|w} \mu(d)\, h_{w/d}.$$

Note that, by Corollary 3.11, $d_w = d''_w$. This gives us the desired formula for d_w. □

4. Generators of the stuffle algebra

4.1. **The main result.**

In this section we will prove the following theorem:

Theorem 4.1. *The algebra $(\mathfrak{A}, *)$ is a polynomial algebra over the $p-$adic prime-to-p Lyndon words.*

Theorem 4.1 is a consequence of the following proposition:

Proposition 4.2. *Let $n = \{n_1 \cdot \mathfrak{t}_1, n_2 \cdot \mathfrak{t}_2, \ldots, n_k \cdot \mathfrak{t}_k\}$ be a multiset in $\mathcal{D}''$. Let $\{m_1 \cdot \mathfrak{s}_1, m_2 \cdot \mathfrak{s}_2, \ldots, m_l \cdot \mathfrak{s}_l\} = G(n)$ and $\mathfrak{s} = g \circ G(n)$ be the corresponding multiset*

in $\mathrm{Mult}_{<p}(\mathcal{D}')$ *and word in* $\langle A\rangle$*. Then the expansion of the* $*$*monomial* $\mathfrak{t}_1^{*n_1} * \mathfrak{t}_2^{*n_2} * \cdots * \mathfrak{t}_k^{*n_k}$ *in* $\mathfrak{A}$ *has the form:*

$$\mathfrak{t}_1^{*n_1} * \mathfrak{t}_2^{*n_2} * \cdots * \mathfrak{t}_k^{*n_k} = \sum_{\mathfrak{s}' \leq \mathfrak{s}, w(\mathfrak{s}')=w(\mathfrak{s})} c_{\mathfrak{s}'\mathfrak{s}'}.$$

The coefficients $c_{\mathfrak{s}'}$ *are in* $\mathbb{F}_p$*.*

Furthermore, $c_{\mathfrak{s}} = m_1!\, m_2!\, \cdots\, m_s!$*. In partticular,* $c_{\mathfrak{s}} \neq 0$*.*

We postpone the proof of Proposition 4.2 until the end of this section (see §4.2) and explain why it implies Theorem 4.1.

Proof of Theorem 4.1. First, let us show that $(\mathfrak{A}, *)$ can be generated as an algebra by $\mathcal{D}''$. Indeed, it suffices to show that any word $\mathfrak{s}$ in $\langle A\rangle$ can be expressed as a $*-$polynomial with coefficients in $\mathbb{F}_p$ of elements of $\mathcal{D}''$. If $w(\mathfrak{s}) = 0$, that is $\mathfrak{s}$ is the empty word, then the conclusion is trivial. Suppose that $w = w(\mathfrak{s}) > 0$.

By Proposition 4.2, we can express

$$c_{\mathfrak{s}}\mathfrak{s} = \mathfrak{t}_1^{*n_1} * \mathfrak{t}_2^{*n_2} * \cdots * \mathfrak{t}_k^{*n_k} - \sum_{\mathfrak{s}' < \mathfrak{s}, wt(\mathfrak{s}')=w} c_{\mathfrak{s}'}\mathfrak{s}'.$$

Note that the subset of $\langle A\rangle$ of words with weight w is finite whose smallest element is x_w. Therefore, if $\mathfrak{s} = x_w$ then the sum on the right hand side is empty and the conclusion is immediate as $c_{\mathfrak{s}} \neq 0$. Suppose that the conclusion holds for every word $\mathfrak{s}'$ of weight w such that $\mathfrak{s}' < \mathfrak{s}$. Then each term $c_{\mathfrak{s}'}\mathfrak{s}'$ can be expressed as a $*-$polynomials of elements of $\mathcal{D}''$ with coefficients in $\mathbb{F}_p$ and the above identity shows that $\mathfrak{s}$ can also be expressed as a $*-$polynomials of elements of $\mathcal{D}''$ with coefficients in $\mathbb{F}_p$.

It remains to show that the elements of $\mathcal{D}''$ are algebraically independent over $\mathbb{F}_p$. Suppose the contrary, that there are some linear dependence relations among the $*-$ monomials:

$$\sum_{n\in S} b_n \mathfrak{t}_1^{*n_1} * \mathfrak{t}_2^{*n_2} * \cdots * \mathfrak{t}_k^{*n_k} = 0,$$

where the sum is taken over a finite, non-empty subset S of $\mathrm{Mult}(\mathcal{D}'')$; and by abuse of notation, we identify the $*-$monomial $\mathfrak{t}_1^{*n_1} * \mathfrak{t}_2^{*n_2} * \cdots * \mathfrak{t}_k^{*n_k}$ with the element $n = \{n_1 \cdot \mathfrak{t}_1, \ldots, n_k \cdot \mathfrak{t}_k\}$ of $\mathrm{Mult}(\mathcal{D}'')$ and the coefficients b_n of $\mathfrak{t}_1^{*n_1} * \mathfrak{t}_2^{*n_2} * \cdots * \mathfrak{t}_k^{*n_k}$ are nonzero. By Proposition 4.2, each term $b_n \mathfrak{t}_1^{*n_1} * \mathfrak{t}_2^{*n_2} * \cdots * \mathfrak{t}_k^{*n_k}$ has an expansion in $\mathfrak{A}$ of the form

$$b_n \mathfrak{t}_1^{*n_1} * \mathfrak{t}_2^{*n_2} * \cdots * \mathfrak{t}_k^{*n_k} = b_n c_{\mathfrak{s}(n)}\mathfrak{s}(n) + b_n \left(\sum_{\mathfrak{s}' < \mathfrak{s}(n), wt(\mathfrak{s}')=wt(\mathfrak{s}(n))} c_{\mathfrak{s}'}\mathfrak{s}' \right)$$

where $\mathfrak{s}(n) = g \circ G(n)$. Since $g \circ G$ a bijection between $\mathrm{Mult}(\mathcal{D}'')$ and $\langle A\rangle$, the words $g \circ G(n)$ $(n \in S)$ are pairwise distinct. It follows that if we denote by $\mathfrak{s}(n_0) = g \circ G(n_0)$ the largest element among them then we have an expansion of the form

$$\sum_{n\in S} b_n \mathfrak{t}_1^{*n_1} * \mathfrak{t}_2^{*n_2} * \cdots * \mathfrak{t}_k^{*n_k} = b_{n_0} c_{\mathfrak{s}(n_0)}\mathfrak{s}(n_0) + \sum_{\mathfrak{s}' < \mathfrak{s}(n_0)} d_{\mathfrak{s}'}\mathfrak{s}'.$$

Since $b_{n_0} c_{\mathfrak{s}(n_0)} \neq 0$, the right hand side does not vanish, while the left hand side is equal to 0, contradiction. □

4.2. **Proof of Proposition 4.2.**

4.2.1. *Premilinaries.*

Let us recall the stuffle and shuffle algebras over the integers $\mathbb{Z}$ as follows.

Definition 4.3. Let $\mathfrak{A}_{\mathbb{Z}}$ the free $\mathbb{Z}$-module with basis $\langle A\rangle$. Then we recursively define two products on $\mathfrak{A}_{\mathbb{Z}}$ as $\mathbb{Z}$-bilinear maps

$$\sqcup\!\sqcup\colon \mathfrak{A}_{\mathbb{Z}}\times\mathfrak{A}_{\mathbb{Z}}\longrightarrow\mathfrak{A}_{\mathbb{Z}} \quad\text{and}\quad *\colon \mathfrak{A}_{\mathbb{Z}}\times\mathfrak{A}_{\mathbb{Z}}\longrightarrow\mathfrak{A}_{\mathbb{Z}}$$

by setting $1\sqcup\!\sqcup\mathfrak{a}=\mathfrak{a}\sqcup\!\sqcup 1=\mathfrak{a}, 1*\mathfrak{a}=\mathfrak{a}*1=\mathfrak{a}$ and

$$\begin{aligned}\mathfrak{a}\sqcup\!\sqcup\mathfrak{b}&=x_a(\mathfrak{a}_-\sqcup\!\sqcup\mathfrak{b})+x_b(\mathfrak{a}\sqcup\!\sqcup\mathfrak{b}_-),\\ \mathfrak{a}*\mathfrak{b}&=x_a(\mathfrak{a}_-*\mathfrak{b})+x_b(\mathfrak{a}*\mathfrak{b}_-)+x_{a+b}(\mathfrak{a}_-*\mathfrak{b}_-).\end{aligned}$$

Note that the algebra $(\mathfrak{A},*)$ is simply a reduction modulo p of $(\mathfrak{A}_{\mathbb{Z}},*)$.

Definition 4.4. Let $\mathfrak{s}_1,\mathfrak{s}_2$ be two words. Suppose that the expansions of $\mathfrak{s}_1*\mathfrak{s}_2$ and $\mathfrak{s}_1\sqcup\!\sqcup\mathfrak{s}_2$ in the algebra $\mathfrak{A}_{\mathbb{Z}}$ are of the form

$$\begin{aligned}\mathfrak{s}_1*\mathfrak{s}_2&=\sum_{\mathfrak{s}\leq\mathfrak{a}}c_{\mathfrak{s}}\mathfrak{s},\\ \mathfrak{s}_1\sqcup\!\sqcup\mathfrak{s}_2&=\sum_{\mathfrak{s}\leq\mathfrak{b}}d_{\mathfrak{s}}\mathfrak{s}\end{aligned}$$

where $c_{\mathfrak{a}},d_{\mathfrak{b}}$ are nonzero integers. Then we say that $c_{\mathfrak{a}}\mathfrak{a},d_{\mathfrak{b}}\mathfrak{b}$ are the largest terms of $\mathfrak{s}_1*\mathfrak{s}_2$ and $\mathfrak{s}_1\sqcup\!\sqcup\mathfrak{s}_2$ respectively. For simplicity, we denote them by $LT(\mathfrak{s}_1*\mathfrak{s}_2)$ and $LT(\mathfrak{s}_1\sqcup\!\sqcup\mathfrak{s}_2)$. This definition and notation naturally generalize to products of more than two words.

Proposition 4.5. *Over $\mathbb{Z}$, we have, for any words $\mathfrak{s}_1,\mathfrak{s}_2,\ldots,\mathfrak{s}_k\in\langle A\rangle$, we have*

$$LT(\mathfrak{s}_1*\mathfrak{s}_2*\cdots*\mathfrak{s}_k)=LT(\mathfrak{s}_1\sqcup\!\sqcup\mathfrak{s}_2\sqcup\!\sqcup\cdots\sqcup\!\sqcup\mathfrak{s}_k).$$

Proof. First we consider the case when $k=2$. Let us prove that $LT(\mathfrak{a}*\mathfrak{b})=LT(\mathfrak{a}\sqcup\!\sqcup\mathfrak{b})$ by induction on the sum of the lengths $|\mathfrak{a}|+|\mathfrak{b}|$. If $|\mathfrak{a}|+|\mathfrak{b}|=0$, then both $\mathfrak{a},\mathfrak{b}$ are empty words and we are done. More generally, the identity holds if one of the words $\mathfrak{a},\mathfrak{b}$ is empty, since the $*-$ product and the $\sqcup\!\sqcup-$ product of any word $\mathfrak{s}$ with the empty word are both equal to $\mathfrak{s}$. So we can assume that $\mathfrak{a},\mathfrak{b}$ are not empty, and that the identity holds for any two words whose the sum of lengths is less than $|\mathfrak{a}|+|\mathfrak{b}|$. Let us write $\mathfrak{a}=x_a\mathfrak{a}_-,\mathfrak{b}=x_b\mathfrak{b}_-$, so that

$$\begin{aligned}\mathfrak{a}\sqcup\!\sqcup\mathfrak{b}&=x_a(\mathfrak{a}_-\sqcup\!\sqcup\mathfrak{b})+x_b(\mathfrak{a}\sqcup\!\sqcup\mathfrak{b}_-),\\ \mathfrak{a}*\mathfrak{b}&=x_a(\mathfrak{a}_-*\mathfrak{b})+x_b(\mathfrak{a}*\mathfrak{b}_-)+x_{a+b}(\mathfrak{a}_-*\mathfrak{b}_-).\end{aligned}$$

Since $\mathfrak{a},\mathfrak{b}$ are not empty words, a,b are positive integers. By the definition of the order on the alphabet, $x_{a+b}\prec x_a, x_{a+b}\prec x_b$ so that the largest term of $\mathfrak{a}*\mathfrak{b}$ has no contribution from the expansion of $x_{a+b}(\mathfrak{a}_-*\mathfrak{b}_-)$, that is

$$LT(\mathfrak{a}*\mathfrak{b})=LT(x_a(\mathfrak{a}_-*\mathfrak{b})+x_b(\mathfrak{a}*\mathfrak{b}_-)).$$

Suppose $a<b$. Then $x_b\prec x_a$ and the largest term of $\mathfrak{a}*\mathfrak{b}$ must come from $x_a(\mathfrak{a}_-*\mathfrak{b})$, i.e., $LT(\mathfrak{a}*\mathfrak{b})=LT(x_a(\mathfrak{a}_-*\mathfrak{b}))=x_aLT(\mathfrak{a}_-*\mathfrak{b})$. Similarly, $LT(\mathfrak{a}\sqcup\!\sqcup\mathfrak{b})=LT(x_a(\mathfrak{a}_-\sqcup\!\sqcup\mathfrak{b}))=x_aLT(\mathfrak{a}_-\sqcup\!\sqcup\mathfrak{b})$. But, by the induction hypothesis, $LT(\mathfrak{a}_-*\mathfrak{b})=LT(\mathfrak{a}_-\sqcup\!\sqcup\mathfrak{b})$. It follows that $LT(\mathfrak{a}_-*\mathfrak{b})=LT(\mathfrak{a}_-\sqcup\!\sqcup\mathfrak{b})$. Similar arguments apply to the case $a>b$ (or by swapping the order of $\mathfrak{a}$ and $\mathfrak{b}$ and using the commutativity of the shuffle and stuffle products).

Suppose that $a = b$. In this case, if the largest words in the expansions of $\mathfrak{a}_- * \mathfrak{b}$ and $\mathfrak{a} * \mathfrak{b}_-$ are equal then $LT(\mathfrak{a} * \mathfrak{b}) = LT(\mathfrak{a}_- * \mathfrak{b}) + LT(\mathfrak{a} * \mathfrak{b}_-)$, and by induction hypothesis $LT(\mathfrak{a}_- * \mathfrak{b}) = LT(\mathfrak{a}_- \sqcup\!\sqcup \mathfrak{b}), LT(\mathfrak{a} * \mathfrak{b}_-) = LT(\mathfrak{a} \sqcup\!\sqcup \mathfrak{b}_-)$, which, in turn, implies that the largest words in $\mathfrak{a}_- \sqcup\!\sqcup \mathfrak{b}$ and $\mathfrak{a} \sqcup\!\sqcup \mathfrak{b}_-$ are equal and $LT(\mathfrak{a} \sqcup\!\sqcup \mathfrak{b}) = LT(\mathfrak{a}_- \sqcup\!\sqcup \mathfrak{b}) + LT(\mathfrak{a} \sqcup\!\sqcup \mathfrak{b}_-)$, giving the desired identity. If the largest words in the expansions of $\mathfrak{a}_- * \mathfrak{b}$ and $\mathfrak{a} * \mathfrak{b}_-$ are not equal, e.g., the largest word in $\mathfrak{a}_- * \mathfrak{b}$ is larger than the one in $\mathfrak{a} * \mathfrak{b}_-$, then $LT(\mathfrak{a} * \mathfrak{b}) = x_a LT(\mathfrak{a}_- * \mathfrak{b})$. By the induction hypothesis, $LT(\mathfrak{a}_- * \mathfrak{b}) = LT(\mathfrak{a}_- \sqcup\!\sqcup \mathfrak{b}), LT(\mathfrak{a} * \mathfrak{b}_-) = LT(\mathfrak{a} \sqcup\!\sqcup \mathfrak{b}_-)$, which shows that the largest word in $\mathfrak{a}_- \sqcup\!\sqcup \mathfrak{b}$ is larger than the one in $\mathfrak{a} \sqcup\!\sqcup \mathfrak{b}_-$, thus $LT(\mathfrak{a} \sqcup\!\sqcup \mathfrak{b}) = LT(\mathfrak{a}_- \sqcup\!\sqcup \mathfrak{b})$, implying $LT(\mathfrak{a} * \mathfrak{b}) = LT(\mathfrak{a} \sqcup\!\sqcup \mathfrak{b})$. This completes the proof for the case $k = 2$.

The general case follows immediately by induction on k, using the associativity of the shuffle and stuffle products. □

The following result is due to Radford (see [31, Theorem 3.2.1, Part a]):

Proposition 4.6. *Let $\mathfrak{s}_1 \succ \mathfrak{s}_2 \succ \cdots \succ \mathfrak{s}_k$ be a decreasing sequence of $p-$adic Lyndon words and $m_1, m_2, \ldots, m_k$ a sequence of positive integers strictly less than p. Then*

$$LT(\mathfrak{s}_1^{\sqcup\!\sqcup m_1} \sqcup\!\sqcup \mathfrak{s}_2^{\sqcup\!\sqcup m_2} \sqcup\!\sqcup \cdots \sqcup\!\sqcup \mathfrak{s}_k^{\sqcup\!\sqcup m_k}) = m_1!\ m_2!\ \cdots\ m_k!\, \mathfrak{s}_1^{m_1} \cdots \mathfrak{s}_k^{m_k}.$$

4.2.2. *Proof of Proposition 4.2.* Let $n = \{n_1 \cdot \mathfrak{t}_1, n_2 \cdot \mathfrak{t}_2, \ldots, n_k \cdot \mathfrak{t}_k\}$ be a multiset in $\mathcal{D}''$. For each i, let $n_i = \sum_{j=0}^{+\infty} k_{i,j} p^j$ be the $p-$adic expansion of n_i ($0 \leq k_{i,j} \leq p-1$ and $k_{i,j} = 0$ for all but finitely many j). Then

$$\mathfrak{t}_i^{*n_i} = \mathfrak{t}_i^{*k_{i,0}} * \mathfrak{t}_i^{*k_{i,1}p} * \mathfrak{t}_i^{*k_{i,2}p^2} * \cdots$$

Thanks to Proposition 2.7, each factor $\mathfrak{t}_i^{*k_{i,j}p^j}$ simplifies to

$$\mathfrak{t}_i^{*k_{i,j}p^j} = \underbrace{\mathfrak{t}_i^{*p^j} * \mathfrak{t}_i^{*p^j} * \cdots * \mathfrak{t}_i^{*p^j}}_{k_{i,j} \text{ times}} = \underbrace{(\mathfrak{t}_i \star p^j) * (\mathfrak{t}_i \star p^j) * \cdots * (\mathfrak{t}_i \star p^j)}_{k_{i,j} \text{ times}}$$

It follows that $\mathfrak{t}_1^{*n_1} * \mathfrak{t}_2^{*n_2} * \cdots * \mathfrak{t}_k^{*n_k}$ is equal to the $*$-product of $\mathfrak{t}_i \star p^j$, $1 \leq i \leq k, 0 \leq j < +\infty$, where each factor $\mathfrak{t}_i \star p^j$ appears with multiplicity $k_{i,j}$. Recall that, by definition,

$$G(n) = \sum_{i=1}^{l} \sum_{j=0}^{+\infty} k_{i,j} \cdot (\mathfrak{t}_i \star p^j).$$

We arrange the elements of the multiset $m = G(n) \in \mathrm{Mult}_{<p}(\mathcal{D}')$ in decreasing order $m = \{m_1 \cdot \mathfrak{s}_1, m_2 \cdot \mathfrak{s}_2, \ldots, m_\ell \cdot \mathfrak{s}_\ell\}$ where $\mathfrak{s}_1 \succ \mathfrak{s}_2 \succ \cdots \succ \mathfrak{s}_\ell$. Then,

$$\mathfrak{t}_1^{*n_1} * \mathfrak{t}_2^{*n_2} * \cdots * \mathfrak{t}_k^{*n_k} = \mathfrak{s}_1^{*m_1} * \mathfrak{s}_2^{*m_2} * \cdots * \mathfrak{s}_\ell^{*m_\ell}.$$

Now, Propostion 4.5, combined with Proposition 4.6, states that the expansion of $\mathfrak{s}_1^{*m_1} * \mathfrak{s}_2^{*m_2} * \cdots * \mathfrak{s}_\ell^{*m_\ell}$ in $\mathfrak{A}$, is an integral linear combination of words in $\langle A \rangle$, the largest of which is $\mathfrak{s}$, appearing with a nonzero coefficient. This concludes the proof of Proposition 4.2.

5. Applications

In this section we present an application of Theorem 4.1 to multiple zeta values in positive characteristic which is the starting point of this work.

5.1. **Motivation and setup.**

In the classical setting, zeta values and multiple zeta values were studied by Euler in the 18th century. They were resurrected by Zagier in his seminal paper [38] and then by physicists such as Broadhurst, Kreimer [3]. Since then, they have become ubiquitous in many branches in mathematics and physics (see for example [1, 4, 11, 13, 17, 23, 24, 33]). We refer the reader to [5, 6, 38] for more details and further references.

By the analogy between number fields and function fields, there exists the notion of zeta values and multiple zeta values in positive characteristic which has attracted growing interest in recent years (see for example [8, 14, 28, 32, 34]). We briefly recall these objects and collect some results from [18, 19, 20, 28].

Let q be a power of prime p and $\mathbb{F}_q$ be a finite field of order q. Let $A = \mathbb{F}_q[\theta]$ be the polynomial ring in θ over $\mathbb{F}_q$ and A_+ the set of monic polynomials in A. We denote by $K = \mathbb{F}_q(\theta)$ the fraction field of A equipped with the rational point ∞. Let $K_\infty = k(\!(1/\theta)\!)$ be the completion of K at ∞ and $\mathbb{C}_\infty$ be the completion of a fixed algebraic closure $\overline{K}$ of K at ∞. Further, let v_∞ be the discrete valuation on K associated to the place ∞ normalized as $v_\infty(\theta) = -1$ and $|\cdot|_\infty = q^{-v_\infty(\cdot)}$ be the corresponding norm on K.

Let $\mathfrak{s} = (s_1, \ldots, s_n)$ be a tuple of positive integers. Then $w(\mathfrak{s}) = s_1 + \cdots + s_n$ (resp. n) is called the weight (resp. the depth) of $\mathfrak{s}$. We introduce the multiple zeta value (MZV for short) attached to $\mathfrak{s}$ given by the convergent series

$$\zeta_A(\mathfrak{s}) = \sum \frac{1}{a_1^{s_1} \ldots a_r^{s_r}} \in K_\infty$$

where the sum is over all tuples $(a_1, \ldots, a_r) \in A_+^r$ with $\deg(a_1) > \cdots > \deg(a_r)$. We also call $w(\mathfrak{s})$ (resp. n) the weight (resp. the depth) of $\zeta_A(\mathfrak{s})$. Then it is proved that $\zeta_A(\mathfrak{s})$ does not vanish. Furthermore, it is known that the product of two MZV's is a K-linear combination of MZV's, but the formula is complicated. We denote by $\mathcal{Z}$ (resp. $\mathcal{Z}_w$) the K-vector space spanned by all the MZV's (resp. all the MZV's of fixed weight w).

Theorem 5.1. *We keep the above notation. Then $\mathcal{Z}$ is a commutative graded K-algebra.*

Proof. The commutativity of $\mathcal{Z}$ is easy to prove (see for example [36]). The fact that $\mathcal{Z}$ is graded was proved in [8]. The associativity of $\mathcal{Z}$ was proved in [19, Theorem A]. □

5.2. **The stuffle algebra structure of MZV's.**

We now review the notion of multiple polylogarithms (or Carlitz multiple polylogarithms) in positive characteristic. We put $\ell_0 := 1$ and $\ell_d := \prod_{i=1}^d (\theta - \theta^{q^i})$ for all $d \in \mathbb{N}$. For $\mathfrak{s} = (s_1, \ldots, s_n) \in \mathbb{N}^n$, we introduce the Carlitz multiple polylogarithm at roots of unity (CMPL at roots of unity for short) as follows:

$$\mathrm{Li}(\mathfrak{s}) = \sum_{d_1 > \cdots > d_n \geq 0} \frac{1}{\ell_{d_1}^{s_1} \ldots \ell_{d_n}^{s_n}} \in K_\infty.$$

We denote by $\mathcal{L}$ (resp. $\mathcal{L}_w$) the K-vector space spanned by all the CMPL's (resp. all the MZV's of fixed weight w). An advantage when working with CMPL's is that

we can equip $\mathcal{L}$ with the stuffle product described as in the previous sections. Then one proves that $\mathcal{L}$ is also a commutative graded K-algebra.

The following result explains the connection between MZV's and CMPL's:

Lemma 5.2. *For all $\mathfrak{s} = (s_1, \ldots, s_n) \in \mathbb{N}^n$ such that $s_i \leq q$ for all i, we have $\zeta_A(\mathfrak{s}) = \mathrm{Li}(\mathfrak{s})$.*

Proof. We refer the reader to [35] for a proof. □

Combining the above lemma with the techniques of [28, §2 and §3] we get

Theorem 5.3. *For all w, the K-vector spaces $\mathcal{Z}_w$ and $\mathcal{L}_w$ are spanned by $\mathrm{Li}(\mathfrak{s})$ where $\mathfrak{s}$ runs through the set of $\mathfrak{s} = (s_1, \ldots, s_n) \in \mathbb{N}^n$ such that $s_i \leq q$ for all i and $s_n < q$. In particular, they are equal.*

Proof. We outline the proof. Theorem A of [28] says that $\mathcal{Z}_w$ is spanned by $\mathrm{Li}(\mathfrak{s})$ where $\mathfrak{s}$ runs through the set of $\mathfrak{s} = (s_1, \ldots, s_n) \in \mathbb{N}^n$ such that $s_i \leq q$ for all i and $s_n < q$. We extend the techniques developed in its proof to obtain the statement for $\mathcal{L}_w$. Combining these results with Lemma 5.2 gives the theorem. We refer the reader to [18, Theorem 4.3] for more details. □

We define the stuffle map in positive characteristic by the K-linear map

$$\varphi : \mathfrak{A} \to \mathcal{Z},$$

which sends a word $\mathfrak{s} \in \langle A \rangle$ to $\mathrm{Li}(\mathfrak{s})$. We have proved that this is a homomorphism of graded K-algebras: for all words $\mathfrak{a}, \mathfrak{b} \in \mathfrak{A}$,

$$\mathrm{Li}(\mathfrak{a} * \mathfrak{b}) = \mathrm{Li}(\mathfrak{a})\ \mathrm{Li}(\mathfrak{b}).$$

5.3. **An application of Theorem 4.1.**

We present an application of Theorem 4.1 to study the transcendence degree of MZV's of small weights. We recall Theorem B and Corollary C of [28] which state that

Theorem 5.4. *For $w < q$ the induced map $\varphi : \mathfrak{A}_w \to \mathcal{Z}_w$ is an isomorphism of K-vector spaces.*

We derive the following result:

Theorem 5.5. *For all $w < q$ the transcendence degree of the K-algebra generated by MZV's of weight at most w equals $\sum_{i=1}^{w} |\mathcal{D}_i|$ where $|\mathcal{D}_i|$ is given as in Proposition 3.12.*

Proof. Since $w < q$, Theorem 5.4 states that the K-algebra generated by MZV's of weight at most w can be identified with the K-algebra generated by the words $\mathfrak{s} \in \mathfrak{A}$ of weight at most w. By Theorem 4.1 the latter is the polynomial algebra over the $p-$adic prime-to-p Lyndon words of weight at most w. Thus the transcendence degree of the K-algebra generated by MZV's of weight at most w is $\sum_{i=1}^{w} |\mathcal{D}_i''|$. Combining this with Corollary 3.11 gives the theorem and we are done. □

Remark 5.6. Mishiba [26, 27] studied the transcendence degree of the K-algebra of two particular sets of MZV's:

- In [26] he considered the set consisting of two MZV's $\zeta_A(2n)$ and $\zeta_A(n, n)$ for fixed n. If $n = 1$, we get the previous theorem for $w = 2$.

- In [27] he considered distinct positive integers $n_1, \dots, n_d$ such that $q-1 \nmid n_i$ and n_i/n_j is not a power of p for $i \neq j$. Then the set of MZV's consists of all $\zeta_A(n_i, n_{i+1}, \dots, n_j)$ for $1 \leq i \leq j \leq d$.

His method is completely different from ours and based on the techniques from algebraic geometry and the powerful tool developed in [29].

References

[1] P. Banks, E. Panzer, and B. Pym. Multiple zeta values in deformation quantization. *Invent. Math.*, 222(1):79–159, 2020.

[2] D. J. Broadhurst. Multiple Deligne Values: a data mine with empirically tamed denominators. *arXiv:1409.7204v1*, 2014.

[3] D. Broadhurst. and D. Kreimer. Association of multiple zeta values with positive knots via Feynman diagrams up to 9 loops. *Phys. Lett. B*, 393(3-4):403–412, 1997.

[4] F. Brown. Mixed Tate motives over $\mathbb{Z}$. *Ann. of Math. (2)*, 175:949–976, 2012.

[5] F. Brown. Motivic periods and $\mathbb{P}^1 \setminus \{0, 1, \infty\}$. In *Proceedings of the International Congress of Mathematicians—Seoul 2014. Vol. II*, pages 295–318. Kyung Moon Sa, Seoul, 2014.

[6] J. Burgos Gil and J. Fresan. *Multiple zeta values: from numbers to motives*. to appear, Clay Mathematics Proceedings.

[7] L. Carlitz. On certain functions connected with polynomials in Galois field. *Duke Math. J.*, 1(2):137–168, 1935.

[8] C.-Y. Chang. Linear independence of monomials of multizeta values in positive characteristic. *Compos. Math.*, 150(11):1789–1808, 2014.

[9] K.-T. Chen, R. H. Fox, and R. C. Lyndon. Free differential calculus. IV. The quotient groups of the lower central series. *Ann. of Math. (2)*, 68:81–95, 1958.

[10] P. Deligne. Le groupe fondamental unipotent motivique de $G_m - \mu_N$, pour $N = 2, 3, 4, 6$ ou 8. *Publ. Math. Inst. Hautes Études Sci.*, 112:101–141, 2010.

[11] P. Deligne and A. Goncharov. Groupes fondamentaux motiviques de Tate mixte. *Ann. Sci. École Norm. Sup. (4)*, 38(1):1–56, 2005.

[12] L. Euler. Meditationes circa singulare serierum genus. *Novi commentarii academiae scientiarum Petropolitanae*, 140–186, 1776.

[13] H. Gangl, M. Kaneko, and D. Zagier. Double zeta values and modular forms. In *Automorphic forms and zeta functions*, pages 71–106. World Sci. Publ., Hackensack, NJ, 2006.

[14] D. Goss. *Basic Structures of function field arithmetic*, volume 35 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*. Springer-Verlag, Berlin, 1996.

[15] M. Hoffman. The algebra of multiple harmonic series. *J. Algebra*, 194:477–495, 1997.

[16] M. Hoffman. Quasi-shuffle products. *J. Algebraic Combin.*, 11(1):49–68, 2000.

[17] K. Ihara, M. Kaneko, and D. Zagier. Derivation and double shuffle relations for multiple zeta values. *Compos. Math.*, 142(2):307–338, 2006.

[18] B.-H. Im, H. Kim, K. N. Le, T. Ngo Dac, and L. H. Pham. Zagier-Hoffman's conjectures in positive characteristic. *available at https://arxiv.org/abs/2205.07165*, 2022.

[19] B.-H. Im, H. Kim, K. N. Le, T. Ngo Dac, and L. H. Pham. Hopf algebras and multiple zeta values in positive characteristic. *available at https://arxiv.org/abs/2301.05906*, 2023.

[20] B.-H. Im, H. Kim, K. N. Le, T. Ngo Dac, and L. H. Pham. Zagier-Hoffman's conjectures in positive characteristic II. *available at https://arxiv.org/abs/2402.11539*, 2024.

[21] B.-H. Im, H. Kim, K. N. Le, T. Ngo Dac, and L. H. Pham. Work in progress. 2024.

[22] K. Iwasawa. Analogies between number fields and function fields. In *Some Recent Advances in the Basic Sciences, Vol. 2 (Proc. Annual Sci. Conf., Belfer Grad. School Sci., Yeshiva Univ., New York, 1965-1966)*, pages 203–208. Yeshiva Univ., Belfer Graduate School of Science, New York, 1969.

[23] M. Kontsevich. Operads and motives in deformation quantization. *Lett. Math. Phys.*, 48(1):35–72, 1999. Moshé Flato (1937–1998).

[24] M. Kontsevich. Deformation quantization of Poisson manifolds. *Lett. Math. Phys.*, 66(3):157–216, 2003.

[25] B. Mazur and A. Wiles. Analogies between function fields and number fields. *Amer. J. Math.*, 105(2):507–521, 1983.

[26] Y. Mishiba. Algebraic independence of the Carlitz period and the positive characteristic multizeta values at n and (n, n). *Proc. Amer. Math. Soc.*, 143(9):3753–3763, 2015.
[27] Y. Mishiba. On algebraic independence of certain multizeta values in characteristic p. *J. Number Theory*, 173:512–528, 2017.
[28] T. Ngo Dac. On Zagier-Hoffman's conjectures in positive characteristic. *Ann. of Math. (2)*, 194(1):361–392, 2021.
[29] M. Papanikolas. Tannakian duality for Anderson-Drinfeld motives and algebraic independence of Carlitz logarithms. *Invent. Math.*, 171(1):123–174, 2008.
[30] G. Racinet. Doubles mélanges des polylogarithmes multiples aux racines de l'unité. *Publ. Math. Inst. Hautes Études Sci.*, (95):185–231, 2002.
[31] D. Radford. A natural ring basis for the shuffle algebra and an application to group schemes. *J. Algebra*, 58(2):432–454, 1979.
[32] F. Pellarin. Values of certain L-series in positive characteristic. *Ann. of Math. (2)*, 176(3):2055–2093, 2012.
[33] T. Terasoma. Mixed Tate motives and multiple zeta values. *Invent. Math.*, 149(2):339–369, 2002.
[34] D. Thakur. *Function field arithmetic*. World Scientific Publishing Co., Inc., River Edge, NJ, 2004.
[35] D. Thakur. Relations between multizeta values for $\mathbb{F}_q[t]$. *Int. Math. Res. Not.*, (12):2318–2346, 2009.
[36] D. Thakur. Multizeta values for function fields: a survey. *J. Théor. Nombres Bordeaux*, 29(3):997–1023, 2017.
[37] A. Weil. Sur l'analogie entre les corps de nombres algébrique et les corps de fonctions algébrique. *Revue Scient.*, 77:104–106, 1939.
[38] D. Zagier. Values of zeta functions and their applications. In *First European Congress of Mathematics, Vol. II Paris, 1992)*, volume 120 of *Progr. Math.*, pages 497–512. Birkhäuser, Basel, 1994.

Normandie Université, Université de Caen Normandie - CNRS, Laboratoire de Mathématiques Nicolas Oresme (LMNO), UMR 6139, 14000 Caen, France.

Email address: tuan.ngodac@unicaen.fr

Institute of Mathematics, Vietnam Academy of Science and Technology, 18 Hoang Quoc Viet, 10307 Hanoi, Viet Nam

Email address: ncgvuong@math.ac.vn

Institute of Mathematics, Vietnam Academy of Science and Technology, 18 Hoang Quoc Viet, 10307 Hanoi, Viet Nam

Email address: plhuong@math.ac.vn