We can ask if the group is determined by the group ring. The answer is "no" if the group ring is considered as an associative algebra: for example, the complex group ring of a finite abelian group is just a sum of copies of $\mathbb{C}$ corresponding to the irreducible representations, so two finite abelian groups have isomorphic group rings if and only if they have the same order. However the group can be recovered from the Hopf algebra as the group-like elements:

Definition 38 *An element of a Hopf algebra is called group-like if* $\Delta(a) = a \otimes a$ *and* $(a) = 1$.

Exercise 39 Show that the group-like elements of a Hopf algebra form a group. Show that the group-like elements of a group ring of G form a group that can be naturally identified with the group G. What is the group of group-like elements of the universal enveloping algebra of a Lie algebra?

The universal enveloping algebra is not the only analogue of the group ring for a Lie group. Another analogue, often used in analysis, is the algebra of continuous (or smooth) functions of compact support (or L^1 functions, or finite measures...) under convolution. For p-adic groups one can take the locally constant functions with compact support. These algebras look more like the group algebra of a finite group, but is less convenient in some ways as they need not have a coproduct.

Example 40 The main point of all this is that the UEA of a Lie algebra is a Hopf algebra. In other words it behaves as if it were a group or group ring, which is of course an approximation to the Lie group of the Lie algebra. The map from Ug to $Ug \otimes Ug$ is given by the Leibniz formula $g \mapsto 1 \otimes g + g \times 1$ from calculus. This is really just the formula telling you how to differentiate a product: $\frac{d}{dx}(fg) = \frac{d}{dx}(f)g + f\frac{d}{dx}(g)$, where you can see the map $\frac{d}{dx} \mapsto \frac{d}{dx} \otimes 1 + 1 \otimes \frac{d}{dx}$.

The fact that the map Δ extends to a ring homomorphism follows from the universal property of the UEA.

We would like to reconstruct the Lie algebra from its universal enveloping algebra in the same way we reconstructed a group from its group algebra.

Definition 41 *An element of a Hopf algebra is called primitive if it satisfies the Leibniz identity* $\Delta(a) = a \otimes 1 + 1 \otimes a$.

Exercise 42 Show that the primitive elements of a Hopf algebra form a Lie algebra.

A natural guess is that the Lie algebra consists of the primitive elements of the universal enveloping algebra. This fails over fields of positive characteristic p:

Exercise 43 If a is primitive in a Hopf algebra of prime characteristic $p > 0$, so is a^p. Find the Lie algebra of primitive elements of the universal enveloping algebra of a 1-dimensional Lie algebra over the finite field $\mathbb{F}_p$.

Sometimes in characteristic p one works with restricted Lie algebras: these are Lie algebras together with a "p'th power operation" $a \mapsto a^[p]$ behaving like the p-th power of derivations.

Lemma 44 *Over a field of characteristic 0, an element of the UEA is primitive if and only if it is in the Lie algebra.*

Proof It is obvious that elements of the Lie algebra are primitive, so we need to show that primitive elements are in the Lie algebra. By the PBW theorem, the coalgebra structures on any two Lie algebras of the same dimension are isomorphic, so we can just the lemma for one Lie algebra of any dimension, say the abelian one. But in this case the dual of the coalgebra is a ring of power series (since we are in char 0). Primitive elements have to vanish on all decomposable elements, which are all elements of degree at least 2, so primitive elements have degree 1 and are therefore in the Lie algebra. □ The proof fails

in positive characteristic because the dual algebra of the coalgebra of a UEA is no longer a power series ring. If the coalgebra is $Z[D]$ then the dual algebra is $Z[\{x^i/i!\}]$, so reducing mod p we get an algebra generated by elements of degrees p^n each of which has p'th power 0. This is another indication that the UEA is the wrong object if we are not working over fields of char 0.

There is a second way to associate a Hopf algebra to a Lie group, which is in some sense dual to the UEA, which is to take the ring of polynomial functions on an (algebraic) Lie group. The UEA consists of (left invariant) differential operators and is cocommutative but not usually commutative, while the ring of (polynomial) functions is commutative but not usually cocommutative. It works as follows: suppose that G is an algebraic group contained in R^n. Then it has a coordinate ring $O(G) = R[x_1.\cdots,x_n]/(I)$ where the ideal I is the polynomials vanishing on R. The product map $G \times G \mapsto G$ induces a dual map $O(G) \mapsto O(G) \otimes O(G)$, and similarly the unit of G induces a map $O(G) \mapsto R$, so we have all the data for a commutative Hopf algebra.

Example 45 Suppose G is the general linear group $SL_2(R)$. Then the coordinate ring is $O(G) = R[a,b,c,d]/(ad - bc - 1)$. The coproduct is given by the group product:

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}$$

so $\Delta(a) = a \otimes a + b \otimes c$, $\Delta(b) = a \otimes b + b \otimes d$, $\Delta(c) = c \otimes a + d \otimes b$, $\Delta(d) = c \otimes b + d \otimes d$. The counit is given by $\eta(a) = 1$, $\eta(b) = 0$, $\eta(c) = 0$, $\eta(d) = 1$. The antipode is $S(a) = d$, $S(b) = -b$, $S(c) = -c$, $S(d) = a$.

Example 46 Following Quillen and Milnor, we will show that the Steenrod algebra in algebraic topology is a sort of infinite dimensional Lie group.

First recall the original definition of the Steenrod algebra. The Steenrod algebra is the algebra of stable cohomology operations mod 2, so can be found by calculating the cohomology of Eilenberg–Maclane spaces, which was originally done by H. Cartan and Serre. They showed that the Steenrod algebra is the algebra over F_2 generated by elements Sq^q for $q = 1, 2, 3 \cdots$ modulo the Adem relations

$$Sq^i Sq^j = \sum_{k=0}^{[i/2]} \binom{j-k-1}{i-2k} Sq^{i+j-k} Sq^k$$

which not even algebraic topologists are able to remember. Cartan also gave a formula for the action of Steenrod squares on a cup product

$$Sq^n(x \cup y) = \sum_{i+j=n} (Sq^i x) \cup (Sq^j y)$$

which we know should be interpreted as a coproduct on the Steenrod algebra

$$\Delta Sq^n = \sum_{i+j=n} Sq^i \otimes Sq^j$$

In other words the Steenrod algebra is a cocommutative Hopf algebra over the field with 2 elements. A cocommutative Hopf algebra should be thought of as something like a (universal enveloping algebra of a Lie) group, so should be related to the automorphisms of something. We will show that the Steenrod algebra is in some sense the automorphism group of the 1-dimensional additive group.

At first sight this makes no sense. The automorphism group of the additive Lie group R is just R^* which looks nothing like the Steenrod algebra. This is because we need to look more closely at this group, where by "more closely" we mean infinitesimally.

So first look at infinitesimal automorphisms of the real line fixing 0. These can be written as formal power series

$$x \mapsto a_0 x + a_1 x^2 + \cdots$$

with a_0 invertible. The product of this group is by composition of power series (which accounts for the funny grading of the coefficients). We can do this all over the integers Z. Then this group is represented by the ring $Z[a_0, a_0^{-1}, a_1, a_2, \ldots]$, which has a complicated coproduct map describing the group product.

Exercise 47 Find the image of a_0, a_1, and a_2 under the coproduct map.

To get the Steenrod algebra, we restrict to the subgroup of automorphisms of the line preserving the additive group structure, in other words we want the power series f with $f(x+y) = f(x) + f(y)$. The problem is that there are non (except for multiplication by constants). This is because we forgot to reduce mod p. If we work mod a prime p there are now plenty of additive homomorphisms, in particular the Frobenius map $x \mapsto x^p$ and its powers $x \mapsto x^{p^n}$. So the group of infinitesimal automorphisms of the additive group consists of the maps

$$x \mapsto a_0 x + a_{p-1} x^p + a_{p^2-1} x^{p^2} + \cdots$$

. (with a_0 invertible). So the coordinate ring of the corresponding group is $F_p[x_0, x_0^{-1}, a_{p-1}, a_{p^2-1}, \cdots]$. Now we need to find the coproduct on this corresponding to composition of functions. Suppose we have two group elements

$$x \mapsto f(x) = a_0 x + a_{p-1} x^p + a_{p^2-1} x^{p^2} + \cdots$$

and

$$x \mapsto g(x) = b_0 x + b_{p-1} x^p + b_{p^2-1} x^{p^2} + \cdots$$

. We want to calculate $f(g(x))$. This is given by

$$f(g(x)) = \sum a_{p^i-1}(\sum b_{p^j-1}x^{p^j})^{p^i} \tag{3}$$

$$= \sum a_{p^i-1}b_{p^j-1}^{p^i}x^{p^{i+j}} \tag{4}$$

so the coproduct is given by Milnor's formula

$$\Delta(a_{p^n-1}) = \sum_{i+j=n} a_{p^i-1} \otimes a_{p^j-1}^{p^i}.$$

or

$$\Delta(a_0) = a_0 \otimes a_0$$

$$\Delta(a_1) = a_0 \otimes a_1 + a_1 \otimes a_0^2$$

$$\Delta(a_3) = a_0 \otimes a_3 + a_1 \otimes a_1^2 + a_3 \otimes a_0^4$$

$$\Delta(a_7) = a_0 \otimes a_7 + a_1 \otimes a_3^2 + a_3 \otimes a_1^4 + a_7 \otimes a_0^8$$

We get the classical Steenrod algebra from this (for $p = 2$) by making 2 minor changes: we identify a_0 with 1, and (following Milnor) we take the graded dual (so that the Steenrod algebra is cocommutative rather than commutative). So, as Quillen pointed out, the mysterious Adem relations turn out to be a disguised form of the rule for composing two formal power series.

We can try to understand the structure of the Steenrod algebra by pretending that it is a Lie group. So we should ask if it is solvable/nilpotent/simple. It is graded by the non-negative integers, so it has an abelian degree 0 piece on the top, and then the rest of it is almost nilpotent: more precisely it is pro-nilpotent, a projective limit of nilpotent objects. So the Steenrod algebra itself should be thought of as a pro-solvable infinite dimensional Lie group. (The correct terminology is affine group scheme.) For any commutative R ring the group $S(R)$ has a decreasing filtration $S_0 \subset S_{p-1} \subseteq S_{p^2-1} \subseteq \cdots$, where S_{p^n-1} for $n > 0$ consists of the automorphisms $x \mapsto x + a_{p^n-1}x^{p^n} + \cdots$. So S_0/S_{p-1} is the multiplicative group of R, and $S_{p^n-1}/S_{p^{n+1}-1}$ is the additive group of R.