THE MODULE OF INDECOMPOSABLES
FOR FINITE H-SPACES

BY
RICHARD KANE

ABSTRACT. The module of indecomposables obtained from the mod p cohomology of a finite H-space is studied for p odd. General structure theorems are obtained, first, regarding the possible even dimensions in which this module can be nonzero and, secondly, regarding how the Steenrod algebra acts on the module.

1. Introduction. An H-space \((X, \mu)\) is a pointed topological space \(X\) which has the homotopy type of a connected CW complex of finite type together with a basepoint preserving map \(\mu: X \times X \to X\) with two-sided homotopy unit. An H-space \((X, \mu)\) will be said to be mod \(p\) finite if \(H^*(X; \mathbb{Z}_p)\) is a finite-dimensional \(\mathbb{Z}_p\) module. \((\mathbb{Z}_p\) are the integers reduced mod \(p\).) If \((X, \mu)\) is a mod \(p\) finite H-space then a knowledge of the module of indecomposables \(Q(H^*(X; \mathbb{Z}_p))\) is important and useful for several reasons. It would be a major step in determining the possible Hopf algebra structures on \(H^*(X; \mathbb{Z}_p)\). Moreover, as the results of [2] and [5] indicate, a knowledge of \(Q(H^*(X; \mathbb{Z}_p))\) and, in particular, of \(Q(H^\text{even}(X; \mathbb{Z}_p))\), is necessary for any systematic understanding of the occurrence of \(p\) torsion in \(H^*(X; \mathbb{Z})\). In this paper we will study the structure of \(Q(H^\text{even}(X; \mathbb{Z}_p))\) when \(p\) is odd.

Given a positive integer \(m\) let \(m = \Sigma m_s p^s\) be its \(p\)-adic expansion. We say \(m\) is binary (with respect to \(p\)) if \(m_s = 0\) or \(1\) for each \(s\).

**Theorem 1.1.** Let \(p\) be odd and let \((X, \mu)\) be a mod \(p\) finite H-space such that \(H^*(X; \mathbb{Z}_p)\) is a coassociative Hopf algebra. Then \(Q(H^{2m}(X; \mathbb{Z}_p)) = 0\) unless \(m\) is binary.

We will speak of \(Q(H^\text{even}(X; \mathbb{Z}_p))\) as being binary if the condition in 1:1 is satisfied.

Now \(Q(H^*(X; \mathbb{Z}_p))\) is a module over the Steenrod algebra \(A^*(p)\). If \(X\) is
mod $p$ finite then, by [1], $\beta_p Q(H^{even}(X; Z_p)) = 0$. Hence, $Q(H^{even}(X; Z_p))$ is a Steenrod submodule of $Q(H^*(X; Z_p))$. Theorem 1:1 has consequences for this Steenrod module structure.

We first define some functions. Let $\gamma(0) = 0$ and, for $s \geq 1$, let $\gamma(s) = \sum_{t=0}^{s-1} p^t$. Suppose $m$ is binary and $m \equiv \gamma(s) \mod p^s$ but $m \not\equiv \gamma(s + 1) \mod p^{s+1}$. Then, let $\rho(m) = \gamma(s)$ and $\delta(m) = (m - \gamma(s))/p$. Given $m$ with $p$-adic expansion $\Sigma_{s \geq 0} m_s p^s$ let $\omega(m) = \Sigma_s m_s$.

**Theorem 1:2.** Let $p$ be odd and let $(X, \mu)$ be a mod $p$ finite $H$-space such that $H^*(X; Z_p)$ is a coassociative Hopf algebra. Then the function $\omega$ defines a splitting of $Q(H^{even}(X; Z_p))$ as a Steenrod module, namely $Q(H^{even}(X; Z_p)) = \bigoplus_{s \geq 1} M_s$ where $M_s = \Sigma_{\omega(m) = s} Q(H^{2m}(X; Z_p))$.

**Theorem 1:3.** Let $p$ be odd and let $(X, \mu)$ be a mod $p$ finite $H$-space such that $H^*(X; Z_p)$ is a coassociative Hopf algebra. Then, for $m$ binary $Q(H^{2m}(X; Z_p)) = p^\delta(m) Q(H^{2\delta(m) + 2p(m)}(X; Z_p))$.

In particular $Q(H^{2m}(X; Z_p)) = 0$ unless $m \equiv 1 \mod p$.

By using the results of [2] we can also deduce from 1:3:

**Theorem 1:4.** Let $p$ be odd and let $(X, \mu)$ be a mod $p$ finite $H$-space such that $H^*(X; Z_p)$ is a coassociative Hopf algebra. Then, for $m \geq 1$, the rank of $Q(H^{2m}(X; Z_p))$ as a $Z_p$-module is bounded by the rank of $Q(H^{2m-1}(X; Z_p))$ as a $Z_p$-module.

Results 1:1, 1:2 and 1:3 are motivated by the result of Zabrodsky [10] that $Q(H^{even}(X; Z_p))$ is generated as a Steenrod module by $\Sigma_{s \geq 1} Q(H^{2\gamma(s)}(X; Z_p))$. Our approach, while based on [10], is somewhat different. The principal tool used is that of secondary operations. We first generalize the construction of secondary operations in the cohomology of $H$-spaces as given in [9]. We then apply these secondary operations to study $Q(H^{even}(X; Z_p))$. However, as compared to [10], our approach places more emphasis on algebra and less on homotopy theory. This will make the paper relatively self-contained.

In §2 we will do some Hopf algebra preliminaries and, in particular, study the Hopf algebra structure of $H^*(X; Z_p)$ and $H_*(X; Z_p)$. In §3 we will describe the method of constructing secondary operations for the cohomology of $H$-spaces. In §4 we will study the structure of $Q(H^{even}(X; Z_p))$ and, in particular, prove 1:2, 1:3, 1:4, at least assuming 1:1 is true. In §5 we will prove 1:1.

2. **Hopf algebras.** The basic reference for Hopf algebras is [8]. We will use the term "Hopf algebra" in the sense of what is there called a
"quasi-Hopf algebra". We will assume that all Hopf algebras are over \( \mathbb{Z}_p \) and are graded, connected and of finite type. Given a graded module \( A \) we use the symbol \( \overline{A} \) to denote the elements of positive dimension. Let \( (X, \mu) \) be an \( H \)-space. Then \( H^* = H^*(X; \mathbb{Z}_p) \) and \( H_*(X; \mathbb{Z}_p) \) have natural structures as Hopf algebras over \( A^*(p) \) induced by \( \mu \) and the diagonal map \( \Delta : X \rightarrow X \times X \). The action of \( A^*(p) \) on \( H_* \) is a right one and is obtained by duality from the usual left action of \( A^*(p) \) on \( H^* \). All Hopf algebras will be assumed to be either associative and commutative like \( H^* \) or coassociative and cocommutative like \( H_* \).

Given a Hopf algebra \( A \) we define its dual \( A^* \) by the rule
\[
(A^*)^n = \text{Hom}_0(A^n; \mathbb{Z}_p).
\]

We use \( P(A) \) and \( Q(A) \) to indicate primitives and indecomposables respectively. We observe that \( P(A) \) and \( Q(A^*) \) are dual in the sense of a submodule of \( A \) being dual to a quotient module of \( A^* \). In particular \( H^* \) and \( H_* \) are dual Hopf algebras and, in that case, the Steenrod module structures of \( Q(H^*) \) and \( P(H_*) \) are dual as well.

(2:1) The natural map \( P(A) \rightarrow Q(A) \) is injective in odd dimension if \( A \) is commutative and associative. It is surjective in odd dimension if \( A \) is cocommutative and coassociative.

If \( B \) is a normal sub Hopf algebra of \( A \) then the quotient Hopf algebra \( A/B = A/BA \) is defined. Where there is no confusion we will use the same symbol for an element in \( A \) and for its image in a quotient module. We will do likewise for induced maps between quotient modules.

Given a Hopf algebra with comultiplication \( \psi \) we will use the symbol \( \overline{\psi} \) to denote the reduced comultiplication defined by the rule
\[
\overline{\psi}(x) = \psi(x) - x \otimes 1 - 1 \otimes x \quad \text{for any } x \in A.
\]

Given \( x \in A \) we let \( |x| \) denote the dimension of \( x \). Given an algebra \( A \) we define the Lie bracket product \([ , ]\) by the rule
\[
[x, y] = xy - (-1)^{|x||y|} yx \quad \text{for any } x, y \in A.
\]

In the rest of this section we will study the Hopf algebra structure of \( H^* \) when \( (X, \mu) \) is an \( H \)-space as in 1:1. Our principal result is

**Theorem 2.2.** Let \( (X, \mu) \) be a mod \( p \) finite \( H \)-space such that \( H^* \) is a coassociative Hopf algebra. Then \( H^* \) contains a sub Hopf algebra \( \Gamma \) over \( A^*(p) \) such that

(i) the natural map \( Q(\Gamma) \rightarrow Q(H^*) \) is surjective in even dimensions,

(ii) \( \Gamma^{2j+1} = 0 \) for all \( j \).
The rest of this section will be devoted to proving 2:2. First, recall the following facts obtained by Browder using the Bockstein spectral sequence.

**Lemma 2.3.** If \( u, v \in \mathcal{P}(H_{\text{odd}}) \) then \( u^2 = v^2 = 0, u\beta_p = v\beta_p = 0 \), and \( uv = -vu \).

See [6] for proofs. Let \( \Lambda \) be the sub Hopf algebra of \( H_\ast \) generated over \( A_\ast(p) \) by \( \mathcal{P}(H_{\text{odd}}) \). By 2:3 it is the exterior Hopf algebra generated by \( \mathcal{P}(H_{\text{odd}}) \).

Suppose for the moment that the following is true.

**Lemma 2.4.** \( \Lambda \) is a normal sub Hopf algebra of \( H_\ast \).

Then \( \Omega = H_\ast/\Lambda \) is defined as a Hopf algebra over \( A_\ast(p) \). We let \( \Gamma = \Omega_\ast \subset H_\ast \). Then \( \Gamma \) satisfies (i) and (ii) of 2:2.

**Property (i).** Since \( H_\ast/\Gamma = \Lambda_\ast \) there is an exact sequence

\[
(*) \quad Q(\Gamma) \rightarrow Q(H_\ast) \rightarrow Q(\Lambda_\ast) \rightarrow 0
\]

(see 3:11 of [8]). But, by construction, \( P_{\text{even}}(\Lambda) = 0 \) and so \( Q_{\text{even}}(\Lambda_\ast) = 0 \).

**Property (ii).** It suffices to show \( Q_{\text{odd}}(\Gamma) = 0 \). We will do this by induction. We have that \( Q^{-1}(\Gamma) = 0 \). So assume by induction that \( Q^{2i+1}(\Gamma) = 0 \) if \( i < k \). To show that \( Q^{2k+1}(\Gamma) = 0 \) it suffices to show that the natural map \( Q^{2k+1}(\Gamma) \rightarrow Q(H^{2k+1}) \) is: (a) trivial, and, (b) a monomorphism. Fact (a) follows from the exact sequence \( (*) \) since, by construction \( P_{\text{odd}}(\Lambda) = \mathcal{P}(H_{\text{odd}}) \) and so \( Q(H_{\text{odd}}) \cong Q_{\text{odd}}(\Lambda_\ast) \). Fact (b) follows from the commutative diagram

\[
P^{2k+1}(\Gamma) \rightarrow Q^{2k+1}(\Gamma) \quad \downarrow \downarrow
P(H^{2k+1}) \rightarrow Q(H^{2k+1}).
\]

For, by 2:1 and the induction hypothesis, the top vertical map is an isomorphism and the bottom vertical map is a monomorphism. Further, the left vertical map is an obvious monomorphism.

Thus to prove 2:2 we are left with proving 2:4. We first recall some facts about normal sub Hopf algebras. Let \( A \) be an associative, coassociative, cocommutative Hopf algebra. Let \( B \) be a sub Hopf algebra of \( A \) and \( C \) a sub Hopf algebra of \( B \). Suppose \( C \) is normal in both \( A \) and \( B \).

**Lemma 2.5.** \( B/\!\!/C \) is a sub Hopf algebra of \( A/\!\!/C \), that is, the induced map \( B/\!\!/C \rightarrow A/\!\!/C \) is a monomorphism.

**Lemma 2.6.** \( B/\!\!/C \) is normal in \( A/\!\!/C \) if, and only if, \( B \) is normal in \( A \).

**Lemma 2.7.** If \( B \) is normal in \( A \) then \( A/\!\!/B \) and \( (A/\!\!/C)/\!\!(B/\!\!/C) \) are isomorphic as Hopf algebras.
Lemma 2.8. If $B$ is normal in $A$ then the sequence $0 \to P(B) \to P(A) \to P(A/B) \to 0$ is exact in odd dimensions.

Lemma 2.5 follows from the fact (see 4.4 of [8]) that we can form a commutative diagram of $C$-modules:

\[
\begin{array}{ccc}
B = C \otimes B/\!\!/C \\
\downarrow & & \downarrow \\
A = C \otimes A/\!\!/C
\end{array}
\]

Lemma 2.6 is an exercise in working with cosets. Regarding Lemma 2.7 we have a surjective map of Hopf algebras $(A/\!\!/C)/(A/\!\!/B) \to A/\!\!/B$ induced from the map $A/\!\!/C \to A/\!\!/B$. The following identities (see 4.4 of [8]) then show the map must be an isomorphism:

\[
B \otimes A/\!\!/B \cong A \cong C \otimes A/\!\!/C \cong C \otimes B/\!\!/C \otimes A/\!\!/C/\!\!/B \otimes C \cong B \otimes A/\!\!/C/\!\!/B/\!\!/C.
\]

For Lemma 2.8 we need only show $P(A) \to P(A/\!\!/B)$ is surjective in odd dimensions. The rest follows by an argument similar to that given in the proof of 2:2(ii). If we dualize it suffices to show $Q(D) \to Q(A^*)$ is injective where $D$ is a sub Hopf algebra of $A^*$. Given $x \in Q(D^{2n+1})$ represented by $x \in D^{2n+1}$ let $D'$ be the sub Hopf algebra of $D$ generated by the elements of dimension $2n$ or less. Then $x$ is nonzero and primitive in $D/\!\!/D'$. As in 2:5 $x$ is nonzero and primitive in $A^*/\!\!/D'$. By 4:21 of [8] $x$ is nondecomposable in $A^*/\!\!/D'$ and thus in $A^*$ as well.

Now let $\Lambda(n)$ be the sub Hopf algebra generated by $\Sigma_{2 \geq n} P(H_{2s+1})$. To prove 2:4 we will show by decreasing induction on $n$ that $\Lambda(n)$ is normal in $H_\bullet$. Now if we pick $n$ large then $\Lambda(n)$ is trivial since $H_\bullet$ is finite. Assume, by induction, that $\Lambda(n + 1)$ is normal in $H_\bullet$. Let $\Omega(n + 1) = H_\bullet/\!\!/\Lambda(n + 1)$. By 2:3 $\Lambda(n + 1)$ is normal in $\Lambda(n)$. Let $\Phi(n + 1) = \Lambda(n)/\!\!/\Lambda(n + 1)$. By 2:5 $\Phi(n + 1)$ is a sub Hopf algebra of $\Omega(n + 1)$. By 2:6, in order to show $\Lambda(n)$ is normal in $H_\bullet$, it suffices to show $\Phi(n + 1)$ is normal in $\Omega(n + 1)$. We will show more, namely,

Lemma 2.9. $\Phi(n + 1)$ is central in $\Omega(n + 1)$ i.e. $[x, y] = 0$ for all $x \in \Phi(n + 1), y \in \Omega(n + 1)$ where $[,]$ is the Lie bracket product.

Proof. Since $\Phi(n + 1)$ is a primitively generated exterior Hopf algebra on generators of dimension $2n + 1$, we can assume $x$ is such a generator. We can assume $y$ is indecomposable. If $y$ is odd dimensional then by 2:1 $y$ can be assumed to be primitive and hence, by 2:3 and 2:8, $[x, y] = 0$. If $y$ is even dimensional then by an (increasing) induction on the dimension of $\Omega(n + 1)$ we can
assume \([x, y]\) is primitive. For, if \(\Delta_*(y) = \sum y' \otimes y''\), then
\[
\Delta_*[x, y] = \sum_s [x, y'_s] \otimes y'' \pm y'_s \otimes [x, y''_s].
\]

By 2:8, \(\Omega(n + 1)\) has no nonzero primitive elements of odd dimension greater than \(2n + 1\). Hence \([x, y] = 0\).

3. Secondary operations. Secondary operations are associated to Adem relations and are constructed by means of universal example \((E, u, v)\) (see §1 of [10]). For our purposes we are interested in unstable Adem relations. By an unstable relation in dimension \(s\) we mean any relation which holds among the elements of \(A^*(p)\) as they act on the fundamental class \(t_s \in H^s(K(Z_p, s); Z_p)\). Any such relation is obtained from an ordinary stable Adem relation by equating to zero all Steenrod operations which act trivially on \(t_s\). An element \(\theta \in A^*(p)\) is said to be of excess \(s\) or less (\(e(\theta) \leq s\)) if \(\theta(t_s) \neq 0\).

Now suppose \(m > k > 0\). Let \(0 \in A_k(p)\) where \(e(0) < 2m - k\). Let
\[
(3:1) \quad \sum_q q_s b_s = \beta_p P^m \theta
\]
be an unstable Adem relation in dimension \(2m - k + 1\) such that, for each \(s\), \(|b_s| > |\theta| = k\) or \(e(b_s) < e(\theta)\). It gives rise to the unstable Adem relation
\[
(3:2) \quad \sum q_s b_s = 0
\]
in dimension \(2m - k\). We will define, by means of universal example \((E, u, v)\) an unstable secondary operation \(\phi\) associated with 3:2 such that

**Proposition 3:3.** If \(\phi(x)\) and \(\phi(y)\) are defined then
\[
\phi(x + y) = \phi(x) + \phi(y) + \sum_{i=1}^{p-1} \frac{1}{p} \begin{pmatrix} p \\ i \end{pmatrix} \theta(x)^i \otimes \theta(y)^{p-i}.
\]

Equivalently, if \(\alpha: E \times E \rightarrow E\) is the loop multiplication defined on \(E\), then
\[
\alpha^*(u) = \sum_{i=1}^{p-1} \frac{1}{p} \begin{pmatrix} p \\ i \end{pmatrix} \theta(u)^i \otimes \theta(u)^{p-i}.
\]

For a proof of 3:3 see [3] and [4].

Because of the manner in which 3:3 is obtained we will violate the usual terminology and speak of \(\phi\) as the unstable secondary operation associated with 3:1 (rather than 3:2).

From 3:3 we obtain our basic result about secondary operations.

**Theorem 3:4.** Let \((X, \mu)\) be an H-space. Let \(\phi\) be the unstable operation associated with 3:1. Let \(B \subset H^*\) be an \(A^*(p)\) module and let \(I(B)\) be the ideal
generated by \( \bar{B} \). Given \( x \in H^{2m-k}, y \in H^{2m} \) such that \( y = \theta(x), x \in \cap_s \ker b_s \) and \( \bar{\mu}^s(x) \in I(B) \otimes I(B) \) then, in \( H^*/|B \otimes H^*/|B, \)

\[
\bar{\mu}^s \phi(x) \equiv \sum_{i=1}^{p-1} \frac{1}{p} \left( \binom{p}{i} \right) y^i \otimes y^{p-i} \mod \sum_s \im a_s.
\]

**Remark.** This theorem generalizes 3:2 of [9]. Those cases are obtained by letting \( x = y \) and \( \theta = 1 \in A^0(p) \). However applications of 3:2 of [9] cannot be generalized so easily. There is a difficulty encountered when we attempt to apply our new operations. For, assume \( x \) and \( y \) are nondecomposable and that \( \phi \) is defined on \( x \). This will be the usual situation. Then we can find \( B \) such that \( \bar{\mu}^s(x) \in I(B) \otimes I(B) \). If \( x \neq y \), the difficulty is to find \( B \) such that \( y \not\in B \) as well. We overcome this difficulty when proving Proposition 5:3 by assuming that \( H^* \) is coassociative.

Theorem 3:4 is obtained from 3:3 in the same way as Theorem 3:2 of [9] is obtained from Proposition 3:1 of [9]. Our restrictions on the \( b_s \) element ensure that \( \theta(u) \neq 0 \).

4. The \( A^*(p) \) structure of \( Q(H^*) \). For this section assume that \( p \) is odd and that \( (X, \mu) \) is a \( \mod p \) finite \( H \)-space such that \( H^* \) is a coassociative Hopf algebra. We will study the structure of \( Q(H^{even}) \) and, in particular, prove 1:2, 1:3 and 1:4, at least modulo the proof of 1:1.

We begin with some results obtained by using the secondary operations discussed in the last section. We will state the results in terms of \( P(H^*) \) since they are clearer in that form. Let \( \{Q_s\}_{s \geq 0} \) be the Milnor elements of \( A^*(p) \) (see [7]). In particular \( Q_0 = \beta_p \). Given \( s, m \geq 0 \) we have the relation

\[
Q_s P^m = P^m Q_s - Q_{s+1} P^m - p^s.
\]

We can deduce from 4:1 the relation

\[
Q_0 P^m = \sum_s (-1)^s P^{m - \gamma(s)} Q_s.
\]

(In both 4:1 and 4:2 and in any later case we use the convention that \( P^n = 0 \) if \( n \) is negative.)

**Proposition 4:3.** Given \( 0 \neq y \in P(H_{2m}) \) where \( m \neq \gamma(s) \) for any \( s \geq 1 \) and \( \bigotimes_{i=1}^p y \in \cap_{s \geq 1} \ker P^{m - \gamma(s)} \), then \( y^p \neq 0 \). (Here \( \bigotimes_{i=1}^p y \) is an element of \( \bigotimes_{i=1}^p H^* \) and the action of \( A^*(p) \) on \( \bigotimes_{i=1}^p H^* \) is the one obtained by the Cartan formula from the action of \( A^*(p) \) on \( H^* \).)

**Proof of 4:3.** For \( k \geq 1 \) define a map \( u^k : H^* \rightarrow \bigotimes_{i=1}^k H^* \) by the recursive formula that \( u^1 = \) the identity and \( u^k = (u^{k-1} \otimes 1) \bar{u}^* \) where \( \bar{u}^* \) is the
reduced comultiplication. Expand $y$ to a basis of $P(H_{2m})$ and pick $x \in Q(H^{2m})$ dual to $y$. Let $\Gamma$ be as in 2:2. Let $F_q$ be the sub Hopf algebra of $\Gamma$ over $A*(p)$ generated by $\Sigma_{i \leq q} \Gamma_{2i}$. By (ii) of 2:2 we can pick $q$ such that $x \in Q(F_q)$, $x \notin Q(F_{q-1})$. Also $x$ is represented by an element $x \in \Gamma_{2m}$ and we can choose it such that $x \in F_q$. Then $\bar{u}^*(x) \in F_{q-1} \otimes F_{q-1}$. By (i) of 2:2 $Q_s(x) = 0$ for $s > 0$. Hence the unstable secondary operation $\phi$ corresponding to 4:2 (obtained by letting $a_s = (-1)^s P^{m-\gamma(s)}$, $b_s = Q_s$ for each $s$) is defined on $x$ and, in $H^*//F_{q-1} \otimes H^*//F_{q-1},$

$$\bar{u}^* \phi(x) \equiv \sum_{i=1}^{p-1} \frac{1}{p} \left( \begin{array}{c} p \\ i \end{array} \right) x^{p-i} \otimes x^i \mod \sum_{s \geq 0} \text{Image } P^{m-\gamma(s)}.$$  

Hence, in $\bigotimes_{i=1}^p Q(H^*//F_{q-1}),$

$$u^p \phi(x) \equiv \bigotimes_{i=1}^p x \mod \sum_{s \geq 1} \text{Image } P^{m-\gamma(s)}.$$  

(Here we have mapped into $\bigotimes_{i=1}^p H^*//F_q$ using $\mu^p$ and then projected onto $\bigotimes_{i=1}^p Q(H^*//F_q)$ in the obvious manner. We can ignore $\text{Image } P^m$ since $x$ is indecomposable while $P^m$ can be equated with the $p$th power map because of the dimensions involved). By the duality between $x$ and $y$, 4:3 follows. Q.E.D.

**Lemma 4:4.** Given $x \neq y \in P(H_{2m})$; if $m \neq \gamma(s)$ for some $s > 1$ then $y^q \neq 0$ for some $q > 1$. In particular, $y^p = 0$ if, and only if, $m \equiv 1 \mod p$.

**Proof.** The first statement follows from 4:3 by a (decreasing) inductive argument on the dimension of $y$ (or see [10]). Regarding the second statement, if $m \equiv 1 \mod p$ then $m - \gamma(s) \equiv 0 \mod p$ for any $s > 1$. Hence $P^1 P^{m-\gamma(s)-1} = \alpha P^{m-\gamma(s)}$ ($\alpha \in Z_p$) and $y^p = 0$ by 4:3. It then follows from the Adem relation $(P^1)^p = 0$ that $y^p = 0$ if $m \equiv 1 \mod p$. Q.E.D.

The rest of this section is devoted to showing that if 1:1 is true then 1:2, 1:3, 1:4 are true. The proofs of 1:2 and 1:4 are straightforward.

(I) **Proof of 1:2.** The following is quite obvious.

**Lemma 4:5.** Let $Q(h_{\text{even}})$ be binary. Given $x \in Q(H^{2n})$, $y \in Q(H^{2m})$ such that $y = P^p(x) \neq 0$ then, in the $p$-adic expansions $n = \Sigma n_p p^s$, $m = \Sigma m_p p^s$, we must have $m_{k+1} = 1$, $m_k = 0$, $n_{k+1} = 0$, $n_k = 1$.

Hence $P^{pk}$ merely "permutes" $0$ and $1$ and $\omega(n) = \omega(m)$. Since the elements $\{P^{pk}\}$ are together with $\beta_p$ generate $A^*(p)$, 1:2 follows from 1:1 and 4:5. Q.E.D.

(II) **Proof of 1:4.** This is merely a refinement of the proof of Theorem 4:7 of [2]. For a justification of all the statements of our proof we refer to [2].
Let \( \{ B_r, d_r \} \) \( r \geq 1 \) be the mod \( p \) cohomology Bockstein spectral sequence for \( X \). In particular \( B_1 = H^* \). Given \( x \in Q(H^{2m}) = Q(B_1^{2m}) \) we can find \( r \geq 1 \) such that \( x \) survives to \( B_r \) and \( d_r(y) = x \) for \( y \in Q(B_r^{2m-1}) \). If \( m \not\equiv 0 \mod p \) then every element of \( Q(B_r^{2m-1}) \) is represented in \( B_r^{2m-1} \) by a nondecomposable element \( B_r^{2m-1} = H^{2m-1} \) which has survived to \( B_r^{2m-1} \). But, if 1:3 is true then \( m \equiv 1 \mod p \). Hence, modulo the proof of 1:3, we are done. Q.E.D.

Before proving 1:3 we obtain some Steenrod module structure theorems for \( Q(H^{\text{even}}) \). Since we will have constant need of them we explicitly state the following Adem relations.

For \( a, b \geq 0 \) and \( p \) odd,

\[ p^a p^b = \sum_{s \leq (a/p)} \alpha_s p^{a+b-s} p^s \] where \( \alpha_s = (-1)^{a+s} \left( \frac{(p-1)(b-s)-1}{a-ps} \right) \).

We also note the following consequence of 4:5:

**Lemma 4:7.** If \( Q(H^{\text{even}}) \) is binary then, for \( s \geq 0 \), \( (p^s)^2 = 0 \) on \( Q(H^{\text{even}}) \).

The main technical result which we need is

**Proposition 4:8.** Let \( Q(H^{\text{even}}) \) be binary. Let \( K \geq 1 \). If \( m \equiv 0 \mod p^K \) then \( p^{m-q} p^q = 0 \) on \( Q(H^{\text{even}}) \) unless \( q \equiv 0 \mod p^K \).

**Proof.** By induction on \( K \).

**Case** \( K = 1 \). Suppose \( q \not\equiv 0 \mod p \). Hence \( m-q \not\equiv 0 \mod p \). We wish to show \( p^{m-q} p^q = 0 \) on \( Q(H^{\text{even}}) \). Let

\[ q = p^a + a, \quad m - q = p^b + b, \]

where \( a \neq 0, b \neq 0 \) and \( a + b = p \). From 4:6 we deduce

\[ p^q = \alpha(p^1)^a p^p, \quad p^{m-q} = \beta(p^1)^b p^p, \]

where \( \alpha, \beta \in \mathbb{Z}_p \). But either \( a \) or \( b \) > 1. Hence, by 4:7, either \( p^q = 0 \) or \( p^{m-q} = 0 \) on \( Q(H^{\text{even}}) \).

Now suppose the lemma is true for \( i < K \) and consider the

**General case** \( K \). Suppose \( q \not\equiv 0 \mod p^K \). Hence \( m-q \not\equiv 0 \mod p^K \). We again wish to show \( p^{m-q} p^q = 0 \) on \( Q(H^{\text{even}}) \). By the induction hypothesis we can assume \( q \equiv -q \equiv 0 \mod p^{K-1} \). Let

\[ q = p^K \alpha + p^{K-1} a, \quad m - q = p^K b + p^{K-1} b, \]

where \( a \neq 0, b \neq 0 \) and \( a + b = p \). From the induction hypothesis and 4:6 we can deduce that, in \( Q(H^{\text{even}}) \),

\[ p^q = \alpha(p^{K-1})^a p^{K-1} \alpha, \quad p^{m-q} = \beta(p^{K-1})^b p^{K-1} b, \]

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
where \( \alpha, \beta \in \mathbb{Z}_p \). Again, since either \( a \) or \( b > 1 \) it follows, from 4:7, that 
\( p^{m-q} p^q = 0 \) on \( Q(H_{\text{even}}) \). Q.E.D.

Proposition 4:8 has one immediate corollary. For, from 4:8 and 4:6, it follows that, if \( m = \Sigma m_p s^i \) is the \( p \)-adic expansion of \( m \), then

\[
p^m = \alpha (p^1)^{m_0} (p^p)^{m_1} \cdots (p^p)^{m_r}
\]

where \( \alpha \in \mathbb{Z}_p \). By 4:7 we can conclude

**Proposition 4:9.** \( P^m \) acts trivially on \( Q(H_{\text{even}}) \) unless \( m \) is binary. If \( m = \Sigma p^{s_i} (s_1 < s_2 < \cdots < s_t) \) then

\[
P^m = \alpha p^{s_1} p^{s_2} \cdots p^{s_t} \quad \text{on} \quad Q(H_{\text{even}}) \quad (\alpha \in \mathbb{Z}_p).
\]

(III) **Proof of 1:3.** We prove 1:3 by increasing induction on dimension. For \( m = 1 \) the result is trivial. Assume 1:3 is true in dimensions less than \( 2m \) and that \( Q(H^{2m}) \neq 0 \). Since we are assuming 1:1 is true \( m \) is binary.

**Lemma 4:10.** \( \rho(m) > 0 \).

**Proof.** By contradiction. Suppose \( m \equiv 0 \mod p \). By 4:4 \( Q(H^{2m}) = P^1 Q(H^{2n}) \) where \( n = m - p + 1 \). By 4:5 \( n \equiv 1 \mod p^2 \). By the induction hypothesis \( Q(H^{2n}) = P^{\delta(n)} Q(H^{2\delta(n)+2}) \). Then \( Q(H^{2m}) = P^1 P^{\delta(n)} Q(H^{2\delta(n)+2}) = 0 \) since, in dimension \( 2\delta(n) + 2 \), \( P^{\delta(n)+1} \) agrees with the \( p \)-th power map. Q.E.D.

**Lemma 4:11.** Given \( y \in P(H_{2m}) \) then \( y^p = 0 \).

**Proof.** By 4:10 \( m \equiv 1 \mod p \). By 4:4 \( y \in \ker P^1 \). Hence \( y^p \in P(H_{2pm}) \cap \ker P^1 \). By 4:4 \( y^p = 0 \). Q.E.D.

Now pick \( 0 \neq y \in P(H_{2m}) \). By 4:3 and 4:11 \( \bigotimes_{i=1}^s y \notin \bigcap_{i \geq 1} \ker P^{m-\gamma(s)} \).

From this we will deduce that \( y P^{\delta(m)} \neq 0 \). This proves 1:3 since \( y \) is arbitrary.

Pick \( K > 0 \) such that \( m \equiv \gamma(K) \mod p^{K+1} \). By 4:10 \( K > 0 \). From 4:5 and 4:9 we can deduce

**Lemma 4:12.** (i) \( y^p q = 0 \) unless \( q \equiv 0 \mod p^K \);
(ii) \( y P^q = 0 \) if \( q > \delta(m) \).

We consider how \( P^{m-\gamma(s)} \) acts on \( \bigotimes_{i=1}^p y \) in three cases:

(i) \( 1 < s < K \): Since \( m - \gamma(s) \neq 0 \mod p^K \) it follows, from 4:12(i), and the Cartan formula that \( \bigotimes_{i=1}^s y \in \ker P^{m-\gamma(s)} \).

(ii) \( s = K \): Since \( m - \gamma(K) = p\delta(m) \) it follows, from 4:12(ii), and the Cartan formula that \( (\bigotimes_{i=1}^p y) P^{m-\gamma(K)} = \bigotimes_{i=1}^p y P^{\delta(m)} \). Hence, we can
assume \( \bigotimes_{i=1}^{p} y \in \ker P^{m-\gamma(K)} \) since, otherwise, we are done.

(iii) \( s > K \): By (i) and (ii) there exists \( s > K \) such that \( \bigotimes_{i=1}^{p} y \in \ker P^{m-\gamma(s)} \neq 0 \).

(a) We show \( y P^{\rho K} \neq 0 \). Now, by the definition of \( K \), \( m - \gamma(s) \equiv (p - 1)p^{K} \mod p^{K+1} \). Hence, by the Cartan formula and 4:12(i), we can find \( q \) where \( q \equiv \alpha p^{K} \mod p^{K+1} \) \( (1 \leq \alpha \leq p - 1) \) such that \( y P^{q} \neq 0 \). By 4:6 and 4:12(i), we conclude

\[
y P^{\rho K} P^{q} = \beta y P^{q} \neq 0
\]

where \( \beta \in \mathbb{Z}_{p} \). Hence \( y P^{\rho K} \neq 0 \).

(b) We show \( y P^{\delta(m)} \neq 0 \). Let \( n = m - p^{K+1} + p^{K} \). By the induction hypothesis \( y P^{\rho K} P^{\delta(n)} \neq 0 \). Now \( \delta(m) = \delta(n) + p^{K} \) and \( \delta(n) \equiv 0 \mod p^{K} \).
For, since \( m \equiv \gamma(K) \mod p^{K+1} \) it follows, from 4:5, that \( m \equiv p^{K+1} + \gamma(K) \mod p^{K+2} \) and, thus, \( n \equiv \gamma(K + 1) \mod p^{K+2} \). From 4:6 and 4:12(i) we then deduce that

\[
y P^{\rho K} P^{\delta(n)} = \lambda y P^{\delta(n) + p^{K}} = \lambda y P^{\delta(m)}
\]

where \( \lambda \in \mathbb{Z}_{p} \). Hence \( y P^{\delta(m)} \neq 0 \). Q.E.D.

5. Proof of Theorem 1:1. In this section we will prove Theorem 1:1. We will prove it by increasing induction on the dimension. For \( m = 1 \) the theorem is true. Assume that \( Q(H^{2i}) \neq 0 \) only for binary \( i \) if \( i < m \). By the proofs given in the last section (which were also by induction on the dimension) we can assume 1:2 and 1:3 hold in dimensions less than 2m. Assume \( Q(H^{2m}) \neq 0 \) and \( m \) is not binary. We will produce a contradiction thereby showing these two conditions are incompatible.

Let \( k \) be the minimal \( s > 0 \) such that \( P^{p^{s}} \) acts nontrivially on \( P(H_{2m}) \).
Let \( n = m - p^{K+1} + p^{K} \). By the induction hypothesis \( n \) is binary. Although \( m \) is not binary we define \( \delta(m) = \delta(n) + p^{K} \). Let \( t \) be the maximal \( s > 0 \) such that \( m_{s} \neq 0 \) in the \( p \)-adic expansion \( \Sigma m_{s} p^{s} \) of \( m \).

Pick \( 0 \neq y \in P(H_{2m}) \). We will prove three propositions which, together, clearly produce the desired contradiction.

**Proposition 5:1.** \( y P = 0 \).

**Proposition 5:2.** \( \bigotimes_{i=1}^{p} y \in \ker P^{m-\gamma(s)} \) for \( s > 0 \) unless \( s = t \) and \( m - \gamma(t) = (p - 1)\delta(m) \). And, in that case \( \bigotimes_{i=1}^{p} y \in \ker P^{(p-1)\delta(m) + p^{K}} \).

**Proposition 5:3.** If \( \bigotimes_{i=1}^{p} y \in \bigcap_{0 < s < t} \ker P^{m-\gamma(s)} \) and \( \bigotimes_{i=1}^{p} y \in \ker P^{m-\gamma(t)} P^{\delta(m)} \) where \( m - \gamma(t) = (p - 1)\delta(m) \), then \( y P \neq 0 \).
Before proving these propositions we establish some technical results.

**Lemma 5.4.** \( P^q \) acts trivially on \( P(H_{2m}) \) unless \( m \equiv 0 \mod p^k \).

**Proof.** This follows from the definition of \( k \) and 4:6. We work by induction as in 4:8. Q.E.D.

Let \( m = \Sigma m_s p^s \) and \( n = \Sigma n_s p^s \) be the \( p \)-adic expansions of \( m \) and \( n \) respectively.

**Proposition 5.5.** \( m \equiv 2p^{k+1} + \gamma(k) \mod p^{k+2} \). Furthermore, for \( s \geq k + 2 \), \( m_s = n_s \).

**Proof.** It suffices to show \( n \equiv \gamma(k + 1) \mod p^{k+1} \). For then, in order for \( n \) to be binary and \( m \) not binary, 5:5 is the only possibility. Hence we can assume \( k \geq 1 \) since, by 1:3, \( n \equiv 1 \mod p \). We break our proof into two stages:

(a) We show \( \delta(n) \equiv 0 \mod p^{k-1} \). Pick \( 0 \neq y \in P(H_{2m}) \). Then, since \( m = n \equiv 1 \mod p \), it follows as in 4:11 that \( y^p = 0 \). By 4:3, \( \otimes_i y_i \notin \bigcap_{s \leq k} \ker P^{m-\gamma(s)} \). Hence, by 5:4 and the Cartan formula, there exists \( s \geq 1 \) such that \( m \equiv \gamma(s) \equiv 0 \mod p^k \). Hence \( n \equiv m \equiv \gamma(s) \mod p^k \) and \( \delta(n) \equiv 0 \mod p^{k-1} \).

(b) We show \( \rho(n) \equiv \gamma(k + 1) \). Pick \( y \in P(H_{2m}) \) such that \( y P^n \neq 0 \). By 1:3 \( y P^n P^\delta(n) \neq 0 \). Since \( \delta(n) \equiv 0 \mod p^{k-1} \) it follows, from 5:4 and 4:6, that

\[
\gamma P^n P^\delta(n) = \alpha y P^\delta(n) + p^k + \beta y P^\delta(n) + p^k \mod p^{k-1} \]

where \( \alpha, \beta \in Z_p \). We wish to eliminate the possibility that \( y P^\delta(n) + p^k \mod p^{k-1} \neq 0 \). First, \( y P^\delta(n) + p^k \mod p^{k-1} \neq 0 \) implies, by 5:4, that \( \delta(n) \equiv p^{k-1} \mod p^k \). Then, secondly, when we dualize, \( P^{p-1} \) acting nontrivially on \( Q(H^{2\delta(n) + 2\rho(n)}) \) implies, by 4:5, that \( \delta(n) \equiv p^{k-1} \mod p^{k+1} \). Thus \( n \equiv p^k + \gamma(s) \mod p^{k+2} \) where \( s < k \). But then, thirdly, \( n \) binary implies \( m \) binary which is not true.

Thus (\( \ast \)) reduces to

\[
\gamma P^n P^\delta(n) = \alpha y P^\delta(n) + p^k \neq 0.
\]

But \( P^\delta(n) + p^k \) acting nontrivially on \( Q(H^{2\delta(n) + 2\rho(n)}) \) implies \( \rho(n) > p^k \). Hence \( \rho(n) \geq \gamma(k + 1) \). Q.E.D.

(I) **Proof of Proposition 5.1.** Let \([ , ]\) be the Lie bracket product.

**Lemma 5.6.** If \( u, v \in H_\ast \) then \([u, v] P^q = \Sigma_{i+j=q} [u P^i, v P^j] \).

The proof of 5:6 is straightforward.

**Lemma 5.7.** If \( u \in P(H_{2i}), v \in P(H_{2j}), i, j < m \), then \([u, v] = 0\).
Proof. By 1:3, \( i \equiv j \equiv 1 \mod p \). Hence \( uP^1 = vP^1 = 0 \). By 5:6, \([u, v] P^1 = 0\). But \( u, v \) primitive implies that \([u, v] \in \mathcal{P}(H_{2i+2j})\). Since \( i + j \equiv 2 \mod p \) it follows by 4:4 that \([u, v] = 0\). Q.E.D.

Lemma 5:8. If \( u \in \mathcal{P}(H_{2i}), v \in \mathcal{P}(H_{2m}) \) and \( i < m \) then \([u, v] = 0\).

Proof. By contradiction. Pick the minimal \( i \) such that \([u, v] \neq 0\) where \( u \in \mathcal{P}(H_{2i}) \) and \( v \in \mathcal{P}(H_{2m}) \). Then \([u, v] \in \mathcal{P}(H_{2m+2i})\). But, by 5:6, 5:7, and our choice of \( i \), \([u, v] P^q = 0\) if \( q > 0 \). Hence, by 4:4, \([u, v] \neq 0\) implies \( m + i = \gamma(s) \) for some \( s \geq 1 \). But by 5:5 and the fact that \( i \) is binary this is impossible. Q.E.D.

We now prove 5:1. By 4:4 it suffices to prove \( y_P P^1 = 0 \) since \( y_P \in \mathcal{P}(H_{2pm}) \). And, by 5:8, \( y_P P^1 = P(y_P^1)y_{P^{-1}} = 0 \). Q.E.D.

(II) Proof of Proposition 5:2. We begin by seeing how \( P^q \) acts on \( y \in \mathcal{P}(H_{2m}) \).

Lemma 5:9. \( yP^q = 0 \) unless \( q \equiv 0 \mod p^{k+1} \).

Proof. By contradiction. We suppose that \( yP^q \neq 0 \) and that \( q \equiv 0 \mod p^{k+1} \) for \( q > 0 \).

(a) We show \( y_{P_p^{k+1}} \neq 0 \). By 5:5 and the fact that 1:1 is true in dimensions less than \( 2m \), we must have \( q \neq 0 \mod p^{k+2} \). By 4:6 and 5:4 we have

\[
y_P P^q = \alpha y_{P_p^{k+1}} P^{q-p^{k+1}} + \beta y_{P_p p^{k} p^{p}}
\]

where \( \alpha, \beta \in \mathbb{Z} \). But \( q - p^k \equiv (p - 1)p^k \mod p^{k+1} \). Therefore, by 5:5 and the fact that 1:1 is true in dimensions less than \( m \), \( y_{P_p q - p^k} = 0 \). Hence, \( y_P P_p^{k+1} P^{q-p^{k+1}} \neq 0 \).

(b) By 5:5 and the fact that 1:1 is true in dimensions less than \( 2m \), \( y_{P_p^{k+1}} \neq 0 \) produces an obvious contradiction unless \( p = 3 \). We now give an argument which shows there is a contradiction for \( p = 3 \) as well. Let \( l = m - 2 \cdot 3^k \). By 5:5, \( \delta(l) \equiv 0 \mod 3^{k+1} \) and \( \rho(l) = \gamma(k) < 3^{k+1} \). By 1:3, \( y_P 3^{k+1} \neq 0 \) implies \( y_P 3^{k+1} P_6(l) \neq 0 \). By an argument similar to that in (a)

\[
y_P \delta(l) + 3^{k+1} = \lambda y_{P_p 3^{k+1} \delta(l)} \neq 0
\]

where \( \lambda \in \mathbb{Z}_p \). Dualizing, we have \( P_6(l) + 3^{k+1} \) acting nontrivially on \( Q(H_{2\delta(l)} + 2^p(l)) \). Since \( \rho(l) < 3^{k+1} \) this is a contradiction. Q.E.D.

Lemma 5:10. If \( yP^q \neq 0 \) then \( q \equiv p^k \mod p^{k+2} \). Also \( q \) is binary and \( \delta(m) - q \) is binary. In particular, \( q \leq \delta(m) \).

Proof. The first statement follows from 5:5, 5:9 and the fact that 1:1 is true in dimensions less than \( 2m \). Regarding the second statement, we can deduce
from 4:6, 5:4 and the first statement that
\[ \gamma p^k p^{-q} p^k = \alpha y p^q \neq 0 \]
(\(\alpha \in \mathbb{Z}_p\)). Then, since \(p^q - p^k\) acts nontrivially on \(P(H_{2n})\), we can deduce, from 4:9 and 4:5, that \(q - p^k\) and \(\delta(n) - (q - p^k)\) are binary. Hence \(q\) and \(\delta(m) - q = \delta(n) + p^k - q = \delta(n) - (q - p^k)\) are binary. Q.E.D.

This is one more technical lemma we will have need of.

**Lemma 5:11.** For \(s < t, m - \gamma(s) > (p - 1)\delta(m)\).

**Proof.** Since \(m = n + (p - 1)p^k\) and \((p - 1)\delta(m) = (p - 1)(\delta(n) + p^k) = (p - 1)\delta(n) + (p - 1)p^k\), it suffices to show \(n - \gamma(s) > (p - 1)\delta(n)\). Now \(n = p\delta(n) + \rho(n)\). Hence \(n - (\delta(n) + \rho(n)) = (p - 1)\delta(n)\). Therefore it suffices to show \(\delta(n) + \rho(n) > \gamma(s)\) for \(s < t\). And this is obvious. Q.E.D.

We now prove 5:2. The first part of the proof consists of determining when \(\bigotimes_{i=1}^p y \in \ker \ Delta_{m-\gamma(s)}\). Given \(s\) it suffices to show \(\bigotimes_{i=1}^p y p^q i = 0\) whenever \(\Sigma_{i=1}^q i = m - \gamma(s)\). We consider \(s\) in four cases.

(i) \(0 < s < k\). Since \(\Sigma_{i=1}^q i = m - \gamma(s) \equiv 0 \mod p^k\) it follows by 5:4 that \(\bigotimes_{i=1}^p y \in \ker \ Delta_{m-\gamma(s)}\).

(ii) \(s = k, k + 1\). Since \(\Sigma_{i=1}^q i = m - \gamma(s) \equiv 2p^k + 1\) or \(p^k + 1 + (p - 1)p^k \mod p^{k+2}\) it follows from 5:10 that \(\bigotimes_{i=1}^p y \in \ker \ Delta_{m-\gamma(s)}\).

(iii) \(k + 1 \leq s < t\). Since \(\Sigma_{i=1}^q i = m - \gamma(s) \equiv (p - 1)p^k \mod p^{k+2}\) we must have, by 5:10, \(q_i = 0\) for some \(i\) and \(\Sigma_{i=1}^q i \leq (p - 1)\delta(m)\) if \(\bigotimes_{i=1}^p y \Delta_{m-\gamma(s)} \neq 0\). By 5:11 \(\bigotimes_{i=1}^p y \notin \ker \ Delta_{m-\gamma(s)}\).

(iv) \(s = t\). Suppose \(\bigotimes_{i=1}^p y \notin \ker \ Delta_{m-\gamma(t)}\). We will show \(m - \gamma(t) = (p - 1)\delta(m)\).

Let \(\Sigma q_i p^s\) and \(\Sigma b_i p^s\) be the \(p\)-adic expansion of \(m - \gamma(t)\) and \((p - 1)\delta(m)\) respectively. By arguing as in (iii) we see that \(q_i = 0\) for some \(i\). Also \(q_i\) and \(\delta(m) - q_i\) are binary for each \(i\). Since \(\Sigma q_i = m - \gamma(t)\) it follows that

\[ a_s \neq 0 \quad \text{only if } b_s \neq 0. \]  

But if \(\Sigma m_i p^s\) is the \(p\)-adic expansion of \(m\) it follows from the definition of \(\delta(m)\) that \(b_s \neq 0\) only if \(m_{s+1} \neq 0\). Hence

\[ a_s \neq 0 \quad \text{only if } m_{s+1} \neq 0. \]  

Let \(r\) be the minimum \(s \geq k + 2\) such that \(m_s = 0\). Then \(r < t\) since otherwise \(m - \gamma(t) = (p - 1)\delta(m) = (p - 1)p^k\) and we are done.

But it is easy to see

\[ a_s \neq 0 \quad \text{for } r \leq s < t. \]
It follows that \( m_s \neq 0 \) for \( r < s \leq t \). From this we deduce that
\[
m - \gamma(t) = (p - 1)\delta(m) = (p - 1)p^k + \sum_{r \leq s < t} (p - 1)p^s.
\]

The second and final part of the proof of 5:2 consists of showing that
\[
\bigotimes_{l=1}^{p} y \in \ker p^{\delta(m)} \text{ when } m - \gamma(t) = (p - 1)\delta(m).
\]
Let \( z = y p^{\delta(m)} \). Since the dimension of \( z \) is \( m - (p - 1)\delta(m) = \gamma(t) \) it follows from 1:2 that \( z^{P^i} = 0 \) for \( i > 0 \). Now, by 5:10,
\[
\left( \bigotimes_{l=1}^{p} y \right) p^{(p-1)\delta(m)} = \sum_{i=1}^{p} z \otimes z \otimes \cdots \otimes z \otimes y \otimes z \otimes \cdots \otimes z
\]
in the \( i \)th place.

Hence
\[
\left( \bigotimes_{l=1}^{p} y \right) p^{(p-1)\delta(m)} p^{\delta(m)} = p \left( \bigotimes_{l=1}^{p} z \right) = 0.
\]
Q.E.D.

(III) Proof of Proposition 5:3.

Lemma 5:12. \( Q(H^{2m}) = p^{\delta(m)}Q(H^{2\delta(n)+2p(n)}) \).

Proof. Pick \( 0 \neq y \in P(H_{2m}) \). By 4:4 there exists \( q > 0 \) such that \( y P^q \neq 0 \). By 5:10 \( q \equiv p^k \mod p^k + 1 \). By 4:6 and 5:4 \( y P^{p^k} P^q P^{-p^k} = \alpha_y P^q \neq 0 \). Hence \( y P^{p^k} \neq 0 \). By 1:3, \( y P^{p^k} P^{\delta(n)} \neq 0 \). By 5:5, \( \delta(n) \equiv 0 \mod p^k \). Again, using 4:6 and 5:4,
\[
y P^{\delta(m)} = y P^{\delta(n)} + p^k = \alpha_y P^{p^k} P^{\delta(n)} \neq 0.
\]
Q.E.D.

Lemma 5:13. \( \delta(n) + \rho(n) = m - (p - 1)\delta(m) = \gamma(t) \).

This follows from the identities \( m - \gamma(t) = (p - 1)\delta(m) \) and
\[
m = n + (p - 1)p^k = p\delta(n) + \rho(n) + (p - 1)p^k = \delta(n) + \rho(n) + (p - 1)\delta(m).
\]
Q.E.D.

From 4:1, 4:2 and the definition of \( t \) we can deduce the Adem relation
\[
Q_0 P^m P^{\delta(m)} = \sum_{0 \leq s < t} (-1)^s p^{m - \gamma(s)} Q_s P^{\delta(m)} + (-1)^t p^{m - \gamma(t)} P^{\delta(m)} Q_t.
\]

Our proof of 5:3 is a variation of that for 4:3. We use the notation of that proof. Expand \( y \) to a basis of \( P(H_{2m}) \) and pick \( x \in Q(H^{2m}) \) dual to \( y \). By 5:12 and 5:13 there exists \( z \in Q(H^{\gamma(t)}) \) such that \( x = P^{\delta(m)}(z) \). Now \( z \) is represented by \( z \in H^{\gamma(t)} \) such that \( \overline{\mu}(z) \in F_{\gamma(t)-1} \otimes F_{\gamma(t)-1} \). Let \( \phi \) be the unstable secondary operation corresponding to 5:14 where \( \theta = P^{\delta(m)} \), \( a_s = (-1)^s p^{m - \gamma(s)} \) and
$b_s = Q_s P_\delta(m)$ if $s < t$ while $a_t = (-1)^{\gamma} P_{m-\gamma(t)} P_\delta(m)$ and $b_t = Q_t$. Then $\phi$ is defined on $z$. The rest of the proof follows as in 4:3. There is one extra complication which arises however. Since $|\theta| = |P_\delta(m)| > 0$ we have to ensure that the difficulty discussed after 3:4 does not arise. That is, we have to show that $x \notin Q(F_{\gamma(t)-1})$. But, as was shown in the proof of 5:10, if $yP_q \neq 0$ then $yP_q = \alpha yP_\delta P_{n-q} = \alpha (\in Z_p)$. Thus $P_q$ acting on $y$ factors through $P(H_{2n})$. By 1:2 it then follows that $x \notin Q(F_{\gamma(t)-1})$. Q.E.D.

REFERENCES


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ALBERTA, EDMONTON, ALBERTA, CANADA T6G 2G1