UMI

A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor MI 48106-1346 USA
313/761-4700 800/521-0600

University of Alberta

Lie theory for some quotients of the affine group represented by the Hopf Shuffle algebra

by

Jorge J. Valencia ©

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfilment of the requirements for the degree of Doctor of Philosophy

in

Mathematics.

Department of Mathematical Sciences

Edmonton, Alberta
Fall 1998

0-612-34850-4

University of Alberta

Release Form

Name of Author: Jorge J. Valencia

Title of Thesis: Lie theory for some quotients of the affine group represented by the Hopf Shuffle algebra

Degree: Doctor of Philosophy

Year this Degree Granted: 1998

(Signed) J. J. Valencia

Jorge J. Valencia
Department of Mathematical Sciences
University of Alberta
Edmonton, Alberta
T6G 2G1
Canada

Date: 2/10/98

Nadie puede escribir un libro. Para
Que un libro sea verdaderamente,
Se requieren la aurora y el poniente,
Siglos, armas y el mar que une y separa.

Jorge Luis Borges

University of Alberta

Faculty of Graduate Studies and Research

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies and Research for acceptance, a thesis entitled **Lie theory for some quotients of the affine group represented by the Hopf Shuffle algebra** submitted by Jorge J. Valencia in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Mathematics.

Bruce N. Allison

Dr. B. Allison (Chair)

Hans H. Brungs

Dr. H. Brungs

Dr. ~~H.~~ Hoover

Dr. J. Lewis

Dr. J. Morita,
University of Tsukuba, Ibaraki, Japan,

Dr. A. Pianzola (Supervisor)

Date: 30/9/98

Abstract

I develop a Lie theory for certain unipotent algebraic quotients of the affine group scheme G represented by the Hopf Shuffle algebra.

I prove that the Lie algebra of the Hopf Shuffle algebra is an algebra of Lie Series and that the Lie algebras of some unipotent algebraic quotients of G are quotients of the free Lie algebra.

I show that the affine group scheme of upper triangular unipotent matrices U_n, for all $n \in \mathbb{N}$, is a quotient of the affine group scheme represented by the Hopf shuffle algebra by injecting the representing algebra of U_n into the Hopf Shuffle algebra as a sub Hopf algebra.

As an application of the Lie theory that I constructed, I give a simple proof that the Hopf shuffle algebra is a free commutative algebra, a result first proved by Radford [Rad79] in a rather involved way using combinatorics.

To M. P. M.

Acknowledgements

With deep pleasure, I wish to express my gratitude to **Marion M. Benedict, Gerald H. Cliff, James D. Lewis and Sherdashar K. Sehgal.**

To **Marion Benedict** for all the work she put in and her willingness to help me in any way she could to make it possible that I reached my final defence.

To **Jim Lewis** for his encouragement and advice throughout the preparation of this thesis. Particularly appreciated was his immediate attention to any question I asked to him throughout the last 4 years and for the time he spent teaching me algebraic geometry and commutative algebra.

To **Gerald Cliff** and **Sudarshan Sehgal** for many discussions about my research work. Although they were not members of my examination committee they always had the time to listen to my mathematical questions and they were also willing to help me to finish my program.

Contents

Introduction

In chapter 1 I give the basic definitions of Hopf algebras and their morphisms taken from [Swe69]. Following Gerhard P. Hochschild [Hoc81], I attach a Hopf algebra over a field to every abstract group and I define algebraic groups and their Hopf algebras of polynomial maps.

I prove that every finitely generated Hopf algebra over an algebraic closed field with no non-zero nilpotents is isomorphic to the algebra of polynomial maps of some algebraic group. This motivates the concept of affine scheme to be used in the next chapter.

In chapter 2 I introduce the Hopf Shuffle algebra A [Ree58]. Let $G := \mathrm{Hom}_{F\text{-alg}}(A, -)$ be the affine group represented by A. I define some quotients G_N of G represented by some subalgebras A_N of A. I prove that the Lie algebra of G is an algebra of Lie series and that the Lie algebra of G_N is a quotient of the free Lie algebra on a finite alphabet I. I prove that the upper triangular unipotent group scheme is a quotient of G.

In chapter 3 I prove that the Hopf shuffle algebra A and its subalgebras A_N are coconnected which will show that their corresponding affine group schemes G and G_N are unipotent.

If the alphabet I is finite, G_N will be an algebraic unipotent affine group to which classical Lie theory will apply: I construct an exponential map and a logarithm map for the affine group G_N. I prove that these maps are polynomial maps inverse of each other.

Since Lie(G_N) is a vector space, it has the structure of a vector group. The exponential map will provide an isomorphism of algebraic sets between the vector group Lie(G_N) and the algebraic affine group $G_N(F)$ which will allow me to identify polynomial maps on $G_N(F)$ with polynomial maps on Lie(G_N). This will show that A_N is a polynomial ring. Finally, I will prove that the Hopf shuffle algebra A is a free commutative algebra, which was first proved by [Rad79]. My proof uses no combinatorics like his and it is based on the Lie theory that I developed for the quotients G_N of G.

Chapter 1

Hopf Algebras and algebraic groups

In this chapter we give the basic definitions of Hopf algebras and their morphisms. Following Gerhard P. Hochschild [Hoc81], we attach a Hopf algebra over a field to every abstract group.

We define algebraic groups and their Hopf algebras of polynomial maps. Then, we show that every finitely generated Hopf algebra over an algebraic closed field with no non–zero nilpotents is isomorphic to the algebra of polynomial maps of some algebraic group. This motivates the concept of affine scheme to be used in chapter 2.

Let F be a commutative ring with 1, which will be our base ring throughout this chapter. If S is a set, let $\mathrm{id}_S : S \to S$ be the identity map.

1.1 Algebras and coalgebras, and their morphisms

An **F–algebra** is a triple (A, μ, u) where

A-1 A is an F–module,

A-2 (multiplication) $\mu : A \bigotimes A \to A$ is an F–linear map,

A-3 (unit) $u : F \to A$ is an F–linear map, such that for all $\alpha \in F$, $a \in A$, if $p_1 : F \bigotimes A \to A$, $\alpha \otimes a \mapsto \alpha a$, and $p_2 : A \bigotimes F \to A$, $a \otimes \alpha \mapsto a\alpha$, are the **canonical maps**, then the following diagrams commute.

$$\begin{tikzcd}
F \bigotimes A \arrow[r, "p_1"] \arrow[d, "u\otimes \mathrm{id}_A"'] & A \\
A \bigotimes A \arrow[ur, "\mu"'] &
\end{tikzcd}
\qquad
\begin{tikzcd}
A \bigotimes F \arrow[r, "p_2"] \arrow[d, "\mathrm{id}_A\otimes u"'] & A \\
A \bigotimes A \arrow[ur, "\mu"'] &
\end{tikzcd}$$

$$\begin{tikzcd}
A \bigotimes A \bigotimes A \arrow[r, "\mu\otimes \mathrm{id}_A"] \arrow[d, "\mathrm{id}_A\otimes\mu"'] & A \bigotimes A \arrow[d, "\mu"] \\
A \bigotimes A \arrow[r, "\mu"'] & A
\end{tikzcd}$$

F is an F–algebra where $\mu = p_1 = p_2$ and $u = \mathrm{id}_F$.

Let (A, μ, u) and (A', μ', u') be F–algebras. A **morphism of F–algebras** is a linear map $h : A \to A'$ such that the following diagrams commute.

$$\begin{tikzcd}
A \bigotimes A \arrow[r, "\mu"] \arrow[d, "h\otimes h"'] & A \arrow[d, "h"] \\
A' \bigotimes A' \arrow[r, "\mu'"'] & A'
\end{tikzcd}
\qquad
\begin{tikzcd}
F \arrow[r, "u"] \arrow[dr, "u'"'] & A \arrow[d, "h"] \\
 & A'
\end{tikzcd}$$

Dually, we define an **F–coalgebra** as a triple (C, δ, ε) where

C-1 C is an F–module,

C-2 (comultiplication) $\delta : C \to C \bigotimes C$ is an F–linear map,

C-3 (counit) $\varepsilon : C \to F$ is an F–linear map,

such that for all $c \in C$, if $q_1 : C \to F \bigotimes C$, $c \mapsto 1 \otimes c$, and $q_2 : C \to C \bigotimes F$, $c \mapsto c \otimes 1$, are the **canonical maps**, then the following diagrams commute.

$$\begin{tikzcd}
F \bigotimes C & C \arrow[l, "q_1"'] \arrow[dl, "\delta"] \\
C \bigotimes C \arrow[u, "\varepsilon\otimes \mathrm{id}_C"] &
\end{tikzcd}
\qquad
\begin{tikzcd}
C \bigotimes F & C \arrow[l, "q_2"'] \arrow[dl, "\delta"] \\
C \bigotimes C \arrow[u, "\mathrm{id}_C\otimes\varepsilon"] &
\end{tikzcd}$$

$$\begin{tikzcd}
C \bigotimes C \bigotimes C & C \bigotimes C \arrow[l, "\delta\otimes \mathrm{id}_C"'] \\
C \bigotimes C \arrow[u, "\mathrm{id}_C\otimes\delta"] & C \arrow[l, "\delta"] \arrow[u, "\delta"']
\end{tikzcd}$$

F is also an F–coalgebra where $\delta = q_1 = q_2$ and $\varepsilon = \mathrm{id}_F$.

Let (C, δ, ε) and $(C', \delta', \varepsilon')$ be F–coalgebras. A **morphism of F–coalgebras** is a linear map $h : C' \to C$ such that the following diagrams commute.

$$\begin{tikzcd}
C \bigotimes C & C \arrow[l, "\delta"'] \\
C' \bigotimes C' \arrow[u, "h\otimes h"] & C' \arrow[l, "\delta'"] \arrow[u, "h"']
\end{tikzcd}
\qquad
\begin{tikzcd}
F & C \arrow[l, "\varepsilon"'] \\
 & C' \arrow[ul, "\varepsilon'"] \arrow[u, "h"']
\end{tikzcd}$$

1.2 Bialgebras and Hopf algebras, and their morphisms

An **F–bialgebra** is a five tuple $(B, \mu, u, \delta, \varepsilon)$ where

B-1 (B, μ, u) is an F–algebra,

B-2 (B, δ, ε) is an F–coalgebra,

B-3 δ and ε are F–algebra morphisms.

Let $(B, \mu, u, \delta, \varepsilon)$ and $(B, \mu', u', \delta', \varepsilon')$ be bialgebras. A **morphism of F–bialgebras** is a linear map $h : B \to B'$ such that h is an algebra and a coalgebra morphism.

The multiplication to be defined in the following proposition will be used throughout this thesis.

1.2.1 Proposition Let (C, δ, ε) be an F–coalgebra and let (A, μ, u) be an F-algebra. Let $\mathrm{Hom}_F(C, A)$ be the F–module of all linear maps from C to A. Then, there is an F–algebra structure on $\mathrm{Hom}_F(C, A)$ where the multiplication of two linear maps $h, k : C \to A$ is defined as the composite $\mu_A \circ (h \otimes k) \circ \delta_C$, and the neutral element is $u_A \circ \varepsilon_C$.

Proof. For $h, k, l \in \mathrm{Hom}_A(C, A)$,

$$\begin{aligned}
(hk)l &= \mu_A \circ ((h \otimes k \circ \delta) \otimes l) \circ \delta \\
&= \mu_A \circ (h \otimes k \otimes l) \circ (\delta \otimes id_C \circ \delta) \\
&= \mu_A \circ (h \otimes k \otimes l) \circ (id_C \otimes \delta \circ \delta), \text{ since } C \text{ is a coalgebra} \\
&= \mu_A \circ (h \otimes (k \otimes l \circ \delta)) \circ \delta \\
&= h(kl).
\end{aligned}$$

Also, we have

$$\begin{aligned} h(u_A \circ \varepsilon_C) &= \mu_A \circ (h \otimes (u_A \circ \varepsilon_C)) \circ \delta_C \\ &= \mu_A \circ (h \otimes u_A) \circ (\mathrm{id}_C \otimes \varepsilon_C) \circ \delta_C \\ &= \mu_A \circ (h \otimes u_A) \circ q_2, \text{ since } C \text{ is a coalgebra} \\ &= \mu_A \circ (\mathrm{id}_A \otimes u_A) \circ (h \otimes \mathrm{id}_F) \circ q_2 \\ &= p_2 \circ (h \otimes \mathrm{id}_F) \circ q_2, \text{ since } A \text{ is an algebra} \\ &= h, \text{ since } A \text{ is a module.} \end{aligned}$$

Similarly, one shows that $(u_A \circ \varepsilon_C)h = h$. □

We will usually write $hk = (h \otimes k) \circ \delta_C$ omitting μ_A.

Let $(H, \mu, u, \delta, \varepsilon)$ be a bialgebra. Letting $C = A = H$ in proposition 1.2.1, we obtain an F-algebra structure on $\mathrm{End}_F(H) = \mathrm{Hom}_F(H, H)$. The multiplication of this algebra structure on $\mathrm{End}_F(H)$ is called **convolution.**

An **F–Hopf algebra** is a bialgebra $(H, \mu, u, \delta, \varepsilon)$ such that id_H has an inverse η with respect to the convolution in $\mathrm{End}_F(H)$ which is an algebra antimorphism. η is called the **antipode** of the Hopf algebra H. So for the antipode of a Hopf algebra the following diagram commutes.

$$\begin{tikzcd}
H \otimes H \arrow[d, "\mathrm{id}_H \otimes \eta"'] & H \arrow[l, "\delta"'] \arrow[r, "\delta"] \arrow[d, "\varepsilon"] & H \otimes H \arrow[d, "\eta \otimes \mathrm{id}_H"] \\
H \otimes H \arrow[dr, "\mu"'] & F \arrow[d, "u"] & H \otimes H \arrow[dl, "\mu"] \\
 & H &
\end{tikzcd}$$

F is a Hopf algebra where $\eta = id_F$.

Let $(H, \mu, u, \delta, \varepsilon, \eta)$ and $(H', \mu', u', \delta', \varepsilon', \eta')$ be Hopf algebras. A **morphism of F–Hopf algebras** is a bialgebra morphism $h : H \to H'$ such that the following diagram commutes.

$$\begin{tikzcd}
H \arrow[r, "h"] \arrow[d, "\eta"'] & H' \arrow[d, "\eta'"] \\
H \arrow[r, "h"'] & H'
\end{tikzcd}$$

Let (A, μ, u) be an algebra. A **sub–algebra** of A is a submodule A' of A such that $\mu(A' \otimes A') \subset A'$ and $u(F) \subset A'$.

Let $(H, \mu, u, \delta, \varepsilon, \eta)$ be a Hopf algebra. A **sub–Hopf algebra** of H is a sub–algebra H' of H such that $\delta(H') \subset H' \otimes H'$ and $\eta(H') \subset H'$.

1.3 A coalgebra as a locally finite module over its dual

The result of this section is due to Gerhard P. Hochschild, who proved it over a field, but actually it holds over any ring. It will be used to show that certain groups attached to a Hopf algebra are algebraic.

Let (C, δ, ε) be a coalgebra over a ring F and let $C^\circ = \mathrm{Hom}_F(C, F)$ be the set of all linear maps from C into F. By proposition 1.2.1, we know that for the coalgebra C we have a multiplication on C° that makes it into an F-algebra. For any $x \in C^\circ$ let

$$l(x) = (\mathrm{id}_C \otimes x) \circ \delta \text{ and } r(x) = (x \otimes \mathrm{id}_C) \circ \delta.$$

If we identify $C \bigotimes F = C = F \bigotimes C$, then

$$l(x),\ r(x) \in \mathrm{End}_F(C).$$

1.3.1 Proposition Let (C, δ, ε) be a coalgebra. Then,

- the map
$$\begin{aligned} l : C^\circ &\longrightarrow \mathrm{End}_F(C) \\ x &\longmapsto (\mathrm{id}_C \otimes x) \circ \delta \end{aligned}$$
is an injective morphism of F-algebras, i.e. C is a faithful left C°-module,
- the map
$$\begin{aligned} r : C^\circ &\longrightarrow \mathrm{End}_F(C) \\ x &\longmapsto (x \otimes \mathrm{id}_C) \circ \delta \end{aligned}$$
is an injective antimorphism of F-algebras, i.e. C is a faithful right C°-module,
- for all $x,\ y \in C^\circ$,
$$l(x) \circ r(x) = r(x) \circ l(x),$$
so C is a two-sided C°-module,
- this two-sided module is locally finite, i.e. every element of C is contained in a finitely generated sub F-module of C that is two-sided stable under the action of C°.

Proof. We first show that for $x, y \in C^\circ$, $l(xy) = l(x)l(y)$.

$$\begin{aligned} l(x)l(y) &= (\mathrm{id}_C \otimes x) \circ \delta \circ (\mathrm{id}_C \otimes y) \circ \delta \\ &= (\mathrm{id}_C \otimes x) \circ (\mathrm{id}_C \otimes \mathrm{id}_C \otimes y) \circ (\delta \otimes \mathrm{id}_C) \circ \delta, \end{aligned}$$

and since C is a coalgebra

$$\begin{aligned}&= (\mathrm{id}_C \otimes x) \circ (\mathrm{id}_C \otimes \mathrm{id}_C \otimes y) \circ (\mathrm{id}_C \otimes \delta) \circ \delta \\ &= (\mathrm{id}_C \otimes x) \circ (\mathrm{id}_C \otimes \mathrm{id}_C \otimes (y \circ \delta)) \circ \delta \\ &= \Big(\mathrm{id}_C \otimes ((x \otimes y) \circ \delta)\Big) \circ \delta \\ &= l(xy).\end{aligned}$$

Also,

$l(\varepsilon) = (\mathrm{id}_C \otimes \varepsilon) \circ \delta = \mathrm{id}_C$, since C is a coalgebra.

Hence, the map $l : C^\circ \to \mathrm{End}_F(C)$ is a left C°-module on C. From the definitions it follows that

$$xy = x \circ l(y),$$

indeed $x \circ l(y) = x \circ (\mathrm{id}_C \otimes y) \circ \delta = (x \otimes y) \circ \delta = xy$. In particular, $\varepsilon \circ l(x) = \varepsilon x = x$, since ε is the unit of the algebra C°. Hence, l is injective with inverse $\varepsilon \circ -$.

In a similar way, one shows that the map $r : C^\circ \to \mathrm{End}_F(C)$ is a faithful C°-module on C.

Next we show that

$$l(x) \circ r(y) = r(y) \circ l(x).$$

$$\begin{aligned}l(x) \circ r(y) &= (\mathrm{id}_C \otimes x) \circ \delta \circ (y \otimes \mathrm{id}_C) \circ \delta \\ &= (y \otimes \mathrm{id}_C \otimes x) \circ (\mathrm{id}_C \otimes \delta) \circ \delta \\ &= (y \otimes \mathrm{id}_C \otimes x) \circ (\delta \otimes \mathrm{id}_C) \circ \delta, \text{ since } C \text{ is a coalgebra} \\ &= (y \otimes \mathrm{id}_C) \circ \delta \circ (\mathrm{id}_C \otimes x) \circ \delta \\ &= r(y) \circ l(x).\end{aligned}$$

So, C is a two–sided C°-module.

We finally show that C is locally finite. Let $c \in C$. We show that there is a finitely generated sub F-module of C containing c that is two sided–stable under the action of C°. Write

$$\delta(c) = \Sigma_{(c)} c_{(1)} \otimes c_{(2)}.$$

Let $x \in C^\circ$, then $x \cdot c = (l(x))(c) = \mathrm{id}_C \otimes x(\Sigma_{(c)} c_{(1)} \otimes c_{(2)}) = \Sigma_{(c)} x(c_{(2)}) c_{(1)}$, so $l(C^\circ) \cdot c \subset \mathrm{Span}_{(c)}\{c_{(1)}\}$. Similarly, $r(C^\circ) \cdot c \subset \mathrm{Span}_{(c)}\{c_{(2)}\}$. So, for all the $c_{(1)}$'s, $r(C^\circ) \cdot c_{(1)}$ is contained in a finitely generated sub F-module of C, and then $r(C^\circ) \cdot l(C^\circ) \cdot c$ is also. Hence there is a finitely generated sub F-module of C containing c that is two sided-stable under C° since the endomorphisms in $l(C^\circ)$ commute with the endomorphisms in $r(C^\circ)$. □

1.4 The Hopf algebra of a group over a field

Let F be a field and let G be an abstract group. If S is a set, let F^S be the F–algebra of maps from S into F. Let δ_{ij} be 1 if $i = j$ and 0 else.

Following Gerhard P. Hochschild, we will define a Hopf algebra $S_F[G]$ of certain maps from G to F. It will turn out that in case G is an algebraic group a certain sub–Hopf algebra of $S_F[G]$, the algebra of polynomial maps, will determine the group structure of G completely.

Let us start with an elementary lemma in linear algebra. This lemma will be needed to characterize the image of a map which will be used to construct the comultiplication of $S_F[G]$.

1.4.1 Lemma Let S be a set and let V be an n–dimensional subspace of F^S. Then, there is a basis $(v_1, v_2, \cdots, v_n)$ of V and a subset $(s_1, s_2, \cdots, s_n)$ of S such that

$$v_i(s_j) = \delta_{ij}, \quad 1 \leq i,\ j \leq n.$$

Proof. By induction on k, where k counts how many s_j's have been selected so far for a given basis of V. Let $k = 0$ and let $v_{1,0}, \cdots, v_{n,0}$ be a basis of V.

Let $k = 1$. Let $s_1 \in S$ such that $v_{1,0}(s_1) \neq 0$. Let $v_{1,1} = v_{1,0}(s_1)^{-1}v_{1,0}$. For $1 < i \leq n$, let

$$v_{i,1} = v_{i,0} - v_{i,0}(s_1)v_{1,1}.$$

Then, for $1 \leq i \leq n$, $v_{i,1}(s_1) = \delta_{i1}$.

Let $k + 1 \leq n$ and assume, by induction, that for $1 \leq j \leq k$, all the s_j's have been chosen with the required property for a given basis $v_{1,k}, \cdots, v_{n,k}$ of V. Let $s_{k+1} \in S$ such that $v_{k+1,k}(s_{k+1}) \neq 0$. Let $v_{k+1,k+1} = v_{k+1,k}(s_{k+1})^{-1}v_{k+1,k}$. For all $1 \leq i \leq n$, $i \neq k + 1$, let

$$v_{i,k+1} = v_{i,k} - v_{i,k}(s_{k+1})v_{k+1,k+1}.$$

Then, for $1 \leq i \leq n$, $1 \leq j \leq k + 1$, $v_{i,k+1}(s_j) = \delta_{ij}$ and the lemma follows by induction. □

If $p \in F^{S \times S}$ let the **partial functions** of p be defined by

$$\begin{aligned} p_x : S &\longrightarrow F & \qquad p_y : S &\longrightarrow F \\ y &\longmapsto p(x,\ y) & x &\longmapsto p(x,\ y). \end{aligned}$$

1.4.2 Proposition The canonical morphism

$$\begin{aligned} \Pi : F^S \bigotimes F^S &\longrightarrow F^{S \times S} \\ \Sigma f \otimes g &\longmapsto \Big((x,\ y) \mapsto \Sigma f(x)g(y)\Big) \end{aligned}$$

is injective and its image is the set of all functions p such that F–Span$\{p_y\}_{y\in S}$ is finitely generated, or equivalently of all functions p such that F–Span$\{p_x\}_{x\in S}$ is finitely generated.

Proof. Let $\Sigma_j f_j \otimes g_j \in \operatorname{Ker}\Pi$. Assume that not all f_j are zero and let $(v_1, \cdots, v_n)$ be a basis of F–Span$\{f_j\}_j$ such that for some $(x_1, \cdots, x_n) \in S$, $v_i(x_j) = \delta_{ij}$ as in lemma 1.4.1. Then, there are $h_i \in F^S$ such that

$$\Sigma_j f_j \otimes g_j = \Sigma_i v_i \otimes h_i.$$

We have $0 = \Pi(\Sigma_i v_i \otimes h_i)_{(x_j,\, y)} = h_j(y)$, for all j and for all $y \in S$. So, all the h_i's are zero and Π is injective.

Let

$$p = \Pi(\Sigma_i f_i \otimes g_i)$$

be in the image of Π and let

$$\begin{aligned} p_y : S &\longrightarrow F \\ x &\longmapsto \big(p(x,\, y) = \Sigma_i f_i(x) g_i(y)\big) \end{aligned}$$

be a partial function of p, then F–Span$\{p_y\}_{y\in S} \subset F$–Span$\{f_i\}_i$. Hence the space spanned by the partial functions of p is finitely generated by the f_i's.

Conversely, assume that for some $p \in F^{S\times S}$, for all $y \in S$, $p_y \in \operatorname{Span}\{f_1, \cdots, f_n\} \subset F^S$. Then, for some $g_i \in F^S$,

$$p_y = g_1(y) f_1 + \cdots + g_n(y) f_n,$$

hence, by definition of Π, $p = \Pi(\Sigma f_i \otimes g_i)$. □

Let $\mathrm{m} : G \times G \to G$ be the **group multiplication** of G. Transposing m we get a map

$$\begin{aligned} \mathrm{m}^t : F^G &\longrightarrow F^{G\times G} \\ f &\longmapsto \big((x,\, y) \mapsto f(\mathrm{m}(x,\, y))\big). \end{aligned}$$

We will write xy for $\mathrm{m}(x,\, y)$ as usual, so

$$\mathrm{m}^t(f)_{(x,\, y)} = f(xy).$$

Similarly, transposing the right and left actions of G on itself by translations, we make F^G into a two sided G-module which we write as

$$(y \cdot f)_{(x)} = f(xy), \qquad (f \cdot x)_{(y)} = f(xy).$$

A function $f \in F^G$ splits iff $\mathrm{m}^t(f) \in \Pi(F^G \bigotimes F^G)$. So, by proposition 1.4.2, f splits iff $\{y \cdot f\}_{y \in G}$ is finite dimensional. Let $\mathbf{S_F(G)}$ be the subalgebra of F^G of all split functions from G into F. From this characterization of split functions we obtain the following result.

1.4.3 Corollary $S_F(G)$ is a two–sided sub G-module and a sub algebra of F^G. □

By definition of $S_F(G)$, we know that $\mathrm{m}^t(S_F(G)) \subset \Pi(F^G \bigotimes F^G)$, but actually there is always a representation of an element of $S_F(G)$ such that the factors in which it splits also lie in $S_F(G)$.

1.4.4 Proposition $\Pi^{-1} \circ \mathrm{m}^t(S_F(G)) \subset S_F(G) \bigotimes S_F(G)$.

Proof. Let $f \in S_F(G)$, then $\mathrm{m}^t(f) \in \Pi(F^G \bigotimes F^G)$. Since Π is injective there is a unique $\Sigma_j f_j \otimes g_j \in F^G \bigotimes F^G$ such that $\Pi(\Sigma_j f_j \otimes g_j) = \mathrm{m}^t(f)$. Let

$$\Pi^{-1}(\mathrm{m}^t(f)) = \Sigma_j f_j \otimes g_j.$$

Assume that not all f_j are zero and let $(v_1, \cdots, v_n)$ be a basis of F-Span$\{f_j\}_j$ such that for some $(x_1, \cdots, x_n) \in G$, $v_i(x_j) = \delta_{ij}$ as in lemma 1.4.1. Then, there are $h_i \in F^G$ such that

$$\Sigma_j f_j \otimes g_j = \Sigma_i v_i \otimes h_i.$$

For $y \in G$,

$$\mathrm{m}^t(f)_{(x_j,y)} = \Pi(\Sigma_i v_i \otimes h_i)_{(x_j,y)} = \Sigma_i v_i(x_j) h_i(y) = h_j(y).$$

So, for all $y \in G$ $f(x_j y) = h_j(y)$, and $h_j = f \cdot x_j$. Since $f \in S_F(G)$ and $S_F(G)$ is a G–module, it follows that $h_j \in S_F(G)$, hence $\Sigma_i v_i \otimes h_i \in F^G \bigotimes S_F(G)$.

Similarly, letting $(w_j)_j$ be a basis of F-Span$\{h_i\}_i$ such that for some $(y_j)_j \in G$, $w_j(y_i) = \delta_{ij}$, one shows that $\Pi^{-1} \circ \mathrm{m}^t(f) \in S_F(G) \bigotimes S_F(G)$. □

Let $\delta = \Pi^{-1} \circ \mathrm{m}^t : S_F(G) \to S_F(G) \bigotimes S_F(G)$. δ is an algebra morphism since Π and m^t are. For $f \in S_F(G)$, if we write $\delta(f) = \Sigma_{(f)} f_{(1)} \otimes f_{(2)}$, then

$$f(xy) = \Sigma_{(f)} f_{(1)}(x) f_{(2)}(y), \text{ for all } x, y \in G.$$

Since the multiplication of G is associative then for all x, y, $z \in G$

$$f(x(yz)) = f((xy)z).$$

Hence,

$$\Sigma_{(f)} f_{(1)}(x) f_{(2)}(yz) = \Sigma_{(f)} f_{(1)}(xy) f_{(2)}(z), \text{ and}$$
$$\Sigma_{(f)} f_{(1)}(x) \Sigma_{(f_{(2)})} f_{(2)_{(1)}}(y) f_{(2)_{(2)}}(z) = \Sigma_{(f)} \Sigma_{(f_{(1)})} f_{(1)_{(1)}}(x) f_{(1)_{(2)}}(y) f_{(2)}(z).$$

Since the canonical map

$$\begin{array}{rcl} F^G \bigotimes F^G \bigotimes F^G & \longrightarrow & F^{G\times G\times G} \\ \Sigma_i f_i \otimes g_i \otimes h_i & \longmapsto & ((x, y, z) \mapsto \Sigma_i f_i(x) g_i(y) h_i(z)) \end{array}$$

is injective (this is shown as the injectivity of the map in proposition 1.4.2), it follows that

$$\Sigma_{(f)} f_{(1)} \otimes \Sigma_{(f_{(2)})} f_{(2)_{(1)}} \otimes f_{(2)_{(2)}} = \Sigma_{(f)} \Sigma_{(f_{(1)})} f_{(1)_{(1)}} \otimes f_{(1)_{(2)}} \otimes f_{(2)}.$$

$$(i_{S_F(G)} \otimes \delta) \circ \delta(f) = (\delta \otimes i_{S_F(G)}) \circ \delta(f),$$

and the following diagram commutes.

$$\begin{tikzcd}
S_F(G) \bigotimes S_F(G) \bigotimes S_F(G) & S_F(G) \bigotimes S_F(G) \arrow[l, "\delta\otimes\mathrm{id}_{S_F(G)}"'] \\
S_F(G) \bigotimes S_F(G) \arrow[u, "\mathrm{id}_{S_F(G)}\otimes\delta"] & S_F(G) \arrow[l, "\delta"] \arrow[u, "\delta"']
\end{tikzcd}$$

Let $\varepsilon : S_F(G) \to F$ be specialization at $1 \in G$, i.e. for $f \in S_F(G)$,

$$\varepsilon(f) = f(1).$$

As any specialization, ε is an algebra homomorphism. Since $1 \in G$ is the identity element then

$$\Sigma_{(f)} f_{(1)}(1) f_{(2)}(x) = f(x1) = f(x) = f(1x) = \Sigma_{(f)} f_{(1)}(x) f_{(2)}(1), \text{ hence}$$

$$(\varepsilon \otimes i_{S_F(G)}) \circ \delta(f) = q_1(f) \quad \text{and} \quad (i_{S_F(G)} \otimes \varepsilon) \circ \delta(f) = q_2(f),$$

and the following diagrams commutes.

$$\begin{tikzcd}
F \bigotimes S_F(G) & S_F(G) \arrow[l, "q_1"'] \arrow[dl, "\delta"] \\
S_F(G) \bigotimes S_F(G) \arrow[u, "\varepsilon\otimes\mathrm{id}_{S_F(G)}"] &
\end{tikzcd}
\qquad
\begin{tikzcd}
S_F(G) \bigotimes F & S_F(G) \arrow[l, "q_2"'] \arrow[dl, "\delta"] \\
S_F(G) \bigotimes S_F(G) \arrow[u, "\mathrm{id}_{S_F(G)}\otimes\varepsilon"] &
\end{tikzcd}$$

So, $(S_F(G), \mu, u, \delta, \varepsilon)$ is a bialgebra.

Let

$$\begin{array}{rrcl} \eta : & S_F(G) & \longrightarrow & S_F(G) \\ & f & \longmapsto & f(-^{-1}), \end{array}$$

where $f(-^{-1}) : G \to F$ is defined by $x \mapsto f(x^{-1})$. By direct verification, one sees that η is an algebra morphism. From the inverse operation of G it follows that

$$\Sigma_{(f)} f_{(1)}(x) f_{(2)}(x^{-1}) = f(xx^{-1}) = f(1) = f(x^{-1}x) = \Sigma_{(f)} f_{(1)}(x^{-1}) f_{(2)}(x), \text{ hence}$$

$$\mu \circ (i_{S_F(G)} \otimes \eta) \circ \delta(f) = u \circ \varepsilon(f) \quad \text{and} \quad \mu \circ (\eta \otimes i_{S_F(G)}) \circ \delta(f) = u \circ \varepsilon(f),$$

so the following diagram commutes.

$$\begin{tikzcd}
S_F(G)\otimes S_F(G) \arrow[d, "\mathrm{id}_{S_F(G)}\otimes\eta"'] & S_F(G) \arrow[l, "\delta"'] \arrow[r, "\delta"] \arrow[d, "\varepsilon"] & S_F(G)\otimes S_F(G) \arrow[d, "\eta\otimes\mathrm{id}_{S_F(G)}"] \\
S_F(G)\otimes S_F(G) \arrow[dr, "\mu"'] & F \arrow[d, "u"] & S_F(G)\otimes S_F(G) \arrow[dl, "\mu"] \\
 & S_F(G) &
\end{tikzcd}$$

1.4.5 Proposition $(S_F(G), \mu, u, \delta, \varepsilon, \eta)$ is a Hopf algebra. □

1.5 Algebraic groups and their morphisms

For a field F, the F–algebra $F[V]$ of regular functions on an algebraic set V (the common zeros of some polynomials in $F[X_1, \cdots, X_n]$) is of finite type, that is, it is generated by finitely many elements, and as an algebra of functions with values in the field F, it is reduced, that is, it has no non-zero nilpotents. If F is algebraically closed, it follows from Hilbert's Nullstellensatz that, by associating with a point $x \in V$ the maximal ideal of regular functions vanishing at x,

$$I(x) = \{f \in F[V] : f(x) = 0\},$$

one gets a bijection between V and the set Specm$(F[V])$ of all maximal ideals of the coordinate ring $F[V]$. Since every maximal ideal of $F[V]$ is the kernel of an F–algebra homomorphism from $F[V]$ into the base field, one gets a bijection between V and all such homomorphism. This motivates the following abstract definition of algebraic set.

Let F be a field. An F–algebraic set is a pair $(V, \mathrm{Pol}_F(V))$ where

AS-1 V is a non–empty set, and

AS-2 $\mathrm{Pol}_F(V)$ is a finitely generated sub algebra cf F^V, such that evaluation at elements of V

$$\begin{array}{rl} \mathrm{Eva}_V : V & \longrightarrow \mathrm{Hom}_{F\text{-alg}}(\mathrm{Pol}_F(V), F) \\ v & \longmapsto (p \mapsto p(v)) \end{array}$$

is a bijection between V and the set of all algebra homomorphisms from $\mathrm{Pol}_F(V)$ into F.

$\mathrm{Pol}_F(V)$ is the algebra of **polynomial functions** of V.

Let $S \subset V$. Consider the restriction map

$$\begin{array}{rl} /_S : \mathrm{Pol}_F(V) & \longrightarrow F^S \\ p & \longmapsto p/_S, \end{array}$$

which is an algebra homomorphism. Let $\mathrm{Pol}_F(S) = \mathrm{Im}(/_S) = \{p/_S : p \in \mathrm{Pol}_F(V)\}$ and let $J_S = \mathrm{Ker}(/_S) = \{p \in \mathrm{Pol}_F(V) : p/_S = 0\}$. Then,

$$\mathrm{Pol}_F(S) \cong \mathrm{Pol}_F(V)/J_S, \text{ as } F\text{-algebras.}$$

Since Eva_V is injective, we see that

$$\begin{array}{rl} \mathrm{Eva}_S : S & \xrightarrow{\hspace{3cm}} \mathrm{Hom}_{F\text{-alg}}(\mathrm{Pol}_F(S), F) \\ s & \longmapsto\hspace{2.6cm} (p \mapsto p(s)) \end{array}$$

is also injective; indeed let $s_1,\ s_2 \in S$ and assume that $\mathrm{Eva}_S(s_1) = \mathrm{Eva}_S(s_2)$. Then $\mathrm{Eva}_S(s_1)(p) = \mathrm{Eva}_S(s_2)(p)$ for all $p \in \mathrm{Pol}_F(S)$. Then $p(s_1) = p(s_2)$ for all $p \in \mathrm{Pol}_F(S)$ by definition of Eva_S. Then $p(s_1) = p(s_2)$ for all $p \in \mathrm{Pol}_F(V)$, since $\mathrm{Pol}_F(S) := \{p/_S : p \in \mathrm{Pol}_F(V)\}$. Then $\mathrm{Eva}_V(s_1) = \mathrm{Eva}_V(s_2)$ by definition of Eva_V. Hence $s_1 = s_2$ since Eva_V is injective and it follows that Eva_S is injective.

We would want Eva_S to be also surjective, so that $(S, \mathrm{Pol}_F(S))$ would be an algebraic set. A **closed subset** of V in the **Zariski topology** is the set of zeros of a subset of $\mathrm{Pol}_F(V)$. Let

$$\mathcal{V}(J_S) = \{v \in V : \mathrm{Eva}_V(v)(J_S) = 0\},$$

clearly, $S \subset \mathcal{V}(J_S)$. Also, $S = \mathcal{V}(J_S)$ if and only if S is a closed set, and in this case, Eva_S is surjective. Since if $\phi : \mathrm{Pol}_F(S) \to F$ is an algebra homomorphism, then composing with the canonical projection $\mathrm{Pol}_F(V) \to \mathrm{Pol}(V)/J_S$ we get an evaluation at some element $v \in V$,

$$\mathrm{Eva}_V(v) : \ \mathrm{Pol}_F(V) \longrightarrow \mathrm{Pol}(V)/J_S \cong \mathrm{Pol}(S) \xrightarrow{\ \phi\ } F.$$

But since $\mathrm{Eva}_V(v)(J_S) = 0$ then $v \in \mathcal{V}(J_S) = S$, since S is closed, and $\phi = \mathrm{Eva}_S(v)$. An **algebraic subset** S of V is a closed subset of V.

Let V and V' be algebraic sets. A **morphism of algebraic sets** or a **polynomial map** is a map $h : V \to V'$ such that

$$\mathrm{Pol}_F(V') \circ h \subset \mathrm{Pol}_F(V).$$

1.5.1 Observation Every abstract F-algebraic set $(V, \mathrm{Pol}_F(V))$ is isomorphic to an algebraic subset (loci of polynomials in the naive sense of classical algebraic geometry over a field) of some suitable affine space F^n. For it suffices to take some generators $p_1, \cdots, p_n$ of the finitely generated algebra $\mathrm{Pol}_F(V)$ and to use them to embed V (via the identification given by Eva_V) in F^n.

Indeed, via Eva_V each element of V is (identified with) an F-algebra homomorphism $\mathrm{Pol}_F(V) \to F$ and every such homomorphism is determined once we know its values on a set of generators

$p_1, \cdots, p_n$ of $\mathrm{Pol}_F(V)$. So, $(p_i)_{1 \le i \le n}$ is a set of coordinate functions for the algebraic set V. i.e.

$$v \mapsto \mathrm{Eva}_V(v) \mapsto \left(\mathrm{Eva}_V(v)(p_i)\right)_{1 \le i \le n} = (p_i(v))_{1 \le i \le n} \in F^n$$

is an injection. Define an F-algebra homomorphism from the polynomial ring in n letters onto $\mathrm{Pol}_F(V)$ by

$$\begin{tikzcd} F[X_1, \cdots, X_n] \arrow[r] & \mathrm{Pol}_F(V) \\ X_i \arrow[r, mapsto] & p_i, \end{tikzcd}$$

(this map surjects since the p_i generate $\mathrm{Pol}_F(V)$) and write the algebra of polynomial maps as a quotient,

$$\mathrm{Pol}_F(V) \cong F[X_1, \cdots, X_n]/I,$$

Then, the ideal of relations I is finitely generated (Hilbert's basis theorem) by, say, $f_1, \cdots, f_s \in F[X_1, \cdots, X_n]$ and

$$f_i(p_1, \cdots, p_n) = 0 \in \mathrm{Pol}_F(V), \text{ for } 1 \le i \le s.$$

So

$$f_i(p_1(v), \cdots, p_n(v)) = 0 \in F, \text{ for all } v \in V \text{ and for } 1 \le i \le s,$$

and hence the elements of V are (identified with) common loci of finitely many polynomials $\{f_i\}_{1 \le i \le s} \subset F[X_1, \cdots, X_n]$, i.e. V is an algebraic subset of the affine space F^n.

We want $V \times V'$ to be an algebraic set. By proposition 1.4.2, we can identify $\mathrm{Pol}_F(V) \bigotimes \mathrm{Pol}_F(V')$ with its image in $F^{V \times V'}$ and we define $\mathrm{Pol}_F(V \times V')$ as this image. By considering elements of the form $p \otimes 1$ and $1 \otimes q$, with $p \in \mathrm{Pol}_F(V)$ and $q \in \mathrm{Pol}_F(V')$, we see that the map

$$\begin{tikzcd} \mathrm{Eva}_{V \times V'} : V \times V' \arrow[r] & \mathrm{Hom}_{F\text{-alg}}(\mathrm{Pol}_F(V \times V'), F) \\ (v, v') \arrow[r, mapsto] & (p \mapsto p(v, v')) \end{tikzcd}$$

is injective. Let us fill out the details, let $v_1, w_1 \in V$ and $v_2, w_2 \in V'$. Suppose that $\mathrm{Eva}_{V \times V'}(v_1, v_2) = \mathrm{Eva}_{V \times V'}(w_1, w_2)$. We show that $(v_1, v_2) = (w_1, w_2)$. By definition, we have

$$\mathrm{Pol}_F(V \times V') = \Pi(\mathrm{Pol}_F(V) \bigotimes \mathrm{Pol}_F(V')).$$

Then, considering elements $p \otimes 1$, with $p \in \mathrm{Pol}_F(V)$ it follows that

$$\mathrm{Eva}_{V \times V'}(v_1, v_2)(\Pi(p \otimes 1)) = \mathrm{Eva}_{V \times V'}(w_1, w_2)(\Pi(p \otimes 1))$$

So, $p(v_1).1_F = p(w_1).1_F$, hence $p(v_1) = p(w_1)$ for all $p \in \mathrm{Pol}_F(V)$. This means that $\mathrm{Eva}_V(v_1) = \mathrm{Eva}_V(w_1)$, and since Eva_V is injective we have $v_1 = w_1$. By considering elements of the form $1 \otimes q$ with $q \in \mathrm{Pol}_F(V')$ one similarly shows that $v_2 = w_2$, and it follows that $\mathrm{Eva}_{V \times V'}$ is injective.

By a direct verification we also see that $\mathrm{Eva}_{V \times V'}$ is surjective;
the details follow. Let $f : \mathrm{Pol}_F(V \times V') \to F$ be an F-algebra homomorphism. So

$$f : \Pi(\mathrm{Pol}_F(V) \bigotimes \mathrm{Pol}_F(V')) \to F. \text{ by definition of } \mathrm{Pol}_F(V \times V').$$

consider now $f \circ \Pi : \mathrm{Pol}_F(V) \bigotimes \mathrm{Pol}_F(V') \to F$ and let

$$\begin{aligned} i_1 :\ \mathrm{Pol}_F(V) &\longrightarrow \mathrm{Pol}_F(V) \bigotimes \mathrm{Pol}_F(V') \\ p &\longmapsto p \otimes 1, \\ i_2 :\ \mathrm{Pol}_F(V') &\longrightarrow \mathrm{Pol}_F(V) \bigotimes \mathrm{Pol}_F(V') \\ q &\longmapsto 1 \otimes q \end{aligned}$$

be the canonical injections. Then, $f \circ \Pi \circ i_1 \in \mathrm{Hom}_{F\text{-alg}}(\mathrm{Pol}_F(V), F)$ and $f \circ \Pi \circ i_2 \in \mathrm{Hom}_{F\text{-alg}}(\mathrm{Pol}_F(V'), F)$. So by the surjectivity of Eva_V and $\mathrm{Eva}_{V'}$ there exist $v \in V$ and $v' \in V'$ such that

$$\begin{aligned} f \circ \Pi \circ i_1 &= \mathrm{Eva}_V(v) \text{ and} \\ f \circ \Pi \circ i_2 &= \mathrm{Eva}_{V'}(v'). \end{aligned}$$

It now easily follows that $f = \mathrm{Eva}_{V \times V'}(v, v')$, indeed let $p \in \mathrm{Pol}_F(V \times V') = \Pi(\mathrm{Pol}_F(V) \bigotimes \mathrm{Pol}_F(V'))$. Then,

$$\begin{aligned} \mathrm{Eva}_{V \times V'}(v, v')(p) &= p(v, v') \\ &= \Pi(\Sigma_i p_i \otimes q_i)(v, v'), \text{ for some } p_i \in \mathrm{Pol}_F(V) \text{ and } q_i \in \mathrm{Pol}_F(V') \\ &= \Sigma_i p_i(v) q_i(v') \\ &= \Sigma_i \mathrm{Eva}_V(v)(p_i) \mathrm{Eva}_{V'}(v')(q_i) \\ &= \Sigma_i f \circ \Pi \circ i_1(p_i) f \circ \Pi \circ i_2(q_i) \\ &= \Sigma_i f \circ \Pi(p_i \otimes 1) f \circ \Pi(1 \otimes q_i) \\ &= \Sigma_i f \circ \Pi(p_i \otimes q_i) \\ &= f(\Pi(\Sigma_i p_i \otimes q_i)) \\ &= f(p). \end{aligned}$$

hence $\mathrm{Eva}_{V \times V'}$ is surjective. So $(V \times V', \mathrm{Pol}_F(V \times V'))$ is an algebraic set.

An **algebraic F–group** is a pair $((G, \mathrm{m}, \mathrm{inv}), \mathrm{Pol}_F(G))$ where

AG-1 $(G, \mathrm{m}, \mathrm{inv})$ is a group,

AG-2 $(G, \mathrm{Pol}_F(G))$ is an algebraic set, and

AG-3 $\mathrm{m} : G \times G \to G$ and $\mathrm{inv} : G \to G$ are morphisms of algebraic sets.

Let $((G, \mathrm{m}, \mathrm{inv}), \mathrm{Pol}_F(G))$ and $((G', \mathrm{m}, \mathrm{inv}), \mathrm{Pol}_F(G'))$ be algebraic groups. A **morphism of algebraic groups** is a polynomial map $h : G \to G'$ which is a group homomorphism.

The following proposition gives a dictionary between algebraic groups and Hopf algebras.

1.5.2 Proposition Let F be a field. Let $(G, \mathrm{m}, \mathrm{inv})$ be a group and let $\mathrm{Pol}_F(G)$ be a finitely generated sub algebra of F^G such that $(G, \mathrm{Pol}_F(G))$ is an algebraic set. $\mathrm{Pol}_F(G)$ is a sub Hopf algebra of $S_F(G)$ iff $\mathrm{m} : G \times G \to G$ and $\mathrm{inv} : G \to G$ are morphisms of algebraic sets.

Proof. Assume that $\mathrm{Pol}_F(G)$ is a sub Hopf algebra of $S_F(G)$,

then $\mathrm{Pol}_F(G) \subset S_F(G)$, $\delta(\mathrm{Pol}_F(G)) \subset \mathrm{Pol}_F(G) \bigotimes \mathrm{Pol}_F(G)$ and $\eta(\mathrm{Pol}_F(G)) \subset \mathrm{Pol}_F(G)$

by definition of sub Hopf algebra,

then for all $f \in \mathrm{Pol}_F(G)$, $f \in S_F(G)$, $\delta(f) \in \mathrm{Pol}_F(G) \bigotimes \mathrm{Pol}_F(G)$ and $\eta(f) \in \mathrm{Pol}_F(G)$,

then for all $f \in \mathrm{Pol}_F(G)$, $f \in S_F(G)$, $\Pi^{-1} \circ \mathrm{m}^t(f) \in \mathrm{Pol}_F(G) \bigotimes \mathrm{Pol}_F(G)$ and $f \circ \mathrm{inv} \in \mathrm{Pol}_F(G)$

by definition of δ and η,

then for all $f \in \mathrm{Pol}_F(G)$, $f \in S_F(G)$, $\mathrm{m}^t(f) \in \Pi(\mathrm{Pol}_F(G) \bigotimes \mathrm{Pol}_F(G))$ and $f \circ \mathrm{inv} \in \mathrm{Pol}_F(G)$,

then for all $f \in \mathrm{Pol}_F(G)$, $f \in S_F(G)$, $f \circ \mathrm{m} \in \Pi(\mathrm{Pol}_F(G) \bigotimes \mathrm{Pol}_F(G))$ and $f \circ \mathrm{inv} \in \mathrm{Pol}_F(G)$

by definition of m^t,

then for all $f \in \mathrm{Pol}_F(G)$, $f \in S_F(G)$, $f \circ \mathrm{m} \in \mathrm{Pol}_F(G \times G)$ and $f \circ \mathrm{inv} \in \mathrm{Pol}_F(G)$

by definition of $\mathrm{Pol}_F(G \times G)$,

then $\mathrm{Pol}_F(G) \subset S_F(G)$, $\mathrm{Pol}_F(G) \circ \mathrm{m} \subset \mathrm{Pol}_F(G \times G)$ and $\mathrm{Pol}_F(G) \circ \mathrm{inv} \subset \mathrm{Pol}_F(G)$,

then m and inv are morphisms of algebraic sets.

Conversely, assume that m and inv are morphisms of algebraic sets. We show that $\mathrm{Pol}_F(G) \subset S_F(G)$, $\delta(\mathrm{Pol}_F(G)) \subset \mathrm{Pol}_F(G)$ and $\eta(\mathrm{Pol}_F(G)) \subset \mathrm{Pol}_F(G)$. Indeed, since $\mathrm{m} : G \times G \to G$ is a morphism of algebraic sets it follows that

$$\mathrm{Pol}_F(G) \circ \mathrm{m} \subset \mathrm{Pol}_F(G \times G),$$

$$\text{then for all } f \in \mathrm{Pol}_F(G),\ f \circ \mathrm{m} \in \Pi(\mathrm{Pol}_F(G) \bigotimes \mathrm{Pol}_F(G))$$

$$\text{by definition of } \mathrm{Pol}_F(G \times G),$$

$$\text{then for all } f \in \mathrm{Pol}_F(G),\ \mathrm{m}^t(f) \in \Pi(\mathrm{Pol}_F(G) \bigotimes \mathrm{Pol}_F(G))$$

$$\text{by definition of } \mathrm{m}^t,$$

$$\text{then for all } f \in \mathrm{Pol}_F(G),\ \mathrm{m}^t(f) \in \Pi(F^G \bigotimes F^G)$$

$$\text{since } \mathrm{Pol}_F(G) \subset F^G \text{ by definition of } \mathrm{Pol}_F(G).$$

$$\text{So, we have proved that for all } f \in \mathrm{Pol}_F(G),\ f \in S_F(G) \text{ by definition of } S_F(G),$$

$$\text{and that } \mathrm{m}^t(f) \in \Pi(\mathrm{Pol}_F(G) \bigotimes \mathrm{Pol}_F(G)),$$

$$\text{then for all } f \in \mathrm{Pol}_F(G),\ f \in S_F(G) \text{ and } \Pi^{-1} \circ \mathrm{m}^t(f) \in \mathrm{Pol}_F(G) \bigotimes \mathrm{Pol}_F(G)$$

$$\text{since } \Pi \text{ is injective,}$$

$$\text{then for all } f \in \mathrm{Pol}_F(G),\ f \in S_F(G) \text{ and } \delta(f) \in \mathrm{Pol}_F(G) \bigotimes \mathrm{Pol}_F(G)$$

$$\text{by definition of } \delta,$$

$$\text{then } \mathrm{Pol}_F(G) \subset S_F(G) \text{ and } \delta(\mathrm{Pol}_F(G)) \subset \mathrm{Pol}_F(G) \bigotimes \mathrm{Pol}_F(G).$$

Also, looking at the morphism of algebraic sets $\mathrm{inv} : G \to G$ we have $\mathrm{Pol}_F(G) \circ \mathrm{inv} \subset \mathrm{Pol}_F(G)$, then for all $f \in \mathrm{Pol}_F(G)$, $f \circ \mathrm{inv} \in \mathrm{Pol}_F(G)$, and it follows that $\eta(\mathrm{Pol}_F(G)) \subset \mathrm{Pol}_F(G)$, by definition of η.

Hence, $\mathrm{Pol}_F(G)$ is a sub Hopf algebra of $S_F(G)$. □

1.5.3 Remark Even if F is not a field, $\mathrm{Pol}_F(G)$ is still a Hopf algebra.

This fact leads to the study of the algebraic group scheme represented by a finitely generated Hopf algebra and, if $\mathrm{Pol}_F(G)$ is not finitely generated, to the study of its associated affine group scheme. A very useful way of studying affine schemes is to approximate them as a projective limit by algebraic schemes, or in the contraequivalent category of Hopf algebras, to approximate $\mathrm{Pol}_F(G)$ as an inductive limit by finitely generated Hopf algebras (cf. proposition 3.1.3). One tries to understand the finitely generated pieces, and then one hopes that the property under consideration passes over the limit. This is exactly what we will do to study an affine group G in the following chapters.

I see two reasons to look at Hopf algebras. Firstly, it is much easier to compute Hopf algebra maps than to compute affine group scheme maps (cf. proposition 2.4.2). Secondly, to study an abstract Hopf algebra (not starting from a group scheme) will hopefully shed light in already known algebraic groups (cf. corollary 2.4.3).

1.6 The algebraic group of a finitely generated Hopf algebra

For a group G and a field F we have $G \subset S_F(G)^\circ$, where for $x \in G$,

$$\begin{aligned} x : S_F(G) &\longrightarrow F \\ p &\longmapsto p(x). \end{aligned}$$

By proposition 1.2.1, we know that for the coalgebra $S_F(G)$ we have a multiplication on $S_F(G)^\circ$ that makes it into an F–algebra. In case G is algebraic, we will see that if we restrict this multiplication to $\mathrm{Hom}_{F\text{-alg}}(\mathrm{Pol}_F(G), F)$ we will recover the group structure of G. This suggests how to attach an algebraic group scheme to any finitely generated Hopf algebra over an arbitrary ring and, more generally, how to attach a group scheme to any Hopf algebra.

Let $(H, \mu, u, \delta, \varepsilon, \eta)$ be a Hopf algebra over a ring F and let

$$\boldsymbol{G_H(F)} = \mathrm{Hom}_{F\text{-alg}}(H, F)$$

be the set of all F–algebra homomorphisms from H into F. We now see that $\boldsymbol{G_H(F)}$ is a group with multiplication

$$xy = \mu_F \circ (x \otimes y) \circ \delta.$$

The neutral element is $u_F \circ \varepsilon$ and the inverse of an F–algebra homomorphism x is $x \circ \eta$. We usually write $xy = (x \otimes y) \circ \delta$ omitting the multiplication of F. We have already proved that $G_H(F)$ is a monoid (see 1.2.1), but for convenience of the reader we will give the whole argument. $G_H(F)$ is a group because H is a Hopf algebra, indeed let $x, y, z \in G_H$,

$$\begin{aligned} (xy)z &= \big((x \otimes y \circ \delta) \otimes z\big) \circ \delta \\ &= (x \otimes y \otimes z) \circ (\delta \otimes id_H \circ \delta) \\ &= (x \otimes y \otimes z) \circ (id_H \otimes \delta \circ \delta), \text{ since } H \text{ is a coalgebra} \\ &= \big(x \otimes (y \otimes z \circ \delta)\big) \circ \delta \\ &= x(yz). \end{aligned}$$

Also,

$$\begin{aligned}
x(u_F \circ \varepsilon_H) &= \mu_F \circ (x \otimes (u_F \circ \varepsilon_H)) \circ \delta_H \\
&= (x \otimes u_F) \circ (\mathrm{id}_H \otimes \varepsilon_H) \circ \delta_H \\
&= (x \otimes u_F) \circ q_2, \text{ since } H \text{ is a coalgebra} \\
&= (\mathrm{id}_F \otimes u_F) \circ (x \otimes \mathrm{id}_F) \circ q_2 \\
&= p_2 \circ (x \otimes \mathrm{id}_F) \circ q_2, \text{ since } F \text{ is an algebra} \\
&= x, \text{ since } F \text{ is a module.}
\end{aligned}$$

Similarly one shows that $(u_F \circ \varepsilon_C)x = x$. Finally, we have

$$\begin{aligned}
xx^{-1} &= (x \otimes x \circ \eta) \circ \delta \\
&= (x \otimes x) \circ (id_H \otimes \eta) \circ \delta, \\
&= x \circ \mu \circ (id_H \otimes \eta) \circ \delta, \text{ since } x \text{ is an algebra morphism} \\
&= x \circ u \circ \varepsilon, \text{ since } H \text{ is a Hopf algebra} \\
&= u_F \circ \varepsilon, \text{ since } x \text{ is an algebra morphism.}
\end{aligned}$$

Similarly one shows that $x^{-1}x = u_F \circ \varepsilon$. □

Incidentally, this same proof shows that the set $\boldsymbol{G_H(A)}$ of all F–algebra homomorphisms from H into *any* F–algebra A forms a group which is completely determined by the Hopf algebra H.

1.6.1 Lemma Let $(H, \mu, u, \delta, \varepsilon, \eta)$ be a Hopf algebra over a field F and let $G = G_H(F)$. Consider the F–algebra morphism

$$\begin{tikzcd}
\widetilde{\ } : H \arrow[r] & F^G \\
p \arrow[r, mapsto] & (x \mapsto x(p)).
\end{tikzcd}$$

Then $\widetilde{H} \subset S_F(G)$ and $\widetilde{\ }$ is a Hopf algebra morphism. If F is algebraically closed and H is finitely generated then $\mathrm{Ker}(\widetilde{\ }) = \mathrm{Nilradical}(H)$.

Proof. To prove that $\widetilde{H} \subset S_F(G)$, by proposition 1.4.2 it is enough to show that $F\text{–Span}_{x \in G}\{x \cdot \widetilde{p}\}$ is finite dimensional for all $p \in H$. We have that

$$\widetilde{x \cdot p} = x \cdot \widetilde{p},$$

where the dot on the left of this equality stands for the action of $G \subset H^\circ$ on H defined in proposition 1.3.1 and the dot on the right stands for the action of the group G on F^G defined on page 9. Indeed, for all $g \in G$

$$\begin{aligned}
\widetilde{x \cdot p}(g) &= \big((\mathrm{id}_H \otimes x) \circ \delta(p)\big)^{\sim}(g) \\
&= g\big((\mathrm{id}_H \otimes x) \circ \delta(p)\big) \\
&= (g \otimes x) \circ \delta(p) \\
&= (gx)(p) \\
&= \widetilde{p}(gx) \\
&= x \cdot (\widetilde{p}(g)).
\end{aligned}$$

By proposition 1.3.1 H is a locally finite H°–module, in particular $F\text{–Span}_{x \in H^\circ}\{x \cdot p\}$ is finite dimensional. Since $G \subset H^\circ$ and $\widetilde{x \cdot p} = x \cdot \widetilde{p}$ then $F\text{–Span}_{x \in G}\{x \cdot \widetilde{p}\}$ is finite dimensional as required.

We now show that $\sim$ is a Hopf algebra morphism. Let $p \in H$. Firstly we show that

$$\delta_{S_F(G)} \circ {}^{\sim} = ({}^{\sim} \otimes {}^{\sim}) \circ \delta_H.$$

$$\begin{aligned}
\delta_{S_F(G)} \circ {}^{\sim}(p) &= \delta_{S_F(G)}(\widetilde{p}) \\
&= \Pi^{-1} \circ \mathrm{m}^t(\widetilde{p}) \\
&= \Pi^{-1}(\widetilde{p} \circ \mathrm{m}) \\
&= \Pi^{-1}(\widetilde{p} \circ \mu_F \circ (- \otimes -) \circ \delta_H)
\end{aligned}$$

writting $\delta_H(p) = \Sigma_{(p)} p_{(1)} \otimes p_{(2)}$ this is equal to

$$\begin{aligned}
&= \Pi^{-1}(\Sigma_{(p)} \widetilde{p_{(1)}}\, \widetilde{p_{(2)}}) \\
&= \Sigma_{(p)} \widetilde{p_{(1)}} \otimes \widetilde{p_{(2)}}) \\
&= ({}^{\sim} \otimes {}^{\sim}) \circ \delta_H(p).
\end{aligned}$$

Secondly we show that $\sim$ preserves counits

$$\varepsilon_H = \varepsilon_{S_F(G)} \circ {}^{\sim};$$

recall that $\varepsilon_{S_F(G)}$ is evaluation at the unit of the group G which in this case is ε_H. Indeed, $\varepsilon_{S_F(G)}(\widetilde{p}) = \widetilde{p}(\varepsilon_H) = \varepsilon_H(p)$. Thirdly, we show that $\sim$ preserves antipodes,

$$\eta_{S_F(G)} \circ {}^{\sim} = {}^{\sim} \circ \eta_H.$$

So we need to show that for all $p \in H$, $\eta_{S_F(G)}(\tilde{p}) = \widetilde{\eta_H(p)}$. Since these are two functions on G let us check that they agree for all $g \in G$.

$$\begin{aligned}\left(\eta_{S_F(G)}(\tilde{p})\right)(g) &= \tilde{p}(g^{-1}) \\ &= \tilde{p}(g \circ \eta_H) \\ &= (g \circ \eta_H)(p) \\ &= \widetilde{\eta_H(p)}(g).\end{aligned}$$

Finally assume that F is algebraically closed and that H is finitely generated. Then, by Hilbert's Nullstellensatz, every maximal ideal of H is the kernel of some F–algebra morphism $g \in G$ and

$$\text{Nilradical}(H) = \bigcap_{M \underset{\max}{\triangle} H} M.$$

Let $p \in H$. $\tilde{p} = 0$ iff for all $g \in G$, $g(p) = 0$, and by Hilbert's Nullstellensatz this happens iff $g \in \text{Nilradical}(H)$. □

1.6.1 Theorem Let $(H, \mu, u, \delta, \varepsilon, \eta)$ be a finitely generated Hopf algebra over an algebraically closed field F. Let $G = G_H(F)$ and let $\text{Pol}_F(G) = \widetilde{H}$, where $\tilde{}$ is the map of the lemma. Then $(G, \text{Pol}_F(G))$ is an algebraic group. Moreover, if H has no non–zero nilpotents then $H \cong \text{Pol}_F(G)$ as Hopf algebras.

Proof. From the lemma it follows that $\text{Pol}_F(G) \cong H/\text{Nilradical}(H)$ as Hopf algebras. Since an algebra homomorphism from H into (the reduced ring) F annihilates nilpotents, every $g \in G$ factors through $\text{Nilradical}(H)$. It follows that there is a bijection between G and $\text{Hom}_{F\text{-alg}}(\widetilde{H}, F)$, so $(G, \text{Pol}_F(G))$ is an algebraic set. Also, from the lemma it follows that $\text{Pol}_F(G)$ is a sub Hopf algebra of $S_F(G)$, hence by proposition 1.5.2 G is an algebraic group. The "moreover" part follows at once from the lemma as well, since if H is reduced then $\tilde{}$ is an injective morphism of Hopf algebras. □

The additive group $\boldsymbol{G_a(F)}$ of F is an algebraic group if one defines its polynomial algebra as the algebra of functions from $F \to F$ generated by $X = \text{id}_F$ which we identify with the polynomial ring $F[X]$. The Hopf algebra structure of $\text{Pol}_F(G_a(F))$ is given by

$$\begin{aligned}&\delta(X) = 1 \otimes X + X \otimes 1 \\ &\varepsilon(X) = 0 \\ &\eta(X) = -X.\end{aligned}$$

A little more general, every vector space F^n is an algebraic group $\boldsymbol{G_a(F^n)}$, called a vector group, if one considers its additive group with polynomial algebra equal to the algebra of maps $F^n \to F$ generated by the coordinate functions, which we identify with $F[X_1, \cdots, X_n]$. The Hopf algebra structure is given by

$$\delta(X_i) = 1 \otimes X_i + X_i \otimes 1$$
$$\varepsilon(X_i) = 0$$
$$\eta(X_i) = -X_i.$$

The multiplicative group $\boldsymbol{G_m(F)}$ of F is an algebraic group if one defines its polynomial algebra as the algebra of functions from F^* into F which can be written as polynomial in X and X^{-1} where X is identified with id_F. So, $\mathrm{Pol}_F(G_m(F)) \cong F[X,Y]/ < XY - 1 >$ with Hopf algebra structure defined by

$$\delta(X) = X \otimes X$$
$$\varepsilon(X) = 1$$
$$\eta(X) = Y.$$

Let $F[X_{11}, \cdots, X_{nn}]$ be a polynomial ring in n^2 letters. Let X be the $n \times n$ matrix whose components are X_{ij}, and let M_{ij} be the matrix obtained from X by deleting the i-th row and j-column.

The group of invertible matrices $\mathbf{GL}_{\boldsymbol{n}}\boldsymbol{(F)}$ is an algebraic group if one defines its polynomial algebra as the quotient ring $F[X_{11}, \cdots, X_{nn}, Y]/ < \det(X)Y - 1 >$, where X_{ij} is identified with the corresponding coordinate function from $\mathrm{GL}_n(F) \to F$, with the following Hopf algebra structure.

$$\delta(X_{ij}) = \Sigma_k X_{ik} \otimes X_{kj}, \text{ hence } \delta(Y) = Y \otimes Y$$
$$\varepsilon(X_{ij}) = \delta_{ij}, \text{ where } \delta_{ij} \text{ is the Kronecker delta}$$
$$\eta(X_{ij}) = (-1)^{i+j} \det(M_{ji})Y.$$

The special linear group $\mathbf{SL}_{\boldsymbol{n}}\boldsymbol{(F)}$ of matrices over F with determinant equal to 1 is an algebraic group if one defines its polynomial algebra as the quotient ring $F[X_{11}, \cdots, X_{nn}]/ < \det(X) - 1 >$ with the following Hopf algebra structure,

$$\delta(X_{ij}) = \Sigma_k X_{ik} \otimes X_{kj}$$
$$\varepsilon(X_{ij}) = \delta_{ij}, \text{ where } \delta_{ij} \text{ is the Kronecker delta}$$
$$\eta(X_{ij}) = (-1)^{i+j} \det(M_{ji}).$$

Lastly, let us introduce a group which will play an essential role in chapter 3. The group of upper triangular unipotent matrices (that is, upper triangular with 1's on the diagonal) $\mathbf{U}_{\boldsymbol{n}}(\boldsymbol{F})$ is an algebraic group with polynomial algebra $F[X_{ij} : i < j]$ whose Hopf algebra structure is defined by

$$\delta(X_{ij}) = X_{ij} \otimes 1 + 1 \otimes X_{ij} + \Sigma_{i<k<j} X_{ik} \otimes X_{kj}$$

$$\varepsilon(X_{ij}) = \delta_{ij}, \text{ where } \delta_{ij} \text{ is the Kronecker delta}$$

$$\eta(X_{ij}) = (-1)^{i+j} \det(M_{ji}).$$

Chapter 2

The affine group G represented by the Hopf Shuffle Algebra and its Lie algebra of Lie Series

In this chapter we introduce the Hopf Shuffle algebra A [Ree58] and study its corresponding affine group scheme G and some quotients G_N of G. We show that the Lie algebra of G is an algebra of Lie series and that the Lie algebra of G_N is a quotient of the free Lie algebra on the alphabet I. We show that the upper triangular unipotent group scheme is a quotient of G.

The introduction of the shuffle product is due to Ree [Ree58] while he was studying Lie polynomials. Actually in a footnote of this paper Ree attributes the idea of using shuffles to the referee. A signed shuffle product appears in earlier papers of MacLane [Mac50] and of Eilenberg and MacLane [EM53]. Today the shuffle product is well understood under the scope of Hopf algebra theory [Swe69]. In the last section we will introduce Lyndon words which appeared in the work of Lyndon [Lyn54, Lyn55]. We use the fact that the shuffle algebra is a free commutative algebra over the set of Lyndon words; this result is due to Radford [Rad79] who gave a combinatorial proof.

2.1 Nilpotent Lie algebras and Free Lie Series

In the theory of Lie algebras over an algebraic closed field of characteristic zero a cornerstone result is Lie's Theorem [Jac62] from which it follows that for any finite dimensional vector space V and any solvable Lie algebra $L \subset gl(V)$ there is a suitable basis of V relative to which the matrices of L are upper triangular. If one considers a nilpotent Lie algebra $L \subset gl(V)$ from Engel's Theorem [Jac62] it follows that there exists a basis of V relative to which the matrices of L are strictly upper triangular.

Among all Lie Algebras, the nilpotent Lie algebras are very important because of strong results such as the ones mentioned above. Given a set X we can construct $LS(X)$ the algebra of **free Lie series on** X [Bou75]. It turns out that $LS(X)$ is a free object in the category of nilpotent Lie algebras which justifies the study of an algebra of Lie Series. In this context it is natural to ask: is there an affine group whose Lie algebra is an algebra of Lie Series?

2.2 The Hopf Shuffle algebra

Let $\mathbb{K}$ be a field of characteristic zero which will be our base ring. An **affine group scheme** [Wat79], or simply an **affine group**, is a representable functor from the category of $\mathbb{K}$-algebras into the category of groups. In [BP96] and [BP97] Billig and Pianzola found that the multiplication of certain basic polynomial functions on a free Kac–Moody group was related to the shuffle product of words over an alphabet. Since the shuffle algebra A (see below) admits a Hopf-algebra structure then Pianzola studied its corresponding affine group scheme $Hom(A, -)$ [Pia].

An **alphabet** is a set I. An **index** or a **letter** is an element of I. Let $W := Mo(I)$ be the **free associative monoid (constructed on I)** [Bou73]. A **word** is an element of W. $\mathbf{1} \in W$ is the **empty word**. If $\mathbf{a} \in W$ then a is the **length** of **a**. If $\mathbf{a} \in W$ is nonempty we can uniquely write

$$\mathbf{a} = \mathbf{a}_1 \cdots \mathbf{a}_a \quad \mathbf{a}_1, \cdots, \mathbf{a}_a \in I. \tag{2.1}$$

There is also a unique **reduced expression**

$$\mathbf{a} = \overline{\mathbf{a}}_1^{n_1} \cdots \overline{\mathbf{a}}_{\overline{a}}^{n_{\overline{a}}} \text{ with } \overline{\mathbf{a}}_n \neq \overline{\mathbf{a}}_{n+1}, \text{ and } n_k > 0. \tag{2.2}$$

Let $\overline{\mathbf{a}} := \overline{\mathbf{a}}_1 \cdots \overline{\mathbf{a}}_{\overline{a}}$, $\overline{\mathbf{1}} = \mathbf{1}$ and $\overline{W} = \{\overline{\mathbf{a}} : \mathbf{a} \in W\}$ **(reduced words)**. By convention we agree that the empty word $\mathbf{1}$ corresponds to the case $a = 0$ in (2.1). The **support** $supp(\mathbf{a})$ **of the word a** is the set of indices appearing in (2.2).

Consider the family of $\mathbb{K}$-modules $\{\mathbb{K}\mathbf{a}\}_{\mathbf{a} \in W}$ and let

$$A := \bigoplus_{\mathbf{a} \in W} \mathbb{K}\mathbf{a}$$

be the coproduct of this family. The $\mathbb{K}$-module A has a $\mathbb{K}$-algebra structure defined by the **shuffle product** [Reu93]

$$\mathbf{a} \otimes \mathbf{b} \mapsto \mathbf{a} \# \mathbf{b} := \Sigma_{s \in Sh(\mathbf{a},\mathbf{b})} \mathbf{s} \quad \mathbf{a},\ \mathbf{b} \in W$$

where $Sh(\mathbf{a},\mathbf{b})$ denotes the set of shuffles of **a** and **b**, each of these shuffles taken into account with multiplicity. The **shuffle algebra (constructed on I)** is the $\mathbb{K}$-module A with the above algebra structure. For example let $I := \{\mathbf{i},\mathbf{j}\}$, then $\mathbf{iii}\#\mathbf{j} = \mathbf{jiii} + \mathbf{ijii} + \mathbf{iiji} + \mathbf{iiij}$.

The shuffle algebra A has a Hopf algebra structure defined by [Reu93]

$$\text{Coproduct: } \Delta : \mathbf{a} \mapsto \Sigma_{\mathbf{a}=\mathbf{uv}} \mathbf{u} \otimes \mathbf{v}$$

$$\text{Counit: } \varepsilon : \mathbf{a} \mapsto \delta_{a,0}$$

$$\text{Antipode: } S : \mathbf{a} \mapsto (-1)^a \mathbf{a}_a \cdots \mathbf{a}_1.$$

The **Hopf shuffle algebra (constructed on I)** is A with the above Hopf algebra structure. For example let $I := \{\mathbf{i},\mathbf{j}\}$, then $\Delta(\mathbf{iji}) = \mathbf{1}\otimes\mathbf{iji}+\mathbf{i}\otimes\mathbf{ji}+\mathbf{ij}\otimes\mathbf{i}+\mathbf{iji}\otimes\mathbf{1}$, $\varepsilon(\mathbf{iij}) = 0$, $\varepsilon(\mathbf{1}) = 1$, $S(\mathbf{ijj}) = -\mathbf{jji}$.

For $N \in \mathbb{N}$ let A_N be the associative subalgebra of the shuffle algebra A generated by all words $\mathbf{a} \in W$ of length $a \leq N$. It follows from the fact that Δ is an algebra homomorphism and S is an algebra anitmorphism that $\Delta(A_N) \subset A_N \otimes A_N$ and $S(A_N) \subset A_N$ hence A_N is a Hopf subalgebra of A.

Consider the affine groups

$$G = Hom_{\mathbb{K}}(A, -)$$

$$G_N = Hom_{\mathbb{K}}(A_N, -).$$

2.3 Lie(G) and Lie($\mathrm{G_N}$)

Let us now define the Lie algebra of an affine group. If B is a $\mathbb{K}$-algebra, a **derivation of** B is a linear map $D : B \to B$ satisfying Leibniz rule for the product, i.e.

$$D(ab) = aD(b) + bD(a), \text{ for } a,\ b \in B.$$

Let Der (B) be the set of derivations of B.

If B is a Hopf algebra, a derivation $D : B \to B$ is **left–invariant** iff

$$\Delta \circ D = (\mathrm{id}_B \otimes D) \circ \Delta.$$

Similarly, D is **right–invariant** iff

$$\Delta \circ D = (D \otimes \mathrm{id}_B) \circ \Delta.$$

Usually Lie algebras for affine groups are defined with left invariant derivations, but for the application that we have in mind it is more natural to work with right invariant derivations.

The **Lie algebra** Lie(G) of the affine group G represented by B is the $\mathbb{K}$–space of all right–invariant derivations $D : B \to B$. If D_1 and D_2 are in Lie(G), one can trivially check that the **bracket** $[D_1, D_2] = D_1D_2 - D_2D_1$ is also in Lie(G) and that Lie(G) is a Lie algebra.

This definition of Lie(G) gives the Lie algebra properties very quickly, but for computations it is much easier to work with ε–derivations. We can identify Lie(G) with the set Der $(B, \mathbb{K})$ of ε–**derivations** of B (i.e those $d \in$ Hom $(B, \mathbb{K})$ satisfying $d(\mathrm{a}\#\mathrm{b}) = \varepsilon(\mathrm{a})d(\mathrm{b}) + \varepsilon(\mathrm{b})d(\mathrm{a})$).

2.3.1 Theorem ([**Wat79**]) Let G be an affine group with representing algebra B. There is a canonical bijection between the ε–derivations Der $(B, \mathbb{K})$ and the right–invariant derivations Lie(G) given by

$$\mathrm{Der}\,(B,\mathbb{K}) \ni d \mapsto (d \otimes id) \circ \Delta \in \mathrm{Lie}(G).$$

Proof. Let $D : B \to B$ be a derivation. Then trivially $d := \varepsilon \circ D : B \to \mathbb{K}$ is an ε–derivation, indeed, for a, $b \in B$

$$\begin{aligned} \varepsilon \circ D(ab) &= \varepsilon(aD(b) + bD(a)) \\ &= \varepsilon(a)\varepsilon \circ D(b) + \varepsilon(b)\varepsilon \circ D(a), \text{ since } \varepsilon \text{ is a } \mathbb{K}\text{–algebra morphism} \\ &= \varepsilon(a)d(b) + \varepsilon(b)d(a). \end{aligned}$$

If, in addition, D is invariant then d determines D, indeed,

$$\begin{aligned} D &= (\mathrm{id}_B \otimes \varepsilon)\Delta D \\ &= (\mathrm{id}_B \otimes \varepsilon)(D \otimes \mathrm{id}_B)\Delta \\ &= (\mathrm{id}_B \otimes d)\Delta. \end{aligned}$$

Conversely, let $d : B \to \mathbb{K}$ be an ε–derivation, then it is routine to check that $D := (d \otimes \mathrm{id}_B)\Delta$ is a derivation, indeed

$$\begin{aligned} D(ab) &= (d \otimes \mathrm{id}_B)\Delta(ab) \\ &= (d \otimes \mathrm{id}_B)\Delta(a)\Delta(b) \\ &= (d \otimes \mathrm{id}_B)\Big(\Sigma_{(a)}a_{(1)} \otimes a_{(2)}\Sigma_{(b)}b_{(1)} \otimes b_{(2)}\Big) \\ &= (d \otimes \mathrm{id}_B)\Big(\Sigma_{(a),(b)}a_{(1)}b_{(1)} \otimes a_{(2)}b_{(2)}\Big) \\ &= \Sigma_{(a),(b)}d(a_{(1)}b_{(1)})a_{(2)}b_{(2)}, \end{aligned}$$

and since d is a ε–derivation,

$$\begin{aligned}
&= \Sigma_{(a),(b)}\Big(\varepsilon(a_{(1)})d(b_{(1)}) + \varepsilon(b_{(1)})d(a_{(1)})\Big)a_{(2)}b_{(2)} \\
&= \Sigma_{(a),(b)}\varepsilon(a_{(1)})d(b_{(1)})a_{(2)}b_{(2)} + \varepsilon(b_{(1)})d(a_{(1)})a_{(2)}b_{(2)} \\
&= \Sigma_{(a),(b)}\varepsilon(a_{(1)})d(b_{(1)})a_{(2)}b_{(2)} + \Sigma_{(a),(b)}\varepsilon(b_{(1)})d(a_{(1)})a_{(2)}b_{(2)} \\
&= \Sigma_{(a)}\varepsilon(a_{(1)})a_{(2)}\Sigma_{(b)}d(b_{(1)})b_{(2)} + \Sigma_{(b)}\varepsilon(b_{(1)})b_{(2)}\Sigma_{(a)}d(a_{(1)})a_{(2)},
\end{aligned}$$

and since ε is a counit for Δ in the Hopf algebra B,

$$\begin{aligned}
&= a\ \Sigma_{(b)}d(b_{(1)})b_{(2)} + b\ \Sigma_{(a)}d(a_{(1)})a_{(2)} \\
&= ad \otimes \mathrm{id}_B\Delta(b) + bd \otimes \mathrm{id}_B\Delta(a) \\
&= aD(b) + bD(a).
\end{aligned}$$

Moreover, it is easy to check that such D are actually invariant, indeed,

$$\begin{aligned}
(D \otimes \mathrm{id}_B)\Delta a &= ((d \otimes \mathrm{id}_B)\Delta \otimes \mathrm{id}_B)\Delta a \\
&= (d \otimes \mathrm{id}_B \otimes \mathrm{id}_B)(\Delta \otimes \mathrm{id}_B)\Delta a;
\end{aligned}$$

and if $\Delta(a) = \Sigma b_i \otimes c_i$, coming from the other side we have

$$\begin{aligned}
\Delta Da &= \Delta(d \otimes \mathrm{id}_B)\Delta a \\
&= \Sigma d(b_i)\Delta(c_i) \\
&= (d \otimes \mathrm{id}_B \otimes \mathrm{id}_B)(\mathrm{id}_B \otimes \Delta)\Delta(a).
\end{aligned}$$

Since B is a Hopf algebra, Δ is coassociative, hence both sides agree. □

For $\mathbf{i} \in I$ let $d_{\mathbf{i}} : A \to \mathbb{K}$ be the linear map defined by

$$d_{\mathbf{i}}(\mathbf{a}) = \begin{cases} 0 & \text{if } \mathbf{a} \neq \mathbf{i}, \\ 1 & \text{if } \mathbf{a} = \mathbf{i}. \end{cases}$$

It is routine to see that $d_{\mathbf{i}}$ is an ε–derivation; indeed, it is enough to show that for $\mathbf{a}, \mathbf{b} \in W$ we have

$$d_{\mathbf{i}}(\mathbf{a}\#\mathbf{b}) = \varepsilon(\mathbf{a})d_{\mathbf{i}}(\mathbf{b}) + \varepsilon(\mathbf{b})d_{\mathbf{i}}(\mathbf{a}).$$

If $\mathbf{a}\#\mathbf{b} = \mathbf{i}$ then, by definition of shuffle product, either $\mathbf{a} = \mathbf{i}$ and $\mathbf{b} = \mathbf{1}$ in which case $\varepsilon(\mathbf{a})d_{\mathbf{i}}(\mathbf{b}) + \varepsilon(\mathbf{b})d_{\mathbf{i}}(\mathbf{a}) = 0.0 + 1.1 = 1 = d_{\mathbf{i}}(\mathbf{a}\#\mathbf{b})$, or $\mathbf{a} = \mathbf{1}$ and $\mathbf{b} = \mathbf{i}$ in which case $\varepsilon(\mathbf{a})d_{\mathbf{i}}(\mathbf{b}) + \varepsilon(\mathbf{b})d_{\mathbf{i}}(\mathbf{a}) = 1.1 + 0.0 = 1 = d_{\mathbf{i}}(\mathbf{a}\#\mathbf{b})$.

If $\mathbf{a}\#\mathbf{b} \neq \mathbf{i}$ then $\mathbf{a}\#\mathbf{b}$ is equal to $\mathbf{1}$, a letter different from $\mathbf{i}$ or a sum of words of length > 1, in any case both sides of (2.3) are zero (by definition of ε and by definition of $d_{\mathbf{i}}$).

The corresponding right invariant derivation (see theorem 2.3.1) $D_{\mathbf{i}} := (d_{\mathbf{i}} \otimes id) \circ \Delta$ satisfies

$$D_{\mathbf{i}}(\mathbf{a}) = \begin{cases} 0 & \text{if } \mathbf{a}_1 \neq i, \\ \mathbf{a}_2 \cdots \mathbf{a}_n & \text{if } \mathbf{a}_1 = i. \end{cases} \tag{2.3}$$

It is clear from this that the associative subalgebra $\mathcal{D}$ of $End_{\mathbb{K}}(A)$ generated by $\{D_{\mathbf{i}} : \mathbf{i} \in I\}$ is a free associative algebra. Indeed, if for $\mathbf{s} = \mathbf{s}_1 \cdots \mathbf{s}_s \in W$ we define

$$D^{\mathbf{s}} = D_{\mathbf{s}_s} \cdots D_{\mathbf{s}_1}$$

then (2.3) shows that the $D^{\mathbf{s}}$'s are $\mathbb{K}$-linearly independent (if there is a $\mathbb{K}$ linear combination $\Sigma_r c_r D^{\mathbf{s}_r} = 0$, by evaluating at each $\mathbf{s}_r$ it follows that each $c_r = 0$). By Witt's Theorem [Jac62] it follows that the Lie subalgebra $L \subset gl(A)$ generated by $\{D_{\mathbf{i}} : \mathbf{i} \in I\}$ is a free Lie algebra.

So from now on we identify the free associative algebra on the alphabet I with $\mathcal{D}$ and the free Lie algebra on the alphabet I with L via identifying a letter $\mathbf{i} \in I$ with the right invariant derivation $D_{\mathbf{i}}$.

For $d \in Hom(A, \mathbb{K})$ and $k \in \mathbb{N}$ define $d_k \in Hom(A, \mathbb{K})$ by

$$d_k(\mathbf{a}) = \begin{cases} d(\mathbf{a}_1 \cdots \mathbf{a}_k), \text{ if } a = k, \\ 0, \text{ if } a \neq k. \end{cases}$$

2.3.1 Proposition Assume that the alphabet I is finite. Let $D \in \mathrm{Lie}(G)$ and let $d \in Der(A, \mathbb{K})$ be such that $D = (d \otimes id) \circ \Delta$. For $k \in \mathbb{N}$ let $D_k := (d_k \otimes id) \circ \Delta$. Then

(i) $D = \Sigma_{k \in \mathbb{N}} D_k$.

(ii) $D_k = \Sigma_{s=k} d_k(\mathbf{s}) D^{\mathbf{s}}$, in particular $D_k \in \mathcal{D}$.

(iii) D_k is a right invariant derivation of A and d_k is an ε–derivation of A.

(iv) $D_k \in L$.

Proof. (i)

$$\begin{aligned} D(\mathbf{a}) &= (d \otimes id) \circ \Delta(\mathbf{a}) \\ &= \Sigma_{k=0}^{a} d(\mathbf{a}_1 \cdots \mathbf{a}_k)\mathbf{a}_{k+1} \cdots \mathbf{a}_a \\ &= \Sigma_{k=0}^{a} d_k(\mathbf{a}_1 \cdots \mathbf{a}_k)\mathbf{a}_{k+1} \cdots \mathbf{a}_a \\ &= \Sigma_{k=0}^{a} D_k(\mathbf{a}) \\ &= \Sigma_{k \geq 0} D_k(\mathbf{a}). \end{aligned}$$

(ii)

$$\begin{aligned}D_k(\mathbf{a}) &= \Sigma_{i=0}^{a} d_k(\mathbf{a}_1\cdots\mathbf{a}_i)\mathbf{a}_{i+1}\cdots\mathbf{a}_a\\ &= d_k(\mathbf{a}_1\cdots\mathbf{a}_k)\mathbf{a}_{k+1}\cdots\mathbf{a}_a\\ &= d_k(\mathbf{a}_1\cdots\mathbf{a}_k)D^{(\mathbf{a}_1\cdots\mathbf{a}_k)}(\mathbf{a}).\end{aligned}$$

So, $D_k = \Sigma_{s\in W: s=k} d_k(\mathrm{s})D^{\mathbf{s}}$. Since the alphabet is finite, there are only finitely many words of length k hence this sum is finite and $D_k \in \mathcal{D}$.

(iii) That D_k is right–invariant is straightforward; indeed, it is enough to show that for $\mathbf{a} \in W$, $\Delta(D_k(\mathbf{a})) = (D_k \otimes \mathrm{id}_A) \circ \Delta(\mathbf{a})$,

$$\begin{aligned}(D_k \otimes \mathrm{id}_A) \circ \Delta(\mathbf{a}) &= D_k \otimes \mathrm{id}_A(\Sigma_{k=0}^{a}\mathbf{a}_1\cdots\mathbf{a}_k \otimes \mathbf{a}_{k+1}\cdots\mathbf{a}_a)\\ &= D_k(1) \otimes \mathbf{a}_1\cdots\mathbf{a}_a +\\ &\quad D_k(\mathbf{a}_1) \otimes \mathbf{a}_2\cdots\mathbf{a}_a +\\ &\quad D_k(\mathbf{a}_1\mathbf{a}_2) \otimes \mathbf{a}_3\cdots\mathbf{a}_a + \cdots +\\ &\quad D_k(\mathbf{a}_1\cdots\mathbf{a}_a) \otimes 1,\end{aligned}$$

but $D_k(\mathbf{a}) = d_k(\mathbf{a}_1\cdots\mathbf{a}_k)\mathbf{a}_{k+1}\cdots\mathbf{a}_a$, so $D_k(\mathbf{w}) = 0$, if $w < k$, hence this is equal to

$$\begin{aligned}&= D_k(\mathbf{a}_1\cdots\mathbf{a}_k) \otimes \mathbf{a}_{k+1}\cdots\mathbf{a}_a +\\ &\quad D_k(\mathbf{a}_1\cdots\mathbf{a}_k\mathbf{a}_{k+1}) \otimes \mathbf{a}_{k+2}\cdots\mathbf{a}_a +\\ &\quad D_k(\mathbf{a}_1\cdots\mathbf{a}_k\mathbf{a}_{k+1}\mathbf{a}_{k+2}) \otimes \mathbf{a}_{k+3}\cdots\mathbf{a}_a + \cdots +\\ &\quad D_k(\mathbf{a}_1\cdots\mathbf{a}_k\mathbf{a}_{k+1}\mathbf{a}_{k+2}\cdots\mathbf{a}_a) \otimes 1\\ &= d_k(\mathbf{a}_1\cdots\mathbf{a}_k) \otimes \mathbf{a}_{k+1}\cdots\mathbf{a}_a +\\ &\quad d_k(\mathbf{a}_1\cdots\mathbf{a}_k)\mathbf{a}_{k+1} \otimes \mathbf{a}_{k+2}\cdots\mathbf{a}_a +\\ &\quad d_k(\mathbf{a}_1\cdots\mathbf{a}_k)\mathbf{a}_{k+1}\mathbf{a}_{k+2} \otimes \mathbf{a}_{k+3}\cdots\mathbf{a}_a + \cdots +\\ &\quad d_k(\mathbf{a}_1\cdots\mathbf{a}_k)\mathbf{a}_{k+1}\mathbf{a}_{k+2}\mathbf{a}_{k+3}\cdots\mathbf{a}_a \otimes 1\\ &= d_k(\mathbf{a}_1\cdots\mathbf{a}_k)\Delta(\mathbf{a}_{k+1}\cdots\mathbf{a}_a)\\ &= \Delta(d_k(\mathbf{a}_1\cdots\mathbf{a}_k)\mathbf{a}_{k+1}\cdots\mathbf{a}_a)\\ &= \Delta(D_k(\mathbf{a})).\end{aligned}$$

If $\mathbf{a}, \mathbf{b} \in W$ then by comparing the terms of degree $a + b - k$ on the left and right side of

$$D(\mathbf{a}\#\mathbf{b}) = \mathbf{a}\#D(\mathbf{b}) + \mathbf{b}\#D(\mathbf{a}) \tag{2.4}$$

one sees that D_k is a derivation; indeed, the terms of degree $a+b-k$ on the left of (2.4) are

$$\mathbf{a}\#d(\mathbf{b}_1\cdots\mathbf{b}_k)\mathbf{b}_{k+1}\cdots\mathbf{b}_b+\mathbf{b}\#d(\mathbf{a}_1\cdots\mathbf{a}_k)\mathbf{a}_{k+1}\cdots\mathbf{a}_a$$

and by definition of d_k this equals to

$$\begin{aligned}&=\mathbf{a}\#d_k(\mathbf{b}_1\cdots\mathbf{b}_k)\mathbf{b}_{k+1}\cdots\mathbf{b}_b+\mathbf{b}\#d_k(\mathbf{a}_1\cdots\mathbf{a}_k)\mathbf{a}_{k+1}\cdots\mathbf{a}_a\\&=\mathbf{a}\#D_k(\mathbf{b})+\mathbf{b}\#D_k(\mathbf{a}).\end{aligned}$$

On the other hand if we expand the right hand side of (2.4) we get

$$\begin{aligned}D(\mathbf{a}\#\mathbf{b})&=d\otimes\mathrm{id}_A\circ\Delta(\mathbf{a}\#\mathbf{b})\\&=d\otimes\mathrm{id}_A(\Delta(\mathbf{a})\Delta(\mathbf{b}))\\&=d\otimes\mathrm{id}_A(\Sigma_{i=0}^{a}\mathbf{a}_1\cdots\mathbf{a}_i\otimes\mathbf{a}_{i+1}\cdots\mathbf{a}_a\Sigma_{j=0}^{b}\mathbf{b}_1\cdots\mathbf{b}_j\otimes\mathbf{a}_{j+1}\cdots\mathbf{b}_b)\\&=d\otimes\mathrm{id}_A(\Sigma_{i=0}^{a}\Sigma_{j=0}^{b}\mathbf{a}_1\cdots\mathbf{a}_i\#\mathbf{b}_1\cdots\mathbf{b}_j\otimes\mathbf{a}_{i+1}\cdots\mathbf{a}_a\#\mathbf{a}_{j+1}\cdots\mathbf{b}_b).\end{aligned}$$

Looking now at the terms of degree $a+b-k$ on this expression we get

$$\begin{aligned}&\Sigma_{h=0}^{k}d(\mathbf{a}_1\cdots\mathbf{a}_h\#\mathbf{b}_1\cdots\mathbf{b}_{k-h})\mathbf{a}_{h+1}\cdots\mathbf{a}_a\#\mathbf{b}_{k-h+1}\cdots\mathbf{b}_b\\&=\Sigma_{h=0}^{k}d_k(\mathbf{a}_1\cdots\mathbf{a}_h\#\mathbf{b}_1\cdots\mathbf{b}_{k-h})\mathbf{a}_{h+1}\cdots\mathbf{a}_a\#\mathbf{b}_{k-h+1}\cdots\mathbf{b}_b\\&=D_k(\mathbf{a}\#\mathbf{b}).\end{aligned}$$

Since the terms of degree $a+b-k$ on the left and right of (2.4) are equal it follows that

$$D_k(\mathbf{a}\#\mathbf{b})=\mathbf{a}\#D_k(\mathbf{b})+\mathbf{b}\#D_k(\mathbf{a}).$$

We have thus establish that $D_k\in\mathrm{Lie}(G)$, hence by theorem 2.3.1 d_k is an ε–derivation.

(iii) The algebra $\mathcal{D}$ being free associative admits a unique comultiplication δ [Reu93] satisfying

$$\delta(D_{\mathbf{i}})=D_{\mathbf{i}}\otimes 1+1\otimes D_{\mathbf{i}}.$$

Let $\#:A\bigotimes A\to A$ be the linear map shuffle product of the Hopf algebra A. We show that for all $D\in\mathcal{D}$

$$\#\delta(D)(x\otimes y)=D(x\#y)\quad\text{for all } x,y\in A \text{ and } \mathbf{w}\in W;\tag{2.5}$$

it is enough to show this for $D=D^{\mathbf{w}}$, $\mathbf{w}\in W$, by definition of $\mathcal{D}$. To show (2.5) for $D^{\mathbf{w}}$ we proceed by induction on the length w of $\mathbf{w}$. That $D_{\mathbf{i}}$ is a derivation of the shuffle algebra gives the beginning of the induction,

$$\#\Big(\delta(D_{\mathbf{i}})(x\otimes y)\Big)=D_{\mathbf{i}}(x\#y)\quad\text{for all } x,\ y\in A;\tag{2.6}$$

indeed,

$$\begin{aligned} D_{\mathbf{i}}(x\#y) &= x\#D_{\mathbf{i}}(y) + y\#D_{\mathbf{i}}(x) \\ &= D_{\mathbf{i}}(y)\#x + y\#D_{\mathbf{i}}(x), \text{ since } \# \text{ is commutative} \\ &= \#(D_{\mathbf{i}}(y) \otimes x) + \#(y \otimes D_{\mathbf{i}}(x)) \\ &= \#(D_{\mathbf{i}}(y) \otimes x + y \otimes D_{\mathbf{i}}(x)) \\ &= \#(\delta(D_{\mathbf{i}})(x \otimes y)). \end{aligned}$$

Trivially one shows the inductive step

$$\#\delta(D^{\mathbf{w}})(x \otimes y) = D^{\mathbf{w}}(x\#y) \quad \text{for all } x, y \in A \text{ and } \mathbf{w} \in W;$$

indeed write $D^{\mathbf{w}} = D^{\mathbf{v}}D_{\mathbf{i}}$ and assume that (2.5) holds for $D^{\mathbf{v}}$, then

$$\begin{aligned} D^{\mathbf{w}}(x\#y) &= D^{\mathbf{v}}D_{\mathbf{i}}(x\#y) \\ &= D^{\mathbf{v}}\#\Big(\delta(D_{\mathbf{i}})(x \otimes y)\Big), \text{ by (2.6)} \\ &= \#\delta(D^{\mathbf{v}})\Big(\delta(D_{\mathbf{i}})(x \otimes y)\Big), \text{ by the inductive hypothesis} \\ &= \#\delta(D^{\mathbf{v}}D_{\mathbf{i}})(x \otimes y), \text{ since } \delta \text{ is a homomorphism for the concatenation product [Reu93]} \\ &= \#\delta(D^{\mathbf{w}})(x \otimes y). \end{aligned}$$

Using (ii) we write

$$\delta(D_k) = D_k \otimes 1 + 1 \otimes D_k + \Sigma_{\substack{a+b=k \\ a<k, b<k}} c_{\mathbf{ab}} D^{\mathbf{a}} \otimes D^{\mathbf{b}}.$$

If $\mathbf{a}$ and $\mathbf{b}$ are as in the sum above then by (2.3), by the definition $D^{\mathbf{s}} = D_{s_r} \cdots D_{s_1}$ and by definition of D_k it follows that

$$\#\delta(D_k)(\mathbf{a} \otimes \mathbf{b}) = c_{\mathbf{ab}}.$$

We now show that all the $c_{\mathbf{ab}}$ are zero.

$$\begin{aligned} c_{\mathbf{ab}} &= \#\delta(D_k)(\mathbf{a} \otimes \mathbf{b}) \\ &= D_k(\mathbf{a}\#\mathbf{b}), \text{ by (2.5) applied to } D_k \in \mathcal{D} \\ &= D_k(\mathbf{a})\#\mathbf{b} + \mathbf{a}\#D_k(\mathbf{b}), \text{ since } D_k \text{ is a derivation of } A \text{ by (ii)} \\ &= 0, \text{ since } a < k,\ b < k. \end{aligned}$$

By Friederick's Theorem [Jac62] $D_k \in L$. □

2.3.2 Theorem Assume that the alphabet I is finite. Then, $\text{Lie}(G_N) \cong L/L_N$ where L_N is the ideal $\Sigma_{n>N}(L \cap A^n)$ of L (A^n is the subspace of A spanned by the words of length n).

Proof. The quotient homomorphism $^-: G \to G_N$ yields a Lie algebra homomorphism

$$^- : \mathrm{Lie}(G) \to \mathrm{Lie}(G_N)$$

such that if $D \in \mathrm{Lie}(G)$ then $\overline{D}$ is the restriction of $\overline{D}$ to A_N. This Lie algebra homomorphism is surjective because given any ε–derivation $d \in \mathrm{Lie}(G_N)$ there is an extension of d to an ε–derivation $\tilde{d} \in \mathrm{Lie}(G)$. Indeed, consider an F–basis $\{v_j\}_j$ of the vector space A_N and extend it to a basis of the vector space A. Simply define $\tilde{d} : A \to F$ as the linear map given by

$$\tilde{d} := \begin{cases} d(v_i) & \text{if } v_i \in A_N, \\ 0 & \text{if } v_i \in A - A_N. \end{cases}$$

As $\varepsilon(\mathbf{w}) = 0$ if $w > 0$ then the ε–Leibniz rule for the product holds:

$$\tilde{d}(\mathbf{a}\#\mathbf{b}) = \varepsilon(\mathbf{a})\tilde{d}(\mathbf{b}) + \varepsilon(\mathbf{b})\tilde{d}(\mathbf{a}), \text{ for } \mathbf{a},\ \mathbf{b} \in W.$$

So $\tilde{d}$ is an ε–derivation in $\mathrm{Lie}(G)$ which extends d. So $\overline{\tilde{d}} = d$ and $^-$is surjective as claimed.

By definition, L is the Lie algebra generated by the right invariant derivations $D_{\mathbf{i}} : A \to A, \mathbf{i} \in I$, hence every $D \in L$ is a right invariant derivation, since the bracket of right invariant derivations is a right invariant derivation. So $L \subset \mathrm{Lie}(G)$ and we have a homomorphism $^- : L \to \mathrm{Lie}(G_N)$ of Lie algebras. Since A_N is generated by words of length $\leq N$, the kernel of this map is precisely L_N. We now show that it is surjective. Given $x \in \mathrm{Lie}(G_N)$ choose $D \in \mathrm{Lie}(G)$ such that $\overline{D} = x$. Now part (i) of proposition 2.3.1 gives $D = \Sigma_{k \in \mathbf{N}} D_k$. Since $x \in \mathrm{Lie}(G_N)$, $x = \Sigma_{k \leq N} \overline{D}_k$. By part (iv) of the same proposition it follows that $\Sigma_{k \leq N} D_k \in L$. So, $x = \overline{\Sigma_{k \leq N} D_k}$ and $^-$ surjects $\mathrm{Lie}(G_N)$ from L.

□

Let I be finite. A **formal series** or series on the alphabet I over $\mathbb{K}$ is a map $S : W(I) \to \mathbb{K}$, where $W(I) = W$ is the free monoid on the alphabet I. As usual, we write a series as a formal infinite linear combination

$$S = \Sigma_{\mathbf{w} \in W} S(\mathbf{w})\mathbf{w}.$$

For example, the usual formal power series from complex analysis are the formal series on $I = \{i\}$ (a singleton set) over $\mathbb{K} = \mathbb{C}$, the field of complex numbers. So, in this case the formal series are the usual series $\mathbb{C}[[T]]$, where T is defined by $i \mapsto 1$, all other words to zero.

Let $\mathcal{A}(I)$ be the free associative algebra on I over $\mathbb{K}$ (so $\mathcal{A}(I) \cong A$ as $\mathbb{K}$-modules, but A has the shuffle product as an algebra and $\mathcal{A}(I)$ has the usual concatenation product as an algebra). Let $\hat{\mathcal{A}}(I)$ be its completion (i.e. $\hat{\mathcal{A}}(I)$ is the product module $\prod_{n \geq 0} A^n(I)$ with multiplication rule

$(a.b)_n = \Sigma_{i=0}^{n} a_i b_{n-i}$ [Bou75]). The free Lie algebra L on I over $\mathbb{K}$ is identified with its canonical image in $\mathcal{A}(I)$ (Witt's theorem [Jac62]). The Lie algebra of **Lie series** $\hat{L}(I)$ is the completion of $L(I)$ in $\hat{A}(I)$ [Bou75]. If we let $S \in \mathcal{A}(I)$ be a series on I over $\mathbb{K}$ and write it as sum of its homogeneous components

$$S = \Sigma_{n \geq 0} S_n$$

(if $w = n$ then $S_n(\mathbf{w}) = S(\mathbf{w})$ and if $w \neq n$ then $S_n(\mathbf{w}) = 0$). Then S is a Lie series if each S_n is a Lie element, i.e. an element of the free Lie algebra on I over $\mathbb{K}$ (with the obvious identification).

The Lie Series form a Lie algebra where the bracket is the unique possible extension of the bracket of the free Lie algebra, i.e. given two Lie series, their Lie bracket is computed as the Lie bracket of the corresponding Lie elements approximating the Lie series up to degree n.

2.3.3 Theorem Lie(G) is the algebra of Lie series on $\{D_{\mathbf{i}} : \mathbf{i} \in I\}$.

Proof. Let $D \in$ Lie(G). By proposition 2.3.1, part (i), $D = \Sigma_{n \in \mathbb{N}} D_k$. We can think of D as an element of the completion $\hat{\mathcal{D}}$ of the free associative algebra $\mathcal{D}$ on I over $\mathbb{K}$. By part (ii) of the same proposition, D_k is the homogeneous component of D of degree k, while part (iv) shows that $D_k \in L$. □

2.4 The affine group of upper triangular unipotent matrices as a quotient of G

From now on we will let our base ring $\mathbb{K}$ be the field of rational numbers $\mathbb{Q}$. Let $\mathbf{a}$, $\mathbf{u}$, $\mathbf{v} \in W$. If $\mathbf{a} = \mathbf{uv}$ then $\mathbf{u}$ is a **left factor** of $\mathbf{a}$ and $\mathbf{v}$ is a **right factor** of $\mathbf{a}$.

By the axiom of choice we can assume that I is totally ordered which in turn induces a lexicographic total order $<$ in the free monoid W. A non-empty word $\boldsymbol{\ell} \in W$ is a **Lyndon word** [Reu93] if it is smaller than all its non-trivial right factors, i.e. if $\boldsymbol{\ell} = \mathbf{uv}$, $u > 0$ and $v > 0$ then $\boldsymbol{\ell} < \mathbf{v}$.

2.4.1 Theorem ([**Rad79**]) The shuffle algebra A is a free commutative algebra over $\mathbb{Q}$ freely generated by $\{\boldsymbol{\ell} \in W : \boldsymbol{\ell}$ is a Lyndon word$\}$. □

We will now make some observations, many of them trivial, to see what the Lyndon words look like. To simplify notation assume that the alphabet has two letters, $I := \{\mathbf{i}, \mathbf{j}\}$, with $\mathbf{i} < \mathbf{j}$.
Length 0: in this case $\mathbf{w} = 1$ so $\mathbf{w}$ is not a Lyndon word by definition.
Length 1: if $\mathbf{w} = \mathbf{i}$ then $\mathbf{w}$ is a Lyndon word since it has no non-trivial right factors. Similarly, for the letter $\mathbf{j}$ (or any other letter if we had more).

Length > 1: For further reference we note that $\mathbf{w} = \mathbf{i}^n$, $n > 1$, is not a Lyndon word because by definition of "$<$" in W, $\mathbf{w} \not< \mathbf{i}^{(n-1)}$. Similarly, $\mathbf{w} = \mathbf{j}^n$ (and $\mathbf{w} = \mathbf{a}^n$ where a is any letter we might have).

A Lyndon word must start with a letter since it is non-empty. What can this letter be? If $\mathbf{w} = \mathbf{jx}$, $\mathbf{x} \in W$, $\mathbf{x} \neq \mathbf{1}$, then $\mathbf{w}$ is not a Lyndon word because

- if $\mathbf{x} = \mathbf{j}^n$, i.e. $\mathbf{w}$ does not contain any $\mathbf{i}$'s, then as noted above, $\mathbf{j}^{(n+1)}$ is not a Lyndon word;
- if $\mathbf{x} = \mathbf{x}'\mathbf{i}\mathbf{x}''$, $\mathbf{x}', \mathbf{x}'' \in W$, then $\mathbf{w} \not< \mathbf{i}\mathbf{x}''$ where $\mathbf{i}\mathbf{x}''$ is a non-trivial right factor of $\mathbf{w}$.

This also shows that if a Lyndon word $\mathbf{w}$ starts with a certain letter, then all the letters in Supp $\mathbf{w}$ must be greater or equal (in the order of the alphabet) to the first letter of the Lyndon word.

E.g.: Let $I = \{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$, $\mathbf{a} < \mathbf{b} < \mathbf{c}$ and let $\mathbf{w} = \mathbf{b}\mathbf{w}'\mathbf{a}\mathbf{w}''$, $\mathbf{w}'$, $\mathbf{w}'' \in W$. $\mathbf{w}$ is not a Lyndon word since $\mathbf{w} \not< \mathbf{a}\mathbf{w}''$, where $\mathbf{a}\ \mathbf{w}''$ is a non-trivial right factor.

A Lyndon word of length > 1 can not start with the greatest letter of the alphabet, if such a letter exists.

So, in our case (an alphabet with two letters), the Lyndon words must start with the letter $\mathbf{i}$. Let $\mathbf{w}$ be a Lyndon word (of length > 1). So, $\mathbf{w} = \mathbf{ix}, \mathbf{x} \neq \mathbf{1}, \mathbf{x} \in W$. By a case above, $\mathbf{w}$ must contain a $\mathbf{j}$ (since $\mathbf{i}^n$, $n > 1$, is not a Lyndon word). So, let

$$\mathbf{w} = \mathbf{i}^{n_1}\mathbf{j}^{m_1}\mathbf{i}^{n_2}\mathbf{j}^{m_2}\cdots\mathbf{i}^{n_k}\mathbf{j}^{m_k}, \text{ where } k >= 1, \text{ and } n_1 > 0 \text{ (it has to start with an } \mathbf{i}).$$

Then $m_k > 0$, i.e. $\mathbf{w}$ can not end in the letter $\mathbf{i}$. If not, $\mathbf{i}$ is a non-trivial right factor of $\mathbf{w}$ and $\mathbf{w} \not< \mathbf{i}$. So we can assume all m_i and n_i are > 0.

A Lyndon word of length > 1 can not end in the smallest letter of the alphabet. □

The last letter of a Lyndon word of length > 1 can not be smaller than the first letter of the word. □

A Lyndon word can not end with a sub-word with which it began. Indeed, if $\mathbf{w} = \mathbf{x}\mathbf{w}'\mathbf{x}$, $\mathbf{x}$, $\mathbf{w}' \in W$, $\mathbf{x} \neq \mathbf{1}$, then $\mathbf{w}$ is not a Lyndon word since $\mathbf{w} \not< \mathbf{x}$, where $\mathbf{x}$ is a non-trivial right factor. □

It follows that $n_1 >= n_i$, for all i. Because if $n_1 < n_i$ for some i then $\mathbf{w} \not< \mathbf{i}^{n_i}\cdots$, where $\mathbf{i}^{n_i}\ldots$ is a non-trivial right factor of $\mathbf{w}$.

E.g.: let $\mathbf{w} = \mathbf{iiijjiiiij}$ then $\mathbf{w} \not< \mathbf{iiiij}$.

So, we must add the restriction $m_i > 0$ (so as to have $n_i <= n_1$).

If $n_i = n_1$ then $m_i > m_1$. If not, $\mathbf{w} \not< \mathbf{i}_i^n\mathbf{j}_i^m\cdots$, where $\mathbf{i}_i^n\mathbf{j}_i^m\cdots$ is a non-trivial right factor of $\mathbf{w}$.

E.g.: $\mathbf{w} = \mathbf{iiiijjjiiiij}$, then $\mathbf{w} \not< \mathbf{iiiij}$.

All these conditions are necessary as we have seen. But, they are also sufficient since any such word $\mathbf{w}$ is a Lyndon word.

So, we have proved the following result.

2.4.1 Proposition If $I := \{\mathbf{i},\mathbf{j}\}$, $\mathbf{i} < \mathbf{j}$, and $\ell \in W$ is a Lyndon with $\ell > 1$ then $\ell = \mathbf{i}^{n_1}\mathbf{j}^{m_1}\mathbf{i}^{n_2}\mathbf{j}^{m_2}\cdots\mathbf{i}^{n_k}\mathbf{j}^{m_k}$, where

- $k \geq 1$,
- $n_i > 0,\ i = 1, \cdots, k$,
- $m_i > 0,\ i = 1, \cdots, k$,
- $n_1 \geq n_k$ for all k;
- if $n_k = n_1$, for some k, then $m_k > m_1$.

Moreover, if $I = \{\mathbf{i}_1, \cdots, \mathbf{i}_t\}$ then $\mathbf{i}_1\mathbf{i}_2\mathbf{i}_3\cdots\mathbf{i}_k$, for $1 \leq k \leq t$, $\mathbf{i}_k < \mathbf{i}_{k+1}$, is a Lyndon word. □

Let $n \in \mathbb{N}$. As define at the end of chapter 1, let $B = \mathbb{K}[X_{ij} \,|\, 1 \leq i < j \leq n]$ with

$$\Delta_B(X_{ij}) = X_{ij} \otimes 1 + 1 \otimes X_{ij} + \Sigma_{i<k<j} X_{ik} \otimes X_{kj}$$

and let UT_n be the **affine group of upper triangular unipotent matrices** represented by B.

2.4.2 Proposition The following gives an injective Hopf algebra map $f : B \to A$, where the alphabet $I = \{\mathbf{i}_1, \ldots, \mathbf{i}_{n-1}\}$ is finite and $\mathbf{i}_k < \mathbf{i}_{k+1}$.

$$(X_{ij}) \mapsto \begin{pmatrix} 1 & \mathbf{i}_1 & \mathbf{i}_1\mathbf{i}_2 & \mathbf{i}_1\mathbf{i}_2\mathbf{i}_3 & \cdots & \cdots & \cdots & \prod_{k=1}^{n-1}\mathbf{i}_k \\ 0 & 1 & \mathbf{i}_2 & \mathbf{i}_2\mathbf{i}_3 & \mathbf{i}_2\mathbf{i}_3\mathbf{i}_4 & \cdots & \cdots & \vdots \\ 0 & 0 & 1 & \mathbf{i}_3 & \mathbf{i}_3\mathbf{i}_4 & \mathbf{i}_3\mathbf{i}_4\mathbf{i}_5 & \cdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 1 \end{pmatrix},$$

where we mean by this the $\mathbb{K}$–algebra map which sends X_{ij} to the entry ij of the above matrix, for $1 < i < j < n$. So

$$f(X_{ij}) = \mathbf{i}_i \cdots \mathbf{i}_{j-1}.$$

.

Proof. By lemma 2.4.1 all the words $\mathbf{i}_1\mathbf{i}_2\mathbf{i}_3\dots$ where $\mathbf{i}_k < \mathbf{i}_{k+1}$ are Lyndon words. By theorem 2.4.1 this map is injective. From the definition of Δ for B and for the shuffle algebra A, it follows that this map preserves the comultiplication. Indeed, we have to show that

$$\Delta_A \circ f = f \otimes f \circ \Delta_B$$

agree. Since both sides of this identity are $\mathbb{K}$-algebra maps, it is enough to show the following.

$$\begin{aligned}\Delta_A \circ f(X_{ij}) &= \Delta_A(\mathbf{i}_i \cdots \mathbf{i}_{j-1}) \\ &= 1 \otimes \mathbf{i}_i \cdots \mathbf{i}_{j-1} + \mathbf{i}_i \otimes \mathbf{i}_{i+1} \cdots \mathbf{i}_{j-1} + \mathbf{i}_i\mathbf{i}_{i+1} \otimes \mathbf{i}_{i+2} \cdots \mathbf{i}_{j-1} + \cdots + \mathbf{i}_i\mathbf{i}_{i+1} \cdots \mathbf{i}_{j-1} \otimes 1.\end{aligned}$$

On the other hand, we have

$$\begin{aligned}f \otimes f \circ \Delta_B(X_{ij}) &= f \otimes f(1 \otimes X_{ij} + X_{ii+1} \otimes X_{i+1j} + X_{ii+2} \otimes X_{i+2j} + \cdots + X_{ij-1} \otimes X_{j-1j} + X_{ij} \otimes 1 \\ &= 1 \otimes \mathbf{i}_i \cdots \mathbf{i}_{j-1} + \mathbf{i}_i \otimes \mathbf{i}_{i+1} \cdots \mathbf{i}_{j-1} + \mathbf{i}_i\mathbf{i}_{i+1} \otimes \mathbf{i}_{i+2} \cdots \mathbf{i}_{j-1} + \cdots + \mathbf{i}_i\mathbf{i}_{i+1} \cdots \mathbf{i}_{j-1} \otimes 1.\end{aligned}$$

So $\Delta_A \circ f(X_{ij}) = f \otimes f \circ \Delta_B(X_{ij})$.

But since any map between groups preserving multiplication also preserves units and inverses, it follows that this is a Hopf algebra map (an algebra homomorphism between Hopf algebras which preserves Δ must automatically preserve the antipode and the counit, see chapter 3, section 1).

□

Let G be an affine group with representing algebra A and let F be another affine group with representing algebra B. A homomorphism $G \to F$ between affine groups is a **quotient map** if the corresponding Hopf algebra map (given by Yoneda's lemma, see chapter 3, section 1) $B \to A$ (notice the reversal of direction) is injective. The reason for this definition is that the following universal property holds [Wat79]: let $F \to G$ be a quotient of affine group schemes with kernel N. Then any affine group homomorphism $F \to G$ vanishing on N factors through G.

2.4.3 Corollary The affine group of upper triangular unipotent matrices is a quotient of G.

□

Chapter 3

The shuffle Algebra as a free commutative algebra

Let F be a field of characteristic zero which will be our base ring throughout. We show that the shuffle algebra is a free commutative algebra using the knowledge of the Lie algebras Lie(G_N) and Lie theory for G_N. Our proof does not make any use of combinatorics.

As in classical Lie theory, we will introduce the exponential map for the affine group G_N. To do this we will need a characterization of unipotence for algebraic affine groups (theorem 3.5.1), namely coconnectedness, taken from [Wat79]. In order to prove this theorem, we will give some background from affine group theory in the first three sections.

We will show that the shuffle algebra A is coconnected, hence G. and in turn G_N, will be unipotent affine groups.

If the alphabet I is finite then there are only finitely many words of length $\leq N$, hence G_N is algebraic, i.e. A_N is finitely generated. So, G_N will be an algebraic unipotent affine group to which classical Lie theory will apply.

Since Lie(G_N) is a vector space, it has the structure of a vector group. The exponential map will provide an isomorphism of algebraic sets between the vector group Lie(G_N) and the algebraic affine group $G_N(F)$. This will show that A_N is a polynomial ring since the Hopf algebra of the vector group Lie(G_N) is the polynomial ring $S(\text{Lie}(G_N))$: the symmetric algebra of the vector space Lie(G_N). In turn, this will allow us to identify polynomial functions on $G_N(F)$ with polynomial functions on Lie(G_N). Since Lie(G_N) has already been computed (cf. theorem 2.3.2), we will be able to relate the algebraically independent generators of the polynomials A_N and A_{N+1}. Finally, this will show that the Hopf shuffle algebra A is itself a polynomial ring.

3.1 Homomorphism of affine groups and closed subgroups

For future reference, let us recall the following well known result.

3.1.1 Lemma (**Yoneda**) Let $\mathcal{C}$ be a category. Let $\mathcal{F} : \mathcal{C} \to$ **Set** be a functor. Let $A \in \mathrm{Ob}(\mathcal{C})$. Let 1_A be the identity $\mathcal{C}$-morphism of A. Then, there is a bijection

$$Y : \mathrm{Nat}(\mathit{Hom}_{\mathcal{C}}(A,-),\mathcal{F}) \cong \mathcal{F}(A)$$

which sends each natural transformation $\big(\mathit{Hom}_{\mathcal{C}}(A,-),\eta,\mathcal{F}\big)$ to $\eta_A(1_A)$.

Proof. Given $x \in \mathcal{F}(A)$ we will define a natural transformation

$$\eta^x : \mathit{Hom}_{\mathcal{C}}(1_A,-) \xrightarrow{\cdot} \mathcal{F}\,.$$

Consider $R \in \mathrm{Ob}(\mathcal{C})$ and define a function

$$\begin{aligned} \eta^x_R : \mathrm{Hom}_{\mathcal{C}}(A,R) &\longrightarrow \mathcal{F}(R) \\ (A \xrightarrow{\lambda} R) &\longmapsto \mathcal{F}(\lambda)(x). \end{aligned}$$

Let $R_1 \xrightarrow{f} R_2 \in \mathrm{Mor}(\mathcal{C})$. We will show that the following rectangle commutes.

$$\begin{tikzcd}
R_1 \arrow[d, "f"] & \mathit{Hom}_{\mathcal{C}}(A,R_1) \arrow[r, "\eta_{R_1}"] \arrow[d, "f_*"] & \mathcal{F}(R_1) \arrow[d, "\mathcal{F}(f)"] \\
R_2 & \mathit{Hom}_{\mathcal{C}}(A,R_2) \arrow[r, "\eta_{R_2}"] & \mathcal{F}(R_2)
\end{tikzcd}$$

If $A \xrightarrow{\lambda} R_1 \in \mathit{Hom}_{\mathcal{C}}(A,R_1)$, then

$$\mathcal{F}(f) \circ \eta^x_{R_1}(\lambda) = \mathcal{F}(f)(\mathcal{F}(\lambda)(x)) = \mathcal{F}(f \circ \lambda)(x)$$
$$\eta^x_{R_2} \circ \mathit{Hom}_{\mathcal{C}}(A,f)(\lambda) = \eta^x_{R_2}(f \circ \lambda) = \mathcal{F}(f \circ \lambda)(x).$$

Hence, $\eta^x \in \mathrm{Nat}(\mathit{Hom}_{\mathcal{C}}(A,-),\mathcal{F})$. Define a function

$$\begin{aligned} \mathcal{F}(A) &\xrightarrow{\Psi} \mathrm{Nat}(\mathit{Hom}_{\mathcal{C}}(A,-),\mathcal{F}) \\ x &\longmapsto \eta^x. \end{aligned}$$

Consider a natural transformation $\eta : \mathit{Hom}_{\mathcal{C}}(A,-) \xrightarrow{\cdot} \mathcal{F}$. Then $\eta_A(1_A)$ is an element of $\mathcal{F}(A)$. Define a function

$$\begin{aligned} \mathrm{Nat}(\mathit{Hom}_{\mathcal{C}}(A,-),\mathcal{F}) &\xrightarrow{\Phi} \mathcal{F}(A) \\ \eta &\longmapsto \eta_A(1_A). \end{aligned}$$

If $x \in \mathcal{F}(A)$, then

$$\Phi \circ \Psi(x) = \Phi(\eta^x) = \eta^x_A(1_A) = \mathcal{F}(1_A)(x) = 1_{\mathcal{F}(A)}(x) = x.$$

If $\eta \in \mathrm{Nat}(Hom_{\mathcal{C}}(A,-), \mathcal{F})$, then

$$\Psi \circ \Phi(\eta) = \Psi(\eta_A(1_A)) = \eta^{\eta_A(1_A)}.$$

We show that $\eta^{\eta_A(1_A)} = \eta$. Let $R \in \mathrm{Ob}(\mathcal{C})$. Let $\lambda : A \to R$ be a $\mathcal{C}$-homomorphism. Then,

$$\eta_R(\lambda) = \eta_R(\lambda \circ 1_A \circ 1_A) = \eta_R(Hom_{\mathcal{C}}(1_A, \lambda)(1_A)) =$$

since η is a natural transformation

$$= \mathcal{F}(\lambda)(\eta_A(1_A)) = \eta_R^{\eta_A(1_A)}(\lambda).$$

Let $Y = \Phi$. □

3.1.2 Corollary Let $\mathbf{F-Alg}$ be the category of F-algebras. Let $A, B \in \mathrm{Ob}(\mathbf{F-Alg})$. Let

$$Hom_{\mathbf{F-Alg}}(B,-) : \mathbf{F-Alg} \to \mathbf{Set}$$

be the hom-functor. Let 1_A be the identity $\mathbf{F-Alg}$-morphism of A. Then, there is a bijection

$$Y : \mathrm{Nat}(Hom_{\mathbf{F-Alg}}(A,-), Hom_{\mathbf{F-Alg}}(B,-)) \cong Hom_{\mathbf{F-Alg}}(B, A)$$

which sends each natural transformation $\Big(Hom_{\mathbf{F-Alg}}(A,-), \eta, Hom_{\mathbf{F-Alg}}(B,-)\Big)$ to $\eta_A(1_A)$.

Proof. Let $\mathcal{F} := Hom_{\mathbf{F-Alg}}(B,-)$. By 3.1.1 the result follows. □

Let G and H be affine groups with representing algebras $F[G] = A$ and $F[H] = B$ respectively. A **homomorphism of affine groups** is a natural transformation $\Phi : G \to H$, i.e. for each $F-$algebra R, $G(R) \to H(R)$ is natural group homomorphism. By Yoneda's lemma such maps correspond to algebra homomorphisms $B \to A$, but since each $G(R) \to H(R)$ is a group homomorphism, it is trivial to check that such natural transformations correspond to *Hopf* algebra homomorphisms $B \to A$. Indeed, let $f : B \to A$ be the F–algebra homomorphism corresponding, by Yoneda's lemma, to Φ. Then, for any F–algebra R and any $g,\ h \in G(R)$ we have $\Phi_R(gh) = \Phi_R(g)\Phi_R(h)$. So, if we denote by μ_R the multiplication in R,

$$\mu_R \circ g \otimes h \circ \Delta_A \circ f = \mu_R \circ (g \circ f) \otimes (h \circ f) \circ \Delta_B,$$

in particular, letting $R = A\bigotimes A$ and $g : a \mapsto a \otimes 1$, $h : a \mapsto 1 \otimes a$, $a \in A$, be the canonical injections, then

$$\mu_{A\bigotimes A} \circ g \otimes h \circ \Delta_A = \mu_{A\bigotimes A} \circ (g \circ f) \otimes (h \circ f) \circ \Delta_B.$$

Since $\mu_{A\bigotimes A} \circ g \otimes h = \mathrm{id}_{A\bigotimes A}$ this gives

$$\Delta_A \circ f = f \circ \Delta_B,$$

i.e. f preserves the comultiplication. From $\Phi_R(1_{G(R)}) = 1_{H(R)}$ it follows, letting $R = F$ that

$$\Phi_F(1_{G(F)}) = 1_{H(F)}.$$

But from chapter 1 we know that $1_{G(F)} = \varepsilon_A$ and $1_{H(F)} = \varepsilon_B$, and

$$\varepsilon_A \circ f = \varepsilon_B.$$

Hence f preserves counits. From $\Phi_R(g^{-1}) = \Phi_R(g)^{-1}$ it follows that, if S_A and S_B are the corresponding antipodes,

$$g \circ S_A \circ f = g \circ f \circ S_B.$$

Hence for $R = A$ and $\mathrm{id}_A \in G(A)$ we get

$$S_A \circ f = f \circ S_B,$$

hence f preserves the antipode. It follows that f is a Hopf algebra map.

Now suppose that $f : B \to A$ is an F-algebra morphism between the two Hopf algebras B and A that it is assumed to preserve only the comultiplication. Let $\Phi : G \to H$ be the corresponding (by Yoneda) natural set transformation. We show that for each F-algebra R, $\Phi_R : G(R) \to G(H)$ is a group homomorphism, which will imply that f must preserve that antipode and the counit also, so that f will be a Hopf algebra morphism. Indeed, we know that

$$f \otimes f \circ \Delta_B = \Delta_A \circ f.$$

Let g, $h \in G(R)$ then

$$\begin{aligned}
\Phi_R(gh) &= \Phi_R(\mu_R \circ g \otimes h \circ \Delta_A) \\
&= \mu_R \circ g \otimes h \circ \Delta_A \circ f \\
&= \mu_R \circ g \otimes h \circ f \otimes f \circ \Delta_B \\
&= \mu_R \circ (g \circ f) \otimes (h \circ f) \circ \Delta_B \\
&= \Phi_R(g)\Phi_R(h).
\end{aligned}$$

Hence Φ_R is a group homomorphism and Φ is an affine group morphism. Since a group homomorphism automatically preserves the unit and the inverses then $\Phi_R(1_{G(F)}) = 1_{H(F)}$ and $\Phi_R(g^{-1}) = \Phi_R(g)^{-1}$. Hence, we have that $\varepsilon_A \circ f = \varepsilon_B$ and $S_A \circ f = f \circ S_B$, and so f is a Hopf algebra morphism.

For example, the determinant of an invertible matrix over R gives an affine group homomorphism det : $\mathrm{GL}_n \to G_m$ and the corresponding Hopf algebra map is

$$\begin{array}{rcl}\det: \ F[X] & \longrightarrow & F[X_{11}, \cdots, X_{nn}, 1/\det] \\ X & \longmapsto & \det(X_{11}, \cdots, X_{nn}).\end{array}$$

Let H' and G be affine groups represented by B' and A respectively. Let $\psi : H' \to G$ be a homomorphism. If the corresponding Hopf algebra map $A \to B'$ is surjective, we call ψ a **closed embedding**. It is then an isomorphism of H' onto a **closed subgroup** H of G represented by a Hopf algebra B (isomorphic to B') which is a quotient of A, i.e. H is defined by the polynomial equations defining G together with some additional ones. For example, SL_n is a closed subgroup of GL_n.

From the definitions of the Hopf shuffle algebra A and of A_N, for $N, M \in \mathbb{N}$ $N \leq M$, it follows that the following diagram commutes, where the arrows are inclusions.

$$\begin{tikzcd}
A_N \arrow[dd] \arrow[dr] & \\
& A \\
A_M \arrow[ur] &
\end{tikzcd}$$

Given any compatible family $\{f_N : A_N \to B\}_{N \in \mathbb{N}}$ of Hopf algebra morphims, there is a unique Hopf algebra homorphism $f : A \to B$, since $A = \bigcup_N A_N$, and for $N, M \in \mathbb{N}$, $N \leq M$, the following diagram commutes.

$$\begin{tikzcd}
A_N \arrow[dd] \arrow[dr] \arrow[drr, "f_N"] & & \\
& A \arrow[r, "f"] & B \\
A_M \arrow[ur] \arrow[urr, "f_M"'] & &
\end{tikzcd}$$

So A, with the inclusions $A_N \to A$, $N \in \mathbb{N}$, as canonical injections, is the inductive limit in the category of Hopf algebras of the system $\{A_N, i_M^N\}_{N,M \in \mathbb{N}, N \leq M}$ where $i_M^N : A_N \to A_M$ is the inclusion morphism:

$$A = \varinjlim A_N.$$

The inclusion $i_M^N : A_N \to A_M$, $N \leq M$, which is a Hopf algebra morphism, induces by Yoneda a morphism of affine group schemes $q_N^M : G_M \to G_N$, $N \leq M$. This simply means that for any F–algebra R, $q_N^M(R) : G_M(R) \to G_N(R)$ is the group homomorphism given by sending any $(g : A_M \to R) \in G_M(R)$ to its restriction $g/_{A_N} : A_N \to R$. Similarly, the inclusion $A_N \to A$ induces a quotient homomorphism of affine group schemes $q_N : G \to G_N$. Since the category of Hopf algebras is contra–equivalent to the category of affine groups schemes we have the following proposition.

3.1.3 Proposition The affine group scheme G, with the quotients $q_N : G \to G_N$, $N \in \mathbb{N}$, as canonical projections, is the inverse limit in the category of affine group schemes of the system $\{G_N, q_N^M\}_{N,M \in \mathbb{N}, N \leq M}$,

$$G \cong \varprojlim G_N.$$

Proof. Let H be an affine group scheme represented by a Hopf algebra B. Suppose that there is a family of affine group homomorphisms $H \to G_N$, $N \in \mathbb{N}$, such that for $N \leq M$ the following diagram commutes.

$$\begin{tikzcd}
G_N & \\
& H \arrow[ul] \arrow[dl] \\
G_M \arrow[uu, "q_N^M"] &
\end{tikzcd} \tag{3.1}$$

Hence, by Yoneda's lemma, there is a corresponding commutative diagram in the category of Hopf algebras with the arrows reversed.

$$\begin{tikzcd}
A_N \arrow[dr] \arrow[dd] & \\
& B \\
A_M \arrow[ur] &
\end{tikzcd}$$

Since $A = \varinjlim A_N$ in the category of Hopf algebras, the above diagram can be completed to the following.

$$\begin{tikzcd}
A_N \arrow[dd] \arrow[dr] \arrow[drr] & & \\
& A \arrow[r] & B \\
A_M \arrow[ur] \arrow[urr] & &
\end{tikzcd}$$

Going back to the category of affine group schemes, diagram (3.1) can be completed to the following commutative diagram.

$$\begin{tikzcd}
G_N & & \\
& G \arrow[ul, "q_N"'] \arrow[dl, "q_M"] & H \arrow[l] \arrow[ull] \arrow[dll] \\
G_M \arrow[uu, "q_N^M"] & &
\end{tikzcd}$$

So, $(G, \{q_N\}_{N\in\mathbb{N}})$ is the projective limit of the system $\{G_N, q_N^M\}_{N,M\in\mathbb{N},N\leq M}$. □

3.2 Comodules of Hopf algebras

A $\mathbb{F}$**–group functor** is a functor from the category of $\mathbb{F}$–algebras into the category of groups (not necessarily affine, i.e. representable).

Let G be a group functor and let V be an F–vector space. For each F–algebra R define

$$\mathrm{GL}_V(R) = \mathrm{Aut}_R(V \bigotimes R),$$

this defines a group functor. A **linear representation** of G on V is a homomorphism $G \to \mathrm{GL}_V$. If V is finite dimensional, then in any fixed basis automorphisms correspond to invertible matrices, and linear representations are maps to GL_n where $n = \dim_F V$.

Let us look at the following Hopf algebra equivalent of a linear representation of an affine group.

3.2.1 Proposition Let G be an affine group represented by A. Then linear representations of G on V correspond to F–linear maps $\rho : V \to V \otimes A$ such that the following diagrams commute.

$$\begin{tikzcd}
V \arrow[r, "\rho"] \arrow[d, "\rho"'] & V \bigotimes A \arrow[d, "\mathrm{id}_V \otimes \Delta"] \\
V \bigotimes A \arrow[r, "\rho \otimes \mathrm{id}_A"'] & V \bigotimes A \bigotimes A
\end{tikzcd}
\qquad
\begin{tikzcd}
V \arrow[r, "\rho"] \arrow[d, "\mathrm{id}_V"'] & V \otimes A \arrow[d, "\mathrm{id}_V \otimes \epsilon"] \\
V \arrow[r, "\cong"] & V \otimes F
\end{tikzcd}$$

□

Proof. Let Φ be a representation. For $\mathrm{id}_A \in G(A)$ we get an A–linear map $\Phi(\mathrm{id}_A) : V \bigotimes A \to V \bigotimes A$ which is determined by its restriction to $V \cong V \bigotimes_F F$. We call this restriction ρ. Let $f : R_1 \to R_2$ be an F–algebra map. Then the naturality of Φ means that the following rectangle commutes.

$$\begin{tikzcd}
R_1 \arrow[d, "f"] & G(R_1) \arrow[r, "\Phi_{R_1}"] \arrow[d, "G(f)"'] & \mathrm{Aut}_{R_1}(V \bigotimes R_1) \arrow[d, "\mathrm{GL}_V(f)=(\mathrm{id}_V \otimes f)(-)"] \\
R_2 & G(R_2) \arrow[r, "\Phi_{R_2}"'] & \mathrm{Aut}_{R_2}(V \bigotimes R_2)
\end{tikzcd}$$

Let $g : A \to R \in G(R)$ for some F–algebra R. Then the following rectangle commutes.

$$\begin{tikzcd}
A \arrow[d, "g"] & G(A) \arrow[r, "\Phi_A"] \arrow[d, "G(f)"'] & \mathrm{Aut}_A(V \bigotimes A) \arrow[d, "\mathrm{GL}_V(g)=(\mathrm{id}_V \otimes g)(-)"] \\
R & G(R) \arrow[r, "\Phi_R"'] & \mathrm{Aut}_R(V \bigotimes R)
\end{tikzcd}$$

Hence, evaluating at $\mathrm{id}_A \in G(A)$,

$$\mathrm{GL}_V(g) \circ \Phi_A(\mathrm{id}_A) = \Phi_R \circ G(g)(\mathrm{id}_A).$$

Note that $G(g)(\mathrm{id}_A) = g \circ \mathrm{id}_A = g$, so

$$\mathrm{GL}_V(g) \circ \Phi_A(\mathrm{id}_A) = \Phi_R(g),$$

and restricting these two maps to V we get

$$(\mathrm{id}_V \otimes g) \circ \rho = \Phi_R(g)/V.$$

That is, Φ is determined by ρ. Since ε is the unit of the group $G(R)$ and Φ_R is an action then $\Phi_R(\varepsilon)v = v$ for all $v \in V$, hence $(\mathrm{id}_V \otimes \varepsilon) \circ \rho = \mathrm{id}_V$ and the second diagram commutes; also for any g, $h \in G(R)$ we have $\Phi_R(g)\Phi_R(h) = \Phi_R(gh)$, and hence if we denote the multiplication of R by μ_R we see that

$$\mathrm{id}_V \otimes g \circ (\rho \otimes \mathrm{id}_R) \circ \mathrm{id}_V \otimes h \circ \rho = \Big(\mathrm{id}_V \otimes \big((g \otimes h) \circ \Delta\big)\Big) \circ \rho$$

$$(\mathrm{id}_V \otimes (\mu_R \circ g \otimes h)) \circ (\rho \otimes \mathrm{id}_A) \circ \rho = (\mathrm{id}_V \otimes (\mu_R \circ g \otimes h)) \circ (\mathrm{id}_V \otimes \Delta) \circ \rho.$$

In particular, setting $R = A \bigotimes A$ and letting $g : a \mapsto a \otimes 1$, $h : a \mapsto 1 \otimes a$ be the canonical injections, it follows that $\mathrm{id}_V \otimes (g \otimes h) = \mathrm{id}_{V \bigotimes A \bigotimes A}$, so we get

$$\mathrm{id}_{V \bigotimes A \bigotimes A} \circ (\rho \otimes \mathrm{id}_A) \circ \rho = \mathrm{id}_{V \bigotimes A \bigotimes A} \circ (\mathrm{id}_V \otimes \Delta) \circ \rho$$

$$(\rho \otimes \mathrm{id}_A) \circ \rho = (\mathrm{id}_V \otimes \Delta) \circ \rho,$$

and the first diagram commutes.

Conversely, for any $\rho : V \to V \bigotimes A$ such that both diagrams commute we obtain a natural set map $\phi : G(R) \to \mathrm{End}_R(V \bigotimes R)$ by defining $\Phi(g) := (\mathrm{id}_V \otimes g) \circ \rho$. From the commutativity of the first diagram it follows that $\Phi(g)\Phi(h) = \Phi(gh)$ and from the second one it follows that $\varepsilon = 1_{G(R)}$ acts like the identity. □

Such a vector space V with an F-linear map $\rho : V \to V \bigotimes A$ satisfying $(\mathrm{id}_V \otimes \varepsilon)\rho = \mathrm{id}_V$ and $(\mathrm{id}_V \bigotimes \Delta)\rho = (\rho \otimes \mathrm{id}_A)\rho$ is called an **A–comodule**. An important example to be used in the linearization theorem of algebraic groups is $V = A$ with $\rho = \Delta$, whose corresponding representation is the **regular representation.**

A subspace W of V is a **subcomodule** if $\rho(W) \subset W \bigotimes A$, or equivalently if $G(R)$ maps $W \otimes R$ to itself.

3.3 Algebraic groups as matrix groups

3.3.1 Proposition Every comodule V for a Hopf algebra A is locally finite.

Proof. Let $v \in V$. We show that v is contained in a finite dimensional subcomodule. Let $\{a_i\}$ be an F-basis of A and let

$$\rho(v) = \Sigma v_i \otimes a_i,$$

where all but finitely many v_i are zero. Let

$$\Delta(a_i) = \Sigma r_{ijk} a_j \otimes a_k.$$

Then,

$$\Sigma\rho(v_i) \otimes a_i = (\rho \otimes \mathrm{id}_A)\rho(v) = (\mathrm{id}_V \otimes \Delta)\rho(v) = \Sigma v_i \otimes r_{ijk} a_j \otimes a_k.$$

Comparing the coefficients of a_k we get $\rho(v_k) = \Sigma v_i \otimes r_{ijk} a_j$. Hence the subspace W spanned by v and v_i is a finite dimensional subcomodule. □

An affine group is **algebraic** iff its representing algebra is finitely generated. We have the following linearization theorem which shows that any possible multiplication for an algebraic affine group is just matrix multiplication.

3.3.1 Theorem Every algebraic affine group G over a field F is isomorphic to a closed subgroup of some GL_n.

Proof. Let A be the Hopf algebra representing the given algebraic affine group. Then A is a comodule with $\rho = \Delta$. By proposition 3.3.1, there is a finite–dimensional subcomodule V

of A containing finitely many algebra generators of A. Let $\{v_j\}$ be a basis of V, and write $\Delta(v_j) = \Sigma v_i \otimes a_{ij}$. Consider the Hopf algebra map

$$F[X_{11}, \cdots, X_{nn}, 1/\det] \to A$$

corresponding (by Yoneda's lemma) to the regular representation of G. The image of this map contains the a_{ij}, images of X_{ij}. But $v_j = (\varepsilon \otimes id_A)\Delta(v_j) = \Sigma\varepsilon(v_i)a_{ij}$, so the image contains V and hence is all of A. □

Whenever we want to make sense of a concept for the affine group G represented by the Hopf shuffle algebra A, we can look at the algebraic affine groups G_N since G is an inverse limit of these algebraic affine groups, or equivalently, the Hopf shuffle algebra A is an inductive limit of the finitely generated A_N. And by the above linearization theorem, we should always look at matrices first.

3.4 Unipotent matrices

We want to define an exponential map for certain affine groups, so let us look at a version of nilpotence which makes sense for elements of a matrix group. A matrix $g \in \mathrm{GL}_n(F)$ is **unipotent** if $g - 1$ is nilpotent, i.e. all eigenvalues of g are 1. In order to motivate the definition of unipotent affine group let us look at a classical theorem from group theory which is the precise analogue of Engel's Theorem for Lie algebras.

3.4.1 Theorem **(Lie–Kolchin fixed point theorem)** Let G be a subgroup of $\mathrm{GL}_n(F)$ such that all its elements are unipotent. Then in some basis all elements of G are unipotent upper triangular matrices (that is, zero below the diagonal and 1 on the diagonal). □

3.4.1 Remark This is a fixed point theorem because it is enough to have some $v_1 \neq 0 \in F^n$ fixed by all $g \in G$. Indeed, if such a fixed point exists then G acts by unipotent maps on F^n/Fv_1. If $v \in F^n$ let $[v] = v + F^n \in F^n/Fv_1$. By induction on the dimension there is a basis $[v_2], \cdots, [v_n]$ of the quotient with each $g[v_{i+1}] - [v_{i+1}]$ lying in $k[v_2] + \cdots + k[v_i]$. Hence every g in G is strictly upper triangular in the basis $v_1, \cdots, v_n$.

By the above remark we see that to prove the theorem all we need is a fixed point. A system of linear equations on v_1

$$(g-1)v_1 = 0, \; g \in G$$

has a non zero solution in F^n iff it has a non-zero solution in its algebraic closure $\overline{F}^n$. So it can be assumed that F is algebraically closed. Let W be a non-zero subspace of minimal dimension mapped to itself by G and denote by $\mathrm{Tr}(f)$ the trace of an endomorphism f of W. An application of Schur's lemma to an irreducible subspace of $\{f \in \mathrm{End}_F(W) : \mathrm{Tr}(gf) = 0, \text{ for all } g \in G\}$ gives the existence of a fixed point. The details can be found in [Wat79].

3.5 Unipotent affine groups

The above fixed point theorem suggests how to define unipotence for an arbitrary affine group. An affine group is **unipotent** iff every non–zero linear representation has a non–zero **fixed vector** $v \in V$, i.e. for the corresponding comodule

$$\rho(v) = v \otimes 1,$$

hence for any $g \in G(R)$, $g.v = v$.

Let us recall from chapter 1 the affine group of upper triangular unipotent matrices (that is, upper triangular with 1's on the diagonal) $\mathbf{U_n(F)}$ which is an algebraic affine group with representing algebra $F[X_{ij} : i < j]$ whose Hopf algebra structure is defined by

$$\begin{aligned}
&\delta(X_{ij}) = X_{ij} \otimes 1 + 1 \otimes X_{ij} + \Sigma_{i<k<j} X_{ik} \otimes X_{kj} \\
&\varepsilon(X_{ij}) = \delta_{ij}, \text{ where } \delta_{ij} \text{ is the Kronecker delta} \\
&\eta(X_{ij}) = (-1)^{i+j} \det(M_{ji}).
\end{aligned}$$

Geometrically, we think of $\mathrm{U}_n(F)$ as the subgroup of automorphisms of F^n preserving the complete flag $\{V_i\}$ where V_i is the span of the standard basis vectors $e_1, \cdots, e_i$, and acting as the identity on the successive quotients V_{i+1}/V_i.

3.5.1 Theorem Let G be an algebraic affine group. The following are equivalent.

1. G is unipotent.

2. In any closed embedding of G in GL_n, some element of $\mathrm{GL}_n(F)$ conjugates G to a closed subgroup of the affine group of upper triangular unipotent matrices U_n.

3. G is isomorphic to a closed subgroup of some U_n.

4. The Hopf algebra A representing G is **coconnected**, i.e. there is a chain of subspaces $C_0 \subset C_1 \subset C_2 \subset \cdots$ with $C_0 = F$ and $\bigcup C_r = A$ such that $\Delta(C_r) \subset \Sigma_0^r C_i \bigotimes C_{r-i}$.

The proof of this theorem will be included for the sake of completeness.

Proof. The Lie–Kolchin fixed point Theorem shows that 1. implies 2. Theorem 3.3.1 gives 2. implies 3.

We now show that 3. implies 4. It is enough to show 4. for U_n. Indeed let A be the representing algebra of U_n. Since G is a closed subgroup of U_n hence its representing algebra is a Hopf algebra quotient A/I and taking images of the C_i shows that 4. holds for the quotient A/I.

Let $j-i$ be the weight of $X_{ij} \in A$, so that a monomial $\prod X_{ij}^{n_{ij}}$ has weight $\Sigma n_{ij}(j-i)$. Let C_m be the span of the monomials of weight $\leq m$. Then $C_0 = F$ and $A = \bigcup C_m$, and also we have $C_iC_j \subset C_{i+j}$. We just need to show that $\Delta(C_m) \subset \Sigma C_i \bigotimes C_{m-i}$, which follows by direct checking for the X_{ij}. Inductively, if it holds for monomials P, Q of weights r, s respectively, we have $\Delta(PQ) = \Delta(P)\Delta(Q)$ lying in

$$(\Sigma C_i \bigotimes C_{r-i})(\Sigma C_j \bigotimes C_{s-j}) \subset \Sigma(C_iC_j \bigotimes C_{r-i}C_{s-j}) \subset \Sigma C_{i+j} \bigotimes C_{r+s-i-j}.$$

Finally, assume 4. and let $\rho : V \to V \bigotimes A$ give a comodule. Let $V_r = \{v \in V : \rho(v) \in V \bigotimes C_r\}$. Then, $V = \bigcup V_r$. If $0 \neq v$ is in V_0, then $\rho(v)$ has the form $v' \otimes 1$, and applying ε we see that $v' = v$, so that v is a fixed point. So it is enough to show that $V_r = 0$ would imply $V_{r+1} = 0$. We have $\rho(V_{r+1}) \subset V \bigotimes C_{r+1}$, and so $(\mathrm{id}_V \bigotimes \Delta)\rho(V_{r+1}) \subset V \bigotimes \Sigma C_i \bigotimes C_{r+1-i}$. Hence V_{r+1} goes to 0 in the induced map down to $V \bigotimes A/C_r \bigotimes A/C_r$. But the map $(\mathrm{id}_V \bigotimes \Delta) \circ \rho$ is equal to $(\rho \otimes id_A) \circ \rho$, since ρ is a comodule. We have $V \to V \bigotimes A/C_r$ injective since $V_r = 0$, and again applying $\rho \bigotimes id_A$ we have $V \to (V \bigotimes A/C_r) \bigotimes A/C_r$ injective. Hence $V_{r+1} = 0$. □

3.5.1 Observation Let G be a not necessarily algebraic affine group with representing algebra A. If A is coconnected then G is unipotent.

Proof. In the proof of the above theorem, the fact that the representing algebra is finitely generated was not used to show that 4. implies 1. □

3.5.2 Proposition The affine group G represented by the Hopf shuffle algebra A is unipotent.

Proof. Let A^n be the subspace of A spanned by the words of length n. Define $C_i = \bigoplus_{n=0}^{i} A^n$. Clearly, the C_i form a chain of subspaces

$$C_0 \subset C_1 \subset C_2 \subset \cdots,$$

$C_0 = F$ and $\bigcup C_r = A$. Also, by definition of the comultiplication of the Hopf shuffle algebra it follows that $\Delta(C_r) \subset \Sigma_0^r C_i \bigotimes C_{r-i}$, hence A is coconnected and G is unipotent. □

3.5.3 Proposition Any quotient of a unipotent affine group is unipotent.

Proof. Let G be a unipotent affine group with representing algebra A. Let H be a quotient of G represented by a Hopf algebra B. Then, there exists an injective Hopf algebra morphism $B \to A$. Let R be an F–algebra. If V is a comodule for B then it is a comodule for A where $g \in G(R)$ acts on V as the restriction g/B. Since G is unipotent, then V has a fixed point which is also a fixed point for the action of H on V. Then H is unipotent. □

3.5.4 Corollary G_N is unipotent.

Proof. The representing algebra A_N of G_N is a sub Hopf algebra of the Hopf shuffle algebra A. So, G_N is a quotient of the unipotent affine group G represented by the Hopf Shuffle algebra. Hence G_N is unipotent by the above proposition. □

3.5.5 Corollary Assume that the alphabet I is finite. Then A_N is an integral domain.

Proof. Since the alphabet is finite there are only finitely many words of length $\leq N$. hence A_N is finitely generated. So G_N is a unipotent algebraic affine group over a field of characteristic zero, and hence G_N is connected as an affine group, i.e. A_N modulo its nilradical is an integral domain [Wat79]. But by Cartier's Theorem (loc. cit.), Hopf algebra over fields of characteristic zero are reduced. □

3.6 Lie Theory for G_N

3.6.1 Observation Let K be a Q–algebra. Let x be a nilpotent element of K. Define

$$EXP(x) = 1 + \frac{x}{1} + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} + \cdots.$$

Then, $EXP(x+y) = EXP(x)EXP(y)$ if x, y are nilpotents elements which commute.

Let u be a unipotent element of K (i.e. $1-u$ is nilpotent). Define

$$LOG(u) = -\frac{1-u}{1} - \frac{(1-u)^2}{2} - \cdots - \frac{(1-u)^n}{n} - \cdots.$$

If x is nilpotent then $EXP(x)$ is unipotent and $LOG(EXP(x)) = x$. If u is unipotent then $LOG(u)$ is nilpotent and $EXP(LOG(u)) = u$. □

Assume that the alphabet I is finite. Then there are only finitely many words of length $\leq N$, hence G_N is algebraic, i.e. A_N is finitely generated. In particular, Lie(G_N) is finite dimensional.

In chapter 1 we saw that given any finite dimensional vector space V, the group $(V, +)$ is an algebraic group with the symmetric algebra on the dual of V, $S(V^\circ)$, as its algebra of polynomial maps. Let us view the vector space $\mathrm{Lie}(G_N)$ as a vector group where the polynomial functions are the polynomials in the elements of the dual vector space $\mathrm{Lie}(G_N)^\circ$.

For any linear functional $x \in \mathrm{Hom}_F(A_N, F)$ let

$$r(x) = (x \otimes \mathrm{id}_{A_N}) \circ \Delta.$$

If we identify $A_N \bigotimes F = A_N = F \bigotimes A_N$, then $r(x) \in \mathrm{End}_F(A_N)$.

By corollary 3.5.4 and theorem 3.5.1 it follows that A_N is coconnected, so there is a chain of subspaces $C_0 \subset C_1 \subset C_2 \subset \cdots$ with $C_0 = F$ and $\bigcup C_r = A_N$ such that $\Delta(C_r) \subset \Sigma_0^r C_i \bigotimes C_{r-i}$.

We now show that for any ε–derivation $d : A_N \to F$, $r(d)$ is locally nilpotent on A_N. Actually, $r(d)(C_r) \subset C_{r-1}$. Indeed

$$\begin{aligned}(d \otimes \mathrm{id}_{A_N}) \circ \Delta(C_r) &\subset d \otimes \mathrm{id}_{A_N}(\Sigma_0^r C_i \bigotimes C_{r-i})\\ &= \Sigma_{i=0}^r d(C_i) C_{r-i}\\ &= d(C_0) C_r + \Sigma_{i=1}^r d(C_i) C_{r-i},\end{aligned}$$

and since $C_0 = F$,

$$\begin{aligned}&= \Sigma_{i=1}^r d(C_i) C_{r-i}\\ &\subset C_{r-1}.\end{aligned}$$

Since $r(d)(C_0) = 0$, if $a \in C_r$ then $r(d)^{r+1}(a) = 0$. Consequently, $EXP(r(d)) = \Sigma_{n>0} \frac{r(d)^n}{n!}$ is a well defined F–automorphism of A_N for every $d \in \mathrm{Lie}(G_N)$. By theorem 2.3.1, since d is an ε–derivation then $r(d)$ is a derivation. So, $EXP(r(d))$ is an F–algebra endomorphism of A, hence $\varepsilon \circ EXP(r(d))$ is an element of the group $G_N(F)$. Let

$$exp(d) := \varepsilon \circ EXP(r(d)).$$

Assume that F is algebraically closed. We now show that $exp : \mathrm{Lie}(G_N) \to G_N(F)$ is a polynomial map, i.e. that $\mathrm{Pol}(G_N(F)) \circ exp \subset \mathrm{Pol}(\mathrm{Lie}(G_N))$. Let $f : G_N(F) \to F \in \mathrm{Pol}(G_N(F))$. The algebra A_N is finitely generated and with no nilpotents (actually it is a domain by corollary 3.5.5). By theorem 1.6.1 f is evaluation at an element $a \in A_N$: $f = \mathrm{Eva}(a)$. Since $A_N = \bigcup C_r$, assume that $a \in C_r$ for some $\mathbf{r} \in \mathbb{N}$ then

$$\begin{array}{rl}\mathrm{Eva}(a) \circ exp : \ \mathrm{Lie}(G_N) & \longrightarrow F\\ d & \longmapsto \varepsilon \circ \Sigma_{i=0}^{\mathbf{r}} \frac{l(d)^i}{i!}(a)\end{array}$$

is an element of Pol(Lie(G_N)). This means the following: let $\{X_1, \cdots, X_s\}$ be an F-basis for Lie(G_N), the dual basis of which gives coordinates for the vector group Lie(G_N). Write

$$d = \Sigma_t X_t^\circ(d) X_t, \tag{3.2}$$

so the coordinates of an element d in the vector group are $(X_t^\circ(d))_{1<t<s}$. Replacing with (3.2) in $\varepsilon \circ \Sigma_{i=0}^{r} \frac{l(d)^i}{i!}(a)$ and recalling that ε vanishes on every word of length ≥ 1, it follows that this expression is a polynomial in the coordinate functions $(X_t^\circ(-))_{1<t<s}$.

Let $g \in G_N(F)$. Then $\mathrm{id}_{A_N} - r(g)$ is locally nilpotent on A_N because $(\mathrm{id}_{A_N} - r(g))(C_r) \subset C_{r-1}$ and $(\mathrm{id}_{A_N} - r(g))(C_0) = 0$. Indeed, if $a \in C_r$ then

$$\begin{aligned} \mathrm{id}_{A_N}(a) - r(g)(a) &= a - g \otimes \mathrm{id}_{A_N}(a) \\ &\subset a - g(1)a - \Sigma_0^r g(C_i) C_{r-i} \\ &= -\Sigma_{i=1}^r g(C_i) C_{r-i} \\ &\subset C_{r-1} \end{aligned}$$

and since $(\mathrm{id}_{A_N} - r(g))(F) = 0$ then $(\mathrm{id}_{A_N} - r(g))(a)^{r+1} = 0$. It follows that $LOG(r(g)) = -\Sigma_{n>0} \frac{(\mathrm{id}_A - r(g))^n}{n}$ is an element of $\mathrm{End}_F(A_N)$ which clearly is locally nilpotent on A_N. Following an idea of Gerhard P. Hochschild we now show that $LOG(r(g))$ is a derivation. Consider the polynomial ring $A_N[T]$ and the formal power series ring $A_N[[T]]$. For $x \in A_N$ consider the formal power series for the exponential,

$$EXP(xT) = \Sigma_{n \geq 0} \frac{x^n}{n!} T^n.$$

Given elements a and b in A_N, there is a positive integer m such that $LOG(r(g))^{m+1}$ annihilates a, b, and the shuffle product $a \# b$, since $LOG(r(g))$ is locally nilpotent on A_N. Then, if c is any of these elements, we have

$$EXP(LOG(r(g))(c)T) = \Sigma_{n=0}^{m} \frac{LOG(r(g))^n(c)}{n!} T^n.$$

Hence the formal power series

$$EXP(LOG(r(g))(a \# b)T) - EXP(LOG(r(g))(a)T) EXP(LOG(r(g))(b)T) \in A_N[[T]]$$

is actually a polynomial $p(T) \in A_N[T]$. From the calculus of formal power series we know that $EXP(x_1 T + x_2 T) = EXP(x_1 T) EXP(x_2 T)$ and that $EXP(LOG(r(g))(x)) = r(g)(x)$, for x_1, x_2, $x \in A_N$. For every natural number n, write $nLOG(r(g))(x) = LOG(r(g))(x) + \cdots +$

$LOG(r(g))(x)$, then we have

$$\begin{aligned} EXP(nLOG(r(g))(x)) &= EXP(LOG(r(g))(x) + \cdots + LOG(r(g))(x)) \\ &= EXP(LOG(r(g))(x)). \cdots .EXP(LOG(r(g))(x)), \text{ n times} \\ &= r(g)^n(x). \end{aligned}$$

By a direct computation it follows that if g is an F-algebra homomorphism from $A_N \to F$ then $r(g)$ is an F-algebra endomorphism of A_N. Let $n \in \mathbb{N}$, then $p(n) = r(g)^n(a\#b) - r(g)^n(a)\#r(g)^n(b) = 0$. Hence the polynomial $p(T)$ has infinitely many roots (i.e. all the natural numbers) which implies that every coefficient of it is zero. Equating the coefficient of T to zero it follows that

$$LOG(r(g))(a\#b) = LOG(r(g))(a)b + aLOG(r(g))(b),$$

and thus $LOG(r(g))$ is indeed a derivation of A_N. Therefore $\varepsilon \circ LOG(r(g))$ is an ε-derivation and belongs to Lie(G_N). Let

$$log(g) := \varepsilon \circ LOG(r(g)).$$

We now show that $log : G_N(F) \to \text{Lie}(G_N)$ is a polynomial map, i.e. that $\text{Pol}(\text{Lie}(G_N)) \circ log \subset \text{Pol}(G_N(F))$. Let $f : \text{Lie}(G_N) \to F \in \text{Pol}(\text{Lie}(G_N))$. Let $\{X_1, \cdots, X_s\}$ be the Lie elements in the free Lie algebra L on the alphabet I over F of degree $\leq N$. By theorem 2.3.2, these Lie elements form an F-basis of Lie(G_N). So, any polynomial map in Lie(G_N) is a polynomial on the dual basis $\{X_1^\circ, \cdots, X_s^\circ\}$. Since $A_N = \bigcup C_r$, assume that all these Lie elements $\{X_1, \cdots, X_s\} \subset C_r$ for some $\mathbf{r} \in \mathbb{N}$. It is enough to look at $f = X_i^\circ$, for $1 \leq i \leq s$ since the X_i° generate the algebra of polynomial maps Pol(Lie(G_N)) and a polynomial of polynomial maps is a polynomial map since Pol(Lie(G_N)) is an algebra. Then

$$\begin{aligned} X_i^\circ \circ log :\ G_N(F) &\longrightarrow F \\ g &\longmapsto \varepsilon \circ -\Sigma_{t>0}^{\mathbf{r}} \frac{(\text{id}_{A_N} - l(g))^t}{t}(X_i) \end{aligned}$$

is an element of Pol(Lie(G_N)) and hence log is a polynomial map. This simply means the following: any set of algebra generators of A_N provides coordinate functions for the algebraic group $G_N(F)$ by theorem 1.6.1, i.e. if $\{\mathbf{w}_k\}_k$ are the words of length $\leq N$ which generate A_N then the coordinates of $g \in G_N(F)$ are $(g(\mathbf{w}_k))_k$. So a set of coordinate functions for the algebraic group $G_N(F)$ are $\{eva(\mathbf{w}_k)\}_k$ where $eva(\mathbf{w}_k)(g) = g(\mathbf{w}_k)$. Expanding $\varepsilon \circ -\Sigma_{t>0}^{\mathbf{r}} \frac{(\text{id}_{A_N} - l(g))^t}{t}(X_i)$ and recalling that ε vanishes on words of length ≥ 1 it follows that this is a polynomial in the coordinates of $G_N(F)$ $\{eva(\mathbf{w}_k)\}_k$.

For example, let $I = \{\mathbf{a}, \mathbf{b}\}$, and look at A_2. Let us use the Hall basis for the free Lie algebra, so we know that $\mathrm{Lie}(G_2) = F\mathbf{a} + F\mathbf{b} + F[\mathbf{a}, \mathbf{b}]$. Let $X_1 = \mathbf{a}$, $X_2 = \mathbf{b}$, $X_3 = [\mathbf{a}, \mathbf{b}] = \mathbf{ab} - \mathbf{ba}$. Let $g \in G_2(F)$. Then,

$$\begin{aligned}
X_1^\circ \circ \log(g) &= g(\mathbf{a}), \text{ so } X_1^\circ \circ \log = eva(\mathbf{a}).\\
X_2^\circ \circ \log(g) &= g(\mathbf{b}), \text{ so } X_2^\circ \circ \log = eva(\mathbf{b}).\\
X_3^\circ \circ \log(g) &= g(\mathbf{ab}) + g(\mathbf{a})g(\mathbf{b}) - g(\mathbf{ba}) - g(\mathbf{b})g(\mathbf{a}) = g(\mathbf{ab}) - g(\mathbf{ba})\\
&= g(\mathbf{ab} - \mathbf{ba}), \text{ so } X_3^\circ \circ \log = eva(\mathbf{ab} - \mathbf{ba}).
\end{aligned}$$

From formal properties of the power series for the exponential and the logarithm it follows that the polynomial maps

$$exp : \mathrm{Lie}(G_N) \to G_N \text{ and } log : G_N \to \mathrm{Lie}(G_N)$$

are mutually inverse of each other; indeed, first we observe that for any linear functional $x \in \mathrm{Hom}_F(A_N, F)$

$$\varepsilon \circ r(x) = x, \tag{3.3}$$

because if $a \in A_N$ writing $\Delta(a) = \Sigma b_i \otimes c_i$ we have

$$\begin{aligned}
\varepsilon(r(x))(a) &= \varepsilon \circ (x \otimes id_{A_N})(\Sigma b_i \otimes c_i)\\
&= \varepsilon(\Sigma x(b_i)c_i)\\
&= \Sigma x(b_i)\varepsilon(c_i)\\
&= x(\Sigma b_i \otimes \varepsilon(c_i))\\
&= x(a), \text{ since } \varepsilon \text{ is a counit for the Hopf algebra } A_N.
\end{aligned}$$

Let $g \in G_N(F)$ then

$$\begin{aligned}
exp(log(g)) &= exp(\varepsilon \circ LOG(r(g)))\\
&= \varepsilon \circ EXP\Big(r(\varepsilon \circ LOG(r(g)))\Big)\\
&= EXP\Big(\varepsilon \circ r(LOG(\varepsilon \circ r(g)))\Big), \text{ since } \varepsilon \text{ is an } F\text{–algebra homomorphism}\\
&= EXP(LOG(g)) \text{ by (3.3)}\\
&= g, \text{ by formal properties of EXP and LOG.}
\end{aligned}$$

Similarly, let $d \in \mathrm{Lie}(G_N)$

$$\begin{aligned} log(exp(d)) &= log(\varepsilon \circ EXP(r(d))) \\ &= \varepsilon \circ LOG\Big(r(\varepsilon \circ EXP(r(d)))\Big) \\ &= LOG\Big(\varepsilon \circ r(EXP(\varepsilon \circ r(d)))\Big), \text{ since } \varepsilon \text{ is an } F\text{–algebra homomorphism} \\ &= LOG(EXP(d)) \text{ by (3.3)} \\ &= d, \text{ by formal properties of EXP and LOG.} \end{aligned}$$

So, we have proved the following result.

3.6.1 Theorem Let F be an algebraically closed field of characteristic zero and let the alphabet I be finite. The map sending each ε–derivation $d \in \mathrm{Lie}(G_N)$ onto the element $exp(d) \in G_N(F)$ is an isomorphism of affine algebraic F–sets from $\mathrm{Lie}(G_N)$ to $G_N(F)$. The inverse of which is given by the map sending each $g \in G_N(F)$ onto the element $log(g) \in \mathrm{Lie}(G_N)$. □

3.7 The Hopf shuffle algebra A as a polynomial ring

3.7.1 Theorem Let F be a field of characteristic zero and let the alphabet I be finite. Then the Hopf shuffle algebra A is a free commutative algebra over F.

Proof.

First we prove the theorem assuming that the field F is algebraically closed.

Consider the algebra A_N which is finitely generated and with no nilpotents. Then, by theorem 1.6.1, we can identify A_N with the algebra of polynomial maps of the algebraic group $G_N(F)$ of F–algebra homomorphisms from A_N to F,

$$A_N \cong \mathrm{Pol}_F(G_N(F)). \tag{3.4}$$

Recall from theorem 1.6.1 that this identification simply means "an element a in A_N is the polynomial function on $G_N(F)$ evaluation at a". By theorem 3.6.1, the exponential map is an isomorphism of algebraic F–sets, hence we can identify

$$\mathrm{Pol}_F(G_N(F)) \cong \mathrm{Pol}_F(\mathrm{Lie}(G_N)). \tag{3.5}$$

From the identifications (3.4) and (3.5), and because $\mathrm{Pol}_F(\mathrm{Lie}(G_N))$ is a polynomial ring by definition of a vector group it follows that A_N is a polynomial ring.

By theorem 2.3.2 Lie(G_N) can be identified with the subspace of L spanned by the Lie elements of degree $\leq N$, if we take the brackets modulo degree$(N+1)$, i.e.

$$\text{Lie}(G_N) \cong L/L_N,$$

where L_N is the ideal $\Sigma_{n>N}(L \cap A^n)$ of L (A^n is the subspace of A spanned by the words of length n). Suppose that L has an F–basis $\{X_j\}_{j \in \mathbb{N}}$. Then the X_j of degree $\leq N$ form an F–basis of Lie(G_N). The dual of which, say $\{X_1^\circ, \cdots, X_r^\circ\}$, is an algebraically independent set of generators for the polynomial algebra Pol$_F($Lie$(G_N))$ since Lie(G_N) is a vector group. The identification (3.5) means that the functional $X_j^\circ :$ Lie$(G_N) \to F$, $1 \leq j \leq r$, goes to

$$G_N(F) \xrightarrow{\log} \text{Lie}(G_N) \xrightarrow{X_j^\circ} F$$

which is a polynomial map on G_N "evaluation at Y_j" for some $Y_j \in A_N$. So, if $\{X_1, \cdots, X_r\}$ are the Lie elements of a basis for L of degree $\leq N$ then A_N is a commutative free algebra on the corresponding elements $\{Y_j\}_j \subset A_N$, i.e.

$$A_N = F[Y_1, \cdots, Y_r].$$

Let B be a commutative F–algebra and let $\phi : \{Y_j\}_{j \in \mathbb{N}} \to B$ be a set map. Then $\phi/ : \{Y_1, \cdots, Y_r\} \to B$ extends to an algebra map $\phi_N : A_N \to B$. Note that the following diagram is commutative where the horizontal arrow is the inclusion.

$$\begin{tikzcd}
A_N \arrow[rr, hook] \arrow[dr, "\phi_N"'] & & A_{N+1} \arrow[dl, "\phi_{N+1}"] \\
& B &
\end{tikzcd}$$

Since $A = \varinjlim A_N$ the family $\{\phi_N\}_{N \in \mathbb{N}}$ gives a unique algebra map $\tilde{\phi} : A \to B$ extending ϕ, by the universal property of $\varinjlim A_N$. This finishes the proof of the theorem for the case of an algebraic closed field F.

Now suppose that F is a field of characteristic zero (not necessarily algebraically closed). Let $\{X_j\}_{j \in \mathbb{N}}$ be an F–basis of L. Extending scalars to an algebraic closed field $\overline{F}$ containing F, we see, by what we have just proved, that for the $\overline{F}$–basis $\{1 \otimes X_j\}_{j \in \mathbb{N}}$ of $\overline{F} \bigotimes_F L$ there is a free generating set $\{Y_j\}_{j \in \mathbb{N}}$ of $\overline{F} \bigotimes_F A$ over $\overline{F}$. The theorem now follows from the following proposition.

3.7.1 Proposition Let $k \subset K$ be a tower of fields. Let $A = \bigoplus_{n \geq 0} A^n$ be a graded k–algebra. If $K \bigotimes_k A$ is a polynomial ring over K then A is a polynomial ring over k.

Proof. Consider the k–vector space $V = \bigoplus_{n\geq 1} A^n / \bigoplus_{n\geq 2} A^n$ and its symmetric algebra $S(V)$. We show that $A \cong S(V)$ as k–algebras.

Let $\{\overline{X_j}\}_{j\in J}$ be a k–basis of V. The k–linear map

$$\begin{aligned} f:\ V &\longrightarrow A \\ \overline{X_j} &\longmapsto X_j \end{aligned}$$

extends, by the universal property of the symmetric algebra, to a k–algebra map $S(f) : S(V) \to A$ which we will show is a k–linear isomorphism. It is enough to show that $S(f)^n : S(V)^n \to A^n$ is a k–linear isomorphism.

The grading of A induces a compatible grading in the extension

$$K \bigotimes_k A = \bigoplus_{n\geq 0} (K \bigotimes_k A^n).$$

Since $K \otimes_k A \cong S(K \otimes_k V)$ as K–algebras then $K \otimes_k S(f) : K \otimes_k S(V) \to K \otimes_k A$ is a homogeneous K–algebra isomorphism. In particular, $(K \otimes_k S(f))^n : K \otimes_k S(V)^n \to K \otimes_k A^n$ is a K–linear isomorphism. Since we are tensoring over a field, this happens iff $S(f)^n : S(V)^n \to A^n$ is a k–linear isomorphism. □

Bibliography

[Bou73] N. Bourbaki, *Algebra I*, Addison–Wesley, Reading, Massachusetts, 1973.

[Bou75] N. Bourbaki, *Groupes et Algèbres de Lie*, Hermann, Paris, 1975.

[BP96] Y. Billig and A. Pianzola, *Free groups of Lie type*, Comp. Rend. Math. Acad. Sci. Canada **18** (1996), 159–162.

[BP97] Y. Billig and A. Pianzola, *Free Kac–Moody groups and their Lie algebras*, Preprint, 1997.

[EM53] S. Eilenberg and S. MacLane, *On the embedding of rings in skew fields*, Annals of Mathematics **58** (1953), 55–106.

[Hoc81] G. P. Hochschild, *Basic theory of algebraic groups and Lie algebras*, Springer–Verlag, New York, 1981.

[Jac62] N. Jacobson, *Lie algebras*, Dover publications, New York, 1962.

[Lyn54] R. C. Lyndon, *On Burnside's problem*, Transactions of the American Mathematical Society **77** (1954), 202–15.

[Lyn55] R. C. Lyndon, *On Burnside's problem II*, Transactions of the American Mathematical Society **78** (1955), 329–32.

[Mac50] S. MacLane, *Cohomology of abelian groups*, International Congress of Mathematicians, Proceedings **2** (1950), 8–14.

[Pia] A. Pianzola, *Free group functors*, Jour. Pure and Appl. Alg. To appear.

[Rad79] D. E. Radford, *A natural ring basis for the shuffle algebra and an application to group schemes*, Journal of algebra **58** (1979), 432–54.

[Ree58] R. Ree, *Lie elements and an algebra associated with shuffles*, Annals of Mathematics **68** (1958), 210–220.

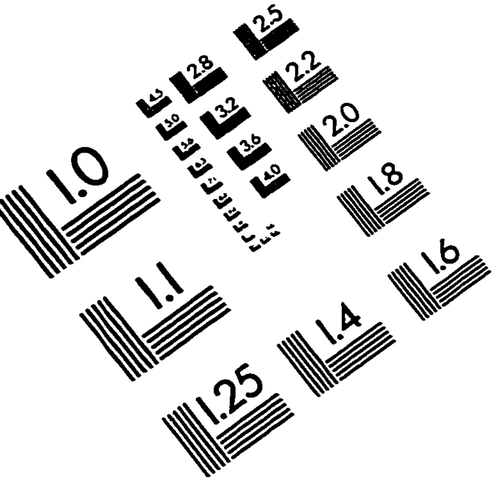
[Reu93] C. Reutenauer, *Free Lie algebras*, London Math. Soc. Monographs 7, Clarendon Press, Oxford, 1993.

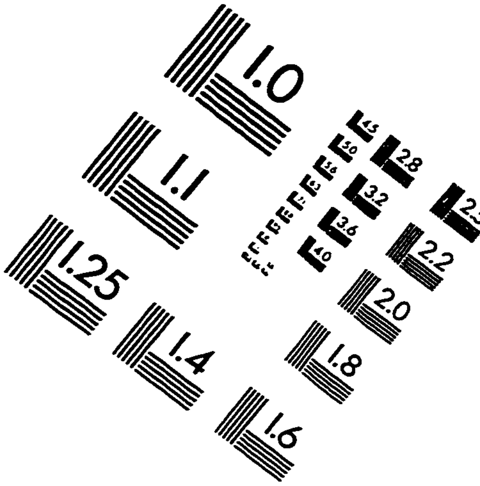
[Swe69] M. Sweedler, *Hopf algebras*, Benjamin, New York, 1969.

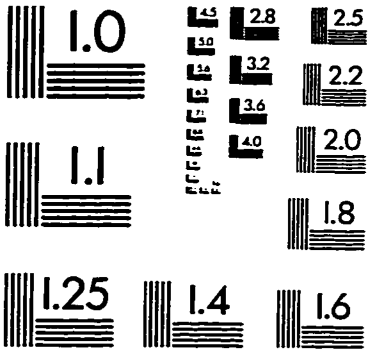
[Wat79] W. C. Waterhouse, *Introduction to affine group schemes*, GTM 66, Springer Verlag, New York, 1979.

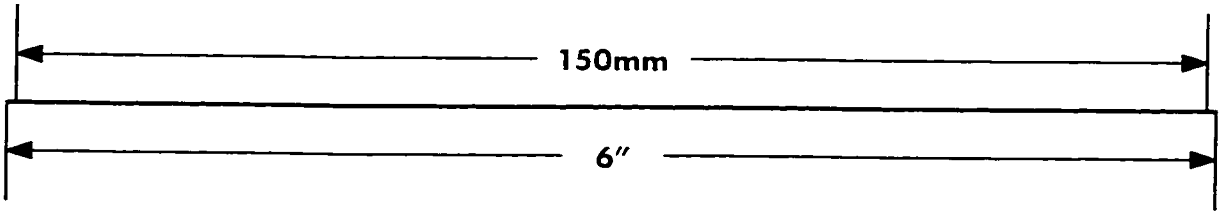
Index

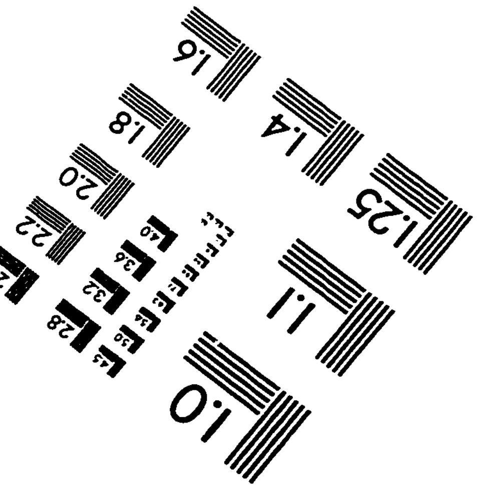
IMAGE EVALUATION TEST TARGET (QA-3)

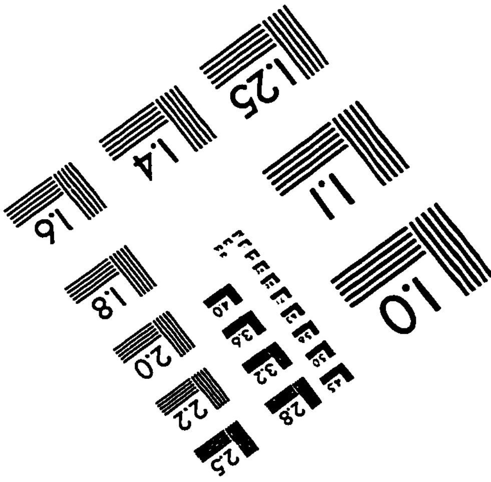












APPLIED IMAGE . Inc
1653 East Main Street
Rochester, NY 14609 USA
Phone: 716/482-0300
Fax: 716/288-5989