Comment. Math. Helvetici **68** (1993) 622–632 0010–2571/93/040622–11$1.50 + 0.20/0

A classification of polynomial algebras as modules over the Steenrod algebra

JEANNE DUFLOT, NICHOLAS J. KUHN* AND MARK WINSTEAD

1. Introduction

Suppose that $\mathscr{A}_2$ is the mod-2 Steenrod algebra, and that $R = \mathbf{F}_2[x_1, \ldots, x_n]$ is the polynomial ring in n variables over the prime field $\mathbf{F}_2$. Campbell and Selick [3] observed that the equations $\mathrm{Sq}^1 x_i = x_{i-1}^2$ for $2 \leq i \leq n$, and $\mathrm{Sq}^1 x_1 = x_n^2$, define an action of $\mathscr{A}_2$ on R that makes R isomorphic as an $\mathscr{A}_2$-module to the $\mathscr{A}_2$-module defined by the standard action on R. In that paper, they also pose the following question, due to Tom Hunter: does the equation $\mathrm{Sq}^1 x_i = \Sigma_j m_{ij} x_j^2$ (where $M = [m_{ij}]$ is any n-by-n matrix over $\mathbf{F}_2$) define an action of $\mathscr{A}_2$ on R?

In this paper we given an affirmative answer to the above question and classify the actions defined in this way. More precisely, let $S(V)$ be the symmetric algebra generated by a finite dimensional $\mathbf{F}_2$ vector space V concentrated in degree 1. Then we have

THEOREM 1.1. *Given $M \in \mathrm{End}(V)$, the equation $\mathrm{Sq}^1 v = (Mv)^2$ extends to an unstable action of $\mathscr{A}_2$ on $S(V)$ satisfying the Cartan formula.*

Let $S_M(V)$ denote $S(V)$ with this $\mathscr{A}_2$-action.

THEOREM 1.2. *Given two elements of $\mathrm{End}(V)$, M_1 and M_2, $S_{M_1}(V)$ is isomorphic to $S_{M_2}(V)$ as $\mathscr{A}_2$-modules if and only if*

$$\dim(\ker(M_1^i)) = \dim(\ker(M_2^i)) \qquad \text{for all } i \geq 1.$$

In particular, if M is invertible, $S_M(V)$ is isomorphic to $S_1(V)$, i.e., $S(V)$ with the standard $\mathscr{A}_2$-action.

---

* Research supported in part by the NSF.

Theorem 1.1 is proved in sections 2 and 3 using the Bullett and McDonald approach to the Adem relations introduced in [2]. Theorem 1.2 is proved in section 4. The proof[1] uses nothing more than basic linear algebra and Galois theory, and avoids the use of Davenport's normal basis theorem needed in [3]. The last section contains an alternate proof of a critical step of Theorem 1.2, as well as some remarks about the obvious generalizations of our results to odd primes.

2. Higher derivations and $\mathscr{A}_2$-algebras

Suppose F is a commutative ring of characteristic 2, and let R be a $\mathbf{Z}$-graded F-*algebra.*

It is convenient to introduce the idea of a higher derivation, adapted from commutative algebra (*e.g., see* [4]).

A *higher derivation*[2] of R over F is a sequence

$$D_* = \{D_0, D_1, \ldots, D_n, \ldots\}$$

such that

1. D_i is an endomorphism of the graded F-module R of degree i, and
2. $D_i(fg) = \Sigma_{j=0}^{i} D_j(f)D_{i-j}(g)$, for every $f, g \in R$ and for every $i \in \{0, 1, 2, \ldots\}$.

Suppose that T and U are indeterminates. If D_* is a higher derivation of R over F, then D_* induces a ring homomorphism

$$D_*(T) : R \to R[[T]]$$

defined by

$$D_*(T)(f) = \sum_{i=0}^{\infty} D_i(f)T^i.$$

Therefore, D_* also induces a ring homomorphism

$$D_*(T, U) : R[[T]] \to R[[T, U]]$$

---

[1] Special thanks to Thann Ward for showing us Lemma 3.4 of [5].

[2] Some refer to higher derivations as *divided sequences.*

defined by

$$D_*(T, U)\left(\sum_{i=0}^{\infty} a_i T^i\right) = \sum_{i=0}^{\infty} D_*(T)(a_i)U^i$$

$$= \sum_{i=0}^{\infty}\left(\sum_{j=0}^{\infty} D_j(a_i)T^j\right)U^i$$

$$= \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} D_k(a_{n-k})T^k U^{n-k}\right).$$

Mimicking Bullett and MacDonald [2], we say that a higher derivation D_* of R over F satisfies the *mod*-2 *Adem relations* on R if and only if

$$(D_*(s^2 + st)D_*(t^2))(f) = (D_*(t^2 + st)D_*(s^2))(f) \qquad \text{for every } f \in R. \tag{1}$$

In the equation (1) we interpret $D_*(s^2 + st)D_*(t^2)$ as the ring homomorphism defined by the composite

$$R \xrightarrow{D_*(T)} R[[T]] \xrightarrow{D_*(T, U)} R[[T, U]] \to R[[s, t]]$$

$$T \mapsto s^2 + st$$

$$U \mapsto t^2$$

and similarly for the right hand side of the equation (1). (Here, s and t are new indeterminates.)

A higher derivation D_* of R over F is *unstable* if and only if

$$D_i(f) = 0 \qquad \text{for every } i > \deg f.$$

Following Bullett and Macdonald [2], we see that the next thing to do is to prove

THEOREM 2.1. *Let R be a graded F-algebra that is generated by elements of degree* 1 *as an F-algebra. Suppose that D_* is a higher derivation of R over F such that*

(i) *D_* is unstable*

(ii) *$D_0 D_1 = D_1 D_0$, and*

(iii) *$D_1 D_1 = 0$.*

Then D_* satisfies the mod-2 *Adem relations on R.*

Proof. In view of the fact that R is generated as a ring by $F = R_0$ and R_1; and the fact that both $D_*(s^2 + st)D_*(t^2)$ and $D_*(t^2 + st)D_*(s^2)$ are ring homomorphisms, we need only verify (1) for $f \in F$ and for $f \in R_1$.

If $f \in F$, then $D_i(f) = 0$ if $i > 0$, so both sides of (1) reduce to $D_0D_0(f)$. If $f \in R_1$ then $D_*(T, U)(D_*(T)(f)) = \Sigma_{n=0}^{\infty}(\Sigma_{k=0}^{n} D_k(D_{n-k}(f))T^kU^{n-k})$. Since $D_kD_{n-k}(f) = 0$ if $n - k > 1$ or if $k > n - k + 1$, and $D_1D_1 = 0$, we see that

$$D_*(T, U)(D_*(T)(f)) = D_0D_0(f) + D_1D_0(f)T + D_0D_1(f)U + D_2D_1(f)T^2U.$$

Setting $T = s^2 + st$ and $U = t^2$, we get

$$D_0D_0(f) + D_1D_0(f)(s^2 + st) + D_0D_1(f)t^2 + D_2D_1(f)(s^2 + st)^2t^2,$$

and setting $T = t^2 + st$ and $U = s^2$, we get

$$D_0D_0(f) + D_1D_0(f)(t^2 + st) + D_0D_1(f)s^2 + D_2D_1(f)(t^2 + st)^2s^2.$$

Since $(t^2 + st)^2s^2 = s^2t^4 + 2s^3t^3 + s^4t^2 = t^2(s^2 + st)^2$, and $D_0D_1(f) = D_1D_0(f)$, the theorem is proved. □

Let $\mathscr{A}_2$ denote the mod-2 Steenrod algebra. Thus $\mathscr{A}_2$ is the graded $\mathbf{F}_2$-algebra generated by elements Sq^i of degree i, $i \geq 0$, satisfying $\mathrm{Sq}^0 = 1$ and certain quadratic Adem relations. The point of Bullett and Macdonald's article [2] is that these relations can be encoded in the following elegant way. Let $D_*(T) = \Sigma_{i=0}^{\infty} \mathrm{Sq}^i T^i$, where T is an indeterminant. Then the Adem relations are equivalent to the power series identity

$$D_*(s^2 + st)D_*(t^2) = D_*(t^2 + st)D_*(s^2).$$

Thus Theorem 2.1 has the following corollary.

COROLLARY 2.2. *Suppose that R and D_* are as in Theorem* 2.1. *In addition, suppose that $D_0 =$ identity. Then the equation*

$$\mathrm{Sq}^i(f) \equiv D_i(f)$$

defines an action of $\mathscr{A}_2$ on R. This action is F-linear, satisfies the Cartan formula and the unstable $\mathscr{A}_2$-module condition

$$\mathrm{Sq}^i(f) = 0 \qquad \text{if } i > \deg f,$$

but does not necessarily satisfy the unstable $\mathcal{A}_2$-algebra condition

$$\mathrm{Sq}^{\deg f}(f) = f^2.$$

3. Proof of Theorem 1.1 and other examples

In this section V is a free F-module of rank n. The symmetric algebra $S(V)$ is graded in the usual way by requiring the elements of V to have degree 1.

A *derivation* of $S(V)$ (over F) is a linear endormoprhism D_1 of the graded F-*module* $S(V)$ of degree 1 such that $D_1(fg) = D_1(f)g + fD_1(g)$ for every $f, g \in S(V)$.

LEMMA 3.1. *If $\partial : V = S(V)_1 \to S(V)_2$ is an F-linear map, then there exists a unique derivation D_1 of $S(V)$ such that $D_1 = \partial$ on V, and $D_1 = 0$ on F.*

LEMMA 3.2. *Suppose D_1 is any derivation of $S(V)$ such that $D_1 = 0$ on F. Then there exists a unique unstable higher derivation D_* of $S(V)$ over F such that $D_* = \{id, D_1, \ldots\}$.*

The proofs of the above lemmas can be derived from the following formula. Let $x_1, \ldots, x_n$ be a basis for V. Then

$$D_k(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) = \sum_{\substack{j_1 + \cdots + j_n = k \\ j_i \geq 0}} \binom{\alpha_1}{j_1} \cdots \binom{\alpha_n}{j_n} x_1^{\alpha_1 - j_1} \cdots x_n^{\alpha_n - j_n} (\partial x_1)^{j_1} \cdots (\partial x_n)^{j_n}.$$

Proof of Theorem 1.1

Let $F = \mathbf{F}_2$. Suppose that $M \in \mathrm{End}_F(V)$. Using Lemmas 3.1 and 3.2, define a higher derivation M_* of $S(V)$ over F by $M_1(v) = (M(v))^2$ for every $v \in V$. Since $F = \mathbf{F}_2$, M_1 is linear. Since M_* is unstable, to check that $M_1 M_1 = 0$, it suffices to show $M_1 M_1(v) = 0$ for $v \in V$. Setting $w = Mv$, we see that

$$M_1 M_1(v) = M_1((Mv)^2) = M_1(w^2) = wM_1(w) + M_1(w)w = 0.$$

Theorem 1.1 now follows from Corollary 2.2. □

From now on, we refer to this particular example of an A_2-module as

$$S_M(V).$$

EXAMPLE 3.3. Again, let $F = \mathbf{F}_2$ and let $n = 2$ and choose a basis $\{x_1, x_2\}$ for V, i.e., $S(V) = \mathbf{F}_2[x_1, x_2]$. Let D_* be the unstable higher derivation of $S(V)$ over $\mathbf{F}_2$ defined by

$$D_1(x_1) = x_1^2 + x_1x_2 \quad \text{and} \quad x_1(x_2) = x_1x_2 + x_2^2.$$

Then

$$D_1D_1(x_1) = D_1(x_1^2 + x_1x_2) = D_1(x_1x_2) = (x_1^2 + x_1x_2)x_2 + x_1(x_1x_2 + x_2^2) = 0.$$

Similarly, $D_1D_1(x_2) = 0$, so that D_* defines an $\mathscr{A}_2$ action on $S(V)$. Call this module R. This $\mathscr{A}_2$-module R cannot be isomorphic (as an $\mathscr{A}_2$-module) to any of the examples given in Theorem 1.1. For, we see immediately that D_1 is zero on R_2; however, if $M \in \mathrm{End}_2(F)$ and $M = [m_{ij}]$ as a matrix with respect to our basis $\{x_1, x_2\}$, then

$$\begin{aligned} M_1(x_1x_2) &= (m_{11}x_1^2 + m_{12}x_2^2)x_2 + x_1(m_{21}x_1^2 + m_{22}x_2^2) \\ &= m_{21}x_1^3 + m_{11}x_1^2x_2 + m_{22}x_1x_2^2 + m_{12}x_2^3, \end{aligned}$$

and this quantity cannot be zero if M is not zero.

$\mathscr{A}_2$-modules similar to those in this section can be constructed over any commutative ring F of characteristic 2.

4. The classification of the twisted $\mathscr{A}_2$-actions on $S(V)$

Suppose that $q = 2^s$ for some $s > 0$, and let $\mathbf{F}_q$ be a finite field of order q. Let $G = \mathrm{Gal}(\mathbf{F}_q \backslash \mathbf{F}_2)$; i.e., G is a cyclic group $\{1, \varphi, \varphi^2, \ldots, \varphi^{s-1}\}$ of order s generated by the Frobenius automorphism φ of $\mathbf{F}_q$. From algebra, we know that there exists an element $\omega \in \mathbf{F}_q$ such that $\{\omega, \varphi(\omega), \ldots, \varphi^{s-1}(\omega)\}$ is a basis for $\mathbf{F}_q$ over $\mathbf{F}_2$. Thus we have

LEMMA 4.1. *Corresponding to this choice of basis, there is an isomorphism* $\alpha : \mathbf{F}_q \to \mathbf{F}_2[G]$ *of* $\mathbf{F}_2[G]$*-modules given by*

$$\alpha(\xi_1\omega + \cdots + \xi_s\varphi^{s-1}(\omega)) = \xi_1 + \cdots + \xi_s\varphi^{s-1},$$

where $\xi_i \in \mathbf{F}_2$ *for every* i.

If N is a graded $\mathbf{F}_2[G]$-module, we let N_{triv} denote the same underlying vector space with the trivial G-action. Furthermore, if N is a graded vector space over $\mathbf{F}_2$, and N is simultaneously an $\mathscr{A}_2$-module and an $\mathbf{F}_2[G]$-module such that the actions of $\mathscr{A}_2$ and G on N commute, then we will say that N is a *G-$\mathscr{A}_2$-module.*

In what follows, let N be a G-$\mathscr{A}_2$-module.

The tensor products $\mathbf{F}_q \otimes N$ and $\mathbf{F}_2[G] \otimes N$ (all tensor prducts are taken over $\mathbf{F}_2$) have $\mathscr{A}_2$-module structures via the formula

$$\theta(z \otimes n) = z \otimes \theta(n) \qquad \text{for } \theta \in \mathscr{A}_2.$$

They also have $\mathbf{F}_2[G]$-module structures, given by the (standard) diagonal action of G, i.e.,

$$g(z \otimes n) = gz \otimes gn.$$

Note that this action of G commutes with the $\mathscr{A}_2$-action on both $\mathbf{F}_q \otimes N$ and $\mathbf{F}_2[G] \otimes N$, hence both $\mathbf{F}_q \otimes N$ and $\mathbf{F}_2[G] \otimes N$ are G-$\mathscr{A}_2$-modules.

Define the map $\beta : \mathbf{F}_2[G] \otimes N_{triv} \to \mathbf{F}_2[G] \otimes N$ by

$$\beta(g \otimes n) = g \otimes gn.$$

LEMMA 4.2. *The map β is an isomorphism of $\mathbf{F}_2[G] \otimes N_{triv}$ and $\mathbf{F}_2[G] \otimes N$ as G-$\mathscr{A}_2$-modules.*

COROLLARY 4.3. *The map*

$$\Phi : \mathbf{F}_q \otimes N_{triv} \to \mathbf{F}_q \otimes N$$

given by the composite

$$\mathbf{F}_q \otimes N_{triv} \xrightarrow{\alpha \otimes 1} \mathbf{F}_2[G] \otimes N \xrightarrow{\beta} \mathbf{F}_2[G] \otimes N \xrightarrow{\alpha^{-1} \otimes 1} \mathbf{F}_q \otimes N$$

is an isomorphism of G-$\mathscr{A}_2$-modules.

Since Φ takes fixed points to fixed points and noting that

$$N_{triv} \cong \mathbf{F}_2 \otimes N_{triv} \cong (\mathbf{F}_q \otimes N_{triv})^G,$$

we have

COROLLARY 4.4. *The fixed point map is an isomorphism of $\mathscr{A}_2$-modules*

$$\Phi^G : N \to (\mathbf{F}_q \otimes N)^G \equiv N_\varphi.$$

Explicitly,

$$\Phi^G(n) = \sum_{j=0}^{s-1} \varphi^j(\omega) \otimes \varphi^j(n). \tag{2}$$

Now suppose that N is a graded algebra and that G acts on N via algebra maps. Furthermore, suppose that N is an $\mathscr{A}_2$-*algebra*, i.e., an algebra with an $\mathscr{A}_2$-module structure satisfying the Cartan formula. For example, N might be $H^*(X; \mathbf{F}_2)$, where X is a G-space.

By construction, N_φ will be a sub-$\mathscr{A}_2$-algebra of $\mathbf{F}_q \otimes N$. Inspection of formula (2) reveals that the isomorphism of $\mathscr{A}_2$-modules, $\Phi^G : N \to N_\varphi$, is *not* an algebra map. However, if we let $\tilde{\imath} : \mathbf{F}_q \otimes N_\varphi \to \mathbf{F}_q \otimes N$ denote the inclusion $i : N_\varphi \hookrightarrow \mathbf{F}_q \otimes N$ with the scalars in the domain extended to $\mathbf{F}_q$, then $\tilde{\imath}$ is visibly a map of $\mathscr{A}_2$-algebras and we have

PROPOSITION 4.5. *The $\mathscr{A}_2$-algebra map*

$$\tilde{\imath}: \mathbf{F}_q \otimes N_\varphi \to \mathbf{F}_q \otimes N$$

is an isomorphism.

This is Lemma 3.4 of [5]. The proof is a pleasant and elegant exercise in basic Galois theory, using nothing deeper than the nondegeneracy of the trace form of $\mathbf{F}_q$ over $\mathbf{F}_2$.

Let us investigate what this discussion implies about our modules $S_M(V)$. Suppose that $M \in \mathrm{End}\,(V)$ and $A \in \mathrm{Gl}\,(V)$ satisfy $AM = MA$ and $A^s = \mathrm{I}$. If we set $q = 2^s$ and $G = \mathrm{Gal}\,(\mathbf{F}_q \backslash \mathbf{F}_2)$, then G will act on $S_M(V)$ via $\mathscr{A}_2$-algebra maps by letting $\varphi x = Ax$. Applying Corollary 4.4 and Proposition 4.5 to $N = S_M(V)$, we conclude

$$\Phi^G : S_M(V) \to S_M(V)_\varphi \text{ is an isomorphism of } \mathscr{A}_2\text{-modules,} \tag{3}$$

and

$$\mathbf{F}_q \otimes S_M(V)_\varphi \text{ is a symmetric algebra.} \tag{4}$$

These statements comprise most of the proof of the next theorem.

THEOREM 4.6

$$S_M(V)_\varphi \cong S_{AM}(V)$$

as $\mathscr{A}_2$-algebras. In particular, $S_M(V) \cong S_{AM}(V)$ as $\mathscr{A}_2$-modules.

Proof. We start by observing that for many graded $\mathbf{F}_2$-algebras N, e.g. finitely generated polynomial algebras, it will be true that

$$\mathbf{F}_q \otimes N' \cong \mathbf{F}_q \otimes N \text{ as algebras } \Rightarrow N' \cong N \text{ as algebras.}$$

Thus (4) implies that $S_M(V)_\varphi$ is the symmetric algebra generated by its degree 1 part, which, by (3), can be identified with $\Phi^G(V)$. Therefore to show that $S_M(V)_\varphi \cong S_{AM}(V)$ as $\mathscr{A}_2$-algebras, it suffices to show that if $v \in V$ then $\mathrm{Sq}^1(\Phi^G(v)) = (\Phi^G(AM(v)))^2$. We compute:

$$\begin{aligned}
\mathrm{Sq}^1(\Phi^G(v)) &= \mathrm{Sq}^1\left(\sum_{j=0}^{s-1} \varphi^j(\omega) \otimes A^j(v)\right) \\
&= \sum_{j=0}^{s-1} \varphi^j(\omega) \otimes A^j((\mathrm{Sq}^1(v)) \\
&= \sum_{j=0}^{s-1} \varphi^j(\omega) \otimes A^j((Mv)^2) \\
&= \sum_{j=0}^{s-1} \varphi^j(\omega) \otimes A^j(M)(v^2) \\
&= \left(\sum_{j=0}^{s-1} \varphi^{j-1}(\omega) \otimes A^{j-1}(AM(V))\right)^2 \\
&= (\Phi^G(AM(v)))^2. \qquad \square
\end{aligned}$$

With this last theorem, we can now prove Theorem 1.2.

Proof of Theorem 1.2

$\Rightarrow$): We first establish that

$$\ker(M^j : V \to V) = \ker(\mathrm{Sq}^{2^{j-1}} \cdots \mathrm{Sq}^2 \mathrm{Sq}^1 : V \to S^{2^j}_M(V)) \qquad \text{if } j \geq 1. \tag{5}$$

To see this, we note that in $S_M(V)$, we have

$$\mathrm{Sq}^{\deg(f)}(f) = (Mf)^2 = M(f^2).$$

We can see this by induction on $\deg(f)$. It is true for $i = 1$ by definition; suppose that $\deg(f) = i > 1$. We may suppose that f is a monomial by linearity of both

sides of the equation; say $f = m_1 m_2$ where $\deg(m_1) = 1$ and $\deg(m_2) = \deg(f) - 1$. Since the $\mathscr{A}_2$-action is unstable and satisfies the Cartan formula,

$$\mathrm{Sq}^{\deg(f)}(f) = \mathrm{Sq}^1(m_1)\,\mathrm{Sq}^{\deg(m_2)}(m_2) = (M(m_1))^2(M(m_2))^2 = (M(m_1 m_2))^2$$

since M is a ring homomorphism.

It follows that if $v \in V$, then in $S_M(V)$,

$$\mathrm{Sq}^{2^j-1} \cdots \mathrm{Sq}^2\,\mathrm{Sq}^1(v) = (M^j(v))^{2^j} \qquad \text{for all } j \geq 1.$$

Since $S_M(V)$ has no nonzero nilpotent elements, (5) holds.

Now, if $S_{M_1}(V)$ is isomorphic to $S_{M_2}(V)$ as $\mathscr{A}_2$-modules, then (5) implies that

$$\dim(\ker(M_1^i)) = \dim(\ker(M_2^i)) \qquad \text{for all } i \geq 1.$$

$\Leftarrow$): In Theorem 4.6 and the discussion preceding it we have established that $S_M(V) \cong S_{AM}(V)$ as $\mathscr{A}_2$-modules if $A \in \mathrm{Gl}(V)$ commutes with $M \in \mathrm{End}(V)$. It is also clear $S_M(V) \cong S_{CMC^{-1}}(V)$ as $\mathscr{A}_2$-modules for all $C \in \mathrm{Gl}(V)$. The following exercise in linear algebra completes the proof of Theorem 1.2.

PROPOSITION 4.7. *Let* $\approx$ *be the equivalence relation on* $\mathrm{End}(V)$ *generated by*

(a) $M \approx CMC^{-1}$ *if* $C \in \mathrm{Gl}(V)$, *and*

(b) $M \approx AM$ if $A \in \mathrm{Gl}(V)$ *is such that* $AM = MA$.

Suppose that M_1 *and* M_2 *are in* $\mathrm{End}(V)$. *Then* $M_1 \approx M_2$ *if and only if* $\dim(\ker(M_1^i)) = \dim(\ker(M_2^i))$ *for each* $i \geq 1$.

Proof. $\Rightarrow$): This is straightforward.

$\Leftarrow$): Regard M_1 and M_2 as matrices. Then M_1 and M_2 are conjugate to matrices of the form $N_t \oplus P_t$, where N_t is nilpotent and P_t is invertible. The hypothesis that $\dim(\ker(M_1^i)) = \dim(\ker(M_2^i))$ for all i is precisely the condition that ensures that N_1 and N_2 are conjugate. Multiplying A_t by $\mathrm{I} \oplus P_t^{-1}$ (which commutes with A_t) we thus obtain conjugate matrices, hence $M_1 \approx M_2$. □

5. Final remarks

We begin this section by offering an alternate, more explicit, proof of the fact that, in the situation of Theorem 4.6, the twisted algebra $S_M(V)_\varphi$ is, in fact, a symmetric algebra. This proof uses a result about the action of the Frobenius map on algebraic groups defined over finite fields.

Let K be an algebraic closure of $\mathbf{F}_q$. The Frobenius map φ of $\mathbf{F}_q$ is of course defined on K and defines a Frobenius map φ on $K \otimes V$, $\mathrm{End}_K(K \otimes V)$, and $S(K \otimes V) = K \otimes S(V)$ with the property that $\{z \in Z \mid \varphi^s(z) = z\}$ equals $\mathbf{F}_q \otimes V$, $\mathrm{End}_{\mathbf{F}_q}(\mathbf{F}_q \otimes V)$, or $\mathbf{F}_q \otimes S(V)$, if Z equals $K \otimes V$, $\mathrm{End}_K(K \otimes V)$, or $K \otimes S(V)$, respectively. According to a theorem of Lang (see, e.g., [1, V 16.3, p. 211]), there exists an element $B \in \mathrm{Gl}(K \otimes V)$ such that $A = B^{-1}\varphi(B)$. Since $A^s = \mathrm{I}$ and $\varphi(A) = A$, we see that $\varphi^s(B) = B$ (since $\mathrm{I} = A\varphi(A) \cdots \varphi^{s-1}(A) = B^{-1}\varphi^s(B)$). thus $B \in \mathrm{End}_{\mathbf{F}_q}(\mathbf{F}_q \otimes V)$ and so can also be considerd as an algebra isomorphism of the symmetric algebra $\mathbf{F}_q \otimes S_M(V)$.

PROPOSITION 5.1. *B induces an isomorphism between the subalgebras $S_M(V)_\varphi$ and $\mathbf{F}_2 \otimes S_M(V)$ of $\mathbf{F}_q \otimes S_M(V)$.*

Proof. It suffices to show that if $y \in S_M(V)_\varphi$, then $\varphi(By) = By$ where φ is just acting on the scalars of $\mathbf{F}_q \otimes S_M(V)$. To see this, we suppose that $y = \Phi^G x$ with $x \in S_M(V)$. Then

$$B(\Phi^G(x)) = \sum_{i=0}^{s-1} \varphi^i(\omega) \cdot BA^i(x) = \sum_{i=0}^{s-1} \varphi^i(\omega) \cdot (\varphi(B)A^{i-1})(x) = \varphi(B\Phi^G(x)).$$

Finally we note that the odd prime analogues of this proposition and all the arguments in section 4 clearly hold. Thus the odd prime version of Theorem 1.2 will hold, assuming the odd prime version of Theorem 1.1 has been established. For this, most of the arguments in sections 2 and 3 will generalize in a straightforward manner, though property (iii) of Theorem 2.1 will obviously need modification.

REFERENCES

[1] BOREL, A., *Linear Algebraic Groups*, Springer-Verlag, 1991.
[2] BULLETT, S. R. and MACDONALD, I. G., *On the Adem relations*, Topology *21* (1982), 329–332.
[3] CAMPBELL, H. E. A. and SELICK, P. S., *Polynomial algebras over the Steenrod algebra*, Comment. Math. Helvetici *65* (1990), 171–180.
[4] MATSUMURA, H., *Commutative Ring Theory*, Cambridge University Press, 1980.
[5] WARD, H. N., *Representations of symplectic groups*, Journal of Algebra *20* (1972), 182–195.

Dept. of Mathematics
Colorado State University
Ft. Collins, CO 80523

Dept. of Mathematics
University of Virginia
Charlottesville, VA 22903

Received April 24, 1992