THEOREM OF POINCARE-BIRKHOFF-WITT, LOGARITHM AND SYMMETRIC GROUP REPRESENTATIONS OF DEGREES EQUAL TO STIRLING NUMBERS.

Christophe Reutenauer

Université du Québec à Montréal
et
CNRS (Paris)

à S.P.

0. Introduction

The (historical) starting point of the present work is a paper of Ree [10], where an extension of a formula of Baker-Campbell-Hausdorff is given. We give it here in a slightly different formulation.

Let A be an alphabet and Q<<A>> the algebra of noncommutative formal power series over Q, equipped with the usual noncommutative product ("concatenation algebra") The space Q<<A>> possesses another product, the shuffle product: the shuffle algebra is commutative; see [10], [8] for the definition of the shuffle.

Let $\mathcal{T}$ be the complete tensor product

$$\mathcal{T} = Q\langle\langle A\rangle\rangle \otimes Q\langle\langle A\rangle\rangle$$

where the left factor is the shuffle algebra and the right factor the concatenation algebra. For instance, if a,b are in A, then

$$(a\otimes b)(b\otimes a) = (ab+ba) \otimes ba$$

Each element of $\mathcal{T}$ is an infinite linear combination of couple of words over A

$$\sum_{u,v\in A^*} \alpha_{u,v}\, u\otimes v \qquad (\alpha_{u,v}\in Q)$$

where A* denotes the free monoid generated by A. In $\mathcal{T}$, consider the particular element

$$S = \sum_{\omega\in A^*} \omega\otimes\omega$$

(a kind of diagonal). As

$$S = 1\otimes 1 + T$$

(1 is the empty word), as $1\otimes 1$ is the neutral element of $\mathcal{T}$ and as

$$\lim_{n\to 0} T^n = 0$$

(in the usual topology of $\mathcal{T}$), one may define log S by the usual formula

$$\log S = \sum_{n\geq 1} \frac{(-1)^{n-1}}{n} T^n \tag{0.1}$$

Note that, because of the special form of S, one has

$$\log S = \sum_{u\in A^*} u \otimes P_u \tag{0.2}$$

where P_u is an homogeneous polynomial of degree length(u).

Theorem (Ree, see [10] th. 2.5)

The polynomials P_u are Lie polynomials, that is, they belong to the Lie algebra generated by the elements of A.

One has, for instance

$$P_{abc} = \frac{1}{6}(2abc - acb - bac - bca - cab + 2cba) \tag{0.3}$$
$$= \frac{1}{3}[[a,b],c] - \frac{1}{6}[[a,c],b]$$

Remarks

1. One may recover the Baker-Campbell-Hausdorf formula in the following way. Let A = {a,b} and define a linear mapping f

$$Q\langle\langle A\rangle\rangle \to Q$$

by

$$\omega \to \frac{1}{i!j!} \text{ if } \omega = a^i b^j$$

$$0 \text{ otherwise}$$

for any word ω. Then it is easily verified that this mapping is a homomorphism with respect to the shuffle product (or use the fact that $a^i b^j$ are Lyndon words, and that the latter form a transcendance basis for the shuffle [8] ex. 5.3.6, [9]).

Now, apply the homomorphism f ⊗ id to (0.2), obtaining that

$$\log\left(\sum_{i,j\geq 0} \frac{a^i b^j}{i!j!}\right) = \log(e^a e^b)$$

is a Lie element c, hence $e^a e^b = e^c$, which is the B. - C. - H. formula.

2. Ree uses his formula to prove a theorem of Chen [2]: the (non-commutative) formal series defined by iterated integrals of a given path in $R^{|A|}$ is a Lie element; this formula may also be applied to nonlinear system theory [4], [5], to algebraic groups [11] and to combinatorics on words [12].

The aim of the present work is to compute explicitly the coefficients

of the series (0.2) (section 1). Moreover, we show that this series corresponds to the canonical projection π_1 of the free associative algebra onto the free Lie Algebra; in terms of Hopf algebras, this would be written $id = \exp(\pi_1)$. The free associative algebra U is, by the theorem of Poincaré-Birkhoff-Witt, the direct sum of its subspaces U^q, $q \geq 0$, where U^q is the linear span of the q-th powers of Lie elements. We show that the corresponding projections π_q satisfy $\pi_q = \pi_1^q$, in the algebra structure of End (U) deduced from the Hopf algebra structure of U. This may be interpreted by the fact that certain polynomials P_u of (0.2), viewed as elements of the algebra of the

symmetric group, are idempotents (section 2). Finally, we study the action of the symmetric group S_n on the spaces U^q. This leads to representations of S_n whose orders are the Stirling numbers, and whose corresponding idempotents are given by the series (0.2).

1. Coefficients

We want to compute explicitly the polynomials P_u of formula (0.2). By (0.1), we have

$$(1.1) \qquad \sum_{u \in A^*} u \otimes P_u = \sum_{k \geq 1} \frac{(-1)^{k-1}}{k} \Big(\sum_{\omega \in A^+} \omega \otimes \omega \Big)^k$$

where $A^+ = A^* \backslash 1$ (the semigroup of nonempty words).

By definition of the product in $\mathcal{T}$,

$$\Big(\sum_{\omega \in A^+} \omega \otimes \omega \Big)^k = \sum_{u_1, \ldots, u_k \in A^+} (u_1 \circ \ldots \circ u_k) \otimes (u_1 \ldots u_k)$$

where $\circ$ denotes the shuffle product. Denote by (P,v) the coefficient of the word v in the polynomial P. Then we obtain

$$(1.3) \qquad P_u = \sum_{k \geq 1} \frac{(-1)^{k-1}}{k} \sum_{u_1, \ldots, u_k \in A^+} (u_1 \circ \ldots \circ u_k, u) u_1 \ldots u_k$$

We shall compute explicitly the coefficients of P_u in the case where u is <u>multilinear</u> (i.e. no letter occurs more than once in u). In this case, we may write $u = a_1 \ldots a_n$, where the a_i's are distinct letters.

<u>Theorem 1.1.</u> <u>Let</u> $u = a_1 \ldots a_n$ <u>be a multilinear word. Then</u>

$$(1.4) \qquad P_u = \sum_{\sigma \in S_n} \frac{(-1)^{d_\sigma - 1}}{d_\sigma} \binom{n}{d_\sigma}^{-1} a_{\sigma(1)} \ldots a_{\sigma(n)}$$

<u>where</u> d_σ <u>is the number of ascending runs of</u> σ (= 1+ <u>number of descents of</u> σ)

We prove first a lemma.

Lemma 1.2: Let $a_1,\dots,a_n$ be distinct letters. Then

$$(1.5)\qquad \sum_{u_1,\dots,u_k\in A^+} (u_1 \circ \dots \circ u_k,\ a_1\dots a_n)\ u_1\dots u_k = \sum_{\sigma\in S_n} \binom{n-d_\sigma}{k-d_\sigma}\ a_{\sigma(1)}\dots a_{\sigma(n)}$$

Proof Denote by Q_k the polynomial on the left-hand side. Let $w = a_{\sigma(1)}\dots a_{\sigma(n)}$. Then the coefficient (Q_k,w) of w in Q_k is

$$(1.6)\qquad (Q_k,w) = \sum_{\substack{u_1,\dots,u_k\in A^+ \\ w=u_1\dots u_k}} (u_1 \circ \dots \circ u_k,\ a_1\dots a_n)$$

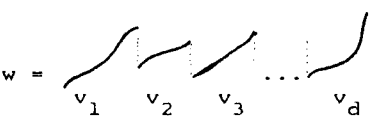
Let us say that a word is growing if it may be written as $a_{i_1}\dots a_{i_\ell}$, with $i_1 < \dots < i_\ell$.

Then, by definition of the shuffle, the coefficient $(u_1 \circ \dots \circ u_k,\ a_1\dots a_n)$ vanishes, unless each u_i is growing, in which case this coefficient is 1. Hence, the value of (1.6) is the number of factorizations of ω in k growing nonempty words. Let

$$(1.7)\qquad \omega = v_1\dots v_d$$

where each v_i is growing and where d is the number of ascending runs of σ.

Schematically



A factorization of w into growing words is necessarily a subfactorization of (1.7). Thus we have to factorize each v_i in s_i nonempty words, where the s_i's are such that $\Sigma s_i = k$. If p_i = length (v_i), then there are $\binom{P_i-1}{s_i-1}$ factorizations of v_i in s_i nonempty words. Thus

$$(Q_k,w) = \sum_{s_1+\dots+s_d=k} \binom{P_1-1}{s_1-1} \dots \binom{P_d-1}{s_d-1}$$

Now, note that

$$(1+x)^{p-1} = \sum_{1\le s\le p} \binom{p-1}{s-1} x^{s-1}$$

hence

$$\prod_{1\le i\le d} (1+x)^{p_i-1} = \prod_i \Big(\sum_{1\le s_i\le p} \binom{p_i-1}{s_i-1} x^{s_i-1} \Big),$$

$$= \sum_\ell x^\ell \Big(\sum_{s_1+\ldots+s_d-d=\ell} \binom{p_1-1}{s_1-1}\ldots\binom{p_d-1}{s_d-1} \Big)$$

But it is also equal to

$$(1+x)^{p_1+\ldots+p_d-d} = (1+x)^{n-d} = \sum_\ell \binom{n-d}{\ell} x^\ell$$

which shows that

$$\sum_{s_1+\ldots+s_d=\ell+d} \binom{p_1-1}{s_1-1}\ldots\binom{p_d-1}{s_d-1} = \binom{n-d}{\ell}$$

This shows that

$$(Q_k, w) = \binom{n-d}{k-d}$$

as desired. □

We still need another lemma

Lemma 1.3 The following relation holds

$$\sum_{k\ge 1} \frac{(-1)^{k-1}}{k} \binom{n-d}{k-d} = \frac{(-1)^{d-1}}{d} \binom{n}{d}^{-1}$$

Proof Denote by a(n,d) the left-hand side. We prove the lemma by induction on n-d. If n-d = 0, it is obvious. Let n-d ≥ 1. Using the usual relation for binomial coefficients, we obtain

$$a(n,d) = a(n-1,d) + a(n,d+1)$$

This is equal, by induction, to

$$\frac{(-1)^{d-1}}{d} \binom{n-1}{d}^{-1} + \frac{(-1)^d}{d+1} \binom{n}{d+1}^{-1}$$

$$= \frac{(-1)^{d-1}}{d} \frac{d!\ (n-1-d)!}{(n-1)!} + \frac{(-1)^d}{d+1} \frac{(d+1)!\ (n-d-1)!}{n!}$$

$$= \frac{(-1)^{d-1}\ (d-1)!\ (n-d-1)!}{n!} (n-d)$$

$$= \frac{(-1)^{d-1}}{d} \binom{n}{d}^{-1}$$

as desired. □

Now, the theorem follows, using (1.3) and the two lemmas.

Remark If $u=a_1 \cdots a_n$ is any word, not necessarily multilinear, then formula (1.4) still holds (but the words $a_{\sigma(1)} \cdots a_{\sigma(n)}$ are not all distinct). This is a consequence of (1.1) (or see lemma 2.4). For instance, one obtains P_{aba} from P_{abc} by replacing c by a in (0.3):

$$P_{aba} = \frac{1}{6} (2\ aba - aab - baa - baa - aab + 2\ aba)$$

$$= \frac{1}{6} (4\ aba - 2\ aab - 2\ baa)$$

$$= \frac{1}{3} (2\ aba - aab - baa)$$

$$= \frac{1}{3} [[a,b], a]$$

2. The canonical projection

Consider an alphabet $A = \{a_1, \ldots, a_n\}$. Then each multilinear word of length n may be viewed as a permutation, element of S_n. For instance, if $A = \{a_1, a_2, a_3\}$. the word $a_1a_2a_3$ will represent 1 (the identity permutation), and $a_3a_2a_1$ will be the transposition (13).

Consequently, a polynomial which is a linear combination of such words may be viewed as an element of the group algebra $Q\{S_n\}$. For instance, the polynomial P_{abc} of (0.3) will be

$$\frac{1}{6} (2 - (23) - (12) - (123) - (132) + 2\ (13))$$

A direct calculation shows that this element of $Q[S_3]$ is idempotent!

We shall now explain this fact.

Let $Q\langle A\rangle$ be the algebra of noncommutative polynomials (it is a subalgebra of the concatenation algebra $Q\langle\langle A\rangle\rangle$). Let $\mathcal{L}\langle A\rangle$ denote the Lie algebra generated, in $Q\langle A\rangle$, by the letters (= elements of A); an element in $\mathcal{L}\langle A\rangle$ is called a Lie polynomial. It is known that $\mathcal{L}\langle A\rangle$ is the free Lie algebra generated by A, with $Q\langle A\rangle$ as an enveloping algebra (see [8]). Let U^q denote the subspace of $Q\langle A\rangle$ generated by the polynomials P^q, where P ranges over $\mathcal{L}\langle A\rangle$. Then, by the theorem of Poincaré-Birkhoff-Witt

$$(2.1) \qquad Q\langle A\rangle = \bigoplus_{q \geq 0} U^q$$

see [3], 2.4.6.

The direct sum decomposition (2.1) defines a family of linear projections

$$(2.2) \qquad \pi_q : Q\langle A\rangle \to Q\langle A\rangle$$

defined by $\pi_q \mid U^q = id$, $\pi_q \mid U^{q'} = 0$ if $q' \neq q$. Note that $U^1 = \mathcal{L}\langle A\rangle$. The projection π_1 is called the canonical projection of $Q\langle A\rangle$ onto $\mathcal{L}\langle A\rangle$.

Theorem 2.1 The canonical projection $\pi_1 : Q\langle A\rangle \to \mathcal{L}\langle A\rangle$ is also defined by the condition

$$\pi_1(u) = P_u$$

for any word u (where P_u is defined by (0.2)). In particular, if $u = a_1 \ldots a_n$ is a multilinear word and if P_u is considered as an element of $Q[S_n]$, then P_u is idempotent in $Q[S_n]$.

We need some lemmas. The first one is well-known.

Lemma 2.2 Define the concatenation homomorphism

$$C_k : Q\langle A\rangle \to Q\langle A\rangle^{\otimes k}$$

by

$$C_k(a) = a\otimes 1\otimes \ldots \otimes 1 + 1\otimes a\otimes \ldots \otimes 1 + \ldots + 1\otimes \ldots \otimes 1\otimes a$$

for any letter a. Then, for any w one has

$$(2.3)\quad C_k(w) = \sum_{u_1,\ldots,u_k \in A^*} (u_1 \circ \ldots \circ u_k, w)\, u_1 \otimes \ldots \otimes u_k$$

Furthermore if P is a Lie polynomial, then

$$C_k(P) = P\otimes 1\otimes \ldots \otimes 1 + 1\otimes P\otimes \ldots \otimes 1 + \ldots + 1\otimes \ldots \otimes 1\otimes P$$

Proof The first relation is a simple consequence of the definition of the shuffle product. For the second, it is enough to note that it is true when P is a letter, and then check that if it is true for P, Q, then also for their Lie bracket $[P,Q] = PQ - QP$. □

Lemma 2.3 Let $f_1, \ldots, f_k, g$ be linear endomorphisms $Q\langle A\rangle \to Q\langle A\rangle$ such that the following equality holds in the algebra $\mathcal{T}$ (see section 0):

$$\prod_{1\leq i\leq k} \Big(\sum_{u\in A^*} u \otimes f_i(u) \Big) = \sum_{w\in A^*} w \otimes g(w)$$

Then, for any polynomial P

$$g(P) = p_k \circ (f_1 \otimes \ldots \otimes f_k) \circ c_k(P)$$

where $p_k : Q\langle A\rangle^{\otimes k} \to Q\langle A\rangle$ is the concatenation product:

$$p_k(u_1 \otimes \ldots \otimes u_k) = u_1 \ldots u_k$$

Proof By definition of the product in $\mathcal{T}$, one has

$$\sum_{w\in A^*} w\otimes g(w) = \sum_{u_1,\dots,u_k} (u_1 o \dots o u_k)\otimes(f_1(u_1)\dots f_k(u_k))$$

This shows that

$$g(w) = \sum_{u_1,\dots,u_k} (u_1 o \dots o u_k, w) f_1(u_1)\dots f_k(u_k)$$

Now, by (2.3), we obtain

$$P_k o(f_1\otimes\dots\otimes f_k)\, o c_k(w)$$

$$= P_k\Big(\sum_{u_1,\dots,u_k} (u_1 o \dots o u_k, w)\ f_1(u_1)\otimes\dots\otimes f_k(u_k)\Big)$$

$$= \sum_{u_1,\dots,u_k} (u_1 o \dots o u_k, w)\ f_1(u_1)\dots f_k(u_k)$$

which proves the lemma, because A^* is a basis of $Q\langle A\rangle$. □

Remark The product $(f,g) \to f*g$ in $\mathrm{End}\,(Q\langle A\rangle)$ defined by

$$(f*g)(P) = p_2 o(f\otimes g) o\ c_2(P)$$

is a classical one in the context of bialgebras, see [7] p. 5. It is associative, and

$$f_1*\dots*f_k = p_k o(f_1\otimes\dots\otimes f_k) o\ c_k$$

Lemma 2.4 Let I be the endomorphism of $Q\langle A\rangle$ defined by $I(w) = w$ if $w \neq 1$ and $I(1) = 0$. Let α be the endomorphism defined by

$$\alpha = p_k o\ I^{\otimes k} o\ c_k$$

Let f be an algebra homomorphism $Q\langle A\rangle \to Q\langle A\rangle$ such that f(a) is a Lie polynomial for any letter a. Then

$$\alpha\ o\ f = f\ o\ \alpha$$

Proof If $w = a_1\dots a_n$ $(a_i\in A)$, then

$$c_k(w) = \prod_{1\le i\le n} (a_i\otimes\dots\otimes 1 + \dots + 1\otimes\dots\otimes a_i)$$

Moreover, $c_k\ o\ f(w) = c_k\ (\prod_{1\le i\le n} f(a_i))$

$$= \prod_{1\le i\le n} c_k(f(a_i))$$

Because each $f(a_i)$ is a Lie polynomial, this is equal, by lemma 2.2, to

$$\prod_{1\le i\le n} (f(a_i)\otimes\dots\otimes 1 + \dots + 1\otimes\dots\otimes f(a_i))$$

This shows that we have

$$c_k \circ f = f^{\otimes k} \circ c_k$$

Now, because any Lie polynomial has zero constant term, we have

$$I \circ f = f \circ I$$

Moreover, as f is an algebra homomorphism, we have

$$p_k \circ f^{\otimes k} = f \circ p_k$$

Taking these relations together, we obtain

$$\begin{aligned}
\alpha \circ f &= p_k \circ I^{\otimes k} \circ c_k \circ f \\
&= p_k \circ I^{\otimes k} \circ f^{\otimes k} \circ c_k \\
&= p_k \circ (I \circ f)^{\otimes k} \circ c_k \\
&= p_k \circ (f \circ I)^{\otimes k} \circ c_k \\
&= p_k \circ f^{\otimes k} \circ I^{\otimes k} \circ c_k \\
&= f \circ p_k \circ I^{\otimes k} \circ c_k = f \circ \alpha
\end{aligned}$$

what was to be shown. □

Proof of theorem 2.1

Let π be the endomorphism of Q<A> defined by

$$\pi(u) = P_u$$

for any word u. We have to show that $\pi = \pi_1$. For this, it is enough to show that for any Lie polynomial P, one has $\pi(P) = P$ and $\pi(P^q) = 0$ if $q \neq 1$.
Let $I : Q\langle A\rangle \to Q\langle A\rangle$ the endomorphism defined by $I(1) = 0$ and $I(w) = w$ if w is a nonempty word. Then, by (1.1),

$$\sum_u u \otimes P_u = \sum_{k \geq 1} \frac{(-1)^{k-1}}{k} \Big(\sum_w w \otimes I(w)\Big)^k$$

By lemma 2.3,

$$\Big(\sum_w w \otimes I(w)\Big)^k = \sum_w w \otimes (p_k \circ I^{\otimes k} \circ c_k(w))$$

This shows that

$$(2.4) \qquad \pi(u) = \sum_{k \geq 1} \frac{(-1)^{k-1}}{k} p_k \circ I^{\otimes k} \circ c_k(u)$$

As π is linear, this relation holds also for any polynomial P instead of u.
By lemma 2.4, we thus obtain that

$$\pi \circ f = f \circ \pi$$

for any algebra endomorphism f of $Q\langle A\rangle$ such that f(a) is a Lie polynomial for each letter a. Now let P be any Lie polynomial and f an algebra endomorphism of $Q\langle A\rangle$ such that f(a) = P for some fixed letter a. Then $\pi(P^q) = \pi \circ f(a^q) = f \circ \pi(a^q)$. This shows that it is enough to prove the above assertions for a. For this, let g be the algebra endomorphism of $Q\langle A\rangle$ such that g(a) = a and g(b) = 0 for the other

letters. Then

$$\pi(a) = \pi \circ g(a)$$

which shows that we just have to consider the one-letter case. But

$$\sum_{n \in N} a^n \otimes a^n = \exp(a \otimes a)$$

in $\mathcal{T}$, because the n-th shuffle power of a is $n!\, a^n$. Hence

$$\log\left(\sum_n a^n \otimes a^n\right) = a \otimes a$$

which shows that

$$\pi(a^q) = \delta_{q,1}\, a$$

as desired.

Now, let $a_1, \ldots, a_n$ be distinct letters and

$$\pi(a_1 \cdots a_n) = \sum_{\sigma \in S_n} \alpha_\sigma\, a_{\sigma(1)} \cdots a_{\sigma(n)}$$

For $\sigma \in S_n$, let f_σ be the algebra endomorphism of $Q\langle A\rangle$ defined by

$$f_\sigma(a_i) = a_{\sigma(i)}$$

As π is a projection, we have

$$\sum_{\sigma \in S_n} \alpha_\sigma\, a_{\sigma(1)} \cdots a_{\sigma(n)} = \pi(a_1 \cdots a_n)$$

$$= \pi \circ \pi(a_1 \cdots a_n)$$

$$= \sum_\sigma \alpha_\sigma\, \pi(a_{\sigma(1)} \cdots a_{\sigma(n)})$$

$$= \sum_{\sigma} \alpha_{\sigma} \pi \circ f_{\sigma} (a_1 \cdots a_n)$$

$$= \sum_{\sigma} \alpha_{\sigma} f_{\sigma} \circ \pi (a_1 \cdots a_n)$$

by lemma 2.5.

Hence

$$\sum_{\sigma} \alpha_{\sigma} a_{\sigma(1)} \cdots a_{\sigma(n)} = \sum_{\sigma} \alpha_{\sigma} f_{\sigma} \left(\sum_{\tau} \alpha_{\tau} a_{\tau(1)} \cdots a_{\tau(n)} \right)$$

$$= \sum_{\sigma,\tau} \alpha_{\sigma}\alpha_{\tau} a_{\sigma\tau(1)} \cdots a_{\sigma\tau(n)}$$

which shows that

$$\sum_{\sigma} \alpha_{\sigma} \sigma = \sum_{\sigma,\tau} \alpha_{\sigma}\alpha_{\tau}\sigma\tau$$

is idempotent in $Q[S_n]$. □

Remark We have used, in the course of the proof, the fact that in the one-letter case, one has in $\mathcal{T}$: $\sum_{n \in N} a^n \otimes a^n = \exp(a \otimes a)$. Note that when $|A| \geq 2$, it is not true in $\mathcal{T}$ that

$$\sum_{w \in A^*} w \otimes w = \exp\left(\sum_{a \in A} a \otimes a \right)$$

This is only true in the one-letter case.

Corollary 1.6 The canonical projection $\pi_1 : Q\langle A \rangle \to \mathcal{L}\langle A \rangle$ is given, for any Lie polynomials $P_1, \ldots, P_n$, by

$$\pi_1(P_1 \cdots P_n) = \sum_{\sigma \in S_n} \frac{(-1)^{d_\sigma - 1}}{d_\sigma} \binom{n}{d_\sigma}^{-1} P_{\sigma(1)} \cdots P_{\sigma(n)}$$

$$= \sum_{\sigma \in S_n} \frac{(-1)^{d_\sigma - 1}}{d_\sigma \, n} \binom{n}{d_\sigma}^{-1} [P_{\sigma(1)} \cdots P_{\sigma(n)}]$$

where $[Q_1 \cdots Q_n]$ denotes the bracketing (from left to right) $[\ldots[Q_1 Q_2] \ldots\ldots Q_n]$.

The last formula has already been proved by Solomon [14]; he starts directly from the P. - B. - W theorem, and does not use the logarithm as here.

Proof The first formula is a consequence of theorem 1.1, theorem 2.1 and lemma 2.5. For the second, apply the formula of Dynkin - Specht - Wever, see e.g. [10] th. 2.3. □

3. The other projections

We have shown that the canonical projection $\pi_1 : Q\langle A\rangle \to \mathfrak{L}\langle A\rangle$ is determined by the logarithm of $\sum_{w\in A^*} w \otimes w$; in fact in terms of the product of End $(Q\langle A\rangle)$ introduced in the remark after lemma 2.3, one has $\pi_1 = \log(\mathrm{id})$, where id is the identity of $Q\langle A\rangle$ (this seems to be a formal analogue of the exponential function in a Lie group). What about the other projections?

Theorem 3.1 *The projection $\pi_q : Q\langle A\rangle \to Q\langle A\rangle$ is completely specified by the formula*

$$(3.1)\qquad \frac{1}{q!}\,(\log(\sum_{w\in A+} w\otimes w))^q = \sum_{u\in A^*} u\otimes \pi_q(u)$$

which holds in the algebra $\mathcal{T}$. Moreover, with $A = \{a_1,\dots,a_n\}$, one has

$$(3.2)\qquad \pi_q(a_1\dots a_n) = \sum_{\sigma\in S_n}\Big(\sum_k \frac{s(k,q)}{k!}\binom{n-d_\sigma}{k-d_\sigma}\Big)\, a_{\sigma(1)}\cdots a_{\sigma(n)}$$

where $s(k,q)$ is the Stirling number of first kind. Viewed as elements of $Q[S_n]$, the n elements $\pi_q(a_1\dots a_n)$, $1\le q\le n$, are orthogonal idempotents of sum 1 (for $q = 0$ or $q > n$, $\pi_q(a_1\dots a_n) = 0$).

Formula 3.1 was already proved by Hain [6], in the context of graded Hopf algebras.

Recall that the Stirling numbers are defined by

$$x(x-1)(x-2)\dots(x-k+1) = \Sigma_q\, s(k,q)\, x^q, \text{ see [13]}.$$

Unfortunately, I could not completely identify the coefficient of $a_{\sigma(1)}\cdots a_{\sigma(n)}$ in (3.2). One obtains for each n, an n by n table of coefficients, depending on q and d_σ. I give the table for $n = 6$, and a description of the known parts of the table.

q \ d_σ	1	2	3	4	5	6
1	$\frac{1}{6}$	$\frac{-1}{30}$	$\frac{1}{60}$	$\frac{-1}{60}$	$\frac{1}{30}$	$\frac{-1}{6}$
2	$\frac{137}{360}$	$\frac{-13}{360}$	$\frac{1}{180}$	$\frac{1}{180}$	$\frac{-13}{360}$	$\frac{137}{360}$
3	$\frac{5}{16}$	$\frac{1}{48}$	$\frac{-1}{48}$	$\frac{1}{48}$	$\frac{-1}{48}$	$\frac{-5}{16}$
4	$\frac{17}{144}$	$\frac{5}{144}$	$\frac{-1}{144}$	$\frac{-1}{144}$	$\frac{5}{144}$	$\frac{17}{144}$
5	$\frac{1}{48}$	$\frac{1}{80}$	$\frac{1}{240}$	$\frac{-1}{240}$	$\frac{-1}{80}$	$\frac{-1}{48}$
6	$\frac{1}{720}$	$\frac{1}{720}$	$\frac{1}{720}$	$\frac{1}{720}$	$\frac{1}{720}$	$\frac{1}{720}$

First row: inverses of the binomial coefficients of order n - 1 multiplied by $\pm \frac{1}{n}$

First and last column: Stirling numbers s(n,q) multiplied by $\pm \frac{1}{n!}$

Last row: $\frac{1}{n!}$

Sum of the first column: 1

Sum of the other columns: 0

Proof of theorem 3.1

Let the left-member of (3.1) be equal to $\sum u \otimes \alpha(u)$, for some linear endomorphism α of $Q\langle A\rangle$. We want to show that $\alpha = \pi_q$. By lemma 2.3, we have

$$\alpha = \frac{1}{q!} P_q \circ \pi_1^{\otimes q} \circ c_q$$

From this, the first assertion will easily follow. Let P be a Lie polynomial. Then $c_q(P^q) = c_q(P)^q = (P\otimes 1\otimes\ldots\otimes 1+\ldots+ 1\otimes\ldots\otimes 1\otimes P)^q$ by lemma 2.2: it is the sum of q! $P\otimes\ldots\otimes P$ and of terms $P_1\otimes\ldots\otimes P_q$ where at least one P_i is equal to 1. Hence, as $\pi_1(1) = 0$, we obtain that $\pi_1^{\otimes q} \circ c_q (P^q) = q!\ P \otimes\ldots\otimes P$, by the definition of π_1. Thus $\alpha (P^q) = P^q$. Now, let $r \neq q$. Then $C_q(P^r)$ is a sum of terms $P_1 \otimes\ldots\otimes P_q$ where at least one P_i is equal to P^j for some $j \neq 1$: as $\pi_1 (P^j) = 0$, we obtain that
$\alpha (P^r) = 0$. Thus $\alpha = \pi_q$, by definition of π_q.

It is well-known [13] that

$$\frac{1}{q!} (\log (1+x))^q = \sum_k \frac{s(k,q)}{k!} x^k$$

Thus we have by (3.1)

$$\sum u \otimes \pi_q(u) = \sum_k \frac{s(k,q)}{k!} \Big(\sum_{w\in A^*} w \otimes w\Big)^k$$

Hence, by (1.2), we obtain

$$\pi_q(u) = \sum_k \frac{s(k,q)}{k!} \sum_{u_1,\ldots,u_k\in A^+} (u_1 \circ\ldots\circ u_k, u) u_1\ldots u_k$$

Now, this and lemma 1.2 imply formula (3.2).

It is obvious, from the definition of π_q, that $\pi_q(a_1\ldots a_n) = 0$ if $q = 0$ or $q > n$. Evidently $id = \sum_q \pi_q$ which shows that

$$\sum_{1\leq q\leq n} \pi_q(a_1\cdots a_n) = a_1\cdots a_n,$$

and hence the last assertion follows. The fact that $\pi_q(a_1\cdots a_n)$ is idempotent is a consequence, as in the proof of theorem 2.1, of the fact that π_q is a projection. The fact that these idempotents are orthogonal is similarly proved by using the relations

$$\pi_q \circ \pi_{q'} = 0$$

if $q \neq q'$. □

4. Representations of the symmetric group.

We have obtained n orthogonal idempotents of sum 1 of $Q[S_n]$, which are $\pi_q(a_1\cdots a_n)$, $1\leq q\leq n$. We compute now the degrees of the associated representations of the symmetric group. A surprising fact is that Stirling numbers step in again.

Note that if $A = \{a_1\cdots a_n\}$, then $Q[S_n]$ acts naturally on $Q\langle A\rangle$ by $\sigma.a_i = a_{\sigma(i)}$, extended in an algebra endomorphism of $Q\langle A\rangle$. In particular, let E be the subspace of $Q\langle A\rangle$ generated by the words $a_{\sigma(1)}\cdots a_{\sigma(n)}$, $\sigma \in S_n$. This is of course stable under the action of S_n, and the associated representation is the left regular representation of S_n.

Moreover, let $V^q = U^q \cap E$, where $U^q = \pi_q(Q\langle A\rangle)$, see section 2. Now, it is well-known, by multilinearization, that U^q is generated by the polynomials

$$(P_1,\ldots,P_q) = \sum_{\sigma \in S_q} P_{\sigma(1)}\cdots P_{\sigma(q)}$$

where $P_1,\ldots,P_q$ are Lie polynomials. This shows that one has

$$E = \bigoplus_q V^q$$

and that each V^q is stable under the action of S_n. It is easy to show that $V^q = 0$ if $q = 0$ or $q > n$. Hence

$$E = \bigoplus_{1\leq q\leq n} V^q$$

or equivalently

$$Q[S_n] = \bigoplus_{1\leq q\leq n} Q[S_n]\,\pi_q(a_1\cdots a_n)$$

if $\pi_q(a_1\cdots a_n)$, defined by (3.2), is viewed as an element of $Q[S_n]$. Note that we have also, by lemma 2.4

$$\pi_q(\sigma.P) = \sigma.\pi_q(P)$$

for any polynomial P (which implies in fact all the previous assertions). Now, we have the perhaps classical result.

Theorem 4.1 The dimension of V^q is $|s(n,q)|$.

Proof. We show that each permutation σ in S_n defines an element $[\sigma]$ of a basis of V^q, where q is the number of cycles of σ. As it is well-known ([13] p. 71) that the number of permutations in S_n with q cycles is $|s(n,q)|$, the result will follow.

First, we associate to σ a multilinear word: decompose σ in cycles

$$\sigma = (i_1,i_2,\ldots,i_u)(j_1,\ldots,j_v)(k_1,\ldots,k_w)\ldots$$

with $i_1 = \inf\{i_1,\ldots,i_u\} > j_1 = \inf\{j_1,\ldots,j_v\} > k_1 = \inf\{k_1,\ldots,k_w\}$ etc...

Then associate to σ the word

$$w = a_{i_1}a_{i_2}a_{i_u}\,a_{j_1}\ldots a_{j_v}\,a_{k_1}\ldots a_{k_w}\ldots$$

This is clearly a bijection. Moreover, the factorization of w

$$w = (a_{i_1}\ldots a_{i_u})(a_{j_1}\ldots a_{j_v})(a_{k_1}\ldots a_{k_w})\ldots$$

is just the decomposition of w into Lyndon words, see [8]. Denote by [u] the Lie polynomial which corresponds to a Lyndon word in the Lyndon basis of $\mathcal{L}\langle A\rangle$ (ibid.). If $w = u_1\ldots u_q$ is the decomposition of w into Lyndon words, then let

$$[\sigma] = [w] = \sum_{\sigma \in S_q} [u_{\sigma(1)}]\ldots[u_{\sigma(q)}]$$

Let B be a subset of A. Let M_B be the set of multilinear words which have exactly B as set of letters. Let E_B be the space generated by M_B and $V_B^q = U^q \cap E_B$. Then the space $V_B^1 = \mathcal{L}\langle A\rangle \cap E_B$ admits as a basis the set of

$$[u],\ u \in M_B,\ u \text{ Lyndon, see [8].}$$

Now, let $1 \le q \le n$. By homogeneity, the space V^q is generated by the polynomials

$$(P_1,\ldots,P_q)$$

where $P_i \in V_{B_i}^1$ for some partition $A = \bigcup_{1\le i\le q} B_i$. This shows, by multilinearity, that V^q is generated by the polynomials

$$([u_1],\ldots,[u_q])$$

where $u_i \in M_{B_i}$ is a Lyndon word. But there are $|s(n,q)|$ polynomials of this type (by the above bijection); thus $n! = \sum_q \dim (V_q) \leq \sum_q |s(n,q)| = n!$. This shows that these polynomials form a basis of V^q, whose dimension is consequently $|s(n,q)|$. □

Example A = {a,b,c}

$$\left.\begin{array}{l}[abc] = [a,[b,c]] \\ [acb] = [[a,c],b]\end{array}\right\} \quad V^1$$

$$\left.\begin{array}{l}[bac] = b[a,c] + [a,c]b \\ [bca] = [b,c]a + a[b,c] \\ [cab] = c[a,b] + [a,b]c\end{array}\right\} \quad V^2$$

$$[cba] = cba + cab + bca + bac + acb + abc \} \; V^3$$

([x,y] denotes xy - y x).

5. Conclusion

In the course of computing the coefficients of the series of Ree, we were lead to discover several striking facts. First, that the elements of the algebra of the symmetric group which appear, as noncommutative polynomials, are idempotents: this is a priori not obvious, due to the fact that they are defined by concatenation and shuffle of words, and not in term of the product of the symmetric group.

To explain this idempotence, we have shown that Ree's series may be interpreted as the canonical projection of the free associative algebra onto the free Lie algebra (any enveloping algebra would however work).

More precisely, in terms of the product of the endomorphism algebra defined by the Hopf algebra structure of Q<A>, this projection is the logarithm of the identity; or, the identity is the exponential of the projection, which seems to be a kind of analogue of the exponential in a Lie group.

Another surprising fact is that Stirling numbers intervene separately twice: once, in the coefficients of the idempotents and secondly as dimensions of the associated representations.

What should be done now is the exact identification of the coefficients in formula (3.2). Moreover, more information should be given about the representations of the symmetric group which were introduced here.

Let me give some more comments . As pointed out above, it is surprising that concatenation and shuffle of words have something to

do with the composition of permutations. I give here two other illustrations of this. By the formula of Dynkin - Specht - Wever, one has for each homogeneous Lie polynomial P of degree n

$$[P] = n\,P$$

where the endomorphism $P \to [P]$ is defined for any word $a_1 \ldots a_n$ ($a_i \in A$) by

$$[a_1 \ldots a_n] = [\ldots[a_1,a_2],a_3],\ldots,a_n]$$

(bracketing from left to right). Interpreting $[a_1 \ldots a_n]$ as an element e of $Q[S_n]$, this implies that this element satisfies

$$e^2 = n\,e$$

i.e. e/n is idempotent (this may be proved as in theorem 2.1).

Example

$$[[a_1,a_2],a_3] = a_1a_2a_3 - a_2a_1a_3 - a_3a_1a_2 + a_3a_2a_1$$

$$= 1 - (12) - (132) + (13)$$

It is easily shown, moreover that the element $[a_1 \ldots a_n]$ of $Q[S_n]$ may be factorized as

$$[a_1 \ldots a_n] = (1 - (12)(23)\ldots(n-1,n))\ldots\ldots(1 - (12)(23))\,(1 - (12))$$

This gives a further connection between Lie brackets and composition of permutations.

Acknowledgements

The main part of the present work was done during a 6 months stay of the author at the University of Saarbrucken, in spring 1982, by invitation of Pr. G. Hotz, who is gratefully acknowledged.

Correspondence with J. Dixmier and conversations with D. Perrin and P. Leroux were also helpful.

Added in proof:

The representation of the symmetric group on V^1 is obtained by A. Joyal in a different way: it corresponds to the logarithm in the theory of species. Moreover, the methods of generating series of species (more precisely: the "séries indicatrices", see [A. Joyal, une théorie combinatoire des séries formelles, Advances in Maths. 42 (1981) 1-82]) allow him to give formulas for the computation of the multiplicities of the irreducible components of this representation. These where computed up to n = 12 by Nantel Bergeron at UQAM. It seems that, except for the trivial and alternating representations and a few exceptions, each irreducible representation appears in V^1 (personal communication).

References

[1] N. Bourbaki, Groupes et algèbres de Lie, chapitre 1, Hermann (1971).

[2] K.T. Chen, Integration of paths, geometric invariants and a generalized Baker-Haussdorff formula, Annals Maths 65 (1957) 163-178.

[3] J. Dixmier, Algèbres enveloppantes, Hermann (1974)

[4] M. Fliess, D. Normand-Cyrot, Algèbres de Lie nilpotentes, intégrales itérées de K.T. Chen et formule de Baker-Campbell-Hausdorff, Lect. Notes Maths 920 (1982) 257-265.

[5] M. Fliess, C. Reutenauer, Picard-Vessiot theory of bilinear systems, IEEE 23rd Congress on Decision and Control, Proc., 1153-1157 (1983).

[6] R.M. Hain, On the indecomposable elements of the bar construction, preprint (1985); see also: de Rham homotopy theory of complex algebraic varieties, manuscript (1984), appendix.

[7] G.P. Hochschild, Basic theory of algebraic groups and Lie algebras, Springer Verlag (1981).

[8] M. Lothaire, Combinatorics on words, Addison Wesley (1983)

[9] D. Perrin, G. Viennot, A note on shuffle algebras (1981), manuscript.

[10] R. Ree, Lie elements and an algebra associated with shuffles, Annals Maths 68 (1958) 210-220.

[11] C. Reutenauer, Point générique du plus petit groupe algébrique dont l'algèbre de Lie contient plusieurs matrices données, Comptes Rendus Acad. Sci. Paris 293 (1981) 577-580.

[12] C. Reutenauer, The shuffle algebra on the factors of a word is free, J. Combin. Theory 38 (1985) 48-57.

[13] J. Riordan, An introduction to combinatorial analysis, John Wiley 1967.

[14] L. Solomon, On the Poincaré-Birkhoff-Witt theorem, J. Combin. Theory (A) 4 (1968) 363-375.