Lie Groups: Fall 2025 Lecture V: Free Lie Algebras, Completions, and the Formal Baker-Campbell-Hausdorff Formula

October 1, 2025

1 Free (Non-Associative) Algebras and Free Lie Algebras

Definition 1.1. By an *algebra* (over K) we mean a K-vector space V with a multiplication, which is a K-linear map $\mu\colon V \otimes_K V \to V$. A map of algebras is a K-linear map preserving the multiplications.

Let S be a set. (We are primarily interested in the case when S has cardinality 2.) By induction on $i \geq 1$ we define sets S_i. We begin with $S_1 = S$. Given S_i for $i < n$. we define $S_n = \coprod_{i+j=n;i,j\geq 1} S_i \times S_j$. Using a multiplicative notation we can view S_n as all expressions that are a composition of ordered binary products of pairs of elements. Fox example, $S_2 = \{(x \cdot y)\}$ for $x, y \in S_1$. S_3 has two types of elements: those of the form $(x_1 \cdot (x_2 \cdot x_3))$ and those of the form $((x_1 \cdot x_2) \cdot x_3)$ for $x_1, x_2, x_3 \in S$. S_4 has the following types of elements:

$$\begin{aligned} S_1 \times S_3 :&\quad (x_1 \cdot ((x_2 \cdot x_3) \cdot x_4)), (x_1 \cdot (x_2 \cdot (x_3 \cdot x_4))) \\ S_2 \times S_2 :&\quad ((x_1 \cdot x_2) \cdot (x_3 \cdot x_4)) \\ S_3 \times S_1 :&\quad (((x_1 \cdot x_2) \cdot x_3) \cdot x_4), ((x_1 \cdot (x_2 \cdot x_3)) \cdot x_4) \end{aligned}$$

We set $S_\infty = \coprod_{n=1}^{\infty} S_n$, and we denote by $F(S)$ to be the K-vector space generated by S_∞. The multiplication of $x \in S_i$ and $y \in S_j$ is the element $(x \cdot y) \in S_i \times S_j \subset S_{i+j}$. We extend this multiplication on the basis elements S_∞ by bilinearity to a multiplication on $F(S)$. The freeness of $F(S)$ is captured in the following property.

Lemma 1.2. *Given an algebra A and a set function $\psi\colon S \to A$, There is a unique extension of the function of ψ to a map of algebras $\hat{\psi}\colon F(S) \to A$.*

Proof. Exercise. □

The grading on S_∞ induces a grading on $F(S)$ making $F(S)$ a graded algebra.

Definition 1.3. Let S be a set. The *free Lie algebra generated by* S, denoted $FL(S)$, is the quotient of $F(S)$ by the two-sided ideal generated by $Q(a.a) = a \cdot a$ and $J(a,b,c) = a \cdot (b \cdot c) + c \cdot (a \cdot b) + b \cdot (c \cdot a)$ for $a, b, c \in S$. The Lie bracket on $FL(S)$ is given by $[\overline{a}, \overline{b}] = \overline{(a \cdot b)}$ for $a, b \in F(S)$ and $\overline{a}$ and $\overline{b}$ their images in $FL(S)$. Clearly, the relations imposed in forming the quotient $FL(S)$ imply that with this definition of bracket it is a Lie algebra. Since the relations are homogeneous with respect to the grading on $F(S)$, there is an induced grading on $FL(S)$ that makes it a graded Lie algebra.

Each element of S_∞ maps in the quotient to a legitimate expression of iterated brackets in the Lie algebra generated by $FL(S)$. The fact that it is a free Lie algebra generated by S is the content of the next proposition.

Proposition 1.4. *Given a Lie algebra L and a set function $\varphi\colon S \to L$, there is a unique extension of φ to a homomorphism of Lie algebras $\hat{\varphi}\colon FL(\varphi)\colon FL(S) \to L$.*

Proof. First use the universal property of $F(S)$ to define an algebra map $F(\varphi)\colon F(S) \to L$ extending $S \to L$ and sending the product in $F(S)$ to the bracket in L. Then notice that the generators of the two-sided ideal $Q(a,a)$ and $J(a,b,c)$ map to zero in L since L is a Lie algebra. This implies that $F(\varphi)$ factors through the quotient $FL(S)$, and thus defines a Lie algebra homomorphism $FL(\varphi)\colon FL(S) \to L$. Uniqueness of the extension is clear since S generates $F(S)$ and hence $FL(S)$. □

2 The Universal Enveloping Algebra $U(FL(S))$

Since $FL(S)$ is a Lie algebra, it has a universal enveloping algebra, $U(FL(S))$ with co-muiltiplication as defined in Proposition 2.9 of Lecture 4. Like all universal enveloping algebras is it a associative, co-associative, co-commutative bi-algebra with a unit and co-unit. In this case giving $U(FL(S))$ the grading coming from the grading on S_∞ both the multiplication and the co-multiplication preserve the grading. Also, as established in Proposition 2.13 in Lecture 4 the space of primitive elements of the co-multiplication c is the subspace $FL(S) \subset U(FL(S))$.

In this case, we understand the algebra structure on $U(FL(S))$. Denote by $T(S)$ the tensor algebra on the K vector space with basis S. As we have

seen this is the free associative algebra (with unit) generated by S meaning that if A is any associative algebra with unit and $S \to A$ is a set function, then there is a unique unital algebra map $T(S) \to A$ extending the given map $S \to A$. The tensor algebra $T(S)$ has a multiplicative grading by setting the elements of S to be homogeneous of degree 1. This is the usual grading on $T(S)$

Proposition 2.1. *Let S be a set.*

1. *The inclusion $S \to T(S)$ extends uniquely to a map of Lie algebras $\psi_S \colon FL(S) \to T(S)$, where the Lie algebra structure on $T(S)$ is the $XY - YX$ bracket $T(S)$. This map preserves the gradings.*

2. *The map ψ_S extends uniquely to a map of associative algebras*

$$\hat{\psi}_S \colon U(FL(S)) \to T(S).$$

   This map also preserves the gradings

3. *The map $\hat{\psi}_S$ is an isomorphism of graded, associative algebras and identifies the universal enveloping algebra $U(FL(S))$ with the tensor algebra $T(S)$.*

Proof. By the universal property of the free Lie algebra $FL(S)$, the inclusion of $S \to T(S)$ extends uniquely to a Lie algebra homomorphism $\psi_S \colon FL(S) \to T(S)$, when $T(S)$ is equipped with the $XY - YX$ bracket. This map preserves the gradings. By the universal property of $U(FL(S))$, this map extends uniquely to an algebra homomorphism $\hat{\psi}_S \colon U(FL(S)) \to T(S)$. The relation imposed on $T(FL(S))$ to form the universal enveloping algebra are homogeneous in the induced grading on $T(FL(S))$. Thus, there is an induced grading on $U(FL(S))$. The map $\hat{\psi}$ preserves the gradings and is the identity on the natural inclusions of S into $U(FL(S))$ and into $T(S)$.

On the other hand, the universal property of $T(S)$ implies that the inclusion $S \to U(FL(S))$ extends to an algebra homomorphism $\rho_S \colon T(S) \to U(FL(S))$. Both $\rho_S \circ \hat{\psi}_S$ and $\hat{\psi}_S \circ \rho_S$ are the identity on S and hence by the uniqueness part of the universal properties of $T(S)$ and $U(FL(S))$ both compositions are the identity. Thus, they are inverse isomorphisms and each preserves the gradings. □

This gives us a complete understanding of $U(FL(S))$. As an algebra it is isomorphic to $T(S)$ commuting with the inclusions of S into each as the generators. This embeds $FL(S) \subset T(S)$. For example, for $X, Y \in S$ we

have $[X,Y] \mapsto X \otimes Y - Y \otimes X$. Any iterated bracket of elements of S maps in a similar way and can be computed by induction. Both $FL(S)$ and $T(S)$ are graded and this inclusion preseres the grading.

In addition the co-multiplication $c\colon U(FL(S)) \to U(FL(S)) \otimes U(FL(S))$ satisfies $c(X) = X \otimes 1 + 1 \otimes X$ for all $X \in S$, so that under this identification the co-multiplication for $U(FL(S))$ is identified with the usual co-multiplication of the tensor algebra $T(S)$.

3 Formal completions of $T(S))$ and $FL(S)$

The reason for introducing the completions of the universal enveloping algebra $T(S)$ and the Lie algebra $FL(S)$ is so that our power series will have meaning, without having to worry about convergence issues. Indeed, in this algebraic context no convergence is possible without completing.

Define a decreasing filtration $\mathcal{F}^n(T(S)) = \oplus^{k \geq n} T^k(S)$. This is a decreasing filtration given by the powers of the ideal $F^1(T(S))$. We form the completion $\widehat{T(S)}$ of $T(S)$ with respect to the powers of this ideal. Then $\widehat{T(S)} = \prod_{n=0}^{\infty} T^n(S))$ with the topology being the product topology of the discrete topologies on each factor. We let $\widehat{FL(S)}$ be the closure of $FL(S) \subset T(S)$ in $\widehat{T(S)}$. Since $FL(S) = \oplus_{n \geq 1} FL^n(S)$ where $FL^n(S) = FL(S) \cap T^n(S)$,

$$\widehat{FL(S)} = \prod_{n=0}^{\infty} FL^n(S)$$

with the product topology.

Corollary 3.1. *Let $B^n(S) = \oplus_{i+j=n} T^i(S) \otimes T^j(S)$ and set $\widehat{B(S)} = \prod_{n \geq 0} B^n(S)$ with the product topology. The co-multiplication of $T(S)$ induces a continuous map $\hat{c}\colon \widehat{T}(S) \to \widehat{B(S)}$ defined by*

$$\hat{c}(\sum_{n \geq 0} a_n) = \sum_{n \geq 0} c(a_n).$$

Set

$$\delta'(\sum_{n \geq 0} a_n) = \sum_{n \geq 0} a_n \otimes 1$$

and

$$\delta''(\sum_{n \geq 0} a_n) = \sum_{n \geq 0} 1 \otimes a_n.$$

These are continuous maps of $\widehat{T(S)} \to \widehat{B(S)}$. *An element* $\sum_n a_n$ *is primitive for* $\hat{c}$, *i.e.,*

$$\hat{c}(\sum_{n\geq 0} a_n) = \delta'(\sum_{n\geq 0} a_n) + \delta''(\sum_{n\geq 0} a_n),$$

if and only if $a_n \in FL(S)$ *for all* $n \geq 1$*; i.e., if and only if* $\sum_{n\geq 0} a_n \in \widehat{FL(S)}$.

Proof. All of this is immediate from the fact that the multiplication and co-multiplication preserve the grading, that the only primitive elements in $T^n(S)$ are the elements of $FL^n(S)$, and that $FL(S) = \oplus_{n\geq 1} FL^n(S)$. □

For $x \in \mathcal{F}^1(\widehat{T(S)})$, set $e(x) = \sum_{n\geq 1} x^n/n!$ and $\ell(x) = \sum_{k\geq 1}(-1)^k x^k/k$. These power series are well defined on the maximal ideal $\mathcal{F}^1(\widehat{T(S)})$ and take values in the maximal ideal.. The reason is that for $x \in \mathcal{F}^1(\widehat{T(S)})$, for each $n \geq 1$, all but finitely many of the terms in the series for e or ℓ vanish modulo $\mathcal{F}^n(\widehat{T(S)})$. Thus, the infinite sum represents a well-defined element of the inverse limit $\widehat{T(S)}$. We define a maps EXP and LOG by $\mathrm{EXP}(x) = 1 + e(x)$ and $\mathrm{LOG}(1 + x) = \ell(x)$, for any x in the maximal ideal,. The function EXP maps the maximal ideal to the affine subspace of elements congruent to 1 modulo the maximal ideal and LOG maps the subspace of elements congruent to 1 modulo the maximal ideal to the maximal ideal.

Theorem 3.2. *The continuous maps*

$$\exp\colon \mathcal{F}^1(\widehat{T(S)} \to \{1\} + \mathcal{F}^1(\widehat{T(S)}$$

$$\mathrm{LOG}\colon \{1\} + \mathcal{F}^1(\widehat{T(S)} \to \mathcal{F}^1(\widehat{T(S)}$$

are inverses.

Proof. For $t \in (-1, 1)$ the power series for $e(t)$ and $\ell(t)$ are convergent and converge to $\exp(t) - 1$ and $\log(1 + t)$. Thus, for t sufficiently close to 0 these are inverse functions: we have $e(\ell(t)) = t$ and $\ell(e(t)) = t$. For each n, this leads to finite number algebraic equations for the coefficients terms of degree n of the composition. These manipulations are valid for composing the power series for e and ℓ in either order applied to $x \in \mathcal{F}^1(\widehat{T(S)}$. The reason is that, since all homogeneous terms of $\ell((x)$ and $e(x)$ are rational coefficients times a power of x, all homogeneous terms in both power series commute with each other. Hence, the same manipulations can be carried out for $e(x)$ and $\ell(x)$. Thus, for any $x \in \mathcal{F}^1(\widehat{T(S)})$ we have $\ell(e(x)) = x$ and and $e(\ell(x)) = x$. Hence, for any $x \in \mathcal{F}^1(\widehat{T(S)})$ we have $\mathrm{LOG}(\mathrm{EXP}(x)) = x$ and $\mathrm{EXP}(\mathrm{LOG}(1 + x)) = 1 + x$. □

4 Case $S = \{X, Y\}$ and the exponential and logarithm series

Now we specialize to the case when $S = \{X, Y\}$. Consider

$$\mathrm{LOG}(X) = \sum_{n \geq 0} \frac{X^n}{n!}; \quad \mathrm{EXP}(Y) = \sum_{n \geq 0} \frac{Y^n}{n!}.$$

These formal power series are elements in $\widehat{T(S)}$ and as is their product

$$\sum_{n \geq 0} \left(\sum_{i+j=n} \frac{X^i Y^j}{i!j!} \right).$$

Now consider

$$\mathrm{LOG}(\mathrm{EXP}(X)\mathrm{EXP}(Y)) = \sum_{m \geq 1} \frac{(-1)^{m-1}}{m} \left(\sum_{r,s \geq 0} \frac{X^r Y^s}{r!s!} \right)^m.$$

Working modulo $\mathcal{F}^n(\widehat{T(S)})$ all but finitely many of the terms vanish and thus there is no issue about convergence of the rearrangement of the coefficients modulo $\mathcal{F}^n(\widehat{T(S)})$ for each n. Applying the discussion above in this context we have

$$\mathrm{EXP}(\mathrm{LOG}(\mathrm{EXP}(X)\mathrm{EXP}(Y))) = \mathrm{EXP}(X)\mathrm{EXP}(Y).$$

Clearly

$$\mathrm{EXP}(\mathrm{LOG}(\mathrm{EXP}(0)\mathrm{EXP}(X))) = \mathrm{EXP}(\mathrm{LOG}(\mathrm{EXP}(X)\mathrm{EXP}(0))) = \mathrm{EXP}(X),$$

and $\mathrm{EXP}(X)\mathrm{EXP}(-X) = 1$ so that

$$\mathrm{EXP}(\mathrm{LOG}(\mathrm{EXP}(X)\mathrm{EXP}(-X))) = \mathrm{EXP}(\mathrm{LOG}(1)) = 1.$$

Lastly, we claim that letting $S = \{X, Y, Z\}$

$$\mathrm{EXP}(X)(\mathrm{EXP}(Y)\mathrm{EXP}(Z)) = (\mathrm{EXP}(X)\mathrm{EXP}(Y))\mathrm{EXP}(Z)$$

in $\widehat{T(S)}$. The terms from the left-hand side are of the form $\frac{(X_1^n Y^{n_2})(Z^{n_3})}{n_1! n_2! n_3!}$, whereas the terms from the right-hand side are $\frac{X_1^n (Y^{n_2} Z^{n_3})}{n_1! n_2! n_3!}$. Since $\widehat{T(S)}$ is associative, these terms are equal.

5 The Hausdorff Series

Theorem 5.1. *Let $X, Y \in S$. Then the series $H(X,Y) = \mathrm{LOG}(\mathrm{EXP}(X)\mathrm{EXP}(Y))$ in $\widehat{T(S)}$ actually lies in $\widehat{FL(S)}$, meaning that $H(X,Y) = \sum_{n\geq 1} H_n(X,Y)$ with $H_n(X,Y) \in FL^n(S)$ for all n.*

Definition 5.2. $H(XY) = \sum_{n\geq 1} H_n(X,Y)$ is the universal Hausdorff series.

Proof. The proof of this result takes up almost all of the rest of this subsection. By Corollary 3.1 the only primitive elements for the map $\hat{c}\colon \widehat{T(S)} \to \widehat{B(S)} = \prod_n B_n(S)$ given in are elements of $\widehat{FL(S)}$. That is to say, $\hat{c}(x) = x \otimes 1 + 1 \otimes x$ if and only if $x \in \widehat{FL(S)}$, or equivalently $x = \sum_{n\geq 0} x_n$ with $x_n \in FL_n(S)$ for all $n \geq 1$. We prove the theorem by showing that $\hat{c}(H(X,Y)) = H(X,Y) \otimes 1 + 1 \otimes H(X,Y)$.

We have the inverse homeomorphisms EXP and LOG between the maximal ideal of $\widehat{T(S)}$ and the affine subspace of elements congruent to 1 modulo the maximal ideal. Since $\hat{c}$ is an algebra map, for any x in the maximal ideal, we have

$$\hat{c}(\mathrm{EXP}(x)) = \mathrm{EXP}(\hat{c}(x))$$

For any y congruent to 1 modulo the maximal ideal we have

$$\hat{c}(\mathrm{LOG}(y)) = \mathrm{LOG}(\hat{c}(y)).$$

Definition 5.3. Elements $x \in \widehat{T(S)}$ congruent to 1 modulo the maximal ideal and satisfying $\hat{c}(x) = \delta'(x)\delta''(x) = x \otimes x$ are called *group-like* elements.

Claim 5.4. *If a, b in $\widehat{T(S)}$ are group-like, then so is ab.*

Proof. Suppose a, b are group-like. Then $\hat{c}(a) = \delta'(a)\delta''(a)$ and $\hat{c}(b) = \delta'(b)\delta''(b)$. But $\delta''(a)$ and $\delta'(b)$ commute so that

$$\hat{c}(ab) = \hat{c}(a)\hat{c}(b) = \delta'(a)\delta''(a)\delta'(b)\delta''(b) = \delta'(a)\delta'(b)\delta''(a)\delta''(b) = \delta'(ab)\delta''(ab),$$

showing that ab is group-like. □

Claim 5.5. *1.* EXP *maps primitive elements in the maximal ideal to group-like elements congruent to* 1 *modulo the maximal ideal.*

2. LOG *sends group-like elements congruent to* 1 *modulo the maximal ideal to primitive elements in $\mathcal{F}^1(\widehat{T(S)})$*

3. EXP *and* LOG *are inverse isomorphisms between these primitive elements and group-like elements.*

Proof. Let us prove the first item. Let X be a primitive element of $\widehat{T(S)}$. Thus,

$$\hat{c}(\mathrm{EXP}(X)) = \mathrm{EXP}(c(X)) = \mathrm{EXP}(X \otimes 1 + 1 \otimes X).$$

Since $X \otimes 1$ and $1 \otimes X$ commute we have

$$\begin{aligned}\hat{c}(\mathrm{EXP}(X)) &= \mathrm{EXP}(X \otimes 1)\mathrm{EXP}(1 \otimes X) \\ &= (\mathrm{EXP}(X) \otimes 1)(1 \otimes \mathrm{EXP}(X)) \\ &= \delta'(\mathrm{EXP}(X))\delta''(\mathrm{EXP}(X)).\end{aligned}$$

Thus, $\mathrm{EXP}(X)$ is group-like.

Now we consider the second item. Suppose that a is a group-like element congruent to 1 modulo the maximal ideal. Then

$$\hat{c}(\mathrm{LOG}(a)) = \mathrm{LOG}(\hat{c}(a)) = \mathrm{LOG}(\delta'(a)(\delta''(a)).$$

Since $\delta'(a)$ and $\delta''(a)$ commute we have

$$\begin{aligned}\mathrm{LOG}(\delta'(a)(\delta''(a)) &= \mathrm{LOG}((\delta'(a)) + \mathrm{LOG}(\delta''(a)) \\ &= \mathrm{LOG}((a \otimes 1) + \mathrm{LOG}(1 \otimes a)) \\ &= \mathrm{LOG}(a) \otimes 1 + 1 \otimes \mathrm{LOG}(a),\end{aligned}$$

so that $\mathrm{LOG}(a)$ is a primitive element of $\mathcal{F}^1(\widehat{T(S)}$. This shows that LOG maps group-like elements congruent to 1 modulo $\mathcal{F}^1)(\widehat{T(S)})$ to elements of $\mathcal{F}^1(\widehat{T(S)})$.

Lastly, we know that LOG and EXP are inverse isomorphisms between the subspaces of elements congruent to 1 modulo the maximal ideal and elements in the maximal ideal. From this and the first two items the third item follows. □

Now suppose that that $X, Y \in FL(S)$. Then they are primitive elements and hence $\mathrm{EXP}(X)$ and $\mathrm{EXP}(Y)$ are group-like. Then $\mathrm{EXP}(X) \cdot \mathrm{EXP}(Y)$ is group-like. Consequently, $H(X,Y) = \mathrm{LOG}(\mathrm{EXP}(X) \cdot \mathrm{EXP}(Y))$ is primitive. By the discussion in Section 2, it follows that $H(X,Y) = \sum_{n \geq 1} H_n(X,Y)$ and $H_n(X,Y) \in FL^n(S) \subset \widehat{T^n(S)}$. This means that $H_n(X,Y)$ is a sum of iterated brackets of copies of X and Y of length n. □

Remark 5.6. Because of skew symmetry and the Jacobi identity, there are many different ways expressions in $FL^n(S)$for $H_n(X,Y)$. But they all give the same element of $FL^n(S)$. These elements for the Hausdorff series. It is a universal expression and given two elements A and B in any Lie algebra L, there is a resulting series $\sum_{n\geq 1} H_n(A,B)$ is written as a series of n^{th} order iterated brackets of A and B. If the series converges it is an element of L.

5.1 Formal Group Properties

The direct computations above translate to $H(0,X) = H(X,0) = X$, proving that 0 is the identity for the multiplication defined by H. Also, $H(X,-X) = 0$, which means that $-X$ is the inverse of X. This shows at the formal level 0 is the identity of the formal group law defined by H and inverse is given $X \mapsto -X$. Here is the formal analogue of the associative law.

Claim 5.7. *$S = \{X,Y,Z\}$ we have $H(X,H(Y,Z)) = H((X,Y),Z)$.*

Proof. We have the following expressions:

$$H(X,H(Y,Z)) = \sum_{r,s,t} \frac{X^r}{r!}\Big(\frac{Y^sZ^t}{s!t!}\Big)$$

$$H(H(X,Y),Z) = \sum_{r,s,t}\Big(\frac{X^rY^s}{r!s!}\Big)\frac{Z^t}{t!}.$$

Since $\widehat{T(S)}$ is an associative algebra, these expressions are equal. □

6 Appendix: Algebraic Foundations

6.1 I-adic Topology and Completions

Suppose that we have an algebra A and an ideal $I \subset A$. We define the I-adic topology on A by taking as the open neighborhoods 0 as I^n (and then the open neighborhoods of $a \in A$ as $a + I^n$). We can then form a complete algebra with respect to this topology by setting $\hat{A} = \lim_n A/I^n$ with the natural homomorphisms $\pi_{n,k}\colon A/I^n \to A/I^k$ for $k < n$. By the definition of (projective) limits there are homomorphisms $\hat{\pi}_n\colon \hat{A} \to A/I^n$ compatible with the $\pi_{n,k}$ in the sense that $\pi_{n,k} \circ \hat{\pi}_n = \hat{\pi}_k$. Furthermore, for any algebra B a system of compatible homomorphisms $B \to A/I^n$ is equivalent to a

homomorphism $B \to \hat{A}$ The ideal I generates an ideal $\hat{I}$ of $\hat{A}$, namely all elements in the kernel of $\hat{\pi}_1 \colon \hat{A} \to A/I$.

The algebra $\hat{A}$ is *complete* with respect to the $\hat{I}$-adic topology in the sense that any sequence of elements x_n that is eventually constant modulo $\hat{I}^r$ for each $r > 0$ converges to a point of $\hat{A}$ in the $\hat{I}$-adic topology. If $\cap_{n>0} I^n = 0$, the the natural homomorphism $A \to \hat{A}$ is an injection with dense image in the I-adic topology. In this case $\hat{A}$ is the *completion* of A with respect to the I-adic topology.

Example (i). For a prime p, the p-adic integers $\hat{\mathbb{Z}}_p$ is the completion of $\mathbb{Z}$ with respect to the p-adic topology where the ideal is the prime ideal (p) generated by p. An element of this ring can be written uniquely as a power series

$$\sum_{n \geq 0} a_n p^n,$$

where the integers a_n range from 0 to $p-1$. More generally, any series $\sum_{n \geq 0} a_n p^n$ for arbitrary integers a_n determines an element of $\hat{\mathbb{Z}}_p$.

Example (ii). Let $K[x]$ be a polynomial ring over a field and let $I = (x)$ be the ideal generated by x. Then the I-adic completion of $K[x]$ is the ring of formal power series in one variable $K[[x]]$.

Example (iii). Let $K[x_1, \ldots, x_n]$ be the polynomial ring in n variables over a field and let $I = (0)$ be the ideal of all polynomials vanishing at 0. This is the ideal generated by $(x_1, \ldots, x_n)$. The I-adic completion of $K[x_1, \ldots, x_n]$ is the formal power series ring on n variables $K[[x_1, \ldots, x_n]]$. This is thought of as the function field of a formal neighborhood of 0 in affine n-space.

Example (iv). Let $A = \oplus_{n=0}^{\infty} A^n$ be a graded ring or algebra, meaning that the multiplication is homogeneous with respect to the grading in the sense that $m \colon A^k \otimes A^\ell \to A^{k+\ell}$. Then let $I = \oplus_{n \geq 1} A^n$ be the ideal of element of positive degree. Clearly, I^k is the ideal of elements of degree at least k and $\cap_{k=1}^{\infty} I^k = 0$. The completion $\hat{A}$ with respect to the I-adic topology is $\prod_{n=0}^{\infty} A^n$ with the obvious multiplication. Elements in this ring are formal sums $\sum_{n=0}^{\infty} a_n$, with a_n of degree n and the multiplication is the natural one on these infinite series.

Example (v). There is a generalization of Example (iv). Instead of a graded ring or algebra we consider a ring or algebra A with an increasing filtration

$$F_0(A) \subset F_1(A) \subset \cdots \subset F_n(A \subset \cdots$$

that is required to be multiplicative in the sense that $m \colon F_k(A) \otimes F_\ell(A) \to F_{k+\ell}(A)$. Then we can form the associated graded algebra

$$Gr^F(A) = \oplus_{n=0}^{\infty} F_n(A)/F_{n-1}(A)$$

with the induced graded multiplication. We can then form the completion of this graded ring as in Example (iv).

6.2 Bi-Algebras

Recall that if A and B are associatve unital algebras then so is $A \otimes B$. Its unit is the tensor product of the units of A and B and the multiplication is given by $(a \otimes b) \cdot (c \otimes d) = ac \otimes bd$.

Definition 6.1. Let A be an associative algebra over a field K with multiplication m with unit 1. A *bi-algebra structure* on A is in addition a *comultiplication*

$$c\colon A \to A \otimes A$$

that (i) is a (unital) algebra homomorphism and (ii) has a co-unit, which is a K-linear map $\epsilon A \to K$ satisfying

$$K \otimes A \xrightarrow[\mathrm{Id}_A \otimes \epsilon]{} A \otimes A \xrightarrow[m]{} A$$

is the natural identification of $K \otimes A \to A$, and analogously for $m \circ (\epsilon \otimes \mathrm{Id}_A)$.

Equivalently, we can suppose that $c\colon A \to A \otimes A$ is a co-algebra with co-unit and $m\colon A \otimes A \to A$ is an associative algebra with unit and a homomorphism of co-unital co-algebras.

We say that the bi-algebra is *co-commutative* if $T \circ c = c$ where $T\colon A \otimes A \to A \otimes A$ is the interchange of factors. We say that the bi-algebra is *co-associative* if

$$(1 \otimes c) \circ c = (c \otimes 1) \circ c.$$

Definition 6.2. In a co-algebra of a bi-algebra an element x is *primitive* if $c(x) = x \otimes 1 + 1 \otimes x$. In a co-algebra or bi-algebra an element is *group-like* if

$$c(x) = x \otimes x.$$

Example (i). Let $P(V)$ be the polynomial algebra on a finite dimensional vector space over a field of characteristic 0. The usual multiplication of polynomials makes this an associative algebra. Define $c\colon V \to V \otimes V$ by $c(v) = v \otimes 1 + 1 \otimes v$. Since V generates $P(V)$ as an algebra there is at most one algebra map $c_0\colon P(V) \to P(V) \otimes P(V)$ extending c. Since $P(V)$ is the free commutative and associative algebra generated by V and since $P(V) \otimes P(V)$ is also a commutative, associative algebra, there is a unique extension of c to a co-algebra map

$$c_0\colon P(V) \to P(V) \otimes P(V).$$

Its value on an n^{th} power is given by

$$c_0(v^n) = \sum_{k=0}^{n} \binom{n}{k} v^k \otimes v^{n-k}.$$

This is the *standard* co-multiplication on $P(V)$. It is an easy exercise to show it makes a co-commutative, co-associative bi-algebra.

It is an exercise to show (since K has characteristic 0) that every homogeneous polynomial of degree n is a sum of n^{th} powers.

Corollary 6.3. *For V a finite dimensional vector space over a field of characteristic the only primitive elements in $P(V)$ the usual co-multiplication are the homogeneous polynomials of degree* 1.

Proof. Since c_0 is homogeneous with respect to degree, if x is a primitive element then each of its homogeneous terms is. Thus, it suffices to assume that x is homogeneous, say of degree n. Polynomials of degree 0 are elements of K and since $c_0(1) = 1 \otimes 1$, there are no primitive elements of degree 0. Suppose that x is non-zero and homogeneous of degree $n \geq 1$. Then $x = \sum_i \lambda_i v_i^n$ and hence the terms of degree $(1, n-1)$ in $c(x)$ are $\sum_i n\lambda_i v_i \otimes v_i^{n-1}$ and the product of this term in $P(V)$ is nx. Thus, this term is non-zero. Hence, x is not primitive if $n \neq 1$. Lastly, if x is homogeneous of degree 1 then $x \in V$ and $c_0(x) = x \otimes 1 + 1 \otimes x$, so that x is primitive $\square$

6.3 Hopf Algebras or Quantum Groups (According to Drinfeld)

Definition 6.4. A Hopf algebra is an associative, co-associative bi-algebra H with a unit and co-unit with one piece of extra structure, called *an antipode*. We denote the algebra multiplication by m and the co-algebra structure c. The antipod is an anti-homomorphism of algebras $S\colon H \to H$ with the property that for any $x \in H$ we write $c(x) = \sum_i a_i \otimes b_i$ then $\sum_i m(S(a_i), b_i) = \sum_i m(a_i S(b_i)) = \epsilon(x)1$, where ϵ is the co-unit and 1 is the unit.

In the case of a universal enveloping algebra, $U(L)$, the antipode is determined by $S(X) = -X$ for $X \in L$. That, and the condition that it be an anti-homomorphism, determine it. For example,

$$S([X, Y]) = S(XY - YX) = YX - XY = -[X, Y].$$

Another example of a Hopf algebra is the rational group ring $Q[G]$. The multiplication comes from the multiplication in G. The co-multiplication is determined by $c(g) = g \otimes 1 + 1 \otimes g$ for any $g \in G$. Lastly, $S(g) = g^{-1}$.

Dually, the functions on a group $Fun(G)$, in various categories form a Hopf algebra where the comultiplication is dual to the product on the group.

All the examples of Hopf algebras coming from groups are commutative Hopf algebras. Drinfeld's idea is that non-commutative Hopf algebras correspond to truly quantum groups.