ACTA MATHEMATICA VIETNAMICA
Volume 18, Number 2, 1993

MODULAR INVARIANTS AND THE mod p COHOMOLOGY ALGEBRA OF THE INFINITE SYMMETRIC GROUP

NGUYEN HUU VIET HUNG

Abstract. We determine the mod p cohomology algebra of the infinite symmetric group for p an odd prime by using what we call the Dickson characteristic classes. These classes are constructed by means of the Dickson-Mùi invariants of $GL(n,\mathbb{Z}_p)$ on the algebra $E(x_1,\dots,x_n)\otimes\mathbb{Z}_p[y_1,\dots,y_n]$. They are closely related to the classical Chern classes.

Introduction

Cohomology of symmetric groups was first studied by Steenrod [23],[24],[25],[26] in close connection with his history on cohomology operations and then by several authors (see Nakaoka [10],[11],[12], Nakamura [9], Cardenas [1], Quillen [20],[21], Mùi [4] ...). It is applied to investigate iterated loop spaces, configuration spaces and homotopy of spheres (see e.g. Priddy [19], May [7], Nishida [18]).

Let Σ_m be the symmetric group of m letters and $\mathbb{Z}_p$ the prime field of p elements. Nakaoka has computed in [10] the module $H^*(\Sigma_m;\mathbb{Z}_p)$ by a geometrical method using symmetric products of spheres. Independently, Nakamura has determined in [9] this module by means of Cartan's work on homology of the Eilenberg-MacLane spaces $K(\mathbb{Z},n)$.

Eventually, the algebra structure of $H^*(\Sigma_m;\mathbb{Z}_p)$ became the next important target. The algebra $H^*(\Sigma_m;\mathbb{Z}_p)$ has been computed for $m<p^2$ in Steenrod [27; V.7], for $m=4$ in Nakaoka [12] and for $m=p^2$, p odd in Cardenas [1]. To deal

Received December 24, 1992.
1980 *AMS subject classification.* Primary 55R40, Secondary 57R20.
Key words and phrases. Modular invariants, Cohomology of groups.

with the general case, in the last two decades there was an algebraic approach offered by Quillen [20] and Mùi [4]. Quillen showed that the homomorphism

$$Res\ : H^*(\Sigma_m; \mathbb{Z}_p) \to \prod_A H^*(A; \mathbb{Z}_p)$$

induced by the restrictions $Res\ (A, \Sigma_m) : H^*(\Sigma_m; \mathbb{Z}_p) \to H^*(A; \mathbb{Z}_p)$ is injective, where the direct product runs over all maximal elementary abelian p-subgroups A of Σ_m. Further, after developing the classical modular invariant theory of Dickson [3], Huỳnh Mùi in [4] has computed the image of the restriction $Res\ (A, \Sigma_m)$ in the important case where $m = p^n$ and A is a maximal elementary abelian p-subgroup of order p^n and indicated how to consider the remaining cases.

The purpose of this paper is to apply invariant theory to determine the cohomology algebra of the infinite symmetric group

$$H^*(\Sigma_\infty; \mathbb{Z}_p) = \varprojlim_m H^*(\Sigma_m; \mathbb{Z}_p)$$

for p an odd prime. By the same method, we have computed this algebra for $p = 2$ in [13],[16]. Our main idea to reach this end has been explained in [16]. For the convenience of the readers we recall it briefly here.

First we determine the homology coalgebra $H_*(\Sigma_\infty; \mathbb{Z}_p)$ in which the comultiplication

$$\Delta : H_*(\Sigma_\infty; \mathbb{Z}_p) \to H_*(\Sigma_\infty; \mathbb{Z}_p) \otimes H_*(\Sigma_\infty; \mathbb{Z}_p)$$

is induced by the diagonals $\Sigma_m \to \Sigma_m \times \Sigma_m (m \geq 1)$. Then by passage to the dual we obtain the algebra $H^*(\Sigma_\infty; \mathbb{Z}_p)$.

Perhaps, the most important step in our paper is to compute the diagonal map Δ. According to Nakaoka [11], $H_*(\Sigma_\infty; \mathbb{Z}_p)$ is equipped also with a Hopf algebra structure of which Δ is the comultiplication. Nakaoka himself studied this Hopf algebra. He offered a generator system for the Hopf algebra in [11] and formulated Δ in terms of these generators in [12]. Since his formula is quite complicated, one would face with serious problems if one desires to follow Nakaoka's geometrical way.

To overcome the difficulty, we introduce the Dickson elements in $H_*(\Sigma_\infty; \mathbb{Z}_p)$ by means of the Dickson-Mùi invariants of the general linear groups $GL(n, \mathbb{Z}_p)$. The Hopf algebra structure of $H_*(\Sigma_\infty; \mathbb{Z}_p)$ is simply described in terms of the Dickson elements. We have obtained this description for $p = 2$ in [13] by combining the geometrical approach based on the "global" results of Nakamura [9] with the algebraic approach based on the "local" results of Mùi [4]. In this paper, the description of $H_*(\Sigma_\infty; \mathbb{Z}_p)$ will be made by a mostly algebraic approach.

Considering the dual version we determine the algebra $H^*(\Sigma_\infty; \mathbb{Z}_p)$ by constructing what we call the (universal mod p) Dickson characteristic classes. It should be mentioned that in both cases where p is either even or odd, the free Dickson classes are derived from Dickson's invariants. Meanwhile, the nilpotent Dickson classes, which occur only in the case of odd p, are derived from Mùi's invariants. At some special dimensions, free Dickson classes "become" mod p reduced Chern classes (resp. Stiefel-Whitney classes for $p = 2$).

We think that it would be interesting to study Dickson classes for permutation representations of finite groups and for finite coverings over paracompact spaces. The close relationships between Dickson classes, Chern classes (resp. Stiefel-Whitney classes when $p = 2$) and the Dickson-Mùi invariants permit us to predict that Dickson classes measure the obstructions for the existence of certain structures, which would be richer than those measured by Chern classes (resp. Stiefel-Whitney classes).

Dickson classes have been used to determine the mod p cohomology algebra of the iterated loop space $\Omega^n S^n$ for $p = 2$ in [14] and for p an odd prime in [17].

Throughout this paper, the coefficient ring is allways assumed to be $\mathbb{Z}_p$ with p an odd prime.

The paper is organized as follows:

§1. Preliminaries

§2. The Hopf algebra $H_*(\Sigma_\infty)$ and the Dickson elements

§3. The p^r-th power of the Dickson elements

§4. The Dickson elements as free generators of the algebra $H_*(\Sigma_\infty)$

§5. Dickson characteristic classes and the algebra $H^*\Sigma_\infty$

§6. The algebraic relations between the Dickson classes

After recalling some needed information in Section 1, we derive in Section 2 the Dickson elements of $H_*(\Sigma_\infty)$ from the coinvariants of the groups $GL(m, \mathbf{Z}_p)$. The main theorem of Section 2 is proved in the next two sections. In Section 5 we construct the Dickson classes and determine the algebra $H^*(\Sigma_\infty)$. Finally, we postpone until Section 6 the proof for the lemata of Section 5 on the algebraic relations between the Dickson classes.

The main results of the paper have been announced in [15].

Recently, we have learnt that the classes we named after Dickson were independently studied for $p = 2$ in [6; Chapter 3] without detailed proofs. The algebra $H^*(\Sigma_\infty; \mathbf{Z}_p)$ was also computed by Nakaoka [11] for $p = 2$ and by Madsen and May (unpublished) for p an odd prime (see [28], p .31). However, the algebraic and geometrical nature of the generators given by them was not specified.

ACKNOWLEDGEMENT. The author expresses his warmest thanks to Professor H. Mùi for several fruitful suggestions and discussions.

1. Preliminaries

For the convenience of the readers we briefly sketch in the first part of this section the Steenrod theory on the homology of the wreath products of finite groups.

Let E be a cyclic group of order p and G a finite group. We denote by $E \int F$ the semi-product $G^p \tilde{\times} E$, where E acts on G^p by cyclic permutations of the factors.

Steenrod showed that

$$H_*(G \textstyle\int E) \cong H_*(E; (H_*G)^p) \cong H_*(H_*(G)^p \otimes_E W),$$

where $W = WE$ means an E-free acyclic complex. So one can define the Steenrod map in homology as follows

$$P = P_* : H_*(G) \to H_*(G \textstyle\int E),$$

$$P(x) = x^p \otimes_E 1.$$

The map is natural but not a homomorphism of modules in general.

Next we pass to the dual version.

Let BG be a regular classifying complex of G. In Chapter VI of [27] Steenrod defined the natural map

$$P = P^* : H^q(G) = H^q(BG) \to H^{pq}(BG^p \otimes_E W) = H^{pq}(G\textstyle\int E),$$

which brings each cohomology class represented by q-cocycle $u : BG \to \mathbb{Z}_p$ to the class Pu represented by the E-equivariant pq-cocycle

$$u^p \otimes \epsilon : BG^p \otimes W \to \mathbb{Z}_p,$$

where $\epsilon : W \to \mathbb{Z}_p$ denotes the augmentation of W.

The map P is not a homomorphism of modules, but it preserves the multiplication up to sign. Furthermore, we observe that

$$P(u+v) - Pu - Pv \in \text{Im } T$$

for any $u, v \in H^*(G)$, where T is the transfer $H^*(G^p) \to H^*(G \int E)$ induced from the inclusion $1 \subset E$. So P gives rise to the homomorphism

$$\bar{P} : H^*(G) \to H^*(G\textstyle\int E)/\text{Im } T.$$

Let $l : G \int E \to E$ denote the projection. The induced homomorphism $l^* : H^*(E) \to H^*(G \int E)$ equips $H^*(G \int E)$ with a structure of module over $H^*(E)$.

Let $d^* : H^*(G \int E) \to H^*(G \times E)$ be the restriction. It is obviously a homomorphism of $H^*(E)$-modules. Since $Ker\ d^* = \text{Im } T$(cf. Steenrod [27]), d^* induces the homomorphism

$$\bar{d}^* : H^*(G\textstyle\int E)/\text{Im } T \to H^*(G \times E).$$

1.1. THEOREM (STEENROD [27]).

(i) We have a split exact sequence of $H^*(E)$-modules

$$H^*(G^p) \xrightarrow{T} H^*(G\textstyle\int E) \xrightarrow{d^*} H^*(G \times E).$$

Then we obtain an isomorphism of $H^*(E)$-modules

$$H^*(G\textstyle\int E) = \text{Im } T \oplus \text{Im } \bar{P} \otimes H^*(E).$$

Here Im T is a trivial module over $H^*(E)$ and Im $\bar{P}\otimes H^*(E)$ is a free module over $H^*(E)$ where the action of $\omega\in H^*(E)$ is defined by the multiplication of $1\otimes\omega$.

(ii) $d^*P = d^*\bar{P}$ is a monomorphism and d^* induces an isomorphism

$$d^* : Im\ \bar{P}\otimes H^*(E) \cong d^*PH^*(G).d^*l^*H^*(E).$$

(iii) Denote $j^* = Res(G^p, G\int E)$. Then Im $j^* = H^*(G^p)^E$, and j^* gives rise to the isomorphism $j^* :$ Im $T \cong$ Im j^*T. So we get a monomorphism

$$(j^*, d^*) : H^*(G\textstyle\int E) \to H^*(G^p)\times H^*(G\times E).$$

If we need to clarify the source and target, then T, P and $\bar{P}$ will be denoted by $T(G\int E, G)$, $P(G\int E, G)$ and $\bar{P}(G\int E, G)$, respectively.

Let us think of Σ_{p^n} as the symmetric group on (the point set of) the vector space $\mathbb{Z}_p^n$ of dimension n over $\mathbb{Z}_p$. Let $E^n = E_1\times\cdots\times E_n$ denote the subgroup of Σ_{p^n} consisting of all translations on $\mathbb{Z}_p^n$, where E_i is the cyclic group of order p generated by the translation defined by the i-th unit vector e^i of $\mathbb{Z}_p^n$, for $1\le i\le n$. Then E^n is a maximal elementary abelian p-subgroup of Σ_{p^n} and $\Sigma_{p^n,p} = E_1\int E_2\int\cdots\int E_n$ is a Sylow p-subgroup of Σ_{p^n}.

Now we apply Steenrod theorem to the case $G = \Sigma_{p^{n-1}}, E = E_n$.

1.2. LEMMA. *Under the identification given in 1.1 (i) we have*

$$\begin{aligned} Ker\ Res\ (E^n, \Sigma_{p^{n-1}}\textstyle\int E) = Im\ \ & T(\Sigma_{p^{n-1}}\textstyle\int E, \Sigma^p_{p^{n-1}}) \\ & \oplus \bar{P}(\Sigma_{p^{n-1}}\textstyle\int E, \Sigma_{p^{n-1}}) Ker\ Res\ (E^{n-1}, \Sigma_{p^{n-1}})\otimes H^*(E). \end{aligned}$$

This lemma can be proved by the same argument as in the case $p=2$ given in [16; 3.12].

Using also Theorem 1.1, Huỳnh Mùi gave in [4; II.2.3 and II.3.8], an alternative proof of the following result.

1.3. LEMMA (QUILLEN [20]). *The homomorphism*

$$H^*(\Sigma_{p^n}) \to H^*(\Sigma^p_{p^{n-1}})\times H^*(E^n)$$

given by the restrictions is injective.

In the remaining part of this section we recall Huỳnh Mùi's computation of the algebra $\mathcal{B}_n(p) = \text{Im Res }(E^n, \Sigma_{p^n})$.

Let $x_1, \ldots, x_n$ be the elements of $H^1(E^n) = Hom(E^n, \mathbf{Z}_p)$ given by $x_j(e^i) = \delta^i_j$ for $1 < i, j \leq n_i$ where δ^i_j means the Kronecker delta. We set $y_j = \beta x_j \in H^2(E^n)$ for $1 \leq j \leq n$, where β denotes the Bockstein operation. It is well-known that

$$H^*(E^n) = E(x_1, \ldots, x_n) \otimes \mathbf{Z}_p[y_1, \ldots, y_n].$$

The Weyl group $W = W_{\Sigma_{p^n}}(E^n) \cong GL(n, \mathbf{Z}_p)$ acts on $H^*(E^n)$ by means of the adjoint isomorphisms. A classical result (see e.g. Steenrod [27; V, 7] asserts that the image of the restriction Res $(E^n, \Sigma_{p^n}) : H^*(\Sigma_{p^n}) \to H^*(E^n)$ satisfies

$$\text{Im Res }(E^n, \Sigma_{p^n}) \subset H^*(E^n)^W = (E(x_1, \ldots, x_n) \otimes \mathbf{Z}_p[y_1, \ldots, y_n])^{GL_n}. \quad (1.4)$$

Here $GL_n = GL(n, \mathbf{Z}_p)$ acts on $E(x_1, \ldots, x_n) \otimes \mathbf{Z}_p[y_1, \ldots, y_n]$ as usual.

To determine $\mathcal{B}_n(p) = \text{Im Res }(E^n, \Sigma_{p^n})$ Huỳnh Mùi first computed in [4] the invariant algebra given in (1.4) as follows.

Following Dickson [3] and Mùi [4] we set

$$L_{n,p} = \begin{vmatrix} y_1 & \cdots & y_n \\ y_1^p & \cdots & y_n^p \\ \cdot & \cdots & \cdot \\ y_1^{p^r} & \cdots & y_n^{p^r} \\ \cdot & \cdots & \cdot \\ y_1^{p^n} & \cdots & y_n^{p^n} \end{vmatrix}, \quad M_{n,s} = \begin{vmatrix} x_1 & \cdots & x_n \\ y_1 & \cdots & y_n \\ \cdot & \cdots & \cdot \\ y_1^p & \cdots & y_n^{p^s} \\ \cdot & \cdots & \cdot \\ y_1^{p^{n-1}} & \cdots & y_n^{p^{n-1}} \end{vmatrix}$$

for $0 \leq r \leq n, 0 \leq s \leq n$. Since $L_{n,r}$ is divisible by $L_{n,n}$ for $0 \leq r < n$ (Dickson [3]) and $M_{n,s_1}, \ldots, M_{n,s_k}$ divisible by $L^{k-1}_{n,n}$ for $0 \leq s_1 < \cdots < s_k < n$ (Mùi [4; I.4.5]) one defines

$$Q_{n,r} = L_{n,r}/L_{n,n} \quad (0 \leq r < n),$$

$$R_{n,s_1,\ldots,s_k} = (-1)^{k(k-1)/2} M_{n,s_1}, \ldots, M_{n,s_k} L^{p-k-1}_{n,n} \quad (0 \leq s_1 < \cdots < s_k < n).$$

1.5. THEOREM (DICKSON [3], HUỲNH MÙI [4;I.4.17]).

$$(E(x_1,\dots,x_n)\otimes \mathbf{Z}_p[y_1,\dots,y_n])^{GL_n} = \mathbf{Z}_p[Q_{n,0},\dots,Q_{n,n-1}]\oplus$$
$$\sum_{k=1}^{n}\oplus \sum_{0\le s_1<\dots<s_k<n} \oplus R_{n,s_1,\dots,s_k}\mathbf{Z}_p[Q_{n,0},\dots,Q_{n,n-1}].$$

The algebraic relations holding between the generators are as follows:

$$R^2_{n,s} = 0$$
$$R_{n,s_1}\dots R_{n,s_k} = (-1)^{k(k-1)/2}R_{n;s_1,\dots,s_k}.Q^{k-1}_{n,0},$$

for $0\le s<n$ *and* $0\le s_1<\dots<s_k<n$.

Further, Huỳnh Mùi determined the image of Res (E^n,Σ_{p^n}).

1.6. THEOREM (H. MÙI [4; II.6.1]). *$\mathcal{B}_n(p) = Im$ Res (E^n,Σ_{p^n}) is the subalgebra of the algebra given in 1.5 generated by $Q_{n,s}, R_{n,s}$ $(0\le s<n), R_{n,r,s}$ $(0\le r<s<n)$.*

1.7. REMARK.

(i) We observe that

$$dim\ Q_{n,s} = 2(p^n-p^s),$$
$$dim\ R_{n,s} = 2(p^n-p^s)-1,$$
$$dim\ R_{n,r,s} = 2(p^n-p^r-p^s).$$

(ii) Let $C_{n,s}$ be the mod p reduced Chern class of dimension $2(p^n-p^s)$ for the natural representation $\Sigma_{p^n}\to U(p^n)$, where $U(p^n)$ denotes the unitary group of degree p^n. According to Quillen, Milgram (see [22]) and Mùi [4; Appendix] one has

$$\text{Res }(E^n,\Sigma_{p^n})C_{n,s} = (-1)^{n+s}Q_{n,s}.$$

2. The Hopf algebra $H_*(\Sigma_\infty)$ and the Dickson elements

In this section we construct the Dickson additive basis for $H_*(\Sigma_\infty)$ derived from the Dickson-Huỳnh Mùi coinvariants of the general linear groups $GL(n,\mathbf{Z}_p)$, $0<n<\infty$. Then we describe the structure of the Hopf algebra $H_*(\Sigma_\infty)$ in terms of the Dickson basis. This description will be proved in the next two sections.

Let ${}_nJ$ be the set of all sequences

$$(H,R)=(h_0,\ldots,h_{n-1};r_1,\ldots,r_t)$$

with h_i, r_j non-negative integers, $0\le r_1<\cdots<r_t<n, t\ge 0$. Following Theorem 1.6, $\mathcal{B}_n(p)$ has the additive basis consisting of all the elements $Q_{(H,R)}=Q_{H,R}$, for $(H,R)\in {}_nJ$, defined as follows

$$Q_{H,R}=\begin{cases}\Pi_{i=0}^{n-1}Q_{n,i}^{h_i}.\Pi_{j=1}^{t/2}R_{n,r_{2j-1},r_{2j}}, & t \text{ even},\\ \Pi_{i=0}^{n-1}Q_{n,i}^{h_i}.\Pi_{j=1}^{(t-1)/2}R_{n,r_{2j-1},r_{2j}}.R_{n,r_t}, & t \text{ odd}.\end{cases} \quad (2.1)$$

To describe the multiplication of the algebra $\mathcal{B}_n(p)$ in terms of this basis we define a partial summation in ${}_nJ$ as follows.

Given $(H,R)=(h_0,\ldots,h_{n-1};r_1,\ldots,r_t)$, $(K,S)=(k_0,\ldots,k_{n-1};s_1,\ldots,s_i)$ in ${}_nJ$, we write $|H|=|K|=n, |R|=t, |S|=i$. Further, suppose $R\cap S=\emptyset$, that means there is no common entry in the sequences R and S. In this case, let R_oS be the monotone increasing sequence obtained from the sequence $R*S=(r_1,\ldots,r_t,s_1,\ldots,s_i)$ by a certain permutation of the coordinates. *The signature of this permutation is denoted by* $\operatorname{sgn}(R,S)$.

2.2. DEFINITION. For $|H|=|K|=n, R\cap S=\emptyset$, we define

$$(H,R)+(K,S)=(H\hat{+}K,R_oS),$$

where

$$H\hat{+}K=\begin{cases}H+K & |R|.|S| \text{ even},\\ H+K+\underbrace{(1,0,\ldots,0)}_{n} & |R|.|S| \text{ odd}.\end{cases}$$

Here the summation in the right hand side is formally defined in terms of the coordinates.

Now it is easy to see that

$$Q_{H,R}.Q_{K,S}=\begin{cases}(-1)^{sgn(S,T)+|S|.|T|}Q_{(H,R)+(K,S)}, & R\cap S=\emptyset,\\ 0 & \text{otherwise}.\end{cases}$$

Let $H_*(n)$ be the coalgebra dual to the algebra $\mathcal{B}_n(p)=\text{Im Res}\,(E^n,\Sigma_{p^n})$, and $q_{H,R}\in H_*(n)$ the dual element of $Q_{H,R}$ with respect to the above mentioned basis of $\mathcal{B}_n(p)$. Considering the dual version of Huỳnh Mùi's Theorem 1.6 one obtains

2.3. COROLLARY. *The comultiplication of $H_*(n)$ is described in terms of the additive basis $\{q_{H,R} \mid (H,R) \in {}_nJ\}$ as follows*

$$\Delta q_{H,R} = \sum_{(K,S)+(L,T)=(H,R)} (-1)^{sgn(S,T)} q_{K,S} \otimes q_{L,T}.$$

Since Res $(E^n, \Sigma_{p^n}) : H^*(\Sigma_{p^n}) \to \mathcal{B}_n(p)$ is surjective, the dual homomorphism

$$i_n : H_*(n) \to H_*(\Sigma_{p^n}) \subset H_*(\Sigma_\infty)$$

is injective.

2.4. DEFINITION. For $(H,R) = (h_0, \ldots, h_{n-1}; r_1, \ldots, r_t)$ we define

$$D_{H,R} = D_{(h_0,\ldots,h_{n-1};r_1,\ldots,r_t)} = (-1)^{\|H,R\|} i_n(q_{H,R}),$$

where

$$\|H,R\| = \sum_i (n+i)h_i + \sum_j r_j.$$

REMARK. $D_{H,R}$ is distinguished by a sign from the element denoted by the same notation in [15; 3.3]. Compare with Remarks 1.7 (ii), and 4.7 (i).

Note that

$$dim\ D_{H,R} = \begin{cases} 2\Sigma_i h_i(p^n - p^i) + tp^n - 2\Sigma_j p^{r_j}, & t \text{ even,} \\ 2\Sigma_i h_i(p^n - p^i) + (t+1)p^n - 2\Sigma_j p^{r_j} - 1, & t \text{ odd.} \end{cases}$$

In particular, $dim\ D_{H,R} = |R|\ (mod 2)$.

2.5. NOTATIONS. We set

$$J = \left(\coprod_{n>0} {}_nJ \right) / \sim .$$

Here the equivalent relation $\sim$ is defined as follows. $(0_n, \emptyset) = ((\underbrace{0, \ldots, 0}_{n}, \emptyset)$ is equivalent to $(0_m, \emptyset)$ for every m, n. Any other element is only equivalent to itself. The equivalent class of $(0_n, \emptyset)$ is denoted by $(\emptyset, \emptyset)$. One gets

$$D_{\emptyset,\emptyset} = D_{0_n,\emptyset} = 1 \text{ in } H_*(\Sigma_\infty).$$

So J is equipped with a partial summation defined as in 2.2 for elements in the same ${}_nJ$.

Let J^+ be the subset of J consisting of all $(h_o, \ldots, h_{n-1}; r_1, \ldots, r_t)$ which satisfies either 1) $h_0 > 0$, 2) t is odd, or 3) $r_1 = 0$. Furthermore, set

$$J^+_{od} = \{(H,R) \in J^+ \mid |R| \text{ is odd } \},$$
$$J^+_{ev} = J^+ \setminus J^+_{od}$$

We now state the main result of this section which describes the structure of the Hopf algebra $H_*(\Sigma_\infty)$.

2.6. THEOREM.

(i) $H_*(\Sigma_\infty)$ is the free graded commutative algebra over $\mathbb{Z}_p$ generated freely by $D_{H,R}$ with $(H,R) \in J^+$. More precisely,

$$H_*(\Sigma_\infty) = E(D_{H,R}; (H,R) \in J^+_{od}) \otimes \mathbb{Z}_p[D_{H,R}; (H,R) \in J^+_{ev}].$$

(ii) Its comultiplication Δ satisfies the formula

$$\Delta D_{H,R} = \sum_{(K,S)+(L,T)=(H,R)} (-1)^{sgn(S,T)+n.|S||T|} D_{K,S} \otimes D_{L,T},$$

where $n = |H| = |K| = |L|$ and $(H,R),(K,S),(L,T) \in J$.

(iii)

$$D^{p^r}_{(h_0,\ldots,h_{n-1};r_1,\ldots,r_t)} = \begin{cases} D_{(\underbrace{0,\ldots,0}_{r\ times},h_0,\ldots,h_{n-1};r_1+r,\ldots,r_t+r)}, & t \text{ even},\\ 0, & t \text{ odd},\end{cases}$$

for $h_0, \ldots, h_{n-1} \geq 0, 0 \leq r_1 < \cdots < r_t < n$.

The part (ii) immediately follows from 2.3 and 2.4. The remaining parts (i) and (ii) will be proved in the next two sections.

3. The p^r-th power of the Dickson elements.

This section is devoted to the proof for part (iii) of Theorem 2.6.

Hinted by Definition 2.4, we choose some elements $\bar{\bar{Q}}_{n,s}$, $\bar{\bar{R}}_{n,s}$, $(0 \leq s < n)$, $\bar{\bar{R}}_{n,r,s}$ $(0 \leq r < s < n)$ in $H^*(\Sigma_{p^n})$ such that their images under Res (E^n, Σ_{p^n}) are $(-1)^{n+s}Q_{n,s}, (-1)^s R_{n,s}$, $(-1)^{r+s}R_{n,r,s}$ respectively.

Let $H^*(n)$ denote the $\mathbb{Z}_p$-submodule spanned by $Q_{H,R}$ for $(H,R) \in {}_nJ$. In general, $H^*(n)$ is not a subalgebra of $H^*(\Sigma_{p^n})$. By Lemma 1.2, we have

$$\begin{aligned} &H^*(\Sigma_{p^n} \int E_{n+1}) \\ &\quad \cong \text{Ker Res}\,(E^{n+1}, \Sigma_{p^n} \int E_{n+1}) \oplus \bar{P} H^*(n) \otimes H^*(E_{n+1}). \end{aligned} \tag{3.1}$$

We denote by $\tilde{Q}_{n+1,s+1}, \tilde{R}_{n+1,s+1}, \tilde{R}_{n+1,r+1,s+1}$ the images of $(-1)^{n+s}\bar{\bar{Q}}_{n,s}$, $(-1)^s \bar{\bar{R}}_{n,s}$, $(-1)^{r+s}\bar{\bar{R}}_{n,r,s}$ respectively, under the composite homomorphism Res $(E^{n+1}, \Sigma_{p^n} \int E_{n+1})P$. These elements generate a subalgebra of $H^*(E^{n+1})$, which is denoted by $\tilde{\mathcal{B}}_n(p)$.

The following lemma claims that $\tilde{Q}_{n+1,s+1}, \tilde{R}_{n+1,s+1}, \tilde{R}_{n+1,r+1,s+1}$ and $\tilde{\mathcal{B}}_n(p)$ are well defined, i.e. they are independent from the choice of $\bar{\bar{Q}}_{n,s}$, $\bar{\bar{R}}_{n,s}$, $\bar{\bar{R}}_{n,r,s}$.

3.2. LEMMA. *Let $d^* = \text{Res}\,(E^{n+1}, E^n \int E_{n+1})$. Then d^*P gives rise to a module isomorphism preserving the product up to sign*

$$d^*P|_{\mathcal{B}_n(p)} : \mathcal{B}_n(p) \to \tilde{\mathcal{B}}_n(p),$$

which sends $Q_{n,s}, R_{n,s}, R_{n,r,s}$ to $\tilde{Q}_{n+1,s+1}, \tilde{R}_{n+1,s+1}, \tilde{R}_{n+1,r+1,s+1}$, respectively.

PROOF. By the naturality of the Steenrod map P we have the commutative diagram

$$\begin{array}{ccccc} H^*(\Sigma_{p^n}) & \xrightarrow{P} & H^*(\Sigma_{p^n} \int E_{n+1}) & \searrow^{\text{Res}} & \\ \text{Res}\downarrow & & \text{Res}\downarrow & & \\ H^*(E^n) & \xrightarrow{P} & H^*(E^n \int E_{n+1}) & \xrightarrow{d^* = \text{Res}} & H^*(E^{n+1}). \end{array} \tag{3.3}$$

So we get

$$\begin{aligned} \tilde{Q}_{n+1,s+1} &= (-1)^{n+s}\text{Res}\,(E^{n+1}, \Sigma_{p^n} \int E_{n+1}) P(\bar{\bar{Q}}_{n,s}) \\ &= (-1)^{n+s} d^*P \text{ Res}\,(E^n, \Sigma_{p^n})(\bar{\bar{Q}}_{n,s}) = d^*P(Q_{n,s}). \end{aligned}$$

Likewise

$$\tilde{R}_{n+1,s+1} = d^*P(R_{n,s}), \tilde{R}_{n+1,r+1,s+1} = d^*P(R_{n,r,s}).$$

On the other hand, according to Theorem 1.1 of Steenrod, d^*P is a monomorphism preserving the product up to sign. Hence we have

$$\tilde{\mathcal{B}}_n(p) = d^*P\mathcal{B}_n(p).$$

The lemma follows.

3.4. LEMMA. *As algebras*

$$Im\ \ Res\,(E^{n+1}, \Sigma_{p^n} \textstyle\int E_{n+1}) \cong \tilde{\mathcal{B}}_n(p) \otimes H^*(E_{n+1}).$$

PROOF. Under the isomorphism 3.1, combining 3.3 and by the fact that Res $(E^{n+1}, \Sigma_{p^n} \int E_{n+1})$ is a homomorphism of $H^*(E_{n+1})$-modules, we obtain

$$\begin{aligned}\text{Im}\ \ \text{Res}\,(E^{n+1}, \Sigma_{p^n} \textstyle\int E_{n+1}) &= \text{Res}\,(E^{n+1}, \Sigma_{p^n} \textstyle\int E_{n+1})(\bar{P}H^*(n) \otimes H^*(E_{n+1}))\\ &= d^*P\ \text{Res}\,(E^n, \Sigma_{p^n})H^*(n) \otimes H^*(E_{n+1})\\ &= d^*P\mathcal{B}_n(p) \otimes H^*(E_{n+1}) = \tilde{\mathcal{B}}_n(p) \otimes H^*(E_{n+1}).\end{aligned}$$

The lemma is proved.

The inclusions $E^{n+1} \subset \Sigma_{p^n} \int E_{n+1} \subset \Sigma_{p^{n+1}}$ induce the commutative diagram

$$\begin{array}{ccc} H^*(\Sigma_{p^n} \textstyle\int E_{n+1}) & \longleftarrow & H^*(\Sigma_{p^{n+1}}) \\ \downarrow & & \downarrow \\ \tilde{\mathcal{B}}_n(p) \otimes H^*(E_{n+1}) & \supset & \mathcal{B}_{n+1}(p) \end{array} \qquad (3.5)$$

Recall that $H^*(E_{n+1}) = E(x_{n+1}) \otimes \mathbb{Z}_p[y_{n+1}]$. So the inclusion in Diagram 3.5 satisfies the following

3.6. LEMMA.

(i)

$$\begin{aligned} Q_{n+1,s+1} &= \tilde{Q}_{n+1,s+1}\ mod\ (y_{n+1}^{p-1}) \quad (0 \le s < n),\\ Q_{n+1,0} &= 0 \qquad mod\ (y_{n+1}^{p-1}). \end{aligned}$$

(ii)

$$R_{n+1,r+1,s+1} = \tilde{R}_{n+1,r+1,s+1}\ mod\ (y_{n+1}^{p-1}) \quad (0 \le r < s < n).$$

Here (y_{n+1}^{p-1}) *denotes the ideal of* $\tilde{B}_n(p)\otimes H^*(E_{n+1})$ *generated by* y_{n+1}^{p-1}.

PROOF. (i) According to Dickson [3] we have

$$Q_{n+1,0} = L_{n+1,n+1}^{p-1}.$$

By the definition of the determinant $L_{n+1,n+1}$, it has the factor y_{n+1}. The second equality follows.

To deal with the first one, we set

$$V_{n+1} = \prod_{c_i\in \mathbf{Z}_p}(c_1y_1+\cdots+c_ny_n+y_{n+1}).$$

Again, according to Dickson [3] we have

$$\begin{aligned} Q_{n+1,s+1} &= Q_{n,s}^p + Q_{n,s+1}.V_{n+1}^{p-1}\\ &= Q_{n,s}^p \bmod (y_{n+1}^{p-1}). \end{aligned}$$

Since the subalgebra $\mathbf{Z}_p[Q_{n,s},\ldots,Q_{n,n-1}] = \mathbf{Z}_p[y_1,\ldots,y_n]^{GL_n}$ is closed under the actions of the Steenrod operations,

$$d^*P(Q_{n,s}) \in \mathbf{Z}_p[Q_{n,0,\ldots},Q_{n,n-1}]\otimes \mathbf{Z}_p[y_{n+1}].$$

According to Steenrod [27; Chapter VII] we have

$$d^*PQ_{n,s} = Q_{n,s}^p \bmod (y_{n+1}).$$

Combining these discussions with the fact that $dim\ Q_{n,s} = 2(p^n-p^s)$, we obtain

$$d^*PQ_{n,s} = Q_{n,s}^p \bmod (y_{n+1}^{p-1}).$$

Hence the first formula of the lemma follows.

(ii) We need the following notation

$$N_{n,t} = \begin{vmatrix} x_1 & \cdots & x_n\\ \hat{y}_1 & \cdots & \hat{y}_n\\ \cdot & \cdots & \cdot\\ \hat{y}_1^{p^t} & \cdots & \hat{y}_n^{p^t}\\ \cdot & \cdots & \cdot\\ \hat{y}_1^{p^n} & \cdots & \hat{y}_n^{p^n} \end{vmatrix} \quad (0<t\le n).$$

Applying the Laplace development to the last columns of the determinants $M_{n+1,r+1}, M_{n+1,s+1}, L_{n+1,n+1}$ we have

$$
\begin{aligned}
&R_{n+1,r+1,s+1}\\
&= -M_{n+1,r+1}.M_{n+1,s+1}.L_{n+1,n+1}\\
&= (L_{n,r+1}.N_{n,s+1} - N_{n,r+1}.L_{n,s+1})L_{n,n}^{p(p-3)} \otimes x_{n+1}y_{n+1}^{p-2} \bmod (y_{n+1}^{p-1}).
\end{aligned}
$$

On the other hand, by Lemma 3.2 we have

$$\tilde{R}_{n+1,r+1,s+1} = d^*P(R_{n,r,s}).$$

According to Steenrod [27; Chapter VII), for each $u \in H^q(E^n)$ we have

$$d^*P(u) = m(q)(\sum_i(-1)^iP^iu \otimes y_{n+1}^{(q-2i)h} + \sum_i(-1)^{i+q}\beta P^iu \otimes x_{n+1}y_{n+1}^{(q-2i)h-1}),$$

where $h = (p-1)/2, m(q) = (h!)^{-q}(-1)^{h(q^2+q)/2}$. A simple computation shows that

$$d^*P(R_{n,r,s}) = (L_{n,r+1}N_{n,s+1} - N_{n,r+1}L_{n,s+1})L_{n,n}^{p(p-3)} \otimes x_{n+1}y_{n+1}^{p-2} \bmod (y_{n+1}^{p-1}).$$

As a consequence, the equality of the part (ii) holds. The lemma is completely proved.

Let $\tilde{H}_*(n)$ be the coalgebra dual to $\tilde{B}_n(p)$. We define $\tilde{Q}_{H,R}$ for $(H,R) \in {}_nJ$ by substituting $Q_{n,s}R_{n,s}, R_{n,r,s}$ by $\tilde{Q}_{n+1,s+1}, \tilde{R}_{n+1,s+1}, \tilde{R}_{n+1,r+1,s+1}$ in 2.1 respectively. Denote by $\tilde{q}_{H,R}$ the dual element of $\tilde{Q}_{H,R}$ with respect to the basis $\{\tilde{Q}_{K,S}|(K,S) \in {}_nJ\}$ for $\tilde{H}^*(n)$. Then, according to Lemma 3.2, the homomorphism

$$
\begin{aligned}
\tilde{H}_*(n) &\to H_*(n)\\
\tilde{q}_{H,R} &\mapsto q_{H,R}, (H,R) \in {}_nJ,
\end{aligned}
$$

is an isomorphism preserving the coproduct up to sign.

Passing Diagram 3.5 to the dual we get the commutative diagram

$$\begin{array}{ccccc} H_*(n) & & \tilde{H}_*(n)\otimes H_*(E_{n+1}) & \xrightarrow{h} & H_*(n+1) \\ \downarrow{\scriptstyle i_n} & & \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle i_{n+1}} \\ H_*(\Sigma_{p^n}) & \xrightarrow{P} & H_*(\Sigma_{p^n}\int E_{n+1}) & \xrightarrow{i} & H_*(\Sigma_{p^{n+1}}) \end{array} \tag{3.7}$$

3.8. LEMMA. *For any $(H,R)=(h_0,\dots,h_{n-1};r_1,\dots,r_t)\in {}_nJ$ with t a non-negative even number, we have*

$$h(\tilde{q}_{(h_0,\dots,h_{n-1};r_1,\dots,r_t)})=q_{(0,h_0,\dots,h_{n-1};r_1+1,\dots,r_t+1)}.$$

By convention, for $t=0, R=(r_1,\dots,r_t)=\emptyset$, we set $(r_1+1,\dots,r_t+1)=\emptyset$.

PROOF. Using Lemma 3.6 we get

$$\begin{aligned} Q^{h_0}_{n+1,1}\cdots Q^{h_{n-1}}_{n+1,n} &= \tilde{Q}^{h_0}_{n+1,1}\cdots\tilde{Q}^{h_{n-1}}_{n+1,n} \bmod (y^{p-1}_{n+1}),\\ Q_{(0,h_0,\dots,h_{n-1};r_1+1,\dots,r_t+1)} &= \tilde{Q}_{(h_0,\dots,h_{n-1};r_1,\dots,r_t)} \bmod (y^{p-1}_{n+1}). \end{aligned} \tag{a}$$

Remark that the dimensions of these elements are divisible by $2p$.

On the other hand, suppose that we are given $(K,S)=(k_0,\dots,k_n;s_1,\dots,s_u)\in {}_{n+1}J$ such that $dim\ Q_{K,S}$ is divisible by $2p$. Obviously, (K,S) must satisfy the following conditons

$$|S|=u \text{ is even.} \tag{b1}$$

$$\text{If } u>0 \text{ and } s_1=0 \text{ then } k_0>0. \tag{b2}$$

Indeed, $Q_{n+1,0}, R_{n+1,s}, R_{n+1,0,s}$ are the only elements whose dimensions are not divisible by $2p$ among the invariants $Q_{n+1,s}, R_{n+1,s}, R_{n+1,r,s}$ (see Remark 1.7 (i)).

Assume that (K,S) satisfies (b2). Using Lemma 3.6 we have

$$Q_{K,S}=0 \bmod (y^{p-1}_{n+1}). \tag{c}$$

Considering the dual version of (a) and (c) we obtain

$$h(\tilde{q}_{H,R})=q_{(0,h_0,\dots,h_{n-1};r_1+1,\dots,r_t+1)}.$$

The lemma is proved.

3.9. LEMMA. $P(D_{H,R}) = (-1)^{\|H,R\|} j(\tilde{q}_{H,R})$ *for any* $(H,R) \in {}_nJ$.

PROOF. Using the isomorphism 3.1 we will show that both sides of the formula are the same function on $H^*(\Sigma_{p^n} \int E_{n+1})$.

(a) Since j is dual to Res $(E^{n+1}, \Sigma_{p^n} \int E_{n+1})$, we get

$$\langle \text{Im } j, \text{Ker Res } (E^{n+1}, \Sigma_{p^n} \int E_{n+1}) \rangle = \langle H_*(\Sigma_{p^n} \int E_{n+1}), 0 \rangle = 0.$$

Hence, by 3.1, the dual pairing gives rise to the homomorphism

$$j(x) : \bar{P}H^*(n) \otimes H^*(E_{n+1}) \to \mathbb{Z}_p$$

for any $x \in H_*(\Sigma_{p^n})$.

On the other hand, by the definition of the Steenrod power map P we obtain

$$\langle \text{Im } P, \text{Ker Res } (\Sigma_{p^n} \times E_{n+1}, \Sigma_{p^n} \int E_{n+1}) \rangle = 0.$$

So, from Theorem 1.1 the dual pairing also gives rise to the homomorphism

$$P(x) : \bar{P}H^*(\Sigma_{p^n}) \otimes H^*(E_{n+1}) \to \mathbb{Z}_p$$

for every $x \in H_*(\Sigma_{p^n})$. Additionally we have

$$\langle P(D_{H,R}), \bar{P}\text{Ker Res } (E^n, \Sigma_p^n) \otimes H^*(E_{n+1}) \rangle = 0$$

for $(H,R) \in {}_nJ$. Then, using Lemma 1.2 and 3.1 we get the following homomorphism induced from the dual pairing

$$P(D_{H,R}) : \bar{P}H^*(n) \otimes H^*(E_{n+1}) \to \mathbb{Z}_p.$$

(b) By the definitions of $\tilde{q}_{H,R}$ and $P(D_{H,R})$ we have

$$\langle j(\tilde{q}_{H,R}), \bar{P}H^*(n) \otimes H^*(E_{n+1})^+ \rangle = \langle \tilde{q}_{H,R}, \tilde{\mathcal{B}}_n(p) \otimes H^*(E_{n+1})^+ \rangle = 0,$$

$$\langle P(D_{H,R}), \bar{P}H^*(n) \otimes H^*(E_{n+1})^+ \rangle = 0.$$

Here $H^*(E_{n+1})^+$ denotes the ideal of all elements of positive degrees in $H^*(E_{n+1})$.

(c) Obviously,

$$\langle P(D_{H,R}), \bar{P}\bar{\bar{Q}}_{K,S} \rangle = \delta^{K,S}_{H,R},$$

where the right hand side is the Kronecker delta. Further,

$$\begin{aligned}\langle j(\tilde{q}_{H,R}), \bar{P}\bar{\bar{Q}}_{K,S}\rangle &= \langle \tilde{q}_{H,R}, \text{Res } (E^{n+1}, \Sigma_{p^n} \textstyle\int E_{n+1}) P\bar{\bar{Q}}_{K,S}\rangle \\ &= \langle \tilde{q}_{H,R}, (-1)^{\|K,S\|} \tilde{Q}_{K,S}\rangle \\ &= (-1)^{\|H,R\|} \delta^{K,S}_{H,R}.\end{aligned}$$

From the discussions (a) (b) (c) the lemma follows.

PROOF OF THEOREM 2.6. (iii). If t is odd, then the formula follows from the commutativity of the algebra $H_*(\Sigma_\infty)$ and the fact that

$$dim\ D_{H,R} = |R| = t\ (\text{mod}2).$$

Assume that t is even. It suffices to prove the formula only in the case $r = 1$. For $(H, R) = (h_0, \ldots, h_{n-1}; r_1, \ldots, r_t)$, combining the commutativity of Diagram 3.7 with 2.4, 3.8 and 3.9 we have

$$\begin{aligned}D_{(0,h_0,\ldots,h_{n-1};r_1+1,\ldots,r_t+1)} &= (-1)^{\|H,R\|+t} i_{n+1}(q_{(0,h_0,\ldots,h_{n-1};r_1+1,\ldots,r_t+1)}) \\ &= (-1)^{\|H,R\|} i_{n+1} h(\tilde{q}_{H,R}) = (-1)^{\|H,R\|} ij(\tilde{q}_{H,R}) \\ &= iP(D_{H,R}) = D^p_{H,R}\end{aligned}$$

The part (iii) of Theorem 2.6 is completely proved.

4. The Dickson elements as free generators of the algebra $H_*(\Sigma_\infty)$

The aim of this section is to prove Theorem 2.6 (i).

Recall that the homomorphism

$$H^*(\Sigma_m) \to \prod_A H^*(A) \tag{4.1}$$

induced by the restrictions Res $(A, \Sigma_m) : H^*(\Sigma_m) \to H^*(A)$ is injective, where the direct product runs over a set of representatives for the conjugacy classes of maximal elementary abelian p-subgroups of Σ_m (see Quillen [20],[21], Huỳnh Mùi [4]).

Huỳnh Mùi determined in [4] such a set of representatives as follows. For a given natural number m, let $A(m) = A_p(m)$ denote the set of all infinite sequences of non-negative integers $M = (m_0, m_1, \ldots)$ such that $m = \Sigma_{n\geq 0} m_n p^n$.

Using the result of Nakaoka [10] on the module $H^*(\Sigma_\infty)$ we can easily check that this module is isomorphic to the source of the epimorphism as graded $\mathbf{Z}_p$-modules of finite type. Hence the epimorphism is actually an isomorphism of algebras.

The proof is complete.

Taking the dual version of Theorem 2.6 we have the following

4.6. REMARKS.

(i) There exist uniquely the elements $\bar{Q}_{n,s}, \bar{R}_{n,s} (0 \le s < n), \bar{R}_{n,r,s} \quad (0 \le r < s < n)$ satisfying the following conditions:

$$\text{Res }(E^n, \Sigma_{p^n})\bar{Q}_{n,s} = (-1)^{n+s} Q_{n,s},$$
$$\text{Res }(E^n, \Sigma_{p^n})\bar{R}_{n,s} = (-1)^{s} R_{n,s},$$
$$\text{Res }(E^n, \Sigma_{p^n})\bar{R}_{n,r,s} = (-1)^{r+s} R_{n,r,s},$$

$$\text{Res }(\Sigma^p_{p^{n-1}}, \Sigma_{p^n})\bar{Q}_{n,s} = \begin{cases} \underbrace{\bar{Q}_{n-1,s-1} \otimes \cdots \otimes \bar{Q}_{n-1,s-1}}_{p \text{ times}} & s > 0, \\ 0 & s = 0, \end{cases}$$

$$\text{Res }(\Sigma^p_{p^{n-1}}, \Sigma_{p^n})\bar{R}_{n,s} = 0$$

$$\text{Res }(\Sigma^p_{p^{n-1}}, \Sigma_{p^n})\bar{R}_{n,r,s} = \begin{cases} \underbrace{\bar{R}_{n-1,r-1,s-1} \otimes \cdots \otimes \bar{R}_{n-1,r-1,s-1}}_{p \text{ times}} & r > 0, \\ 0 & r = 0. \end{cases}$$

(By convention, we forget the conditions on Res $(\Sigma^p_{p^{n-1}}, \Sigma_{p^n})$ when $n = 1$.)

The first formula corrects the mistake in sign of the corresponding formula in [15; Theorem 2.2]. Compare with Remark 1.7 (ii).

(ii) By means of obstruction theory we can show

$$\bar{Q}_{n,s} = C_{n,s} \; (0 \le s < n),$$

(see the definition of $C_{n,s}$ in Remark 1.7 (ii)).

(iii) Let $I(n)$ be the ideal of $H^*(\Sigma_{p^n})$ generated by $\bar{Q}_{n,0}, \bar{R}_{n,s}$ $(0 \le s < n)$ and $\bar{R}_{n,0,s}$ $(0 < s < n)$. Denoting ${}_nJ^+ = {}_nJ \cap J^+$ we have

$$I(n) = \text{Ker Res }(\Sigma^p_{p^{n-1}}, \Sigma_{p^n}) = Span\{\bar{Q}_{H,R} \mid (H,R) \in {}_nJ^+\}.$$

Here $\bar{Q}_{H,R}$ denotes the unique element satisfying

$$\text{Res }(E^n, \Sigma_{p^n})\bar{Q}_{H,R} = (-1)^{\|H,R\|}Q_{H,R},$$
$$\text{Res }(\Sigma^p_{p^{n-1}}, \Sigma_{p^n})\bar{Q}_{H,R} = 0,$$

for $(H, R) \in {}_nJ^+$.

5. Dickson characteristic classes and the algebra $H^*(\Sigma_\infty)$

In this section, considering the dual version of Theorem 2.6, we define the mod p universal *Dickson characteristic classes* and use them to explicitly describe the algebra $H^*(\Sigma_\infty)$. For this end, one can apply the direct argument as given in Section 4 of [16] for the case $p = 2$. However, we explain here an improved argument, which we obtained after valuable discussions with Huỳnh Mùi and Nguyen Viet Dung. We thank them both for their suggestions.

Recall that for any $(H, R) \in J$ we have defined in 2.4 the Dickson element $D_{H,R}$ in $H_*(\Sigma_\infty)$. Let us equip J with a total order $<$ such that $(\emptyset, \emptyset)$ is the minimum element. For instance, we can choose $<$ to be the lexicographic order.

According to Theorem 2.6, $H_*(\Sigma_\infty)$ admits the Dickson additive basis consisting of all elements of the form

$$D^{t_1}_{H_1,R_1} \cdot \ldots \cdot D^{t_s}_{H_s,R_s} \tag{5.1}$$

Here the indices must satisfy the following conditions

$$\begin{aligned}
&(H_1, R_1) < \cdots < (H_s, R_s), \quad (H_i, R_i) \neq (\emptyset, \emptyset) \text{ if } s > 0,\\
&t_i = 1 \text{ for } |R_i| \text{ odd},\\
&1 \leq t_i < p \text{ for } |R_i| \text{ even},\\
&0 \leq s < \infty.
\end{aligned} \tag{5.2.}$$

CONVENTION. For $s = 0$, the element in 5.1 becomes

$$D_{\emptyset,\emptyset} = 1.$$

5.3. DEFINITION. For any $(H, R) \in J$ we set

$$C_{H,R} = (D_{H,R})^* \in H^*(\Sigma_\infty),$$

where the dual * is taken with respect to the Dickson basis given in 5.1.

5.4. REMARK.

(i) $C_{H,R}$ does not depend on the order $<$ chosen in J.

(ii) For $R = \emptyset$, the empty sequence of indices, $C_{H,\emptyset}$ has a close relationship to the Chern classes of the natural representation $\Sigma_{p^n} \subset U(p^n)$. Indeed, by means of Remark 4.6 (ii) it is easy to prove that

$$\mathrm{Res}\,(\Sigma_{p^n}, \Sigma_\infty) C_{H,\emptyset} = \prod_{i=0}^{n-1} C_{n,i}^{h_i}$$

for $H = (h_0, \ldots, h_{n-1})$. Here $C_{n,i}$ denotes the Chern class of dimension $2(p^n - p^i)$ for the above representation of the symmetric group Σ_{p^n}. (Compare with Remark 1.7 (ii).)

We now state the main result of this section.

Let us consider the following subsets of J given in 2.5:

$$J_0 = \{(H, \emptyset) \in J \mid H \text{ is not divisible by } p\},$$

$$J_1 = \{(H, R) \in J \mid |R| \text{ is odd }\},$$

$$J_2 = \{(H, R) \in J \mid |R| \text{ is even and positive}\}.$$

Here $H = (h_0, \ldots, h_{n-1})$ is said to be not divisible by p if there exists h_i which is not a multiple of p $(0 \le i < n)$. Remember that for $R = (r_1, \ldots, r_t)$ we have defined the length of R to be $|R| = t$ (see the beginning of Section 2).

5.5. THEOREM. *We have an isomorphism of graded algebras*

$$\begin{aligned} H^*(\Sigma_\infty) \cong\ & \mathbf{Z}_p[C_{H,\emptyset}; (H,\emptyset) \in J_0] \otimes E(C_{H,R}; (H,R) \in J_1) \\ & \otimes \mathbf{Z}_p[C_{H,R}; (H,R) \in J_2]/(C_{H,R}^p; (H,R) \in J_2). \end{aligned}$$

So we call $C_{H,R}$ the (mod p universal) *Dickson characteristic class* of the type (H, R).

Now we need the following notion of polynomial degree, which plays a key role in the proof of Theorem 5.5.

5.6. DEFINITION.

(i) Given $(H, R) \in J$, according to Theorem 2.6 (iii), $D_{H,R}$ can be written uniquely in the form

$$D_{H,R} = D_{H',R'}^{p^m}$$

for some $(H', R') \in J^+$. (See the definition of J^+ just before Theorem 2.6). By the polynomial degree of this element we mean

$$d(D_{H,R}) = p^m.$$

(ii) The polynomial degree of an element in the Dickson basis is defined by

$$d(D^{t_1}_{H_1,R_1} \dots D^{t_1}_{H_s,R_s}) = t_1 d(D_{H_1,R_1}) + \dots + t_s d(D_{H_s,R_s}).$$

To prove Theorem 5.5 we now state some lemmata, which will be proved in the next section.

5.7. LEMMA. *Let* $C = C^{t_1}_{H_1,R_1} \dots D^{t_s}_{H_s,R_s}$, *where the indices satisfy the condition 5.2. Then* $D = D^{t_1}_{H_1,R_1} \dots D^{t_s}_{H_s,R_s}$ *is the unique element in the Dickson basis with polynomial degree* $\geq d(D)$ *and having non-zero dual pairing with* C. *Furthermore,* $\langle D, C\rangle = t_1 \dots t_s$.

We remind the readers that the product defining C is the cup product whereas that defining D is the Pontriagin product.

As a consequence of this lemma, we obtain

5.8. LEMMA. $H^*(\Sigma_\infty)$ *is spanned as a* $\mathbb{Z}_p$*-module by the elements*

$$C^{t_1}_{H_1,R_1} \dots C^{t_s}_{H_s,R_s},$$

where the indices satisfy the condition 5.2.

5.9. LEMMA.

(i)

$$C^p_{H,\emptyset} = C_{pH,\emptyset}$$

where $pH = H + \dots + H$ *(p times) and the sum is defined in terms of coordinates.*

(ii)

$$C^p_{H,R} = 0$$

for $|R|$ *even and positive.*

(iii)

$$C^2_{H,R} = 0$$

for $|R|$ *odd.*

PROOF OF THEOREM 5.5. Combining Lemmata 5.8 and 5.9 we obviously obtain an epimorphism of graded algebras

$$\begin{aligned} h : \mathbb{Z}_p[C_{H,\emptyset}; (H,\emptyset) \in J_0] \otimes E(C_{H,R}; (H,R) \in J_1) \\ \otimes \mathbb{Z}_p[C_{H,R}; (H,R) \in J_2]/(C^p_{H,R}; (H,R) \in J_2) \\ \to H^*(\Sigma_\infty). \end{aligned}$$

Comparing the module generators for the source of h with the Dickson basis of $H_*(\Sigma_\infty)$ we see that the source of h is isomorphic to $H_*(\Sigma_\infty)$, hence it is isomorphic to $H^*(\Sigma_\infty)$, as graded $\mathbb{Z}_p$-modules of finite type. As a consequence, the epimorphism h is actually an isomorphism of algebras.

Theorem 5.5 is completely proved.

6. The algebraic relations between the Dickson classes.

This section is devoted to prove the lemmata of the preceding section.

First of all we compute the comultiplication of $H_*(\Sigma_\infty)$ in terms of the Dickson basis.

Note that if A is a commutative graded algebra, then one has

$$(a_1 + \cdots + a_n)^t = \sum_{\substack{t^1+\cdots+t^n=t \\ t^i \in \mathbb{Z}_+}} e(t^1, \ldots, t^n) \frac{t!}{t^1! \ldots t^n!} a_1^{t^1} \ldots a_n^{t^n},$$

for $a_1, \ldots, a_n \in A$ and t a natural number. Here $e(t^1, \ldots, t^n)$ is a certain sign depending on the partition $t = t^1 + \cdots + t^n$ and the degrees of $a_1, \ldots, a_n$.

Applying this fact to $A = H_*(\Sigma_\infty)$, from Theorem 2.6 we get

$$\begin{aligned} \Delta D^t_{H,R} &= \left(\sum_{(K,S)+(L,T)=(H,R)} sgn(K,S,L,T) D_{K,S} \otimes D_{L,T} \right)^t \\ &= \sum_\pi sgn(\pi) \frac{t!}{t^1! \ldots t^n!} \prod_{i=1}^n D^{t^i}_{K^i,S^i} \otimes \prod_{i=1}^n D^{t^i}_{L^i,T^i}. \end{aligned} \tag{6.1}$$

Here the summation runs over the set of all partitions

$$t = t^1 + \cdots + t^n,\ (H,R) = (K^i,S^i) + (L^i,T^i),\ 1 \le i \le n < \infty, \tag{π}$$

and $sgn(\pi)$ is a certain sign depending on π. Remark that if $t = t^1 + \cdots + t^n < p$ then

$$\frac{t!}{t^1! \dots t^n!} \neq 0 \ (\mathrm{mod} p).$$

Hence, for $\mathcal{H} = (H_1, R_1) \dots (H_s, R_s), T = (t_1, \dots, t_s)$ satisfying the condition 5.2 we obtain

$$\begin{aligned} \Delta D^T_{\mathcal{H}} &= \Delta(D^{t_1}_{H_1,R_1} \cdots D^{t_s}_{H_s,R_s}) \\ &= \sum_{\pi} b(\pi) \prod_{i,j} D^{t^i_j}_{K^i_j,S^i_j} \otimes \prod_{i,j} D^{t^i_j}_{L^i_j,T^i_j}, \end{aligned} \tag{6.2}$$

where the summation runs over all partitions $\pi = (\pi_1, \dots, \pi_s)$ with

$$t_j = t^1_j + \cdots + t^{n_j}_j, \ (H_j, R_j) = (K^i_j, S^i_j) + (L^i_j, T^i_j), \ 1 \leq i \leq n_j < \infty, \qquad (\pi_j)$$

and $b(\pi)$ is a certain non-zero scalar in $\mathbf{Z}_p$.

6.3. REMARK. For simplicity, let us reformulate (6.2) in the form

$$\Delta(D^{t_1}_{H_1,R_1} \cdots D^{t_s}_{H_s,R_s}) = \sum_{\pi} b(\pi) D^{u_1}_{K_1,S_1} \cdots D^{u_r}_{K_r,S_r} \otimes D^{u_1}_{L_1,T_1} \cdots D^{u_r}_{L_r,T_r},$$

where $b(\pi)$ is non-zero in $\mathbf{Z}_p$ and $r = r(\pi)$ is a certain number depending on the partition π.

It is easy to see that for any term $D^{u_1}_{K_1,S_1} \cdot \ldots \cdot D^{u_r}_{K_r,S_r} \otimes D^{u_1}_{l_1,T_1} \cdot \cdots \cdot D^{u_r}_{L_r,T_r}$ in the right hand side of 6.3 we have

$$d(D^{t_1}_{H_1,R_1} \cdots D^{t_s}_{H_s,R_s}) \leq d(D^{u_1}_{K_1,S_1} \cdots D^{u_r}_{K_r,S_r}) + d(D^{u_1}_{L_1,T_1} \cdots D^{u_r}_{L_r,T_r}).$$

Moreover, equality happens if and only if $r = s$ and additionally either

$$D^{u_i}_{K_i,S_i} = 1, \quad D^{u_i}_{L_i,T_i} = D^{t_i}_{H_i,R_i},$$

or

$$D^{u_i}_{K_i,S_i} = D^{t_i}_{H_i,R_i}, \quad D^{u_i}_{L_i,T_i} = 1.$$

for any $i (1 \leq i \leq s)$. In this case, we have

$$D^{t_1}_{H_1,R_1} \cdots D^{t_s}_{H_s,R_s} = (D^{u_1}_{K_1,S_1} \cdots D^{u_r}_{K_r,S_r}).(D^{u_1}_{L_1,T_1} \cdots D^{u_r}_{L_r,T_r}).$$

We are now ready to prove the lemmata in Section 5.

PROOF OF LEMMA 5.7. We prove the lemma by induction on s.

For $s = 1$ we simply write $C = C^t_{H,R}, D = D^t_{H,R}$. For $t = 1$ the lemma follows directly from Definition 5.3. Assume that $t < p$ and the lemma holds for $t-1$. Suppose that

$$d(D^{v_1}_{I_1,Q_1} \dots D^{v_q}_{I_q,Q_q}) \geq d(D), \tag{a}$$

where the element $D^{v_1}_{I_1,Q_1} \dots D^{v_q}_{I_q,Q_q}$ on the left hand side belongs to the Dickson basis given in 5.1. Using the formula for the coproduct taken in 6.3 we get

$$\begin{aligned}\langle D^{v_1}_{I_1,Q_1} \dots D^{v_q}_{I_q,Q_q}, C^t_{H,R}\rangle &= \langle \Delta(D^{v_1}_{I_1,Q_1} \dots D^{v_q}_{I_q,Q_q}), C^{t-1}_{H,R} \otimes C_{H,R}\rangle \\ &= \sum_\pi b(\pi)\langle D^{u_1}_{K_1,S_1} \dots D^{u_r}_{K_r,S_r}, C^{t-1}_{H,R}\rangle \quad \langle D^{u_1}_{L_1,T_1} \dots D^{u_r}_{L_r,T_r}, C_{H,R}\rangle\end{aligned}$$

If the sum is non-zero, then it contains at least one non-zero term. Suppose that this term is

$$\langle D^{u_1}_{K_1,S_1} \dots D^{u_r}_{K_r,S_r}, C^{t-1}_{H,R}\rangle\langle D^{u_1}_{L_1,T_1} \dots D^{u_r}_{L_r,T_r}, C_{H,R}\rangle \neq 0 \tag{b}$$

By Definition 5.3 it implies

$$D^{u_1}_{L_1,T_1} \dots D^{u_r}_{L_r,T_r} = D_{H,R}. \tag{c}$$

Combining (a), (c) and Remark 6.3 we obtain

$$d(D^{u_1}_{K_1,S_1} \dots D^{u_r}_{K_r,S_r} \geq d(D) - d(D_{H,R}) = d(D^{t-1}_{H,R}).$$

Using this fact together with (b) and the inductive hypothesis on t we have

$$D^{u_1}_{K_1,S_1} \dots D^{u_r}_{K_r,S_r} = D^{t-1}_{H,R}. \tag{d}$$

Combine (a), (c), (d) with Remark 6.3 we get

$$d(D) \leq d(D^{v_1}_{I_1,Q_1} \dots D^{v_q}_{I_q,Q_q}) \leq d(D^{t-1}_{H,R}) + d(D_{H,R}) = d(D).$$

So the two inequalities $\leq$ become equalities. Again, by means of Remak 6.3 we obtain

$$D^{v_1}_{I_1,Q_1} \dots D^{v_1}_{I_q,Q_q} = D^{t-1}_{H,R}.D_{H,R} = D^t_{H,R}.$$

Next we will prove that

$$\langle D^t_{H,R}, C^t_{H,R}\rangle = t \tag{e}$$

for $t, (H, R)$ satisfying 5.2. We observe that

$$\langle D^t_{H,R}, C^t_{H,R}\rangle = \langle \Delta D^t_{H,R}, C^{t-1}_{H,R} \otimes C_{H,R}\rangle.$$

Using the same argument mentioned above we see that the only term in $\Delta D^t_{H,R}$, whose dual pairing with $C^{t-1}_{H,R} \otimes C_{H,R}$ is non-zero, is of the form $bD^{t-1}_{H,R} \otimes D_{H,R}$ $(b \in \mathbf{Z}_p)$. Obviously it coincides with the term of the same form in the sum

$$(1 \otimes D_{H,R} + D_{H,R} \otimes 1)^t = tD^{t-1}_{H,R} \otimes D_{H,R} + (\text{other terms}).$$

Hence, (e) follows. The lemma holds for $s = 1$.

Now suppose that $s > 1$ and the lemma is true for $s - 1$. By Remark 6.3, an argument similar to that for $s = 1$ shows that D is the unique element among the Dickson ones with polynomial degree $\geq d(D)$, which could have non-zero dual pairing with C. Now we must prove

$$\langle D, C\rangle = t_1 \dots t_s.$$

Note that

$$\langle D, C\rangle = \langle \Delta(D^{t_1}_{H_1,R_1} \dots D^{t_{s-1}}_{H_{s-1},R_{s-1}} . D^{t_s}_{H_s,R_s}), C^{t_1}_{H_1,R_1} \dots C^{t_{s-1}}_{H_{s-1},R_{s-1}} \otimes C^{t_s}_{H_1,R_1}\rangle.$$

Using again Remark 6.3 to do some simple computations on the right hand side we get

$$\begin{aligned}\langle D, C\rangle &= \langle D^{t_1}_{H_1,R_1} \dots D^{t_{s-1}}_{H_{s-1},R_{s-1}}, C^{t_1}_{H_1,R_1} \dots C^{t_{s-1}}_{H_{s-1},R_{s-1}}\rangle \quad \times \langle D^{t_s}_{H_s,R_s}, C^{t_s}_{H_s,R_s}\rangle \\ &= t_1 \dots t_{s-1} . t_s.\end{aligned}$$

The lemma is completely proved.

Proof of Lemma 5.8. It suffices to prove that if $x \in H_*(\Sigma_\infty)$ has zero dual pairing with all the elements given in 5.8, then $x = 0$.

Assume the contrary that $x \neq 0$. We take the linear expansion of x in terms of the Dickson basis. Suppose that

$$D' = D^{u_1}_{K_1,S_1} \dots D^{u_r}_{K_r,S_r}$$

is the element with smallest polynomial degree among the ones of the Dickson basis appearing in this expansion. By means of Lemma 5.7 we get

$$\langle x, C^{u_1}_{K_1,S_1}\dots C^{u_r}_{K_r,S_r}\rangle = \langle D', C^{u_1}_{K_1,S_1}\dots C^{u_r}_{K_r,S_r}\rangle \neq 0.$$

This is a contradiction. The lemma follows.

PROOF OF LEMMA 5.9. We need only to prove (i) and (ii), since (iii) follows directly from the information on dimensions.

Given a natural number t and any $(H,R)\in J$, by induction on t one easily get

$$C^t_{H,R} = \sum(\text{coeff.})(D^{t_1}_{H_1,R_1}\dots D^{t_s}_{H_s,R_s})^*, \tag{a}$$

where the sum is taken over the dual of some Dickson elements satisfying 5.2 and additionally the condition

$$|H_i| = |H|$$

for every i.

On the other hand, let P^i be the i-th Steenrod cohomology operation. Then one has

$$C^p_{H,R} = P^k(C_{H,R}) \tag{b}$$

where $k = 1/2 \dim C_{H,R}$.

Let P^i_* be the homology operation dual to P^i. Obviously, Res (E^n, Σ_{p^n}) is a homomorphism of $A(p)$-modules, where $A(p)$ denotes the mod p Steenrod algebra. So by passing to the dual, the module

$$\text{Im}\ \ i_n = Span\{D_{H,R} \mid |H| = n\}$$

is closed under the action of P^i_* for any i.

Recall that one has the Cartan formula

$$P^i_*(x.y) = \sum_j P^j_*(x).P^{i-j}_*(y)$$

for $x,y\in H_*(\Sigma_\infty)$ (see e.g. [8]).

We define the multiplicity for Dickson elements by putting

$$\mu(D_{H,R}) = p^{|H|},$$
$$\mu(x.y) = \mu(x) + \mu(y).$$

By convention, zero is considered to have every multiplicity. An element in $H_*(\Sigma_\infty)$ is called to be of homogeneous multiplicity m if its expansion in terms of the Dickson basis contains only Dickson elements of multiplicity m. The set of all such elements forms a submodule of $H_*(\Sigma_\infty)$. It is denoted by ${}_mH$.

From the above discussions we observe that P_*^i preserves the multiplicity. That means that P_*^i acts closely in ${}_mH : P_*^i({}_mH) \subset {}_mH$.

Passing to the dual and combining the obtained result with (a) and (b) we get

$$C^p_{H,R} = \sum (\text{coeff.}) D^*_{K,S},$$

where the sum runs over some (K, S) with $|K| = |H|$. In other words,

$$C^p_{H,R} \in \text{ Span } \{C_{K,S} \mid |K| = |H|\}.$$

Set $n = |H|$. From Definitions 2.4 and 5.3 it immediately follows that

$$\text{Res } (E^n, \Sigma_{p^n}) : Span\{C_{K,S} \mid |K| = n\} \to \mathcal{B}_n(p)$$

is an isomorphism, which takes $C_{K,S}$ to $Q_{K,S}$. So we have

$$\text{Res } (E^n, \Sigma_{p^n}) C^p_{H,R} = Q^p_{H,R} = \begin{cases} Q_{pH,\emptyset} & \text{for } R = 0, \\ 0 & \text{otherwise }. \end{cases}$$

The lemma follows.

References

[1] H. Cardenas, *El algebra de cohomologia del group simetrio de grado p^2*, Bol. Soc. Math. Mexic. Segunda Serie **10** (1965), 1-30.

[2] H. Cartan, "Seminaire H. Cartan," E.N.S. 1954-1955.

[3] L.E. Dickson, *A fundamental system of invariants of the general modular linear group with a solution of the form problem*, Trans. Amer. Math. Soc. **12** (1911), 75-98.

[4] Huỳnh Mùi, *Modular invariant theory and cohomology algebras of symmetric groups*, J. Fac. Sci., Univ. Tokyo, Sect. IA **22** (1975), 319-369.

[5] Huỳnh Mùi, *Duality in the infinite symmetric products*, Acta Math. Vietnam. **5**, No 1 (1980), 100-149.

[6] I. Madsen and R.J. Milgram, "The classifying spaces for surgery and cobordism of manifolds," Ann. of Math. Studies, No **92**, Princeton Univ. Press, 1979.

[7] J.P. May, "The geometry of iterated loop spaces," Lect. Notes in Math, **271**, Springer, 1972.

[8] J.P. May, "The homology of E_∞ spaces," Lect. Notes in Math. **533**, Springer 1976, pp. 1-68.

[9] T. Nakamura, *On cohomology operations*, Japan J. Math **33** (1963), 93-145.

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

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

[12] M. Nakaoka, *Note on cohomology algebras of symmetric groups*, J. Math, Osaka City Univ. **13** (1962), 45-55.

[13] N.H.V. Hung, *The mod 2 cohomology algebras of symmetric groups*, Acta Math. Vietn **6**, No 2 (1981), 41-48.

[14] N.H.V. Hung, *The mod 2 equivariant cohomology algebras of configuration spaces*, Acta Math. Vietnam. **7**, No 1 (1982), 95-100.

[15] N.H.V. Hung, *Algèbre de cohomology du groupe symétrique infini et classes caractéristiques de Dickson*, C.R. Acad. Sci. Paris **297**, Série I (1983), 611-614.

[16] N.H.V. Hung, *The modulo 2 cohomology algebras of symmetric groups,*, Japan J. Math. **13**, No 1 (1987), 169-208.

[17] N.H.V. Hung, *Classes de Dickson et algèbres de cohomologie des espaces de lacets itér'es*, C.R. Acad. Sci. Paris **307**, Série I (1988), 911-914.

[18] G. Nishida, *The nilpotency of elements of the stable homotopy of spheres*, J. Math. Soc. Japan **25**, No 4 (1973), 707-732.

[19] S.B. Priddy, *On $\Omega^\infty S^\infty$ and the infinite symmetric group*, Proc. Symp. Pure Math Am. Math. Soc. **22** (1971), 217-220.

[20] D. Quillen, *The Adams conjecture*, Topology **10** (1971), 67-80.

[21] D. Quillen, *The spectrum of an equivariant cohomology ring I, II*, Ann. of Math. **94** (1971), 449-602.

[22] D. Quillen, *The mod 2 cohomology rings of extra-special 2-groups and the spinor groups*, Math Ann. **11** (1972), 197-212.

[23] N.E. Steenrod, *Reduced powers of cohomology classes*, Ann. of Math. **56** (1952), 47-67.

[24] N.E. Steenrod, *Homology groups of symmetric groups and reduced power operations*, Proc. Nat. Acad. Acs. U.S.A. **39** (1953), 213-217.

[25] N.E. Steenrod, *Cyclic reduced powers of cohomology classes*, Proc. Nat. Acad. Sci. U.S.A. **39** (1953), 217-223.

[26] N.E. Steenrod, "Cohomology Operations and Obstructions to Extending Continuous Functions," Colloquium Lecture Notes, Princeton Univ., 1957.

[27] N.E. Steenrod and D.B. Epstein, *Cohomology operations*, Ann. of Math. Studies, No 50, Princeton Univ. Press, 1962.

[28] R.J. Wellington, "The unstable Adams spectral sequence for free iterated loop spaces," Memoirs Amer. Math. Soc. **36**, No 258 (1982).

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF HANOI