

# Math 128 Lecture 4

Completion of the algebraic proof of the Campbell-Baker-Hausdorff theorem. Free Lie algebras.

# Review: Statement of the PBW theorem.

$L$  is a Lie algebra and  $U(L)$  its universal enveloping algebra.

Suppose that we choose a basis  $x_i$ ,  $i \in I$  of  $L$  where  $I$  is a totally ordered set. Since

$$\overline{\epsilon(x_i)\epsilon(x_j)} = \overline{\epsilon(x_j)\epsilon(x_i)}$$

we can rearrange any product of  $\overline{\epsilon(x_i)}$  so as to be in increasing order. This shows that the elements

$$x_M := \epsilon(x_{i_1}) \cdots \epsilon(x_{i_m}), \quad M := (i_1, \dots, i_m) \quad i_1 \leq \cdots \leq i_m$$

span  $UL$  as a vector space.

**Theorem 1 Poincaré-Birkhoff-Witt.** *The elements  $x_M$  form a basis of  $UL$ .*

# Proof of PBW: construction of a module.

Let  $V$  be the vector space with basis  $z_M$  where  $M$  runs over all ordered sequences  $i_1 \leq i_2 \leq \cdots \leq i_n$ . (Recall that we have chosen a well ordering on  $I$  and that the  $x_i$   $i \in I$  form a basis of  $L$ .)

Furthermore, the empty sequence,  $z_\emptyset$  is allowed, and we will identify the symbol  $z_\emptyset$  with the number  $1 \in k$ . If  $i \in I$  and  $M = (i_1, \dots, i_n)$  we write  $i \leq M$  if  $i \leq i_1$  and then let  $(i, M)$  denote the ordered sequence  $(i, i_1, \dots, i_n)$ . In particular, we adopt the convention that if  $M = \emptyset$  is the empty sequence then  $i \leq M$  for all  $i$  in which case  $(i, M) = (i)$ . Recall that if  $M = (i_1, \dots, i_n)$  we set  $\ell(M) = n$  and call it the length of  $M$ . So, for example,  $\ell(i, M) = \ell(M) + 1$  if  $i \leq M$ .

**Lemma 1** *We can make  $V$  into an  $L$  module in such a way that*

$$x_i z_M = z_{iM} \quad \text{whenever } i \leq M. \quad (20)$$

# Proof of the lemma, I.

$$x_i z_M = z_{iM} \quad \text{whenever } i \leq M. \quad (20)$$

**Proof of lemma.** We will inductively define a map

$$L \times V \rightarrow V, \quad (x, v) \mapsto xv$$

and then show that it satisfies the equation

$$xyv - yxv = [x, y]v, \quad x, y \in L, \quad v \in V, \quad (21)$$

which is the condition that makes  $V$  into an  $L$  module. Our definition will be such that (20) holds. In fact, we will define  $x_i z_M$  inductively on  $\ell(M)$  and on  $i$ . So we start by defining

$$x_i z_\emptyset = z_{(i)}$$

which is in accordance with (20). This defines  $x_i z_M$  for  $\ell(M) = 0$ .

# Proof of the lemma, 2.

We want

$$x_i z_M = z_{iM} \quad \text{whenever } i \leq M. \quad (20)$$

and

$$xyv - yxv = [x, y]v, \quad x, y \in L, \quad v \in V, \quad (21)$$

For  $\ell(M) = 1$  we define

$$x_i z_{(j)} = z_{(i,j)} \quad \text{if } i \leq j$$

while if  $i > j$  we set

$$x_i z_{(j)} = x_j z_{(i)} + [x_i, x_j] z_\emptyset = z_{(j,i)} + \sum c_{ij}^k z_{(k)}$$

where

$$[x_i, x_j] = \sum c_{ij}^k x_k$$

is the expression for the Lie bracket of  $x_i$  with  $x_j$  in terms of our basis. These  $c_{ij}^k$  are known as the **structure constants** of the Lie algebra,  $L$  in terms of the given basis. Notice that the first of these two cases is consistent with (and forced on us) by (20) while the second is forced on us by (21).

# Proof of the lemma. 3.

We want  $x_i z_M = z_{iM}$  whenever  $i \leq M$ . (20)

and  $xyv - yxv = [x, y]v$ ,  $x, y \in L$ ,  $v \in V$ , (21)

We have defined  $x_i z_{(j)} = z_{(i,j)}$  if  $i \leq j$

while if  $i > j$   $x_i z_{(j)} = x_j z_{(i)} + [x_i, x_j] z_\emptyset = z_{(j,i)} + \sum c_{ij}^k z_{(k)}$

We now have defined  $x_i z_M$  for all  $i$  and all  $M$  with

$\ell(M) \leq 1$ , and we have done so in such a way that (20) holds, and (21) holds where it makes sense (i.e. for  $\ell(M) = 0$ ).

So suppose that we have defined  $x_j z_N$  for all  $j$  if  $\ell(N) < \ell(M)$  and for all  $j < i$  if  $\ell(N) = \ell(M)$  in such a way that

$x_j z_N$  is a linear combination of  $z_L$ 's with  $\ell(L) \leq \ell(N) + 1$  (\*).

# Proof of the lemma, 4.

So suppose that we have defined  $x_j z_N$  for all  $j$  if  $\ell(N) < \ell(M)$  and for all  $j < i$  if  $\ell(N) = \ell(M)$  in such a way that

$$x_j z_N \text{ is a linear combination of } z_L \text{'s with } \ell(L) \leq \ell(N) + 1 \quad (*).$$

We then define

$$\begin{aligned} x_i z_M &= z_{iM} \text{ if } i \leq M \\ &= x_j(x_i z_N) + [x_i, x_j] z_N \text{ if } M = (jN) \text{ with } i > j. \end{aligned} \quad (22)$$

This makes sense since  $x_i z_N$  is already defined as a linear combination of  $z_L$ 's with  $\ell(L) \leq \ell(N) + 1 = \ell(M)$  and because  $[x_i, x_j]$  can be written as a linear combination of the  $x_k$  as above. Furthermore  $(*)$  holds with  $j$  and  $N$  replaced by  $M$ . Furthermore, (20) holds by construction. We must check (21).

$$xyv - yxv = [x, y]v, \quad x, y \in L, \quad v \in V, \quad (21)$$

# Proof of the lemma, 4.

$$xyv - yxv = [x, y]v, \quad x, y \in L, \quad v \in V, \quad (21)$$

We must check (21). By linearity, this means that we must show that

$$x_i x_j z_N - x_j x_i z_N = [x_i, x_j] z_N.$$

If  $i = j$  both sides are zero. Also, since both sides are anti-symmetric in  $i$  and  $j$ , we may assume that  $i > j$ . If  $j \leq N$  and  $i > j$  then this equation holds by definition. So we need only deal with the case where  $j \not\leq N$  which means that  $N = (kP)$  with  $k \leq P$  and  $i > j > k$ . So we have, by definition,

$$\begin{aligned} x_j z_N &= x_j z_{(kP)} \\ &= x_j x_k z_P \\ &= x_k x_j z_P + [x_j, x_k] z_P. \end{aligned}$$

# Proof of the lemma, 5.

To prove:

$$xyv - yxv = [x, y]v, \quad x, y \in L, \quad v \in V, \quad (21)$$

$$\begin{aligned} x_j z_N &= x_j z_{(kP)} \\ &= x_j x_k z_P \\ &= x_k x_j z_P + [x_j, x_k] z_P. \end{aligned}$$

Now if  $j \leq P$  then  $x_j z_P = z_{(jP)}$  and  $k < (jP)$ . If  $j \not\leq P$  then  $x_j z_P = z_Q + w$  where still  $k \leq Q$  and  $w$  is a linear combination of elements of length  $< \ell(N)$ . So we know that (21) holds for  $x = x_i, y = x_k$  and  $v = z_{(jP)}$  (if  $j \leq P$ ) or  $v = z_Q$  (otherwise). Also, by induction, we may assume that we have verified (21) for all  $N'$  of length  $< \ell(N)$ . So we may apply (21) to  $x = x_i, y = x_k$  and  $v = x_j z_P$  and also to  $x = x_i, y = [x_j, x_k], v = z_P$ . So

$$x_i x_j z_N = x_k x_i x_j z_P + [x_i, x_k] x_j z_P + [x_j, x_k] x_i z_P + [x_i, [x_j, x_k]] z_P.$$

This argument depended only on the fact that  $k < j$ . So we may interchange  $i$  and  $j$  and get a similar formula.

# Proof of the lemma, end.

$$x_i x_j z_N = x_k x_i x_j z_P + [x_i, x_k] x_j z_P + [x_j, x_k] x_i z_P + [x_i, [x_j, x_k]] z_P.$$

Similarly, the same result holds with  $i$  and  $j$  interchanged. Subtracting this interchanged version from the preceding equation the two middle terms from each equation cancel and we get

$$\begin{aligned} (x_i x_j - x_j x_i) z_N &= x_k (x_i x_j - x_j x_i) z_P + ([x_i, [x_j, x_k]] - [x_j, [x_i, x_k]]) z_P \\ &= x_k [x_i, x_j] z_P + ([x_i, [x_j, x_k]] - [x_j, [x_i, x_k]]) z_P \\ &= [x_i, x_j] x_k z_P + ([x_k, [x_i, x_j]] + [x_i, [x_j, x_k]] - [x_j, [x_i, x_k]]) z_P \\ &= [x_i, x_j] z_N. \end{aligned}$$

(In passing from the second line to the third we used (21) applied to  $z_P$  (by induction) and from the third to the last we used the anti-symmetry of the bracket and Jacobi's equation.) QED

# Proof of PBW from the lemma.

**Proof of the PBW theorem.** We have made  $V$  into an  $L$  and hence into a  $U(L)$  module. By construction, we have, inductively,

$$x_M z_\emptyset = z_M.$$

But if

$$\sum c_M x_M = 0$$

then

$$0 = \sum c_M z_M = \left( \sum c_M x_M \right) z_\emptyset$$

contradicting the fact that the  $z_M$  are independent. QED

In particular, the map  $\epsilon : L \rightarrow U(L)$  is an injection, and so we may identify  $L$  as a subspace of  $U(L)$ .

# Review: the bialgebra structure of the universal enveloping algebra,

Consider the map  $L \rightarrow U(L) \otimes U(L)$ :

$$x \mapsto x \otimes 1 + 1 \otimes x.$$

Then

$$\begin{aligned} (x \otimes 1 + 1 \otimes x)(y \otimes 1 + 1 \otimes y) = \\ xy \otimes 1 + x \otimes y + y \otimes x + 1 \otimes xy, \end{aligned}$$

and multiplying in the reverse order and subtracting gives

$$[x \otimes 1 + 1 \otimes x, y \otimes 1 + 1 \otimes y] = [x, y] \otimes 1 + 1 \otimes [x, y].$$

Thus the map  $x \mapsto x \otimes 1 + 1 \otimes x$  determines an algebra homomorphism

$$\Delta : U(L) \rightarrow U(L) \otimes U(L).$$

Define

$$\varepsilon : U(L) \rightarrow k, \quad \varepsilon(1) = 1, \quad \varepsilon(x) = 0, \quad x \in L$$

and extend as an algebra homomorphism. Then

$$(\varepsilon \otimes \text{id})(x \otimes 1 + 1 \otimes x) = 1 \otimes x, \quad x \in L.$$

We identify  $k \otimes L$  with  $L$  and so can write the above equation as

$$(\varepsilon \otimes \text{id})(x \otimes 1 + 1 \otimes x) = x, \quad x \in L.$$

The algebra homomorphism

$$(\varepsilon \otimes \text{id}) \circ \Delta : U(L) \rightarrow U(L)$$

is the identity (on 1 and on)  $L$  and hence is the identity. Similarly

$$(\text{id} \otimes \varepsilon) \circ \Delta = \text{id}.$$

A vector space  $C$  with a map  $\Delta : C \rightarrow C \otimes C$ , (called a **comultiplication**) and a map  $\varepsilon : C \rightarrow k$  (called a **co-unit**) satisfying

$$(\varepsilon \otimes \text{id}) \circ \Delta = \text{id}$$

and

$$(\text{id} \otimes \varepsilon) \circ \Delta = \text{id}$$

is called a **co-algebra**. If  $C$  is an algebra and both  $\Delta$  and  $\varepsilon$  are algebra homomorphisms, we say that  $C$  is a **bi-algebra**(sometimes shortened to “bigebra”). So we have proved that  $(U(L), \Delta, \varepsilon)$  is a bialgebra.

# Primitive elements of $U(L)$ .

An element  $x$  of a bialgebra is called **primitive** if

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

So the elements of  $L$  are primitives in  $U(L)$ .

We claim that *these are the only primitives*.

First prove this for the case  $L$  is abelian so  $U(L) = S(L)$ . Then we may think of  $S(L) \otimes S(L)$  as polynomials in twice the number of variables as those of  $S(L)$  and

$$\Delta(f)(u, v) = f(u + v).$$

For example, since  $\Delta$  is a homomorphism for multiplication, the element  $x^2$  is sent by  $\Delta$  into

$$\Delta(x)^2 = (x \otimes 1 + 1 \otimes x)^2 = x^2 \otimes 1 + 2x \otimes x + 1 \otimes x^2.$$

If we write  $x \otimes 1 = u$  and  $1 \otimes x = v$  this is just the expression for  $(u + v)^2$ .

# Proof that the elements of $L$ are the only primitive elements of $U(L)$ .

The condition of being primitive says that

$$f(u + v) = f(u) + f(v).$$

Taking homogeneous components, the same equality holds for each homogeneous component. But if  $f$  is homogeneous of degree  $n$ , taking  $u = v$  gives

$$2^n f(u) = 2f(u)$$

so  $f = 0$  unless  $n = 1$ .

Taking  $\text{gr}$ , this shows that for any Lie algebra the primitives are contained in  $U_1(L)$ . But

$$\Delta(c + x) = c(1 \otimes 1) + x \otimes 1 + 1 \otimes x$$

so the condition on primitivity requires  $c = 2c$  or  $c = 0$ . QED

# Magmas.

A set  $M$  with a map:

$$M \times M \rightarrow M, \quad (x, y) \mapsto xy$$

is called a **magma**. Thus a magma is a set with a binary operation with no axioms at all imposed.

# Free magmas and non-associative words.

Let  $X$  be any set. Define  $X_n$  inductively by  $X_1 := X$  and

$$X_n = \coprod_{p+q=n} X_p \times X_q$$

for  $n \geq 2$ . Thus  $X_2$  consists of all expressions  $ab$  where  $a$  and  $b$  are elements of  $X$ . (We write  $ab$  instead of  $(a, b)$ .) An element of  $X_3$  is either an expression of the form  $(ab)c$  or an expression of the form  $a(bc)$ . An element of  $X_4$  has one out of five forms:  $a((bc)d)$ ,  $a(b(cd))$ ,  $((ab)(cd))$ ,  $((ab)c)d$  or  $(a(bc))d$ .

Set

$$M_X := \prod_{n=1}^{\infty} X_n.$$

An element  $w \in M_X$  is called a non-associative word, and its length  $\ell(w)$  is the unique  $n$  such that  $w \in X_n$ . We have a “multiplication” map  $M_X \times M_X$  given by the inclusion

$$X_p \times X_q \hookrightarrow X_{p+q}.$$

Thus the multiplication on  $M_X$  is concatenation of non-associative words.

# The free magma on a set is universal for maps of the set into a magma.

If  $N$  is any magma, and  $f : X \rightarrow N$  is any map, we define  $F : M_X \rightarrow N$  by  $F = f$  on  $X_1$ , by

$$F : X_2 \rightarrow N, \quad F(ab) = f(a)f(b)$$

and inductively

$$F : X_p \times X_q \rightarrow N, \quad F(uv) = F(u)F(v).$$

Any element of  $X_n$  has a unique expression as  $uv$  where  $u \in X_p$  and  $v \in X_q$  for a unique  $(p, q)$  with  $p + q = n$ , so this inductive definition is valid.

It is clear that  $F$  is a magma homomorphism and is uniquely determined by the original map  $f$ . Thus  $M_X$  is the “free magma on  $X$ ” or the “universal magma on  $X$ ” in the sense that it is the solution to the universal problem associated to a map from  $X$  to any magma.

# The free algebra on a set.

Let  $A_X$  be the vector space of finite formal linear combinations of elements of  $M_X$ . So an element of  $A_X$  is a finite sum  $\sum c_m m$  with  $m \in M_X$  and  $c_m$  in the ground field. The multiplication in  $M_X$  extends by bi-linearity to make  $A_X$  into an algebra. If we are given a map  $X \rightarrow B$  where  $B$  is any algebra, we get a unique magma homomorphism  $M_X \rightarrow B$  extending this map (where we think of  $B$  as a magma) and then a unique algebra map  $A_X \rightarrow B$  extending this map by linearity.

Notice that the algebra  $A_X$  is graded since every element of  $M_X$  has a length and the multiplication on  $M_X$  is graded. Hence  $A_X$  is the free algebra on  $X$  in the sense that it solves the universal problem associated with maps of  $X$  to algebras.

## The Free Lie Algebra $L_X$ .

In  $A_X$  let  $I$  be the two-sided ideal generated by all elements of the form  $aa$ ,  $a \in A_X$  and  $(ab)c + (bc)a + (ca)b$ ,  $a, b, c \in A_X$ . We set

$$L_X := A_X/I$$

and call  $L_X$  the free Lie algebra on  $X$ . Any map from  $X$  to a Lie algebra  $L$  extends to a unique algebra homomorphism from  $L_X$  to  $L$ .

## The ideal $I$ is graded.

We claim that the ideal  $I$  defining  $L_X$  is graded. This means that if  $a = \sum a_n$  is a decomposition of an element of  $I$  into its homogeneous components, then each of the  $a_n$  also belong to  $I$ . To prove this, let  $J \subset I$  denote the set of all  $a = \sum a_n$  with the property that all the homogeneous components  $a_n$  belong to  $I$ . Clearly  $J$  is a two sided ideal. We must show that  $I \subset J$ . For this it is enough to prove the corresponding fact for the generating elements. Clearly if

$$a = \sum a_p, \quad b = \sum b_q, \quad c = \sum c_r$$

then

$$(ab)c + (bc)a + (ca)b = \sum_{p,q,r} ((a_p b_q) c_r + (b_q c_r) a_p + (c_r a_p) b_q).$$

But also if  $x = \sum x_m$  then

$$x^2 = \sum x_n^2 + \sum_{m < n} (x_m x_n + x_n x_m)$$

and

$$x_m x_n + x_n x_m = (x_m + x_n)^2 - x_m^2 - x_n^2 \in I$$

so  $I \subset J$ .

The fact that  $I$  is graded means that  $L_X$  inherits the structure of a graded algebra.

## The free associative algebra $\text{Ass}(X)$ .

Let  $V_X$  be the vector space of all finite formal linear combinations of elements of  $X$ . Define

$$\text{Ass}_X = T(V_X),$$

the tensor algebra of  $V_X$ . Any map of  $X$  into an associative algebra  $A$  extends to a unique linear map from  $V_X$  to  $A$  and hence to a unique algebra homomorphism from  $\text{Ass}_X$  to  $A$ . So  $\text{Ass}_X$  is the free associative algebra on  $X$ .

$$U(L_X) \cong \text{Ass}_X.$$

We have the maps  $X \rightarrow L_X$  and  $\epsilon : L_X \rightarrow U(L_X)$  and hence their composition maps  $X$  to the associative algebra  $U(L_X)$  and so extends to a unique homomorphism

$$\Psi : \text{Ass}_X \rightarrow U(L_X).$$

On the other hand, the commutator bracket gives a Lie algebra structure to  $\text{Ass}_X$  and the map  $X \rightarrow \text{Ass}_X$  thus give rise to a Lie algebra homomorphism

$$L_X \rightarrow \text{Ass}_X$$

which determines an associative algebra homomorphism

$$\Phi : U(L_X) \rightarrow \text{Ass}_X.$$

both compositions  $\Phi \circ \Psi$  and  $\Psi \circ \Phi$  are the identity on  $X$  and hence, by uniqueness, the identity everywhere. We obtain the important result that  $U(L_X)$  and  $\text{Ass}_X$  are canonically isomorphic:

$$U(L_X) \cong \text{Ass}_X. \tag{23}$$

# The Lie algebra generated by $X$ in $\text{Ass}_X$ .

$$U(L_X) \cong \text{Ass}_X. \quad (23)$$

Now the Poincaré-Birkhoff-Witt theorem guarantees that the map  $\epsilon : L_X \rightarrow U(L_X)$  is injective. So under the above isomorphism, the map  $L_X \rightarrow \text{Ass}_X$  is injective. On the other hand, by construction, the map  $X \rightarrow V_X$  induces a surjective Lie algebra homomorphism from  $L_X$  into the Lie subalgebra of  $\text{Ass}_X$  generated by  $X$ . So we see that under the isomorphism (23)  $L_X \subset U(L_X)$  is mapped isomorphically onto the Lie subalgebra of  $\text{Ass}_X$  generated by  $X$ .

# The primitive elements of $\text{Ass}_X$ .

Now the map

$$X \rightarrow \text{Ass}_X \otimes \text{Ass}_X, \quad x \mapsto x \otimes 1 + 1 \otimes x$$

extends to a unique algebra homomorphism

$$\Delta : \text{Ass}_X \rightarrow \text{Ass}_X \otimes \text{Ass}_X.$$

Under the identification (23) this is none other than the map

$$\Delta : U(L_X) \rightarrow U(L_X) \otimes U(L_X)$$

and hence we conclude that  $L_X$  is the set of primitive elements of  $\text{Ass}_X$ :

$$L_X = \{w \in \text{Ass}_X \mid \Delta(w) = w \otimes 1 + 1 \otimes w.\} \quad (24)$$

under the identification (23).

# Completions.

We recall our constructs of the past few sections:  $X$  denotes a set,  $L_X$  the free Lie algebra on  $X$  and  $\text{Ass}_X$  the free associative algebra on  $X$  so that  $\text{Ass}_X$  may be identified with the universal enveloping algebra of  $L_X$ . Since  $\text{Ass}_X$  may be identified with the non-commutative polynomials indexed by  $X$ , we may consider its completion,  $F_X$ , the algebra of formal power series indexed by  $X$ . Since the free Lie algebra  $L_X$  is graded we may also consider its completion which we shall denote by  $\mathbf{L}_X$ . Finally let  $m$  denote the ideal in  $F_X$  generated by  $X$ . The maps

$$\exp : m \rightarrow 1 + m, \quad \log : 1 + m \rightarrow m$$

are well defined by their formal power series and are mutual inverses. (There is no convergence issue since everything is within the realm of formal power series.) Furthermore  $\exp$  is a bijection of the set of  $\alpha \in m$  satisfying  $\Delta\alpha = \alpha \otimes 1 + 1 \otimes \alpha$  to the set of all  $\beta \in 1 + m$  satisfying  $\Delta\beta = \beta \otimes \beta$ .

# Abstract version of CBH and its algebraic proof.

In particular, since the set  $\{\beta \in 1 + m \mid \Delta\beta = \beta \otimes \beta\}$  forms a group, we conclude that for any  $A, B \in \mathbf{L}_X$  there exists a  $C \in \mathbf{L}_X$  such that

$$\exp C = (\exp A)(\exp B).$$

This is the abstract version of the Campbell-Baker-Hausdorff formula. It depends basically on two algebraic facts: That the universal enveloping algebra of the free Lie algebra is the free associative algebra, and that the set of primitive elements in the universal enveloping algebra (those satisfying  $\Delta\alpha = \alpha \otimes 1 + 1 \otimes \alpha$ ) is precisely the original Lie algebra.

## Explicit formula for CBH.

Define the map

$$\Phi : m \cap \text{Ass}_X \rightarrow L_X,$$

$$\Phi(x_1 \cdots x_n) := [x_1, [x_2, \dots, [x_{n-1}, x_n] \cdots]] = \text{ad}(x_1) \cdots \text{ad}(x_{n-1})(x_n),$$

and let  $\Theta : \text{Ass}_X \rightarrow \text{End}(L_X)$  be the algebra homomorphism extending the Lie algebra homomorphism  $\text{ad} : L_X \rightarrow \text{End}(L_X)$ . We claim that

$$\Phi(uv) = \Theta(u)\Phi(v), \quad \forall u \in \text{Ass}_X, v \in m \cap \text{Ass}_X. \quad (25)$$

**Proof.** It is enough to prove this formula when  $u$  is a monomial,  $u = x_1 \cdots x_n$ . We do this by induction on  $n$ . For  $n = 0$  the assertion is obvious and for  $n = 1$  it follows from the definition of  $\Phi$ . Suppose  $n > 1$ . Then

$$\begin{aligned} \Phi(x_1 \cdots x_n v) &= \Theta(x_1)\Phi(x_2 \cdots x_n v) \\ &= \Theta(x_1)\Theta(x_2 \cdots x_n)\Phi(v) \\ &= \Theta(x_1 \cdots x_n)\Phi(v). \text{ QED} \end{aligned}$$

Recall that  $\Phi(x_1 \dots x_n) := [x_1, [x_2, \dots, [x_{n-1}, x_n] \dots]] = \text{ad}(x_1) \dots \text{ad}(x_{n-1})(x_n)$

Let  $L_X^n$  denote the  $n$ -th graded component of  $L_X$ . So  $L_X^1$  consists of linear combinations of elements of  $X$ ,  $L_X^2$  is spanned by all brackets of pairs of elements of  $X$ , and in general  $L_X^n$  is spanned by elements of the form

$$[u, v], \quad u \in L_X^p, \quad v \in L_X^q, \quad p + q = n.$$

We claim that

$$\Phi(u) = nu \quad \forall u \in L_X^n. \quad (26)$$

For  $n = 1$  this is immediate from the definition of  $\Phi$ . So by induction it is enough to verify this on elements of the form  $[u, v]$  as above. We have

$$\begin{aligned} \Phi([u, v]) &= \Phi(uv - vu) \\ &= \Theta(u)\Phi(v) - \Theta(v)\Phi(u) \\ &= q\Theta(u)v - p\Theta(v)u \quad \text{by induction} \\ &= q[u, v] - p[v, u] \\ &\quad \text{since } \Theta(w) = \text{ad}(w) \text{ for } w \in L_X \\ &= (p + q)[u, v] \quad \text{QED.} \end{aligned}$$

We can now write down an explicit formula for the  $n$ -th term in the Campbell-Baker-Hausdorff expansion. Consider the case where  $X$  consists of two elements  $X = \{x, y\}$ ,  $x \neq y$ . Let us write

$$z = \log((\exp x)(\exp y)) \quad z \in \mathbf{L}_X, \quad z = \sum_1^{\infty} z_n(x, y).$$

We want an explicit expression for  $z_n(x, y)$ . We know that

$$z_n = \frac{1}{n} \Phi(z_n)$$

and  $z_n$  is a sum of non-commutative monomials of degree  $n$  in  $x$  and  $y$ .

$$z_n = \frac{1}{n} \Phi(z_n)$$

$$\begin{aligned}
 (\exp x)(\exp y) &= \left( \sum_{p=0}^{\infty} \frac{x^p}{p!} \right) \left( \sum_{q=0}^{\infty} \frac{y^q}{q!} \right) \\
 &= 1 + \sum_{p+q \geq 1} \frac{x^p y^q}{p! q!} \quad \text{so} \\
 z &= \log((\exp x)(\exp y)) \\
 &= \sum_{m=1}^{\infty} \frac{(-1)^{m+1}}{m} \left( \sum_{p+q \geq 1} \frac{x^p y^q}{p! q!} \right)^m \\
 &= \sum_{p_i + q_i \geq 1} \frac{(-1)^{m+1}}{m} \frac{x^{p_1} y^{q_1} x^{p_2} y^{q_2} \dots x^{p_m} y^{q_m}}{p_1! q_1! \dots p_m! q_m!}.
 \end{aligned}$$

We want to apply  $\frac{1}{n} \Phi$  to the terms in this last expression which are of total degree  $n$  so as to obtain  $z_n$ .

$$z_n = \frac{1}{n} \Phi(z_n)$$

$$z = \sum_{p_i + q_i \geq 1} \frac{(-1)^{m+1}}{m} \frac{x^{p_1} y^{q_1} x^{p_2} y^{q_2} \dots x^{p_m} y^{q_m}}{p_1! q_1! \dots p_m! q_m!}.$$

We want to apply  $\frac{1}{n} \Phi$  to the terms in this last expression which are of total degree  $n$  so as to obtain  $z_n$ . So let us examine what happens when we apply  $\Phi$  to an expression occurring in the numerator: If  $q_m \geq 2$  we get 0 since we will have  $\text{ad}(y)(y) = 0$ . Similarly we will get 0 if  $q_m = 0, p_m \geq 2$ . Hence the only terms which survive are those with  $q_m = 1$  or  $q_m = 0, p_m = 1$ . Accordingly we decompose  $z_n$  into these two types:

$$z_n = \frac{1}{n} \sum_{p+q=n} (z'_{p,q} + z''_{p,q}), \quad (27)$$

# Explicit CBH formula.

$$z_n = \frac{1}{n} \sum_{p+q=n} (z'_{p,q} + z''_{p,q}), \quad (27)$$

where

$$z'_{p,q} = \sum \frac{(-1)^{m+1}}{m} \frac{\text{ad}(x)^{p_1} \text{ad}(y)^{q_1} \cdots \text{ad}(x)^{p_m} y}{p_1! q_1! \cdots p_m!} \text{ summed over all}$$

$$p_1 + \cdots + p_m = p, \quad q_1 + \cdots + q_{m-1} = q - 1, \quad q_i + p_i \geq 1, \quad p_m \geq 1$$

and

$$z''_{p,q} = \sum \frac{(-1)^{m+1}}{m} \frac{\text{ad}(x)^{p_1} \text{ad}(y)^{q_1} \cdots \text{ad}(y)^{q_{m-1}} (x)}{p_1! q_1! \cdots q_{m-1}!} \text{ summed over}$$

$$p_1 + \cdots + p_{m-1} = p - 1, \quad q_1 + \cdots + q_{m-1} = q,$$

$$p_i + q_i \geq 1 \quad (i = 1, \dots, m-1) \quad q_{m-1} \geq 1.$$

# The first four terms.

The first four terms are:

$$\begin{aligned}z_1(x, y) &= x + y \\z_2(x, y) &= \frac{1}{2}[x, y] \\z_3(x, y) &= \frac{1}{12}[x, [x, y]] + \frac{1}{12}[y, [y, x]] \\z_4(x, y) &= \frac{1}{24}[x, [y, [x, y]]].\end{aligned}$$