ANNALS OF MATHEMATICS
Vol. 67, No. 1, January, 1958
Printed in Japan

THE STEENROD ALGEBRA AND ITS DUAL[1]

BY JOHN MILNOR

(Received May 15, 1957)

1. Summary

Let $\mathscr{S}^*$ denote the Steenrod algebra corrresponding to an odd prime p. (See §2 for definitions.) Our basic results (§3) is that $\mathscr{S}^*$ is a Hopf algebra. That is in addition to the product operation

$$\mathscr{S}^* \otimes \mathscr{S}^* \xrightarrow{\phi^*} \mathscr{S}^*$$

there is a homomorphism

$$\mathscr{S}^* \xrightarrow{\psi^*} \mathscr{S}^* \otimes \mathscr{S}^*$$

satisfying certain conditions. This homomorphism ψ^* relates the cup product structure in any cohomology ring $H^*(K, Z_p)$ with the action of $\mathscr{S}^*$ on $H^*(K, Z_p)$. For example if $\mathscr{P}^n \in \mathscr{S}^{2n(p-1)}$ denotes a Steenrod reduced p^{th} power then

$$\psi^*(\mathscr{P}^n) = \mathscr{P}^n \otimes 1 + \mathscr{P}^{n-1} \otimes \mathscr{P}^1 + \cdots + 1 \otimes \mathscr{P}^n .$$

The Hopf algebra

$$\mathscr{S}^* \xrightarrow{\psi^*} \mathscr{S}^* \otimes \mathscr{S}^* \xrightarrow{\phi^*} \mathscr{S}^*$$

has a dual Hopf algebra

$$\mathscr{S}_* \xleftarrow{\psi_*} \mathscr{S}_* \otimes \mathscr{S}_* \xleftarrow{\phi_*} \mathscr{S}_* .$$

The main tool in the study of this dual algebra is a homomorphism

$$\lambda^*: H^*(K, Z_p) \to H^*(K, Z_p) \otimes \mathscr{S}_*$$

which takes the place of the action of $\mathscr{S}^*$ on $H^*(K, Z_p)$. (See §4.) The dual Hopf algebra turns out to have a comparatively simple structure. In fact as an algebra (ignoring the "diagonal homomorphism" ϕ_*) it has the form

$$E(\tau_0, 1) \otimes E(\tau_1, 2p-1) \otimes \cdots \otimes P(\xi_1, 2p-2) \otimes P(\xi_2, 2p^2-2) \otimes \cdots ,$$

where $E(\tau_i, 2p^i - 1)$ denotes the Grassmann algebra generated by a certain element $\tau_i \in \mathscr{S}_{2p^i-1}$, and $P(\xi_i, 2p^i-2)$ denotes the polynomial algebra generated by $\xi_i \in \mathscr{S}_{2p^i-2}$.

[1] The author holds an Alfred P. Sloan fellowship.

In § 6 the above information about $\mathscr{S}_*$ is used to give a new description of the Steenrod algebra $\mathscr{S}^*$. An additive basis is given consisting of elements

$$Q_0^{\varepsilon_0} Q_1^{\varepsilon_1} \cdots \mathscr{P}^{r_1 r_2 \cdots}$$

with $\varepsilon_i = 0, 1$; $r_i \geqq 0$. Here the elements Q_i can be defined inductively by

$$Q_0 = \delta,\ Q_{i+1} = \mathscr{P}^{p^i} Q_i - Q_i \mathscr{P}^{p^i} ;$$

while each $\mathscr{P}^{r_1 \cdots r_k}$ is a certain polynomial in the Steenrod operations,[2] of dimension

$$r_1(2p-2) + r_2(2p^2-2) + \cdots + r_k(2p^k-2) .$$

The product operation and the diagonal homomorphism in $\mathscr{S}^*$ are explicitly computed with respect to this basis.

The Steenrod algebra has a canonical anti-automorphism which was first studied by R. Thom. This anti-automorphism is computed in § 7. Section 8 is devoted to miscellaneous remarks. The equation $\theta \mathscr{P}^1 = 0$ is studied; and a proof is given that $\mathscr{S}^*$ is nil-potent.

A brief appendix is devoted to the case $p = 2$. Since the sign conventions used in this paper are not the usual ones (see § 2), a second appendix is concerned with the changes necessary in order to use standard sign conventions.

2. Prerequisites: sign conventions, Hopf algebras, the Steenrod algebra

If a and b are any two objects to which dimensions can be assigned, then whenever a and b are interchanged the sign $(-1)^{\dim a \dim b}$ will be introduced. For example the formula for the relationship between the homology cross product and the cohomology cross product becomes

$$(1) \qquad \langle \mu \times \nu, \alpha \times \beta \rangle = (-1)^{\dim \nu \dim \alpha} \langle \mu, \alpha \rangle \langle \nu, \beta \rangle .$$

This contradicts the usual usage in which no sign is introduced. In the same spirit we will call a graded algebra *commutative* if

$$ab = (-1)^{\dim a \dim b} ba .$$

Let $A = (\cdots, A_{-1}, A_0, A_1, \cdots)$ be a graded vector space over a field F. The dual A' is defined by $A'_n = \mathrm{Hom}\,(A_{-n}, F)$. The value of a homomorphism a' on $a \in A$ will be denoted by $\langle a', a \rangle$. It is understood that $\langle a', a \rangle = 0$ unless $\dim a' + \dim a = 0$. (By an element of A we mean an element of some A_n.) Similarly we can define the dual A'' of A'. Identify

[2] This has no relation to the generalized Steenrod operations $\mathscr{P}^I$ defined by Adem.

each $a \in A$ with the element $a'' \in A''$ which satisfies

$$(2) \qquad \langle a'', a' \rangle = (-1)^{\dim a'' \dim a'} \langle a', a \rangle$$

for each $a' \in A'$. Thus every graded vector space A is contained in its double dual A''. If A is of finite type (that is if each A_n is a finite dimensional vector space) then A is equal to A''.

Now if $f\colon A \to B$ is a homomorphism of degree zero then $f'\colon B' \to A'$ and $f''\colon A'' \to B''$ are defined in the usual way. If A and B are both of finite type it is clear that $f = f''$.

The tensor product $A \otimes B$ is defined by $(A \otimes B)_n = \sum_{i+j=n} A_i \otimes B_j$, where "$\sum$" stands for "direct sum". If A and B are both of finite type and if $A_i = B_i = 0$ for all sufficiently small i (or for all sufficiently large i) then the product $A \otimes B$ is also of finite type. In this case the dual $(A \otimes B)'$ can be identified with $A' \otimes B'$ under the rule

$$(3) \qquad \langle a' \otimes b', a \otimes b \rangle = (-1)^{\dim a \dim b'} \langle a', a \rangle \langle b', b \rangle .$$

In practice we will use the notation A_* for a graded vector space A satisfying the condition $A_i = 0$ for $i < 0$. The dual will then be denoted by A^* where $A^n = A'_{-n} = \mathrm{Hom}(A_n, F)$. A similar notation will be used for homomorphisms.

By a *graded algebra* (A_*, ψ_*) is meant a graded vector space A_* together with a homomorphism

$$\psi_*\colon A_* \otimes A_* \to A_* .$$

It is usually required that ψ_* be associative and have a unit element $1 \in A_0$. The algebra is *connected* if the vector space A_0 is generated by 1.

By a *connected Hopf algebra* (A_*, ψ_*, ϕ_*) is meant a connected graded algebra with unit (A_*, ψ_*), together with a homomorphism

$$\phi_*\colon A_* \to A_* \otimes A_*$$

satisfying the following two conditions.

2.1. ϕ_* is a homomorphism of algebras with unit. Here we refer to the product operation ψ_* in A_* and the product

$$(a_1 \otimes a_2)\cdot(a_3 \otimes a_4) = (-1)^{\dim a_2 \dim a_3} (a_1 \cdot a_3) \otimes (a_2 \cdot a_4)$$

in $A_* \otimes A_*$.

2.2. For $\dim a > 0$, the element $\phi_*(a)$ has the form $a \otimes 1 + 1 \otimes a + \sum b_i \otimes c_i$ with $\dim b_i, \dim c_i > 0$.

Appropriate concepts of associativity and commutativity are defined, not only for the product operation ψ_*, but also for the diagonal homomorphisms ϕ_*. (See Milnor and Moore [3]).

To every connected Hopf algebra (A_*, ψ_*, ϕ_*) of finite type there is associated the *dual Hopf algebra* (A^*, ϕ^*, ψ^*), where the homomorphisms

$$A^* \xrightarrow{\psi^*} A^* \otimes A^* \xrightarrow{\phi_*} A^*$$

are the duals in the sense explained above. For the proof that the dual is again a Hopf algebra see [3].

(As an example, for any connected Lie group G the maps $G \xrightarrow{d} G \times G \xrightarrow{p} G$ give rise to a Hopf algebra $(H_*(G), p_*, d_*)$. The dual algebra $(H^*(G), \smile, p^*)$ is essentially the example which was originally studied by Hopf.)

For any complex K the Steenrod operation $\mathscr{P}^i$ is a homomorphism

$$\mathscr{P}^i\colon H^j(K, Z_p) \to H^{j+2i(p-1)}(K, Z_p) .$$

The basic properties of these operations are the following. (See Steenrod [4].)

2.3. Naturality. If f maps K into L then $f^*\mathscr{P}^i = \mathscr{P}^i f^*$.

2.4. For $\alpha \in H^j(K, Z_p)$, if $i > j/2$ then $\mathscr{P}^i\alpha = 0$. If $i = j/2$ then $\mathscr{P}^i\alpha = \alpha^p$. If $i = 0$ then $\mathscr{P}^i\alpha = \alpha$.

2.5. $\mathscr{P}^n(\alpha \smile \beta) = \sum_{i+j=n} \mathscr{P}^i\alpha \smile \mathscr{P}^j\beta$.

We will also make use of the coboundary operation $\delta\colon H^j(K, Z_p) \to H^{j+1}(K, Z_p)$ associated with the coefficient sequence

$$0 \to Z_p \to Z_{p^2} \to Z_p \to 0 .$$

The most important properties here are

2.6. $\delta\delta = 0$ and

2.7. $\delta(\alpha \smile \beta) = (\delta\alpha) \smile \beta + (-1)^{\dim \alpha}\alpha \smile \delta\beta$, as well as the naturality condition.

Following Adem [1] the Steenrod algebra $\mathscr{S}^*$ is defined as follows. The free associative graded algebra $\mathscr{F}^*$ generated by the symbols δ, $\mathscr{P}^0$, $\mathscr{P}^1$, $\cdots$ acts on any cohomology ring $H^*(K, Z_p)$ by the rule $(\theta_1\theta_2 \cdots \theta_k)\cdot\alpha = (\theta_1(\theta_2 \cdots (\theta_k\alpha) \cdots))$. (It is understood that δ has dimension 1 in $\mathscr{F}^*$ and that $\mathscr{P}^i$ has dimension $2i(p-1)$.) Let $\mathscr{J}^*$ denote the ideal consisting of all $f \in \mathscr{F}^*$ such that $f\alpha = 0$ for all complexes K and all cohomology classes $\alpha \in H^*(K, Z_p)$. Then $\mathscr{S}^*$ is defined as the quotient algebra $\mathscr{F}^*/\mathscr{J}^*$. It is clear that $\mathscr{S}^*$ is a connected graded associative algebra of finite type over Z_p. However $\mathscr{S}^*$ is not commutative.

(For an alternative definition of the Steenrod algebra see Cartan [2]. The most important difference is that Cartan adds a sign to the operation δ.)

The above definition is non-constructive. However it has been shown by Adem and Cartan that $\mathscr{S}^*$ is generated additively by the "basic monomials"

$$\delta^{\varepsilon_0}\mathscr{P}^{s_1}\delta^{\varepsilon_1}\cdots\mathscr{P}^{s_k}\delta^{\varepsilon_k}$$

where each ε_i is zero or 1 and

$$s_1 \geqq ps_2 + \varepsilon_1,\ s_2 \geqq ps_3 + \varepsilon_2,\ \cdots,\ s_{k-1} \geqq ps_k + \varepsilon_{k-1},\ s_k \geqq 1\ .$$

Furthermore Cartan has shown that these elements form an additive basis for $\mathscr{S}^*$.

3. The homomorphism ψ^*

LEMMA 1. *For each element θ of $\mathscr{S}^*$ there is a unique element $\psi^*(\theta) = \sum \theta'_i \otimes \theta''_i$ of $\mathscr{S}^* \otimes \mathscr{S}^*$ such that the identity*

$$\theta(\alpha \smile \beta) = \sum (-1)^{\dim\theta''_i \dim\alpha}\, \theta'_i(\alpha) \smile \theta''_i(\beta)$$

is satisfied for all complexes K and all elements $\alpha, \beta \in H^*(K)$. Furthermore

$$\mathscr{S}^* \xrightarrow{\psi^*} \mathscr{S}^* \otimes \mathscr{S}^*$$

is a ring homomorphism.

(By an "element" of a graded module we mean a homogeneous element. The coefficient group Z_p is to be understood.)

It will be convenient to let $\mathscr{S}^* \otimes \mathscr{S}^*$ act on $H^*(X) \otimes H^*(X)$ by the rule

$$(\theta' \otimes \theta'')(\alpha \otimes \beta) = (-1)^{\dim\theta''\dim\alpha}\,\theta'(\alpha) \otimes \theta''(\beta)\ .$$

Let $c\colon H^*(X) \otimes H^*(X) \to H^*(X)$ denote the cup product. The required identity can now be written as

$$\theta c(\alpha \otimes \beta) = c\psi^*(\theta)(\alpha \otimes \beta)\ .$$

PROOF OF EXISTENCE. Let $\mathscr{R}$ denote the subset of $\mathscr{S}^*$ consisting of all θ such that for some $\rho \in \mathscr{S}^* \otimes \mathscr{S}^*$ the required identity

$$\theta c(\alpha \otimes \beta) = c\rho(\alpha \otimes \beta)$$

is satisfied. We must show that $\mathscr{R} = \mathscr{S}^*$.

The identities

$$\delta(\alpha \smile \beta) = \delta\alpha \smile \beta + (-1)^{\dim\alpha}\,\alpha \smile \delta\beta$$

and

$$\mathscr{P}^n(\alpha \smile \beta) = \textstyle\sum_{i+j=n} \mathscr{P}^i\alpha \smile \mathscr{P}^j\beta$$

clearly show that the operations δ and $\mathscr{P}^n$ belong to $\mathscr{R}$. If θ_1, θ_2 belong to $\mathscr{R}$ then the identity

$$\theta_1\theta_2 c(\alpha \otimes \beta) = \theta_1 c\rho_2(\alpha \otimes \beta) = c\rho_1\rho_2(\alpha \otimes \beta)$$

show that $\theta_1\theta_2$ belongs to $\mathscr{R}$. Similarly $\mathscr{R}$ is closed under addition. Thus $\mathscr{R}$ is a subalgebra of $\mathscr{S}^*$ which contains the generators δ, $\mathscr{P}^n$ of $\mathscr{S}^*$. This proves that $\mathscr{R} = \mathscr{S}^*$.

PROOF OF UNIQUENESS. From the definition of the Steenrod algebra we see that given an integer n we can choose a complex Y and an element $\gamma \in H^*(Y)$ so that the correspondence

$$\theta \to \theta\gamma$$

defines an isomorphism of $\mathscr{S}^i$ into $H^{k+i}(Y)$ for $i \leqq n$. (For example take $Y = K(Z_p, k)$ with $k > n$.) It follows that the correspondence

$$\theta' \otimes \theta'' \xrightarrow{j} (-1)^{\dim\theta''\dim\gamma}\,\theta'(\gamma) \times \theta''(\gamma)$$

defines an isomorphism j of $(\mathscr{S}^* \otimes \mathscr{S}^*)^i$ into $H^{2k+i}(Y \times Y)$ for $i \leqq n$.

Now suppose that $\rho_1, \rho_2 \in \mathscr{S}^* \otimes \mathscr{S}^*$ both satisfy the identity $\theta c(\alpha \otimes \beta) = c\rho_i(\alpha \otimes \beta)$ for the same element θ of $\mathscr{S}^n$. Taking $X = Y \times Y$, $\alpha = \gamma \times 1$, $\beta = 1 \times \gamma$, we have $c\rho_i(\alpha \otimes \beta) = j(\rho_i)$. But the equality $j(\rho_1) = j(\rho_2)$ with $\dim \rho_1 = \dim \rho_2 = n$ implies that $\rho_1 = \rho_2$. This completes the uniqueness proof. Since the assertion that ψ^* is a ring homomorphism follows easily from the proof used in the existence argument, this completes the proof.

As a biproduct of the proof we have the following explicit formulas:

$$\psi^*(\delta) = \delta \otimes 1 + 1 \otimes \delta$$

$$\psi^*(\mathscr{P}^n) = \mathscr{P}^n \otimes 1 + \mathscr{P}^{n-1} \otimes \mathscr{P}^1 + \cdots + 1 \otimes \mathscr{P}^n .$$

THEOREM 1. *The homomorphisms*

$$\mathscr{S}^* \xrightarrow{\psi^*} \mathscr{S}^* \otimes \mathscr{S}^* \xrightarrow{\phi^*} \mathscr{S}^*$$

give $\mathscr{S}^*$ the structure of a Hopf algebra. Furthermore the product ϕ^* is associative and the "diagonal homomorphism" ψ^* is both associative and commutative.

PROOF. It is known that $(\mathscr{S}^*, \phi^*)$ is a connected algebra with unit; and that ψ^* is a ring homomorphism. Hence to show that $\mathscr{S}^*$ is a Hopf algebra it is only necessary to verify Condition 2.2. But this condition is clearly satisfied for the generators δ, and $\mathscr{P}^n$ of $\mathscr{S}^*$, which implies that it is satisfied for all positive dimensional elements of $\mathscr{S}^*$.

It is also known that the product ϕ^* is associative. The assertions that ψ^* is associative and commutative are expressed by the identities

(1) $$(\psi^* \otimes 1)\psi^*\theta = (1 \otimes \psi^*)\psi^*\theta ,$$

$$(2) \qquad T\psi^*\theta = \psi^*\theta$$

for all θ, where $T(\theta' \otimes \theta'')$ is defined as $(-1)^{\dim\theta' \dim\theta''}\,\theta'' \otimes \theta'$. Both identities are clearly satisfied if θ is one of the generators δ or $\mathscr{P}^n$ of $\mathscr{S}^*$. But since each of the homomorphisms in question is a ring homomorphism, this completes the proof.

As an immediate consequence we have:

COROLLARY 1. *There is a dual Hopf algebra*

$$\mathscr{S}_* \xrightarrow{\phi_*} \mathscr{S}_* \otimes \mathscr{S}_* \xrightarrow{\psi_*} \mathscr{S}_*$$

with associative, commutative product operation.

4. The homomorphism λ^*

Let H_*, H^* denote the homology and cohomology, with coefficients Z_p, of a finite complex. The action of $\mathscr{S}^*$ on H^* gives rise to an action of $\mathscr{S}^*$ on H_* which is defined by the rule:

$$\langle \mu\theta, \alpha \rangle = \langle \mu, \theta\alpha \rangle$$

for all $\mu \in H_*$, $\theta \in \mathscr{S}^*$, $\alpha \in H^*$. This action can be considered as a homomorphism

$$\lambda_*: H_* \otimes \mathscr{S}^* \to H_* .$$

The dual homomorphism

$$\lambda^*: H^* \to H^* \otimes \mathscr{S}_*$$

will be the subject of this section.

Alternatively, the restricted homomorphism $H_{n+i} \otimes \mathscr{S}^i \to H_n$ has a dual which we will denote by

$$\lambda^i: H^n \to H^{n+i} \otimes \mathscr{S}_i .$$

In this terminology we have

$$\lambda^* = \lambda^0 + \lambda^1 + \lambda^2 + \cdots$$

carrying H^n into $\sum_i H^{n+i} \otimes \mathscr{S}_i$. The condition that H^* be the cohomology of a finite complex is essential here, since otherwise λ^* would be an infinite sum.

The identity

$$\mu(\theta_1\theta_2) = (\mu\theta_1)\theta_2$$

can easily be derived from the identity $(\theta_1\theta_2)\alpha = \theta_1(\theta_2\alpha)$ which is used to define the product operation in $\mathscr{S}^*$. In other words the diagram

$$\begin{tikzcd} H_* \otimes \mathscr{S}^* \otimes \mathscr{S}^* \arrow[r, "1 \otimes \phi^*"] \arrow[d, "\lambda_* \otimes 1"] & H_* \otimes \mathscr{S}^* \arrow[d, "\lambda_*"] \\ H_* \otimes \mathscr{S}^* \arrow[r, "\lambda_*"] & H_* \end{tikzcd}$$

is commutative. Therefore the dual diagram

$$\begin{tikzcd} H^* \otimes \mathscr{S}_* \otimes \mathscr{S}_* & H^* \otimes \mathscr{S}_* \arrow[l, "1 \otimes \phi_*"'] \\ H^* \otimes \mathscr{S}_* \arrow[u, "\lambda^* \otimes 1"] & H^* \arrow[l, "\lambda^*"'] \arrow[u, "\lambda^*"'] \end{tikzcd}$$

is also commutative. Thus we have proved:

LEMMA 2. *The identity*

$$(\lambda^* \otimes 1)\lambda^*(\alpha) = (1 \otimes \phi_*)\lambda^*(\alpha)$$

holds for every $\alpha \in H^*$.

The cup product in H^* and the ψ_* product in $\mathscr{S}_*$ induce a product operation in $H^* \otimes \mathscr{S}_*$.

LEMMA 3. *The homomorphism* $\lambda^*: H^* \to H^* \otimes \mathscr{S}_*$ *is a ring homomorphism.*

PROOF. Let K and L be finite complexes, let θ be an element of $\mathscr{S}^*$, and let $\psi^*(\theta) = \sum \theta'_i \otimes \theta''_i$. Then for any $\alpha \in H^*(K)$, $\beta \in H^*(L)$ we have $\theta \cdot (\alpha \times \beta) = \sum (-1)^{\dim \theta''_i \dim \alpha}\, \theta'_i\alpha \times \theta''_i\beta$. Using the rule

$$\langle \mu \times \nu, \theta \cdot (\alpha \times \beta) \rangle = \langle (\mu \times \nu) \cdot \theta, \alpha \times \beta \rangle$$

we easily arive at the identity

$$(\mu \times \nu) \cdot \theta = \sum (-1)^{\dim \nu \dim \theta'_i}\, \mu\theta'_i \times \nu\theta''_i \,.$$

In other words the diagram

$$\begin{tikzcd} H_*(K) \otimes H_*(L) \otimes \mathscr{S}^* \otimes \mathscr{S}^* \arrow[d, "1 \otimes T \otimes 1"] & H_*(K) \otimes H_*(L) \otimes \mathscr{S}^* = H_*(K \times L) \otimes \mathscr{S}^* \arrow[l, "1 \otimes 1 \otimes \psi^*"'] \arrow[d, "\lambda_*"] \\ H_*(K) \otimes \mathscr{S}^* \otimes H_*(L) \otimes \mathscr{S}^* \arrow[r, "\lambda_* \otimes \lambda_*"] & H_*(K) \otimes H_*(L) = H_*(K \times L) \end{tikzcd}$$

is commutative (where T interchanges two factors as in §3). Therefore the dual diagram is also commutative. Setting $K = L$, and letting $d: K \to K \times K$ be the diagonal homomorphism we obtain a larger commutative diagram

$$\begin{tikzcd} H^* \otimes H^* \otimes \mathscr{S}_* \otimes \mathscr{S}_* \arrow[r, "1 \otimes 1 \otimes \psi_*"] & H^* \otimes H^* \otimes \mathscr{S}_* = H^*(K \times K) \otimes \mathscr{S}_* \arrow[r, "d^* \otimes 1"] & H^* \otimes \mathscr{S}_* \\ H^* \otimes \mathscr{S}_* \otimes H^* \otimes \mathscr{S}_* \arrow[u, "1 \otimes T \otimes 1"] & H^* \otimes H^* = H^*(K \times K) \arrow[l, "\lambda^* \otimes \lambda^*"'] \arrow[u, "\lambda^*"] \arrow[r, "d^*"] & H^* \arrow[u, "\lambda^*"] \end{tikzcd}$$

Now starting with $\alpha \otimes \beta \in H^* \otimes H^*$ and proceeding to the right and up in this diagram, we obtain $\lambda^*(\alpha \smile \beta)$. Proceeding to the left and up, and then to the right, we obtain $\lambda^*(\alpha)\cdot\lambda^*(\beta)$. Therefore

$$\lambda^*(\alpha\beta) = \lambda^*(\alpha)\lambda^*(\beta)$$

which proves Lemma 3.

The following lemma shows how the action of $\mathscr{S}^*$ on $H^*(K)$ can be reconstructed from the homomorphism λ^*.

LEMMA 4. *If $\lambda^*(\alpha) = \sum \alpha_i \otimes \omega_i$ then for any $\theta \in \mathscr{S}^*$ we have*

$$\theta\alpha = \sum (-1)^{\dim \alpha_i \dim \omega_i} \langle \theta, \omega_i \rangle \alpha_i \; .$$

PROOF. By definition

$$\begin{aligned} \langle \mu, \theta\alpha \rangle &= \langle \mu\theta, \alpha \rangle = \langle \lambda_*(\mu \otimes \theta), \alpha \rangle \\ &= \langle \mu \otimes \theta, \lambda^*\alpha \rangle = \sum \pm \langle \mu, \alpha_i \rangle \langle \theta, \omega_i \rangle \; . \end{aligned}$$

Since this holds for each $\mu \in H_*$, the above equality holds.

REMARK. To complete the picture, the operation $\eta^*: \mathscr{S}^* \otimes H^* \to H^*$ has a dual $\eta_*: H_* \to \mathscr{S}_* \otimes H_*$. Analogues of Lemmas 2 and 4 are easily obtained for η_*. If a product operation $K \times K \to K$ is given, so that H_*, and hence $\mathscr{S}_* \otimes H_*$, have product operations; then a straightforward proof shows that η_* is a ring homomorphism. (As an example let K denote the loop space of an $(n+1)$-sphere, or an equivalent CW-complex. Then $H_*(K)$ is known to be a polynomial ring on one generator $\mu \in H_n(K)$. The element

$$\eta_*(\mu) \in (\mathscr{S}_0 \otimes H_n) \oplus (\mathscr{S}_1 \otimes H_{n-1}) \oplus \cdots \oplus (\mathscr{S}_n \otimes H_0)$$

is evidently equal to $1 \otimes \mu$. Therefore $\eta_*(\mu^k) = 1 \otimes \mu^k$ for all k. Passing to the dual, this proves that the action of $\mathscr{S}^*$ on $H^*(K)$ is trivial.)

5. The structure of the dual algebra $\mathscr{S}_*$

As an example to illustrate this operation λ^* consider the Lens space $X = S^{2N+1}/Z_p$ where N is a large integer, and where the cyclic group Z_p acts freely on the sphere S^{2N+1}. Thus X can be considered as the $(2N+1)$-skeleton of the Eilenberg-MacLane space $K(Z_p, 1)$. The cohomology ring $H^*(X)$ is known to have the following form. There is a generator $\alpha \in H^1(X)$ and $H^2(X)$ is generated by $\beta = \delta\alpha$. For $0 \leqq i \leqq N$, the group $H^{2i}(X)$ is generated by β^i and $H^{2i+1}(X)$ is generated by $\alpha\beta^i$.

The action of the Steenrod algebra on $H^*(X)$ is described as follows. It will be convenient to introduce the abbreviations

$$M_0 = 1\,,\; M_1 = \mathscr{P}^1\,,\; M_2 = \mathscr{P}^p\mathscr{P}^1,\; \cdots,\; M_k = \mathscr{P}^{p^{k-1}} \cdots \mathscr{P}^p\mathscr{P}^1,\; \cdots \; .$$

LEMMA 5. *The element* $M_k \in \mathscr{S}^{2p^k-2}$ *satisfies* $M_k\beta = \beta^{p^k}$. *However if* θ *is any monomial in the operations* δ, $\mathscr{P}^1$, $\mathscr{P}^2$, $\cdots$ *which is not of the form* $\mathscr{P}^{p^{k-1}} \cdots \mathscr{P}^p\mathscr{P}^1$ *then* $\theta\beta = 0$. *Similarly* $(M_k\delta)\alpha = \beta^{p^k}$ *but* $\theta\alpha = 0$ *if* θ *is any monomial in the operations* δ, $\mathscr{P}^1$, $\mathscr{P}^2$, $\cdots$ *which does not have the form* $\theta = \mathscr{P}^{p^{k-1}} \cdots \mathscr{P}^1\delta$ *or* $\theta = 1$.

PROOF. It is convenient to introduce the formal operation $\mathscr{P} = 1 + \mathscr{P}^1 + \mathscr{P}^2 + \cdots$. It follows from 2.4 that $\mathscr{P}\beta = \beta + \beta^p$. Since $\mathscr{P}$ is a ring homomorphism according to 2.5, it follows that $\mathscr{P}\beta^i = (\beta + \beta^p)^i$. In particular if $i = p^r$ this gives $\mathscr{P}\beta^{p^r} = (\beta + \beta^p)^{p^r} = \beta^{p^r} + \beta^{p^{r+1}}$. In other words

$$\mathscr{P}^j\beta^{p^r} = \begin{cases} \beta^{p^r} & \text{if } j = 0 \\ \beta^{p^{r+1}} & \text{if } j = p^r \\ 0 & \text{otherwise} . \end{cases}$$

Since $\delta\beta^i = i\beta^{i-1}\delta\beta = i\beta^{i-1}\delta\delta\alpha = 0$ it follows that the only nontrivial operation δ or $\mathscr{P}^j$ which can act on β^{p^r} is $\mathscr{P}^{p^r}$. Using induction, this proves the first assertion of Lemma 5. To prove the second it is only necessary to add that $\mathscr{P}^j\alpha = 0$ for all $j > 0$, according to 2.4.

Now consider the operation $\lambda^*: H^*(X) \to H^*(X) \otimes \mathscr{S}_*$.

LEMMA 6. *The element* $\lambda^*\alpha$ *has the form* $\alpha \otimes 1 + \beta \otimes \tau_0 + \beta^p \otimes \tau_1 + \cdots + \beta^{p^r} \otimes \tau_r$ *where each* τ_k *is a well defined element of* $\mathscr{S}_{2p^k-1}$, *and where* p^r *is the largest power of* p *with* $p^r \leqq N$. *Similarly* $\lambda^*\beta$ *has the form*

$$\beta \otimes \xi_0 + \beta^p \otimes \xi_1 + \cdots + \beta^{p^r} \otimes \xi_r ,$$

where $\xi_0 = 1$, *and where each* ξ_k *is a well defined element of* $\mathscr{S}_{2p^k-2}$.

PROOF. For any element θ of $\mathscr{S}^i$, Lemma 5 implies that $\theta\beta = 0$ unless i is the dimension of one of the monomials $M_0, M_1, \cdots$: that is unless i has the form $2p^k - 2$. Therefore, according to Lemma 4, we see that $\lambda^i\beta = 0$ unless i has the form $2p^k - 2$. Thus

$$\lambda^*\beta = \lambda^0(\beta) + \lambda^{2p-2}(\beta) + \cdots + \lambda^{2p^r-2}(\beta) .$$

Since $\lambda^{2p^k-2}(\beta)$ belongs to $H^{2p^k}(X) \otimes \mathscr{S}_{2p^k-2}$, it must have the form $\beta^{p^k} \otimes \xi_k$ for some uniquely defined element ξ_k. This proves the second assertion of Lemma 6. The first assertion is proved by a similar argument.

REMARK. These elements ξ_k and τ_k have been defined only for $k \leqq r = [\log_p N]$. However the integer N can be chosen arbitrarily large, so we have actually defined ξ_k and τ_k for all $k \geqq 0$.

Our main theorem can now be stated as follows.

THEOREM 2. *The algebra* $\mathscr{S}_*$ *is the tensor product of the Grassmann algebra generated by* $\tau_0, \tau_1, \cdots$ *and the polynomial algebra generated by* ξ_1, $\xi_2, \cdots$.

The proof will be based on a computation of the inner products of monomials in τ_i and ξ_j with monomials in the operations $\mathscr{P}^n$ and δ. The following lemma is an immediate consequence of Lemmas 4, 5 and 6.

LEMMA 7. *The inner product*

$$\langle M_k, \xi_k \rangle$$

equals one, but $\langle \theta, \xi_k \rangle = 0$ *if* θ *is any other monomial. Similarly*

$$\langle M_k \delta, \tau_k \rangle = 1$$

but $\langle \theta, \tau_k \rangle = 0$ *if* θ *is any other monomial.*

Consider the set of all finite sequences $I = (\varepsilon_0, r_1, \varepsilon_1, r_2, \cdots)$ where $\varepsilon_i = 0, 1$ and $r_i = 0, 1, 2, \cdots$. For each such I define

$$\omega(I) = \tau_0^{\varepsilon_0} \xi_1^{r_1} \tau_1^{\varepsilon_1} \xi_2^{r_2} \cdots .$$

Then we must prove that the collection $\{\omega(I)\}$ forms an additive basis for $\mathscr{S}_*$.

For each such I define

$$\theta(I) = \delta^{\varepsilon_0} \mathscr{P}^{s_1} \delta^{\varepsilon_1} \mathscr{P}^{s_2} \cdots$$

where

$$s_1 = \sum_{i=1}^{\infty} (\varepsilon_i + r_i) p^{i-1}, \cdots, \; s_k = \sum_{i=k}^{\infty} (\varepsilon_i + r_i) p^{i-k} .$$

It is not hard to verify that these elements $\theta(I)$ are exactly the "basic monomials" of Adem or Cartan. Furthermore $\theta(I)$ has the same dimension as $\omega(I)$. Order the collection $\{I\}$ lexicographically from the right. (For example $(1, 2, 0, \cdots) < (0, 0, 1, \cdots)$.)

LEMMA 8. *The inner product* $\langle \theta(I), \omega(J) \rangle$ *is equal to zero if* $I < J$ *and* ± 1 *if* $I = J$.

Assuming this lemma for the moment, the proof of Theorem 2 can be completed as follows. If we restrict attention to sequences I such that

$$\dim \omega(I) = \dim \theta(I) = n ,$$

then Lemma 8 asserts that the resulting matrix $\langle \theta(I), \omega(J) \rangle$ is a non-singular triangular matrix. But according to Adem or Cartan the elements $\theta(I)$ generate $\mathscr{S}^n$. Therefore the elements $\omega(J)$ must form a basis for $\mathscr{S}_n$; which proves Theorem 2. (Incidentally this gives a new proof of Cartan's assertion that the $\theta(I)$ are linearly independent.)

PROOF OF LEMMA 8. We will prove the assertion $\langle \theta(I), \omega(I) \rangle = \pm 1$ by induction on the dimension. It is certainly true in dimension zero.

Case 1. The last non-zero element of the sequence $I = (\varepsilon_0, r_1, \cdots, \varepsilon_{k-1}, r_k, 0, \cdots)$ is r_k. Set $I' = (\varepsilon_0, r_1, \cdots, \varepsilon_{k-1}, r_k - 1, 0, \cdots)$ so that $\omega(I) = \omega(I')\xi_k$. Then

$$\begin{aligned}\langle \theta(I), \omega(I) \rangle &= \langle \theta(I), \psi_*(\omega(I') \otimes \xi_k) \rangle \\ &= \langle \psi^*\theta(I), \omega(I') \otimes \xi_k \rangle .\end{aligned}$$

Since $\theta(I) = \delta^{\varepsilon_0}\mathscr{P}^{s_1} \cdots \delta^{\varepsilon_{k-1}}\mathscr{P}^{s_k}$ we have

$$\psi^*\theta(I) = \sum \pm \delta^{\varepsilon_0'} \cdots \mathscr{P}^{s_k'} \otimes \delta^{\varepsilon_0''} \cdots \mathscr{P}^{s_k''}$$

where the summation extends over all sequences $(\varepsilon_0', \cdots, s_k')$ and $(\varepsilon_0'', \cdots, s_k'')$ with $\varepsilon_i' + \varepsilon_i'' = \varepsilon_i$ and $s_i' + s_i'' = s_i$. Substituting this in the previous expression we have

$$\langle \theta(I), \omega(I) \rangle = \sum \pm \langle \delta^{\varepsilon_0'} \cdots \mathscr{P}^{s_k'}, \omega(I') \rangle \langle \delta^{\varepsilon_0''} \cdots \mathscr{P}^{s_k''}, \xi_k \rangle .$$

But according to Lemma 7 the right hand factor is zero except for the special case

$$\delta^{\varepsilon_0''} \cdots \mathscr{P}^{s_k''} = \mathscr{P}^{p^{k-1}} \cdots \mathscr{P}^{p}\mathscr{P}^{1} ,$$

in which case the inner product is one. Inspection shows that the corresponding expression $\delta^{\varepsilon_0'} \cdots \mathscr{P}^{s_k'}$ on the left is equal to $\theta(I')$; and hence that $\langle \theta(I), \omega(I) \rangle = \pm \langle \theta(I'), \omega(I') \rangle = \pm 1$.

Case 2. The last non-zero element of $I = (\varepsilon_0, r_1, \cdots, r_k, \varepsilon_k, 0, \cdots)$ is $\varepsilon_k = 1$. Define $I' = (\varepsilon_0, r_1, \cdots, r_k, 0, \cdots)$ so that

$$\omega(I) = \omega(I')\tau_k .$$

Carrying out the same construction as before we find that the only non-vanishing right hand term is $\langle \mathscr{P}^{p^{k-1}} \cdots \mathscr{P}^{1}\delta, \tau_k \rangle = 1$. The corresponding left hand term is again $\langle \theta(I'), \omega(I') \rangle$; so that $\langle \theta(I), \omega(I) \rangle = \pm \langle \theta(I'), \omega(I') \rangle = \pm 1$, with completes the induction.

The proof that $\langle \theta(I), \omega(J) \rangle = 0$ for $I < J$ is carried out by a similar induction on the dimension.

Case 1a. The sequence J ends with the element r_k and the sequence I ends at the corresponding place. Then the argument used above shows that

$$\langle \theta(I), \omega(J) \rangle = \pm \langle \theta(I'), \omega(J') \rangle = 0 .$$

Case 1b. The sequence J ends with the elements r_k, but I ends earlier. Then in the expansion used above, every right hand factor

$$\langle \delta^{\varepsilon_0''}\mathscr{P}^{s_1''} \cdots \delta^{\varepsilon_{k-1}''}, \xi_k \rangle$$

is zero. Therefore $\langle \theta(I), \omega(J) \rangle = 0$.

Similarly Case 2 splits up into two subcases which are proved in an analogous way. This completes the proof of Lemma 8 and Theorem 2.

To complete the description of $\mathscr{S}_*$ as a Hopf algebra it is necessary to compute the homomorphism ϕ_*. But since ϕ_* is a ring homomorphism it is only necessary to evaluate it on the generators of S_*.

THEOREM 3. *The following formulas hold.*

$$\phi_*(\xi_k) = \sum_{i=0}^{k} \xi_{k-i}^{p^i} \otimes \xi_i$$
$$\phi_*(\tau_k) = \sum_{i=0}^{k} \xi_{k-i}^{p^i} \otimes \tau_i + \tau_k \otimes 1 .$$

The proof will be based on Lemmas 2 and 3. Raising both sides of the equation

$$\lambda^*(\beta) = \sum \beta^{p^j} \otimes \xi_j$$

to the power p^i we obtain

$$\lambda^*(\beta^{p^i}) = \sum \beta^{p^{i+j}} \otimes \xi_j^{p^i} .$$

Now

$$(\lambda^* \otimes 1)\lambda^*(\beta) = (\lambda^* \otimes 1) \sum \beta^{p^i} \otimes \xi_i$$
$$= \sum_{i,j} \beta^{p^{i+j}} \otimes \xi_j^{p^i} \otimes \xi_i .$$

Comparing this with

$$(1 \otimes \phi_*)\lambda^*(\beta) = \sum \beta^{p^k} \otimes \phi_*(\xi_k)$$

We obtain the required expression for $\phi_*(\xi_k)$.

Similarly the identity

$$(\lambda^* \otimes 1)\lambda^*(\alpha) = (1 \otimes \phi_*)\lambda^*(\alpha)$$

can be used to obtain the required formula for $\phi_*(\tau_k)$.

6. A basis for $\mathscr{S}^*$

Let $R = (r_1, r_2, \cdots)$ range over all sequences of non-negative integers which are almost all zero, and define $\xi(R) = \xi_1^{r_1}\xi_2^{r_2} \cdots$. Let $E = (\varepsilon_0, \varepsilon_1, \cdots)$ range over all sequences of zeros and ones which are almost all zero, and define $\tau(E) = \tau_0^{\varepsilon_0}\tau_1^{\varepsilon_1} \cdots$. Then Theorem 2 asserts that the elements

$$\{\tau(E)\xi(R)\}$$

form an additive basis for $\mathscr{S}_*$. Hence there is a dual basis $\{\rho(E, R)\}$ for $\mathscr{S}^*$. That is we define $\rho(E, R) \in \mathscr{S}^*$ by

$$\langle \rho(E, R), \tau(E')\xi(R') \rangle = \begin{cases} 1 & \text{if} \quad E = E',\ R = R' \\ 0 & \text{otherwise.} \end{cases}$$

Using Lemma 8 it is easily seen that $\rho(\mathbf{0}, (r, 0, 0, \cdots))$ is equal to the Steenrod power $\mathscr{P}^r$. This suggests that we define[2] $\mathscr{P}^R$ as the basis element $\rho(\mathbf{0}, R)$ dual to $\xi(R)$. (Abbreviations such as $\mathscr{P}^{01}$ in place of $\mathscr{P}^{(0,1,0,0,\cdots)}$ will be frequently be used.)

Let Q_k denote the basis element dual to τ_k. For example $Q_0 = \rho((1, 0, \cdots), \mathbf{0})$ is equal to the operation δ. It will turn out that any basis element $\rho(E, R)$ is equal to the product $\pm Q_0^{\varepsilon_0} Q_1^{\varepsilon_1} \cdots \mathscr{P}^R$.

THEOREM 4a. *The elements*

$$Q_0^{\varepsilon_0} Q_1^{\varepsilon_1} \cdots \mathscr{P}^R$$

form an additive basis for the Steenrod algebra $\mathscr{S}^*$ which is, up to sign, dual to the known basis $\{\tau(E)\xi(E)\}$ for $\mathscr{S}_*$. The elements $Q_k \in \mathscr{S}^{2p^k-1}$ generate a Grassmann algebra: that is they satisfy

$$Q_j Q_k + Q_k Q_j = 0 .$$

They permute with the elements $\mathscr{P}^R$ according to the rule

$$\mathscr{P}^R Q_k - Q_k \mathscr{P}^R = Q_{k+1} \mathscr{P}^{R-(p^k, 0, \cdots)} + Q_{k+2} \mathscr{P}^{R-(0, p^k, 0, \cdots)} + \cdots .$$

(By the difference $(r_1, r_2, \cdots) - (s_1, s_2, \cdots)$ of two sequences we mean the sequence $(r_1 - s_1, r_2 - s_2, \cdots)$. It is understood, for example, that $\mathscr{P}^{R-(p^k, 0, \cdots)}$ is zero in case $r_1 < p^k$.)

As an example we have the following where $[a, b]$ denote the "commutator" $ab - (-1)^{\dim a \dim b} ba$.

COROLLARY 2. *The elements $Q_k \in \mathscr{S}^{2p^k-1}$ can be defined inductively by the rule*

$$Q_0 = \delta , \quad Q_{k+1} = [\mathscr{P}^{p^k}, Q_k] .$$

To complete the description of $\mathscr{S}^*$ as an algebra it is necessary to find the product $\mathscr{P}^R \mathscr{P}^S$. Let X range over all infinite matrices

$$\begin{Vmatrix} * & x_{01} & x_{02} & \cdots \\ x_{10} & x_{11} & \cdots & \\ x_{20} & \cdots & & \\ \cdots & & & \end{Vmatrix}$$

of non-negative integers, almost all zero, with leading entry ommitted. For each such X define $R(X) = (r_1, r_2, \cdots)$, $S(X) = (s_1, s_2, \cdots)$, and $T(X) = (t_1, t_2, \cdots)$, by

$$\begin{aligned} r_i &= \textstyle\sum_j p^j x_{ij} && \text{(weighted row sum)}, \\ s_j &= \textstyle\sum_i x_{ij} && \text{(column sum)}, \\ t_n &= \textstyle\sum_{i+j=n} x_{ij} && \text{(diagonal sum)}. \end{aligned}$$

Define the coefficient $b(X) = \prod t_n! / \prod x_{ij}!$.

THEOREM 4b. *The product $\mathscr{P}^R \mathscr{P}^S$ is equal to*

$$\textstyle\sum_{R(X)=R,\, S(X)=S} b(X) \mathscr{P}^{T(X)}$$

where the sum extends over all matrices X satisfying the conditions $R(X) = R$, $S(X) = S$.

As an example consider the case $R = (r, 0, \cdots)$, $S = (s, 0, \cdots)$. Then the equations $R(X) = R$, $S(X) = S$ become

$$x_{10} + px_{11} + \cdots = r\ , \quad x_{ij} = 0 \quad \text{for } i > 1\ ,$$

$$x_{01} + x_{11} + \cdots = s\ , \quad x_{ij} = 0 \quad \text{for } j > 1, \text{ respectively.}$$

Thus, letting $x = x_{11}$, the only suitable matrices are those of the form

$$\begin{Vmatrix} * & s - x & 0 & \cdot \\ r - px & x & 0 & \cdot \\ 0 & 0 & 0 & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{Vmatrix}$$

with $0 \leqq x \leqq \operatorname{Min}(s, [r/p])$. The corresponding coefficients $b(X)$ are the binomial coefficients $(r - px, s - x)$. Therefore we have

COROLLARY 3. *The product $\mathscr{P}^r \mathscr{P}^s$ is equal to*

$$\sum_{x=0}^{\operatorname{Min}(s,[r/p])} (r - px, s - x)\mathscr{P}^{r-px+s-x,\, x}\ .$$

(For example $\mathscr{P}^{p+1}\mathscr{P}^1 = 2\mathscr{P}^{p+2} + \mathscr{P}^{1,1}$.)

The simplest case of this product operation is the following

COROLLARY 4. *If $r_1 < p, r_2 < p, \cdots$ then $\mathscr{P}^R\mathscr{P}^S = (r_1, s_1)(r_2, s_2) \cdots \mathscr{P}^{R+S}$.*

As a final illustration we have:

COROLLARY 5. *The elements $\mathscr{P}^{(0\cdots 010\cdots)}$ can be defined inductively by*

$$\mathscr{P}^{0,1} = [\mathscr{P}^p, \mathscr{P}^1],\ \mathscr{P}^{0,0,1} = [\mathscr{P}^{p^2}, \mathscr{P}^{0,1}]\ , \quad \text{etc.}$$

The proofs are left to the reader.

PROOF OF THEOREM 4b. Given any Hopf algebra A_* with basis $\{a_i\}$ the diagonal homomorphism can be written as

$$\phi_*(a_i) = \sum_{j,k} c_i^{jk} a_j \otimes a_k\ .$$

The product operation in the dual algebra is then given by

$$a^j a^k = \phi^*(a^j \otimes a^k) = \sum_i (-1)^{\dim a^j \dim a^k} c_i^{jk} a^i\ ,$$

where $\{a^i\}$ is the dual basis. In carrying out this program for the algebra $\mathscr{S}_*$ we will first use Theorem 3 to compute $\phi_*(\xi(T))$ for any sequence $T = (t_1, t_2, \cdots)$.

Let $[i_1, i_2, \cdots, i_k]$ denote the generalized binomial coefficient

$$(i_1 + i_2 + \cdots + i_k)!/i_1!\,i_2! \cdots i_k!\ ;$$

so that the following identity holds

$$(y_1 + \cdots + y_k)^n = \sum_{i_1+\cdots+i_k=n} [i_1, \cdots, i_k] y_1^{i_1} \cdots y_k^{i_k}$$

Applying this to the expression

$$\phi_*(\xi_k) = \xi_k \otimes 1 + \xi_{k-1}^p \otimes \xi_1 + \cdots + \xi_1^{p^{k-1}} \otimes \xi_{k-1} + 1 \otimes \xi_k$$

we obtain

$$\begin{aligned}\phi_*(\xi_k^{t_k}) &= \sum [x_{k0}, \cdots, x_{0k}](\xi_k^{x_{k0}} \xi_{k-1}^{px_{k-11}} \cdots \xi_1^{p^{k-1}x_{1k-1}}) \otimes (\xi_1^{x_{k-11}} \cdots \xi_k^{x_{0k}}) \\ &= \sum [x_{k0}, \cdots, x_{0k}] \xi(p^{k-1}x_{1\,k-1}, \cdots, x_{k0}) \otimes \xi(x_{k-1\,1}, \cdots, x_{0k})\end{aligned}$$

summed over all integers $x_{k0}, \cdots, x_{0k}$ satisfying $x_{i\,k-i} \geqq 0$, $x_{k0} + \cdots + x_{0k} = t_k$. Now multiply the corresponding expressions for $k = 1, 2, 3, \cdots$. Since the product $[x_{10}, x_{01}][x_{20}, x_{11}, x_{02}][x_{30}, \cdots, x_{03}] \cdots$ is equal to $b(X)$, we obtain

$$\phi_*(\xi(T)) = \sum_{T(X)=T} b(X)\xi(R(X)) \otimes \xi(S(X)) ,$$

summed over all matrices X satisfying the condition $T(X) = X$.

In order to pass to the dual ϕ^* we must look for all basis elements $\tau(E)\xi(T)$ such that $\phi_*(\tau(E)\xi(T))$ contains a term of the form

$$(\text{non-zero constant}) \cdot \xi(R) \otimes \xi(S) .$$

However inspection shows that the only such basis elements are the ones $\xi(T)$ which we have just studied. Hence we can write down the dual formula

$$\phi^*(\mathscr{P}^R \otimes \mathscr{P}^S) = \sum_{R(X)=R,\ S(X)=S} b(X)\mathscr{P}^{T(X)} .$$

This completes the proof of Theorem 4b.

PROOF OF THEOREM 4a. We will first compute the products of the basis elements $\rho(E, \mathbf{0})$ dual to $\tau_0^{\varepsilon_0}\tau_1^{\varepsilon_1} \cdots$. The dual problem is to study the homomorphism $\phi_*: \mathscr{S}_* \to \mathscr{S}_* \otimes \mathscr{S}_*$ ignoring all terms in $\mathscr{S}_* \otimes \mathscr{S}_*$ which involve any factor ξ_k. The elements $1 \otimes \xi_1, 1 \otimes \xi_2, \cdots, \xi_1 \otimes 1, \cdots$ of $\mathscr{S}_* \otimes \mathscr{S}_*$ generate an ideal $\mathscr{I}$. Furthermore according to Theorem 3:

$$\begin{aligned}\phi_*(\tau_k) &\equiv \tau_k \otimes 1 + 1 \otimes \tau_k \qquad &(\mathrm{mod}\ \mathscr{I}) \\ \phi_*(\xi_k) &\equiv 0 &(\mathrm{mod}\ \mathscr{I}) .\end{aligned}$$

Therefore $\phi_*(\tau(E)\xi(R) \equiv 0$ if $R \neq 0$ and $\phi_*(\tau(E)) \equiv \sum_{E_1+E_2=E} \pm\, \tau(E_1) \otimes \tau(E_2)$ (mod $\mathscr{I}$). The dual statement is that

$$\rho(E_1, \mathbf{0})\rho(E_2, \mathbf{0}) = \pm\, \rho(E_1 + E_2, \mathbf{0}) ,$$

where it is understood that the right side is zero if the sequences E_1 and E_2 both have a "1" in the same place. Thus the basis elements $\rho(E, \mathbf{0})$ multiply as a Grassmann algebra.

Similar arguments show that the product $\rho(E, \mathbf{0})\rho(\mathbf{0}, R)$ is equal to

$\rho(E, R)$. From this the first assertion of 4a follows immediately.

Computation of $\mathscr{P}^R Q_k$: We must look for basis elements $\tau(E)\xi(R')$ such that $\phi_*(\tau(E)\xi(R'))$ contains a term

$$(\text{non-zero constant})\cdot\xi(R)\otimes\tau_k\ .$$

Inspection shows that the only such basis elements are $\tau_k\xi(R)$, $\tau_{k+1}\xi(R-(p^k, 0, \cdots))$, $\tau_{k+2}\xi(R-(0, p^k, 0, \cdots))$, $\cdots$ etc. Furthermore the corresponding constants are all $+1$. This proves that

$$\mathscr{P}^R Q_k = Q_k\mathscr{P}^R + Q_{k+1}\mathscr{P}^{R-(p^k, 0, \cdots)} + \cdots ,$$

and completes the proof of Theorem 4.

To complete the description of $\mathscr{S}^*$ as a Hopf algebra we must compute the homomorphism ψ^*.

LEMMA 9. *The following formulas hold*

$$\psi^*(Q_k) = Q_k \otimes 1 + 1 \otimes Q_k$$
$$\psi^*(\mathscr{P}^R) = \sum\nolimits_{R_1+R_2=R} \mathscr{P}^{R_1} \otimes \mathscr{P}^{R_2}\ .$$

(For example $\psi^*(\mathscr{P}^{011}) = \mathscr{P}^{011}\otimes 1 + 1 \otimes \mathscr{P}^{011} + \mathscr{P}^{01}\otimes\mathscr{P}^{001} + \mathscr{P}^{001}\otimes\mathscr{P}^{01}$.)

REMARK. An operation $\theta \in \mathscr{S}^*$ is called a *derivation* if it satisfies

$$\theta(\alpha\smile\beta) = (\theta\alpha)\smile\beta + (-1)^{\dim\theta\dim\alpha}\alpha\smile\theta\beta\ .$$

This is clearly equivalent to the assertion that θ is primitive. It can be shown that the only derivations in $\mathscr{S}^*$ are the elements $Q_0, Q_1, \cdots, \mathscr{P}^1, \mathscr{P}^{0,1}, \mathscr{P}^{0,0,1}, \cdots$ and their multiples.

7. The canonical anti-automorphism

As an illustration consider the Hopf algebra $H_*(G)$ associated with a Lie group G. The map $g \to g^{-1}$ of G into itself induces a homomorphism $c\colon H_*(G) \to H_*(G)$ which satisfies the following two identities:

(1) $c(1) = 1$

(2) if $\psi_*(a) = \sum a'_i \otimes a''_i$, where $\dim a > 0$, then $\sum a'_i c(a''_i) = 0$.

More generally, for any connected Hopf algebra A_*, there exists a unique homomorphism $c\colon A_* \to A_*$ satisfying (1) and (2). We will call $c(a)$ the *conjugate* of a. Conjugation is an anti-automorphism in the sense that

$$c(a_1a_2) = (-1)^{\dim a_1 \dim a_2} c(a_2)c(a_1)\ .$$

The conjugation operations in a Hopf algebra and its dual are dual homomorphisms. For details we refer the reader to [3].

For the Steenrod algebra $\mathscr{S}^*$ this operation was first used by Thom. (See [5] p. 60). More precisely the operation used by Thom is $\theta \to (-1)^{\dim\theta} c(\theta)$.

If θ is a primitive element of $\mathscr{S}^*$ then the defining relation becomes $\theta\cdot 1 + 1\cdot c(\theta) = 0$ so that $c(\theta) = -\theta$. This shows that $c(Q_k) = -Q_k$, $c(\mathscr{P}^1) = -\mathscr{P}^1$. The elements $c(\mathscr{P}^n)$, $n > 0$, could be computed from Thom's identity

$$\sum_i \mathscr{P}^{n-i} c(\mathscr{P}^i) = 0 \ ;$$

however it is easier to first compute the operation in the dual algebra and then carry it back.

By an *ordered partition* α of the integer n with *length* $l(\alpha)$ will be meant an ordered sequence

$$(\alpha(1), \alpha(2), \cdots, \alpha(l(\alpha)))$$

of positive integers whose sum is n. The set of all ordered partitions of n will be denoted by Part (n). (For example Part (3) has four elements: (3), (2,1) (1,2), and (1,1,1). In general Part (n) has 2^{n-1} elements.) Given an ordered partition $\alpha \in$ Part (n), let $\sigma(i)$ denote the partial sum $\sum_{j=1}^{i-1} \alpha(j)$.

LEMMA 10. *In the dual algebra $\mathscr{S}_*$ the conjugate $c(\xi_n)$ is equal to*

$$\sum_{\alpha \in \mathrm{Part}(n)} (-1)^{l(\alpha)} \prod_{i=1}^{l(\alpha)} \xi_{\alpha(i)}^{p^{\sigma(i)}} \ .$$

(For example $c(\xi_3) = -\xi_3 + \xi_1\xi_2^p + \xi_2\xi_1^{p^2} - \xi_1\xi_1^p\xi_1^{p^2}$.)

PROOF. Since $\phi_*(\xi_n) = \sum_{i=0}^{n} \xi_{n-i}^{p^i} \otimes \xi_i$, the defining identity becomes

$$\sum_{i=0}^{n} \xi_{n-i}^{p^i} c(\xi_i) = 0 \ .$$

This can be written as

$$c(\xi_n) = -\xi_n - c(\xi_1)\xi_{n-1}^{p} - \cdots - c(\xi_{n-1})\xi_1^{p^{n-1}} \ .$$

The required formula now follows by induction.

Since the operation $\omega \to c(\omega)$ is an anti-automorphism, we can use Lemma 10 to determine the conjugate of an arbitrary basis element $\xi(R)$. Passing to the dual algebra $\mathscr{S}^*$ we obtain the following formula. (The details of the computation are somewhat involved, and will not be given.)

Given a sequence $R = (r_1, \cdots, r_k, 0, \cdots)$ consider the equations

$$(*) \qquad r_i = \sum_{n=1}^{\infty} \sum_{\alpha \in \mathrm{Part}(n)} \sum_{j=1}^{l(\alpha)} \delta_{i\alpha(j)}\, p^{\sigma(j)} y_\alpha \ ,$$

for $i = 1, 2, 3, \cdots$; where the symbol $\delta_{i\alpha(j)}$ denotes a Kronecker delta; and where the unknowns y_α are to be non-negative integers. For each solution Y to this set of equations define $S(Y) = (s_1, s_2, \cdots)$ by

$$s_n = \sum_{\alpha \in \mathrm{Part}(n)} y_\alpha \ .$$

(Thus $s_1 = y_1$, $s_2 = y_2 + y_{1,1}$, etc.) Define the coefficient $b(Y)$ by

$$b(Y) = [y_2, y_{11}][y_3, y_{21}, y_{12}, y_{111}] \cdots$$
$$= \textstyle\prod_n s_n! \,/\, \prod_\alpha y_\alpha! \;.$$

THEOREM 5. *The conjugate* $c(\mathscr{P}^R)$ *is equal to*

$$(-1)^{r_1+\cdots+r_k} \sum b(Y) \mathscr{P}^{S(Y)}$$

where the summation extends over all solutions Y *to the equations* $(*)$.

To interpret these equations $(*)$ note that the coefficient

$$\textstyle\sum_{j=1}^{l(\alpha)} \delta_{i\alpha(j)}\, p^{\sigma(j)}$$

of y_α in the i^{th} equation is positive if the sequence

$$\alpha = (\alpha(1), \cdots, \alpha(l(\alpha)))$$

contains the integer i, and zero otherwise. In case the left hand side r_i is zero, then for every sequence α containing the integer i it follows that $y_\alpha = 0$. In particular this is true for all $i > k$.

As an example, suppose that $k = 1$ so that $R = (r, 0, 0, \cdots)$. Then the integers y_α must be zero whenever α contains an integer larger than one. Thus the only partitions α which are left are: (1), (1,1), (1,1,1), $\cdots$. Therefore we have $s_1 = y_1$, $s_2 = y_{11}$, $s_3 = y_{111}$, etc. The equations $(*)$ now reduce to the single equation

$$r = s_1 + (1+p)s_2 + (1+p+p^2)s_3 + \cdots \;.$$

But this is just the dimensional restriction that $\dim \mathscr{P}^S = (2p-2)s_1 + (2p^2-2)s_2 + \cdots$ be equal to $\dim \mathscr{P}^r = (2p-2)r$. Thus we obtain:

COROLLARY 6. *The conjugate* $c(\mathscr{P}^r)$ *is equal to* $(-1)^r \sum \mathscr{P}^S$ *where the sum extends over all* $\mathscr{P}^S$ *having the correct dimension.* (For example $c(\mathscr{P}^{2p+3}) = -\mathscr{P}^{2p+3} - \mathscr{P}^{p+2,1} - \mathscr{P}^{1,2}$.)

8. Miscellaneous remarks

The following question, which is of interest in the study of second order cohomology operations, was suggested to the author by A. Dold: *What is the set of all solutions* $\theta \in \mathscr{S}^*$ *to the equation* $\theta\mathscr{P}^1 = 0$? In view of the results of §7 we can equally well study the equation $\mathscr{P}^1\theta = 0$. The formula

$$\mathscr{P}^1 \mathscr{P}^{r_1 r_2 \cdots} = (1 + r_1)\mathscr{P}^{1+r_1, r_2 \cdots}$$

implies that this equation $\mathscr{P}^1\theta = 0$ has as solution the vector space spanned by the elements

$$\mathscr{P}^{r_1 r_2 \cdots} Q_0^{\varepsilon_0} Q_1^{\varepsilon_1} \cdots$$

with $r_1 \equiv -1 \pmod{p}$. The first such element is $\mathscr{P}^{p-1}$, and every element of the ideal $\mathscr{P}^{p-1}\mathscr{S}^*$ will also be a solution. Now the identity

$$\begin{aligned}\mathscr{P}^{p-1}\cdot\mathscr{P}^{s_1 s_2\cdots} &= (p-1, s_1)\mathscr{P}^{s_1+p-1, s_2, \cdots} \\ &= \begin{cases} 0 & \text{if } s_1 \not\equiv 0 \pmod p \\ -\mathscr{P}^{s_1+p-1, s_2, \cdots} & \text{if } s_1 \equiv 0 \pmod p \end{cases}\end{aligned}$$

shows that every element $\mathscr{P}^{r_1 r_2\cdots}Q_0^{\varepsilon_0}\cdots$ with $r_1 \equiv -1 \pmod p$ actually belongs to the ideal. Applying the conjugation operation, this proves the following:

PROPOSITION 1. *The equation* $\theta\mathscr{P}^1 = 0$ *has as solutions the elements of the ideal* $\mathscr{S}^*\mathscr{P}^{p-1}$. *An additive basis is given by the elements*

$$Q_0^{\varepsilon_0}Q_1^{\varepsilon_1}\cdots c(\mathscr{P}^{r_1 r_2\cdots}) \text{ with } r_1 \equiv -1 \pmod p .$$

Next we will study certain subalgebras of the Steenrod algebra. Adem shown that $\mathscr{S}^*$ is generated by the elements Q_0, $\mathscr{P}^1$, $\mathscr{P}^p$, $\cdots$. Let $\mathscr{S}^*(n)$ denote the subalgebra generated by Q_0, $\mathscr{P}^1$, $\cdots$, $\mathscr{P}^{p^{n-1}}$.

PROPOSITION 2. *The algebra* $\mathscr{S}^*(n)$ *is finite dimensional, having as basis the collection of all elements*

$$Q_0^{\varepsilon_0}\cdots Q_n^{\varepsilon_n}\mathscr{P}^{r_1, \cdots, r_n}$$

which satisfy

$$r_1 < p^n,\ r_2 < p^{n-1},\ \cdots,\ r_n < p .$$

Thus $\mathscr{S}^*$ is a union of finite dimensional subalgebras $\mathscr{S}^*(n)$. This clearly implies the following.

COROLLARY 7. *Every positive dimensional element of* $\mathscr{S}^*$ *is nil-potent.*

It would be interesting to discover a complete set of relations between the given generators of $\mathscr{S}^*(n)$. For $n = 0$ there is the single relation $[Q_0, Q_0] = 0$, where $[a, b]$ stands for $ab - (-1)^{\dim a \dim b}ba$. For $n = 1$ there are three new relations

$$[Q_0, [\mathscr{P}^1, Q_0]] = 0 , \quad [\mathscr{P}^1, [\mathscr{P}^1, Q_0]] = 0 \quad \text{and} \quad (\mathscr{P}^1)^p = 0 .$$

For $n = 2$ there are the relations

$$\begin{aligned}&[\mathscr{P}^1, [\mathscr{P}^p, \mathscr{P}^1]] = 0 , \quad [\mathscr{P}^p, [\mathscr{P}^p, \mathscr{P}^1]] = 0 , \\ &\qquad\qquad \text{and} \quad (\mathscr{P}^p)^p = \mathscr{P}^1[\mathscr{P}^p, \mathscr{P}^1]^{p-1} ,\end{aligned}$$

as well as several new relations involving Q_0. (The relations $(\mathscr{P}^p)^{2p} = 0$ and $[\mathscr{P}^p, \mathscr{P}^1]^p = 0$ can be derived from the relations above.) The author has been unable to go further with this.

PROOF OF PROPOSITION 2. Let $\mathscr{A}(n)$ denote the subspace of $\mathscr{S}^*$ spanned by the elements $Q_0^{\varepsilon_0}\cdots Q_n^{\varepsilon_n}\mathscr{P}^{r_1\cdots r_n}$ which satisfy the specified restrictions. We will first show that $\mathscr{A}(n)$ is a subalgebra. Consider the product

$$\mathscr{P}^{r_1\cdots r_n}\mathscr{P}^{s_1\cdots s_n} = \sum_{R(X)=(r_1\cdots),\, S(X)=(s_1,\,\ldots)} b(X)\mathscr{P}^{T(X)}$$

where both factors belong to $\mathscr{A}(n)$. Suppose that some term $b(X)\mathscr{P}^{t_1t_2\cdots}$ on the right does not belong to $\mathscr{A}(n)$. Then t_l must be $\geqq p^{n+1-l}$ for some l. If $x_{l0}, x_{l-1,1}, \ldots, x_{0l}$ were all $< p^{n+1-l}$, then the factor

$$\frac{t_l!}{x_{l0}!\cdots x_{0l}!}$$

would be congruent to zero modulo p. Therefore $x_{ij} \geqq p^{n+1-l}$ for some $i + j = l$. If $i > 0$ this implies that

$$r_i = \sum_j p^j x_{ij} \geqq p^j p^{n+1-l} = p^{n+1-i}$$

which contradicts the hypothesis that $\mathscr{P}^{r_1\cdots r_n} \in \mathscr{A}(n)$. Similarly if $i = 0$, $j = l$, then

$$s_j = \sum_i x_{ij} \geqq p^{k+1-l} = p^{k+1-j}$$

which is also a contradiction.

Since it is easily verified that $\mathscr{A}(n)Q_k \subset \mathscr{A}(n)$ for $k \leqq n$, this proves that $\mathscr{A}(n)$ is a subalgebra of $\mathscr{S}^*$. Since $\mathscr{A}(n)$ contains the generators of $\mathscr{S}^*(n)$, this implies that $\mathscr{A}(n) \supset \mathscr{S}^*(n)$.

To complete the proof we must show that every element of $\mathscr{A}(n)$ belongs to $\mathscr{S}^*(n)$. Adem's assertion that $\mathscr{S}^*$ is the union of the $\mathscr{S}^*(n)$ implies that every element of $\mathscr{S}^k$ with $k < \dim(\mathscr{P}^{p^n})$ automatically belongs to $\mathscr{S}^*(n)$. In particular we have:

Case 1. Every element $\mathscr{P}^{0\cdots 0p^i}$ in $\mathscr{A}(n)$ belongs to $\mathscr{S}^*(n)$.

Ordering the indices $(r_1, \cdots, r_n)$ lexicographically from the right, the product formulas can be written as

$$\mathscr{P}^{r_1\cdots r_n}\mathscr{P}^{s_1\cdots s_n} = (r_1, s_1)\cdots(r_n, s_n)\mathscr{P}^{r_1+s_1,\cdots, r_n+s_n} + (\text{higher terms})\,.$$

Given $\mathscr{P}^{t_1\cdots t_n} \in \mathscr{A}(n)$ assume by induction that

(1) every $\mathscr{P}^{r_1\cdots r_n} \in \mathscr{A}(n)$ of smaller dimension belongs to $\mathscr{S}^*(n)$, and

(2) every "higher" $\mathscr{P}^{r_1\cdots r_n} \in \mathscr{A}(n)$ in the same dimension belongs to $\mathscr{S}^*(n)$. We will prove that $\mathscr{P}^{t_1\cdots t_n} \in \mathscr{S}^*(n)$.

Case 2. $(t_1\cdots t_n) = (0\cdots 0t_i0\cdots 0)$ where t_i is not a power of p. Choose $r_i, s_i > 0$ with $r_i + s_i = t_i$, $(r_i, s_i) \not\equiv 0$. Then $\mathscr{P}^{0\cdots r_i}\mathscr{P}^{0\cdots s_i} = (r_i, s_i)\mathscr{P}^{0\cdots t_i} + (\text{higher terms})$.

Case 3. Both t_i and t_j are positive, $i < j$. Then

$$\mathscr{P}^{t_1\cdots t_i}\mathscr{P}^{0\cdots 0t_{i+1}\cdots t_n} = \mathscr{P}^{t_1\cdots t_n} + (\text{higher terms})\,.$$

In either case the inductive hypothesis shows that $\mathscr{P}^{t_1\cdots t_n}$ belongs to $\mathscr{S}^*(n)$. Since $Q_0, \cdots, Q_n$ belong to $\mathscr{S}^*(n)$ by Corollary 3, this completes the proof of Proposition 2.

Appendix 1. The case $p = 2$

All the results in this paper apply to the case $p = 2$ after some minor changes. The cohomology ring of the projective space $\mathscr{P}^N$ is a truncated polynomial ring with one generator α of dimension 1. It turns out that $\lambda^*(\alpha) \in H^*(P^N, Z_2) \otimes \mathscr{S}_*$ has the form

$$\alpha \otimes \zeta_0 + \alpha^2 \otimes \zeta_1 + \cdots + \alpha^{2^r} \otimes \zeta_r$$

where $\zeta_0 = 1$ and where each ζ_i is a well defined element of $\mathscr{S}_{2^i-1}$. The algebra $\mathscr{S}_*$ is a polynomial algebra generated by the elements $\zeta_1, \zeta_2, \cdots$.

Corresponding to the basis $\{\zeta_1^{r_1}\zeta_2^{r_2}\cdots\}$ for $\mathscr{S}_*$ there is a dual basis $\{Sq^R\}$ for $\mathscr{S}^*$. These elements $Sq^{r_1r_2\cdots}$ multiply according to the same formula as the $\mathscr{P}^R$. The other results of this paper generalize in an obvious way.

Appendix 2. Sign conventions

The standard convention seems to be that no signs are inserted in formulas 1, 2, 3 of §2. If this usage is followed then the definition of λ^* becomes more difficult. However Lemmas 2 and 3 still hold as stated, and Lemma 4 holds in the following modified form.

LEMMA 4′. *If* $\lambda^*(\alpha) = \sum \alpha_i \otimes \omega_i$ *then for any* $\theta \in \mathscr{S}^*$:

$$\theta\alpha = (-1)^{\frac{1}{2}d(d-1)+d\dim\alpha} \sum \langle \theta, \omega_i \rangle \alpha_i$$

where $d = \dim\theta$.

It is now necessary to define $\tau_i \in \mathscr{S}_{2p^i-1}$ by the equation

$$\lambda^*(\alpha) = \alpha \otimes 1 - \beta \otimes \tau_0 - \beta^p \otimes \tau_1 - \cdots .$$

Otherwise there are no changes in the results stated.

PRINCETON UNIVERSITY

REFERENCES

1. J. ADEM, The relations on Steenrod powers of cohomology classes, Algebraic geometry and topology, Princeton University Press, 1957, 191–238.
2. H. CARTAN, *Sur l'itération des opérations de Steenrod*, Comment. Math. Helv., 29 (1955), 40–58.
3. J. MILNOR and J. MOORE, On the structure of Hopf algebras, to appear.
4. N. STEENROD, *Cyclic reduced powers of cohomology classes*, Proc. Nat. Acad. Sci. U.S.A., 39 (1953), 217–223.
5. R. THOM, *Quelques propriétés globales des variétés différentiables*, Comment. Math. Helv., 28 (1954), 17–86.