In general there is no exponential map from a Lie algebra to its UEA, but we can define one to its completion if the Lie algebra is graded with all pieces of positive degree. In this case the UEA is also graded so we can take its completion, and the exp and log maps are well defined on elements with constant terms 0 and 1 in this completion. We can define group-like elements in the completed UEA in the obvious way (but note that the map Δ has image in the completion of $Ug \otimes Ug$, which is larger than the tensor products of the completions). For nilpotent Lie algebras things are even better as the series are finite as elements of the Lie algebra are nilpotent, so we do not need to take completions.

Lemma 60 *exp is an isomorphism from primitive elements to group-like elements in the completion of the UEA, with inverse given by log*

Proof This is an easy calculation: for example, if a is primitive so that $\Delta(a) = 1 \otimes a + a \otimes 1$, then $\Delta(\exp(a)) = \exp(\Delta(a)) = \exp(1 \otimes a)\exp(a \otimes 1) = \exp(a) \otimes \exp(a)$. □

Proof (of the Baker-Campbell-Hausdorff formula) If we grade the free Lie algebra by giving A and B degree 1 then it is trivial that $\exp(A)\exp(B) = \exp(C)$ for some C in the completion of the UEA: we just take C to be $\log(\exp(A)\exp(B))$. The problem is to prove that C is in the completion of the Lie algebra, in other words can be written in terms of A and B using just the Lie bracket but not the product of the UEA. In other words we have to show that C is primitive. But this follows easily from the remarks above: A and B are primitive, so $\exp(A)$ and $\exp(B)$ are group-like, so their product $\exp(A)\exp(B)$ is also group-like, so the log of the product is primitive. □

One application of this formula is to prove Lie's rather hard theorem that there is a Lie group for every Lie algebra: roughly speaking the CBH formula allows us to define a sort of local chunk of the Lie group near the identity, and we can construct a global Lie group by carefully pasting such chunks together.

This does not quite give an explicit expression for $\exp(a)\exp(b)$; in fact there are many different explicit expressions, because there are many ways to write elements of the free Lie algebra. We will now use the Campbell-Baker-Hausdorff to find an explicit expression.

Dynkin gave an explicit formula for the Campbell-Baker-Hausdorff formula as follows. We can write

$$\log(e^x e^y) = \sum_{m>0} \frac{(-1)^m}{m} \left(\sum_{i+j>0} \frac{x^i}{i!} \frac{y^j}{j!} \right)$$

(remembering that x and y do not commute) which gives an explicit non-commuting power series, though not written in terms of the Lie bracket. However we know the right hand side is primitive by the Baker-Campbell-Hausdorff theorem, so if we apply any linear map Φ from the free associative algebra to the free Lie algebra on x, y that is the identity on primitive elements we will get an explicit expression for $\log(e^x e^y)$ in terms of the Lie bracket. One such linear map ϕ was found by Dynkin as follows. Put

$$\Phi(x_1 x_2 \cdots x_{n-1} x_n) = [x_1, [x_2, \ldots, [x_{n-1}, x_n] \cdots]]$$

if $n \geq 1$. Then by definition of Φ, if $\deg v > 0$ we have $\Phi(uv) = \theta(u)\Phi(v)$, where θ is the algebra homomorphism from the associative algebra to $\mathrm{End}(A)$ taking x_i to $[x_i, *]$ (so $\theta(u)v = [u, v]$ whenever u is primitive). Then $\Phi(u) = \deg(u)u$ for all primitive elements u. This follows by induction on the degree of u as $\Phi([u, v]) = \Phi(uv - vu) = \theta(u)\Phi(v) - \theta(v)\Phi(u) = \deg(v)[u, v] - \deg(u)[v, u] = \deg([u, v])[u, v]$.

So we define ϕ by $\phi(u) = \Phi(u)/\deg(u)$ if $\deg(u) > 0$, giving the desired retraction from the associative algebra to the Lie algebra.

Exercise 61 Work out the terms of Dynkins formula of degree up to 3. (Answer: $x + y + [x, y]/2 + [x, [x, y]]/12 + [y, [y, x]]/12$.)

5 Free things

The free monoid on n generators $a_1, \ldots a_n$ has elements $a_{i_1} a_{i_2}$ corresponding to all finite sequences $i_1, i_2, \ldots$ of $1, \ldots n$ in the obvious way. These elements form a basis of the free algebra on these generators (which is the monoid ring of the free monoid). In particular the free algebra, graded so that all generators have degree 1, and a degree m piece of dimension n^m.

Example 62 The free Lie algebra on n generators $a, b, c, \ldots$ is graded by giving all generators degree 1, and we can ask for the dimension of the piece of degree m; in other words how many independent expressions can we form using the Lie bracket $m - 1$ times. We can solve this using the PBW theorem. The point is that the UEA of a free Lie algebra is the free associative algebra on $a, b, c, \ldots$,whose piece of degree m has dimension n^m. By the PBW theorem the UEA is the "same size" as the polynomial algebra over the free Lie algebra. So if the free Lie algebra has k_m independent elements of degree m, then

$$\frac{1}{(1-t)^{k_1}} \frac{1}{(1-t^2)^{k_2}} \cdots = 1 + nt + n^2 t^2 + \cdots$$

(where the left is the Poincare series of the symmetric algebra of the UEA, and the right is the Poincare series of the free associative algebra). So this gives a recursive way to calculate the numbers k_m, especially if we take logs of both sides:

$$\sum_i k_i t^{ij}/j = \log(1/(1-nt)) = \sum_i n^i t^i / i$$

The dimension $M(\alpha, n)$ of the degree n piece of the free Lie algebra on α generators is called a necklace polynomial, and by Moebius inversion is given by

$$M(\alpha, n) = \frac{1}{n} \sum_{d|n} \mu(n/d) \alpha^d$$

$$M(\alpha, 1) = \alpha$$

$$M(\alpha, 2) = \frac{\alpha^2 - \alpha}{2}$$

$$M(\alpha, 3) = \frac{\alpha^3 - \alpha}{3}$$

$$M(\alpha, 4) = \frac{\alpha^4 - \alpha^2}{4}$$

Exercise 63 Show that the necklace polynomial $M(\alpha, n)$ counts the number of aperiodic necklaces with n beads of α colors. (Apreiodic means that the necklace cannot be obtained by repeating some smaller necklace. Neckalces are the same if one can be obtained by rotating another, but "flipping" is not allowed.) Show that if q is a prime power then $M(q, n)$ is the number of irreducible monic polynomials of degree n over the field of q elements. Show that

$$(1 - \alpha z) = \prod_n (1 - z^n)^{M(\alpha, n)}.$$

We can construct a totally ordered basis H for the free Lie algebra on a totally ordered set X using Hall sets as follows. The set H is the union of sets H_1, H_2, of degrees 1, 2, ...and if u has length less than v then $u < v$. The set H_1 is just X. The set H_2 is the elements $[u, v]$ with $u, v \in H_1, u < v$. The elements of length at least 3 are those of the form $[u[vw]]$ with $v \leq u < [u, v]$ and $v < w$ and $u, v, w, [[vw]$ all in H. We choose any total ordering on H_n. We will not give a proof that this works as we do not use this result later.

Exercise 64 Find the sets H_1, H_2, H_3, H_4, H_5 for a free Lie algebra on 2 generators (for some choice of ordering in H_i).

A useful variation of the free monoid is the free group on generators $a, b, \ldots$, which is the same as the monoid on generators $a, A, b, B, \ldots$ with the relations $aA = Aa = 1$ and so on. We review some basic facts about free groups.

Lemma 65 *Each element of the free group has a unique representative given the product of a sequence of elements $a, A = a^{-1}, b, B = b^{-1}, \ldots$ such that no generator occurs next to its inverse. In other words, there are no "unexpected" relations between generators of a free group.*

Proof It is obvious that any element of the free group can be written in this form, and the problem is to show that this representative is unique. If $X = Y$ then $XY^{-1} = 1$, so this reduces to checking that non-empty representative is not the identity element. This is the usual problem for things given by generators and relations of showing that there is no unexpected collapse, and a good way to show this is to find explicit representations where given elements are obviously nontrivial. We will do this by constructing some explicit finite permutation representations.

Given a product $X = x_n \cdots x_2 x_1 \cdots$ of $n > 0$ elements $a, A, b, B, \ldots$ with no generator next to its inverse we will construct an action of the free group on a finite set of $n + 1$ points $1, 2, \ldots n + 1$ such that X takes 1 to $n + 1$. We first decree that $x_1(1) = 2$, $x_2(2) = 3$, and so on. We need to extend this to an action of each generator a on 1, 2, ..., $n + 1$. But since a does not occur next to A in X, the conditions on a are consistent so we can extend the action of a to the whole of $1, \ldots, n + 1$. So we get an action of the free group on $n + 1$ points with X acting nontrivially, which shows that X is not the identity. □

In fact we have shown a little more: free groups are residually finite, meaning that for any nontrivial element we can find a finite index (normal) subgroup

containing it. Another way of thinking about this is that elements can be detected by homomorphisms to finite groups. (In general if P is some property of groups, then "residually P" means that any two distict elements of the group can be separated by a quotient group with property P.)