Journal of the Institute of Polytechnics,
Osaka City University,
Vol. 10, No. 2, Series A

Cohomology mod p of symmetric products of spheres II

By Minoru NAKAOKA*

(Received April 22, 1959)

Introduction

In the previous paper [8] a method[1] to calculate the mod p cohomology of the m-fold symmetric product $\mathfrak{S}_m(K)$ of a finite simplicial complex K was explained, and the method was practiced to calculate the cohomology group $H^*(\mathfrak{S}_m(S^n); Z_p)$ in 'stable' range. In the present paper it will be shown that the use of the method is also successful practically in the determination of the 'entire' cohomology $H^*(\mathfrak{S}_m(S^n); Z_p)$.

Throughout this paper, a prime p and a positive integer n are fixed. We assume always that $n>1$ if $p=2$.

§1. Statement of the result

We denote by $\Omega(p, u)$ the set of all sequences

$$I = (i_1, \cdots, i_l) \qquad (l \geqq 0)$$

satisfying the following conditions:

(1) Each i_k is a positive integer $\equiv 0$ or $1 \bmod 2(p-1)$,

(2) $i_k \geqq p i_{k+1} \quad (1 \leqq k < l)$,

(3) $p i_1 < (p-1) D_n(I)$,

(4) $i_l \neq 1$,

where

$$D_n(I) = n + i_1 + \cdots + i_l .$$

We refer to $D_n(I)$ as the *n-degree* of I, and $l = l(I)$ as the *length* of I.

We define the *free commutative Z_p-algebra $U(p, n)$ on $\Omega(p, n)$* to be the Z_p-algebra which is generated by all elements $I \in \Omega(p, n)$ subject to the relations

$$IJ = (-1)^{D_n(I) D_n(J)} JI, \qquad I, J \in \Omega(p, n) .$$

The *monomial* of $U(p, n)$ is an element which is not zero and is of type:

$$\prod_{i=1}^{c} I_i^{e(i)} = I_1^{e(1)} \cdots I_c^{e(c)}, \qquad I_i \in \Omega(p, n) .^{2)}$$

---

* The author is supported by the National Science Foundation through The Institute for Advanced Study.

1) This is different from the method due to Steenrod [10] which uses the Cartan's computation for the homology of Eilenberg-MacLane complex.

2) For this to be not zero, it is necessary and sufficient that $e(i)=0$ or 1 whenever $pD_n(I_i)$ is odd.

The definition of n-degree is extended to any monomial $\theta=\prod_{i=1}^{c} I_i^{e(i)}$:

$$D_n(\theta) = \sum_{i=1}^{c} e(i)\, D_n(I_i)\,.$$

Define $U^q(p, n)$ to be the submodule generated in the module $\Omega(p, n)$ by all monomials θ such that $D_n(\theta)=q$. Then

$$U(p, n) = \sum_q U^q(p, n)$$

becomes a graded algebra.

REMARK. Let $\Omega_0(p, n)$ (resp. $\Omega_1(p, n)$) denote the totality of elements $I \in \Omega(p, n)$ such that $D_n(I)$ are even (resp. odd), and for any set X denote by $P(X)$ (resp. $E(X)$) the polynomial (resp. exterior) algebra on X with coefficients in Z_p. Then the algebra $U(p, n)$ is isomorphic as graded algebra with the tensor product $P(\Omega_0(p, n))\otimes E(\Omega_1(p, n))$ if $p>2$ and with $P(\Omega(p, n))$ if $p=2$.

We shall next define another gradation in $U(p, n)$, and make $U(p, n)$ a bigraded algebra:

$$U(p, n) = \sum_{q,r} U_r^q(p, n)\,.$$

This is done by assigning to each monimal θ a positive integer $R_p(\theta)$ defined as follows:

$$R_p(\theta) = \sum_{i=1}^{c} e(i) p^{l(I_i)}\,,$$

where $\theta=\prod_{i=1}^{c} I_i^{e(i)}$. $R_p(\theta)$ is called the *p-rank* of θ. Now $U_r^q(p, n)$ is the submodule generated in the module $U(p, n)$ by all monomials θ such that $D_n(\theta)=q$ and $R_p(\theta)=r$. We write

$$U_r(p, r) = \sum_q U_r^q(p, n)\,.$$

It should be noticed that $\sum_{r>m} U_r(p, n)$ is an ideal in $U(p, n)$ for any integer m.

For any complex K the Steenrod reduced power is denoted by

$$Sq^s : H^q(K; Z_2) \longrightarrow H^{q+s}(K; Z_2) \qquad (p=2)\,,$$
$$\mathcal{P}^s : H^q(K; Z_p) \longrightarrow H^{q+2s(p-1)}(K; Z_p) \qquad (p>2)\,,$$

and the Bockstein homomorphism by

$$\Delta : H^q(K; Z_p) \longrightarrow H^{q+1}(K; Z_p)\,.$$

With H. Cartan [2] we define for each sequence $I=(i_1, i_2, \cdots, i_l)$ satisfying (1) a homomorphism

$$St^I : H^q(K; Z_p) \longrightarrow H^{q+i_1+\cdots+i_l}(K; Z_p)$$

by

$$St^I = St^{i_1}\circ St^{i_2}\circ \cdots \circ St^{i_l}\,,$$

where $St^i = Sq^i$ if $p=2$, and $= \Delta^{\varepsilon}\mathcal{P}^s$ if $i=2s(p-1)+\varepsilon$ ($\varepsilon=0$ or 1) and $p>2$. If $l(I)=0$, St^I denotes the identity.

Suppose that there are given a complex K and a cohomology class $y \in H^n(K; Z_p)$. We may then have a homomorphism of algebra $T_y : U(p, n) \longrightarrow H^*(K; Z_p)$ such that

$$T_y\left(\prod_{i=1}^{c} I_i^{e(i)}\right) = \prod_{i=1}^{c} (St^{I_i} y)^{e(i)}, \tag{5}$$

because of the anti-commutativity of the cohomology algebra $H^*(K; Z_p)$. In the right side of (5), the product and the power are of course taken in the sense of the cup product. T_y is a homomorphism of graded algebra.

Now the mod p cohomology structure of the m-fold symmetric product $\mathfrak{S}_m(S^n)$ of an n-sphers S^n is given as follows:

MAIN THEOREM. *Let $u(m) \in H^n(\mathfrak{S}_m(S^n); Z_p) \approx Z_p$ be a generator. Then the homomorphism $T_{u(m)}: U(p, n) \longrightarrow H^*(\mathfrak{S}_m(S^n); Z_p)$ is onto, and its kernel is the ideal $\sum_{r>m} U_r(p, n)$.*

As a corollary we obtain the following which was proved in the previous paper [8]:

COROLLARY 1. *Let $q<n$ and $p^h \leq m < p^{h+1}$. Then a basis for the module $H^{n+q}(\mathfrak{S}_m(S^n); Z_p)$ can be formed with all elements $St^I(u(m))$, where I satisfies $l(I) \leq h$, $D_n(I) = n+q$ in addition to the conditions* (1), (2) *and* (4).

If we regard $\mathfrak{S}_{m-1}(S^n)$ as a subset of $\mathfrak{S}_m(S^n)$ canonically, the sequence

$$0 \longrightarrow H^*(\mathfrak{S}_m(S^n), \mathfrak{S}_{m-1}(S^n); Z_p) \xrightarrow{j^*_{m-1,m}} H^*(\mathfrak{S}_m(S^n); Z_p) \xrightarrow{i^*_{m-1,m}} H^*(\mathfrak{S}_{m-1}(S^n); Z_p) \longrightarrow 0$$

is exact, where $i^*_{m-1,m}$ and $j^*_{m-1,m}$ are the injection homomorphisms. (See [3], [7], [10].) Therefore the main theorem implies

COROLLARY 2. *The cohomology algebra $H^*(\mathfrak{S}_m(S^n), \mathfrak{S}_{m-1}(S^n); Z_p)$ is isomorphic with $U_m(p, n)$ regarded as an algebra by giving trivial multiplicative structure.*

If we notice that $H^{mn-q}(\mathfrak{S}_{m-1}(S^n); Z_p) = 0$ for $q<n$, we have furthermore

COROLLARY 3. *If $q<n$ then the homomorphism $T_{u(m)}$ restricted to $U_m^{mn-q}(p, n)$ is an isomorphism onto $H^{mn-q}(\mathfrak{S}_m(S^n); Z_p)$.*

§ 2. Reduction of the main theorem

In what follows we shall omit to write up the coefficient group Z_p, and use $H^*(K)$, $H^q(K)$ in places of $H^*(K; Z_p)$, $H^q(K; Z_p)$ respectively. Since we take only Z_p as coefficient group, no confusion will occur.

Let K, L be complexes and $f: L \longrightarrow K$ be a map. Consider the homomorphism

$f^*: H^*(K) \longrightarrow H^*(L)$ induced by f. Then, as a direct consequence of the naturality of cup product and St^I, we have

$$(1) \qquad f^* \circ T_y = T_z \quad \text{with} \quad z = f^*(y)$$

for any $y \in H^*(K)$.

Proof of the first part of Main Theorem

Recall first the following well-known facts:

2.1. The infinite symmetric product $\mathfrak{S}_\infty(S^n)$ of an n-sphere S^n is the Eilenberg-MacLane complex $\mathcal{K}(Z, n)$. (See [4], [5])

2.2. The homomorphism $T_{u(\infty)}: U(p, n) \longrightarrow H^*(\mathcal{K}(Z, n))$ is onto[3], where $u(\infty) \in H^n(\mathcal{K}(Z, n))$ is the fundametal class. (See [2], [8])

2.3. The homomorphism $i^*_{m,\infty}: H^*(\mathfrak{S}_\infty(S^n)) \longrightarrow H^*(\mathfrak{S}_m(S^n))$ induced by the natural inclusion $i_{m,\infty}$; $\mathfrak{S}_m(S^n) \subset \mathfrak{S}_\infty(S^n)$ is onto[4]. (See [8])

Let $u(m) = i^*_{m,\infty}(u(\infty))$. Then we have $T_{u(m)} = i^*_{m,\infty} \circ T_{u(\infty)}$ by virtue of (1) and 2.1. Therefore it follows from 2.2 and 2.3 that $T_{u(m)}$ is onto. However $u(m)$ is a generator of $H^n(\mathfrak{S}_m(S^n))$. (See [8]) This completes the proof.

Let $\mathfrak{S}_{m,p}$ denote a p-Sylow subgroup of the symmetric group $\mathfrak{S}_m$ of degree m, and $\mathfrak{S}_{m,p}(S^n)$ the orbit space over the m-fold cartesian product $S^n \times S^n \times \cdots \times S^n$ relative to $\mathfrak{S}_{m,p}$ operating naturally on it. Let $\rho_m: \mathfrak{S}_{m,p}(S^n) \longrightarrow \mathfrak{S}_m(S^n)$ be the natural projection, and put

$$(2) \qquad v(m) = \rho^*_m(u(m)) \in H^n(\mathfrak{S}_{m,p}(S^n)),$$

where $\rho^*_m: H^*(\mathfrak{S}_m(S^n)) \longrightarrow H^*(\mathfrak{S}_{m,p}(S^n))$ is the homomorphism induced by ρ_m.

Denote by A_r the set of all monomials $\theta \in U_r(p, n)$. A_r is a basis for the module $U_r(p, n)$.

THEOREM 1. *$T_{v(m)}(\theta) = 0$ if $\theta \in A_r$ and $r > m$. The elements $T_{v(m)}(\theta)$, $\theta \in A_m$, are linearly independent.*

The second part of the main theorem will be obtained as a corollary of this theorem which will be proved in §7 after making many preliminaries. We show here that Theorem 1 implies the second part of the main theorem.

It follows from (1) and (2) that $\rho^*_m \circ T_{u(m)} = T_{v(m)}$. However, as is shown in [8], the homomorphism ρ^*_m is a monomorphism. Therefore if we assume Theorem 1 we have

2.4. $T_{u(m)}(\theta) = 0$ if $\theta \in A_r$ and $r > m$. The elements $T_{u(m)}(\theta)$, $\theta \in A_m$, are linearly independent.

On the other hand, the set of elements $\theta \in A_r$, $r \geqq 0$, is a basis for the module $U(p, n)$, so that it is sufficient for our purpose to show

3) It is known [2] that $T_{u(\infty)}$ is also a monomorphism, but we do not need this fact. Rather that is a consequence of our final result.

4) This is valid for any complex.

2.5. $T_{u(m)}(\theta)=0$ if $\theta \in A_r$ and $r>m$. The elements $T_{u(m)}(\theta)$, $\theta \in A_r$ with $r \leqq m$, are linearly independent.

Thus it remains to prove that 2.4 implies 2.5. To do this, we assume inductively that the elements $T_{n(m-1)}(\theta)$, $\theta \in A_r$ with $r \leqq m-1$, are linearly independent, and prove that an equation

$$(3) \qquad \sum_{\theta \in A_r, r \leqq m} \alpha_\theta T_{u(m)}(\theta) = 0 \qquad (\alpha \in Z_p)$$

yields $\alpha_\theta=0$ for every θ.

Consider the homomorphism $i^*_{m-1,m}: H^*(\mathfrak{S}_m(S^n)) \longrightarrow H^*(\mathfrak{S}_{m-1}(S^n))$. Then $i^*_{m-1,m} \circ T_{u(m)} = T_{u(m-1)}$ in view of (1). Therefore if we apply to (3) the homomorphism $i^*_{m-1,m}$ and use the first part of 2.4, we obtain

$$\sum_{\theta \in A_r, r \leqq m-1} \alpha_\theta T_{u(m-1)}(\theta) = 0 .$$

By the hypothesis of induction this implies $\alpha_\theta=0$ for every $\theta \in A_r$ ($r \leqq m-1$). Consequently (3) becomes

$$\sum_{\theta \in A_m} \alpha_\theta T_{u(m)}(\theta) = 0 ,$$

so that α_θ must be 0 for also every $\theta \in A_m$ according to the second part of 2.4. Thus we have $\alpha_\theta=0$ for every $\theta \in A_r$ ($r \leqq m$), and the proof is complete.

To conclude this section, we remark that Theorem 1 is considered as a problem on the p-fold cyclic product. In fact, as is shown in [8], $\mathfrak{S}_{m,p}(S^n)$ is homomorphic with the product:

$$\prod_{r=0}^{h} (\mathfrak{Z}_p^r(S^n))^{a(r)}$$

if the p-adic expansion of m is $\sum_{r=0}^{h} a(r)p^r$, where the product and the power are of the cartesian product, and $\mathfrak{Z}_p^r(S^n)$ is the r-times iterated p-fold cyclic product of S^n.[4] We shall use in full the results on the mod p cohomology of the p-fold cyclic product to prove Theorem 1.

§3. Cohomology of cyclic products

For convenience of the reader, we shall in this section recall from [6] the results on the mod p cohomology of the p-fold cyclic product $\mathfrak{Z}_p(K)$ of a complex. We assume that K is a connected finite simplicial complex.

Let the homomorphisms $\phi_0^*: H^q(K^p) \longrightarrow H^q(\mathfrak{Z}_p(K), \mathfrak{d}_p(K))$ and $E_m: H^q(K) \longrightarrow H^{q+m}(\mathfrak{Z}_p(K), \mathfrak{d}_p(K))$ ($m \geqq 1$) denote the same as in [6], where K^p is the p-fold cartesian product of K and $\mathfrak{d}_p(K)$ is the diagonal of $\mathfrak{Z}_p(K)$. These homomorphisms followed by the injection homomorphism $j^*: H^*(\mathfrak{Z}_p(K), \mathfrak{d}_p(K)) \longrightarrow H^*(\mathfrak{Z}_p(K))$ will be denoted by

$$\phi^*: H^q(K^p) \longrightarrow H^q(\mathfrak{Z}_p(K))$$

and

$$\Phi_m : H^q(K) \longrightarrow H^{q+m}(\mathfrak{Z}_p(K)), \qquad (m \geqq 1)$$

respectively. In the description of the cohomology $H^*(\mathfrak{Z}_p(K))$ in terms of the cohomology $H^*(K)$, ϕ^* and Φ_m are fundamental, as the properties 3.1–3.5 below show. It is convenient for the present purpose to define Φ_m for $m=0$ by

$$\Phi_0(y) = -\phi^*(y \times 1 \times \cdots \times 1) \qquad y \in H^*(K),$$

where 1 is the unit cohomology class and $\times$ stands for the cross product. For the proof of 3.1–3.5, see §§11–12 of [6].

3.1. Let $\{z_i\}$ be a basis for the module $H^*(K)$. Then $H^*(\mathfrak{Z}_p(K))$ is the module having as generators all elements of types: 1, $\Phi_m(z_i)$ with $2 \leqq m \leqq (p-1) \dim z_i$, $\phi^*(z_{i_1} \times \cdots \times z_{i_p})$ where $i_j \neq i_k$ for some j, k; and as relations the following: $\Phi_1(z_i)=0$, $\phi^*(z_{i_1} \times z_{i_2} \times \cdots \times z_{i_p}) = (-1)^{q_1(d-1)} \phi^*(z_{i_2} \times \cdots \times z_{i_p} \times z_{i_1})$, where $q_j = \dim z_{i_j}$ and $d = \sum_{j=1}^{k} q_j$.

3.2. $$Sq^s \circ \Phi_m = \sum_{k=0}^{s} \binom{m-1}{k} \Phi_{m+k} \circ Sq^{s-k} \qquad (p=2),$$

$$\mathcal{P}^s \circ \Phi_m = \sum_{.=0}^{s} \binom{t+\eta-1}{k} \Phi_{2k(p-1)+m} \circ \mathcal{P}^{s-k}$$
$$(p>2,\ m=2t+\eta \text{ with } \eta=0 \text{ or } 1),$$

$$\Delta \circ \Phi_m = (-1)^m \Phi_m \circ \Delta + (1+(-1)^m)/2\, \Phi_{m+1},$$

where $m \geqq 0$ and ( ) denotes the binomial coefficient. (See Appendix)

3.3. $$Sq^s \circ \phi^*(y_1 \times y_2) = \phi^* \circ Sq^s(y_1 \times y_2) + \sum_{k=1}^{s} \Phi_k \circ Sq^{s-k}(y_1 y_2)$$

$$\mathcal{P}^s \circ \phi^*(y_1 \times \cdots \times y_p) = \phi^* \circ \mathcal{P}^s(y_1 \times \cdots \times y_p)$$
$$+ \sum_{k=1}^{s} (-1)^{k+1} \Phi_{2k(p-1)} \circ \mathcal{P}^{s-k}(y_1 \cdots y_p) \qquad (p>2),$$

$$\Delta \circ \phi^* = \phi^* \circ \Delta,$$

where $y, y_i \in H^*(K)$ and $y_1 y_2 \cdots y_p$ denotes the cup product of y_i's.

3.4. Let $x, y, x_i, y_i \in H^*(K)$ and $l, m \geqq 1$. Then the cup products $\Phi_l(x) \cdot \Phi_m(y)$ and $\Phi_l(x) \cdot \phi^*(y_1 \times \cdots \times y_p)$ are trivial.

3.5. Let $q_i = \dim y_i$ and put $d(i) = (q_1 + \cdots + q_p)(q_1 + \cdots + q_{i-1})$. Then we have

$$\phi^*(x_1 \times \cdots \times x_p) \cdot \phi^*(y_1 \times \cdots \times y_p)$$
$$= \sum_{i=1}^{p} (-1)^{d(i)} \phi^*((x_1 \times \cdots \times x_p) \cdot (y_i \times \cdots \times y_{i-1})).$$

3.6. (Theorem of Bott-Thom) Let $y \in H^q(K)$, then $\phi^*(y \times \cdots \times y)$

$$= \sum_{k=0}^{q=1} \Phi_{q-k} \circ Sq^k(y) \qquad \text{if } p=2, \text{ and}$$
$$= \alpha \sum_{0 \leqq k < q/2} (-1)^k \Phi_{(p-1)(q-2k)} \circ \mathcal{P}^k(y) \text{ with } 0 \neq \alpha \in Z_p \text{ if } p>2.$$

3.7. (Theorem of Wu) Let $y \in H^q(K)$ and $j \geqq 1$, then $\Phi_{(p-1)q+j}(y)$

$$= \sum_{k=1}^{q} \Phi_{q-k+j} \circ Sq^k(y) \qquad \text{if } p=2, \text{ and}$$
$$= \sum_{(k,\varepsilon)} (-1)^{k+1} \Phi_{(p-1)(q-2k)+j-\varepsilon} \circ \Delta^{\varepsilon} \circ \mathcal{P}^k(y) \quad \text{with } \varepsilon=0 \text{ or } 1 \text{ if } p>2,$$

where the sum is taken over all pairs (k, ε) such that $1 \leqq 2k(p-1)+\varepsilon \leqq (p-1)q$.

§4. Auxiliary propositions on $H^*(\mathfrak{Z}_p(K))$

We prove in this section some propositions on $H^*(\mathfrak{Z}_p(K))$ which are needed later. The proofs will depend only on 3.1–3.7.

PROPOSITION 1. *We may replace in 3.1 the generators by all elements of type*: 1, $\Phi_m(z_i)$ *with* $2 \leqq m < (p-1) \dim z_i$, $\phi^*(z_{i_1} \times \cdots \times z_{i_p})$ *with dimension* >0. *Here we assume* $H^1(K)=0$ *if* $p=2$.

PROOF. Immediate from 3.1 and 3.6.

Given a submodule G of $H^*(K)$, denote by $\Phi(G)$ the submodule generated in the module $H^*(\mathfrak{Z}_p(K))$ by all elements $\Phi_m(y)$ for which $y \in G$ and $m \geqq 0$.

LEMMA 1. *Assume that every element of a submodule* $G \subset H^*(K)$ *is of positive dimension, and let* $\{x_i\}$ *be a basis for* G. *Then a basis for the module* $\Phi(G)$ *can be formed with all elements* $\Phi_m(x_i)$ *for which* $0 \leqq m \leqq (p-1) \dim x_i$ *and* $m \neq 1$.

PROOF. For any element $y \in H^*(K)$ and any $l \geqq 0$, $\Phi_l(y)$ can be represented as a linear combination of elements with type $\Phi_m(z)$, where $z \in H^*(K)$, $0 \leqq m \leqq (p-1) \dim z$ and $m \neq 1$. This is easily seen from the fact $\Phi_1=0$ and 3.7 by induction on $l-(p-1) \dim y$. Therefore the elements described in Lemma 1 generate $\Phi(G)$. It is obvious from 3.1 that these are linearly independent.

PROPOSITION 2. *If* $\sum_{i=1}^{c} e(i) \geqq 2$ *then*

$$\prod_{i=1}^{c} (St^{I_i} \circ \Phi_0(y))^{e(i)} = \prod_{i=1}^{c} (\Phi_0 \circ St^{I_i}(y))^{e(i)}$$

for any $y \in H^*(K)$ *and any* I_i, *where the product and the power are of the cup product.*

PROOF. Let $\Phi'(G)$ denote the submodule obtained if in the definition of $\Phi(G)$ the condition $m \geqq 0$ is replaced by $m>0$. Then we have

$$St^I \circ \Phi_0(y) - \Phi_0 \circ St^I(y) \subset \Phi'(H^*(K)) .$$

In fact, this is obvious by 3.2 if the length $l(I)=1$. Since 3.2 implies also that $\Phi'(H^*(K))$ is closed under the operations St^i, the above assertion for general I is easily proved by induction on $l(I)$. Therefore for each i we have

$$St^{I_i} \circ \Phi_0(y) = \Phi_0 \circ St^{I_i}(y) + w_i , \qquad w_i \in \Phi'(H^*(K)) .$$

On the other hand

$$(\Phi_0 \circ St^{I_i}(y)) \cdot w_k = 0 , \qquad w_i \cdot w_k = 0$$

by 3.4. Thus we obtain the proposition.

Given integers $e, r\geqq 0$, we denote by $\pi^r(e)$ the set of all sequences $E=(e(1), \cdots, e(r))$ of *non-negative* integers whose sum is e. The set of all elements $E=(e(1), \cdots, e(r))\in\pi^r(e)$ for which $e(1)=\cdots=e(r)$ do not hold, will be denoted by $\pi_0^r(e)$. Any two elements $E, E'\in\pi_0^r(e)$ are defined to be equivalent if and only if the one is obtained from the other by a cyclic permutation of terms. We shall denote by $\bar{\pi}_0^r(e)$ an arbitrary but fixed system of representatives in $\pi_0^r(e)$ for the set of the equivalence classes. Consequently $\bar{\pi}_0^r(e)\subset\pi_0^r(e)\subset\pi^r(e)$.

Given a sequence $E=(e(1), \cdots, e(r))$ of integers $(r\geqq 2)$, we shall denote the *polynomial coefficient* by $P(E)=P(e(1), \cdots, e(r))$ (see Appendix for the definition).

PROPOSITION 3. *Let $y\in H^q(K)$ then the following formula holds for any $e\geqq 1$ if pq is even, and for $e=1$ if pq is odd:*

$$(-\Phi_0(y))^e=\sum_E P(E)\phi^*(y^{e(1)}\times\cdots\times y^{e(p)})$$
$$+P(e/p-1, e/p, \cdots, e/p)\phi^*(y^{e/p}\times\cdots\times y^{e/p}),$$

where $E=(e(1), \cdots, e(p))$ runs over $\bar{\pi}_0^p(e)$, and it is understood that the last term is 0 if e is not a multiple of p.

PROOF. Since the assertion for odd pq is trivial, we assume pq is even, i.e. q is even if $p>2$ and is any if $p=2$. By 3.5 and the 'polynomial theorem' we have

$$(-\Phi_0(y))^e=(\phi^*(y\times 1\times\cdots\times 1))^e$$
$$=\phi^*((y\times 1\times\cdots\times 1)(y\times 1\times\cdots 1+\cdots+1\times 1\times\cdots\times y)^{e-1})$$
$$=\phi^*((y\times 1\times\cdots\times 1)(\sum_I P(I)y^{i(1)}\times\cdots\times y^{i(p)})$$
$$=\sum_I P(I)\phi^*(y^{i(1)+1}\times\cdots\times y^{i(p)})$$

where $I=(i(1), \cdots, i(p))$ runs over $\pi^p(e-1)$. Since $P(I)=P(i(1), \cdots, i(p))=0$ if some $i(k)<0$ (cf. Appendix), the above expression is equal to

$$\sum_K P(k(1)-1, k(2), \cdots, k(p))\phi^*(y^{k(1)}\times y^{k(2)}\times\cdots\times y^{k(p)})$$
$$+P(e/p-1, e/p, \cdots, e/p)\phi^*(y^{e/p}\times y^{e/p}\times\cdots\times y^{e/p})$$

where $K=(k(1), \cdots, k(p))$ runs over $\pi_0^p(e)$. However, by the relation in 3.1 and Lemma 1 in Appendix, the sum $\sum_K$ is equal to

$$\sum_E\sum_{i=1}^p P(e(1), \cdots, e(i)-1, \cdots, e(p))\phi^*(y^{e(1)}\times\cdots\times y^{e(p)})$$
$$=\sum_E P(E)\phi^*(y^{e(1)}\times\cdots\times y^{e(p)})$$

where $E=(e(1), \cdots, e(p))$ runs over $\bar{\pi}_0^p(e)$. This completes the proof.

PROPOSITION 4. *Let $y_i\in H^{q_i}(K)$, and assume that $e(i)=1$ if pq_i is odd. Then for $c\geqq 2$ we have*

$$\prod_{i=1}^{c} (\phi_0(y_i))^{e(i)}$$
$$= \sum (\pm \prod_{i=1}^{c} P(E_i))\phi^*((\prod_{i=1}^{c} y_i^{e(i,1)})\times \cdots \times(\prod_{i=1}^{c} y_i^{e(i,p)}))$$

where the sum is taken over all sequences $(E_1, \cdots, E_c)$ *such that* $E_1=(e(1,1), \cdots, e(1,p))\in\bar{\pi}_0^p(e(1))$ *and* $E_i=(e(i,1), \cdots, e(i,p))\in\pi_0^p(e(i))$ *for* $i=2, \cdots, c$.

PROOF. Let x_i, $x\in H^*(K)$, and assume that $p(\dim x)$ is even. Then 3.5 implies

$$\begin{aligned}&\phi^*(x_1\times \cdots \times x_p)\cdot\phi^*(x\times \cdots \times x)\\ &= \phi^*((x_1\times \cdots \times x_p)\cdot p(x\times \cdots \times x))\\ &= 0.\end{aligned}$$

In view of this fact, it follows from Proposition 3 that

$$\begin{aligned}&\prod_{i=1}^{c} (\Phi_0(y_i))^{e(i)}\\ &= \prod_{i=1}^{c} ((-1)^{e(i)} \sum_{E_i} P(E_i)\,\phi^*(y_i^{e(i,1)}\times \cdots \times y_i^{e(i,p)}))\\ &= \pm \sum (\prod_{i=1}^{c} P(E_i))(\prod_{i=1}^{c} \phi^*(y_i^{e(i,1)}\times \cdots \times y_i^{e(i,p)}))\end{aligned}$$

where the sum is taken over all sequences $(E_1, \cdots, E_c)$ such that $E_i\in\bar{\pi}_0^p(e(i))$ for $i=1, \cdots, c$. Now the proposition follows from 3.5 and the definitions of $\pi_0^p(e(i)$ and $\bar{\pi}_0^p(e(i))$.

§5. The submodule $H_0^*(\mathfrak{Z}_p^r(S^n))$

For any integer $r\geq 1$, write

$$\pi^r = \bigcup_{i\geqq 0} \pi^r(i).$$

Denote by e^n a fixed generator of $H^n(S^n)$. Given $M=(m_1, \cdots, m_r)\in\pi^r$, we shall define an element $[M]=[m_1, \cdots, m_r]\in H^*(\mathfrak{Z}_p^r(S^n))$ by

$$[M] = \Phi_{m_1}\circ\Phi_{m_2}\circ \cdots \circ\Phi_{m_r}(e^n),$$

where $\Phi_{m_i}: H^*(\mathfrak{Z}_p^{r-i}(S^n)) \longrightarrow H^*(\mathfrak{Z}_p(\mathfrak{Z}_p^{r-i}(S^n)))=H^*(\mathfrak{Z}_p^{r-i+1}(S^n))$ is the homomorphism defined in §3. The dimension of $[M]$ is $D_n(M)=n+m_1+ \cdots +m_r$.

The following lemma is a direct consequence of 3.1.

LEMMA 2. $H^q(\mathfrak{Z}_p^r(S^n))=0$ *for* $0<q<n$, *and* $H^n(\mathfrak{Z}_p^r(S^n))$ *is a cyclic group of order* p *generated by* $[0_r]=[0, 0, \cdots, 0]$.

Define $H_0^*(\mathfrak{Z}_p^r(S^n))$ to be the submodule generated in the module $H^*(\mathfrak{Z}_p^r(S^n))$ by all elements $[M]$ for which $M\in\pi^r$. The purpose of this section is to study the structure of the module $H_0^*(\mathfrak{Z}_p^r(S^n))$.

Let B_0^r denote a set consisting of all elements $[m_1, \cdots, m_r]\in H^*(\mathfrak{Z}_p^r(S^n))$ such that

$$pm_k \leqq (p-1)(n+m_k+ \cdots +m_r) \text{ and } m_k\neq 1 \qquad (k=1,2, \cdots, r).$$

Then we have

PROPOSITION 5. *Set B_0^r is a basis for the module $H_0^*(\mathfrak{Z}_p^r(S^n))$.*

PROOF. Using the notation in §4, $H_0^*(\mathfrak{Z}_p^r(S^n))=\Phi(H_0^*(\mathfrak{Z}_p^{r-1}(S^n))$. Therefore the proposition follows from Lemma 1 by induction on r.

Order the set π^r by the lexicographic order from the left, i.e. for any two elements $M=(m_1, \cdots, m_r)$, $N=(n_1, \cdots, n_r)\in\pi^r$, write $M<N$ if and only if $m_1=n_1$, $\cdots$, $m_{k-1}=n_{k-1}$ and $m_k<n_k$ for some k.

LEMMA 3. *Let $N\in\pi^r$ and let*

$$[N]=\sum_M a_M[M], \quad a_M\in Z_p, \ [M]\in B_0^r.$$

Then $a_M\neq 0$ implies $M\leqq N$.

PROOF. Since the lemma is trivial if $r=1$, we proceed by induction on r. Let $N=(n_1, \cdots, n_r)$ and put $N'=(n_2, \cdots, n_r)$. Then

$$[N']=\sum_L b_L[L], \quad b_L\in Z_p, \ [L]\in B_0^{r-1}.$$

Applying Φ_{n_1} to this equation, we have $[N]=\sum_L b_L\Phi_{n_1}[L]$. Let

$$\Phi_{n_1}[L]=\sum_M c_{L,M}[M], \quad c_{L,M}\in Z_p, \ [M]\in B_0^r.$$

Then we obtain $\sum_M a_M[M]=\sum_L\sum_M b_L c_{L,M}[M]$, hence $a_M=\sum_L b_L c_{L,M}$. Therefore if $a_M\neq 0$ then there is an element L such that $b_L\neq 0$ and $c_{L,M}\neq 0$. Take such an L and put $L=(l_2, \cdots, l_r)$.

Case 1: $n_1\leqq(p-1)D_n(L)$.
Since $\Phi_{n_1}[L]=[n, l_2, \cdots, l_r]\in B$, $c_{L,M}\neq 0$ implies $M=(n, l_2, \cdots, l_r)$. Since $b_L\neq 0$ we have $L\leqq N'$ by the hypothesis of induction. Therefore $M=(n_1, l_2, \cdots, l_r)\leqq(n_1, n_2, \cdots, n_l)=N$.

Case 2: $n_1>(p-1)D_n(L)$.
Since $D_n(N)=D_n(M)$, $D_n(N')=D_n(L)$ and $D_n(N)=n_1+D_n(N')$, we have $D_n(M)=n_1+D_n(L)$. On the other hand $pm_1\leqq(p-1)D_n(M)$ because of $[M]\in B_0^r$. Therefore we obtain $pm_1\leqq(p-1)(n_1+D_n(L))=(p-1)n_1+(p-1)D_n(L)<pn_1$, hence $m_1<n_1$. This shows $M<N$, and completes the proof.

The following formulas can be obtained from 3.2 by induction on r. The calculations are straightforward, and are left to the reader.

5.1. $$Sq^s[m_1, \cdots, m_r]$$
$$=\sum_S\binom{m_1-1}{s_1}\cdots\binom{m_r-1}{s_r}[m_1+s_1, \cdots, m_r+s_r] \quad (p=2),$$
$$\mathcal{P}^s[m_1, \cdots, m_r]$$
$$=\sum_S\binom{t_1+\eta_1-1}{s_1}\cdots\binom{t_r+\eta_r-1}{s_r}[m_1+2s_1(p-1), \cdots, m_r+2s_r(p-1)] \quad (p>2),$$

$$\begin{aligned}&\Delta[m_1, \cdots, m_r]\\ &=\sum_{i=1}^{r}((-1)^{m(i-1)}+(-1)^{m(i)})/2[m_1, \cdots, m_i+1, \cdots, m_r],\end{aligned}$$

where $S=(s_1, \cdots, s_r)$ runs over the set $\pi^r(s)$, $m_i=2t_i+\eta_i$ with $\eta_i=0$ or 1, and $m(i)=m_1+\cdots+m_i$.

A direct consequence is:

5.2. $St^I[M]\in H_0^*(\mathfrak{Z}_p^*(S^n))$ for $M\in\pi^r$.

A sequence $I=(i_1, \cdots, i_l)$ satisfying the conditions (1) and (2) in §1 is called to be *admissible*.

Proposition 6. *Let I be an admissible sequence such that $l(I)>r$. Then we have $St^I[O_r]=0$.*

Proof. Let $I=(i_1, \cdots, i_l)$ and put $d=i_1+\cdots+i_l$.

Case 1: $d<n$.
The proposition is Theorem 3 of [8].

Case 2: $d\geqq n$.

Take an integer n' such that $d<n'$. For any $M\in\pi^r$ define $[M]'\in H^*(\mathfrak{Z}_p^s(S^{n'}))$ as the analogy of the element $[M]\in H^*(\mathfrak{Z}_p^s(S^n))$, and $B_0'^r$ the analogy of B_0^r. Then all the elements $[M]'=[m_1, \cdots, m_r]'$ such that $m_1+\cdots+m_r=d$ and $m_i\neq 1$ for each i are contained in $B_0'^r$ because $m_1+\cdots+m_r<n'$ implies $pm_i<(p-1)(n'+m_i+\cdots+m_r)$ for each i. Therefore there is a homomorphism $\sigma_{n',n}^d: H_0^{n'+d}(\mathfrak{Z}_p^s(S^{n'}))\longrightarrow H_0^{n+d}(\mathfrak{Z}_p^s(S^n))$ such that

$$\sigma_{n',n}^d([M]')=[M] \qquad \text{for} \quad M\in\pi^r.$$

It follows from 5.1 that

$$\sigma_{n',n}^d\circ St^I[O_r]'=St^I[O_r].$$

However by the fact in Case 1 we have $St^I[O_r]'=0$. These prove $St^I[O_r]=0$ and we complete the proof.

Since it is easily seen that $pi_k<(p-1)(n+i_k+\cdots+i_r)$ is equivalent with $(i_k-pi_{k+1})+\cdots+(i_{r-1}-pi_r)+i_r<(p-1)n$, the definition of $\Omega(p, n)$ implies

5.3. If $I=(i_1, \cdots, i_r)\in\Omega(p, n)$, then $pi_k<(p-1)(n+i_k\cdots+i_r)$ for any k; hence $I\in B_0^r$.

Lemma 4. *Let I be an admissible sequence with $l(I)=r$, and*

$$St^I[O_r]=\sum_M a_M[M], \qquad a_M\in Z_p,\ [M]\in B_0^r.$$

(See 5.2) Then $a_M\neq 0$ implies $M\leqq I$; if $I\in\Omega(p, n)$ then $a_I\neq 0$. (See 5.3)

Proof. We retain the usage of the notations in the proof of the above proposition.

Case 1: $d<n$.

The lemma is Proposition 8 of [8].

Case 2: $d\geqq n$.

Take an integer n' such that $d<n'$, and let

$$St^I[O_r]'=\sum_N b_N[N]', \qquad b_N\in Z_p,\ [N]'\in B_0'^r.$$

Applying $o^d_{n',n}$ to this equation, we obtain

$$St^I[O_r]=\sum_N b_N[N]$$

so that

$$\sum_M a_M[M]=\sum_N b_N[N].$$

Let

$$[N]=\sum_M c_{N,M}[M], \qquad c_{N,M}\in Z_p,\ [M]\in B_0^r.$$

Then $a_M=\sum_N b_N c_{n,m}$. Therefore if $a_M\neq 0$, there is an $[N']\in B_0'^r$ such that $b_N\neq 0$ and $c_{N,M}\neq 0$. Take such an N, then $b_N\neq 0$ implies $N\leqq I$ in view of the result in Case 1, and $c_{N,M}\neq 0$ implies $M\leqq N$ in view of Lemma 3. This proves $M\leqq I$

Assume $I\in\Omega(p,n)$. Then $[I]\in B_0^r$ by 5.3, and $a_I=\sum_N b_N c_{N,I}$. Therefore the above arguments show that $a_I=b_I$. However $b_I\neq 0$ by the fact in Case 1, so that $a_I\neq 0$. Thus the proof has been finished.

Denote by B_{01}^r (resp. B_{02}^r) the set of all $M=(m_1,\cdots,m_r)\in B_0^r$ such that $pm_1<(p-1)D_n(M)$ (resp. $pm_1=(p-1)D_n(M)$).

LEMMA 5. *Let $M=(m_1,\cdots,m_r)\in B_{02}^r$ and put $M'=(m_2,\cdots,m_r)$. Then $M'\in B_0^{r-1}$ and*

$$[M]=\beta\phi^*([M']\times\cdots\times[M'])-\sum_N a_N[N],$$

where $0\neq\beta\in Z_p$, $a_N\in Z_p$, $[N]\in B_{01}^r$ and $N<M$.

PROOF. It is clear that $M'\in B_0^{r-1}$. Put $q=\dim[M']=D_n(M')$. Then it follows from 3.6 that

$$\begin{aligned}&\phi^*([M']\times\cdots\times[M'])\\ &=\Phi_q[M']+\sum_{k=1}^{p-1}\Phi_{q-k}\circ Sq^k[M'] \qquad (p=2),\\ &=\alpha(\Phi_{(p-1)q}[M']+\sum_{1\leqq k<q/2}(-1)^k\Phi_{(p-1)(q-2k)}\circ\mathcal{P}^k[M'])\\ &\qquad\qquad \textit{with}\quad 0\neq\alpha\in Z_p \qquad (p>2).\end{aligned}$$

Since $(p-1)q=(p-1)D_n(M')=m_1$, this implies

$$\begin{aligned}[M]&=\phi^*([M']\times[M'])-\sum_{k=1}^{p-1}\Phi_{q-k}\circ Sq^k[M'] \qquad (p=2)\\ &=\alpha^{-1}\phi^*([M']\times\cdots\times[M'])-\sum_{1\leqq k<q/2}(-1)^k\Phi_{(p-1)(q-2k)}\circ\mathcal{P}^k[M']\\ &\qquad\qquad (p>2).\end{aligned}$$

In view of 5.2, $Sq^k[M']$ and $\mathcal{P}^k[M']$ are in $H_0^*(\mathfrak{Z}_p^{r-1}(S^n))$, so that they may be written as $\sum_L b_{k,L}[L]$ for which $b_{k,L}\in Z_p$ and $[L]\in B_0^{r-1}$. Put

$$[N_{k,L}]=\Phi_{q-k}[L] \quad \text{for } 1\leqq k<q \quad (p=2),$$
$$=\Phi_{(p-1)(q-2k)}[L] \quad \text{for } 1\leqq k<q/2 \quad (p>2).$$

Then we have

$$[M]=\phi^*([']\times[M'])-\sum_{k=1}^{q-1}\sum_L b_{k,L}[N_{k,L}] \qquad (p=2)$$
$$=\alpha^{-1}\phi^*([M'])-\sum_{1\leqq k<q/2}\sum_L(-1)^k b_{k,L}[N_{k,L}] \qquad (p>2).$$

Since it is easily seen that $[N_{k,L}]\in B_{01}^r$ and $N_{k,L}<M$, this completes the proof.

Denote by $\bar{B}_{02}^r$ the set of all elements $\phi^*([M']\times\cdots\times[M'])$ for which $M'\in\bar{B}_0^{r-1}$, and put $\bar{B}_0^r=B_{01}^r\cup\bar{B}_{0b}^r$. Since $B_0^r=B_{01}^r\cup B_{02}^r$ is a basis for the module $H_0^*(\mathfrak{Z}_p^r(S^n))$ by Proposition 5, Lemma 5 yields

Proposition 7. *Set $\bar{B}_0^r$ is a basis for the module $H_0^*(\mathfrak{Z}_p(S^n))$.*

From with Lemmas 4 and 5 we get easily

Proposition 8. *Let I be an admissible sequence with $l(I)=r$, and represent $St^I[O_r]$ in terms of the basis $\bar{B}_0^r$:*

$$St^I[O_r]=\sum_N b_N[N]+\sum_{M'}b_{M'}\phi^*([M']\times\cdots\times[M']) \qquad b_N,\ b_{M'}\in Z_p.$$

Then $b_N\neq 0$ implies $N\leqq I$, and if $I\in\Omega(p,n)$ we have $b_I\neq 0$. (Note that $[I]\in B_{01}^r$ by 5.3 if $I\in\Omega(p,n)$).

Remark. If we regard an admissible sequence $I=(i_1,\cdots,i_l)$ with $l\leqq r$ as an element $(i_1,\cdots,i_l,0,\cdots,0)\in\pi^r$, then the assumption $l(I)=r$ may be weaken in Lemma 4, and hence in Proposition 8, to $l(I)\leqq r$. (See Proposition 8 of [8].)

§6. Poof of Theorem 1 for $m=p^r$

As is stated at the end of §2 the space $\mathfrak{S}_{p^r,p}(S^n)$ is homeomorphic with $\mathfrak{Z}_p^r(S^n)$, and we know by Lemma 2 that $H^n(\mathfrak{Z}_p^r(S^n))$ is generated by $[O_r]$. Therefore we may regard $v(p^r)=[O_r]$ in the proof of Theorem 1.

To simplify the notation, we shall write T_r for $T_{[O_r]}: U(p,n)\longrightarrow H^*(\mathfrak{Z}_p^r(S^n))$.

Theorem 2 (the first part of Theorem 1 for $m=p^r$). *If θ is a monomial of $U(p,n)$ such that $R_p(\theta)>p^r$, then $T_r(\theta)=0$.*

Proof. We do this by induction on r. Let $\theta=\prod_{i=1}^c I_i^{e(i)}$.

Case 1: $\sum_{i=1}^c e(i)=1$.

In this case $\theta=I\in\Omega(p,n)$ and $l(I)>r$. Therefore $T_r(\theta)=St^I[O_r]=0$ follows from Proposition 6.

Case 2: $\sum_{i=1}^c e(i)\geqq 2$.

It follows from Proposition 2 that

$$T_r(\theta) = T_r(\prod_{i=1}^{c} I_i^{e(i)}) = \prod_{i=1}^{c} (St^{I_i}[O_r])^{e(i)}$$
$$= \prod_{i=1}^{c} (St^{I_i} \circ \Phi_0[O_{r-1}])^{e(i)} = \prod_{i=1}^{c} (\Phi_0 \circ St^{I_i}[O_{r-1}])^{e(i)}.$$

By Propositions 3 and 4, this can be expressed as a linear combination of elements with type:

$$(1) \qquad \phi^*(\prod_{i=1}^{c} (St^{I_i}[O_{r-1}])^{e(i,1)} \times \cdots \times \prod_{i=1}^{c} (St^{I_i}[O_{r-1}])^{e(i,p)})$$
$$= \phi^*(T_{r-1}(\prod_{i=1}^{c} I_i^{e(i,1)}) \times \cdots \times T_{r-1}(\prod_{i=1}^{c} I_i^{e(i,p)}))$$

where $\sum_{k=1}^{p} e(i,k) = e(i)$ for $i=1, \cdots, c$. It follows that each element (1) has k_0 such that

$$\sum_{i=1}^{c} e(i,k_0) p^{l(I_i)} > p^{r-1}.$$

In fact otherwise we should have $R_p(\theta) = \sum_{i=1}^{c} e(i) p^{l(I_i)} \leqq p^r$ which contradicts with our assumption. Hence the hypothesis of induction implies

$$T_{r-1}(\prod_{i=1}^{c} I_i^{e(i,k_0)}) = 0$$

so that each element (1) is zero. Thus we have $T_r(\theta)=0$, and complete the proof.

LEMMA 6. *Assume that* $\sum_{i=1}^{c} e(i) p^{l(I_i)} = p^r$ *and* $\sum_{i=1}^{c} e(i) \geqq 2$. *Then we have*

$$(2) \qquad T_r(\prod_{i=1}^{c} I_i^{e(i)})$$
$$= \alpha\phi^*(T_{r-1}(I_1^{e(1)/p}) \times T_{r-1}(I_1^{e(1)/p}) \times \cdots \times T_{r-1}(I_1^{e(1)/p})) \qquad \text{if} \quad c=1,$$
$$= \sum (\pm \prod_{i=1}^{c} P(E_i)) \phi^*(T_{r-1}(\prod_{i=1}^{c} I_i^{e(i,1)}) \times \cdots \times T_{r-1}(\prod_{i=1}^{c} I_i^{e(i,p)}))$$
$$\text{if} \quad c \geqq 2,$$

where $0 \neq \alpha \in Z_p$, *and the sum runs through all sequences* $(E_1, \cdots, E_c)$ *such that* $E_1 = (e(1,1), \cdots, e(1,p)) \in \bar{\pi}_0^p(e(1))$, $E_i = (e(i,1), \cdots, e(i,p)) \in \pi_0^p(e(i))$ $(2 \leqq i \leqq p)$ *and* $\sum_{i=1}^{c} e(i,k) p^{l(I_i)} = p^{r-1}$ $(1 \leqq k \leqq p)$.

PROOF. Case: $c=1$

Put $I=I_1$ and $e=e(1)$. Since $e \geqq 2$ we have

$$T_r(I^e) = (\Phi_0 \circ St^I[O_{r-1}])^e$$

in view of Proposition 2. Therefore it follows from Proposition 3 and Theorem 2 that

$$(-1)^e T_r(I^e) = \sum_E P(E) \phi^*(T_{r-1}(I^{e_1}) \times \cdots \times T_{r-1}(I^{e_p}))$$
$$+ P(e/p-1, e/p, \cdots, e/p) \phi^*(T_{r-1}(I^{e/p}) \times \cdots \times T_{r-1}(I^{e/p}))$$

where the sum runs through all elements $E = (e_1, \cdots, e_p) \in \bar{\pi}_0^p(e)$ such that

$$e_k p^{l(I)} \leqq p^{r-1} \qquad \text{for} \quad k=1, \cdots, p.$$

However $\sum_{k=1}^{p} e_k p^{l(I)} = ep^{l(I)} = p^r$, so that each $e_k p^{l(I)}$ must be p^{r-1}. Therefore $e_1 = \cdots = e_p$. This shows that $\sum_{E} = 0$. On the other hand, since $2 \leqq e = p^{r-l(I)}$, if we put $q = r - l(I) - 1$, then $q \geqq 0$ and

$$P(e/p-1, e/p, \cdots, e/p) = P(p^q-1, p^q, \cdots, p^q).$$

Therefore by virtue of Lemma 2 in Appendix $P(e/p-1, e/p, \cdots, e/p) \not\equiv 0 \bmod p$. Thus we obtain the desired result.

Case 2: $c \geqq 2$.

The proof is similar as above if Proposition 4 is used instead of Proposition 3 and is left to the reader.

THEOREM 3 (the second part of Theorem 1 for $m = p^r$). *The elements $T_r(\theta)$, $\theta \in A_{p^r}$, are linearly independent.*

PROOF. Since the theorem for $r = 0$ is trivial, we proceed by induction on r.

Let $\{J_1, \cdots, J_\sigma\}$ be the totality of elements of $\Omega(p, n)$ having length r. We assume $J_1 < \cdots < J_\sigma$. Regarding J_s as an element of A_{p^r}, we write

$$Q_s^r = A_{p^r} - \{J_{s+1}, \cdots, J_\sigma\}.$$

Since $Q_\sigma^r = A_{p^r}$, Theorem 3 is established by proving the following 6.1 and 6.2.

6.1. The elements $T_r(\theta)$, $\theta \in Q_0^r$, are linearly independent.

6.2. If the elements $T_r(\theta)$, $\theta \in Q_{s-1}^r$, are linearly independent, then so are $T_r(\theta)$, $\theta \in Q_s^r$.

(PROOF of 6.1.) Let $\theta = \prod_{i=1}^{c} I_i^{e(i)} \in Q_0^r$. Then $\sum_{i=1}^{c} e(i) p^{l(I_i)} = p^r$ and $\sum_{i=1}^{c} e(i) \geqq 2$, so that $T_r(\theta)$ is equal to (2) in Lemma 6. Therefore if we denote by $H_1^*(\mathfrak{Z}_p^r(S^n))$ the submodule generated in the module $H^*(\mathfrak{Z}_p^r(S^n))$ by all elements of type:

$$\phi^*(T_{r-1}(\theta_1') \times \cdots \times T_{r-1}(\theta_p')), \quad \theta_p' \in A_{p^{r-1}}, \tag{3}$$

then it follows that

$$T_r(\theta) \in H_1^*(\mathfrak{Z}_p^r(S^n)) \quad \text{if} \quad \theta \in Q_0^r. \tag{4}$$

Let B_1^r be a basis for $H_1^*(\mathfrak{Z}_p^r(S^n))$ whose elements are of type (3). We shall now prove that (2) gives the representation of $T_r(\theta)$ in terms of the basis B_1^r.

Since the elements $T_{r-1}(\theta')$, $\theta' \in A_{p^{r-1}}$, are linearly independent by the hypothesis of induction, it follows from Proposition 1[5] that for every sequence $(\theta_1', \cdots, \theta_p')$ of elements of $A_{p^{r-1}}$ there is determined uniquely $\varepsilon = 1$ or -1 such that $\varepsilon\phi^*(T_{r-1}(\theta_q') \times \cdots \times T_{r-1}(\theta_{q-1}')) \in B_1^r$. Therefore the above assertion follows from that if $(E_1, \cdots, E_c) \neq (E_1', \cdots, E_c')$ then $\phi^*(T_{r-1}(\prod_{i=1}^{c} I_i^{e'(i,1)}) \times \cdots \times T_{r-1}(\prod_{i=1}^{c} I_i^{e'(i,p)})) \neq \varepsilon\phi^*(T_{r-1}(\prod_{i=1}^{c} I_i^{e(i,1)}) \times \cdots \times T_{r-1}(\prod_{i=1}^{c} I_i^{e(i,p)}))$. This is proved as follows: Assume

5) Here the assumption that $n > 1$ if $p = 2$ is needed.

otherwise, then according to 3.1 we have $T_{r-1}(\prod_{i=1}^{c} I_i^{e'(i,k)}) = T_{r-1}(\prod_{i=1}^{c} I_i^{e(i,k+q)})$ for some q $(0\leqq q<p)$ and any k $(1\leqq k\leqq p)$, where $e(i, k+q)$ means $e(i, k+q-p)$ if $k+q>p$. By the hypothesis of induction, this shows that $e'(i, k)=e(i, k+q)$ for $1\leqq i\leqq c$ and $1\leqq k\leqq p$. Therefore E_1 and E_1' are equivalent. However $E_1, E_1'\in \bar{\pi}_0^{p}(e(1))$, so that $E_1=E_1'$. Consequently we have $q=0$, hence $(E_1, \cdots, E_c)=(E_1', \cdots, E_c')$ which contradicts with the assumption.

In view of Lemma 4 in Appendix it follows that in the representation (2) of $T_r(\theta)$ there is at least one element of B_1^r having non-zero coefficient. Furthermore it is readily seen that if $\theta\neq\bar{\theta}$ then the elements of B_1^r arising with non-zero coefficients in the representations (2) of $T_r(\theta)$ and $T_r(\bar{\theta})$ are entirely different. These show that $T_r(\theta)$, $\theta\in Q_0^r$, are linearly independent.

(Proof of 6.2.) We shall first make some preliminaries. Denote by $\tilde{H}_0^*(\mathfrak{Z}_p^{r-1}(S^n))$ the subalgebra generated in the algebra $H^*(\mathfrak{Z}_p^{r-1}(S^n))$ by the unit cohomology class 1 and all elements of B_0^{r-1}, and take a basis $\tilde{B}_0^{r-1}$ for the module $\tilde{H}_0^*(\mathfrak{Z}_p^{r-1}(S^n))$ such that $\tilde{B}_0^{r-1}\supset B_0^{r-1}$. Then it follows from Proposition 5 that the product of elements of $H_0^*(\mathfrak{Z}_p^{r-1}(S^n))$ is in $\tilde{H}_0^*(\mathfrak{Z}_p^{r-1}(S^n))$. Since $T_{r-1}(I)=St^I[O_{r-1}]\in H_0^*(\mathfrak{Z}_p^{r-1}(S^n))$ by 5.2, we have that

(5) $$T_{r-1}(\theta')\in \tilde{H}_0^*(\mathfrak{Z}_p^{r-1}(S^n))$$

for any monomial $\theta'\in U(p, n)$. We shall next define $H_2^*(\mathfrak{Z}_p^r(S^n))$ (resp. $H_3^*(\mathfrak{Z}_p^r(S^n))$) as the submodule generated in the module $H^*(\mathfrak{Z}_p^r(S^n))$ by all elements of the following type (6) (resp. (7)).

(6) $\phi_m(z)$ for which $z\in\tilde{B}_0^{r-1}$ and $2\leqq m<(p-1)\dim z$,

(7) $\phi^*(z_1\times\cdots\times z_p)$ for which $z_i\in\tilde{B}_0^{r-1}$ and $\dim(z_1\times\cdots\times z_p)>0$.

Using (5), compare (3) and (7). Then it follows that $H_1^*(\mathfrak{Z}_p^r(S^n))\supset H_3^*(\mathfrak{Z}_p^r(S^n))$. Therefore (4) implies

(8) $$T_r(\theta)\in H_3^*(\mathfrak{Z}_p^r(S^n)),\qquad \theta\in Q_0^r.$$

According to Proposition 1 and the fact $B_0^{r-1}\subset\tilde{B}_0^{r-1}$, a basis B_4^r for the module $H_4^*(\mathfrak{Z}_p^r(S^n))=H_2^*(\mathfrak{Z}_p^r(S^n))+H_3^*(\mathfrak{Z}_p^r(S^n))$ can be taken as follows:

(9) $$\bar{B}_0^r\subset B_4^r\ ^{5)}$$

and

(10) $$B_2^r\subset B_4^r,$$

where B_2^r is the set of all elements of type (6). Since $J^i\in\Omega(p, n)$, the following (11) is obvious from the definitions.

(11) $$[J_i]\in B_2^r\subset H_2^*(\mathfrak{Z}_p^r(S^n)),\qquad (1\leqq i\leqq\sigma).$$

Since $B_0^{r-1}\subset\tilde{B}_0^{r-1}$, Proposition 7 implies $H_0^*(\mathfrak{Z}_p^r(S^n))\subset H_4^*(\mathfrak{Z}_p^r(S^n))$. Therefore we have

(12) $$T_r(J_i) \in H_4^*(\mathfrak{Z}_p^r(S^n)), \quad (1 \leqq i \leqq \sigma).$$

We shall now proceed to the proof of 6.2, and show that an equation

(13) $$\sum_\theta \alpha_\theta T_r(\theta) + \sum_{i=1}^s \beta_i T_r(J_i) = 0 \qquad (\alpha_\theta, \beta_i \in Z_p, \ \theta \in Q_0^r)$$

implies $\alpha_\theta = 0$ for every θ and $\beta_i = 0$ for every i.

In view of (8) and (12) we have

(14) $$\sum_\theta \alpha_\theta T_r(\theta) \in H_3^*(\mathfrak{Z}_p^r(S^n)) \subset H_4^*(\mathfrak{Z}_p^r(S^n)),$$
$$\sum_{i=1}^s \beta_i T_r(J_i) \in H_4^*(\mathfrak{Z}_p^r(S^n)).$$

Therefore we shall let R_1 (resp. R_2) to be the representation of $\sum_\theta \alpha_\theta T_r(\theta)$ (resp. $\sum_{i=1}^s \beta_i T_r(J_i)$) in terms of the basis B_4^r. According to (10) and (11), $[J_s]$ is an element of B_4^r. We shall calculate the coefficients of $[J_s]$ in R_1 and R_2. It follows from (11) and (14) immediately that the coefficient of $[J_s]$ in R_1 is 0. Proposition 8 shows that $T_r[J_i]$ is a linear combination of elements of $\bar{B}_0^r$:

$$T_r[J_i] = \sum_N b_N^i[N] + \sum_{M'} b_{M'}^i \phi^*([M'] \times \cdots \times [M']),$$

$b_N^i, b_{M'}^i \in Z_p$. Here $b_N^i = 0$ if $N > J_i$ and $b_{J_i}^i \neq 0$. Owing to (9) the above expression may be regarded as the representation in terms of the basis B_4^r. Therefore it follows that the coefficient of $[J_s]$ in R_2 is $\beta_s b_{J_s}^s$. Thus the representation $R_1 + R_2$ of the left side of (13) in terms of the basis B_4^r has $\beta_s b_{J_s}^s$ as the coefficient of $[J_s]$, so that we have $\beta_s b_{J_s}^s = 0$. Since $b_{J_s}^s \neq 0$ this implies $\beta_s = 0$. Now (12) becomes

$$\sum_\theta \alpha_\theta T_r(\theta) + \sum_{i=1}^{s-1} \beta_i T_r(J_i) = 0.$$

Since the left side of this equation belongs to Q_{s-1}^r, we have $\alpha_\theta = 0$ for every $\theta \in Q_0^r$ and $\beta_1 = 0$ for every $1 \leqq i \leqq s-1$ by the hypothesis of induction. This completes the proof of 6.2, hence that of Theorem 3.

§7. Proof of Theorem 1

If $m = \sum_{r=0}^h a(r)p^r$ is the p-adic expansion of m, we may identify $\mathfrak{S}_{m,p}(S^n)$ with the product

$$\underbrace{S^n \times \cdots \times S^n}_{a(0)} \times \underbrace{\mathfrak{Z}_p^1(S^n) \times \cdots \times \mathfrak{Z}_p^1(S^n)}_{a(1)} \times \cdots \times \underbrace{\mathfrak{Z}_p^h(S^n) \times \cdots \times \mathfrak{Z}_p^h(S^n)}_{a(h)}$$

especially $\mathfrak{S}_{p^r,p}(S^n)$ with $\mathfrak{Z}_p^r(S^n)$. (See the final part of §2) For each pair (r, j) of integers such that $0 \leqq r \leqq h$ and $1 \leqq j \leqq a(r)$, define maps $\xi_j^k : \mathfrak{S}_{p^r,p}(S^n) \longrightarrow \mathfrak{S}_m(S^n)$ and $\eta_j^r : \mathfrak{S}_m(S^n) \longrightarrow \mathfrak{S}_{p^r,p}(S^n)$ to be the injection and the projection respectively to the $(a_0 + \cdots + a_{r-1} + j)$-th factor. Then it is obvious that $\xi_j^{r*} \circ \eta_k^{t*} =$

the identy if $(r, j)=(t, k)$ and $=0$ otherwise, and that the commutativity holds in the diagram:

$$\begin{array}{ccc} \mathfrak{S}_{p^r,p}(S^n) & \xrightarrow{\xi_p^r} & \mathfrak{S}_{m,p}(S^n) \\ \downarrow \rho_{p^r} & & \downarrow \rho_m \\ \mathfrak{S}_{p^r}(S^n) & \xrightarrow{i_{p^r,m}} & \mathfrak{S}_m(S^n) \end{array} .$$

Furthermore it follows from Lemma 2 and Künneth formula that the module $H^n(\mathfrak{S}_{m,p}(S^n))$ is generated by all elements $\eta_j^{r*}([O_r])$, so that the element $v(m)$ can be expressed as a linear combination $\sum_{r=0}^{h}\sum_{j=1}^{a(r)}\alpha_j^r\xi_j^{r*}([O_r])$. Now we have

$$\begin{aligned} \xi_j^{r*}(v(m)) &= \xi_j^{r*}\circ\rho_m(u(m)) = \rho_{p^r}^*\circ i_{p^r,m}^*(u(m)) \\ &= \rho_{p^r}^*(u(p^r)), \end{aligned}$$

and

$$\xi_j^{r*}(v(m)) = \sum_{t=0}^{h}\sum_{k=1}^{a(t)}\alpha_k^t\xi_j^{r*}\circ\eta_k^{t*}([O_r]) = \alpha_j^r[O_r].$$

Consequently $\rho_{p^r}^*(u(p^r))=\alpha_j^r[O_r]$. This shows $\alpha_j^r\not\equiv 0 \bmod p$, because $\rho_{p^r}^*$ is a monomorphism. Thus we have proved that
$v(m)=\sum_{r=0}^{h}\sum_{j=1}^{a(r)}\alpha_j^r\eta_j^{r*}([O_r])$ with $0\neq\alpha_j^r\in Z_p$ for every pair (r, j).

Proof of Theorem 1. Let $\theta=\prod_{i=1}^{c}I_i^{e(i)}$ be a monomial of $U(p, n)$. Then it follows from the above fact by a straightforward calculation that

$$\begin{aligned} (1)\qquad T_{v(m)}(\theta) &= T_{v(m)}(\prod_{i=1}^{c}I_i^{e(i)}) \\ &= \sum Q(E_1, \cdots, E_c)\,(T_0(\prod_{i=1}^{c}I_i^{e(i,1)})\times\cdots\times T_0(\prod_{i=1}^{c}I_i^{e(i,a(0))}) \\ &\quad \times T_1(\prod_{i=1}^{c}I_i^{e(i,a(0)+1)})\times\cdots\times T_h(\prod_{i=1}^{c}I_i^{e(i,a(0)+\cdots+a(h))}), \end{aligned}$$

where $Q(E_1, \cdots, E_c)=\alpha(E_1, \cdots, E_c)\prod_{i=1}^{c}P(E_i)$ with $0\neq\alpha(E_1, \cdots, E_c)\in Z_p$, and the sum runs through all sequences $(E_1, \cdots, E_c)$ such that $E_i=(e(i, 1), \cdots, e(i, a))\in \pi^a(e(i))$ for $1\leq i\leq c$ $(a=a(0)+\cdots+a(h))$. Owing to Theorem 2 we may assume in (1) that

$$\sum_{i=1}^{c}e(i, j)p^{l(I_i)}\leq p^r$$

for $a(0)+\cdots+a(r-1)<j\leq a(0)+\cdots+a(r)$ and $0\leq r\leq h$. Therefore in order to $T_{v(m)}(\theta)\neq 0$ we must have

$$\begin{aligned} R_p(\theta) &= \sum_{i=1}^{c}e(i)p^{l(I_i)} = \sum_{i=1}^{c}\sum_{j=1}^{a}e(i, j)p^{l(I_i)} \\ &\leq \sum_{r=0}^{h}a(r)p^r = m. \end{aligned}$$

This proves the first part of Theorem 1.

It follows from Theorem 3 and Künneth formula that a basis for the module

$H^*(\mathfrak{S}_{m,p}(S^n))$ can be formed with a set C_m containing all elements of type:

$$T_0(\theta_1)\times \cdots \times T_0(\theta_{a(0)})\times T_1(\theta_{a(0)+1})\times \cdots \times T_1(\theta_{a(0)+a(1)})$$
$$\times \cdots \times T_h(\theta_{a(0)+\cdots+a(h-1)+1})\times \cdots \times T_h(\theta_{a(0)+\cdots+a(h)})$$

where $\theta_j \in A_{p^r}$ if $a_0+\cdots+a_{r-1}<j\leqq a_0+\cdots+a_r$, $(0\leqq r\leqq h)$. Let θ be a monomial with $R_p(\theta)=m$, and consider again (1). Then the above arguments show that we may assume

$$\sum_{i=1}^{c} e(i, j)p^{l(I_i)} = p^r$$

for $a(0)+\cdots+a(r-1)<j\leqq a(0)+\cdots+a(r)$ and $0\leqq r\leqq h$. Therefore (1) is regarded as the representation of $T_{v(m)}(\theta)$ in terms of the basis C_m. According to Lemma 5 in Appendix, it follows that in the representation (1) there is at least one element of the basis C_m having non-zero coefficient. Furthermore it is easily seen that if θ, $\bar{\theta}\in A_m$ are different, then the elements of C_m arising with non-zero coefficients in the representations (1) of $T_{v(m)}(\theta)$ and $T_{v(m)}(\bar{\theta})$ are entirely different. These show that the elements $T_{v(m)}(\theta)$, $\theta\in B_m$, are linearly independent, and complete the proof of the second part of Theorem 1.

Appendix

We give in this appendix proofs of the arithmetical lemmas used in §§4, 6 and 7.

For any integers i and j we define the *binomial coefficient* by

$$\binom{i}{j} = \frac{i(i-1)\cdots(i-j+1)}{j!} \quad \text{if } j>0,$$
$$= 1 \text{ if } j=0, \text{ and } =0 \quad \text{if } j<0.$$

For every sequence $E=(e(1),\cdots,e(r))$ of integers $(r\geqq 2)$, we define the *polynomial coefficient* $P(E)=P(e(1),\cdots,e(r))$ inductively by

$$(1) \qquad P(e(1),\cdots,e(r) = \binom{e}{e(1)}P(e(2),\cdots,e(r))$$

where $e=\sum_{i=1}^{r} e(i)$ and we agree $P(e(2))=1$. It follows that $P(e(1),\cdots,e(r))= e!/\prod_{i=1}^{r} e(i)!$ if $e(i)\geqq 0$ for every i, and $=0$ otherwise. Since

$$\binom{i}{j} = \binom{i-1}{j-1}+\binom{i-1}{j},$$

induction on r proves easily

Lemma 1. $P(e(1),\cdots,e(r))=\sum_{i=0}^{r} P(e(1),\cdots,e(i)-1,\cdots,e(r))$.

As is well-knon [1], the following formula is very useful if we deal with the biomial coefficient mod p.

$$(2) \qquad \binom{b}{c}\equiv \prod_{i=1}^{s}\binom{b_i}{c_i} \bmod p$$

where $b=\sum_{i=1}^{s} b_i p^i$ and $c=\sum_{i=1}^{s} c_i p^i$ are the p-adic expansion of integers b and $c\geqq 0$.

LEMMA 2. *If* $e(1)=p^q-1$ *and* $e(2)=\cdots=e(p)=p^q$ $(q\geqq 0)$, *then* $P(e(1),\cdots, e(p))\not\equiv 0 \bmod p$.

PROOF. From (1) it follows that

$$P(p^q-1, p^q, \cdots, p^q) = \binom{p^{q+1}-1}{p^q-1} \prod_{i=1}^{p-1} \binom{p^{q+1}-ip^q}{p^q}.$$

However (2) implies

$$\binom{p^{q+1}-1}{p^q-1} = \binom{p-1}{0}\binom{p-1}{p-1}^q \equiv 1 \quad \text{and}$$
$$\binom{p^{q+1}-ip^q}{p^q} \equiv \binom{p-i}{1} \equiv -i \qquad (1\leqq i\leqq p-1).$$

Therefore $P(p^q-1, p^q, \cdots, p^q)\equiv(-1)^{p-1}(p-1)!\not\equiv 0$.

LEMMA. 3. *For non-negative integers* $a, h, e(i)$ *and* $h(i)$ *let*

$$\sum_{i=1}^{c} e(i)p^{h(i)} = p^h a. \tag{3}$$

Assume that $c>0$ *if* $a\not\equiv 0 \bmod p$, *and that* $c>a/p$ *if* $a\equiv 0 \bmod p$. *Then we can find integers* $e'(i)$ *such that*

$$\sum_{i=1}^{c} e'(i)p^{h(i)} = p^h \tag{4}$$

and

$$\prod_{i=1}^{c} \binom{e(i)}{e'(i)} \not\equiv 0 \quad \bmod p. \tag{5}$$

PROOF. Without loss of generality we may assume $e(i)>0$ for every i. Let first $h=0$. It follows then that there is i_0 such that $h(i_0)=0$ and $e(i_0)\not\equiv 0$. Because otherwise $\sum_{i=1}^{c} e(i)p^{h(i)}\equiv 0$ and $e(i)p^{h(i)}\geqq p$ for every i, so that we should have $a\equiv 0$ and $a\geqq pc$ which contradicts our assumption. Take such an i_0, and put $e'(i)=1$ if $i=i_0$ and $=0$ otherwise. Then obviously (4) and (5) hold, and we have the lemma.

To establish the general case we proceed by induction on h. It does not lose the generality to assume in (3) the following:

$$\begin{aligned} h(i) &= 0 \text{ if } 1\leqq i\leqq b, \text{ and } \geqq 1 \text{ if } b<i\leqq c, \\ e(i) &= pq(i)+r(i) \text{ with } 0<r(i)<p \text{ if } 1\leqq i\leqq a, \\ &= pq(i) \quad \text{if } a<i\leqq b, \end{aligned}$$

where $1\leqq a\leqq b\leqq c$. Since $\sum_{i=1}^{a} r(i)$ is a multiple of p, it follows that there are integers $t(i)\geqq 0$ such that

$$p\left(\sum_{i=1}^{a} t(i)\right) = \sum_{i=1}^{a} r(i), \qquad t(i)\leqq r(i) \text{ for } 1\leqq i\leqq a.$$

Dividing (3) by p we obtain

$$\sum_{i=1}^{a} t(i)p+\sum_{i=1}^{b} q(i)p+\sum_{i=b+1}^{c} e(i)p^{h(i)-1}=p^{h-1}a\,.$$

Applying to this the hypothesis of induction, we can find $t'(i)$, $q'(i)$ and $e'(i)$ such that

$$(6)\qquad \sum_{i=1}^{a} t'(i)p+\sum_{i=1}^{e} q'(i)p+\sum_{i=b+1}^{c} e'(i)p^{h(i)-1}=p^{h-1}$$

and

$$(7)\qquad \prod_{i=1}^{b}\binom{q(i)}{q'(i)}\not\equiv 0\,,\quad \prod_{i=b+1}^{c}\binom{e(i)}{e'(i)}\not\equiv 0\,,\quad \sum_{i=1}^{a}\binom{t(i)}{t'(i)}\not\equiv 0\,.$$

The last implies $t'(i)\leqq t(i)$ for $1\leqq i\leqq a$, hence

$$p\Big(\sum_{i=1}^{a} t'(i)\Big)\leqq p\Big(\sum_{i=1}^{a} t(i)\Big)=\sum_{i=1}^{a} r(i)\,.$$

Therefore it follows that there are $p'(i)$ such that

$$p\Big(\sum_{i=1}^{a} t'(a)\Big)=\sum_{i=1}^{a} r'(i)\,,\qquad r'(i)\leqq r(i)\ \text{ for } 1\leqq i\leqq a\,.$$

Since $0<r(i)<p$, we have that

$$(8)\qquad \binom{r(i)}{r'(i)}\not\equiv 0\qquad \text{for}\ \ 1\leqq i\leqq a\,.$$

Multiplying (6) by p we have

$$\sum_{i=1}^{a} r'(i)p+\sum_{i=1}^{h} q'(i)p^{1}+\sum_{i=b+1}^{c} e'(i)p^{h(i)}=p^{h}\,.$$

Putting

$$\begin{aligned} e'(i)&=pq'(i)+r'(i) &&\text{if}\ \ 1\leqq i\leqq a\,,\\ &=pq'(i) &&\text{if}\ \ a<i\leqq b\,,\end{aligned}$$

we obtain

$$\sum_{i=1}^{b} e'(i)p+\sum_{i=b+1}^{c} e'(i)p^{h(i)}=p^{h}\,,$$

and

$$\begin{aligned}\binom{e(i)}{e'(i)}&\equiv\binom{q(i)}{q'(i)}\binom{r(i)}{r'(i)} &&\text{if}\ \ 1\leqq i\leqq a\,,\\ &\equiv\binom{q(i)}{q'(i)} &&\text{if}\ \ a<i\leqq b\,.\end{aligned}$$

(see (2)) This, together with (7) and (8), proves (5). Now the inductive step is complete, and we end the proof.

LEMMA 4. *Let non-negative integers h, $h(i)$ and $e(i)$ satisfy an equation*

$$(9)\qquad \sum_{i=1}^{c} e(i)p^{h(i)}=p^{h}\,.$$

Then if $c\geqq 2$ there exists a sequence $(E_1, E_2, \cdots, E_c)$ such that

$$\sum_{i=1}^{c} e(i,k)p^{h(i)}=p^{h-1}\qquad \textit{for}\ \ 1\leqq k\leqq p\,,$$

$$\prod_{i=1}^{c} P(E_i)\not\equiv 0\qquad \bmod p$$

where $E_i=(e(i,1),\cdots,e(i,p))\in\pi_0^p(e(i))$ *for* $1\leqq i\leqq c$.

PROOF. Since $c>p/p=1$, the above Lemma 4 implies the existence of integers $e(i,1)$ such that

$$(10)_1\qquad \sum_{i=1}^{c}e(i,1)p^{h(i)}=p^{h-1},\quad \prod_{i=1}^{c}\binom{e(i)}{e(i,1)}\not\equiv 0\,.$$

Subtracting $(10)_1$ from (9), we have

$$(9)_1\qquad \sum_{i=1}^{c}(e(i)-e(i,1))p^{h(i)}=p^{h-1}(p-1)\,.$$

Since $p-1\not\equiv 0$ and $e(i)-e(i,1)\geqq 0$, the application of Lemma 3 to $(9)_1$ implies the existence of integers $e(i,2)$ such that

$$(10)_2\qquad \sum_{i=1}^{c}e(i,2)p^{h(i)}=p^{h-1},\quad \prod_{i=1}^{c}\binom{e(i)-e(i,1)}{e(i,2)}\not\equiv 0\,.$$

Substract $(10)_1$ from $(9)_1$, and apply Lemma 4 to the result. Continuing this process we can find integers $e(i,k)$ such that

$$(10)\qquad \sum_{i=1}^{c}e(i,k)p^{h(i)}=p^{h-1},$$
$$\prod_{i=1}^{c}\binom{e(i)-e(i,1)-\cdots-e(i,k-1)}{e(i,k)}\not\equiv 0\qquad\text{for}\quad 1\leqq k\leqq p\,.$$

In particular $e(i,p)=e(i)-e(i,1)-\cdots-e(i,p-1)$. Now the desired lemma is readily obtained if we take into consideration the following facts whose proofs are easy:

$$P(e(i,1),\cdots,e(i,p))=\prod_{k=1}^{p}\binom{e(i)-e(i,1)-\cdots-e(i,k-1)}{e(i,k)}$$
$$P(e(1),\cdots,e(p))=\binom{pe}{e}P(e(2),\cdots,e(p))$$
$$\text{if}\qquad e(1)=\cdots=e(p)=e\,.$$

LEMMA 5. *Let* $m, e(i), h(i)$ *be non-negative integers satisfying an equation*

$$(11)\qquad \sum_{i=1}^{c}e(i)p^{h(i)}=m\,,$$

and $m=\sum_{r=0}^{h}a(r)p^r$ *be the* p*-adic expansion of* m. *Put* $a=\sum_{r=0}^{h}a(r)$ *and assume* $a\geqq 2$. *Then there exists a sequence* $(E_1,E_2,\cdots,E_c)$ *satisfying*

$$\sum_{i=1}^{c}e(i,j)p^{h(i)}=p^r$$

for $a(0)+\cdots+a(r-1)<j\leqq a(0)+\cdots+a(r)$ *and* $0\leqq r\leqq h$, *and*

$$\prod_{i=1}^{c}P(E_i)\neq 0\qquad\text{mod } p\,,$$

where $E_i=(e(i,1),\cdots,e(i,a))\in\pi^a(e(i))$ *for* $1\leqq i\leqq c$.

PROOF. We do this by induction on a. Let $a(0)=\cdots=a(q-1)=0$ and $a(q)\neq 0$. Then $m/p^q=(a(q)p^0+\cdots+a(h)p^{h-q})\not\equiv 0$, so that Lemma 3 applied to (11) implies the existence of integers $e(i,1)$ such that

$$\sum_{i=1}^{c} e(i,1)p^{h(i)} = p^q\,, \quad \prod_{i=1}^{c} \binom{e(i)}{e(i,1)} \not\equiv 0\,. \tag{12}$$

Subtracting (12) from (11) we obtain

$$\sum_{i=1}^{c} (e(i)-e(i,1))p^{h(i)} = (a(q)-1)p^q + \sum_{i=1}^{h-q} a(q+i)p^{q+i}\,.$$

Since $(a(q)-1)+\sum_{i=1}^{h-q} a(q+i) = a-1$, we can find by the hypothesis of induction a sequence $(E'_1, \cdots, E'_c)$ such that

$$\begin{aligned} \sum_{i=1}^{c} & e(i,j)p^{h(i)} \\ &= p^q \quad \text{if} \quad 2 \leqq j \leqq a(q)\,, \\ &= p^r \quad \text{if} \quad a(q)+\cdots+a(r-1) \leqq j \leqq a(q)+\cdots+a(r) \text{ and } q<r\leqq h\,, \end{aligned} \tag{13}$$

and

$$\prod_{i=1}^{c} P(E'_i) \not\equiv 0\,,$$

where $E'_i = (e(i,2), \cdots, e(i,a)) \in \pi^{a-1}(e(i)-e(i,1))$ for $1 \leqq i \leqq c$. Put $E_i = (e(i,1), \cdots, e(i,a))$, then $\prod_{i=1}^{c} P(E_i) = \prod_{i=1}^{c} \binom{e(i)}{e(i,1)} P(E'_i) \not\equiv 0$ by (2). Thus (12) and (13) prove the lemma.

Bibliography

[1] J. Adem: The relations on Steenrod power of cohomology classes. Algebraic Geometry and Topology, Princeton University Press (1957), pp. 191–238.

[2] H. Cartan: Sur les groupes d'Eilenberg-MacLane I, II, Proc. Nat. Acad. Sci., U.S.A., vol. 40 (1954), pp. 467–471 and pp. 704–707.

[3] A. Dold: Homology of symmetric products and other functors of complexes, Ann. of Math., vol. 68 (1958), pp. 54–80.

[4] A. Dold–R. Thom: Une generalization de la notion d'espace fibre. Application aux produits symetrique infinis. C. R. Acad. Sci. Paris, vol. 242 (1956), pp. 1680–1682.

[5] A. Dold–R. Thom: Quasifaserunger und unendliche symmetrische Produkte, Ann. of Math., vol 67 (1958), pp. 239–281.

[6] M. Nakaoka: Cohomology theory of a complex with a transformation of prime period and its applications, J. Inst. Polytech., Osaka City Univ., vol. 7 (1956), pp. 51–102.

[7] M. Nakaoka: Cohomology of symmetric products, ibid., vol. 8 (1957), pp. 121–144.

[8] M. Nakaoka: Cohomology mod p of symmetric products of spheres, ibid., vol. 9 (1958), pp. 1–18.

[9] J–P. Serre: Cohomologie modulo 2 des complexes d'Eilenberg-MacLane, Comm. Math. Helv., vol. 27 (1953), pp. 198–232.

[10] N. E. Steenrod: Cohomology Operations and obstructions to extending continuous functions. Colloquium lectures Notes of Princeton University (1957).