Valeurs spéciales de polylogarihmes multiples

par

M. WALDSCHMIDT

0. Introduction - Notation

A quite ambitious goal is to determine the algebraic relations among the numbers

$$\pi,\ \zeta(3),\ \zeta(5), \ldots, \zeta(2n+1), \ldots$$

The expected answer is disappointingly simple: it is widely believed that there are no relations, which means that these numbers should be algebraically independent:
(?) *For any $n \geq 0$ and any nonzero polynomial $P \in \mathbb{Z}[T_0, \ldots, T_n]$,*

$$P\bigl(\pi, \zeta(3), \zeta(5), \ldots, \zeta(2n+1)\bigr) \neq 0.$$

If true, this property would mean that there is no interesting algebraic structure. The situation changes drastically if we enlarge our set so as to include the so-called Multiple Zeta Values (MZV, also called *Polyzeta values, Euler-Zagier numbers* or *multiple harmonic series*):

$$\zeta(s_1, \ldots, s_k) = \sum_{n_1 > n_2 > \cdots > n_k \geq 1} \frac{1}{n_1^{s_1} \cdots n_k^{s_k}}$$

which are defined for k, $s_1, \ldots, s_k$ positive integers with $s_1 \geq 2$. There are plenty of relations between them, providing a rich algebraic structure. The most well known ones are Euler's relations

$$\zeta(2n)/\zeta(2)^n \in \mathbb{Q} \tag{0.1}$$

for any integer $n \geq 1$.

Here is a "proof" of the relation $\zeta(2) = \pi^2/6$ due to Euler, following [A 1976].

If $\alpha_1, \ldots, \alpha_n$ are the roots of the equation $a_0 + a_1 z + \cdots + a_n z^n = 0$, then

$$\sum_{i=1}^{n} \frac{1}{\alpha_i} = -\frac{a_1}{a_0}\cdot$$

Now

$$\cos\sqrt{z} = 1 - \frac{z}{2} + \frac{z^2}{24} + \cdots$$

and the roots of $\cos\sqrt{z} = 0$ are

$$\frac{1}{4}(2n+1)^2\pi^2 \qquad (n = 0, 1, \ldots)$$

and "hence"

$$\sum_{n\ge 0} \frac{1}{(2n+1)^2} = \frac{\pi^2}{8}\cdot$$

Since

$$\sum_{n\ge 0} \frac{1}{(2n+1)^2} = \sum_{n\ge 0} \frac{1}{n^2} - \sum_{n\ge 0} \frac{1}{(2n)^2} = \frac{3}{4}\zeta(2),$$

the relation $\zeta(2) = \pi^2/6$ follows.

It is not difficult to vindicate this proof, starting from the Hadamard product expansion for the cosine function:

$$\cos t = \prod_{n\in\mathbb{Z}} \left(1 - \frac{2t}{(2n+1)\pi}\right) = \prod_{n=0}^{\infty} \left(1 - \frac{4t^2}{(2n+1)^2\pi^2}\right).$$

The point is that there is no extra exponential factor. $\square$

There are very few results on the independence of these numbers: it is known that π is a transcendental numbers, hence so are all $\zeta(2n)$, $n \ge 1$. It is also known that $\zeta(3)$ is irrational (Apéry, 1978), and that infinitely many $\zeta(2n+1)$ are irrational [Ri 2000], [BR 2001] (further sharper more recent results have been achieved by T. Rivoal). This is all for the negative side!

Let us have a look at the positive side.

One easily gets quadratic relations between MZV when one multiplies two such series: it is easy to express the product as a linear combination of MZV. We shall study this phenomenon in detail, but we just give one easy example. Splitting the set of (n, m) with $n \ge 1$ and $m \ge 1$ into three disjoint subsets with respectively $n > m$, $m > n$ and $n = m$, we deduce, for $s \ge 2$ and $s' \ge 2$,

$$\sum_{n\ge 1} n^{-s} \sum_{m\ge 1} m^{-s'} = \sum_{n>m\ge 1} n^{-s} m^{-s'} + \sum_{m>n\ge 1} m^{-s'} n^{-s} + \sum_{n\ge 1} n^{-s-s'},$$

which is Nielsen Reflexion Formula [N 1904]

$$\zeta(s)\zeta(s') = \zeta(s, s') + \zeta(s', s) + \zeta(s + s') \tag{0.2}$$

for $s \geq 2$ and $s' \geq 2$. For instance

$$\zeta(2)^2 = 2\zeta(2,2) + \zeta(4). \tag{0.3}$$

Such expressions of the product of two zeta values as a linear combination of zeta values, arising from the product of two series, will be called "stuffle relations".

We introduce another type of algebraic relations between MZV, coming from their expressions as integrals: the product of two such integrals is a linear combination of MZV.

The classical polylogarithms

$$\mathrm{Li}_s(z) = \sum_{n\geq 1} \frac{z^n}{n^s},$$

are analytic in the unit disk $|z| < 1$. These functions Li_s are also defined recursively, starting from

$$\mathrm{Li}_1(z) = \sum_{n\geq 1} \frac{z^n}{n} = -\log(1-z),$$

and using the differential equations

$$z\frac{d}{dz}\mathrm{Li}_s(z) = \mathrm{Li}_{s-1}(z) \quad (s \geq 2),$$

together with the initial conditions $\mathrm{Li}_s(0) = 0$.

We express these functions as integrals: for $s = 1$ we have

$$\mathrm{Li}_1(z) = -\log(1-z) = \int_0^z \frac{dt}{1-t},$$

where the complex integral is over any path from 0 to z inside the unit circle. Next

$$\mathrm{Li}_2(z) = \int_0^z \mathrm{Li}_1(t)\frac{dt}{t} = \int_0^z \frac{dt}{t}\int_0^t \frac{du}{1-u},$$

and by induction, for $s \geq 2$, (cf. [L 1981], (7.2))

$$\mathrm{Li}_s(z) = \int_0^z \mathrm{Li}_{s-1}(t)\frac{dt}{t} = \int_0^z \frac{dt_1}{t_1}\int_0^{t_1}\frac{dt_2}{t_2}\cdots\int_0^{t_{s-2}}\frac{dt_{s-1}}{t_{s-1}}\int_0^{t_{s-1}}\frac{dt_s}{1-t_s}.$$

As pointed out to me by C. Viola, one also checks this formula with the change of variables

$$\left\{\begin{array}{rclrcl} t_1 & = & x_1, & x_1 & = & t_1,\\ t_2 & = & x_1x_2, & x_2 & = & t_2/t_1,\\ & \vdots & & & \vdots & \\ t_i & = & x_1\cdots x_i, & x_i & = & t_i/t_{i-1},\\ & \vdots & & & \vdots & \\ t_s & = & x_1\cdots x_s, & x_s & = & t_s/t_{s-1}. \end{array}\right. \qquad dt_1\cdots dt_s = x_1^{s-1}x_2^{s-2}\cdots x_{s-1}dx_1\cdots dx_s.$$

Similar integral expressions are valid for multiple polylogarithms in one variable:

$$\mathrm{Li}_{\underline{s}}(z) = \sum_{n_1 > n_2 > \cdots > n_k \geq 1} \frac{z^{n_1}}{n_1^{s_1} \cdots n_k^{s_k}},$$

for $\underline{s} = (s_1, \ldots, s_k)$. We give three examples. From

$$(z-1)\frac{d}{dz}\mathrm{Li}_{(1,1)}(z) = \mathrm{Li}_1(z) \quad \text{with} \quad \mathrm{Li}_{(1,1)}(0) = 0$$

we deduce

$$\mathrm{Li}_{(1,1)}(z) = \int_0^z \mathrm{Li}_1(t)\frac{dt}{1-t} = \int_0^z \frac{dt_1}{1-t_1}\int_0^{t_1}\frac{dt_2}{1-t_2} = \frac{1}{2}\bigl(\log(1-z)\bigr)^2.$$

Next, from

$$(z-1)\frac{d}{dz}\mathrm{Li}_{(1,2)}(z) = \mathrm{Li}_2(z) \quad \text{with} \quad \mathrm{Li}_{(1,2)}(0) = 0$$

we infer

$$\mathrm{Li}_{(1,2)}(z) = \int_0^z \mathrm{Li}_2(t)\frac{dt}{1-t} = \int_0^z \frac{dt_1}{1-t_1}\int_0^{t_1}\frac{dt_2}{t_2}\int_0^{t_2}\frac{dt_3}{1-t_3}.$$

Finally from

$$z\frac{d}{dz}\mathrm{Li}_{(2,1)}(z) = \mathrm{Li}_{(1,1)}(z) \quad \text{with} \quad \mathrm{Li}_{(2,1)}(0) = 0$$

we derive an expression of $\mathrm{Li}_{(2,1)}(z)$ as a triple integral

$$\mathrm{Li}_{(2,1)}(z) = \int_0^z \frac{dt_1}{t_1}\int_0^{t_1}\frac{dt_2}{1-t_2}\int_0^{t_2}\frac{dt_3}{1-t_3}.$$

Consider now the product of $\mathrm{Li}_1(z)$ and $\mathrm{Li}_2(z)$:

$$\mathrm{Li}_1(z)\mathrm{Li}_2(z) = \int_0^z \frac{dt}{1-t}\int_0^z \frac{du_1}{u_1}\int_0^{u_1}\frac{du_2}{1-u_2}.$$

For simplicity of notation, we assume z is real in the range $0 < z < 1$. The set of (t, u_1, u_2) in $\mathbb{R}^3$ satisfying $0 < t < z$ and $0 < u_2 < u_1 < z$ splits into three subsets

$$0 < t < u_2 < u_1 < z, \quad 0 < u_2 < t < u_1 < z, \quad 0 < u_2 < u_1 < t < z,$$

and two further subsets (with either $t = u_1$ or else $t = u_2$) which we are not interested with, since they have Lebesgue dimension 0 and hence do not contribute to the integral. The Cartesian product $\Delta_1(z) \times \Delta_2(z)$ is the union of three domains isomorphic to $\Delta_3(z)$. Indeed, consider the points

$$O = (0,0,0),\ A = (z,0,0),\ B = (z,z,0),\ C = (z,z,z),\ D = (0,z,z),\ E = (0,z,0).$$

Then the domain $\{0 \le x_1 \le z,\ 0 \le x_3 \le x_2 \le z\}$, which is the convex hull of

$$\{O, A, B, E, D, C\},$$

is the union of the three domains

$$0 \le x_3 \le x_2 \le x_1 \le z, \qquad 0 \le x_3 \le x_1 \le x_2 \le z, \qquad 0 \le x_1 \le x_3 \le x_2 \le z,$$

which are the convex hulls of

$$\{O, A, B, C\}, \qquad \{O, B, C, E\}, \qquad \{O, C, D, E\}$$

respectively. Therefore the product $\mathrm{Li}_1(z)\mathrm{Li}_2(z)$ is the sum of three integrals which we already met:

$$\mathrm{Li}_1(z)\mathrm{Li}_2(z) = 2\mathrm{Li}_{(2,1)}(z) + \mathrm{Li}_{(1,2)}(z). \tag{0.4}$$

In the same way, if we decompose the domain

$$1 > z > t_1 > t_2 > 0, \quad 1 > z > u_1 > u_2 > 0$$

into six disjoint domains (and further subsets of zero dimension) obtained by "shuffling" (t_1, t_2) with (u_1, u_2):

$$z > t_1 > t_2 > u_1 > u_2 > 0, \quad z > t_1 > u_1 > t_2 > u_2 > 0, \quad z > u_1 > t_1 > t_2 > u_2 > 0,$$

$$z > t_1 > u_1 > u_2 > t_2 > 0, \quad z > u_1 > t_1 > u_2 > t_2 > 0, \quad z > u_1 > u_2 > t_1 > t_2 > 0,$$

one deduces

$$\mathrm{Li}_2(z)^2 = 4\mathrm{Li}_{(3,1)}(z) + 2\mathrm{Li}_{(2,2)}(z). \tag{0.5}$$

For $z = 1$ we get

$$\zeta(2)^2 = 4\zeta(3,1) + 2\zeta(2,2). \tag{0.6}$$

This is a typical example of a "shuffle relation".

Combining the shuffle relations with the stuffle relations arising from product of series, one deduces linear relations between MZV, like

$$\zeta(4) = 4\zeta(3,1).$$

We also claim

$$\zeta(3) = \zeta(2,1). \tag{0.7}$$

Consider the double polylogarithms in two variables

$$\mathrm{Li}_{(s_1,s_2)}(z_1,z_2)=\sum_{n_1>n_2\geq 1}\frac{z_1^{n_1}z_2^{n_2}}{n_1^{s_1}n_2^{s_2}}.$$

Notice that

$$\mathrm{Li}_{(s_1,s_2)}(z)=\mathrm{Li}_{(s_1,s_2)}(z,1).$$

Then one easily checks, by multiplying the series,

$$\mathrm{Li}_s(z)\mathrm{Li}_{s'}(z)=\mathrm{Li}_{(s,s')}(z,z)+\mathrm{Li}_{(s',s)}(z,z)+\mathrm{Li}_{s+s'}(z^2)$$

for $s\geq 1$ and $s'\geq 1$. In particular

$$\mathrm{Li}_1(z)\mathrm{Li}_2(z)=\mathrm{Li}_{(1,2)}(z,z)+\mathrm{Li}_{(2,1)}(z,z)+\mathrm{Li}_3(z^2). \tag{0.8}$$

We combine with the relation (0.4) arising from integrals and deduce

$$\mathrm{Li}_3(z^2)+\mathrm{Li}_{(2,1)}(z,z)-2\mathrm{Li}_{(2,1)}(z,1)=\mathrm{Li}_{(1,2)}(z,1)-\mathrm{Li}_{(1,2)}(z,z). \tag{0.9}$$

As $z\to 1$ the left hand side converges towards $\zeta(3)-\zeta(2,1)$. We claim that the difference

$$F(z)=\mathrm{Li}_{(1,2)}(z,1)-\mathrm{Li}_{(1,2)}(z,z)=\sum_{n_1>n_2\geq 1}\frac{z^{n_1}(1-z^{n_2})}{n_1n_2^2}$$

tends to 0 as z tends to 1 inside the unit circle. Indeed for $|z|<1$ we have

$$|1-z^{n_2}|=|(1-z)(1+z+\cdots+z^{n_2-1})|<n_2|1-z|,$$

hence

$$\sum_{n_2=1}^{n_1-1}\frac{|1-z^{n_2}|}{n_2^2}<|1-z|\sum_{n_2=1}^{n_1-1}\frac{1}{n_2}$$

and

$$|F(z)|\leq|1-z|\mathrm{Li}_{(1,1)}(|z|)=\frac{1}{2}|1-z|\Big(\log\big(1/(1-|z|)\big)\Big)^2.$$

This completes the proof of Euler's formula (0.7). $\square$

Notation. Given a string $a_1,\dots,a_k$ of integers, the notation $\{a_1,\dots,a_k\}_n$ stands for the kn-tuple

$$(a_1,\dots,a_k,\dots,a_1,\dots,a_k),$$

where the string $a_1,\dots,a_k$ is repeated n times. For instance $\{1,2\}_3=(1,2,1,2,1,2)$.

1. Noncommutative Polynomials and Power Series

1.1. The Free Algebra $\mathfrak{H} = K\langle X\rangle$ on a Set X

Let K be a subfield of $\mathbb{R}$ (most often we shall take either $K = \mathbb{Q}$ or else $K = \mathbb{R}$). Consider the universal problem of constructing a K-algebra $K\langle X\rangle$ and a map $i : X \to K\langle X\rangle$ such that, for any pair (A, f) where A is a K-algebra and f a map $X \to A$, there is a unique morphism $\overline{f}$ of K-algebras for which the diagram

$$\begin{tikzcd} X \arrow[r, "i"] \arrow[dr, "f"'] & K\langle X\rangle \arrow[d, "\bar{f}"] \\ & A \end{tikzcd}$$

commutes.

If X consists of a single point, then the solution is the ring of commutative polynomials in a single variable. For a general set X, if we replace the category of K-algebras by the category of commutative algebras, then the solution is the ring of polynomials in a set of indeterminates indexed by X. For convenience of notation we shall assume that the elements in X are algebraically independent over K. Hence this ring of polynomials can be written simply $K[X]$.

Here we do not require commutativity, and the solution is given by non-commutative polynomials.

Denote by $X^* = X^{(\mathbb{N})}$ the set of finite sequences of elements in X, including the empty sequence e. Write $x_1 \cdots x_p$ with $p \geq 0$ such a sequence (it is called a *word* on the *alphabet* X - the elements x_i in X are the *letters*). This set is endowed with a monoid structure, which produces *the universal free monoid with basis* X, and the law is *concatenation*:

$$(x_1 \cdots x_p)(x_{p+1} \cdots x_{p+q}) = x_1 \cdots x_{p+q}.$$

The neutral element is e.

Next consider the set $K^{(X^*)}$ of maps $X^* \to K$ with finite support; for such a map S write $(S|w)$ the image of $w \in X^*$ in K and write also

$$S = \sum_{w \in X^*} (S|w) w. \tag{1.1}$$

By definition, for $S \in K^{(X^*)}$ the *support* of S is the finite set

$$\mathrm{Supp} S = \{w \in X^* \; ; \; (S|w) \neq 0\}.$$

On $K^{(X^*)}$ define an addition by

$$(S + T|w) = (S|w) + (T|w) \quad \text{for any } w \in X^* \tag{1.2}$$

and a multiplication (*) by

$$(1.3) \qquad (ST|w) = \sum_{uv=w} (S|u)(T|v)$$

where, for each $w \in X^*$, the sum is over the (finite) set of (u,v) in $X^* \times X^*$ such that $uv = w$. Further, for $\lambda \in K$ and $S \in K^{(X^*)}$, define $\lambda S \in K^{(X^*)}$ by

$$(1.4) \qquad (\lambda S|w) = \lambda(S|w) \quad \text{for any } w \in X^*.$$

With these laws one checks that the set $K^{(X^*)}$ becomes a K-algebra, solution of the above universal problem, which is therefore denoted by $K\langle X\rangle$ and is called the *free algebra on* X.

This is a graded algebra, when elements of X are given weight 1: the weight of a word $x_1 \cdots x_p$ is p, and for $p \geq 0$ the set $K\langle X\rangle_p$ of $S \in K\langle X\rangle$ for which

$$(S|w) = 0 \quad \text{if } w \in X^* \text{ has weight} \neq p$$

is the K-vector subspace whose basis is the set of words of length p. For $p = 0$, $K\langle X\rangle_0$ is the set Ke of "constant" polynomials λe, $\lambda \in K$ - it is the K-subspace of dimension 1 spanned by e. For any $S \in K\langle X\rangle_p$ and $T \in K\langle X\rangle_q$, we have

$$ST \in K\langle X\rangle_{p+q}.$$

If X is finite with n elements, then for each $p \geq 0$ there are n^p words of weight p, hence the dimension of $K\langle X\rangle_p$ over K is n^p, and the Poincaré series is

$$\sum_{p\geq 0} t^p \dim_K K\langle X\rangle_p = \frac{1}{1-nt}.$$

We shall consider mainly two examples: the first one is where $X = \{x_0, x_1\}$ has two elements; in this case the algebra $K\langle x_0, x_1\rangle$ will be denoted by $\mathfrak{H}$. Each word w in X^* can be written $x_{\epsilon_1} \cdots x_{\epsilon_p}$ where each ϵ_i is either 0 or 1 and the integer p is the weight of w. The number of $i \in \{1, \ldots p\}$ with $\epsilon_i = 1$ is called the *length* (or the *depth*) of w.

We shall denote by X^*x_1 the set of word which end with x_1, and by $x_0X^*x_1$ the set of words which start with x_0 and end with x_1. The subalgebra of $\mathfrak{H}$ spanned by X^*x_1 is

$$\mathfrak{H}^1 = Ke + \mathfrak{H}x_1,$$

and $\mathfrak{H}x_1$ is a left ideal of $\mathfrak{H}$. Also the subalgebra of $\mathfrak{H}^1$ spanned by $x_0X^*x_1$ is

$$\mathfrak{H}^0 = Ke + x_0\mathfrak{H}x_1.$$

(*) S Sometimes called *Cauchy product* - it is the usual multiplication, in opposition to the *Hadamard product* where $(ST|w) = (S|w)(T|w)$.

The algebra $\mathfrak{H}^1$ is our second example of a free algebra: it is the free algebra on the countable set $Y = \{y_1, \ldots, y_s, \ldots\}$, where, for $s \geq 1$, y_s denotes $x_0^{s-1}x_1$. It is easy to check that the set X^*x_1 is nothing else than the set of $y_{s_1} \cdots y_{s_k}$, where $(s_1, \ldots, s_k)$ ranges over the finite sequences of positive integers with $k \geq 1$ and $s_j \geq 1$ for $1 \leq j \leq k$. For $\underline{s} = (s_1, \ldots, s_k)$ with $k \geq 0$ it will be convenient to write $y_{\underline{s}}$ for $y_{s_1} \cdots y_{s_k}$, so that

$$y_{\underline{s}} = x_0^{s_1-1}x_1 \cdots x_0^{s_k-1}x_1$$

and the empty product (for $k = 0$) is, as usual, the empty word e.

In the same way, $\mathfrak{H}^0$ is nothing but the free algebra $K\langle y_2, \ldots, y_s, \ldots\rangle$, since the set $x_0X^*x_1$ coincides with the set of $y_{s_1} \cdots y_{s_k}$, where $(s_1, \ldots, s_k)$ ranges over the finite sequences of positive integers with $k \geq 1$, $s_1 \geq 2$ and $s_j \geq 1$ for $2 \leq j \leq k$.

An interesting phenomenon, which does not occur in the commutative case, is that the free algebra $k\langle x_0, x_1\rangle$ on a set with only two elements contains as a subalgebra the free algebra $k\langle y_1, y_2, \ldots\rangle$ on a set with countably many elements. Notice that this last algebra also contains as a subalgebra the free algebra on a set with n elements, namely $k\langle y_1, y_2, \ldots, y_n\rangle$. From this point of view it suffices to deal with only two variables!

1.2. The Algebra $\widehat{\mathfrak{H}} = K\langle\langle X\rangle\rangle$ of Formal Power Series

Let us come back for a while to the general case of a set X. According to the definition of $K\langle X\rangle$ as a solution of a universal problem, for each K-algebra A the map $f \to \overline{f}$ defines a bijection between A^X and the set of morphisms of K-algebras $K\langle X\rangle \to A$.

We introduce now the algebra $\widehat{\mathfrak{H}} = K\langle\langle X\rangle\rangle$ *of formal power series on* X and we shall see that it is isomorphic to the *dual* of $K\langle X\rangle$, which is the set $\mathrm{Hom}_K\big(K\langle X\rangle, K\big)$ of K-linear maps $K\langle X\rangle \to K$.

The underlying set of the algebra $K\langle\langle X\rangle\rangle$ is the set K^{X^*} of maps $X^* \to K$ - here there is no restriction on the support. For such a map S write $(S|w)$ the image of $w \in X^*$ in K and write also

$$S = \sum_{w\in X^*} (S|w)w.$$

On this set K^{X^*} the addition is defined by (1.2) and the multiplication is again Cauchy product (1.3). Further, for $\lambda \in K$ and $S \in K^{(X^*)}$, define $\lambda S \in K^{X^*}$ by (1.4). With these laws one checks that the set K^{X^*} becomes a K-algebra which we denote by either $K\langle\langle X\rangle\rangle$ of $\widehat{\mathfrak{H}}$.

To a formal power series S we associate a K-linear map:

$$\begin{array}{ccc} K\langle X\rangle & \longrightarrow & K \\ P & \longmapsto & \displaystyle\sum_{w\in X^*} (S|w)(P|w). \end{array}$$

Notice that the sum is finite since $P \in K\langle X\rangle$ has finite support.

Since X^* is a basis of the K-vector space $K\langle X\rangle$, a linear map $f \in \mathrm{Hom}_K\big(K\langle X\rangle, K\big)$ is uniquely determines by its values $(f|w)$ on the set X^*. Hence the map

$$\begin{array}{ccc} \mathrm{Hom}_K\big(K\langle X\rangle, K\big) & \longrightarrow & \widehat{\mathfrak{H}} \\ f & \longmapsto & \sum_{w\in X^*}(f|w)w \end{array}$$

is an isomorphism of vector spaces between the dual $\mathrm{Hom}_K\big(K\langle X\rangle, K\big)$ of $\mathfrak{H} = K\langle X\rangle$ and $\widehat{\mathfrak{H}}$. This is the classical dual; there are other notions of dual, in particular the "graduate dual", which in the present case is isomorphic to $\mathfrak{H}$, and the "restricted dual", which is the field $\mathrm{Rat}_K(X)$ of series which are "rational" which we now consider.

1.3. Rational Series

We introduce a map, denoted with a star * (not the same star as in the notation X^* for the set of words!), from the set of series S in $\widehat{\mathfrak{H}}$ which satisfy $(S|e) = 0$ to $\widehat{\mathfrak{H}}$, defined by

$$S^\star = \sum_{n\geq 0} S^n = e + S + S^2 + \cdots \tag{1.5}$$

The fact that the right hand side of (1.5) is well defined is a consequence of the assumption $(S|e) = 0$. Notice that $S^\star$ is the unique solution to the equation

$$(1 - S)S^\star = e,$$

and it is also the unique solution to the equation

$$S^\star(1 - S) = e.$$

A *rational* series is a series in $\widehat{\mathfrak{H}}$ which is obtained by using only a finite number of letters (this is a restriction only in case in case X is infinite), as well as a finite number of *rational operations*, namely addition (1.2), product (1.3), multiplication (1.4) by an element in K and the star (1.5). The set of rational series over K is a field $\mathrm{Rat}_K(X)$.

For instance for $x \in X$ the series

$$e + x^2 + x^4 + \cdots + x^{2n} + \cdots = x^\star(-x)^\star$$

is rational, and also the series

$$\sum_{p\geq 0} \varphi_m(p) x^p = (mx)^\star,$$

when $\varphi_m(p) = m^p$ is the number of words of weight p on the alphabet with m letters. Series like

$$\sum_{p\geq 0} x^p/p, \quad \sum_{p\geq 0} x^p/p!, \quad \sum_{p\geq 0} x^{2^p}$$

are not rational: if X has a single elements, say x, rational series can be identified with elements in $K(x)$ with no poles at $x = 0$.

For a series S without constant term, i.e. such that $(S|e) = 0$, one defines

$$\exp(S) = \sum_{n=0}^{\infty} \frac{S^n}{n!}\cdot$$

It is easy to check for instance that if S satisfies $(S|e)=0$ then the series

$$T=\sum_{n=1}^{\infty}\frac{S^n}{n}$$

is well defined and has

$$\exp(T)=S^\star.$$

1.4. The Shuffle Product and the Algebra $\mathfrak{H}_{ш}$

Let again X be a set and K a field. On $K\langle X\rangle$ we define the *shuffle* product as follows. On the words, the map $ш : X^*\times X^*\to\mathfrak{H}$ is defined by the formula

$$(x_1\cdots x_p)ш(x_{p+1}\cdots x_{p+q})=\sum_{\sigma\in\mathfrak{S}_{p,q}}x_{\sigma(1)}\cdots x_{\sigma(p+q)},$$

where $\mathfrak{S}_{p,q}$ denotes the set of permutation σ on $\{1,\ldots,p+q\}$ satisfying

$$\sigma(1)<\sigma(2)<\cdots<\sigma(p)\quad\text{and}\quad\sigma(p+1)<\sigma(p+2)<\cdots<\sigma(p+q).$$

This set $\mathfrak{S}_{p,q}$ has $(p+q)!/p!q!$ elements; it is the disjoint union of two subsets, the first one with $(p-1+q)!/(p-1)!q!$ elements consists of those σ for which $\sigma(1)=1$, and the second one with $(p+q-1)!/p!(q-1)!$ elements consists of those σ for which $\sigma(p+1)=1$. Accordingly, the previous definition of $ш : X^*\times X^*\to\mathfrak{H}$ is equivalent to the following inductive one:

$$e ш w = w ш e = w \quad\text{for any } w\in X^*,$$

and

$$(xu)ш(yv)=x\bigl(uш(yv)\bigr)+y\bigl((xu)шv\bigr)$$

for x and y in X (letters), u and v in X^* (words).

`Example.` For k and ℓ non-negative integers and $x\in X$,

$$x^t ш x^\ell=\frac{(k+\ell)!}{k!\ell!}x^{k+\ell}.$$

From

$$x_1x_2шx_3x_4=x_1x_2x_3x_4+x_1x_3x_2x_4+x_1x_3x_4x_2+x_3x_1x_2x_4+x_3x_4x_1x_2$$

one deduces

$$x_0x_1шx_0x_1=2x_0x_1x_0x_1+4x_0^2x_1^2.$$

In the same way the relation

$$x_0x_1шx_0^2x_1=x_0x_1x_0^2x_1+3x_0^2x_1x_0x_1+6x_0^3x_1^2$$

is easier to check by computing first $x_0x_1 ш x_2x_3x_4$.

Notice that the shuffle product of two words is in general not a word but a polynomial in $K\langle X\rangle$. We extend the definition of $ш : X^* \times X^* \to \mathfrak{H}$ to $ш : \mathfrak{H} \times \mathfrak{H} \to \mathfrak{H}$ by distributivity with respect to addition:

$$\sum_{u\in X^*}(S|u)u \;ш \sum_{v\in X^*}(T|v)v = \sum_{u\in X^*}\sum_{v\in X^*}(S|u)(T|v)u ш v.$$

One checks that the shuffle ш endows $K\langle X\rangle$ with a structure of commutative K-algebra.

From now on we consider only the special case $X = \{x_0, x_1\}$. This algebra will be denoted by $\mathfrak{H}_ш$. Since $\mathfrak{H}^1$ as well as $\mathfrak{H}^0$ are stable under ш, they define subalgebras

$$\mathfrak{H}^0_ш \subset \mathfrak{H}^1_ш \subset \mathfrak{H}_ш.$$

There is a description of the shuffle product in terms of automata due to Schutzenberger (see [R 1993] and [Lo 2002]). We only give an example with a sketch of proof of the following so-called "syntaxic" identity (Minh-Petitot):

Lemma 1.6. *The following identity holds:*

$$(x_0x_1)^\star ш (-x_0x_1)^\star = (-4x_0^2x_1^2)^\star.$$

Sketch of proof. To a series $S^\star$ one associates an automaton, with the following property: the sum of paths going out from the entry gate is S. As an example the series associated to

(1.7)
$$\begin{tikzcd} \overset{\Longleftarrow}{\Longrightarrow} \boxed{1} \arrow[r, shift right, "x_0"'] & \boxed{2} \arrow[l, shift right, "x_1"'] \end{tikzcd}$$

is

$$S_1 = e + x_0x_1 + (x_0x_1)^2 + \cdots + (x_0x_1)^n + \cdots = (x_0x_1)^\star$$

and similarly the series associated to

(1.8)
$$\begin{tikzcd} \overset{\Longleftarrow}{\Longrightarrow} \boxed{A} \arrow[r, shift right, "-x_0"'] & \boxed{B} \arrow[l, shift right, "x_1"'] \end{tikzcd}$$

is

$$S_A = e - x_0x_1 + (x_0x_1)^2 + \cdots + (-x_0x_1)^n + \cdots = (-x_0x_1)^\star.$$

The "shuffle product" of these two automata (we do not give the general definition, only this example) is the following

(1.9)
$$\begin{tikzcd} \overset{\Longleftarrow}{\Longrightarrow} \boxed{1A} \arrow[r, shift right, "x_0"'] \arrow[d, shift right, "-x_0"'] & \boxed{2A} \arrow[l, shift right, "x_1"'] \arrow[d, shift right, "-x_0"'] \\ \boxed{1B} \arrow[u, shift right, "x_1"'] \arrow[r, shift right, "x_0"'] & \boxed{2B} \arrow[u, shift right, "x_1"'] \arrow[l, shift right, "x_1"'] \end{tikzcd}$$

Let S_{1A} be the series associated with this automaton (1.9). One computes it by solving a system of linear (noncommutative) equations as follows. Define also S_{1B}, S_{2A} and S_{2B} as the series associated with the paths going out from the corresponding vertex. Then

$$\begin{aligned}
S_{1A} &= e - x_0 S_{1B} + x_0 S_{2A},\\
S_{1B} &= x_1 S_{1A} + x_0 S_{2B},\\
S_{2A} &= x_1 S_{1A} - x_0 S_{2B},\\
S_{2B} &= x_1 S_{1B} + x_1 S_{2A}.
\end{aligned}$$

The rule is as follows: if Σ is the sum associated with a vertex (also denoted by Σ) with oriented edges $\xi_i : \Sigma \to \Sigma_i \quad (1 \le i \le m)$, then

$$\Sigma = x_1\Sigma_1 + \cdots + x_m\Sigma_m,$$

and $x_i\Sigma_i$ is replaced by e for the entry gate.

In the present situation one deduces

$$S_{1A} = e - x_0(S_{1B} - S_{2A}), \quad S_{1B} - S_{2A} = -2x_0 S_{2B},$$

$$S_{2B} = x_1(S_{1B} + S_{2A}), \quad S_{1B} + S_{2A} = 2x_1 S_{1A}$$

and therefore

$$S_{1A} = e + 4x_0^2 x_1^2 S_{1A},$$

which completes the proof of Lemma 1.6, if we take for granted that the series associated with the automaton (1.9) is the shuffle product of the series associated with the automata (1.7) and (1.8). $\square$

The structure of the commutative algebra $\mathfrak{H}_{\text{Ш}}$ is given by *Radford Theorem* [R 1993]. Consider the lexicographic order on X^* with $x_0 < x_1$. A *Lyndon word* is a word $w \in X^*$ such that, for each decomposition $w = uv$ with $u \ne e$ and $v \ne e$, the inequality $w < v$ holds. Examples of Lyndon words are x_0, x_1, $x_0 x_1^k \quad (k \ge 0)$, $x_0^\ell x_1 \quad (\ell \ge 0)$, $x_0^2 x_1^2$. Denote by $\mathcal{L}$ the set of Lyndon words.

Any Lyndon word starts with x_0 (with the only exception of x_1) and ends with x_1 (with the only exception of x_0). In other terms x_0 is the only Lyndon word which is not in $\mathfrak{H}^1_{\text{Ш}}$, while x_0 and x_1 are the only Lyndon words which are not in $\mathfrak{H}^0_{\text{Ш}}$.

Theorem 1.10. *The three shuffle algebras are (commutative) polynomial algebras*

$$\mathfrak{H}_{\text{Ш}} = K[\mathcal{L}]_{\text{Ш}}, \quad \mathfrak{H}^1_{\text{Ш}} = K\big[\mathcal{L} \setminus \{x_0\}\big]_{\text{Ш}} \quad \textit{and} \quad \mathfrak{H}^0_{\text{Ш}} = K\big[\mathcal{L} \setminus \{x_0, x_1\}\big]_{\text{Ш}}.$$

For instance there are 15 words of weight ≤ 3, and 5 among them are Lyndon words:

$$x_0 < x_0^2 x_1 < x_0 x_1 < x_0 x_1^2 < x_1.$$

We write the 10 non-Lyndon words of weight ≤ 3 as polynomials in these Lyndon words as follows:

$$
\begin{array}{ll}
e = e, & x_0^2 = \frac{1}{2} x_0 ш x_0, \\
x_0^3 = \frac{1}{3} x_0 ш x_0 ш x_0, & x_0 x_1 x_0 = x_0 ш x_0 x_1 - 2 x_0^2 x_1, \\
x_1 x_0 = x_0 ш x_1 - x_0 x_1, & x_1 x_0^2 = \frac{1}{2} x_0 ш x_0 ш x_1 - x_0 ш x_0 x_1 + x_0^2 x_1, \\
x_1 x_0 x_1 = x_0 x_1 ш x_1 - 2 x_0 x_1^2, & x_1^2 = \frac{1}{2} x_1 ш x_1, \\
x_1^2 x_0 = \frac{1}{2} x_0 ш x_1 ш x_1 - x_0 x_1 ш x_1 + x_0 x_1^2, & x_1^3 = \frac{1}{3} x_1 ш x_1 ш x_1.
\end{array}
$$

Corollary 1.11. *We have*

$$
\mathfrak{H}_ш = \mathfrak{H}^1_ш[x_0]_ш = \mathfrak{H}^0_ш[x_0, x_1]_ш \quad \textit{and} \quad \mathfrak{H}^1_ш = \mathfrak{H}^0_ш[x_1]_ш.
$$

References

Voir surtout les §§ 1.1, 1.4, 5.1 et 6.1 de [R 1993]

[A 1976] Abhyankar, S.S. – Historical ramblings in algebraic geometry and related algebra. Amer. Math. Monthly **83** (1976), no. 6, 409–448.

[BR 2001] Ball, K., Rivoal, T. – Irrationalité d'une infinité de valeurs de la fonction zêta aux entiers impairs. Invent. math. **146** (2001) 1, 193-207.
DOI 10.1007/s002220100168

[L 1981] Lewin, L. – *Polylogarithms and associated functions.* North Holland, New-York – Oxford, 1981.

[Lo 2002] Lothaire, M. – *Combinatorics on Words.* Encyclopedia of Mathematics, Vol. **17** (1983), Addison-Wesley; reprinted in 1997 by Cambridge University Press, Cambridge Mathematical Library.
Algebraic Combinatorics on Words. Cambridge University Press, 2002.
http://www-igm.univ-mlv.fr/~berstel/Lothaire/

[N 1904] Nielsen, N. – Nova Acta Leopold **90** (1909).

[R 1993] Reutenauer, C. – *Free Lie Algebras.* London Math. Soc. Monographs New Series **7** (1993), Clarendon Press, Oxford.

[Ri 2000] Rivoal, T. – La fonction Zêta de Riemann prend une infinité de valeurs irrationnelles aux entiers impairs. C. R. Acad. Sci. Paris **331** (2000), 267–270.
http://arXiv.org/abs/math.NT/0008051