# A note on the algebra of $p$-adic multi-zeta values 

Sinan Ünver


#### Abstract

We prove that the algebra of $p$-adic multi-zeta values, as defined in [4] or [2], are contained in another algebra which is defined explicitly in terms of series. The main idea is to truncate certain series, expand them in terms of series all of which are divergent except one, and then take the limit of the convergent one. The main result is Theorem 3.12.


## 1. Introduction

Multi-zeta values were defined by Euler as the sum of the series:

$$
\zeta\left(s_{1}, s_{2}, \ldots, s_{k}\right):=\sum_{0<n_{1}<\cdots<n_{k}} \frac{1}{n_{1}^{s_{1}} n_{2}^{s_{2}} \cdots n_{k}^{s_{k}}},
$$

for $s_{1}, \ldots, s_{k-1} \geq 1$ and $s_{k}>1$. The Euler-Kontsevich formula [3] expresses these numbers in terms of iterated integrals on the thrice punctured line $X:=\mathbb{P}^{1} \backslash\{0,1, \infty\}$. This formula interprets multi-zeta values as real periods of the mixed Tate motive coming from the unipotent fundamental group of $X$ [1], [3]. These imply many relations between the multi-zeta values and the algebra of these values has arithmetic significance as it relates to the tannakian fundamental group of mixed Tate motives over $\mathbb{Z}$ [3].

The $p$-adic version of these values were defined by Deligne (unpublished, explained in [4]) coming from the comparison theorem between the de Rham and the crystalline fundamental group of $X$. The double shuffle relations for these values were proved by Furusho and Jafari and the Drinfel'd-Ihara relations were proved by the author. The question of algebraic independence or even non-vanishing seems to be a more difficult question. We do not even know that $\zeta_{p}(2 k+1)$ are non-zero for all primes $p$, and positive integers $k$. This suggests that in order to prove linear independence among these numbers one might need a somewhat more explicit description of these numbers or the algebra generated by these numbers. This paper is a first attempt in this direction. Our aim in this note is to prove that the algebra of $p$-adic
multi-zeta values lie in another algebra that is described only using certain series. The remaining, but more difficult question is to study these series.

It turns out that the individual truncated series that appear in the expression for $p$-adic multi-zeta values are divergent, but their certain linear combinations converge. The main idea is to consider these divergent series and express them as linear combinations of a convergent series and other divergent series and then take the convergent part. We call this process the regularisation of the series.

In $\S 2$, we describe this process. The main point is that there are certain simple divergent series which we denote by $\sigma_{p}(\underline{s})$, which are linearly independent under the algebra of power series functions. That these series are linearly independent is proved in Proposition 2.3; the fact that all the series we are interested can be expressed in terms of these divergent series is proved in Proposition 2.7. Next in Proposition 2.14, which forms the basis for the inductive arguments, we prove that, under conditions that are satisfied by the series that appear below, if the truncated series that are the coefficients of a power series are regular then so are the coefficients of its antiderivative after it is multiplied by one of the forms $\omega_{i}$.

In $\S 3$, we apply the above results to the truncated series that appear in the expressions for $p$-adic multi-zeta values. The main idea is based on the results of [4]. Namely, using the standard lifting of frobenius on $X$, which is a good choice outside a disc of radius 1 around 1, we obtain a differential equation (3.2) for $\mathfrak{g}$. Next we use [4, Proposition 2] to find an expression for the value of $\mathfrak{g}$ at infinity and the relation (3.1) to relate that value to $g$, whose coefficients are the $p$-adic multi-zeta values. The main result is Theorem 3.12 where we prove that the algebra of $p$-adic multi-zeta values $\mathcal{Z}$ lie inside the algebra $\mathcal{P}$ of values of regularized series. Finally, we prove after Theorem 3.12 that the above result also implies the same statement for the $p$-adic multiple zeta values as defined by Furusho [2], since the algebra that they generate is the same as $\mathcal{Z}$.

Acknowledgements. The author thanks T. Terasoma for a very short discussion which became the main inspiration for this note. This paper was partly written while the author visited H. Esnault's arithmetic geometry group at Freie Universitt Berlin supported by a research fellowship of the Humboldt Foundation.

## 2. Iterated sums

Fix a prime $p$. For $\underline{s}:=\left(s_{1}, \ldots, s_{k}\right)$, with $0 \leq s_{i}$, and $\underline{m}:=\left(m_{1}, \ldots, m_{k}\right)$, with $0 \leq m_{i}<p$, let

$$
\sigma(\underline{s} ; \underline{m})(n):=\sum \frac{1}{n_{1}^{s_{1}} \cdots n_{k}^{s_{k}}}
$$

where the sum is over $0<n_{1}<n_{2}<\cdots<n_{k}<n$ with $p \mid\left(n_{i}-m_{i}\right)$. Similarly, we let $\gamma(\underline{s} ; \underline{m})(n):=n^{-s_{k}} \cdot \sigma\left(\underline{s}^{\prime} ; \underline{m}^{\prime}\right)(n)$, if $p \mid\left(n-m_{k}\right)$ and 0 otherwise, where $\underline{s}^{\prime}=\left(s_{1}, \ldots, s_{k-1}\right)$ and $\underline{m}^{\prime}=\left(m_{1}, \ldots, m_{k-1}\right)$. Let $\sigma_{p}(\underline{s})(n):=$ $\sigma(\underline{s} ; \underline{0})(n)$, where $\underline{0}=(0, \ldots, 0)$. We define the depth as $d(\underline{s})=k$ and the weight as $w(\underline{s}):=\sum s_{i}$.

Let us call a function $f: \mathbb{N}_{\geq n} \rightarrow \mathbb{Q}_{p}$, for some $n$, a power series function, if there exist power series $p_{i}(x) \in \mathbb{Q}_{p}[[x]]$, which converge on the closed unit disc $D\left(r_{i}\right)$ around 0 , for some $r_{i}>|p|$, for $0 \leq i<p$, such that $f(a)=$ $p_{i}(a-i)$ for all $a \geq n$ and $p \mid(a-i)$. Clearly there is a unique power series function $\bar{f}$ with domain $\mathbb{Z}_{\geq 0}$ such that $\bar{f}$ restricts to $f$ on $\mathbb{N}_{\geq n}$. We let $f(0):=\bar{f}(0)$, or more explicitly $f(0)=\lim _{\substack{k \rightarrow 0 \\ k>n}} f(k)$. We will identify two power series functions if they are the same on the intersection of their domains of definition. Note that we have the following [5, Proposition 5.0.5]:

Proposition 2.1. (i) The product and sum of power series functions are also power series functions. So is the function defined as $f(n)=n^{s}$, if $p \nmid n$; and $f(n)=0$, if $p \mid n$, for $s \in \mathbb{Z}$.
(ii) If $f$ is a power series function, let us define $f^{[1]}$ and $f^{(1)}$ as $f^{[1]}(n)=$ $f^{(1)}(n)=(f(n)-f(0)) / n$, if $p \mid n ; f^{[1]}(n)=0, f^{(1)}(n)=f(n) / n$, if $p \nmid n$. Then both $f^{[1]}$ and $f^{(1)}$ are power series functions.
(iii) If $f: \mathbb{N}_{\geq n_{0}} \rightarrow \mathbb{Q}_{p}$ is a power series function and if we define

$$
F(n):=\sum_{n_{0} \leq k \leq n} f(k),
$$

then so is $F$.
The following lemma on power series will be essential while we are proving the linear independence of the $\sigma_{p}$ 's.

Lemma 2.2. Let $f, g \in \mathbb{Q}_{p}[[z]]$ be two power series which are convergent on $D(a)$, for some $a>1$. Suppose that $g \neq 0$, and let $h:=f / g$. If there exist $C_{i} \in \mathbb{Q}_{p}$ and $n \geq 1$ such that $h(z+1)-h(z)=\frac{C_{n}}{z^{n}}+\cdots+\frac{C_{1}}{z}$, for infinitely many $z \in D(a)$ then $h$ is constant and $C_{i}=0$, for all $i$.

Proof. By the Weierstrass preparation theorem, if the above equality holds for infinitely many $z \in D(a)$ then it holds for all $z \in D(a)$, except for the zeros of the denominators involved. Suppose that $f \neq 0$, then again by the Weierstrass preparation theorem there are polynomials $p, q \in \mathbb{Q}_{p}[z]$, and power series $u, v \in \mathbb{Q}_{p}[[z]]$, which converge and are nonzero on $D(a)$ such that $f=p \cdot u$ and $g=q \cdot v$. Therefore the poles of $h(z)$ and $h(z+1)$ in $D(a)$, together with their multiplicities, are exactly those of $p(z) / q(z)$ and $p(z+1) / q(z+1)$. Let $\mathfrak{P}(k)$ denote the set of poles of $k$ in $D(a)$.

Then

$$
\mathfrak{P}(h) \triangle(\mathfrak{P}(h)-1) \subseteq \mathfrak{P}\left(\frac{C_{n}}{z^{n}}+\cdots+\frac{C_{1}}{z}\right) \subseteq \mathfrak{P}(h) \cup(\mathfrak{P}(h)-1),
$$

where $\Delta$ denotes the symmetric difference.
If $C_{i} \neq 0$ for some $i$, then $\mathfrak{P}\left(\frac{C_{n}}{z^{n}}+\cdots+\frac{C_{1}}{z}\right)=\{0\}$, hence $\mathfrak{P}(h) \neq \emptyset$. This implies that $\mathfrak{P}(h) \neq \mathfrak{P}(h)-1$. Since $|\mathfrak{P}(h)|=|\mathfrak{P}(h)-1|$ is finite, this implies that the symmetric difference of $\mathfrak{P}(h)$ and $\mathfrak{P}(h)-1$ contains at least two elements. This is a contradiction. Hence $C_{i}=0$, for all $i$. This implies that $h(z+1)=h(z)$. Choosing an $\alpha$ where $h$ does not have a pole and replacing $h$ with $\bar{h}:=h-h(\alpha)$, we see that $\bar{h}$ has infinitely many zeros in $D(a)$ and hence is 0.

Let $\mathscr{P}$ denote the algebra of power series in $\mathbb{Q}_{p}$ which converge on $D(r)$ for some $r>|p|$. We will identify these power series with the functions that they define from $p \mathbb{N}$ to $\mathbb{Q}_{p}$. Let $\sigma_{p}(\emptyset):=1$. Let $\mathscr{P}_{\sigma}$ denote the module over $\mathscr{P}$ generated by $\sigma_{p}(\underline{s})$ with $\underline{s} \in \cup_{n} \mathbb{N}^{\times n}$. Then by the shuffle product formula for series, $\mathscr{P}_{\sigma}$ is an algebra.

Proposition 2.3. The algebra $\mathscr{P}_{\sigma}$ is free with basis $\left\{\sigma_{p}(\underline{s}) \mid \underline{s} \in \cup_{n} \mathbb{N}^{\times n}\right\}$ as a module over $\mathscr{P}$.

Proof. By induction on $m$ we will show the linear independence of the set $S_{m}:=\left\{\sigma_{p}(\underline{s}) \mid d(\underline{s}) \leq m\right\}$. For any function $f: p \mathbb{N} \rightarrow \mathbb{Q}_{p}$, we let $\delta(f)$ denote the function defined by $\delta(f)(n):=f(n+p)-f(n)$. Note that

$$
\delta \sigma_{p}\left(\alpha_{1}, \ldots, \alpha_{m+1}\right)(n)=\frac{1}{n^{\alpha_{m+1}}} \sigma_{p}\left(\alpha_{1}, \ldots, \alpha_{m}\right)(n)
$$

We know the linear independence for the set $S_{0}=\{1\}$. Assuming that we know the linear independence for $S_{m}$, we will prove it for $S_{m+1}$. Let us suppose that $\left\{\sigma_{p}\left(\alpha_{1}, \ldots, \alpha_{m+1}\right)\right\} \cup S_{m}$ is linearly dependent over $\mathscr{P}$. Then
we have an expression of the form

$$
\sigma_{p}\left(\alpha_{1}, \ldots, \alpha_{m+1}\right)=\sum_{d(\alpha) \leq m} a_{\alpha} \sigma_{p}(\alpha)
$$

with $a_{\alpha}$ in the fraction field of $\mathscr{P}$.
Applying $\delta$ to the last equation we get

$$
\frac{1}{z^{\alpha_{m+1}}} \sigma_{p}\left(\alpha_{1}, \ldots, \alpha_{m}\right)=\sum_{d(\alpha)=m} \delta\left(a_{\alpha}\right) \sigma_{p}(\alpha)+\sum_{d(\alpha)<m} b_{\alpha} \sigma_{p}(\alpha)
$$

with $b_{\alpha}$ in the fraction field of $\mathscr{P}$.
The induction hypothesis implies that $\frac{1}{z^{\alpha_{m+1}}}=\delta\left(a_{\alpha_{1} \cdots \alpha_{m}}\right)$, and this contradicts the lemma above.

Next we do an induction on the number of elements $\sigma_{p}(\alpha)$ with $d(\alpha)=$ $m+1$, and $a_{\alpha} \neq 0$. Suppose that we have a non-trivial equation

$$
\sum_{d(\alpha) \leq m+1} a_{\alpha} \sigma_{p}(\alpha)=0
$$

By the induction assumption on $m$, there is a $\beta=\left(\alpha_{1}, \ldots, \alpha_{m+1}\right)$ such that $a_{\beta} \neq 0$. Dividing by this and rearranging we get

$$
\sigma_{p}(\beta)+\sum_{\substack{d(\alpha)=m+1 \\ \alpha \neq \beta}} b_{\alpha} \sigma_{p}(\alpha)=\sum_{d(\alpha) \leq m} b_{\alpha} \sigma_{p}(\alpha),
$$

where $b_{\alpha}$ are in the fraction field of $\mathscr{P}$. Applying $\delta$ to this equation and using induction on the number of $b_{\alpha} \neq 0$ with $d(\alpha)=m+1$ we obtain $\delta\left(b_{\alpha}\right)=0$ for all $\alpha$ with $d(\alpha)=m+1$, hence these $b_{\alpha}$ are constant and equal to, say $c_{\alpha}$.

So the last equation can be rewritten as

$$
\sigma_{p}(\beta)+\sum_{\substack{d(\alpha)=m+1 \\ \alpha \neq \beta}} c_{\alpha} \sigma_{p}(\alpha)=\sum_{\substack{d(\alpha) \leq m}} b_{\alpha} \sigma_{p}(\alpha),
$$

applying $\delta$ we obtain that

$$
\frac{1}{z^{\alpha_{m+1}}}+\sum_{\substack{k \in \mathbb{N} \\ k \neq \alpha_{m+1}}} c_{\left(\alpha_{1}, \ldots, \alpha_{m}, k\right)} \frac{1}{z^{k}}=\delta\left(b_{\left(\alpha_{1}, \ldots, \alpha_{m}\right)}\right)
$$

The above lemma again gives a contradiction.

Let $\mathscr{F}$ denote the algebra of power series functions and $\iota \in \mathscr{F}$ denote the function that sends $n$ to $n$. Let $\mathscr{F}\left(\frac{1}{\iota}\right)$ be the algebra obtained by inverting $\iota$. Note that $\iota$ is already invertible on the components $i+p \mathbb{N}$ with $0<i<p$. Let $\mathscr{F}_{\sigma}$ be the module over $\mathscr{F}$ generated by $\sigma_{p}(\underline{s})$ with $\underline{s} \in \cup_{n} \mathbb{N}^{\times n}$. Then by the shuffle product formula for series, $\mathscr{F}_{\sigma}$ is an algebra. Let $\mathscr{F}_{\sigma}\left(\frac{1}{\iota}\right)=$ $\mathscr{F}_{\sigma} \otimes_{\mathscr{F}} \mathscr{F}\left(\frac{1}{\iota}\right)$.

Corollary 2.4. The algebra $\mathscr{F}_{\sigma}\left(\right.$ resp. $\left.\mathscr{F}_{\sigma}\left(\frac{1}{\iota}\right)\right)$ is free with basis $\left\{\sigma_{p}(\underline{s}) \mid \underline{s} \in\right.$ $\left.\cup_{n} \mathbb{N}^{\times n}\right\}$ as a module over $\mathscr{F}$ (resp. $\mathscr{F}\left(\frac{1}{l}\right)$ ).

Proof. For a set $S$ let $F\left(S, \mathbb{Q}_{p}\right)$ denote the algebra of functions from $S$ to $\mathbb{Q}_{p}$. We have the following decomposition

$$
F\left(\mathbb{N}, \mathbb{Q}_{p}\right)=\oplus_{1 \leq i \leq p} F\left(p \mathbb{N}, \mathbb{Q}_{p}\right)
$$

where we send $f \in F\left(\mathbb{N}, \mathbb{Q}_{p}\right)$ to the element on the right hand side whose $i$-th component is $f_{i} \in F\left(p \mathbb{N}, \mathbb{Q}_{p}\right)$, defined by

$$
f_{i}(k)=f(k-p+i)
$$

for $k \in p \mathbb{N}$. We have $\sigma_{p}(\underline{s})_{i}=\sigma_{p}(\underline{s})$, for all $1 \leq i \leq p$, where we abuse the notation and denote by $\sigma_{p}(\underline{s})$ both the function on the left hand side of the equality whose domain is $\mathbb{N}$ and also the function on the right hand side of the equation which is its restriction to $p \mathbb{N}$. By the definition of the power series functions, the above decomposition gives the following decompositions:

$$
\mathscr{F}=\oplus_{1 \leq i \leq p} \mathscr{P}
$$

and

$$
\mathscr{F}_{\sigma}=\oplus_{1 \leq i \leq p} \mathscr{P}_{\sigma} .
$$

Using this, the freeness of $\mathscr{F}_{\sigma}$ over $\mathscr{F}$ follows from Proposition 2.3 and the statement for $\mathscr{F}_{\sigma}\left(\frac{1}{\iota}\right)$ follows by localization.

Definition 2.5. Let $\mathfrak{r}: \mathscr{F}_{\sigma} \rightarrow \mathscr{F}$ denote the projection with respect to the above basis. We will denote the projection $\mathscr{F}_{\sigma}\left(\frac{1}{\iota}\right) \rightarrow \mathscr{F}\left(\frac{1}{\iota}\right)$ by the same notation. Similarly, let $\mathfrak{s}: \mathscr{F}\left(\frac{1}{l}\right) \rightarrow \mathscr{F}$ denote the projection that has the effect of deleting the principal part of the Laurent series expansion for the component $p \mathbb{N}$, and is identity on the components $i+p \mathbb{N}$ with $0<i<p$.

Let $\underline{s}:=\left(s_{1}, \ldots, s_{k}\right)$, and $\underline{t}:=\left(t_{1}, \ldots, t_{l}\right)$. We write $\underline{t} \leq \underline{s}$ if there exists an increasing function $j:\{1, \ldots, l\} \rightarrow\{1, \ldots, k\}$ such that $t_{i} \leq s_{j(i)}$, for all $i$.

Lemma 2.6. Let $f$ be a power series function and let $g$ be defined as

$$
g(n)=\sum_{0<a<n} f(a) \sigma_{p}(\underline{s})(a)
$$

for some $\underline{s}:=\left(s_{1}, \ldots, s_{k}\right)$. Then

$$
g=\sum_{\underline{t} \leq \underline{s}} f_{\underline{t}} \sigma_{p}(\underline{t}),
$$

for some power series functions $f_{\underline{t}}$. Similarly, if $h$ is defined as

$$
h(n):=\sum_{\substack{0<a<n \\ p \backslash a}} \frac{f(a)}{a^{s}} \sigma_{p}(\underline{s})(a),
$$

for some $s \geq 1$ then

$$
h=\sum_{\underline{t} \leq \underline{s}^{\prime}} f_{\underline{t}} \sigma_{p}(\underline{t}),
$$

for some power series functions $f_{\underline{t}}$, where $\underline{s}^{\prime}:=\left(s_{1}, \ldots, s_{k}, s\right)$.

Proof. We will prove this by induction on $d(\underline{s})$. Suppose that $d(\underline{s})=0$ and hence $\sigma_{p}(\underline{s})=1$. Then for $g$ the assertion follows from Proposition 2.1. Let $f(z)=\sum_{0 \leq i} b_{i} z^{i}$, for $|z| \leq|p|$, then

$$
h(n)=b_{0} \sigma_{p}(s)(n)+\cdots+b_{s-1} \sigma_{p}(1)(n)+\sum_{\substack{0<a<n \\ p \mid a}} \bar{f}(a),
$$

where $\bar{f}(z):=b_{s}+b_{s+1} z+\cdots$. Again the statement follows from Proposition 2.1.

Now assume the statement for all $\underline{s}$ with $d(\underline{s}) \leq k$ and fix $\underline{s}:=\left(s_{1}, \ldots\right.$, $\left.s_{k+1}\right)$. Let $F$ be as in Proposition 2.1, then

$$
g(n)=F(n-1) \sigma_{p}(\underline{s})(n)-\sum_{\substack{0<n_{k+1}<n \\ p \mid n_{k+1}}} \frac{F\left(n_{k+1}\right)}{n_{k+1}^{s_{k+1}}} \sigma_{p}\left(s_{1}, \ldots, s_{k}\right)\left(n_{k+1}\right)
$$

and the statement follows from the induction hypothesis on $h$.

On the other hand,

$$
\begin{aligned}
h(n) & =\sum_{\substack{0<a<n \\
p \mid a}}\left(\frac{b_{0}}{a^{s}}+\cdots+\frac{b_{s-1}}{a}+\bar{f}(a)\right) \sigma_{p}(\underline{s})(a) \\
& =b_{0} \sigma_{p}(\underline{s}, s)(n)+\cdots+b_{s-1} \sigma_{p}(\underline{s}, 1)(n)+\sum_{\substack{0<a<n \\
p \mid a}} \bar{f}(a) \sigma_{p}(\underline{s})(a)
\end{aligned}
$$

and the statement follows by the statement that we just proved on $g$.
Proposition 2.7. For any $\underline{s}$ and $\underline{m}, \sigma(\underline{s} ; \underline{m}) \in \mathscr{F}_{\sigma}$.
Proof. We will prove this by induction on $d(\underline{s})$. If $d(\underline{s})=1$, then $\sigma(\underline{s}, \underline{m})=$ $\sigma_{p}(\underline{s})$ if $m_{1}=0$; and $\sigma(\underline{s}, \underline{m}) \in \mathscr{F}$ otherwise by Proposition 2.1. Suppose we know the result for $d(\underline{s}) \leq k$, and fix $\underline{s}$ with $d(\underline{s})=k+1$.

Let $\underline{s}=\left(s_{1}, \ldots, s_{k+1}\right), \underline{s}^{\prime}=\left(s_{1}, \ldots, s_{k}\right), \underline{m}=\left(m_{1}, \ldots, m_{k+1}\right)$, and $\underline{m}^{\prime}=$ $\left(m_{1}, \ldots, m_{k}\right)$. Since

$$
\sigma(\underline{s} ; \underline{m})(n)=\sum_{\substack{0<a<n \\ p \mid\left(a-m_{k+1}\right)}} \frac{\sigma\left(\underline{s}^{\prime} ; \underline{m}^{\prime}\right)(a)}{a^{s_{k+1}}}
$$

using the induction hypothesis we realize that we only need to show that functions of the form

$$
\sum_{\substack{0<a<n \\ p \backslash(a-m)}} \frac{f(a)}{a^{s}} \sigma_{p}(\underline{t})(a)
$$

with $f$ a power series function, are in $\mathscr{F}_{\sigma}$ and this is exactly the statement of the previous lemma.

In fact, from the proof above it follows that $\sigma(\underline{s} ; \underline{m})$ is an $\mathscr{F}$-linear combination of $\sigma_{p}(\underline{t})$ with $\underline{t} \leq \underline{s}$.

Definition 2.8. For a function $f \in \mathscr{F}_{\sigma}$, let $\tilde{f}:=\mathfrak{r}(f) \in \mathscr{F}$. We call $\tilde{f}$ the regularization of $f$. Since by the previous proposition $\sigma(\underline{s} ; \underline{m}) \in \mathscr{F}_{\sigma}$, we let $\tilde{\sigma}(\underline{s} ; \underline{m}) \in \mathscr{F}$ its regularization and $\underline{\sigma}(\underline{s} ; \underline{m})=\lim _{n \rightarrow 0} \tilde{\sigma}(\underline{s} ; \underline{m})(n)$.

For a function $f: \mathbb{N} \rightarrow \mathbb{Q}_{p}$ and $0 \leq m<p$, let $f_{[m]}$ denote the function which is equal to $f$ for values $n$ which are congruent to $m$ modulo $p$ and is 0 otherwise. Recall that $\gamma(\underline{s} ; \underline{m})(n):=n^{-s_{k}} \cdot \sigma\left(\underline{s}^{\prime} ; \underline{m}^{\prime}\right)_{\left[m_{k}\right]}(n)$. We will define the regularized version $\tilde{\gamma}(\underline{s} ; \underline{m})$ of $\gamma(\underline{s} ; \underline{m})$ as follows. If $m_{k} \neq 0$, then it is defined by $\tilde{\gamma}(\underline{s} ; \underline{m})(n)=n^{-s_{k}} \cdot \tilde{\sigma}\left(\underline{s}^{\prime} ; \underline{m}^{\prime}\right)_{\left[m_{k}\right]}(n)$. If $m_{k}=0$, and $p(z)=$
$a_{0}+a_{1} z+\cdots$ is such that $\tilde{\sigma}\left(\underline{s}^{\prime} ; \underline{m}^{\prime}\right)(n)=p(n)$ for $p \mid n$, then $\tilde{\gamma}(\underline{s} ; \underline{m})(n)=$ $a_{s_{k}}+a_{S_{k}+1} n+\cdots$, if $p \mid n$ and 0 otherwise. Finally we let $\underline{\gamma}(\underline{t} ; \underline{m})=$ $\lim _{n \rightarrow 0} \tilde{\gamma}(\underline{t} ; \underline{m})(n)$.

Another way to describe this is as follows. For any $\underline{s}$ and $\underline{m}, \gamma(\underline{s} ; \underline{m}) \in$ $\mathscr{F}_{\sigma}\left(\frac{1}{\iota}\right)$, and $\tilde{\gamma}(\underline{s} ; \underline{m}):=\mathfrak{s} \circ \mathfrak{r}(\gamma(\underline{s} ; \underline{m}))$.

Remark 2.9. Note that $\tilde{\sigma}(\underline{s} ; \underline{m})^{(n)}(0)=-n!\cdot \underline{\sigma}(\underline{s}, n ; \underline{m}, 0)=n!\cdot \underline{\gamma}(\underline{s}, n$; $\underline{m}, 0)$. The first identity follows from the fact that if $P_{k}(z)$ is the polynomial such that $P_{k}(n)$ is the sum of the $k$-th powers of the first $n$ positive integers then $(z+1) \mid P_{k}(z)$, for $k \geq 1$.

Definition 2.10. Let $\mathcal{P}_{w}$ (resp. $\mathcal{S}_{w}$, resp. $\tilde{\mathcal{S}}_{w}$ ) denote the $\mathbb{Q}$-space spanned by the $\underline{\sigma}(\underline{s} ; \underline{m})(\operatorname{resp} . \gamma(\underline{s} ; \underline{m})$, resp. $\tilde{\gamma}(\underline{s} ; \underline{m}))$, with $w(\underline{s})=w$, and $\mathcal{P}:=$ $\sum_{w} \mathcal{P}_{w}$ (resp. $\mathcal{S}:=\sum_{w} \mathcal{S}_{w}$, resp. $\left.\tilde{\mathcal{S}}:=\sum_{w} \tilde{\mathcal{S}}_{w}\right)$.

Let $\omega_{i}:=\operatorname{dlog}(z-i)$, for $i=0,1$ and $\omega_{p}:=\operatorname{dlog}\left(z^{p}-1\right)$.
Lemma 2.11. Let $f(z)=\sum_{1 \leq n} a_{n} z^{n}$, such that $d f=\omega \sum_{1 \leq n} \gamma(\underline{s} ; \underline{m})(n) z^{n}$. If $\omega=\omega_{0}$ then $a_{n}=\gamma\left(\left(s_{1}, \ldots, s_{k}+1\right) ; \underline{m}\right)(n)$. If $\omega=\omega_{1}$ then $a_{n}=-\sum_{0 \leq i \leq p-1} \gamma(\underline{s}, 1 ; \underline{m}, i)(n)$. If $\omega=\omega_{p}$ then $a_{n}=-p \gamma\left(\underline{s}, \underline{1} ; \underline{m}, m_{k}\right)(n)$.

Proof. Elementary computation.
Corollary 2.12. Suppose that $f(z)=\sum_{1 \leq n} q(n) z^{n}$, such that

$$
d f=\omega_{i} \sum_{1 \leq i} \alpha(n) z^{n}
$$

with $i=0,1$ or $p$ and $\alpha \in \mathcal{S}_{w}$. Then $q \in \mathcal{S}_{w+1}$.
Remark 2.13. If $g(z)=\sum_{1 \leq n} k(n) z^{n}$, with $k \in \mathscr{F}_{\sigma}\left(\frac{1}{\iota}\right)$, then we let $\mathfrak{r}(g)(z):=\sum_{1 \leq n} \mathfrak{r}(k)(n) z^{n}$. Similarly if $k \in \mathscr{F}\left(\frac{1}{l}\right)$, then we let $\mathfrak{s}(g)(z):=$ $\sum_{1 \leq n} \mathfrak{s}(k)(n) z^{n}$. Clearly, we have $\mathfrak{r}\left(g^{\prime}\right)=\mathfrak{r}(g)^{\prime}$. On the other hand, in general $\mathfrak{s}\left(g^{\prime}\right) \neq \mathfrak{s}(g)^{\prime}$. For example for $g(z)=\sum_{1 \leq n} \frac{z^{n}}{n}$, the left hand side is $\sum_{0 \leq n} z^{n}$, on the other hand the right hand side is $\sum_{\substack{0 \leq n \\ p \nmid n+1)}} z^{n}$. However, if $\mathfrak{s}\left(g^{\prime}\right)=f^{\prime}$ for some $f=\sum_{1 \leq n} t(n) z^{n}$, with $t \in \mathscr{F}$, then $\mathfrak{s}\left(g^{\prime}\right)=\mathfrak{s}(g)^{\prime}$. This follows from the basic observation that if $k(z)$ is a Laurent series such that $\mathfrak{s}(z k(z))=z t(z)$ for some power series $t(z)$, then the coefficient of $1 / z$ in $k(z)$ is 0 and hence $\mathfrak{s}(z k(z))=z \mathfrak{s}(k(z))$.

Proposition 2.14. Suppose that $f(z)=\sum_{1 \leq n} q(n) z^{n}$, such that

$$
\begin{equation*}
d f=\omega_{0} \sum_{1 \leq n} \alpha(n) z^{n}+\omega_{1} \sum_{1 \leq n} \beta(n) z^{n}+\omega_{p} \sum_{1 \leq n} \gamma(n) z^{n} \tag{2.1}
\end{equation*}
$$

with $\alpha, \beta, \gamma \in \sum_{a+b=w} \mathcal{P}_{a} \cdot \tilde{\mathcal{S}}_{b}$. If $\lim _{n \rightarrow 0} q(n)$ exists then $q \in \sum_{a+b=w+1} \mathcal{P}_{a} \cdot \tilde{\mathcal{S}}_{b}$.

Proof. We have

$$
n q(n)=\alpha(n)-\sum_{1 \leq k<n} \beta(k)-p \sum_{\substack{1 \leq k<n \\ p \mid(n-k)}} \gamma(k) .
$$

By Proposition 2.1, the function $n q(n)$ is a power series function and hence so is the function $q(n)$ when restricted to $\mathbb{N} \backslash p \mathbb{N}$. Let $r(z):=\sum_{0 \leq i} b_{i} z^{i}$ be the power series such that $n q(n)=r(n)$ for all $p \mid n$. The assumption on the limit implies that $\lim _{n \rightarrow 0} \frac{b_{0}}{n}$ exists. Hence $b_{0}=0$ and $q \in \mathscr{F}$.

By Corollary 2.12, there is $F(z)=\sum_{1 \leq n} s(n) z^{n}$ such that $s \in \sum_{a+b=w+1}$ $\mathcal{P}_{a} \cdot \mathcal{S}_{b}$ and $\mathfrak{s} \circ \mathfrak{r}\left(F^{\prime}\right) d z$ is equal to the right hand side of (2.1), and hence $\mathfrak{s} \circ \mathfrak{r}\left(F^{\prime}\right)=f^{\prime}$. Let $g=\mathfrak{r}(F)$. Then $\mathfrak{s}\left(g^{\prime}\right)=\mathfrak{s}\left(\mathfrak{r}(F)^{\prime}\right)=\mathfrak{s}\left(\mathfrak{r}\left(F^{\prime}\right)\right)=f^{\prime}$. Since we proved above that $q \in \mathscr{F}$, we conclude by Remark 2.13 that $\mathfrak{s}\left(g^{\prime}\right)=\mathfrak{s}(g)^{\prime}$. Therefore $\mathfrak{s}(g)^{\prime}=f^{\prime}$, and $f=\mathfrak{s}(g)=\mathfrak{s} \circ \mathfrak{r}(F)$. Hence $q$ is of the form as stated above.

Proposition 2.15. $\mathcal{P}$ is a $\mathbb{Q}$-algebra.

Proof. The statement follows from the shuffle product formula since this implies that $\mathcal{P}_{a} \cdot \mathcal{P}_{b} \subseteq \mathcal{P}_{a+b}$.

## 3. $p$-adic multi-zeta values

In this section we follow the notation of [4] with a few modifications. For the convenience of the reader we briefly recall this. For the details we refer the reader to [4]. Let $X$ be the thrice punctured line $\mathbb{P}^{1} \backslash\{0,1, \infty\}$ over $\mathbb{Q}_{p}$.

The category of unipotent vector bundles with connection on $X$ is a tannakian category with a canonical fiber functor $\omega(d R)$ called the de Rham fiber functor [4, §4.1]. The corresponding tannaka group is called the de

Rham fundamental group of $X$ and denoted by $\pi_{1, d R}(X)$. This is a prounipotent pro-algebraic group over $\mathbb{Q}_{p}$. The $\mathbb{Q}_{p}$ valued points of this proalgebraic group are the group-like elements in the Hopf algebra of noncommutative power series $\mathbb{Q}_{p}\left\langle\left\langle e_{0}, e_{1}\right\rangle\right\rangle$ in $e_{0}$ and $e_{1}$. Here $e_{i}$ are the derivations of $\omega(d R)$ which associate to a unipotent vector bundle with connection on $X / \mathbb{Q}_{p}$ its residue at the point $i$, for $i=0,1$. The coalgebra map on $\mathbb{Q}_{p}\left\langle\left\langle e_{0}, e_{1}\right\rangle\right\rangle$ is determined by the property that $\Delta\left(e_{i}\right)=1 \otimes e_{i}+e_{i} \otimes 1$, for $i=0,1$.

For distinct $i, j \in\{0,1, \infty\}, t_{i j}$ denotes the unit tangent vector at the point $i$ pointing towards the point $j$, e.g. $t_{01}$ is the tangent vector 1 at $0, t_{10}$ is the tangent vector -1 at 1 . There is an action $F_{*}$ of the crystalline frobenius on the fundamental groupoid of paths between any two of the tangential basepoints $t_{i j}$. Furthermore there is a canonical identification of the fiber functors at the tangential basepoints $t_{i j}$ and the fiber functor $\omega(d R)$. This last fact provides a path, called the de Rham path, from $t_{i j}$ to $t_{k l}$. We denote this path by $t_{k l} e(d R)_{t_{i j}}$. The composition $t_{01} e(d R)_{t_{10}} F_{*}\left(t_{10} e(d R)_{t_{01}}\right)$ is then a path at $t_{01}$ and under the identification of the fiber functor at $t_{01}$ with $\omega(d R)$, we get an element in $\pi_{1, d R}(X)\left(\mathbb{Q}_{p}\right)$ and hence a group-like element $g$ in $\mathbb{Q}_{p}\left\langle\left\langle e_{0}, e_{1}\right\rangle\right\rangle$. This element is our main object of study. We define $h \in \mathbb{Q}_{p}\left\langle\left\langle e_{0}, e_{1}\right\rangle\right\rangle$ similarly, starting with ${ }_{t_{01}} e(d R)_{t_{\infty 0}} F_{*}\left(t_{\infty 0} e(d R)_{t_{01}}\right)$.

Let $\mathcal{U}$ denote the rigid analytic space obtained by deleting from the projective line the open unit disc of radius 1 centered at 1 . Let $\mathcal{A}$ denote the ring of rigid analytic functions on $\mathcal{U}$. The map $\mathcal{F}(z)=z^{p}$ provides a good lifting of frobenius on $\mathcal{U}$ and thus gives, through various identifications, a group-like element $g(z)$ in $\mathcal{A}\left\langle\left\langle e_{0}, e_{1}\right\rangle\right\rangle$ [4, §5.1], where the last Hopf algebra is defined as above. In this paper we denote $g(z)$ by $\mathfrak{g}$.

Since $\mathfrak{g}$ is defined at $\infty$ it can be evaluated there. In fact, we have $\mathfrak{g}(\infty)=h$. The fundamental equation [4, (2) p.135] that connects $g$ and $h$ takes the form:

$$
\begin{equation*}
\left(e_{0}+e_{1}\right) h=h\left(e_{0}+g^{-1} e_{1} g\right) \tag{3.1}
\end{equation*}
$$

and the fundamental differential equation [4, (1) p.133] takes the form:

$$
\begin{equation*}
d \mathfrak{g}=p\left(e_{0} \mathfrak{g}-\mathfrak{g} e_{0}\right) \cdot \omega_{0}+e_{1} \mathfrak{g} \cdot \mathcal{F}^{*} \omega_{1}-p \mathfrak{g}\left(g^{-1} e_{1} g\right) \cdot \omega_{1} \tag{3.2}
\end{equation*}
$$

For every $e^{I}$, let $\mathfrak{g}\left[e^{I}\right]$ denote the coefficient of $e^{I}$ in $\mathfrak{g}$ and $\mathfrak{g}\left\{e^{I}\right\}$ denote the function that sends $n$ to the coefficient of $z^{n}$ in $\mathfrak{g}\left[e^{I}\right]$. If $I=$ $e_{0}^{i_{1}} e_{1}^{j_{1}} \cdots e_{0}^{i_{k}} e_{1}^{j_{k}}$, let $d(I):=\left|\left\{j_{t} \mid j_{t} \neq 0,1 \leq t \leq k\right\}\right|$ and $w(I):=\sum\left(i_{t}+j_{t}\right)$.

Theorem 3.1. For each $I, \mathfrak{g}\left\{e^{I}\right\} \in \sum_{a+b=w(I)} \mathcal{P}_{a} \cdot \tilde{\mathcal{S}}_{b}$ and $g\left[e^{I}\right] \in \mathcal{P}_{w(I)}$.
Proof. We will prove the statement by induction on $d(I)$.
Lemma 3.2. The statement above is true for $\mathfrak{g}\left\{e^{I}\right\}$, with $d(I) \leq 1$; for $\mathfrak{g}\left\{e_{1} e_{0}^{s} e_{1}\right\}$, with any $s \geq 0$; and for $g\left[e^{I}\right]$, with $d(I) \leq 1$.

Proof. We proved on [4, p. 138] that $\mathfrak{g}\left\{e_{0}^{s-1} e_{1}\right\}(n)=\frac{p^{s}}{n^{s}}$, if $p \nmid n$ and 0 otherwise. Hence $\mathfrak{g}\left\{e_{0}^{s-1} e_{1}\right\}=p^{s} \sum_{1 \leq i<p} \gamma(s ; i) \in \tilde{S}_{s}$, since $\gamma(s ; i)=\tilde{\gamma}(s ; i)$, for $i \neq 0$. The statement for $\mathfrak{g}\left\{e^{I}\right\}$, with $d(I) \leq 1$, then follows from the fact that $\mathfrak{g}$ is group-like.

Similarly, we proved on [4, p. 139] that $\mathfrak{g}\left\{e_{1} e_{0}^{s-1} e_{1}\right\}=$

$$
p^{s+1}\left((-1)^{s+1}\left(\sum_{\substack{0 \leq i, j<p \\ i \neq 0}} \gamma(s, 1 ; i, j)\right)-\sum_{\substack{0<i<p \\ i \neq 0}} \gamma(s, 1 ; i, i)\right) .
$$

Clearly, when $i, j \neq 0, \gamma(a, b ; i, j)=\tilde{\gamma}(a, b ; i, j)$. Note that for $i \neq 0, \gamma(s, 1$; $i, 0)(n)=n^{-1} \sigma(s ; i)(n)$, if $p \mid n$, and is 0 otherwise. Note that $\sigma(s ; i)$ is a power series function such that $\lim _{n \rightarrow 0} \sigma(s ; i)(n)=0[4, \mathrm{p} .139]$. This implies that, for $p \mid n, \sigma(s ; i)(n)=\sum_{1 \leq i} a_{i} n^{i}$, for some $a_{i} \in \mathbb{Q}_{p}$. Therefore $\gamma(s, 1 ; i, 0)=$ $\tilde{\gamma}(s, 1 ; i, 0)$. Combining these, we deduce that $\mathfrak{g}\left\{e_{1} e_{0}^{s-1} e_{1}\right\} \in \tilde{\mathcal{S}}_{s+1}$.

Finally, on $\left[4\right.$, p. 140], we proved that $g\left[e_{1}\right]=0$ and

$$
g\left[e_{0}^{s-1} e_{1}\right]=\frac{p^{s}}{s-1} \sum_{0<i<p} \sigma(s-1 ; i)^{(1)}(0)
$$

for $s \geq 1$. Since $\sigma(s-1 ; i)=\tilde{\sigma}(s-1 ; i)$, the claim follows from Remark 2.9. To deduce the statement for all $I$ with $d(I) \leq 1$, we use the fact that $g$ is group-like [4].

We will prove the result in several steps. Assume that we know the statement for:
(i) $\mathfrak{g}\left\{e^{I}\right\}$, with $d(I) \leq k$;
(ii) $\mathfrak{g}\left\{e_{1} e_{0}^{s_{k}} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right\}$, for all $0 \leq s_{i}$; and
(iii) $g\left[e^{I}\right]$, with $d(I) \leq k$.

Lemma 3.3. For $d(I) \leq k+1, \mathfrak{g}\left\{e^{I}\right\} \in \sum_{a+b=w(I)} \mathcal{P}_{a} \cdot \tilde{\mathcal{S}}_{b}$.
Proof. By (ii), we know the statement for $I=e_{1} e_{0}^{s_{k}} e_{1} \cdots e_{0}^{s_{1}} e_{1}$. It suffices to prove the statement for $e_{0}^{s_{k+1}} e_{1} e_{0}^{s_{k}} e_{1} \cdots e_{0}^{s_{1}} e_{1}$, and we will do this by induction
on $s_{k+1}$. Assume that $\mathfrak{g}\left\{e_{0}^{m} e_{1} e_{0}^{s_{k}} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right\} \in \sum_{a+b=w} \mathcal{P}_{a} \cdot \tilde{\mathcal{S}}_{b}$. Comparing the coefficient of $e_{0}^{m+1} e_{1} e_{0}^{s_{k}} e_{1} \cdots e_{0}^{s_{1}} e_{1}$ on both sides of (3.2), and using the inductive hypothesis, together with (i), (iii) and Proposition 2.15, we see that $d \mathfrak{g}\left[e_{0}^{m+1} e_{1} e_{0}^{s_{k}} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right]$ is of the form as in the statement of Proposition 2.14. Furthermore, we note that $\lim _{n \rightarrow 0} \mathfrak{g}\left\{e_{0}^{m+1} e_{1} e_{0}^{s_{k}} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right\}(n)$ exists [4, Proposition 2]. Therefore we can apply Proposition 2.14 to finish the proof.

Proposition 3.4. If $d(I) \leq k+1$ then $h\left[e^{I}\right] \in \mathcal{P}_{w(I)}$.
Proof. Note that $h\left[e^{I}\right]=\mathfrak{g}\left[e^{I}\right](\infty)=\lim _{n \rightarrow 0} \mathfrak{g}\left\{e^{I}\right\}(n)$. The statement then follows from Lemma 3.3, Remark 2.9, and Proposition 2.15.

The following simple lemma is crucial in what follows.
Lemma 3.5. For $s_{i} \geq 0, g^{-1}\left[e_{1} e_{0}^{s_{k+1}} \cdots e_{1} e_{0}^{s_{1}}\right]+g\left[e_{0}^{s_{k+1}} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right] \in \mathcal{P}_{w}$, where $w=w\left(e_{1} e_{0}^{s_{k+1}} \cdots e_{1} e_{0}^{s_{1}}\right)$.

Proof. Let us compare the coefficient of $e_{1} e_{0}^{s_{k+1}} \cdots e_{1} e_{0}^{s_{1}} e_{1}$ on both sides of (3.1).

The left hand side is $h\left[e_{0}^{s_{k}+1} \cdots e_{1} e_{0}^{s_{1}} e_{1}\right]$, which is in $\mathcal{P}_{w}$ by the Proposition 3.4. The right hand side is $\left(g^{-1} e_{1} g\right)\left[e_{1} e_{0}^{s_{k+1}} \cdots e_{1} e_{0}^{s_{1}} e_{1}\right]$, which is a sum of the expression in the statement of the lemma and sums of products of the form $g^{-1}\left[e^{I_{1}}\right] g\left[e^{I_{2}}\right]$ with $d\left(I_{j}\right) \leq k$, and $w\left(I_{1}\right)+w\left(I_{2}\right)=w$. The statement then follows from (iii) and Proposition 2.15.

Lemma 3.6. For $s_{i} \geq 0, h\left[e_{0}^{s_{k+1}} e_{1} e_{0}^{s_{k}} e_{1} \cdots e_{0}^{s_{1}} e_{1}^{2}\right]+g\left[e_{0}^{s_{k+1}+1} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right] \in$ $\mathcal{P}_{w+1}$, with $w$ as above.

Proof. Let us look at the coefficient of $e_{0}^{s_{k+1}+1} e_{1} e_{0}^{s_{k}} e_{1} \cdots e_{0}^{s_{1}} e_{1}^{2}$ with $s_{i} \geq 0$ in (3.1). The induction hypothesis, the fact that $h\left[e_{0}\right]=0$, and Proposition 3.4, imply that $h\left[e_{0}^{s_{k+1}} e_{1} e_{0}^{s_{k}} e_{1} \cdots e_{0}^{s_{1}} e_{1}^{2}\right]=g^{-1}\left[e_{0}^{s_{k+1}+1} e_{1} e_{0}^{s_{k}} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right]+$ (terms in $\mathcal{P}_{w+1}$ ). Then using Lemma 3.5 we have the statement.

Lemma 3.7. For every $s_{i} \geq 0$ there exist $t\left(\alpha_{k+1}, \ldots, \alpha_{1}\right) \in \mathbb{Q}$, such that

$$
h\left[e_{0}^{s_{k+2}} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right]-\sum t\left(\alpha_{k+1}, \ldots, \alpha_{1}\right) h\left[e_{1} e_{0}^{\alpha_{k+1}} e_{1} \cdots e_{0}^{\alpha_{1}} e_{1}\right]
$$

is in $\mathcal{P}_{w}$, where $w=w\left(e_{0}^{s_{k+2}} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right)$ and the sum is over $\underline{\alpha}=\left(\alpha_{k+1}, \ldots\right.$, $\left.\alpha_{1}\right)$ with $w(\underline{\alpha})=\sum s_{i}$.

Proof. There is nothing to prove if $s_{k+2}=0$, so we assume that $s_{k+2}>0$. Looking at the coefficient of $e_{0}^{s_{k+2}} e_{1} \cdots e_{0}^{s_{1}} e_{1} e_{0}$ on both sides of (3.1), and using the induction hypotheses together with the fact that $h\left[e_{0}\right]=g\left[e_{0}\right]=0$, we find that

$$
h\left[e_{0}^{s_{k+2}-1} e_{1} \cdots e_{0}^{s_{1}} e_{1} e_{0}\right]-h\left[e_{0}^{s_{k+2}} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right] \in \mathcal{P}_{w}
$$

Next using the shuffle formula for $0=h\left[e_{0}^{s_{k+2}-1} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right] h\left[e_{0}\right]$, and the above fact, we obtain that

$$
\left(s_{k+2}+1\right) h\left[e_{0}^{s_{k+2}} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right]+\sum_{1 \leq i \leq k+1}\left(s_{i}+1\right) h\left[e_{0}^{s_{k+2}-1} e_{1} \cdots e_{0}^{s_{i}+1} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right]
$$

is in $\mathcal{P}_{w}$. From this the assertion follows by induction on $s_{k+2}$.
Lemma 3.8. For $s_{i} \geq 0, \mathfrak{g}\left\{e_{1} e_{0}^{s_{k+1}} e_{1} e_{0}^{s_{k}} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right\} \in \tilde{\mathcal{S}}_{w}$, where we have $w=w\left(e_{1} e_{0}^{s_{k+1}} e_{1} e_{0}^{s_{k}} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right)$.

Proof. Let us look at the coefficient of $e_{1} e_{0}^{s_{k+1}} e_{1} e_{0}^{s_{k}} e_{1} \cdots e_{0}^{s_{1}} e_{1}$ in the differential equation (3.2) which gives $d \mathfrak{g}\left[e_{1} e_{0}^{s_{k+1}} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right]=$

$$
\mathfrak{g}\left[e_{0}^{s_{k+1}} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right] \cdot \mathcal{F}^{*} \omega_{1}-p\left(\mathfrak{g}\left(g^{-1} e_{1} g\right)\right)\left[e_{1} e_{0}^{s_{k+1}} e_{1} e_{0}^{s_{k}} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right] \cdot \omega_{1}
$$

By the induction all the terms contribute to give a term in the form that we are seeking except possibly the term $-p \omega_{1}\left(g^{-1}\left[e_{1} e_{0}^{s_{k+1}} \cdots e_{1} e_{0}^{s_{1}}\right]+\right.$ $\left.g\left[e_{0}^{s_{k+1}} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right]\right)$. But this is also in the form that we were looking for by Lemma 3.5.

Corollary 3.9. For $s_{i} \geq 0, h\left[e_{1} e_{0}^{s_{k+1}} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right] \in \mathcal{P}_{w}$, where we have $w=$ $w\left(e_{1} e_{0}^{s_{k+1}} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right)$.

Proof. Clear using the fact that $h=\mathfrak{g}(\infty)$.
Lemma 3.10. For $s_{i} \geq 0$ and $w=w\left(e_{0}^{s_{k+1}+1} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right)$, $g\left[e_{0}^{s_{k+1}+1} e_{1} \cdots\right.$ $\left.e_{0}^{s_{1}} e_{1}\right] \in \mathcal{P}_{w}$.

Proof. This follows from combining Lemma 3.6, Lemma 3.7, and Corollary 3.9.

Lemma 3.11. We have $g\left[e_{1} e_{0}^{s_{k}} e_{1} \cdots e_{0}^{s_{1}} e_{1}\right] \in \mathcal{P}_{w}$, with $w=w\left(e_{1} e_{0}^{s_{k}} \cdots e_{0}^{s_{1}} e_{1}\right)$.

Proof. If all $s_{i}=0$, then the expression is 0 . Otherwise let $j:=\max \left\{i \mid s_{i} \neq\right.$ $0\}$. Then applying Lemma 3.5 several times we see that it is sufficient to prove that $g\left[e_{0}^{s_{j}} e_{1} \cdots e_{0}^{s_{1}} e_{1}^{k+2-j}\right] \in \mathcal{P}_{w}$, which we did in the previous proposition.

This finishes the proof of the theorem.
Recall that the $p$-adic multi-zeta values $\zeta_{p}\left(s_{k}, \ldots, s_{1}\right)$ were defined as

$$
\begin{equation*}
g\left[e_{0}^{s_{k}-1} e_{1} \cdots e_{0}^{s_{1}-1} e_{1}\right]=p^{\sum s_{i}} \zeta_{p}\left(s_{k}, \ldots, s_{1}\right) \tag{3.3}
\end{equation*}
$$

in [4, Definition 3].
Let $\mathcal{Z}$ denote the $\mathbb{Q}$-space generated by the $p$-adic multi-zeta values. By the shuffle product formula this is an algebra.

Theorem 3.12. We have the inclusion $\mathcal{Z} \subseteq \mathcal{P}$.
Proof. This is a consequence of Theorem 3.1 and (3.3).
Furusho defined $p$-adic multiple-zeta values using Coleman's theory of iterated $p$-adic integrals, which is equivalent to studying the frobenius invariant path between the tangential basepoints $t_{01}$ and $t_{10}$. Our approach in [4] and here is based on Deligne's theory of the comparison isomorphism between the de Rham and the crystalline fundamental group. However, the $\mathbb{Q}$-space that these two different definitions generate are the same $[2$, Theorem 2.8, Examples 2.10] and hence the $p$-adic multiple-zeta values as defined by Furusho also lie in $\mathcal{P}$.

For the convenience of the reader, we will describe the relation between Furusho's definition and our definition using the notation above. Let $\gamma$ denote the frobenius invariant path from $t_{01}$ to $t_{10}$. Let $\omega:={ }_{t_{10}} e(d R)_{t_{01}}$ denote the canonical de Rham path from $t_{01}$ to $t_{10}$, and let $f=\omega^{-1} \gamma$. With this notation, we have $g=\omega^{-1} F_{*}(\omega)$. Note that $g$ and $f$ can be seen as group-like elements in $\mathbb{Q}_{p}\left\langle\left\langle e_{0}, e_{1}\right\rangle\right\rangle$. We denote the corresponding elements of $\mathbb{Q}_{p}\left\langle\left\langle e_{0}, e_{1}\right\rangle\right\rangle$ by $g\left(e_{0}, e_{1}\right)$ and $f\left(e_{0}, e_{1}\right)$. Since we have $F_{*}\left(e_{0}\right)=p e_{0}$ and $F_{*}\left(e_{1}\right)=p g^{-1} e_{1} g[4$, p. 131],

$$
F_{*} f\left(e_{0}, e_{1}\right)=f\left(p e_{0}, p g^{-1} e_{1} g\right)
$$

Applying $F_{*}$ to the identity $f=\omega^{-1} \gamma$, the invariance of $\gamma$ under frobenius and the definition of $g$ gives $f=g F_{*}(f)$ and hence

$$
\begin{equation*}
f\left(e_{0}, e_{1}\right)=g\left(e_{0}, e_{1}\right) f\left(p e_{0}, p g^{-1} e_{1} g\right) \tag{3.4}
\end{equation*}
$$

Furusho defines the $p$-adic multiple zeta value $\zeta_{p}^{f}\left(k_{1}, \ldots, k_{m}\right)$, with $k_{m}>$ 1 , as $(-1)^{m}$ times the coefficient of $e_{0}^{k_{m}-1} e_{1} \cdots e_{0}^{k_{1}-1} e_{1}$ in $f[2$, p. 1121]. As usual, by the shuffle product formula we see that all the other coefficients of $f$ can be expressed as $\mathbb{Q}$-linear combinations of these $p$-adic multiple zeta values. Let $\mathcal{Z}^{\prime}$ denote the $\mathbb{Q}$-space generated by the $\zeta_{p}^{f}\left(k_{1}, \ldots, k_{m}\right)$ 's. This is also the space generated by all the coefficients of $f$, just as $\mathcal{Z}$ is the space generated by all the coefficients of $g$. Let $\mathcal{Z}_{\leq w}$ and $\mathcal{Z}_{\leq w}^{\prime}$ denote the subspaces generated by the coefficients of the terms $e^{I}$ in $g$ and $f$ of weight less than or equal to $w$.

Lemma 3.13. For any $w$, we have $\mathcal{Z}_{\leq w}=\mathcal{Z}_{\leq w}^{\prime}$. Hence $\mathcal{Z}=\mathcal{Z}^{\prime}$.
Proof. We will prove the statement by induction on $w$. Comparing the coefficients of $e^{I}$ on both sides of equation (3.4) and letting $w=w(I)$, we have

$$
f\left[e^{I}\right]=g\left[e^{I}\right]+p^{w} f\left[e^{I}\right]+\varepsilon,
$$

where

$$
\varepsilon \in \sum_{1 \leq a \leq w-1} \mathcal{Z}_{a} \cdot \mathcal{Z}_{w-a}^{\prime}
$$

The induction hypothesis implies that $\varepsilon \in \mathcal{Z}_{\leq w}$ and $\varepsilon \in \mathcal{Z}_{\leq w}^{\prime}$. This together with the last identity implies that $f\left[e^{I}\right] \in \mathcal{Z}_{\leq w}$ and $g\left[e^{I}\right] \in \mathcal{Z}_{\leq w}^{\prime}$, which finishes the proof.

## References

[1] P. Deligne, Le groupe fondamental de la droite projective moins trois points. Galois Groups Over $\mathbb{Q}$, Ihara et. al., Editors (1989), 79-297.
[2] H. Furusho, p-adic multiple zeta values II. Tannakian interpretations. Amer. J. Math., 129 (2007), no. 4, 1105-1144.
[3] A. Goncharov, Multiple polylogarithms and mixed Tate motives. Preprint, arXiv:AG/0103059v4.
[4] S. Ünver, p-adic multi-zeta values. J. Number Theor., 108 (2004), 111156.
[5] S. Ünver, Cyclotomic p-adic multi-zeta values in depth two. Manuscripta Math., 149 (2016), no. 3-4, 405-441. DOI:10.1007/s00229-015-0789-8.

Mathematics Department, Koç University
Rumelifeneri Yolu, 34450, Istanbul, Turkey
\& Freie Universität Berlin, FB Mathematik und Informatik Arnimallee 3, 14195 Berlin, Germany
E-mail address: sunver@ku.edu.tr
Received November 24, 2014

