

FREE KAC–MOODY GROUPS AND THEIR LIE ALGEBRAS.

Y. BILLIG

AND

A. PIANZOLA

Dept. of Mathematics & Statistics
University of New Brunswick
Fredericton, New Brunswick
Canada E3B 5A3

Dept. of Mathematical Sciences
University of Alberta
Edmonton, Alberta
Canada T6G 2G1

ABSTRACT. We compute the Lie algebras of continuous right invariant derivations of free Kac–Moody groups.

INTRODUCTION.

Lie’s third Theorem, the existence of a Lie group with given (finite dimensional complex) Lie algebra, is one of the central results of the classical theory of transformation groups. Over arbitrary base fields the analytical tools give way to algebraic geometry and questions of rationality.

For infinite dimensional Lie groups the situation is almost completely uncharted except for a few exceptions, one of which is the case of Kac–Moody groups. The constructions of these groups that is most relevant to us is that of Peterson and Kac as presented in [PK]. The spirit of their construction (at times reminiscent of Chevalley’s Tohoku paper) is to first attach to the Lie algebra a “free” Kac–Moody group \mathcal{F} and then go on to identify those elements of \mathcal{F} whose action on a given representation theory (The integrable

Both authors acknowledge the generous support of NSERC Canada.

representation in this case. But see also [MP] Ch.6) coincide. At the heart of the present paper is the study the Lie algebra that corresponds to \mathcal{F} .

The first question to answer is *how* to attach a Lie algebra to \mathcal{F} to begin with. The answer is rather elegant: There is a natural concept of polynomial function on the group \mathcal{F} . These form an algebra, $Pol\mathcal{F}$, in which the group acts. As in the classical situation, one then defines the Lie algebra to be the derivations of $Pol\mathcal{F}$ which are (right) invariant under the group action.

With the Lie algebra constructed we next look at its structure, which as it turns out, is a certain completion of a free Lie algebra. The two key ingredients to the proof are the fact that all elements of $Pol\mathcal{F}$ can be written as series on certain basic polynomial functions (Theorem 2.10), and secondly that this basic polynomial functions form a shuffle algebra (Theorem 3.7)

We would like to most sincerely thank J. Valencia for his great help in putting together this paper.

NOTATION, CONVENTIONS, AND TERMINOLOGY.

Let I be a non-empty set which will be assumed fixed throughout our discussion. For each commutative ring \mathbb{K} and each $i \in I$ we consider a copy $E_i(\mathbb{K}) := \{E_i(\lambda) | \lambda \in \mathbb{K}\}$ of the additive group of \mathbb{K} . Thus for all $\lambda, \mu \in \mathbb{K}$ $E_i(\lambda)E_i(\mu) = E_i(\lambda + \mu)$. Consider the free product

$$\mathcal{F}(\mathbb{K}) := \ast_{i \in I} E_i(\mathbb{K}).$$

To deal with $\mathcal{F}(\mathbb{K})$ we will introduce a fair amount of notation and terminology. For the reader's convenience we will gather all this information in the present section (even though some of it will not be needed until much later.) This will make back references much more accesible .

Let W be the free multiplicative monoid (words) on I . We denote by $\mathbf{1}$ the empty word (identity) in W . If $\mathbf{w} \in W$, $\mathbf{w} \neq \mathbf{1}$, we can uniquely write

$$\mathbf{w} = \mathbf{w}_1 \cdots \mathbf{w}_w \text{ with } w > 0, \text{ and } \mathbf{w}_1, \cdots, \mathbf{w}_w \in I. \tag{1.1}$$

We thus use bold face characters for words, and the corresponding unbold characters for their lengths.

There is also a unique expression

$$\mathbf{w} = \overline{\mathbf{w}}_1^{n_1} \cdots \overline{\mathbf{w}}_{\overline{w}}^{n_{\overline{w}}} \text{ with } \overline{\mathbf{w}}_n \neq \overline{\mathbf{w}}_{n+1}, \text{ and } n_k > 0. \quad (1.2)$$

We set $\overline{\mathbf{w}} := \overline{\mathbf{w}}_1 \cdots \overline{\mathbf{w}}_{\overline{w}}$, $\overline{W} = \{\overline{\mathbf{w}} : w \in W\}$ (reduced words) and

$$\mathbf{w}! = n_1! \cdots n_{\overline{w}}!. \quad (1.3)$$

1.4 The case $\mathbf{w} = \mathbf{1}$ corresponds to $w = 0$ in (1.1). We will agree that $\mathbf{1} = \overline{\mathbf{1}}$, that $\mathbf{1}! = 1$, and that $\mathbf{1} \in \overline{W}$.

If $N \in \mathbb{Z}_{>0}$ we will denote the interval $\{1, \dots, N\}$ by $[N]$, and agree that $[0]$ is the empty set. By means of (1.1) we define the *degree function* $deg: W \rightarrow \mathbb{N}^I$ by $\mathbf{w} \mapsto deg_{\mathbf{w}}$ where

$$deg_{\mathbf{w}}(i) = Card\{k \in [w] : \mathbf{w}_k = i\}. \quad (1.5)$$

Let \mathbf{s} and \mathbf{r} be elements of W . By a *placing map of \mathbf{s} into \mathbf{r}* we understand a map $\sigma : [s] \rightarrow [r]$ satisfying the following conditions:

PM1. $1 \leq p < q \leq s \implies \sigma(p) \leq \sigma(q)$ (i.e. σ is (non-strictly) monotonic)

PM2. $\mathbf{s}_p = \mathbf{r}_{\sigma(p)}$ for all $p \in [s]$.

The totality of such maps will be denoted by $[\mathbf{s} : \mathbf{r}]$. Given $\mathbf{w} \in W$ we define $W_{\mathbf{w}} = \{\mathbf{s} \in W : [\mathbf{s} : \mathbf{w}] \neq \emptyset\}$

Remark 1.6. Let $\sigma \in [\mathbf{s} : \mathbf{r}]$. For $n \in [r]$ the set $\sigma^{-1}(n) := \{m | \sigma(m) = n\}$ is either empty or an interval $[p, q]$ for some $1 \leq p \leq q \leq s$. We set $\sigma_n := Card \sigma^{-1}(n)$, and $\sigma! := \prod_{n=1}^r \sigma_n!$. Note that $[\mathbf{s} : \overline{\mathbf{s}}]$ consists of just one element, denote by $\rho_{\mathbf{s}}$, and that $\rho_{\mathbf{s}}! = \mathbf{s}!$

1.7 To each $\mathbf{s} \in W$ we attach the polynomial ring $\mathbb{K}[\mathbf{s}] := \mathbb{K}[T_1, \dots, T_s]$. Given a placing map $\sigma \in [\mathbf{s} : \mathbf{r}]$ we define a ring homomorphism $\psi_{\sigma} : \mathbb{K}[\mathbf{r}] \rightarrow \mathbb{K}[\mathbf{s}]$ by

$$\psi_{\sigma} : T_n \mapsto \sum_{m \in \sigma^{-1}(n)} T_m.$$

Note that if $\sigma^{-1}(n) = \emptyset$ then $\psi_{\sigma}(T_n) = 0$. By convention we will assume that $[\mathbf{1} : \mathbf{r}]$ consists of a single placing map σ satisfying $\sigma! = 1$ and whose corresponding $\psi_{\sigma} : \mathbb{K}[\mathbf{r}] \rightarrow \mathbb{K}[\mathbf{1}] := \mathbb{K}$ is given by the augmentation homomorphism.

1.8 If $\sigma \in [\mathbf{s} : \mathbf{r}]$ we define $\mathbf{T}^\sigma \in \mathbb{K}[\mathbf{r}]$ by $\mathbf{T}^\sigma := \prod_{n=1}^r T_n^{\sigma_n}$. Similarly for \mathbf{w} as in (1.3) we define $\mathbf{T}^\mathbf{w} \in \mathbb{K}[\overline{\mathbf{w}}]$ by $\prod_{k=1}^{\overline{w}} T_k^{n_k}$. If $\lambda = (\lambda_1, \dots, \lambda_r) \in \mathbb{K}^r$ we define λ^σ and $\lambda^\mathbf{w}$ by replacing T_n by λ_n in the previous expressions.

Remark 1.9. It is easy to verify that if $\sigma \in [\mathbf{s} : \mathbf{r}]$ and $\tau \in [\mathbf{r} : \mathbf{t}]$ then $\tau \circ \sigma \in [\mathbf{s} : \mathbf{t}]$ and $\psi_{\tau \circ \sigma} = \psi_\sigma \circ \psi_\tau$.

We now single out two special types of placing maps. Let $\sigma \in [\mathbf{s} : \mathbf{r}]$

σ is called a *lift* if σ is injective and $r = s + 1$, and

σ is called a *drop* if σ is surjective and $r = s - 1$.

Remark 1.10. By Remark 1.9 we see that every $\sigma \in [\mathbf{s} : \mathbf{r}]$ can be written as a composition of drops followed by lifts.

1.11 For $\mathbf{w} \in W$ as in (1.1) we let

$$\mathcal{F}(\mathbb{K})^\mathbf{w} = \{E_{\mathbf{w}_1}(\lambda_1) \dots E_{\mathbf{w}_w}(\lambda_w) \mid \lambda_1, \dots, \lambda_w \in \mathbb{K}\} \subset \mathcal{F}(\mathbb{K}).$$

Let e be the identity element of $\mathcal{F}(\mathbb{K})$. If $x \in \mathcal{F}(\mathbb{K})$, $x \neq e$, then there exists a unique $\mathbf{r} \in \overline{W}$ and unique $\lambda_1, \dots, \lambda_r \in \mathbb{K} \setminus \{0\}$ such that $x = E_{\mathbf{r}_1}(\lambda_1) \dots E_{\mathbf{r}_r}(\lambda_r)$. We call this the *reduced expression* of x and say that \mathbf{r} is the *type* of x . By convention $\mathcal{F}(\mathbb{K})^{\mathbf{1}} = \{e\}$ and e is of type $\mathbf{1}$.

POLYNOMIAL FUNCTIONS ON $\mathcal{F}(\mathbb{K})$.

2.1 Given $N \in \mathbb{N}$ we let $\text{Pol}(\mathbb{K}^N)$ be the ring of polynomial functions from \mathbb{K}^N into \mathbb{K} (Bbk Ch. 4). We have a surjective ring homomorphism $\kappa_N : \mathbb{K}[T_1, \dots, T_N] \rightarrow \text{Pol}(\mathbb{K}^N)$. It is easy to verify that κ_1 is injective if and only if κ_N is injective for all $N \in \mathbb{N}$. If these hold we say that \mathbb{K} is *polynomially faithful*, and identify $\text{Pol}(\mathbb{K}^N)$ with $\mathbb{K}[T_1, \dots, T_N]$

Given $\mathbf{w} \in W$ as in (1.1) we define $\pi_\mathbf{w} : \mathbb{K}^w \rightarrow \mathcal{F}(\mathbb{K})^\mathbf{w} \subset \mathcal{F}(\mathbb{K})$ by

$$\pi_\mathbf{w} : (\lambda_1, \dots, \lambda_w) \mapsto E_{\mathbf{w}_1}(\lambda_1) \dots E_{\mathbf{w}_w}(\lambda_w).$$

By convention $\mathbb{K}^0 = \{0\}$ and $\pi_{\mathbf{1}}(0) = e$. (See 1.11.)

A function $f : \mathcal{F}(\mathbb{K}) \rightarrow \mathbb{K}$ is said to be a *polynomial function* if $f \circ \pi_{\mathbf{w}}$ is polynomial for all $\mathbf{w} \in W$: That is $f \circ \pi_{\mathbf{w}} \in \text{Pol}(\mathbb{K}^w)$ for all $\mathbf{w} \in W$. The set of polynomial functions forms a ring which will be denoted by $\text{Pol } \mathcal{F}(\mathbb{K})$.

In this section we will describe the nature of the ring $\text{Pol } \mathcal{F}$ as an inverse limit (Theorem 2.3), and as a completion (Theorem 2.10).

Consider the ring $\mathbb{K}[W] := \prod_{\mathbf{s} \in W} \mathbb{K}[\mathbf{s}]$ as well as its subring $\mathbb{K}[\mathcal{F}] := \varprojlim_{\psi_\sigma} \mathbb{K}[\mathbf{s}]$. A typical element of $\mathbb{K}[\mathcal{F}]$ is thus of the form $F = (F_{\mathbf{r}})_{\mathbf{r} \in W}$ with $\psi_\sigma(F_{\mathbf{r}}) = F_{\mathbf{s}}$ for all $\mathbf{r}, \mathbf{s} \in W$ and $\sigma \in [\mathbf{s} : \mathbf{r}]$.

Proposition 2.2. *Let $f \in \text{Pol } \mathcal{F}(\mathbb{K})$. For $\mathbf{r} \in W$ define $F_{\mathbf{r}} = f \circ \pi_{\mathbf{r}}$. and $F = (F_{\mathbf{r}})_{\mathbf{r} \in W} \in \mathbb{K}[W]$. Then $F \in \mathbb{K}[\mathcal{F}]$.*

Proof. We must show that $\psi_\sigma F_{\mathbf{r}} = F_{\mathbf{s}}$ for all $\sigma \in [\mathbf{s} : \mathbf{r}]$. Assume σ is a lift so that \mathbf{r} is of the form $\mathbf{r} = \mathbf{s}_1 \cdots \mathbf{s}_k \mathbf{i} \mathbf{s}_{k+1} \cdots \mathbf{s}_s$. Then for all $\lambda_1, \dots, \lambda_s \in \mathbb{K}$

$$\begin{aligned} \psi_\sigma F_{\mathbf{r}}(\lambda_1, \dots, \lambda_s) &:= F_{\mathbf{r}}(\lambda_1, \dots, \lambda_{k-1}, 0, \lambda_k, \dots, \lambda_s) \\ &= f(E_{\mathbf{s}_1}(\lambda_1) \cdots E_{\mathbf{s}_s}(\lambda_s)) \\ &= f \circ \pi_{\mathbf{s}}(\lambda_1, \dots, \lambda_s) \\ &:= F_{\mathbf{s}}(\lambda_1, \dots, \lambda_s). \end{aligned}$$

The case of drops follows along similar consideration. Proposition 2.2 now follows from 1.10

□

Theorem 2.3. (i) *There exists a canonical surjective ring homomorphism $\omega_{\mathbb{K}} : \mathbb{K}[\mathcal{F}] \rightarrow \text{Pol } \mathcal{F}(\mathbb{K})$.*

(ii) *For ω to be an isomorphism it is necessary and sufficient that \mathbb{K} be polynomially faithful.*

Proof. Let $F = (F_{\mathbf{r}})_{\mathbf{r} \in W} \in \mathbb{K}[\mathcal{F}]$. Define $\omega_{\mathbb{K}}(F) := \omega(F) : \mathcal{F}(\mathbb{K}) \rightarrow \mathbb{K}$ as follows: Given $x \in \mathcal{F}(\mathbb{K})$ let \mathbf{r} be its type, $E_{\mathbf{r}_1}(\lambda_1) \dots E_{\mathbf{r}_r}(\lambda_r)$ its reduced expression, and set $\omega(F)(x) := F_{\mathbf{r}}(\lambda_1, \dots, \lambda_r)$. We show that $\omega(F)$ is polynomial by establishing that

$$(2.4) \quad \omega(F) \circ \pi_{\mathbf{r}}(\lambda_1, \dots, \lambda_r) = F_{\mathbf{r}}(\lambda_1, \dots, \lambda_r) \quad \text{for all } \lambda_1, \dots, \lambda_r \in \mathbb{K} \text{ and } \mathbf{r} \in W.$$

We now reason by induction on r . If $r = 0$ then (2.4) holds by definition (See 2.1). Assume $r > 0$ and that (2.4) holds for all words of length $< r$. We distinguish two cases:

Case 1: \mathbf{r} is not reduced. Chose k so that $\mathbf{r}_{k-1} = \mathbf{r}_k$. Let $\mathbf{s} = \mathbf{r}_1 \cdots \mathbf{r}_{k-1} \mathbf{r}_{k+1} \cdots \mathbf{r}_r$ and let $\sigma \in [\mathbf{r} : \mathbf{s}]$ be the obvious drop. We have

$$\begin{aligned} \omega(F) \circ \pi_{\mathbf{r}}(\lambda_1, \dots, \lambda_r) &= \omega(F)(E_{\mathbf{r}_1}(\lambda_1) \dots E_{\mathbf{r}_r}(\lambda_r)) \\ &= \omega(F)(E_{\mathbf{r}_1}(\lambda_1) \dots E_{\mathbf{r}_{k-1}}(\lambda_{k-1}) E_{\mathbf{r}_k}(\lambda_k) \dots E_{\mathbf{r}_r}(\lambda_r)) \\ &= \omega(F) \circ \pi_{\mathbf{s}}(\lambda_1, \dots, \lambda_{k-1} + \lambda_k, \dots, \lambda_r) \\ &= F_{\mathbf{s}}(\lambda_1, \dots, \lambda_{k-1} + \lambda_k, \dots, \lambda_r) \quad (\text{by induction}) \\ &= F_{\mathbf{r}}(\lambda_1, \dots, \lambda_{k-1}, \lambda_k, \dots, \lambda_r) \quad (\text{Since } \psi_{\sigma}(F_{\mathbf{s}}) = F_{\mathbf{r}}). \end{aligned}$$

Case 2: \mathbf{r} is reduced. If $\lambda_1, \dots, \lambda_r$ are all nonzero then (2.4) holds by definition: Namely by (2.3). Assume then that $\lambda_k = 0$ for some $1 \leq k \leq r$. Let $\mathbf{s} = \mathbf{r}_1 \cdots \mathbf{r}_{k-1} \mathbf{r}_{k+1} \cdots \mathbf{r}_r$. Let $\sigma \in [\mathbf{s} : \mathbf{r}]$ be the obvious lift (see 1.7 and 2.1 if $r = 1$.) We have

$$\begin{aligned} \omega(F) \circ \pi_{\mathbf{r}}(\lambda_1, \dots, \lambda_r) &= \omega(F)(E_{\mathbf{r}_1}(\lambda_1) \dots E_{\mathbf{r}_r}(\lambda_r)) \\ &= \omega(F)(E_{\mathbf{r}_1}(\lambda_1) \dots E_{\mathbf{r}_{k-1}}(\lambda_{k-1}) E_{\mathbf{r}_{k+1}}(\lambda_{k+1}) \dots E_{\mathbf{r}_r}(\lambda_r)) \\ &= \omega(F) \circ \pi_{\mathbf{s}}(\lambda_1, \dots, \lambda_{k-1}, \lambda_{k+1}, \dots, \lambda_r) \\ &= F_{\mathbf{s}}(\lambda_1, \dots, \lambda_{k-1}, \lambda_{k+1}, \dots, \lambda_r) \quad (\text{by induction}) \\ &= F_{\mathbf{r}}(\lambda_1, \dots, \lambda_{k-1}, 0, \lambda_{k+1}, \dots, \lambda_r) \quad (\text{Since } \psi_{\sigma}(F_{\mathbf{s}}) = F_{\mathbf{r}}) \\ &= F_{\mathbf{r}}(\lambda_1, \dots, \lambda_r). \end{aligned}$$

With (2.4) established we have that the image of $\mathbb{K}[\mathcal{F}]$ under ω does lye inside $\text{Pol } \mathcal{F}(\mathbb{K})$. That ω is a ring homomorphism is clear.

Next we show that ω is surjective. We will do this explicitly by constructing certain polynomial functions $Y_{\mathbb{K}}^{\mathbf{a}}$ which “cover” $\text{Pol } \mathcal{F}(\mathbb{K})$ (Theorem 2.10 below), and then showing that each $Y_{\mathbb{K}}^{\mathbf{a}}$ has a preimage in $\mathbb{K}[\mathcal{F}]$. These polynomial function will play a critical role throughout the paper.

Let $\text{Ass}(\mathbb{Q})$ be the free associative algebra over \mathbb{Q} with free generators $\{x_i\}_{i \in I}$. We attach to $\mathbf{w} \in W$ written as in (1.2) elements $y^{\mathbf{w}}$ and $x^{\mathbf{w}}$ of $\text{Ass}(\mathbb{Q})$ by

$$y^{\mathbf{w}} := \frac{1}{\mathbf{w}!} x_{\mathbf{w}_1}^{n_1} \dots x_{\mathbf{w}_r}^{n_r} =: \frac{1}{\mathbf{w}!} x^{\mathbf{w}}.$$

If $\mathbf{s} = \mathbf{e}$ then we agree that $x^{\mathbf{e}} = y^{\mathbf{e}} = 1$. Thus $\{y^{\mathbf{s}} | \mathbf{s} \in W\}$ is a \mathbb{Q} -basis of $Ass(\mathbb{Q})$. For $i \in I$ and $n \in \mathbb{N}$ the expression y^{i^n} is ambiguous. We will agree that $y^{i^n} = y^{(i^n)}$. Note then that $y^{i^n} = x_i^n/n!$.

The free \mathbb{Z} -module

$$\mathcal{D}(\mathbb{Z}) := \bigoplus_{\mathbf{s} \in W} \mathbb{Z} y^{\mathbf{s}}$$

is a \mathbb{Z} -subalgebra of $Ass(\mathbb{Q})$ (algebra of divided powers).

If $\mathbf{a} \in W$ we define $Y_{\mathbb{Z}}^{(\mathbf{a})} \in \overline{\mathcal{D}(\mathbb{Z})}^*$ and $X_{\mathbb{Q}}^{(\mathbf{a})} \in \overline{Ass(\mathbb{Q})}^*$ (here and elsewhere overbars will denote completions and $*$ duals) by

$$Y_{\mathbb{Z}}^{(\mathbf{a})} \left(\sum_{\mathbf{b} \in W} c_{\mathbf{b}} y^{\mathbf{b}} \right) = c_{\mathbf{a}} \quad \text{and} \quad X_{\mathbb{Q}}^{(\mathbf{a})} \left(\sum_{\mathbf{b} \in W} c_{\mathbf{b}} x^{\mathbf{b}} \right) = c_{\mathbf{a}}.$$

Going back to our base ring \mathbb{K} we consider the ring $\mathcal{D}(\mathbb{K}) = \mathbb{K} \otimes_{\mathbb{Z}} \mathcal{D}(\mathbb{Z})$ and its formal completion $\overline{\mathcal{D}(\mathbb{K})}$. The functionals $Y_{\mathbb{Z}}^{(\mathbf{a})}$ extend naturally to functionals $Y_{\mathbb{K}}^{(\mathbf{a})}$ on $\mathcal{D}(\mathbb{K})$ and $\overline{\mathcal{D}(\mathbb{K})}$.

Consider the (divided power version of the) Magnus group

$$M(\mathbb{K}) := \left\{ 1 + \sum_{\mathbf{b} \in W, b \geq 1} c_{\mathbf{b}} y^{\mathbf{b}} \right\} \subset \overline{\mathcal{D}(\mathbb{K})}.$$

For each $i \in I$ the map $\varepsilon_i : \mathbb{K} \rightarrow M$ given by $\lambda \mapsto \sum \lambda^n y^{i^n}$ is a group homomorphism. By universal nonsense this yields a (unique) group homomorphism $\varepsilon : \mathcal{F}(\mathbb{K}) \rightarrow M(\mathbb{K})$ satisfying

$$\varepsilon : E_{i_1}(\lambda_1) \dots E_{i_N}(\lambda_N) \mapsto \varepsilon_{i_1}(\lambda_1) \dots \varepsilon_{i_N}(\lambda_N).$$

We use this homomorphism to construct the functions $Y_{\mathbb{K}}^{\mathbf{a}} : \mathcal{F}(\mathbb{K}) \rightarrow \mathbb{K}$ that we need:

$$Y_{\mathbb{K}}^{\mathbf{a}} := Y_{\mathbb{K}}^{(\mathbf{a})} \circ \varepsilon. \tag{2.5}$$

Remark 2.6. If \mathbb{K} is a \mathbb{Q} -algebra we can define functions $X_{\mathbb{K}}^{\mathbf{a}} := X_{\mathbb{K}}^{(\mathbf{a})} \circ \varepsilon : \mathcal{F}(\mathbb{K}) \rightarrow \mathbb{K}$. Note that $Y_{\mathbb{K}}^{\mathbf{a}} = \mathbf{a}! X_{\mathbb{K}}^{\mathbf{a}}$.

Proposition 2.7. *Let $\mathbf{a}, \mathbf{s} \in W$ and let $\lambda = (\lambda_1, \dots, \lambda_s) \in \mathbb{K}^s$. Then*

$$Y_{\mathbb{K}}^{\mathbf{a}}(E_{\mathbf{s}}(\lambda)) = \sum_{\sigma \in [\mathbf{a}:\mathbf{s}]} \frac{\mathbf{a}! \lambda^{\sigma}}{\sigma!}.$$

In particular $Y_{\mathbb{K}}^{\mathbf{a}} \circ \pi_{\mathbf{s}}$ is the polynomial function on $\mathbb{K}^{\mathbf{s}}$ defined by $\sum_{\sigma \in [\mathbf{a}:\mathbf{s}]} \frac{\mathbf{a}! T^{\sigma}}{\sigma!}$, and $Y_{\mathbb{K}}^{\mathbf{a}}$ is a polynomial function on $\mathcal{F}(\mathbb{K})$. (Note that $\sigma!$ divides $\mathbf{w}!$ in \mathbb{Z} . This allows us to think of $\frac{\mathbf{a}!}{\sigma!}$ as an element of \mathbb{K} in a natural way.)

Proof.

$$\begin{aligned} Y_{\mathbb{K}}^{\mathbf{a}}(E_{\mathbf{s}}(\lambda)) &:= Y_{\mathbb{K}}^{(\mathbf{a})}(\varepsilon(E_{\mathbf{s}}(\lambda))) \\ &:= Y_{\mathbb{K}}^{(\mathbf{a})}\left(\prod_{i=1}^s \left(\sum_{n_i \geq 0} \lambda_i^{n_i} y^{s_i n_i}\right)\right) \\ &= Y_{\mathbb{K}}^{(\mathbf{a})}\left(\sum_{\mathbf{n} \in \mathbb{N}^s} \lambda^{\mathbf{n}} y^{s_1 n_1} \dots y^{s_s n_s}\right). \end{aligned}$$

With each $\mathbf{n} \in \mathbb{N}^s$ we associate in a natural way a word $\mathbf{w} = \mathbf{s}_1^{n_1} \dots \mathbf{s}_s^{n_s} \in W$ and a placing $\sigma \in [\mathbf{w}:\mathbf{s}]$ such that $n_i = \sigma_i$. This procedure establishes a bijection between $[\mathbf{w}:\mathbf{s}]$ and the occurrences of $y^{\mathbf{w}}$ in the expansion of $\varepsilon(E_{\mathbf{s}}(\lambda))$. Multiplication in the divided powers algebra \mathcal{D} yields

$$y^{s_1 n_1} \dots y^{s_s n_s} = \frac{\mathbf{w}!}{\sigma!} y^{\mathbf{w}}.$$

When acting on the above infinite sum $Y_{\mathbb{K}}^{(\mathbf{a})}$ picks up only summands corresponding to $\mathbf{w} = \mathbf{a}$. Thus

$$Y_{\mathbb{K}}^{\mathbf{a}}(E_{\mathbf{s}}(\lambda)) = \sum_{\sigma \in [\mathbf{a}:\mathbf{s}]} \frac{\mathbf{a}! \lambda^{\sigma}}{\sigma!}$$

□

Corollary 2.8. *Let $\mathbf{a}, \mathbf{s} \in W$. For $Y_{\mathbb{K}}^{\mathbf{a}}$ to vanish in $\mathcal{F}(\mathbb{K})^{\mathbf{s}}$ it is necessary and sufficient that $[\mathbf{a}:\mathbf{s}]$ be empty.*

Proof. If $[\mathbf{a}:\mathbf{s}]$ is empty then $Y_{\mathbb{K}}^{\mathbf{a}} \circ \pi_{\mathbf{s}} = 0$. This shows that $Y_{\mathbb{K}}^{\mathbf{a}}$ vanishes in $\mathcal{F}(\mathbb{K})^{\mathbf{s}}$.

If $[\mathbf{a}:\mathbf{s}]$ is not empty then $\bar{\mathbf{a}}$ is a subword of \mathbf{s} so that $\mathcal{F}(\mathbb{K})^{\bar{\mathbf{a}}} \subset \mathcal{F}(\mathbb{K})^{\mathbf{s}}$. But $\sum_{\sigma \in [\mathbf{a}:\bar{\mathbf{a}}]} \frac{\mathbf{a}! T^{\sigma}}{\sigma!} = T_1^{n_1} \dots T_{\bar{\mathbf{a}}}^{n_{\bar{\mathbf{a}}}}$ (see 1.6), which does not vanish at $T_1 = \dots = T_{\bar{\mathbf{a}}} = 1$.

□

2.9 Given $S \subset W$ and $\mathbf{r} \in W$ define $S_{\mathbf{r}} := \{\mathbf{a} \in S : [\mathbf{a} : \mathbf{r}] \neq \emptyset\}$ (note that $S_{\mathbf{a}} = S_{\bar{\mathbf{a}}}$). Note also that $\mathbf{1} \in S_{\mathbf{r}}$ for all $\mathbf{r} \in W$ (See 1.7.) We say that S is *summable* if it satisfies the following property:

SUM. For all $\mathbf{r} \in \overline{W}$ the set $S_{\mathbf{r}}$ is finite. A family $\{c_{\mathbf{a}}Y_{\mathbb{K}}^{\mathbf{a}} | c_{\mathbf{a}} \in \mathbb{K}\}_{\mathbf{a} \in W}$ is said to be *summable* if its support $\{\mathbf{a} : c_{\mathbf{a}} \neq 0\}$ is summable. In this case by Corollary 2.8 there exists a unique function

$$\sum_{\mathbf{a} \in W} c_{\mathbf{a}}Y_{\mathbb{K}}^{\mathbf{a}} : \mathcal{F}(\mathbb{K}) \rightarrow \mathbb{K}$$

satisfying

$$\left(\sum_{\mathbf{a} \in W} c_{\mathbf{a}}Y_{\mathbb{K}}^{\mathbf{a}}\right)(x) = \sum_{\mathbf{a} \in W} c_{\mathbf{a}}Y_{\mathbb{K}}^{\mathbf{a}}(x)$$

for all $x \in \mathcal{F}(\mathbb{K})$.

Theorem 2.10. (i) Every element of $\text{Pol } \mathcal{F}(\mathbb{K})$ is of the form $\sum_{\mathbf{a} \in W} c_{\mathbf{a}}Y_{\mathbb{K}}^{\mathbf{a}}$ for some summable family $(c_{\mathbf{a}}Y_{\mathbb{K}}^{\mathbf{a}})_{\mathbf{a} \in W}$.

(ii) For the family of (i) to be unique it is necessary and sufficient that \mathbb{K} be polynomially faithful.

Proof. We reason by induction on $N \in \mathbb{N}$ to establish the existence of a summable family

$(c_{\mathbf{a}}(N)Y_{\mathbb{K}}^{\mathbf{a}})_{\mathbf{a} \in W}$ such that

- (a) The restrictions of f and $\sum_{\mathbf{a} \in W} c_{\mathbf{a}}(N)Y_{\mathbb{K}}^{\mathbf{a}}$ to $\mathcal{F}(\mathbb{K})^{\mathbf{r}}$ agree whenever $\mathbf{r} \in \overline{W}$ satisfies $r \leq N$.
- (b) $c_{\mathbf{a}}(N) = 0$ whenever $\bar{\mathbf{a}} > N$.
- (c) $c_{\mathbf{a}}(M) = c_{\mathbf{a}}(N)$ whenever $\bar{\mathbf{a}} \leq M \leq N$.

If $N = 0$ we set $c_{\mathbf{e}}(0) = f(e)$ and $c_{\mathbf{a}}(0) = 0$ for all $\mathbf{a} \in W$, $\mathbf{a} \neq \mathbf{e}$.

Assume $N > 0$, let

$$g = f - \sum_{\mathbf{a} \in W} c_{\mathbf{a}}(N-1)Y_{\mathbb{K}}^{\mathbf{a}}.$$

Then $g \in \text{Pol } \mathcal{F}(\mathbb{K})$ and g vanishes on $F_{\mathbb{K}}^s$ whenever $s < N$. It follows that for $\mathbf{r} \in \overline{W}$ with $r = N$ there is no loss of generality in assuming that $g_{\mathbf{r}}$ is given by a polynomial $p_{\mathbf{r}}$ which is divisible by $T_1 \dots T_N$, hence of the form

$$p_{\mathbf{r}} = \sum_{\overline{\mathbf{a}}=\mathbf{r}} c_{\mathbf{a}}(N) \mathbf{T}^{\mathbf{a}}.$$

for some coefficients $c_{\mathbf{a}}(N) \in \mathbb{K}$. If we now set $c_{\mathbf{a}}(N) := c_{\mathbf{a}}(N-1)$ for all $\mathbf{a} \in W$ with $\overline{\mathbf{a}} < N$ and $c_{\mathbf{a}}(N) = 0$ if $\overline{\mathbf{a}} > N$, the family $\sum_{\mathbf{a} \in W} c_{\mathbf{a}}(N) Y^{\mathbf{a}}$ is as desired.

For $\mathbf{a} \in W$ let $c_{\mathbf{a}} := c_{\mathbf{a}}(\overline{\mathbf{a}})$. The family $(c_{\mathbf{a}} Y_{\mathbb{K}}^{\mathbf{a}})_{\mathbf{a} \in W}$ is summable while by (a) we get $f = \sum_{\mathbf{a} \in W} c_{\mathbf{a}} Y_{\mathbb{K}}^{\mathbf{a}}$. This finishes the proof of (i). The proof of (ii) will be given below.

□

We now finish the proof of Theorem 2.3. Let $f \in \text{Pol } \mathcal{F}(\mathbb{K})$ and write $f = \sum_{\mathbf{a} \in W} c_{\mathbf{a}} Y_{\mathbb{K}}^{\mathbf{a}}$ as in 2.10(i). For $\mathbf{s} \in W$ define $F_{\mathbf{s}} := \sum_{\mathbf{a} \in W} c_{\mathbf{a}} Y_{\mathbb{Z}}^{\mathbf{a}} \circ \pi_{\mathbf{s}} \in \mathbb{K}[\mathbf{s}]$. (To see that this makes sense note that if $Y_{\mathbb{Z}}^{\mathbf{a}} \circ \pi_{\mathbf{s}} \neq 0$ then $[\overline{\mathbf{a}} : \mathbf{s}] \neq \emptyset$ (Corollary 2.8), hence $[\overline{\mathbf{a}} : \overline{\mathbf{s}}] \neq \emptyset$. Then only finitely many $c_{\mathbf{a}}$'s are nonzero because $(c_{\mathbf{a}} Y_{\mathbb{K}}^{\mathbf{a}})$ is summable.) By Propositions 2.2 and 2.7 we see that $F := (F_{\mathbf{s}})_{\mathbf{s} \in W} \in \mathbb{K}[\mathcal{F}]$. It is clear that $\omega(F) = \sum_{\mathbf{a} \in W} c_{\mathbf{a}} Y_{\mathbb{K}}^{\mathbf{a}}$. The proof of part (i) of Theorem 2.3 is now complete.

As for (ii) if ω is not injective there exists $F \in \mathbb{K}[\mathcal{F}]$ and $\mathbf{r} \in W$ with $F_{\mathbf{r}} \neq 0$ and $\omega(F) = 0$. Since $\kappa_r(F_{\mathbf{r}}) = 0$ \mathbb{K} is not polynomially faithful (See 2.1).

Conversely if \mathbb{K} is not polynomially faithful, there exists a nonzero polynomial $p = \sum a_n T^n \in \mathbb{K}[T]$ with $p(\lambda) = 0$ for all $\lambda \in \mathbb{K}$. Choose $i \in I$ and let $f = \sum a_n Y^{i^n}$. (There is no ambiguity here: $Y^{(i^n)} = (Y^i)^n$.) By Proposition 2.7 there exists $F \in \mathbb{K}[\mathcal{F}]$, $F \neq 0$ with $\omega(F) = f$, while by Corollary 2.8 f vanishes everywhere in $\text{Pol } \mathcal{F}(\mathbb{K})$. The uniqueness statement of Theorem 2.10 follows along similar lines. The proofs of both Theorems are now complete.

□

MULTIPLICATION OF POLYNOMIAL FUNCTIONS.

Let $\mathbf{a}, \mathbf{b} \in W$. By a *shuffle* of (\mathbf{a}, \mathbf{b}) we understand a triple $(\alpha, \beta, \mathbf{s})$ where $\mathbf{s} \in W$, $\alpha \in [\mathbf{a} : \mathbf{s}]$, and $\beta \in [\mathbf{b} : \mathbf{s}]$ are such that

Sh 1 α and β are injective.

Sh 2 $\alpha[a] \cap \beta[b] = \emptyset$.

Sh 3 $s = a + b$.

Intuitively \mathbf{s} is a word made out of \mathbf{a} and \mathbf{b} where the support of these subwords do not intersect. It is easy to see that if $(\alpha', \beta', \mathbf{s}')$ is another shuffle of (\mathbf{a}, \mathbf{b}) then $\alpha[a] = \alpha'[a] \iff \beta[b] = \beta'[b]$. In this case we have $\mathbf{s} = \mathbf{s}'$ and the two shuffles are equal.

There is a natural bijection between the set $\text{Sh}(\mathbf{a}, \mathbf{b})$ of all shuffles of (\mathbf{a}, \mathbf{b}) and the set of strictly increasing (hence injective) maps from $[a]$ into $[a + b]$. Thus

$$\text{Card}(\text{Sh}(\mathbf{a}, \mathbf{b})) = \frac{(a + b)!}{a!b!}. \quad (3.1)$$

Next we introduce an equivalence relation \sim on $\text{Sh}(\mathbf{a}, \mathbf{b})$ that will play an important role when dealing with the multiplicative structure of $\text{Pol } \mathcal{F}(\mathbb{K})$ when \mathbb{K} is not a \mathbb{Q} -algebra (See 3.7 below.)

ESh $(\alpha, \beta, \mathbf{s}) \sim (\alpha', \beta', \mathbf{s}') \iff \rho_{\mathbf{s}} \circ \alpha = \rho_{\mathbf{s}'} \circ \alpha' \quad \text{and} \quad \rho_{\mathbf{s}} \circ \beta = \rho_{\mathbf{s}'} \circ \beta'$.

We will denote $\text{Sh}(\mathbf{a}, \mathbf{b})/\sim$ by $\widetilde{\text{Sh}}(\mathbf{a}, \mathbf{b})$. If $\mathcal{P} = (\alpha, \beta, \mathbf{s}) \in \text{Sh}(\mathbf{a}, \mathbf{b})$ then its equivalence class will be denoted by $(\widetilde{\alpha}, \widetilde{\beta}, \widetilde{\mathbf{s}})$. For $\mathcal{P} = (\alpha, \beta, \mathbf{s}) \in \text{Sh}(\mathbf{a}, \mathbf{b})$ we set

$$\begin{aligned} sh(\mathcal{P}) &= sh(\widetilde{\mathcal{P}}) = \mathbf{s} \quad (\text{see next Lemma}) \quad \text{and} \\ \mathcal{P}! &= \widetilde{\mathcal{P}}! = (\rho_{\mathbf{s}} \circ \alpha)! (\rho_{\mathbf{s}} \circ \beta)! \end{aligned} \quad (3.2)$$

Lemma 3.3. *Let $\mathcal{P} = (\alpha, \beta, \mathbf{s}) \in \text{Sh}(\mathbf{a}, \mathbf{b})$. Then*

- (i) *If $(\alpha', \beta', \mathbf{s}') \in \widetilde{\mathcal{P}}$ then $\mathbf{s}' = \mathbf{s}$,*
- (ii) *$\text{Card}(\widetilde{\mathcal{P}}) = \frac{\mathbf{s}!}{\mathcal{P}!}$,*
- (iii) *$\widetilde{\mathcal{P}}!$ divides $\mathbf{a}! \mathbf{b}!$.*

Proof. It is clear that $\rho_{\mathbf{s}} \circ \alpha!$ divides $\mathbf{a}!$, and similarly for β . This shows that (iii) holds.

If $\mathbf{s} = \overline{\mathbf{s}}_1^{\ell_1} \cdots \overline{\mathbf{s}}_{\overline{\mathbf{s}}}^{\ell_{\overline{\mathbf{s}}}}$ is the reduced expression of \mathbf{s} then $\mathbf{a} = \overline{\mathbf{s}}_1^{p_1} \cdots \overline{\mathbf{s}}_{\overline{\mathbf{s}}}^{p_{\overline{\mathbf{s}}}}$ and $\mathbf{b} = \overline{\mathbf{s}}_1^{q_1} \cdots \overline{\mathbf{s}}_{\overline{\mathbf{s}}}^{q_{\overline{\mathbf{s}}}}$ for some unique $p_1, \dots, q_{\overline{\mathbf{s}}} \in \mathbb{Z}_{\geq 0}$ satisfying $p_h + q_h = \ell_h$ for all $1 \leq h \leq \overline{\mathbf{s}}$.

The equivalence class of a shuffle is then determined by the sequence $p_1, \dots, q_{\bar{s}}$. This observation shows that (i) holds. As for (ii) we have

$$\begin{aligned} \text{Card}(\widetilde{\alpha, \beta, \mathbf{s}}) &= \prod_{k=1}^{\bar{s}} \binom{\ell_k}{p_k} \\ &= \prod_{k=1}^{\bar{s}} \frac{\ell_k!}{p_k! q_k!} = \frac{\mathbf{s}!}{(\rho_{\mathbf{s}} \circ \alpha)! (\rho_{\mathbf{s}} \circ \beta)!} . \end{aligned}$$

□

Next we introduce the shuffle product ([Rtn] is an excellent reference for this.) The algebra $\text{Ass}(\mathbb{Q})$ possesses a Hopf algebra structure where the coproduct $\Delta : \text{Ass}(\mathbb{Q}) \rightarrow \text{Ass}(\mathbb{Q}) \otimes \text{Ass}(\mathbb{Q})$ is the unique homomorphism of associative algebras satisfying

$$\Delta(x_i) := x_i \otimes 1 + 1 \otimes x_i.$$

This coproduct is co-commutative and can be extended to $\overline{\text{Ass}}(\mathbb{Q})$. This endows its dual $\overline{\text{Ass}}(\mathbb{Q})^*$ with a commutative multiplication $\#$ given by

$$X \# Y(x) := X \otimes Y(\Delta(x)) \in \mathbb{Q} \otimes \mathbb{Q} \cong \mathbb{Q}, \text{ for all } X, Y \in \overline{\text{Ass}}(\mathbb{Q})^*, \text{ and } x \in \overline{\text{Ass}}(\mathbb{Q}) \quad (3.4)$$

This multiplication is related to the shuffle product. More precisely (See [Rtn] Proposition 1.8)

$$X_{\mathbb{Q}}^{(\mathbf{a})} \# X_{\mathbb{Q}}^{(\mathbf{b})} = \sum_{\mathcal{P} \in \text{Sh}(\mathbf{a}, \mathbf{b})} X_{\mathbb{Q}}^{sh(\mathcal{P})} \quad (3.5)$$

The next Lemma says that the $E_{\mathbf{s}}(\lambda)$'s are group like.

Lemma 3.6. *Let $\mathbf{s} \in W$. Then $\Delta(\epsilon(E_{\mathbf{s}}(\lambda))) = \epsilon(E_{\mathbf{s}}(\lambda)) \otimes \epsilon(E_{\mathbf{s}}(\lambda))$ for all $\lambda \in \mathbb{K}^{\mathbf{s}}$*

Proof. Since $\Delta(1) = 1 \otimes 1$ we may assume $s > 0$. We now reason by induction on

$s > 0$. If $s = 1$ then $s = i \in I$ and for $\lambda \in \mathbb{K}$

$$\begin{aligned}
\Delta(\epsilon(E_i(\lambda))) &= \Delta(\exp(\lambda x_i)) \\
&= \exp(\Delta(\lambda x_i)) \\
&= \exp(\lambda(x_i \otimes 1) + \lambda(1 \otimes x_i)) \\
&= \exp(\lambda(x_i \otimes 1))\exp(\lambda(1 \otimes x_i)) \\
&= (\exp(\lambda x_i) \otimes 1)(1 \otimes \exp(\lambda x_i)) \\
&= \exp(\lambda x_i) \otimes \exp(\lambda x_i) \\
&= \epsilon(E_i(\lambda)) \otimes \epsilon(E_i(\lambda)).
\end{aligned}$$

For the induction step, assume $s = \mathbf{w}i$, $\mathbf{w} \in W$, $i \in I$. Then

$$\begin{aligned}
\Delta(\epsilon(E_{\mathbf{w}}(\lambda)E_i(\lambda_s))) &= \Delta(\epsilon(E_{\mathbf{w}}(\lambda))\Delta(\epsilon(E_i(\lambda_s)))) \\
&= (\epsilon(E_{\mathbf{w}}(\lambda)) \otimes \epsilon(E_{\mathbf{w}}(\lambda)))(\epsilon(E_i(\lambda_s)) \otimes \epsilon(E_i(\lambda_s))) \\
&= \epsilon(E_{\mathbf{w}}(\lambda)E_i(\lambda_s)) \otimes \epsilon(E_{\mathbf{w}}(\lambda)E_i(\lambda_s)).
\end{aligned}$$

Theorem 3.7. (*Multiplication Formula*)

Let $Y(\mathbb{K})$ be the submodule of $\text{Pol } \mathcal{F}(\mathbb{K})$ spanned by $\{Y_{\mathbb{K}}^{\mathbf{a}}\}_{\mathbf{a} \in W}$, and if \mathbb{K} is a \mathbb{Q} -algebra, let $X(\mathbb{K})$ be the submodule of $\text{Pol } \mathcal{F}(\mathbb{K})$ spanned by $\{X_{\mathbb{K}}^{\mathbf{a}}\}_{\mathbf{a} \in W}$ (see Remark 2.6). Then

(i) Multiplication in $X(\mathbb{K})$ coincides with the shuffle product:

$$X_{\mathbb{K}}^{\mathbf{a}} X_{\mathbb{K}}^{\mathbf{b}} = \sum_{\mathcal{P} \in \text{Sh}(\mathbf{a}, \mathbf{b})} X_{\mathbb{K}}^{\text{sh}(\mathcal{P})}.$$

(ii) $Y(\mathbb{K})$ is a subalgebra of $\text{Pol } \mathcal{F}(\mathbb{K})$ whose multiplication is given by

$$Y_{\mathbb{K}}^{\mathbf{a}} Y_{\mathbb{K}}^{\mathbf{b}} = \sum_{\tilde{\mathcal{P}} \in \tilde{\text{Sh}}(\mathbf{a}, \mathbf{b})} \frac{\mathbf{a}! \mathbf{b}!}{\tilde{\mathcal{P}}!} Y_{\mathbb{K}}^{\text{sh}(\tilde{\mathcal{P}})}$$

(Here $\frac{\mathbf{a}! \mathbf{b}!}{\tilde{\mathcal{P}}!} \in \mathbb{Z}$ is viewed naturally as an element of \mathbb{K} . See Lemma 3.3)

(iii) Multiplication in $\text{Pol } \mathcal{F}(\mathbb{K})$ is the (algebraically continuous, in the sense of Section 5) extension of the multiplication in $Y(\mathbb{K})$.

Proof.

$$\begin{aligned}
X_{\mathbb{Q}}^{\mathbf{a}} X_{\mathbb{Q}}^{\mathbf{b}}(E_{\mathbf{s}}(\lambda)) &= X_{\mathbb{Q}}^{\mathbf{a}}(E_{\mathbf{s}}(\lambda)) X_{\mathbb{Q}}^{\mathbf{b}}(E_{\mathbf{s}}(\lambda)) \\
&= X_{\mathbb{Q}}^{(\mathbf{a})}(\epsilon(E_{\mathbf{s}}(\lambda))) X_{\mathbb{Q}}^{(\mathbf{b})}(\epsilon(E_{\mathbf{s}}(\lambda))) \\
&= X_{\mathbb{Q}}^{(\mathbf{a})} \otimes X_{\mathbb{Q}}^{(\mathbf{b})}(\epsilon(E_{\mathbf{s}}(\lambda)) \otimes \epsilon(E_{\mathbf{s}}(\lambda))) \\
&= X_{\mathbb{Q}}^{(\mathbf{a})} \otimes X_{\mathbb{Q}}^{(\mathbf{b})}(\Delta(\epsilon(E_{\mathbf{s}}(\lambda)))) \quad \text{by Lemma 3.6} \\
&= X_{\mathbb{Q}}^{(\mathbf{a})} \sharp X_{\mathbb{Q}}^{(\mathbf{b})}(\epsilon(E_{\mathbf{s}}(\lambda))) \quad \text{by (3.4)} \\
&= \sum_{\mathcal{P} \in \text{Sh}(\mathbf{a}, \mathbf{b})} X_{\mathbb{Q}}^{(sh(\mathcal{P}))}(\epsilon(E_{\mathbf{s}}(\lambda))) \quad \text{by (3.5)} \\
&= \sum_{\mathcal{P} \in \text{Sh}(\mathbf{a}, \mathbf{b})} X_{\mathbb{Q}}^{sh(\mathcal{P})}((E_{\mathbf{s}}(\lambda)))
\end{aligned}$$

This shows that (i) holds in the case $\mathbb{K} = \mathbb{Q}$. The general case follows from Proposition 2.7 and the fact that $\mathbb{K}[\mathbf{s}] \simeq \mathbb{K} \otimes \mathbb{Q}[\mathbf{s}]$

(ii) By identifying $Y(\mathbb{Z})$ inside $X(\mathbb{Q})$ via $Y_{\mathbb{Z}}^{\mathbf{w}} = \mathbf{w}! X_{\mathbb{Q}}^{\mathbf{w}}$ we get from (i) and Lemma 3.3 that (ii) holds in the case $\mathbb{K} = \mathbb{Z}$. The general case now follows by Proposition 2.7 together with the canonical isomorphism $\mathbb{K}[\mathbf{s}] \cong \mathbb{K} \otimes_{\mathbb{Z}} \mathbb{Z}[\mathbf{s}]$.

(iii) Let $f, g \in \text{Pol } \mathcal{F}(\mathbb{K})$. By Theorem 2.10 we can write $f = \sum_{\mathbf{a} \in R} c_{\mathbf{a}} Y_{\mathbb{K}}^{\mathbf{a}}$ and $g = \sum_{\mathbf{b} \in T} d_{\mathbf{b}} Y_{\mathbb{K}}^{\mathbf{b}}$ where R and T are summable set. If $\mathcal{P} = (\alpha, \beta, \mathbf{s}) \in \text{Sh}(\mathbf{a}, \mathbf{b})$ then $\mathbf{a}, \mathbf{b} \in W_{\mathbf{s}}$. It follows that the set $\{(\mathbf{a}, \mathbf{b}) \in R \times T : c_{\mathbf{a}} d_{\mathbf{b}} \neq 0\} \cap W_{\mathbf{s}} \times W_{\mathbf{s}}$ is finite. If we now set

$$\begin{aligned}
h &= \sum_{\mathbf{s} \in W} \left(\sum_{\substack{\mathbf{a}, \mathbf{b} \in W \\ \tilde{\mathcal{P}} \in \tilde{\text{Sh}}(\mathbf{a}, \mathbf{b}) \\ sh(\tilde{\mathcal{P}}) = \mathbf{s}}} \frac{\mathbf{a}! \mathbf{b}!}{\tilde{\mathcal{P}}!} c_{\mathbf{a}} d_{\mathbf{b}} \right) Y_{\mathbb{K}}^{\mathbf{s}} \\
&:= \sum_{\mathbf{s} \in W} k_{\mathbf{s}} Y_{\mathbb{K}}^{\mathbf{s}}
\end{aligned}$$

we see that $S := \{\mathbf{s} \in W : k_{\mathbf{s}} \neq 0\}$ is summable, and that h and fg agree on each $\mathcal{F}^{\mathbf{r}}$. A different proof of this result is given in Remark 5.12.

Remark 3.8 The sum $X(\mathbb{Z}) := \sum_{\mathbf{a} \in W} \mathbb{Z} X_{\mathbb{Q}}^{\mathbf{a}} \subset X(\mathbb{Q})$ is direct and closed under multiplication. In fact $X(\mathbb{Z})$ is the \mathbb{Z} -shuffle algebra (part (i) of the last Theorem).

If \mathbb{K} is polynomially faithful there exists a unique \mathbb{Z} -linear map

$$\begin{aligned}\zeta: Y(\mathbb{Z}) &\rightarrow X(\mathbb{Z}) \\ Y_{\mathbb{Z}}^{\mathbf{a}} &\mapsto \mathbf{a}! X_{\mathbb{Q}}^{\mathbf{a}}.\end{aligned}$$

Part (ii) of the last Theorem shows that ζ is a \mathbb{Z} -algebra homomorphism.

ACTION OF $\mathcal{F}(\mathbb{K})$ ON $\text{Pol } \mathcal{F}(\mathbb{K})$.

The group $\mathcal{F}(\mathbb{K})$ acts on $\text{Pol } \mathcal{F}(\mathbb{K})$ naturally by left and right translations: For $h \in \mathcal{F}(\mathbb{K})$ define L_h and $R_h \in \text{End}_{\mathbb{K}}(\text{Pol } \mathcal{F}(\mathbb{K}))$ by $(L_h f)(g) = f(h^{-1}g)$ and $(R_h f)(g) = f(gh)$ for all $h, g \in \mathcal{F}(\mathbb{K})$ and $f \in \text{Pol } \mathcal{F}(\mathbb{K})$.

The next proposition gives the explicit formula for the action of the generating subgroups of $\mathcal{F}(\mathbb{K})$. To this end we introduce the following notation: given $\mathbf{a} \in W$ and $0 \leq p \leq a$ we let $\vec{\mathbf{a}}^p$ (respectively $\overleftarrow{\mathbf{a}}^p$) be the word obtained by deleting the first (respectively last) p letters of \mathbf{a} . In addition if $i \in I$ we let $\vec{\mathbf{a}}(i)$ (resp. $\overleftarrow{\mathbf{a}}(i)$) be the number of i 's at the beginning (resp. end) of \mathbf{a} .

Proposition 4.1. *Let $\mathbf{a} = \overline{\mathbf{a}}_1^{n_1} \cdots \overline{\mathbf{a}}_{\overline{\mathbf{a}}}^{n_{\overline{\mathbf{a}}}}$ be the reduced expression of an element $\mathbf{a} \in W$. For $i \in I$ and $\lambda \in \mathbb{K}$ we have*

$$\begin{aligned}L_{E_i(\lambda)} Y_{\mathbb{K}}^{\mathbf{a}} &= \sum_{p=0}^{\vec{\mathbf{a}}(i)} \binom{\vec{\mathbf{a}}(i)}{p} (-\lambda)^p Y_{\mathbb{K}}^{\vec{\mathbf{a}}^p} \\ R_{E_i(\lambda)} Y_{\mathbb{K}}^{\mathbf{a}} &= \sum_{p=0}^{\overleftarrow{\mathbf{a}}(i)} \binom{\overleftarrow{\mathbf{a}}(i)}{p} \lambda^p Y_{\mathbb{K}}^{\overleftarrow{\mathbf{a}}^p}\end{aligned}$$

Proof. Let $\mathbf{s} \in W$ and let $\lambda = (\lambda_1, \dots, \lambda_s) \in \mathbb{K}^s$. Set $\mathbf{r} = \mathbf{s}i$ and $\mu = (\lambda_1, \dots, \lambda_s, \lambda)$. Then

$$\begin{aligned}R_{E_i(\lambda)} Y_{\mathbb{K}}^{\mathbf{a}}(E_{\mathbf{s}}(\lambda)) &= Y_{\mathbb{K}}^{\mathbf{a}}(E_{\mathbf{s}}(\lambda)E_i(\lambda)) \\ &= \sum_{\tau \in [\mathbf{a}:\mathbf{r}]} \frac{\mathbf{a}!}{\tau!} \mu^{\tau} \quad (\text{by Proposition 2.7}).\end{aligned} \tag{4.2}$$

If $i \neq \overline{\mathbf{a}}_{\overline{\mathbf{a}}}$ then there is a natural bijection between the sets $[\mathbf{a}:\mathbf{r}]$ and $[\mathbf{a}:\mathbf{s}]$. If under this $\tau \in [\mathbf{a}:\mathbf{r}]$ corresponds to $\sigma \in [\mathbf{a}:\mathbf{s}]$ then $\tau! = \sigma!$ and $\mu^{\tau} = \lambda^{\sigma}$.

Thus in this case we obtain that, as desired,

$$(4.2) = \sum_{\sigma \in [\mathbf{a}:\mathbf{s}]} \frac{\mathbf{a}!}{\sigma!} \lambda^\sigma = Y_{\mathbb{K}}^{\mathbf{a}}(E_{\mathbf{s}}(\lambda)).$$

If $i = \bar{\mathbf{a}}_{\bar{\mathbf{a}}}$ then for any $0 \leq p \leq n_{\bar{\mathbf{a}}}$ there exists a natural bijection between the sets $\{\tau \in [\mathbf{a}:\mathbf{r}]: \tau_{s+1} = p \text{ and } [\bar{\mathbf{a}}^p:\mathbf{s}]\}$ (see 1.6). If $\tau \in [\mathbf{a}:\mathbf{r}]$ corresponds to $\sigma \in [\bar{\mathbf{a}}^p:\mathbf{s}]$ under this bijection then

$$\begin{cases} \tau! = p!\sigma! \text{ and} \\ \bar{\mathbf{a}}^p! \prod_{h=0}^{p-1} (n_{\bar{\mathbf{a}}} - h) = \mathbf{a}! \\ \mu^\tau = \lambda^\sigma \lambda^p. \end{cases} \quad (4.3)$$

Thus

$$\begin{aligned} (4.2) &= \sum_{p=0}^{\bar{\mathbf{a}}(i)} \sum_{\substack{\tau \in [\mathbf{a}:\mathbf{r}] \\ \tau_{s+1}=p}} \frac{\mathbf{a}!}{\tau!} \mu^\tau \\ &= \sum_{p=0}^{\bar{\mathbf{a}}(i)} \sum_{\sigma \in [\bar{\mathbf{a}}^p:\mathbf{s}]} \binom{\bar{\mathbf{a}}(i)}{p} \frac{\bar{\mathbf{a}}^p!}{\sigma!} \lambda^p \lambda^\sigma \quad (\text{by 4.3}) \\ &= \sum_{p=0}^{\bar{\mathbf{a}}(i)} \binom{\bar{\mathbf{a}}(i)}{p} \lambda^p Y_{\mathbb{K}}^{\bar{\mathbf{a}}^p} \quad (\text{Proposition 2.7}) \end{aligned}$$

which is as desired. The proof for the left action runs along similar lines. □

CONTINUOUS OPERATORS.

Throughout this section we will assume that \mathbb{K} is *polynomially faithful*.

Given $\partial \in \text{End}_{\mathbb{K}}(\text{Pol } \mathcal{F}(\mathbb{K}))$ and $\mathbf{s} \in W$ define a family of scalars $\partial_{\mathbf{w}}^{\mathbf{s}}$ by writing

$$\partial Y_{\mathbb{K}}^{\mathbf{s}} = \sum_{\mathbf{w} \in W} \partial_{\mathbf{w}}^{\mathbf{s}} Y_{\mathbb{K}}^{\mathbf{w}}, \quad \partial_{\mathbf{w}}^{\mathbf{s}} \in \mathbb{K}.$$

in the way prescribed by Theorem 2.10

Lemma 5.1. For $\partial \in \text{End}_{\mathbb{K}}(\text{Pol } \mathcal{F}(\mathbb{K}))$ the following two conditions are equivalent

PC1 For every summable S the following two conditions hold:

- (i) For $\mathbf{w} \in W$ the set $\{\mathbf{s} \in S : \partial_{\mathbf{w}}^{\mathbf{s}} \neq 0\}$ is finite
- (ii) For every $\mathbf{w} \in W$ the set $\{\mathbf{u} \in W_{\mathbf{w}} : \exists \mathbf{s} \in S : \partial_{\mathbf{u}}^{\mathbf{s}} \neq 0\}$ is finite. In other words, the set $\{\mathbf{w} \in W : \exists \mathbf{s} \in S : \partial_{\mathbf{w}}^{\mathbf{s}} \neq 0\}$ is summable.

PC2 For all $\mathbf{w} \in W$ there exists $\mathbf{r} \in W$ such that

$$\forall \mathbf{u} \in W_{\mathbf{w}} \quad \text{and} \quad \forall \mathbf{s} \in W \quad \partial_{\mathbf{u}}^{\mathbf{s}} \neq 0 \quad \Rightarrow \quad \mathbf{s} \in W_{\mathbf{r}}.$$

Proof. Suppose **PC2** holds for ∂ . Let S be summable and let $\mathbf{w} \in W$. Choose $\mathbf{r} \in W$ as in **PC2**. Then $\{\mathbf{s} : \partial_{\mathbf{w}}^{\mathbf{s}} \neq 0\} \cap S = \{\mathbf{s} : \partial_{\mathbf{w}}^{\mathbf{s}} \neq 0\} \cap S_{\mathbf{r}}$. Since $S_{\mathbf{r}}$ is finite for every \mathbf{r} **PC1(i)** holds.

As for **PC1(ii)** we have

$$\{\mathbf{u} \in W_{\mathbf{w}} : \exists \mathbf{s} \in S : \partial_{\mathbf{u}}^{\mathbf{s}} \neq 0\} = \{\mathbf{u} \in W_{\mathbf{w}} : \exists \mathbf{s} \in S_{\mathbf{r}} : \partial_{\mathbf{u}}^{\mathbf{s}} \neq 0\} = \bigcup_{\mathbf{s} \in S_{\mathbf{r}}} \{\mathbf{u} \in W_{\mathbf{w}} : \partial_{\mathbf{u}}^{\mathbf{s}} \neq 0\}.$$

Since $\text{supp } \partial(Y_{\mathbb{K}}^{\mathbf{s}}) := \{\mathbf{u} \in W : \partial_{\mathbf{u}}^{\mathbf{s}} \neq 0\}$ is summable, it follows that $\bigcup_{\mathbf{s} \in S_{\mathbf{r}}} \{\mathbf{u} \in W_{\mathbf{w}} : \partial_{\mathbf{u}}^{\mathbf{s}} \neq 0\}$ is a finite union of finite sets, hence finite. The set of **PC1(ii)** is thus summable.

Assume next that **PC1** holds. Fix $\mathbf{w} \in W$, and consider the set

$$\{(\mathbf{u}, \mathbf{s}) \in W_{\mathbf{w}} \times W : \partial_{\mathbf{u}}^{\mathbf{s}} \neq 0\} = \bigcup_{\mathbf{v} \in \overline{W}} P_{\mathbf{v}},$$

where

$$P_{\mathbf{v}} := \{(\mathbf{u}, \mathbf{s}) : \mathbf{u} \in W_{\mathbf{w}}, \bar{\mathbf{s}} = \mathbf{v}, \partial_{\mathbf{u}}^{\mathbf{s}} \neq 0\}.$$

Let $Q_{\mathbf{v}} := \{\mathbf{u} : \exists \mathbf{s} : (\mathbf{u}, \mathbf{s}) \in P_{\mathbf{v}}\}$. Note that the set $R := \{\mathbf{v} \in \overline{W} : Q_{\mathbf{v}} \text{ is infinite}\}$ is finite, for otherwise we can construct a summable set violating **PC1(ii)** as follows: Let $\{\mathbf{v}_{(n)}\}$ be an infinite sequence of distinct elements of R . Construct the sequences $\{\mathbf{s}_{(k)}\}$ and $\{\mathbf{u}_{(k)}\}$ inductively as follows: since $Q_{\mathbf{v}_{(n)}}$ is infinite, there exist $\mathbf{u}_{(n)} \in Q_{\mathbf{v}_{(n)}} \setminus \{\mathbf{u}_{(k)}\}_{k < n}$ and $\mathbf{s}_{(n)}$ such that $(\mathbf{u}_{(n)}, \mathbf{s}_{(n)}) \in P_{\mathbf{v}_{(n)}}$. The set $S = \{\mathbf{s}_{(n)}\}_{n \in \mathbb{N}}$ which is summable (since it contains at most one element for every reduced type) violates **PC1(ii)**.

The set $T := \{\mathbf{v} \in \overline{W} : Q_{\mathbf{v}} \text{ is finite and non empty}\}$ is also finite: For if $\{v(n)\}$ is an infinite sequence of distinct elements of T we can consider an infinite sequence of

pairs $(u_{(n)}, s_{(n)}) \in P_{v_{(n)}}$. If an infinite number of different $u_{(n)}$'s appear in these pairs then **PC1(ii)** fails, while if the different $u_{(n)}$'s are finite in number then a subsequence of the $s_{(n)}$'s violates **PC1(i)**.

Note that **PC1(i)** implies that

$$\forall \mathbf{u} \quad \exists \mathbf{q}(\mathbf{u}) \in W \quad \text{such that} \quad \partial_{\mathbf{u}}^{\mathbf{s}} \neq 0 \quad \Rightarrow \quad \mathbf{s} \in W_{\mathbf{q}(\mathbf{u})}.$$

Construct \mathbf{r} in such a way that $W_{\mathbf{r}}$ contains $W_{\mathbf{q}(\mathbf{u})}$ for all $\mathbf{u} \in T$ and contains $W_{\mathbf{u}}$ for all $\mathbf{u} \in R$. We claim that **PC2** holds. Indeed, if $\partial_{\mathbf{u}}^{\mathbf{s}} \neq 0$ then either $\bar{\mathbf{s}} \in R$, in which case $\mathbf{s} \in W_{\bar{\mathbf{s}}} \subset W_{\mathbf{r}}$, or $\bar{\mathbf{s}} \in T$, in which case $\mathbf{s} \in W_{\mathbf{q}(\mathbf{u})} \subset W_{\mathbf{r}}$. The proof of the Lemma is now complete..

5.2 The functions described in this last Lemma will be referred to as *precontinuous*. ∂ as above will be said to be *algebraically continuous* if it is precontinuous and in addition satisfies the following property

AC For every summable set S and family $c_{\mathbf{s}} \in \mathbb{K}$ we have

$$\partial \left(\sum_{\mathbf{s} \in S} c_{\mathbf{s}} Y_{\mathbb{K}}^{\mathbf{s}} \right) = \sum_{\mathbf{w} \in W} \left(\sum_{\mathbf{s} \in S} c_{\mathbf{s}} \partial_{\mathbf{w}}^{\mathbf{s}} \right) Y_{\mathbb{K}}^{\mathbf{w}}.$$

Remark 5.3 By abuse of notation we will interpret continuity as the following equality:

$$\partial \left(\sum_{\mathbf{s} \in W} c_{\mathbf{s}} Y_{\mathbb{K}}^{\mathbf{s}} \right) = \sum_{\mathbf{s} \in W} c_{\mathbf{s}} \partial \left(Y_{\mathbb{K}}^{\mathbf{s}} \right)$$

Lemma 5.4. For $\mathbf{r} \in W$ and $f \in \text{Pol } \mathcal{F}(\mathbb{K})$ the following conditions are equivalent

- (i) f vanishes in $\mathcal{F}(\mathbb{K})^{\mathbf{r}}$
- (ii) $f \circ \pi_{\mathbf{r}} = 0$
- (iii) If $f = \sum c_{\mathbf{a}} Y_{\mathbb{K}}^{\mathbf{a}}$ then $c_{\mathbf{a}} = 0$ whenever $\mathbf{a} \in W_{\mathbf{r}}$.

Proof. (i) \Rightarrow (ii) is obvious.

(ii) \Rightarrow (iii) In Proposition 2.7 (with \mathbf{s} replaced by \mathbf{r}) note that regardless of \mathbf{a} different σ 's produce different monomials T^{σ} 's. If we now write f as in Theorem 2.10 and take the argument of Corollary 2.8 into account we see that $f \circ \pi_{\mathbf{r}}$ is a nonzero polynomial in $\mathbb{K}[r]$ whenever $\text{supp} f \cap W_{\mathbf{r}} \neq \emptyset$. Our assumption that \mathbb{K} be polynomially faithful shows then that (ii) fails whenever (iii) does.

(iii) \Rightarrow (i) See Corollary 2.8. □

5.5 The set of functions described in this last Lemma will be denoted by $U_{\mathbf{r}}$. Note that $U_{\mathbf{r}} = U_{\overline{\mathbf{r}}}$ and $U_{\mathbf{rs}} \subset U_{\mathbf{r}} \cap U_{\mathbf{s}}$. It follows that the sets $f + U_{\mathbf{r}}$ form a neighborhood base of $f \in \text{Pol } \mathcal{F}(\mathbb{K})$ of a (linear) topology on $\text{Pol } \mathcal{F}(\mathbb{K})$. For this topology continuity of an endomorphism $\partial \in \text{End}_{\mathbb{K}}(\text{Pol } \mathcal{F}(\mathbb{K}))$ is equivalent to

TC For all $w \in W$ there exists $\mathbf{r} \in W$ such that $\partial(U_{\mathbf{r}}) \subset U_{\mathbf{w}}$.

These maps will be called *topologically continuous*.

Proposition 5.6. *Let $\partial \in \text{End}_{\mathbb{K}}(\text{Pol } \mathcal{F}(\mathbb{K}))$.*

- (i) *If ∂ is algebraically continuous it is topologically continuous.*
- (ii) *If ∂ is topologically continuous it is precontinuous.*

Proof.

- (i) Let $\partial \in \text{End}_{\mathbb{K}}(\text{Pol } \mathcal{F}(\mathbb{K}))$ be algebraically continuous. Given $\mathbf{w} \in W$ choose \mathbf{r} as in **PC2**. Taking Lemma 5.4 into account we see that for $\mathbf{s} \in W$ $\partial Y_{\mathbb{K}}^{\mathbf{s}} \notin U_{\mathbf{w}} \Rightarrow \exists \mathbf{u} \in W_{\mathbf{w}}: \partial_{\mathbf{u}}^{\mathbf{s}} \neq 0 \Rightarrow \mathbf{s} \in W_{\mathbf{r}} \Rightarrow Y_{\mathbb{K}}^{\mathbf{s}} \notin U_{\mathbf{r}}$. Thus $Y_{\mathbb{K}}^{\mathbf{s}} \in U_{\mathbf{r}} \Rightarrow \partial Y_{\mathbb{K}}^{\mathbf{s}} \in U_{\mathbf{w}}$. That **TC** holds now follows from **AC**.
- (ii) Let $\partial \in \text{End}_{\mathbb{K}}(\text{Pol } \mathcal{F}(\mathbb{K}))$ be topologically continuous and given $\mathbf{w} \in W$ choose \mathbf{r} as in **TC**. Let $\mathbf{u} \in W_{\mathbf{w}}$ and $\mathbf{s} \in W$ then

$$\begin{aligned} \partial_{\mathbf{u}}^{\mathbf{s}} \neq 0 &\Rightarrow \partial Y_{\mathbb{K}}^{\mathbf{s}} \notin U_{\mathbf{u}} \\ &\Rightarrow \partial Y_{\mathbb{K}}^{\mathbf{s}} \notin U_{\mathbf{w}} \text{ (see 5.4 (iii))} \\ &\Rightarrow Y_{\mathbb{K}}^{\mathbf{s}} \notin U_{\mathbf{r}} \text{ (by TC)} \\ &\Rightarrow \mathbf{s} \in W_{\mathbf{r}} \text{ (Corollary 2.8)} \end{aligned}$$

□

Corollary 5.7.. *The composition $\partial_1 \partial_2$ of two algebraically continuous endomorphisms $\partial_1, \partial_2 \in \text{End}_{\mathbb{K}} \text{Pol } \mathcal{F}(\mathbb{K})$ is algebraically continuous.*

Proof. The Proposition shows that $\partial_1 \partial_2$ is precontinuous. That **AC** holds follows easily from the assumption that **AC** holds for both ∂_1 and ∂_2 .

Remark 5.8. Let $Y(\mathbb{K}) := \sum_{\mathbf{w} \in W} \mathbb{K}Y_{\mathbb{K}}^{\mathbf{w}} \subset \text{Pol } \mathcal{F}(\mathbb{K})$. This is a dense subset of $\text{Pol } \mathcal{F}(\mathbb{K})$. For \mathbb{K} -linear maps from $Y(\mathbb{K})$ into $\text{Pol } \mathcal{F}(\mathbb{K})$ condition **AC** trivially holds: algebraic continuity and precontinuity are thus equivalent in this case.

Proposition 5.9. *Left and right multiplication by elements of the group (see section 4) are algebraically continuous endomorphisms of $\text{Pol}(\mathbb{K}^N)$.*

Proof. We leave this as a (non entirely trivial) exercise.

Proposition 5.10. *Let $\partial \in \text{Hom}_{\mathbb{K}}(Y(\mathbb{K}), \text{Pol } \mathcal{F}(\mathbb{K}))$ be precontinuous. Then*

(i) *There exists a unique algebraically continuous \mathbb{K} -linear endomorphism of $\text{Pol } \mathcal{F}(\mathbb{K})$ extending ∂ .*

(ii) *If ∂ is a derivation or right or left invariant then so is its extension.*

Proof. Taking Theorem 2.10 into account define $\partial \in \text{End}_{\mathbb{K}} \text{Pol } \mathcal{F}(\mathbb{K})$ by means of **AC**. The uniqueness is clear. That ∂ is a derivation follows from the description of the multiplication in $\text{Pol } \mathcal{F}(\mathbb{K})$ given in Theorem 3.7(iii). The invariance follows easily from the last Proposition. \square

As an easy consequence of (i) we get

Corollary 5.11. *If two algebraically continuous endomorphism of $\text{Pol } \mathcal{F}(\mathbb{K})$ coincide in $Y(\mathbb{K})$, they are equal.*

Remark 5.12. Let f, g , and h be as in the proof of Theorem 3.7(iii). We see that fg and h have the same image in each of the quotient rings $\text{Pol } \mathcal{F}(\mathbb{K})/U_{\mathbf{r}}$. That 3.7(iii) holds follows from $\bigcap_{\mathbf{r} \in W} U_{\mathbf{r}} = (0)$.

RIGHT INVARIANT DERIVATIONS AND FREE LIE ALGEBRAS.

Throughout this section we will assume that \mathbb{K} is *polynomially faithful*. Algebraically continuous functions we will simply refer to as *continuous*. Starting with 6.8 we also assume that \mathbb{K} is *torsion free*.

We give the free \mathbb{K} -module $Y(\mathbb{K})$ a \mathbb{Z}^I grading by declaring $Y_{\mathbb{K}}^{\mathbf{w}}$ to be homogeneous of degree $\text{deg}_{\mathbf{w}}$ (See 1.5.) The shuffle product is compatible with this grading

making $Y_{\mathbb{K}}$ into a \mathbb{Z}^I -graded algebra thereof. This grading extends to $\text{Pol } \mathcal{F}(\mathbb{K})$: Every element of $\text{Pol } \mathcal{F}(\mathbb{K})$ is a sum over a summable set of homogeneous elements (see Theorem 2.10.)

Given $\partial \in \text{End}_{\mathbb{K}}(\text{Pol } \mathcal{F}(\mathbb{K}))$ and $\omega \in \mathbb{Z}^I$ define $\partial_{\omega} \in \text{Hom}_{\mathbb{K}}(Y(\mathbb{K}), \text{Pol } \mathcal{F}(\mathbb{K}))$ by

$$\partial_{\omega}(Y_{\mathbb{K}}^{\mathbf{s}}) = \sum_{\substack{\mathbf{w} \\ \deg(\mathbf{w}) = \deg(\mathbf{s}) + \omega}} \partial_{\mathbf{w}}^{\mathbf{s}} Y_{\mathbb{K}}^{\mathbf{w}}. \quad (6.1)$$

Note that this sum is always finite so that ∂_{ω} is always precontinuous. It follows (see Proposition 5.9) that ∂_{ω} extends uniquely to an element, also denoted ∂_{ω} of $\text{End}_{\mathbb{K}}(\text{Pol } \mathcal{F}(\mathbb{K}))$. Note also that $\partial_{\omega} = 0$ unless $\text{supp } \omega := \{i \in I : \omega(i) \neq 0\}$ is finite.

Lemma 6.2. *Let $\partial \in \text{End}_{\mathbb{K}}(\text{Pol } \mathcal{F}(\mathbb{K}))$ be continuous. Let $\omega \in \mathbb{Z}^I$. Then*

- (i) *If ∂ is right-invariant then ∂_{ω} is right-invariant.*
- (ii) *If ∂ is a derivation then ∂_{ω} is a derivation.*

Proof.

(i) Let $i \in I$, $\lambda \in \mathbb{K}$ and $\mathbf{w} \in W$. By Proposition 4.1 and the fact that both ∂ and R_h are continuous we have for $h = E_i(\lambda)$,

$$\begin{aligned} R_h \partial(Y_{\mathbb{K}}^{\mathbf{s}}) &= \sum_{\mathbf{w} \in W} \partial_{\mathbf{w}}^{\mathbf{s}} \sum_{p=0}^{\overleftarrow{\mathbf{w}}(i)} \lambda^p \binom{\overleftarrow{\mathbf{w}}(i)}{p} Y_{\mathbb{K}}^{\overleftarrow{\mathbf{w}}^p} \\ \partial(R_h Y_{\mathbb{K}}^{\mathbf{s}}) &= \sum_{p=0}^{\overleftarrow{\mathbf{s}}(i)} \lambda^p \binom{\overleftarrow{\mathbf{s}}(i)}{p} \partial(Y_{\mathbb{K}}^{\overleftarrow{\mathbf{s}}^p}). \end{aligned}$$

Our assumption on \mathbb{K} (look at the above as polynomials in one variable evaluated at λ) together with the right-invariance of ∂ yields the system of equalities

$$\binom{\overleftarrow{\mathbf{s}}(i)}{p} \partial(Y_{\mathbb{K}}^{\overleftarrow{\mathbf{s}}^p}) = \sum_{\mathbf{w} \in W} \partial_{\mathbf{w}}^{\mathbf{s}} \binom{\overleftarrow{\mathbf{w}}(i)}{p} Y_{\mathbb{K}}^{\overleftarrow{\mathbf{w}}^p}$$

for all $p \geq 0$. Equating now the terms of degree $\deg(\overleftarrow{\mathbf{s}}^p) + \omega$ we obtain, taking Theorem 2.10 into account, that

$$\binom{\overleftarrow{\mathbf{s}}(i)}{p} \partial_{\omega}(Y_{\mathbb{K}}^{\overleftarrow{\mathbf{s}}^p}) = \sum_{\substack{\mathbf{w} \in W \\ \deg(\mathbf{w}) = \deg(\mathbf{s}) + \omega}} \partial_{\mathbf{w}}^{\mathbf{s}} \binom{\overleftarrow{\mathbf{w}}(i)}{p} Y_{\mathbb{K}}^{\overleftarrow{\mathbf{w}}^p},$$

which is equivalent to the right-invariance of ∂_ω .

(ii) Let $\mathbf{u}, \mathbf{v} \in S$. Equating the terms of degree $\deg(\mathbf{u}) + \deg(\mathbf{v}) + \omega$ on the left and on the right of $\partial(Y_{\mathbb{K}}^{\mathbf{u}} Y_{\mathbb{K}}^{\mathbf{v}}) = \partial(Y_{\mathbb{K}}^{\mathbf{u}}) Y_{\mathbb{K}}^{\mathbf{v}} + Y_{\mathbb{K}}^{\mathbf{u}} \partial(Y_{\mathbb{K}}^{\mathbf{v}})$ yields $\partial_\omega(Y_{\mathbb{K}}^{\mathbf{u}} Y_{\mathbb{K}}^{\mathbf{v}}) = \partial_\omega(Y_{\mathbb{K}}^{\mathbf{u}}) Y_{\mathbb{K}}^{\mathbf{v}} + Y_{\mathbb{K}}^{\mathbf{u}} \partial_\omega(Y_{\mathbb{K}}^{\mathbf{v}})$. That ∂_ω is a derivation now follows from Proposition 5.10.

Proposition 6.3. *Let $\partial \in \text{End}_{\mathbb{K}}(\text{Pol } \mathcal{F}(\mathbb{K}))$ be continuous and right-invariant. If $\partial_\omega \neq 0$ then $\omega \in \mathbb{Z}_-^I := \{\omega \in \mathbb{Z}^I : \omega(i) \leq 0 \text{ for all } i \in I\}$*

Proof. Suppose $\omega \notin \mathbb{Z}_-^I$. Let us prove that $\partial_\omega(Y_{\mathbb{K}}^{\mathbf{s}}) = 0$ by induction on s . The proof is based on the observation that the only polynomial functions invariant (left or right) under the group action are the constant functions. If $s = 0$ then $Y_{\mathbb{K}}^{\mathbf{s}} = 1$ is a constant function and $R_h \partial_\omega(1) = \partial_\omega R_h(1) = \partial_\omega(1)$. Thus $\partial_\omega(1)$ is a constant function which is zero since $\omega \neq 0$. Assume now that $\partial_\omega(Y_{\mathbb{K}}^{\mathbf{w}}) = 0$ for all \mathbf{w} with $w < s$. For $h \in \mathcal{F}(\mathbb{K})$ we have by Proposition 4.1 that

$$\begin{aligned} R_h(\partial_\omega Y_{\mathbb{K}}^{\mathbf{s}}) &= \partial_\omega(R_h Y_{\mathbb{K}}^{\mathbf{s}}) \\ &= \partial_\omega(Y_{\mathbb{K}}^{\mathbf{s}}) + \sum_{w < s} c_{\mathbf{w}} \partial_\omega(Y_{\mathbb{K}}^{\mathbf{w}}) = \partial_\omega(Y_{\mathbb{K}}^{\mathbf{s}}). \end{aligned}$$

It follows that $\partial_\omega Y_{\mathbb{K}}^{\mathbf{s}}$ is a constant function. But $\deg(\partial_\omega Y_{\mathbb{K}}^{\mathbf{s}}) = \omega + \deg_{\mathbf{s}} \neq 0$. Hence $\partial_\omega Y_{\mathbb{K}}^{\mathbf{s}} = 0$ and since ∂_ω is continuous $\partial_\omega = 0$. \square

Given $i \in I$ define $\partial_i \in \text{End}_{\mathbb{K}} Y(\mathbb{K})$ as follows: For $\mathbf{s} = \bar{\mathbf{s}}_1^{n_1} \dots \bar{\mathbf{s}}_s^{n_s}$

$$\partial_i(Y_{\mathbb{K}}^{\mathbf{s}}) = \vec{\mathbf{s}}(i) Y_{\mathbb{K}}^{\bar{\mathbf{s}}_1^{n_1} \dots \bar{\mathbf{s}}_s^{n_s}}. \quad (6.4)$$

Note that if \mathbb{K} is a \mathbb{Q} -algebra we have

$$\partial_i(X_{\mathbb{Q}}^{\mathbf{s}}) = \begin{cases} X_{\mathbb{Q}}^{\bar{\mathbf{s}}_1^{n_1}}, & \text{if } i = s_1 \\ 0, & \text{if } i \neq s_1. \end{cases} \quad (6.5)$$

∂_i is clearly precontinuous and its unique continuous extension to $\text{End}_{\mathbb{K}}(\text{Pol } \mathcal{F}(\mathbb{K}))$ will also be denoted by ∂_i .

Proposition 6.6. *$\partial_i \in \text{End}_{\mathbb{K}}(\text{Pol } \mathcal{F}(\mathbb{K}))$ is a continuous homogeneous right-invariant derivation of degree $-\deg_i$,*

Proof. We have just seen that ∂_i is continuous. That ∂_i is homogeneous of degree $-deg_i$ is clear. By Proposition 5.10 to show that ∂_i is right invariant it suffices to show that ∂_i is right invariant when viewed as an element of $End_{\mathbb{K}}Y(\mathbb{K})$, for which in turn it suffices to show that

$$R_h \partial_i(Y_{\mathbb{K}}^{\mathbf{s}}) = \partial_i(R_h Y_{\mathbb{K}}^{\mathbf{s}}), \text{ for all } j \in I, \lambda \in \mathbb{K}, h = E_j(\lambda), \text{ and } \mathbf{s} \in W.$$

By taking Proposition 4.1 into account it is easy to see that this holds if $\bar{s} > 1$. If $\bar{s} = 1$ then the only non trivial case is when $i = j$ and $\mathbf{s} = i^n$. We then have

$$\begin{aligned} R_h \partial_i(Y_{\mathbb{K}}^{\mathbf{s}}) &= n R_h Y_{\mathbb{K}}^{\bar{s}^1} = \sum_{p=0}^{n-1} n \binom{n-1}{p} \lambda^p Y_{\mathbb{K}}^{\bar{s}^{p+1}} \\ &= \sum_{p=0}^{n-1} \frac{n!}{p!(n-p-1)!} \lambda^p Y_{\mathbb{K}}^{\bar{s}^{p+1}} \\ &= \sum_{p=0}^n \binom{n}{p} (n-p) \lambda^p Y_{\mathbb{K}}^{\bar{s}^{p+1}} \\ &= \partial_i \left(\sum_{p=0}^n \binom{n}{p} \lambda^p Y_{\mathbb{K}}^{\bar{s}^p} \right) \\ &= \partial_i(R_h Y_{\mathbb{K}}^{\mathbf{s}}). \end{aligned}$$

Finally, let us prove that ∂_i is a derivation of $Pol \mathcal{F}(\mathbb{K})$. Again it suffices to show that ∂_i is right invariant as an element of $End_{\mathbb{K}}Y(\mathbb{K})$. Since $Y(\mathbb{K}) \cong \mathbb{K} \otimes_{\mathbb{Z}} Y(\mathbb{Z})$ it will suffice to establish the result in the case $\mathbb{K} = \mathbb{Z}$. That this last is the case follows from the commutativity of the diagram in Remark 3.8 commutes, together with the fact that ∂_i is a derivation of $X(\mathbb{Z})$ ([Rtn] 1.4.3.) \square

In what follows \mathcal{D} will denote the associative \mathbb{K} -subalgebra of $End_{\mathbb{K}}(Pol \mathcal{F}(\mathbb{K}))$ generated by the ∂_i 's. If $\mathbf{s} = \mathbf{s}_1 \cdots \mathbf{s}_s \in W$ we set $\partial^{\mathbf{s}} := \partial_{\mathbf{s}_s} \cdots \partial_{\mathbf{s}_1}$. By convention $\partial^{\mathbf{1}} = Id$. The Lie subalgebra of $Der Pol \mathcal{F}(\mathbb{K})$ generated by the ∂_i 's will be denoted by L .

Proposition 6.7. *All elements of \mathcal{D} are continuous and right invariant.*

Proof. Apply Corollary 5.7 and Proposition 6.6. \square

Proposition 6.8. *If \mathbb{K} is torsion free then \mathcal{D} is a free associative algebra. Furthermore the natural \mathbb{Z}^I grading of \mathcal{D} is compatible with that of $Y(\mathbb{K})$.*

Proof. We need to show that the $\partial^{\mathbf{s}}$'s are linearly independent over \mathbb{K} . The constant term of $(\sum_{\mathbf{s} \in W} c_{\mathbf{s}} \partial^{\mathbf{s}}) Y_{\mathbb{K}}^{\mathbf{w}}$ is $c_{\mathbf{w}} \mathbf{w}! \cdot 1$, hence $\sum_{\mathbf{s} \in W} c_{\mathbf{s}} \partial^{\mathbf{s}} = 0$ implies $c_{\mathbf{s}} = 0$ for all $\mathbf{s} \in W$. We assigned $\partial^{\mathbf{s}} = \partial_{s_1} \dots \partial_{s_r}$ degree $-\deg_{\mathbf{s}}$. The compatibility is clear.

Corollary 6.9. *If \mathbb{K} is torsion free L is a free Lie algebra, freely generated by the ∂_i 's.*

Remark 6.10. When \mathbb{K} has torsion L is not free.

Remark 6.11 In Proposition 6.7 and its Corollary $\text{Pol } \mathcal{F}(\mathbb{K})$ may be replaced by $Y(\mathbb{K})$.

For the remainder of the paper we will assume \mathbb{K} is torsion free. The algebra \mathcal{D} , being free associative, affords a unique coproduct $\Delta : \mathcal{D} \rightarrow \mathcal{D} \otimes \mathcal{D}$ satisfying

$$\Delta(\partial_i) = \partial_i \otimes 1 + 1 \otimes \partial_i.$$

Denote by $\mu : \text{Pol } \mathcal{F}(\mathbb{K}) \otimes \text{Pol } \mathcal{F}(\mathbb{K}) \rightarrow \text{Pol } \mathcal{F}(\mathbb{K})$ the multiplication in $\text{Pol } \mathcal{F}(\mathbb{K})$.

Lemma 6.12. *Let $\partial \in \mathcal{D}$, and $f, g \in \text{Pol } \mathcal{F}(\mathbb{K})$. Then*

$$\mu(\Delta(\partial)(f \otimes g)) = \partial(\mu(f \otimes g)).$$

Proof. It is sufficient to prove the Lemma for $\partial = \partial^{\mathbf{w}}$, $\mathbf{w} \in W$. This we shall do by induction in $w > 0$ (The case $w = 0$ being clear: $\partial^0 = Id$.)

If $w = 1$ then $\partial = \partial_i$ and we have

$$\begin{aligned} \mu(\Delta(\partial_i)(f \otimes g)) &= \mu[(\partial_i \otimes 1 + 1 \otimes \partial_i)(f \otimes g)] \\ &= \mu(\partial_i f \otimes g + f \otimes \partial_i g) = (\partial_i f)g + f(\partial_i g) = \partial_i(fg) = \partial_i(\mu(f \otimes g)). \end{aligned}$$

For the inductive step, let $\partial^{\mathbf{w}} = \partial^{\mathbf{v}} \partial_i$ and assume the Lemma holds for $\partial^{\mathbf{v}}$. Then

$$\begin{aligned} \mu(\Delta(\partial^{\mathbf{v}} \partial_i)(f \otimes g)) &= \mu[(\Delta(\partial^{\mathbf{v}}) \Delta(\partial_i))(f \otimes g)] \\ &= \mu(\Delta(\partial^{\mathbf{v}})(\Delta(\partial_i))(f \otimes g)) = \mu[\Delta(\partial^{\mathbf{v}})(\partial_i f \otimes g + f \otimes \partial_i g)] \\ &= \partial^{\mathbf{v}}((\partial_i f)g + f(\partial_i g)) = \partial^{\mathbf{v}}(\partial_i(fg)) = \partial^{\mathbf{v}} \partial_i \mu(f \otimes g). \end{aligned}$$

Proposition 6.13. *Let $\partial \in \mathcal{D}$. Then $\partial \in \text{Der}_{\mathbb{K}}Y(\mathbb{K})$ if and only if $\partial \in L$.*

Proof. Make \mathcal{D} (respectively $Y(\mathbb{K})$) into a \mathbb{Z} -graded algebra by declaring the ∂_i 's (respectively $Y_{\mathbb{K}}^{\mathbf{a}}$) to be of degree -1 (respectively \mathbf{a} .) These gradings are compatible so that we may assume without loss of generality that ∂ is homogeneous of degree $-N$. Then

$$\Delta(\partial) = \partial \otimes 1 + 1 \otimes \partial + \sum_{\substack{\mathbf{a}, \mathbf{b} \\ a < N, b < N \\ a + b = N}} c_{\mathbf{ab}} \partial^{\mathbf{a}} \otimes \partial^{\mathbf{b}}.$$

Thus if $a + b = N, a < N, b < N$ we have

$$\Delta(\partial)(Y^{\mathbf{a}} \otimes Y^{\mathbf{b}}) = \mathbf{a}! \mathbf{b}! c_{\mathbf{ab}} 1 \otimes 1$$

and hence

$$\mu(\Delta(\partial)((Y^{\mathbf{a}} \otimes Y^{\mathbf{b}}))) = \mathbf{a}! \mathbf{b}! c_{\mathbf{ab}} 1.$$

By the last Lemma

$$\begin{aligned} \mu(\Delta(\partial)((Y^{\mathbf{a}} \otimes Y^{\mathbf{b}}))) &= \partial(X^{\mathbf{a}} X^{\mathbf{b}}) \\ &= \partial(Y^{\mathbf{a}}) Y^{\mathbf{b}} + Y^{\mathbf{a}} \partial(Y^{\mathbf{b}}) = 0, \end{aligned}$$

Thus $c_{\mathbf{ab}} = 0$ and $\Delta(\partial) = \partial \otimes 1 + 1 \otimes \partial$. By Friedrichs' Theorem ([Rtn] Corollary 4.17 or [Bbk]Ch.2 §3.1) we conclude that $\partial \in L$.

Proposition 6.14. *Let $\partial \in \text{End}_{\mathbb{K}}(\text{Pol } \mathcal{F}(\mathbb{K}))$ be continuous and right invariant. If $\omega \in \mathbb{Z}_-^I$, then ∂_{ω} is a linear combination of the $\partial^{\mathbf{s}}$ with $\text{deg}_{\mathbf{s}} = -\omega$.*

Proof. Let $\partial_{\omega}(Y^{\mathbf{s}}) = c_{\mathbf{s}} \cdot 1$ for $\mathbf{s} \in W$ with $\text{deg}_{\mathbf{s}} = -\omega$. An argument similar in spirit to that of Proposition 6.3 shows that $\partial_{\omega} - \sum_{\substack{\mathbf{s} \in W \\ \text{deg}_{\mathbf{s}} = -\omega}} c_{\mathbf{s}} \partial^{\mathbf{s}} = 0$. □

Consider the following completions of the free associative algebra \mathcal{D} generated by operators ∂_i :

$$\overline{\mathcal{D}} = \prod_{\mathbf{w} \in W} \mathbb{K} \partial^{\mathbf{w}}$$

and

$$\overline{\mathcal{D}}_0 = \bigoplus_{r \in \overline{W}} \prod_{\substack{\mathbf{w} \in W \\ \overline{\mathbf{w}} = r}} \mathbb{K} \partial^{\mathbf{w}}.$$

Note that $\overline{\mathcal{D}}$ acts on the space $Y(\mathbb{K}) = \bigoplus_{\mathbf{w} \in W} \mathbb{K} Y^{\mathbf{w}}$. If $\partial = \sum_{\mathbf{u} \in W} d_{\mathbf{u}} \partial^{\mathbf{u}}$ then

$$\partial(Y^{\mathbf{s}}) = \sum_{\substack{\mathbf{u}, \mathbf{w} \\ \mathbf{s} = \mathbf{u}\mathbf{w}}} d_{\mathbf{u}} c_{\mathbf{s}, \mathbf{u}} Y^{\mathbf{w}} \quad (6.15)$$

for some coefficients $\{c_{\mathbf{s}, \mathbf{u}}\}$ all but a finite number of which are not zero.

Proposition 6.16. *An endomorphism $\partial \in \overline{\mathcal{D}}$ can be extended to a continuous endomorphism of $\text{Pol } \mathcal{F}(\mathbb{K})$ if and only if $\partial \in \overline{\mathcal{D}}_0$.*

Proof. We maintain the notation of 6.15. If $\partial \in \overline{\mathcal{D}}_0$ then the set $T = \{\mathbf{t} \in \overline{W} \mid \exists \mathbf{v} \in W : \overline{\mathbf{v}} = \mathbf{t} \text{ and } d_{\mathbf{v}} \neq 0\}$ is finite. If we set $\mathbf{r} = \mathbf{t}\mathbf{w}$, where \mathbf{t} is the product in any order of the elements of T then with the aid of 6.16 one shows that PC2 holds. Thus ∂ is precontinuous and hence has a continuous extension (Proposition 5.10.)

Conversely if $\partial \notin \overline{\mathcal{D}}_0$ then the set T above is infinite and we can construct an infinite set $S \subset W$ such that S contains at most one word of every reduced type and for every $s \in S$ $d_s \neq 0$ and $\overline{s} \in T$. Then the set S is summable and since $\partial_1^s = d_s c_{s, s} = d_s s! \neq 0$ we see that PC1 (i) fails. \square

Let \overline{L} be the algebra of Lie series of L (See [Rtn] Ch. 3) Define $\overline{L}_0 = \overline{L} \cap \overline{\mathcal{D}}_0$.

Theorem 6.17. *Let \mathbb{K} be a ring which is torsion free and polinomially faithful. Then there exists a natural isomorphism between \overline{L}_0 and the Lie algebra of all continuous right-invariant derivations of $\text{Pol } \mathcal{F}(\mathbb{K})$.*

Proof. Let $\partial \in \text{End}_{\mathbb{K}}(\text{Pol } \mathcal{F}(\mathbb{K}))$ be a continuous right invariant derivation. By Propositions 6.2, 6.3, and 6.14 we can identify ∂ with $\sum_{\omega \in \mathbb{Z}_-^I} \partial_{\omega} \in \overline{L}$. Now Proposition 6.13 shows that $\partial \in \overline{L}$. Since ∂ is continuous the last Proposition shows that $\partial \in \overline{\mathcal{D}}_0$.

Conversely if $\partial \in \overline{L}_0$ then we can think of ∂ as a continuous element of $\text{End}_{\mathbb{K}}(\text{Pol } \mathcal{F}(\mathbb{K}))$ (again by the last Proposition.) When we restrict ∂ to $Y(\mathbb{K})$ we obtain a right invariant derivation (Propositions 6.7 and 6.13.) The unique continuous extension $\overline{\partial}$ of ∂ to $\text{End}_{\mathbb{K}}(\text{Pol } \mathcal{F}(\mathbb{K}))$ is then right invariant derivation (Proposition 5.10.) Since $\overline{\partial}$ is continuous $\partial = \overline{\partial}$ (Corollary 5.11). \square

REFERENCES.

- [BP] Y. Billig and A. Pianzola, *Free groups of Lie type*, Comp. Rend. Math. Acad. Sci. Canada, **18** No. 4 (1996) 159-162.
- [Chv] C. Chevalley, *Sur certains groupes simples*, Tôhoku Math. Jour. **7** (1955), 14-66.
- [PK] D. Peterson and V. Kac, *Infinite flag varieties and conjugacy theorems*, Proc. Ntl. Acad. Sci. USA **80** 1983, 1778-1782.
- [Ree] R. Ree, *Lie elements and the algebra associated with shuffles.*, Annals of Math, **68** 1958, 210-220.
- [Rtn] C. Reutenauer, *Free Lie algebras*, London Math. Soc. Monographs **7**, Clarendon Press, Oxford, 1993.