Journal of Mathematics,
Osaka City University,
Vol. 13, No. 1.

Note on cohomology algebras of symmetric groups

Dedicated to Professor K. Shoda on his sixtieth birthday

by Minoru NAKAOKA

(*Received June 27, 1962*)

This is a continuation of the paper [3], and deals with the mod p cohomology algebra $H^*(S(m);\ Z_p)$ of the symmetric group $S(m)$ of degree m, where $1 \leqq m \leqq \infty$ and p is a prime. The author gave a basis for the homology module $H_*(S(m);\ Z_p)$ in [3]. In the present paper, we try to describe the diagonal homomorphism

$$d_*:\ H_*(S(m);\ Z_p) \longrightarrow H_*(S(m);\ Z_p) \otimes H_*(S(m);\ Z_p)$$

in terms of the basis, and by its conversion we derive some results on the cohomology algebra $H^*(S(m);\ Z_p)$. Throughout this paper a prime p is fixed.

1. Recapitulation.

For the convenience of the reader, the results which are proved in [2] and [3] are recapitulated in this section.

(A) Denote by $\lambda_m^n : S(m) \longrightarrow S(n)$ the natural inclusion map, where $m \leqq n$. Then, for any coefficient group G, the homomorphism $\lambda_{m*}^n: H_*(S(m); G) \longrightarrow H_*(S(n);G)$ induced by λ_m^n is a monomorphism and its image is a direct summand of $H_*(S(n);G)$; the homomorphism $\lambda_m^{n*}:\ H^*(S(n);G) \longrightarrow H^*(S(m);G)$ induced by λ_m^n is an epimorphism and its kernel is a direct summand of $H^*(S(n);G)$. If $q < (m+1)/2$ then $\lambda_{m*}^{m+1} : H_q(S(m);G) \longrightarrow H_q(S(m+1);G)$ and $\lambda_m^{m+1*} : H^q(S(m+1);G) \longrightarrow H^q(S(m);G)$ are isomorphisms.

(B) Let k be a field, and let μ: $S(m) \times S(n) \longrightarrow S(m+n)$ denote a homomorphism defined by

$$\mu(\alpha\times\beta))(i) = \begin{cases} \alpha(i) & \text{if } 1 \leqq i \leqq m, \\ \beta(i-m) + m & \text{if } m < i \leqq m+n, \end{cases}$$

where $\alpha \in S(m)$ and $\beta \in S(n)$. Then, for elements $a \in H_i(S(m);\ k)$ and $b \in H_j(S(n);\ k)$ we define a product $ab \in H_{i+j}(S(m+n);\ k)$ by

$$ab = \mu_*(a \otimes b),$$

where $\mu_* : H_*(S(m);\ k) \otimes H_*(S(n);\ k) \longrightarrow H_*(S(m+n);\ k)$ is the homomorphism induced by μ. The product is bilinear, associative and (anti-) commutative. Denote by $S(\infty)$ the infinite symmetric group, *i.e.*, the direct limit of $\{S(m), \lambda_m^n\}$. Let λ_m: $S(m) \longrightarrow S(\infty)$ denote the natural inclusion. Then the rule

$$\lambda_{m*}(a)\ \lambda_{n*}(b) = \lambda_{m+n*}(ab)$$

defines on $H_*(S(\infty); k)$ a multiplicative structure, and it makes $H_*(S(\infty); k)$ together with the diagonal homomorphism d_* a commutative associative Hopf algebra. H_* $S(\infty); k)$ is of fiite type.

(C) A p-Sylow subgroup $S(p^f, p)$ of the symmetric group $S(p^f)$ is given by an iterated wreath product of π, where π is the group of cyclic permutations of order p and degree p: $S(p^f, p) = S(p^{f-1}, p) \int \pi$. Denote by $e(i)$ the usual generator of $H_i(\pi; Z_p)$. We associate to each sequence $(k_1, k_2, \ldots, k_f)$ of non-negative integers an element

$$| k_1, k_2, \ldots, k_f | \in H_*(S(p^f, p); Z_p)$$

of dimension $k_1 + pk_2 + \ldots + p^{f-1}k_f$ defined by

$$| k_1, k_2, \ldots, k_f | = | k_2, \ldots, k_f | \int e(k_1),$$

where $\int$ stands for the wreath product of homology classes. Using this we define for a sequence $I=(i_1, i_2, \ldots, i_f)$ satisfying

(1.1) $\quad i_s - (p-1)(i_{s+1} + \ldots + i_f) \geqq 0$

for $1 \leqq s \leqq f$ an element

$$a(I) = a(i_1, i_2, \ldots, i_f) \in H_k(S(p^f); Z_p)$$

as $\varrho_* | k_1, k_2, \ldots, k_f |$ with $k_s = i_s - (p-1)(i_{s+1} + \ldots + i_f)$, where $\varrho_*: H_*(S(p^f, p); Z_p) \longrightarrow H_*(S(p^f); Z_p)$ is the homomorphism induced by the inclusion. The dimension of $a(I)$ is $i_1 + i_2 + \ldots + i_f$.

Denote by $Q(p)$ the set of all sequences of (positive) integers $I = (i_1, i_2, \ldots, i_f)$, $f > 0$, satisfying

(1.2) $\quad i_s \equiv 0$ or $-1 \mod 2(p-1)$ for $1 \leqq s \leqq f$,

(1.3) $\quad i_s \leqq p i_{s+1}$ for $1 \leqq s < f$,

(1.4) $\quad i_1 > (p-1)(i_2 + \ldots + i_f)$.

Then the homology algebra $H_*(S(\infty); Z_p)$ is a free associative commutative graded algebra generated by $\{A(I), I \in Q(p)\}$, where $A(I) = \lambda_{\xi(f)*}(a(I))$[1] for I with length f.

(D) Consider on $Q(p)$ a linear order $<$. Then a basis for the homology module $H_q(S(m); Z_p)$ can be formed with all elements

$$\lambda^m_{r*}(a(I_1)^{c(1)} a(I_2)^{c(2)} \ldots a(I_t)^{c(t)}), \quad t \geqq 0,$$

satisfying the following conditions:

(1.5) $\quad I_1 < I_2 < \ldots < I_t$ are elements of $Q(p)$,

(1.6) $\quad c(k)$ is > 0 or $= 1$ according as $p \dim a(I_k)$ is even or odd,

(1.7) $\quad c(1) \dim a(I_1) + \ldots + c(t) \dim a(I_t) = q$ and $c(1)p^{f(1)} + \ldots + c(t)p^{f(t)} \leqq m$,

where $f(k)$ is the length of I_k.

(E) The height of any element of the cohomology algebra $H^*(S(m); Z_p)$, $1 \leqq m \leqq \infty$, is either ∞ or $\leqq p$ if p is odd, and is ∞ if $p = 2$. The cohomology algebra

1) When p^f occurs as a (lower or upper) suffix, it will be denoted by $\xi(f)$.

$H^*(S(\infty); Z_2)$ is isomorphic as graded algebras to the homology algebra $H_*(S(\infty); Z_2)$ whose structure is known by (C).

(F) Let X be a complex[2] and let $u \in H^*(X; Z_p)$ be even dimensional. Then we have

$$u^{m+n}/ab = (-1)^{ij}(u^m/a)(u^n/b)$$

for $a \in H_i(S(m); Z_p)$ and $b \in H_j(S(n); Z_p)$;

$$u^{\xi(f)}/a(i_1, \ldots, i_f) = c\mathrm{St}^{j(1)} \ldots \mathrm{St}^{j(f)} u$$

where $c \not\equiv 0 \bmod p$, $i_k + j(k) = qp^{f-k}(p-1)$ for $1 \leqq k \leqq f$, and St^j: $H^q(X; Z_p) \longrightarrow H^{q+j}(X; Z_p)$ is the cyclic reduced power. The latter implies that $a(i_1, \ldots, i_f) = 0$ unless $i_k \equiv 0$ or $-1 \bmod 2(p-1)$ for all k.

(G) Denote by $SP^m(S^q)$ the m-fold symmetric product of a q-sphere S^q. Let $u_0 \in H^q(SP^m(S^q); Z_p)$ denote a generator, and assume q is even. Then a homomorphism

$$\varkappa_m: H_i(S(m); Z_p) \longrightarrow H^{qm-i}(SP^m(S^q); Z_p)$$

given by

$$\varkappa_m(a) = u_0{}^m/a$$

is an isomorphism for $i < q$. This is known as Steenrod isomorphism [5].

2. Diagonal homomorphism

Let $\Gamma \subset S(m)$ be a subgroup, and denote by d_*: $H_*(\Gamma; Z_p) \longrightarrow H_*(\Gamma; Z_p) \otimes H_*(\Gamma; Z_p)$ the diagonal homomorphism.

THEOREM 2.1. *Let* $a \in H_*(\Gamma; Z_p)$ *and put*

(i) $$d_*(a) = \textstyle\sum_s a_s' \otimes a_s''.$$

Then, for *any complex* X *and any even dimensional* $u, v \in H^*(X; Z_p)$ *we have*

(ii) $$(uv)^m/a = \textstyle\sum_s (-1)^{d'(s)d''(s)} (u^m/a_s')(v^m/a_s'')$$

with $d'(s) = \dim a_s'$ *and* $d''(s) = \dim a_s''$; *if* Γ *is the finite symmetric group* $S(m)$ *the converse is also true.*

Proof. The first part can be proved by the arguments used by Steenrod to prove the Cartan formula for the cyclic reduced powers (see pp. 219-221 of [4]). We will omit the proof.

We shall prove the second part. Put $Y = SP^m(S^q)$ with even q, and consider a homomorphism

$$\theta: H_i(S(m) \times S(m); Z_p) \longrightarrow H^{2mq-i}(Y \times Y; Z_p)$$

defined by

$$\theta(a' \otimes a'') = (-1)^{\dim a' \dim a''} \varkappa_m(a') \otimes \varkappa_m(a'').$$

Then it follows from (G) that θ is an isomorphism if $i < q$. Denote by p_j^* : $H^*(Y; Z_p) \longrightarrow H^*(Y \times Y; Z_p)$ the homomorphism induced by the j-th projection p_j: $Y \times Y \longrightarrow Y$ $(i=1, 2)$. We have

2) By a complex we mean always a finite regular cell complex.

$$\varkappa_m(a') \otimes \varkappa_m(a'') = (\varkappa_m(a') \otimes 1)(1 \otimes \varkappa_m(a''))$$
$$= (p_1^* \varkappa_m(a'))(p_2^* \varkappa_m(a'')) = (p_1^* (u_0{}^m/a'))(p_2^* (u_0{}^m/a''))$$
$$= ((p_1^* u_0)^m/a)((p_2^* u_0)^m/a) = ((u_0 \otimes 1)^m/a')((1 \otimes u_0)^m/a'').$$

Therefore, putting $X = Y \times Y$, $u = u_0 \otimes 1$ and $v = 1 \otimes u_0$ in (ii), we obtain

$$(u_0 \otimes u_0)^m/a = \sum_s (-1)^{d'(s)d''(s)} \varkappa_m(a_s') \otimes \varkappa_m(a_s'') = \theta \sum_s (a_s' \otimes a_s'').$$

Consequently the first part implies

$$(u_0 \otimes u_0)^m/a = \theta(d_*(a)).$$

Thus if we assume (ii) we have

$$\theta(d_*(a)) = \theta(\sum_s a_s' \otimes a_s'').$$

Taking a sufficiently large q, this establishes (1).

LEMMA 2.2. *For any even dimensional u, $v \in H^*(X, Z_p)$ we have*

$$(uv)^{\xi(f)}/\,|\,k_1, \dots, k_f\,| = \sum \varepsilon (u^{\xi(f)}/\,|\,m_1, \dots, m_f\,|)(v^{\xi(f)}/\,|\,n_1, \dots, n_f\,|)$$

where $\varepsilon = \varepsilon(m_1, \dots, m_f, n_1, \dots, n_f)$ is -1 to the exponent

$$\sum_{i>j} m_i n_j + \frac{1}{2} p(p-1) \sum_{i=2}^{f} (m_i + \dots + m_f)(n_i + \dots + n_f)$$

and the summation extends over all sequences $(m_1, \dots, m_f, n_1, \dots, n_f)$ such that

$$m_i + n_i = k_i, \qquad p m_i n_i \equiv 0 \text{ mod } 2 \ (1 \leqq i \leqq f).$$

Proof. Note first that the arguments in p. 220 of [4] prove that

$$(uv)^p/e(k) = (-1)^{qrp(p-1)/2} \sum (-1)^{n(pq-m)} (u^p/e(m))(v^p/e(n))$$

where $q = \dim u$, $r = \dim v$ and the summation extends over all (m, n) such that $m+n = k$, $pmn \equiv 0$ mod 2. Next note that

$$u^{\xi(f)}/\,|\,k_1, \dots, k_f\,| = \varepsilon' (u^{\xi(f-1)}/\,|\,k_2, \dots, k_f\,|)^p/e(k_1)$$

with $\varepsilon' = -1$ to the exponent $(k_2 + \dots + k_f)\, p(p-1)/2$. Then the lemma can be proved easily by induction on f.

PROPOSITION 2.3. *We have*

$$d_* a(i_1, \dots, i_f) = \sum \varepsilon(t_1, \dots, t_f, s_1, \dots, s_f)\, a(s_1, \dots, s_f) \otimes a(t_1, \dots, t_f)$$

where the summation extends over all sequences $(s_1, \dots, s_f, t_1, \dots, t_f)$ such that

$$s_j + t_j = i_j, \quad p s_j t_j \equiv 0 \text{ mod } 2,$$
$$s_j \geqq (p-1)(s_{j+1} + \dots + s_f), \quad t_j \geqq (p-1)(t_{j+1} + \dots + t_f)$$

for $j = 1, 2, \dots, f$.

Proof. By a fundamental property of the reduced power, it follows from Lemma 2.2. that

$$(uv)^{\xi(f)}/\varrho_*\,|\,k_1, \dots, k_f\,|$$
$$= \sum \varepsilon(m_1, \dots, m_f, n_1, \dots, n_f)(u^{\xi(f)}/\varrho_*\,|\,m_1, \dots, m_f\,|)(u^{\xi(f)}/\varrho_*\,|\,n_1, \dots, n_f\,|).$$

Therefore, in virtue of Theorem 1.1, we have

$$\varrho_*\,|\,k_1, \dots, k_f\,|$$
$$= \sum \varepsilon(n_1, \dots, n_f, m_1, \dots, m_f)\varrho_*\,|\,m_1, \dots, m_f\,| \otimes \varrho_*\,|\,n_1, \dots, n_f\,|.$$

Noting that

$$k_j = i_j - (p-1)(i_{j+1} + \dots + i_f)$$
$$i_j = k_j + (p-1)(k_{j+1} + pk_{j+2} + \dots + p^{f-j-1} k_f)$$

if $a(i_1, \dots, i_f) = \varrho_* | k_1, \dots, k_f |$, rewrite the above formula in terms of $a(i_1, \dots, i_f)$. Then the required theorem is obtained.

Remark. In the above proposition we may restrict ourselves to elements $a(i_1, \dots, i_f)$ such that $i_j \equiv 0$ or $-1 \bmod 2(p-1)$ for $1 \leqq j \leqq f$ (see (F)). In this case the condition $ps_jt_j \equiv 0 \bmod 2$ is superfluous.

PROPOSITION 2.4. *For* $a \in H_*(S(m); Z_p)$ *and* $b \in H_*(S(n); Z_p)$, *put*

$$d_*(a) = \textstyle\sum_s a_s' \otimes a_s'', \quad d_*(b) = \textstyle\sum_t b_t' \otimes b_t''.$$

Then we have

$$d_*(ab) = \textstyle\sum_{s,t} \varepsilon(s, t)\, a_s'b_t' \otimes a_s''b_t''.$$

where $\varepsilon(s,t)$ *is* -1 *to the exponent* $\dim a_s'' \dim b_t''$.

Proof. The following diagram is commutative:

$$\begin{array}{ccc}
S(m)\times S(n) & \xrightarrow{\quad\mu\quad} & S(m+n) \\
\downarrow d\times d & & \Big|\; d \\
S(m)\times S(m)\times S(n)\times S(n) & & \Big| \\
\downarrow 1\times\tau\times 1 & & \downarrow \\
S(m)\times S(n)\times S(m)\times S(n) & \xrightarrow{\mu} & S(m+n)\times S(m+n)
\end{array}$$

where τ stands for the commutation of the second and the third factors. From this, by the definition of ab (see (B)), the proposition is proved easily.

Denote by $V_p(m)$ the basis for the module $H_*(S(m); Z_p)$ stated in (D). If

$$a = \lambda^m_{r*}\,(a(I_1)^{e(1)} \dots a(I_t)^{e(t)}) \in V_p(m),$$

we write

$$M(a) = \underset{1<j<t}{Max}\, f(j)$$

where $f(j)$ is the length of I_j.

LEMMA 2.5. *Let* $a \in V_p(m)$ *and let* $d_*(a) = \sum_s a_s' \otimes a_s''$ *with* $a_s', a_s'' \in V_p(m)$. *Then we have*

$$M(a_s') \leqq M(a), \quad M(a_s'') \leqq M(a)$$

for all s.

Proof. Note that $d_*\lambda^n_{m*} = (\lambda^n_{m*} \otimes \lambda^n_{m*})d_*$, then the lemma is obvious by Propositions 2.3 and 2.4 and (D).

3. Representation in terms of the basis.

In Proposition 2.3, even if $a(i_1, \dots, i_f)$ is an element of $V_p(p^f)$, the elements $a(s_1, \dots, s_f)$ and $a(t_1, \dots, t_f)$ in the right hand are not necessarily in $V_p(p^f)$. Therefore the determination of the cohomology algebra $H^*(S(m); Z_p)$ from the coalgebra $(H_*(S(m); Z_p), d_*)$ will require to seek formulae to represent any $a(i_1, \dots, i_f)$ in terms of the basis $V_p(p^f)$. This is done in this section. For simplicity we shall explain it only for the case $p=2$.

PROPOSITION 3.1.[3] (I) *If* $a(i_2, \dots, i_f) = \sum a(s_2, \dots, s_f)$ *then* $a(i_1, i_2, \dots, i_f) = \sum a(i_1, s_2, \dots, s_f)$ *for any* i_1.

(II) *If* $i_1 > 2i_2$ *then*

$$a(i_1, i_2, \dots, i_f) = \sum_s \binom{s-i_2-1}{2s-i_1} a(i_1+i_2-s, s, \dots, i_f)$$

with $i_1/2 \leqq s \leqq (i_1+i_2)/2$.

(III) *If* $i_1 = i_2 + \dots + i_f$ *then* $a(i_1, i_2, \dots, i_f) = a(i_2, \dots, i_f)^2$

Proof. In view of (G), the proposition is a direct consequence of the following:

(I)′ If $a(i_2, \dots, i_f) = \sum a(s_2, \dots, s_f)$ then

$$u^{\xi(f)}/a(i_1, i_2, \dots, i_f) = \sum u^{\xi(f)}/a(i_1, s_2, \dots, s_f).$$

(II)′ If $i_1 > 2i_2$ then

$$u^{\xi(f)}/a(i_1, \dots, i_f) = \sum_s \binom{s-i_2-1}{2s-i_1} u^{\xi(f)}/a(i_1+i_2-s, s, \dots, i_f).$$

(III)′ If $i_1 = i_2 + \dots + i_f$ then

$$u^{\xi(f)}/a(i_1, \dots, i_f) = u^{\xi(f)}/a(i_2, \dots, i_f)^2,$$

where u is any q-dimentional mod 2 cohomology class of any complex (q: even), and $\xi(f) = 2^f$. Using (F) these are proved as follows.

If $a(i_2, \dots, i_f) = \sum a(s_2, \dots, s_f)$ then we have

$$\mathrm{Sq}^{j(2)} \dots \mathrm{Sq}^{j(f)} u = u^{\xi(f-1)}/a(i_2, \dots, i_f)$$
$$= \sum u^{\xi(f-1)}/a(s_2, \dots, s_f) = \sum \mathrm{Sq}^{t(2)} \dots \mathrm{Sq}^{t(f)} u$$

with $i_k + j(k) = 2^{f-k}q$ and $s_k + t(k) = 2^{f-k}q$ for $1 \leqq k \leqq f$. Therefore, if we put $i_1 = 2^{f-1}q - j(1)$ we obtain

$$u^{\xi(f)}/a(i_1, i_2, \dots, i_f) = \mathrm{Sq}^{j(1)} \mathrm{Sq}^{j(2)} \dots \mathrm{Sq}^{j(f)} u$$
$$= \sum \mathrm{Sq}^{t(1)} \mathrm{Sq}^{t(2)} \dots \mathrm{Sq}^{t(f)} u = \sum u^{\xi(f)}/a(i_1, s_2, \dots, s_f),$$

which is (I)′. Assume $i_1 > 2i_2$ then $j(1) < 2j(2)$. Therefore, in virtue of the well-known Adem-Cartan relation, we have

$$u^{\xi(f)}/a(i_1, i_2, \dots, i_f) = \mathrm{Sq}^{j(1)} \mathrm{Sq}^{j(2)} \dots \mathrm{Sq}^{j(f)} u$$
$$= \sum_t \binom{j(2)-t-1}{j(1)-2t} \mathrm{Sq}^{j(1)+j(2)-t} \mathrm{Sq}^t \mathrm{Sq}^{j(3)} \dots \mathrm{Sq}^{j(f)} u$$
$$= \sum_s \binom{s-i_2-1}{2s-i_1} \mathrm{Sq}^j \mathrm{Sq}^t \mathrm{Sq}^{j(3)} \dots \mathrm{Sq}^{j(f)} u$$
$$= \sum_s \binom{s-i_2-1}{2s-i_1} u^{\xi(f)}/a(i_1+i_2-s, s, i_3, \dots, i_f)$$

with $s = 2^{f-1}q - t$ and $j = 2^{f-1}q - (i_1 + i_2 - s)$. Here we may assume that $2s - i_1 \geqq 0$ and $i_1 + i_2 - s \geqq s + i_3 + \dots + i_f \geqq s$. Thus we obtain (II)′. Assume $i_1 = i_2 + \dots + i_f$, then we have

dim $(\mathrm{Sq}^{j(2)} \dots \mathrm{Sq}^{j(f)} u) = 2^{f-1}q - (i_2 + \dots + i_f) = 2q^{f-1} - \mathrm{i}_1 = j(1)$

in $u^{\xi(f)}/a(i_1, \dots, i_f) = \mathrm{Sq}^{j(1)} \dots \mathrm{Sq}^{j(f)} u$. Therefore we obtain

3) It is understood that $a(i_1, i_2, \dots, i_f) = 0$ if $i_j < (i_{j+1} + \dots + i_f)$ for some j. It it easily seen that under this convention (F) is still true.

$$(u^{\xi(f)}/a(i_1, \dots, i_f) = (\mathrm{Sq}^{j(2)} \dots \mathrm{Sq}^{j(f)} u)^2$$
$$= (u^{\xi(f-1)}/a(i_2, \dots i_f))^2 = u^{\xi(f)}/a(i_2, \dots, i_f)^2,$$

which is (III)$'$. This completes the proof of the proposition.

LEMMA 3.2. *Using the properties* (I) *and* (II), *any* $a(i_1, \dots, i_f)$ *can be transformed to a linear combination of elements* $a(s_1, \dots, s_f)$ *such that* $s_j \leqq 2s_{j+1}$ *for* $1 \leqq j < f$.

Proof. This is done by induction on the length f and the first term i_1 of $(i_1, \dots, i_f)$. By the hypothesis of induction, $a(i_2, \dots, i_f)$ is a linear combination of $a(s_2, \dots, s_f)$ such that $s_j \leqq 2s_{j+1}$ for $2 \leqq j < f$. Therefore, by (I), $a(i_1, i_2, \dots, i_f)$ is a linear combination of the elements $a(i_1, s_2, \dots, s_f)$. Thus we may assume $i_1 > 2i_2$, $i_2 \leqq 2i_3, \dots, i_{f-1} \leqq 2i_f$ for $a(i_1, \dots, i_f)$, In view of (II) we have

$$a(i_1, \dots, i_f) = \sum_s \binom{s-i_2-1}{2s-i_1} a(i_1+i_2-s, s, \dots, i_f)$$

where $i_1/2 \leqq s \leqq (i_1 + i_2)/2$. Since $s \geqq i_1/2 > i_2$ we have $i_1 + i_2 - s < i_1$. Therefore, by the hypothesis of induction, $a(i_1 + i_2 - s, s, \dots, i_f)$ and so $a(i_1, \dots, i_f)$ can be transformed as claimed. This completes the proof.

THEOREM 3.3. *Using the properties* (I) - (III), *any* $a(i_1, \dots, i_f)$ *can be transformed to a linear combination of elements of* $V_2(s^f)$.

Proof. We use induction on f. In view of Lemma 3.2 we may assume that $a(i_1, \dots, i_f)$ satisfies $i_j \leqq 2i_{j+1}$ for $1 \leqq j < f$. Since $a(i_1, \dots, i_f) = 0$ if $i_1 < i_2 + \dots + i_f$, we may further assume that $i_1 = i_2 + \dots + i_f$. Then by (III) we have $a(i_1, i_2, \dots, i_f) = a(i_2, \dots, i_f)^2$. Therefore the hypothesis of induction proves the theorem.

A special case of (II) is that

$$a(2s+1, 0, \dots, 0) = 0 \tag{3.4}$$

if the length is > 1. A corresponding result is obtained for $p > 2$, and this will be used later.

LEMMA 3.5. *Let* $p > 2$. *If the length is* > 1 *and* $s \not\equiv 0$ *mod* p *then we have*

$$a(2s(p-1), 0, \dots, 0) = 0.$$

Proof. If we write the formula corresponding to (II) in the case $p > 2$, the lemma will be its special case. However, we prefer to give a direct proof. In virtue of (G) it suffices to prove

$$u^{\xi(f)}/a(2s(p-1), 0, \dots, 0) = 0$$

for any even dimensional $u \in H^q(X; Z_p)$. Put

$$v = u^{\xi(f-2)}, \ r = \dim v = qp^{f-2}.$$

Then by (F) we have

$$u^{\xi(f)}/a(2s(p-1), 0, \dots, 0)$$
$$= c\mathrm{St}^{q\xi(f-1)-2s)(p-1)} u^{\xi(f-1)}$$
$$= c\mathfrak{P}^{rp/2-s} v^p.$$

Since $\mathfrak{P}^i v = 0$ if $i > r/2$, it follows from the Cartan formula that

$$\mathfrak{P}^{rp/2-s} v^p = \sum (\mathfrak{P}^{r/2-s(1)} v) \dots (\mathfrak{P}^{r/2-s(p)} v)$$

summed over all sequences of non-negative integers $(s(1), \ldots, s(p))$ whose sum is s. If $s \not\equiv 0 \bmod p$ this is clearly 0. Thus the lemma is proved.

4. Cohomology algebra $H^*(S(4); Z_2)$

We shall in this section prove

THEOREM 4.1. *The cohomology algebra* $H^*(S(4); Z_2)$ *is a commutative associative graded algebra generated by* x_1, x_2, y *subject to a relation* $x_1 y = 0$, *where* $\dim x_1 = 1$, $\dim x_2 = 2$ *and* $\dim y = 3$.

By (D) it follows that a basis $V_2(4)$ for the module $H_*(S(4); Z_2)$ can be formed by elements of the following type:

$$a(i+j)a(j) \qquad (i \geqq 0,\ j \geqq 0),$$
$$a(i+j,\ j) \qquad (j \geqq i > 0)$$

where we regard $a(0)$ as the generator of $H_0(S(2); Z_2)$. Consider the dual basis $V_2{}^*(4) = \{a^*,\ a \in V_2(4)\}$ for the module $H^*(S(4); Z_2)$, and put

$$x_1 = (a(1)a(0))^*, \quad x_2 = (a(1)^2)^*, \quad y = a(2,1)^*.$$

For any q, order the subset of q-dimensional elements of $V_2(4)$ linearly as follows:

$$a(i+j)\,a(j) < a(s+t)a(t) \quad \text{if } j < t,$$
$$a(i+j,\ j) < a(s+t,\ t) \quad \text{if } j < t,$$
$$a(i+j)\,a(j) < a(s+t,\ t).$$

Then the theorem is a direct consequence of the following.

LEMMA 4.2. *For* $i \geqq 0$, $j \geqq 0$, $k > 0$ *and* $a \in V_2(4)$, *we have*

(i) $$< x_1{}^i x_2{}^j,\ a > = \begin{cases} 1 & \text{if } a = a(i+j)a(mj), \\ 0 & \text{if } a < a(i+j)a(j); \end{cases}$$

(ii) $$< x_2{}^j y^k,\ a > = \begin{cases} 1 & \text{if } a = a(2k+j,\ k+j) \\ 0 & \text{if } a < a(2k+j,\ k+j); \end{cases}$$

(iii) $x_1 y = 0$

Proof. It follows from Propositions 2.3 and 2.4 that

$$< x_1{}^i x_2{}^j,\ a(s+t)a(t) > = < x_1{}^i x_2{}^{j-1} \otimes x_2,\ d_*(a(s+t)a(t)) >$$
$$= < x_1{}^i x_2{}^{j-1},\ a(s+t-1)\,a(t-1) >.$$

Therefore induction on $i+j$ proves (i). In view of Lemma 2.5 we have

$$< x_2{}^j y^k,\ a(s+t)a(t) > = < x_2{}^j y^{k-1} \otimes y,\ d_*(a(s+t)\,a(t)\,) > = 0;$$

since $a(3,0) = 0$ by (3.4), it follows from Proposition 2.3 that

$$< x_2{}^j y^k,\ a(s+t,\ t) > = < x_2{}^j y^{k-1} \otimes y,\ d_* a(s+t,\ t) >$$
$$= < x_2{}^j y^{k-1},\ a(s+t-2,\ t-1) >,$$

hence induction on $j+k$ proves (ii). The element of $V_2(4)$ with dimension 4 are $a(4)a(0)$, $a(3)a(1)$ and $a(2)^2$. Therefore we have $< x_1 y,\ a > = 0$ for any $a \in V_2(4)$, hence $x_1 y = 0$. This completes the proof.

5. On the cohomology algebra $H^*(S(p^f); Z_p)$

Consider the dual basis $V_p^* = \{a^*,\ a \in V_p(p^f)\}$ for the module $H^*(S(p^f); Z_p)$ and put

$$x = (\lambda_{2*}^{\xi(f)}(a(1))^*, \quad y = (a(2^{f-1}, \dots, 2, 1))^* \qquad \text{for } p = 2,$$
$$x = (\lambda_{p*}^{\xi(f)} a(2p-2))^*, \quad y = (a(2p^{f-1}(p-1), \dots, 2p(p-1), 2(p-1))^* \qquad \text{for } p > 2.$$

Then we have

LEMMA 5.1. *$xy = 0$ if $f > 1$.*

Proof. It follows from Lemma 2.5 that $\langle xy, a\rangle = 0$ for $a \in V_p(p^f)$ such that $M(a) < f$. If $a \in V_p(p^f)$ and $M(a) = f$ then $a = a(i_1, \dots, i_f)$. Therefore it suffices to prove that

$$\langle xy, a(i_1, \dots, i_f) \rangle = 0$$

for $a(i_1, \dots, i_f) \in Q(p)$. For this purpose we show that there is no element $a(I) = a(i_1, \dots, i_f) \in Q(p)$ such that $\dim a(I) = \dim xy = 2(p^f + p - 2)$. Since the proof for the case $p = 2$ is similar we assume $p > 2$. It follows from (1.3) and (1.4) that

$$p^{f-1} i_f + (p^{f-2} + \dots + 1) \leqq \dim a(I) \leqq (p^{f-1} + \dots + 1)\, i_f.$$

Therefore if $i_f \geqq 4(p-1) - 1$ then $\dim a(I) < 2(p^f + p - 2)$, and if $i_f \leqq 2(p-1)$ then $\dim a(I) < 2(p^f + p - 2)$.[4] By (1.2) this shows that if $a(i_1, \dots, i_f) \in Q(p)$ then its dimension is not $2(p^f + p - 2)$. Thus the proof is complete.

THEOREM 5.2. *For $f > 1$ the cohomology algebra $H^*(S(p^f); Z_p)$ can not be a Hopf algebra.*

Proof. Since the result for $p = 2$ is proved similarly, we assume $p > 2$. Suppose that $H^*(S(p^f); Z_p)$ is a Hopf algebra. Then, by Borel's theorem, $H^*(S(p^f); Z_p)$ is isomorphic as algebra to a tensor product of A_i ($i \in \mathrm{I}$), where A_i is a canonical Hopf algebra with one generator x_i (see [1]). Since it follows from (D) that $2p-2$ is the least of even j such that $H^j(S(p^f); Z_p) \neq 0$, we may regard that $x = x_i$ for some $i \in \mathrm{I}$. Therefore it is easily seen from Lemma 5.1 that there is $z \in H^*(S(p^f); Z_p)$ such that $y = xz$. It follows from Lemma 3.5 and (F) that if $a(i_1, \dots, i_f)$ has dimension $2p-2$ then $a(i_1, \dots, i_f) = 0$. Therefore by Proposition 2.3 we have

$$\langle y, a_0 \rangle = \langle xz, a_0 \rangle = \langle x \otimes z, d_* a_0 \rangle = 0$$

for $a_0 = a(2p^{f-1}(p-1), \dots, 2p(p-1), 2(p-1))$. This contradicts with the definition of y. Thus $H^*(S(p^f); Z_p)$ can not be a Hopf algebra if $f > 1$.

6. On the cohomology algebra $H^*(S(\infty); Z_p)$

By Borel's theorem it follows from (B) and (E) that if p is odd the algebra $H^*(S(\infty); Z_p)$ is isomorphic to a tensor product of

(1) exterior algebras with one generator of odd dimension,

---

4) In these proofs the assumption $f > 1$ is needed.

(2) polynomial algebras with one generator of even dimension,

(3) truncated polynomial algebra with one generator of even dimension and height p.

(see [1]). Obviously the type (1) and (2) actually appear in the decomposition. In this section we shll prove that *the type* (3) *also actually appears*. Comparing this with (C) it follows that the algebra $H_*(S(\infty); Z_p)$ and $H^*(S(\infty); Z_p)$ are not isomorphic if p is odd. Recall that if $p=2$ these are isomorphic (see (E)).

It is obvious that the above statement is a direct consequence of the following:

THEOREM 6.1. *If p is odd there exists an even dimensional element x in $H^*(S(\infty); Z_p)$ such that*

$$x^k \neq 0 \ (1 \leqq k < p), \quad x^p = 0$$

and x is not decomposable.

Proof. Let V_p denote the set of all elements

$$A = A(i_1)^{c(1)} \dots A(I_t)^{c(t)}$$

satisfying the conditions (1.5) and (1.6). Then it follows from (C) that V_p is a basis for the module $H_*(S(\infty); Z_p)$. Consider the dual basis V_p^* for the module $H^*(S(\infty); Z_p)$, then it will be proved that

$$(A(2(p-1)^2-1,\ 2(p-1)-1))^* \in H^*(S(\infty); Z_p)$$

has the properties requested for x.

For simplicity of notation, we put $A_0 = A(2(p-1)^2-1,\ 2(p-1)-1)$. The dimension of A is $2(p^2-p-1)$. We shall first prove that

$$A^{*k}_0 = k!\, A^{*k}_0 \text{ for } 1 \leqq k \leqq p,$$

namely, for $A \in V_p$, we have

$$(6.2) \qquad <A_0^{*k},\ A> = \begin{cases} k! & \text{if } A=A_0^k, \\ 0 & \text{if } A \neq A_0^k. \end{cases}$$

Let $A(i_1, \dots, i_f) \in Q(p)$ and $f \geqq 3$, then it follows from (1.2) and (1.4) that $i_1 + \dots + i_f \geqq 2p^3-2p^2-3$, so that we have

$$\dim A(i_1, \dots, i_f) - \dim A_0^k \geqq (2p^3-2p^2-3)-p(2p^2-2p-2) = 2p-3 > 0$$

because of $1 \leqq k \leqq p$. Consequently we may assume that the length of each I_j in A is $\leqq 2$.

To prove (6.2) we use induction on k. Let

$$(6.3) \qquad d_*A(I_j) = \dots + b_j A_0 \otimes B_j + \dots$$

be the represntation of $d_*A(I)$ in terms of a basis $\{A' \otimes A'',\ A',\ A'' \in V_p\}$ for the module $H_*(S(\infty); Z_p) \otimes H_*(S(\infty); Z_p)$. Then it follows from (B) that

$$\begin{aligned} &< A_0^{*k},\ A > \ = \ < A_0^* \otimes A_0^{*k-1},\ d_*A > \\ &= < A_0^{*k-1},\ b_1 B_1 A(I_1)^{c(1)-1} A(I_2)^{c(2)} \dots A(I_t)^{c(t)} > \\ &+ \dots\dots\dots\dots\dots\dots \\ &+ < A_0^{*k-1},\ b_t A(I_1)^{c(1)}\ A(I_2)^{c(2)} \dots A(I_t)^{c(t)-1} B_t >. \end{aligned}$$

Assume now $< A_0^{*k}, A > \neq 0$. Then the hypothesis of induction implies that

$$(6.4) \qquad A_0^{k-1}=cb_jB_jA(I_1)^{c(1)} \dots A_j(I_1)^{c(j)-1} \dots A(I_t)^{c(t)}$$

for some j, say $j(0)$, where $c \neq 0$. Since $A_0^{k-1} \neq 0$ by (C), we have $b_{j(0)} \neq 0$. Therefore we see from (6.3) that the length of $I_{j(0)}$ is 2. Multiplying $A(I_{j(0)})$ to (6.4) we have

$$(6.5) \qquad A_0^{k-1}A(I_{j(0)})=cb_{j(0)}B_{j(0)}A.$$

It is seen from (6.3) that $B_{j(0)} \neq A(I_{j(0)})$, consequently $B_{j(0)}=A_0^{m-1}$ for some m $(1 \leqq m \leqq k)$. Now (6.3) implies

$$\dim A(I_{j(0)}) = \dim A_0 + \dim B_{j(0)} = m \dim A_0 = 2m(p^2-p-1).$$

However, since $I_{j(0)} \in Q(p)$ and its length is 2, it follows from (1.2)—(1.4) that

$$2(tp^2-t-1) \geqq \dim A(I_{j(0)}) \geqq 2(tp^2-tp-1) \qquad (t=1, 2, \dots).$$

This shows that m must be 1. Hence $B_{j(0)}=1$, and by (6.3) we have $A(I_{j(0)})=A_0$. Thus by (6.5) we obtain $A=A_0^k$. Namely we have proved that $< A^{*k}, A > =0$ if $A \neq A_0^k$. On the other hand, since $d_*(A_0)=1 \otimes A_0+A_0 \otimes 1$, we have

$$d_*(A_0^k)=1 \otimes A_0^k+kA_0 \otimes A_0^{k-1}+ \dots +A_0^k \otimes 1,$$

and so

$$< A^{*k}_0, A_0^k > = < A_0^* \otimes A_0^{*k-1}, d_*A_0^k > = k < A_0^{*k-1}, A_0^{k-1} > = k!.$$

This ends the proof of (6.2), and we proved $A_0^{*k} \neq 0$ $(1 \leqq k < p)$ and $A_0^{*p}=0$.

Next we must prove that A_0^* is not decomposable. Assume that $A_0^* =\sum_j y_jz_j$ with $\dim y_j > 0$ and $\dim z_j>0$. Then, since $d_*A_0= I \otimes A_0 + A_0 \otimes 1$, we have

$$1=<A_0^k, A_0> =\sum_j < y_jz_j, A_0 > =\sum_j < y_j \otimes z_j, d_*A_0 > = 0,$$

which is a contradiction. Thus A_0^* is not decomposable. This completes the proof.

References

[1] J. Milnor and J. Moore, *On the structure of Hopf algebras* (mimeographed).

[2] M. Nakaoka, *Decomposition theorem for homology groups of symmetric groups*, Ann of Math., **71** (1960), 16-42.

[3] M. Nakaoka, *Homology of infinite symmetric group*, Ann. of Math., **73** (1961), 229-257.

[4] N. Steenrod, *Cyclic reduced powers of cohomology classes*, Proc. Nat. Acad. Sci., U. S. A., **39** (1953), 210-223.

[5] N. Steenrod, *Cohomology operations and obstructions to extending continuous functions*, Colloquium Lecture, Princeton University (1957).