The Dual Steenrod Algebra (Lecture 13)

We have seen that the Steenrod algebra $\mathbb{A}$ admits a comultiplication map $\mathbb{A} \otimes \mathbb{A} \to \mathbb{A}$, described by the formula

$$\text{Sq}^n \mapsto \sum_{n=n'+n''} \text{Sq}^{n'} \otimes \text{Sq}^{n''}.$$ 

This comultiplication map is obviously symmetric, and therefore endows the graded dual $\mathbb{A}^\vee = \oplus_n (\mathbb{A}^n)^\vee$ with the structure of a commutative ring. Our goal in this lecture is to understand the structure of $\mathbb{A}^\vee$.

For the remainder of this lecture, we will work in the category of (affine) schemes over the field $\mathbb{F}_2$. (In other words, we work in the opposite to the category of commutative $\mathbb{F}_2$-algebras.)

The noncommutative multiplication on $\mathbb{A}$ induces a comultiplication map $\mathbb{A}^\vee \otimes \mathbb{A}^\vee \to \mathbb{A}^\vee$, which in turn determines a map of $\mathbb{F}_2$-schemes

$$\text{Spec } \mathbb{A}^\vee \times \text{Spec } \mathbb{A}^\vee \to \text{Spec } \mathbb{A}^\vee.$$ 

This map exhibits $\text{Spec } \mathbb{A}^\vee$ as a group scheme over the field $\mathbb{F}_2$. Let us henceforth denote this group scheme by $G$.

For every topological space $X$, the Steenrod algebra acts on the cohomology ring $H^*(X)$ via a map $\mathbb{A} \otimes H^*(X) \to H^*(X)$. If the cohomology ring $H^*(X)$ is finite dimensional, then we can transpose this action to obtain a map

$$H^*(X) \to H^*(X) \otimes \mathbb{A}^\vee.$$ 

Rephrasing this in the language of algebraic geometry, we get a map

$$G \times \text{Spec } H^*(X) \to \text{Spec } H^*(X).$$

This map endows the scheme $\text{Spec } H^*(X)$ with an action of the group scheme $G$.

If $H^*(X)$ is not finite-dimensional, then we need to be a bit more careful. Suppose instead that $H^*(X)$ is finite dimensional in each degree. For each $n \geq 0$, the direct sum $R_n = \oplus_{0 \leq k \leq n} H^k(X)$ can be viewed as a quotient of the cohomology ring $H^*(X)$, and inherits the structure of an unstable $\mathbb{A}$-algebra. Using the above argument, we obtain an action

$$G \times \text{Spec } R_n \to \text{Spec } R_n.$$ 

Moreover, if $n = 1$, then this action is trivial.

Let us now specialize to the case where $X$ is the space $\mathbb{R}P^\infty$. In this case, the cohomology ring $H^*(X)$ is isomorphic to $\mathbb{F}_2[t]$. We therefore have isomorphisms $R_n \simeq \mathbb{F}_2[t]/(t^{n+1})$ for $n \geq 0$. For each $n \geq 0$, there exists a group scheme parametrizing automorphisms of $\text{Spec } R_n$ which induce the identity on $\text{Spec } R_1$. We will denote this group scheme by $H_n$. By definition, $H_n$ has the following universal property:

$$\text{Hom}(\text{Spec } B, H_n) \simeq \text{Hom}^0(\text{Spec } B \times \text{Spec } R_n, \text{Spec } R_n) \simeq \text{Hom}^0(\mathbb{F}_2[t]/(t^{n+1}), B[t]/(t^{n+1}B)) \simeq t + t^2 B/(t^{n+1}B),$$

(here the superscripts indicate the requirement that the morphism reduce to the identity on $R_1$) so $H_n$ is just isomorphic to an $(n-1)$-dimensional affine space $\mathbb{A}^{n-1}$. Let $H_\infty$ denote the inverse limit of the tower

$$\ldots \to H_2 \to H_1 \to H_0,$$
so that $H_\infty$ is the infinite dimensional affine space which is the automorphism group of the formal scheme $\text{Spf } \mathbb{F}_2[[t]]$. More concretely, we are just saying that every automorphism of the power series ring $B[[t]]$ which reduces to the identity modulo $t^2$ is given by a transformation

$$t \mapsto t + b_1 t^2 + b_2 t^3 + \ldots,$$

so we get an identification $H_\infty \cong \text{Spec } \mathbb{F}_2[b_1, b_2, \ldots]$.

The above analysis gives us a map of group schemes $\phi : G \to H_\infty$. Our first result is:

**Proposition 1.** The map $\phi : G \to H_\infty$ is a monomorphism.

To prove this, let $G_0 \subseteq G$ be the kernel of the homomorphism $\phi$. Then $G_0$ acts trivially on the formal spectrum $\text{Spf } H^*(\mathbb{R}P^\infty)$. It follows that the diagonal action of $G_0$ on

$$\text{Spf } H^* (\mathbb{R}P^\infty) \times \ldots \times \text{Spf } H^* (\mathbb{R}P^\infty) \cong \text{Spf } H^* (\mathbb{R}P^\infty)$$

is trivial for all $k$.

We observe that $G_0 = \text{Spec } C$, where $C$ is some Hopf algebra quotient of the dual Steenrod algebra $A^\vee$. It is not difficult to see that $C$ inherits a grading from $A^\vee$, so that the graded dual $C^\vee$ can be identified with a subalgebra of the Steenrod algebra $A$. The above analysis shows that $C^\vee$ acts trivially on the cohomology $H^*(\mathbb{R}P^\infty)^k$ for all $k \geq 0$. We claim that $C^\vee \cong \mathbb{F}_2$. If not, then we can find some nonconstant element of $C^\vee$ of the form $\sum I_n \Sigma^{I_n}$, where $I_n$ ranges over some collection of admissible positive sequences. Choosing $k$ larger than the excess of each $I_n$, we see that $C^\vee$ acts nontrivially on $t_1 \ldots t_k \in H^k((\mathbb{R}P^\infty)^k)$, a contradiction. Thus $C^\vee \cong \mathbb{F}_2$, so $G_0 \cong \text{Spec } \mathbb{F}_2$ and the map $\phi$ is a monomorphism as desired.

We now wish to describe the image of the map $\phi$. For this, we observe that the formal affine line $\mathbb{A}^1 \cong \text{Spf } \mathbb{F}_2[[t]]$ is isomorphic to the formal additive group over the field $\mathbb{F}_2$. In other words, we have an addition map

$$\mathbb{A}^1 \times \mathbb{A}^1 \to \mathbb{A}^1,$$

which is described in coordinates by the map of power series rings

$$\mathbb{F}_2[[t]] \to \mathbb{F}_2[[t_1, t_2]]$$

$$t \mapsto t_1 + t_2.$$

In fact, this map comes from topology. The group $\Sigma_2$ is abelian, so the multiplication map

$$\Sigma_2 \times \Sigma_2 \to \Sigma_2$$

is a group homomorphism. It follows that we obtain a map of classifying spaces

$$B\Sigma_2 \times B\Sigma_2 \cong B(\Sigma_2 \times \Sigma_2) \to B\Sigma_2.$$

The induced map on cohomology

$$H^*(\mathbb{R}P^\infty) \to H^*(\mathbb{R}P^\infty \times \mathbb{R}P^\infty)$$

is also described by the formula

$$t \mapsto t_1 + t_2.$$

It follows that the action of the Steenrod algebra $A$ is compatible with the comultiplication on $H^*(\mathbb{R}P^\infty)$. In other words, the action of the group scheme $G = \text{Spec } A^\vee$ on the formal affine line $\mathbb{A}^1$ preserves the group structure on $\mathbb{A}^1$.

Let $\text{End}(\mathbb{A}^1)$ denote the subgroup scheme of $H_\infty$ which preserves the group structure on $\mathbb{A}^1$. We note that a $B$-valued point of $H_\infty$ is an automorphism of $B[[t]]$ of the form

$$t \mapsto t + b_1 t^2 + b_2 t^3 + \ldots.$$
This $B$-valued point belong to $\text{End}(A^1)$ if and only if the power series $f(t) = t + b_1t^2 + b_3t^3 + \ldots$ is additive, in the sense that $f(t_1 + t_2) = f(t_1) + f(t_2) \in B[[t_1, t_2]]$. Since we are working in characteristic 2, additivity is equivalent to the requirement that the terms $b_i t^i$ vanish unless $i$ is a power of 2. In other words, we can identify $\text{End}(A^1)$ with the infinite dimensional affine space parametrizing power series of the form
\[ t + b_1t^2 + b_3t^4 + b_7t^8 + \ldots. \]

**Theorem 2.** The map $\phi$ induces an isomorphism $G \to \text{End}(A^1)$.

In other words, we claim that the corresponding map of commutative rings
\[ \psi : F_2[b_1, b_3, b_7, \ldots] \to A^\vee \]
is an isomorphism. Proposition 1 implies that $\psi$ is surjective. Moreover, $\psi$ is a map of graded rings, where each $b_i$ is regarded as having degree $i$. It will therefore suffice to show that the algebras $F_2[b_1, b_3, b_7, \ldots]$ and $A^\vee$ have the same dimensions in each degree.

Fix an integer $n \geq 0$. The $n$th graded piece of $F_2[b_1, b_3, b_7, \ldots]$ is spanned by monomials
\[ b_1^{i_1}b_3^{i_2}b_7^{i_3} \ldots, \]
which are indexed by sequences of nonnegative integers $(\epsilon_1, \epsilon_2, \ldots)$ satisfying $\sum_k (2^k - 1)\epsilon_k = n$.

We have also seen that the the Steenrod algebra $A$ has a basis consisting of expressions $Sq^I = Sq^{i_1} Sq^{i_2} \ldots Sq^{i_m}$, where the quantities
\[ \delta_k = \begin{cases} 
  i_k - 2i_{k+1} & \text{if } k < m \\
  i_m & \text{if } k = m \\
  0 & \text{if } k > m
\end{cases} \]
are required to be nonnegative. Moreover, we have
\[ i_k = \delta_k + 2\delta_{k+1} + 4\delta_{k+2} + \ldots \]
so that the total degree of $Sq^I$ is
\[ \sum_{k \geq 0} i_k = \sum_{k > 0, m \geq 0} \delta_{k+m}2^m = \sum_{k' > 0} \delta_{k'}(2^{k'} - 1). \]

We therefore obtain a bijection from a basis of $F_2[b_1, b_3, \ldots]^n$ to a basis of $A^n$, given by the correspondence
\[ (\epsilon_1, \epsilon_2, \ldots) \mapsto (\delta_1, \delta_2, \delta_3, \ldots). \]

**Remark 3.** In fact, more is true: the bijection described above is actually upper-triangular with respect to duality between $A$ and $F_2[b_1, b_3, \ldots]$ determined by the ring homomorphism $\psi$. This is implicit in our proof that the admissible monomials are linearly independent in $A$.

**Corollary 4.** The dual Steenrod algebra $A^\vee$ is isomorphic to a polynomial ring $F_2[b_1, b_3, b_7, \ldots]$.

We can describe the comultiplication on $A^\vee$ (and therefore the multiplication on $A$) very concretely in terms of the isomorphism of Corollary 4. This comultiplication corresponds to the group structure on $\text{End}(A^1)$: in other words, it corresponds to composition of transformations having the form $t \mapsto t + b_1t^2 + b_3t^4 + \ldots$. Let $f(t) = \sum_{i \geq 0} b_{2i-1}t^{2i}$ and $g(t) = \sum_{j \geq 0} b_{2j-1}t^{2j}$. Then
\[ (f \circ g)(t) = \sum_{i,j \geq 0} b_{2i-1}(b'_{2j-1})^{2i} t^{2i+j}. \]
Consequently, the comultiplication on the ring $\mathbb{F}_2[b_1, b_3, \ldots]$ can be described by the formula

$$b_{2^{i+j} - 1} \mapsto \sum_{k=i+j} b_{2^{i+j} - 1} \otimes b^{2^i}_{2^j - 1}.$$ 

Here we include the extreme possibilities $i = 0$ and $j = 0$, in which case we agree to the convention that $b_0 = 1 \in \mathbb{F}_2[b_1, b_3, \ldots]$.

**Remark 5.** The results above describe the dual Steenrod algebra $A^\vee$ as the algebra of functions on the algebraic group $G \simeq \text{End}(\mathbb{A}^1)$. We get a dual description of the Steenrod algebra $A$ itself as an algebra of distributions on the group $G$: namely, $A$ is isomorphic to the space of distributions on $G$ which are set-theoretically supported at the identity. In this language, the (noncommutative) multiplication on $A$ is induced by convolution.