*Vietnam Journal of Mathematics* 28:2(2000) 189-193

Vietnam Journal
of
MATHEMATICS


*Short Communication*

# $\mathcal{A}$-Decomposability of the Dickson Algebra*

**Nguyên Hưu Viêt Hưng and Trân Ngoc Nam**

*Department of Mathematics, Vietnam National University*
*334 Nguyen Trai Street, Hanoi, Vietnam*

Received September 16, 1999

## 1. Introduction

Let $P_k := \mathbf{F}_2[x_1, \ldots, x_k]$ be the polynomial algebra over $\mathbf{F}_2$ in $k$ variables, each of degree 1. The general linear group $GL_k := GL(k, \mathbf{F}_2)$ acts on $P_k$ in the usual manner. Dickson proves in [1] that the ring of invariants, $D_k := (P_k)^{GL_k}$, is also a polynomial algebra $D_k \cong \mathbf{F}_2[Q_{k,k-1}, \ldots, Q_{k,0}]$, where $Q_{k,s}$ denotes the Dickson invariant of degree $2^k - 2^s$. It can be defined by the inductive formula

$$Q_{k,s} = Q^2_{k-1,s-1} + V_k \cdot Q_{k-1,s},$$

where, by convention, $Q_{k,k} = 1, Q_{k,s} = 0$ for $s < 0$ and

$$V_k = \prod_{\lambda_j \in \mathbf{F}_2} (\lambda_1 x_1 + \cdots + \lambda_{k-1} x_{k-1} + x_k).$$

Let $\mathcal{A}$ be the mod 2 Steenrod algebra. The usual action of $\mathcal{A}$ on $P_k$ commutes with that of $GL_k$. So $D_k$ is an $\mathcal{A}$-module. One of the authors has been interested in the homomorphism

$$j_k : \mathbf{F}_2 \underset{\mathcal{A}}{\otimes} (P_k)^{GL_k} \to (\mathbf{F}_2 \underset{\mathcal{A}}{\otimes} P_k)^{GL_k},$$

which is induced by the identity map on $P_k$ (see [3]). Observing that $j_1$ is an isomorphism and $j_2$ is a monomorphism, he sets up the following

**Conjecture 1.1.** [3] $j_k = 0$ *in positive degrees for* $k > 2$.

* This paper is supported in part by the National Research Project, No. 1.4.2.
AMS 2000 Subject Classification: Primary 55S10, Secondary 55P47, 55Q45, 55T15.

Let $D_k^+$ and $\mathcal{A}^+$ denote, respectively, the submodules of $D_k$ and $\mathcal{A}$ consisting of all elements of positive degree. Then Conjecture 1.1 is equivalent to $D_k^+ \subset \mathcal{A}^+ \cdot P_k$ for $k > 2$ (see [3]). In other words, it predicts that every $GL_k$-invariant polynomial is hit by the Steenrod algebra acting on $P_k$ for $k > 2$.

In [3], one of the authors proves the equivalence of Conjecture 1.1 and a weak algebraic version of the conjecture on spherical classes stating that: *There are no spherical classes in $Q_0S^0$ except the elements of Hopf invariant one and those of Kervaire invariant one.* He also gives two proofs of Conjecture 1.1 for the case of $k = 3$. The fact that $j_k \neq 0$ for $k = 1$ and 2 is, respectively, an exposition of the exsitence of Hopf invariant one and Kervaire invariant one classes. In this paper, we establish this conjecture for every $k > 2$. We have

**Main Theorem.** *$D_k^+ \subset \mathcal{A}^+ \cdot P_k$ for $k > 2$.*

Recently, F. Peterson and R. Wood privately informed us that they had optained a proof of this theorem for $k = 4$ and probably for $k = 5$. The readers are referred to [5] and [6] for some problems, which are closely related to the Main Theorem. They are also referred to F. Peterson [7], R. Wood [11], W. Singer [9], S. Priddy [8] for other approaches to the hit problem from several classical ones in Homotopy theory.

This note contains three sections. Sec. 2 is a preparation on the action of the Steenrod squares on the Dickson algebra. In Sec. 3, we express an outline of the proof of the Main Theorem.

## 2. Preliminaries

The action of the Steenrod operations on $D_k$ is explicitly described as follows.

**Theorem 2.1.** [2]

$$Sq^i(Q_{k,s}) = \begin{cases} Q_{k,r} & \text{for } i = 2^s - 2^r,\ r \leq s, \\ Q_{k,r}Q_{k,t} & \text{for } i = 2^k - 2^t + 2^s - 2^r,\ r \leq s < t, \\ Q_{k,s}^2 & \text{for } i = 2^k - 2^s, \\ 0 & \text{otherwise.} \end{cases}$$

From now on, we denote $Q_{k,s}$ by $Q_s$ for brevity.

Let $I_n$ $(n \geq 0)$ be the right ideal of $\mathcal{A}$ generated by the operations $Sq^{2^i}$ for $i = 0, \dots, n$.

**Definition 2.2.** *Suppose $R_1, R_2 \in P_k$. Then we write $R_1 \equiv R_2 \pmod{I_n}$ if $R_1 + R_2$ belongs to $I_n \cdot P_k$. By convention, $R_1 \equiv R_2 \pmod{I_n}$ means $R_1 = R_2$ for $n < 0$.*

This is an equivalence relation. We have

**Lemma 2.3.** *Let $k > 1$ and suppose $S$ is a non-empty subset of $\{0, \ldots, k-1\}$ such that $1 \notin S$. Then*

$$QR^2 \equiv 0 \pmod{I_0},$$

*where $Q = \prod_{s \in S} Q_s$ and $R$ is an arbitrary polynomial in $P_k$.*

## 3. Outline of Proof of the Main Theorem

Let $Q$ be a non-zero Dickson monomial. If $Q \neq 1$, it can be written as

$$Q = \prod_{0 \leq i \leq n} A_i^{2^i}$$

where $n$ is some non-negative integer and $A_i$ is some Dickson monomial dividing $\prod_{0 \leq s < k} Q_s$ for $i = 0, \ldots, n$ with $A_n \neq 1$.

Indeed, suppose $Q = \prod_{0 \leq s < k} Q_s^{\alpha_s}$. Since $Q \neq 1$, there exists at least one $\alpha_s \neq 0$. Consider the 2-adic expansions of all the non-zero $\alpha_s$'s:

$$\alpha_s = \sum_{0 \leq i \leq n(s)} \alpha_{si} 2^i,$$

where $\alpha_{sn(s)} = 1$. Now denoting

$$n := \max_{\substack{\alpha_s \neq 0 \\ 0 \leq s < 0}} n(s),$$

$$\alpha_{si} := 0 \text{ if } n(s) < i \leq n \ (0 \leq s < k),$$

$$A_i := \prod_{0 \leq s < k} Q_s^{\alpha_{si}} \ (0 \leq i \leq n),$$

one can easily check that $Q = \prod_{0 \leq i \leq n} A_i^{2^i}$ and each $A_i$ divides $\prod_{0 \leq s < k} Q_s$. Moreover, there exists an integer $r$ such that $0 \leq r < k$, $\alpha_r \neq 0$, and $n = n(r)$. Then $A_n = \prod_{0 \leq s < k} Q_s^{\alpha_{sn}}$ is divisible by $Q_r^{\alpha_{rn}} = Q_r^{\alpha_{rn(r)}} = Q_r$, so $A_n \neq 1$.

**Definition 3.1.**

(i) *We call $n$ the height of $Q$. The monomial $A_i^{2^i} = A_i(Q)^{2^i}$ is called the $i$-th cut of $Q$. It is said to be full if $A_i$ is divisible by $\prod_{0 < s < k} Q_s$. The monomial $Q$ is called full if its cuts are all full.*

(ii) *A Dickson monomial is called a based cut if it is the 0th cut of some $Q \neq 0$ and $\neq 1$.*

The Main Theorem is proved by means of the following two lemmata.

**Lemma 3.2.** *Let $k > 2$ and suppose $R$ is an arbitrary polynomial in $P_k$.*

(a) *If $Q = \prod_{0 \leq i \leq n} A_i^{2^i} \neq 1$ and it is not full, then $QR^{2^{n+1}} \in \mathcal{A}^+ \cdot P_k$.*

(b) *If $Q = \prod_{0 \leq i \leq n} A_i^{2^i}$ is full, then $QSq^{2^{m+n+1}}(R^{2^{n+1}}) \in \mathcal{A}^+ \cdot P_k$ for $0 \leq m < k-1$.*

**Lemma 3.3.** *Suppose $k > 2$. If $A$ is a full based cut, then $A \equiv 0 \pmod{I_1}$.*

*Proof of the Main Theorem.* Suppose $Q = \prod_{0 \leq i \leq n} A_i^{2^i}$ is a Dickson monomial with $A_n \neq 1$.

If $Q$ is not full, then applying Lemma 3.2(a) with $R = 1$, one gets $Q \in \mathcal{A}^+ \cdot P_k$.

If $Q$ is full and $n = 0$, then $Q$ is the full based cut of itself. So using Lemma 3.3, one obtains $Q \equiv 0 \pmod{I_1}$. In particular, $Q \in \mathcal{A}^+ \cdot P_k$.

If $Q$ is full and $n > 0$, then $A_n$ is the full based cut of itself. By Lemma 3.3, one has $A_n = Sq^1(R_1) + Sq^2(R_2)$, with some $R_1, R_2 \in P_k$. Noting that $Q' = \prod_{0 \leq i < n} A_i^{2^i}$ is also full with the height $n - 1$, one can apply Lemma 3.2(b) to it and get

$$Q' Sq^{2^n}(R_1^{2^n}) = \prod_{0 \leq i < n} A_i^{2^i} Sq^{2^n}(R_1^{2^n}) \in \mathcal{A}^+ \cdot P_k,$$

$$Q' Sq^{2^{n+1}}(R_2^{2^n}) = \prod_{0 \leq i < n} A_i^{2^i} Sq^{2^{n+1}}(R_2^{2^n}) \in \mathcal{A}^+ \cdot P_k.$$

(It should be noted that $1 < k - 1$.) Therefore,

$$Q = \prod_{0 \leq i < n} A_i^{2^i} \cdot A_n^{2^n} = \prod_{0 \leq i < n} A_i^{2^i} [Sq^{2^n}(R_1^{2^n}) + Sq^{2^{n+1}}(R_2^{2^n})] \in \mathcal{A}^+ \cdot P_k.$$

The proof is complete. ∎

*Outline of Proof of Lemma 3.2.* The proof is divided into two steps.

*Step 1:* If Lemma 3.2(a) is true for every $n \leq N$, then so is Lemma 3.2(b) for every $n \leq N$.

Indeed, suppose $Q = \prod_{0 \leq i \leq n} A_i^{2^i}$ (with $n \leq N$) is full and $m$ satisfies $0 \leq m < k - 1$. One needs to prove $Q Sq^{2^{m+n+1}}(R^{2^{n+1}}) \in \mathcal{A}^+ \cdot P_k$, where $R \in P_k$. By the Cartan formula, one gets

$$Q Sq^{2^{m+n+1}}(R^{2^{n+1}}) \equiv \sum_{0 < j \leq 2^m} Sq^{2^{n+1} j}(Q) R_j^{2^{n+1}} \pmod{\mathcal{A}^+ \cdot P_k},$$

where $R_j := Sq^{2^m - j}(R)$ for $j = 1, \ldots, 2^m$.

Let $B = \prod_{0 \leq i \leq p} B_i^{2^i}$ be an arbitrary Dickson monomial of $Sq^{2^{n+1} j}(Q)$, with $B_i^{2^i}$ the $i$th cut of $B$. Note that $p \geq n$. If $\prod_{0 \leq i \leq n} B_i^{2^i} = 1$, then $p > n$, so we get $BR_j^{2^{n+1}} = (\prod_{0 \leq i \leq p} B_i^{2^{i-1}} R_j^{2^n})^2 \equiv 0 \pmod{I_0}$. If $\prod_{0 \leq i \leq n} B_i^{2^i} \neq 1$, then it is not full. So we can choose an integer $q$ such that $B_q \neq 1$ $(0 \leq q \leq n \leq N)$ and $\prod_{0 \leq i \leq q} B_i^{2^i}$ is not full. Applying Lemma 3.2(a) to $\prod_{0 \leq i \leq q} B_i^{2^i}$, we obtain

$$BR_j^{2^{n+1}} = \prod_{0 \leq i \leq q} B_i^{2^i} \Big( \prod_{q < i \leq p} B_i^{2^{i-q-1}} R_j^{2^{n-q}} \Big)^{2^{q+1}} \in \mathcal{A}^+ \cdot P_k.$$

Therefore, Step 1 is shown.

*Step 2:* Lemma 3.2(a) holds for every non-negative integer $n$.

Let $q = q(Q)$ be the smallest integer so that $A_q$ is not full $(0 \leq q \leq n)$. Suppose $s$ is the smallest integer with $0 < s < k$ such that $Q_s \nmid A_q$.

Using Step 1, we prove Lemma 3.2(a) by induction on $n$ and for a fixed $n$ by induction on $s$. ■

*Outline of Proof of Lemma 3.3.* Note that to prove Lemma 3.3, it suffices to show

$$Q_2 Q_1 \equiv 0 \ (\mathrm{mod}\, I_1).$$

Let $R_1 := \sum_{sym} x_1 x_2 x_3 x_4^8 \cdots x_k^{2^{k-1}}$, where $\sum_{sym}$ denotes the sum of all symmetrized terms in $x_1, \ldots, x_k$. Using Theorem 2.2 of [4], one can show that

$$Q_2 Q_1 \equiv [Sq^2(R_1)]^2 \ (\mathrm{mod}\, I_1) \equiv 0 \ (\mathrm{mod}\, I_1).$$

Lemma 3.3 is proved. ■

The result of this note will be published in detail elsewhere.

## References

1. 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.
2. Nguyên H. V. Hưng, The action of the Steenrod squares on the modular invariants of linear groups, *Proc. Amer. Math. Soc.* **113** (1991) 1097–1104.
3. Nguyên H. V. Hưng, Spherical classes and the algebraic transfer, *Trans. Amer. Math. Soc.* **349** (1997) 3893–3910.
4. Nguyên H. V. Hưng and F. P. Peterson, Spherical classes and the Dickson algebra, *Math. Proc. Camb. Phil. Soc.* **124** (1998) 253–264.
5. Nguyên H. V. Hưng, The weak conjecture on spherical classes, *Math. Zeit.* **231** (1999) 727–743.
6. Nguyên H. V. Hưng, Spherical classes and the Lambda algebra, *Trans. Amer. Math. Soc.*, to appear.
7. F. P. Peterson, Generators of $H^*(\mathbf{RP}^\infty \wedge \mathbf{RP}^\infty)$ as a module over the Steenrod algebra, Abstracts Amer. Math. Soc. 833-55-89, April 1987.
8. S. Priddy, On characterizing summands in the classifying space of a group, I, *Amer. Jour. Math.* **112** (1990) 737–748.
9. W. M. Singer, The transfer in homological algebra, *Math. Zeit.* **202** (1989) 493–523.
10. N. E. Steenrod and D. B. A. Epstein, *Cohomology Operations*, Ann. of Math. Studies, Vol. 50, Princeton University Press, 1962.
11. R. M. W. Wood, Steenrod squares of polynomials and the Peterson conjecture, *Math. Proc. Camb. Phil. Soc.* **105** (1989) 307–309.