Can. J. Math., Vol. XXVI, No. 2, 1974, pp. 355–364

PRIMITIVE ELEMENTS IN SYMMETRIC ALGEBRAS

GORDON EDWARDS

1. Typical Results. Let R be a commutative ring with 1, and let

$$S(M) = \bigoplus_{i=0}^{\infty} S^i(M)$$

be the symmetric algebra of an R-module M. We regard the isomorphisms $S^0(M) \cong R$ and $S^1(M) \cong M$ as identifications. There is a unique R-algebra homomorphism $\Delta : S(M) \to S(M) \otimes_R S(M)$ (called the comultiplication) satisfying $\Delta(m) = m \otimes 1 + 1 \otimes m$ for all $m \in M$; any element $x \in S(M)$ for which $\Delta(x) = x \otimes 1 + 1 \otimes x$ is said to be primitive. The set of all primitive elements in $S(M)$ is denoted $P(M)$.

Since Δ is a graded homomorphism, $P(M)$ is a graded submodule of $S(M)$; it is the kernel of the graded R-module homomorphism $\sigma_M : S(M) \to S(M) \otimes_R S(M)$ defined by $\sigma_M(x) = \Delta(x) - x \otimes 1 - 1 \otimes x$ for all $x \in S(M)$. Thus $P(M) = \otimes_{i=0}^{\infty} P^i(M)$ where $P^i(M) = P(M) \cap S^i(M)$. It is obvious that $P^0(M) = 0$ and $P^1(M) = M$. We are interested in $P^i(M)$ for $i > 1$.

First we establish a simple technical result. The nth graded component of $S(M) \otimes_R S(M)$ is $\oplus_{j=0}^{n} S^j(M) \otimes S^{n-j}(M)$; let π_j^n be the projection of this component onto the jth summand, and let $\mu : S(M) \otimes_R S(M) \to S(M)$ be the multiplication morphism $[\mu(a \otimes b) = ab]$.

LEMMA 1. $(\mu \circ \pi_j^n \circ \Delta)(x) = \binom{n}{j} x$ *for all* $x \in S^n(M)$.

Proof. Since $S(M)$ is generated (as an R-algebra) by M, it suffices to prove the result for $x = m_1 \ldots m_n$ with $m_i \in M$ for $i = 1, \ldots, n$. Since Δ is an algebra map, we have

$$\begin{aligned}\Delta x &= (\Delta m_1) \ldots (\Delta m_n)\\ &= (m_1 \otimes 1 + 1 \otimes m_1) \ldots (m_n \otimes 1 + 1 \otimes m_n)\\ &= \sum_{j=0}^{n} \sum_{(\lambda)} m_{\lambda_1} \ldots m_{\lambda_j} \otimes m_1 \ldots \hat{m}_{\lambda_1} \ldots \hat{m}_{\lambda_j} \ldots m_n\end{aligned}$$

where the second summation extends over all j-tuples $(\lambda) = (\lambda_1, \ldots, \lambda_j) \in Z^j$ with $1 \leqq \lambda_1 < \ldots < \lambda_j \leqq n$. The number of such j-tuples is $\binom{n}{j}$, so that $(\mu \circ \pi_j^n \circ \Delta)(x) = \binom{n}{j} x$ as claimed.

Received October 20, 1972 and in revised form, September 5, 1973. This research constitutes part of the author's Ph.D. thesis, written at Queen's University under the direction of Professor P. Ribenboim. Financial assistance from the Canada Council is gratefully acknowledged.

https://doi.org/10.4153/CJM-1974-037-1 Published online by Cambridge University Press

Observe that $(\pi_0{}^n \circ \Delta)(x) = 1 \otimes x$ and $(\pi_n{}^n \circ \Delta)(x) = x \otimes 1$ for all $x \in S^n(M)$. Thus a necessary and sufficient condition for x to be primitive is $(\pi_j{}^n \circ \Delta)(x) = 0$ for $0 < j < n$. Combining this with the preceding result, we have the following:

THEOREM 1. *If p is a prime number such that all integers prime to p are units in R, then $P^n(M) = 0$ unless n is a power of p.*

Proof. Let $n = p^r s$ with s not divisible by p. If $x \in P^n(M)$, then $(\pi_j{}^n \circ \Delta)(x) = 0$ and therefore $(\mu \circ \pi_j{}^n \circ \Delta)(x) = \binom{n}{j} x = 0$ for $0 < j < n$ (using lemma 1). Now, in general $\binom{p^r s}{p^r} \equiv s (\mathrm{mod}\, p)$, so $\binom{n}{p^r}$ is not divisible by p if $s \neq 0$, and evidently $0 < p^r < n$ if $s > 1$. Consequently $\binom{n}{p^r} x = 0$ provided $s > 1$, and since $\binom{n}{p^r}$ is a unit in R, $x = 0$. Thus $P^n(M) = 0$ unless n is a power of p (i.e., $s = 1$) or $n = 0$ (i.e., $s = 0$); but we know already that $P^0(M) = 0$.

COROLLARY 1. *$P(M) = M$ for all R-modules M if and only if R is an algebra over $\mathbf{Q}$, the field of rational numbers.*

Proof. R is a $\mathbf{Q}$-algebra if and only if every integer is a unit in R. If R is a $\mathbf{Q}$-algebra, therefore, $P^n(M) = 0$ unless $n = 1$ (from Theorem 1). On the other hand, if R is not a $\mathbf{Q}$-algebra, then some integer t is not a unit in R, and therefore some prime number p (e.g. some prime divisor of t) is not a unit in R. Let $M = R/pR$, so that $S(M) \cong R[X]/(pX)$. In this case x^{p^e} is a non-zero primitive element of degree p^e for all $e \geqq 0$ (where x is the residue class of X modulo pX). For, since $px = 0$, the p-power map is additive in terms involving x, and

$$\Delta(x^{p^e}) = (\Delta x)^{p^e} = (x \otimes 1 + 1 \otimes x)^{p^e} = x^{p^e} \otimes 1 + 1 \otimes x^{p^e}.$$

For this choice of M, therefore, we have $P^{p^e}(M) \neq 0$ for all $e \geqq 0$.

Note that the hypothesis of Theorem 1 covers not only rings of characteristic p, but also rings in which p is nilpotent (such as $Z/(p^r)$) and rings in which p is topologically nilpotent (such as Z_p, the ring of p-adic integers). The example given in Corollary 1 illustrates that in such cases, there do exist modules M with $P^{p^e}(M) \neq 0$ for all $e \geqq 0$.

If R has prime characteristic $p > 0$, there is a well-known characterization of the module $P(M)$ when M is projective of finite type; namely,

$$P(M) = \bigoplus_{r=0}^{\infty} M^{(p^r)},$$

where $M^{(p^r)}$ is the submodule of $S^{p^r}(M)$ generated by $\{m^{p^r} | m \in M\}$. Obviously

https://doi.org/10.4153/CJM-1974-037-1 Published online by Cambridge University Press

$M^{(p^r)} \subset P^{p^r}(M)$ in any event, since the p-power map is additive in characteristic p. The reverse inclusion is first proved for free modules.

THEOREM 2. *If M is free, then $P(M) = \bigoplus_{r=0}^{\infty} M^{(p^r)}$.*

Proof. Let Y be a basis for M, so that $S(M) = R[X_y]_{y\in Y}$, a polynomial algebra in the indeterminates X_y. $S(M) \otimes_R S(M)$ is likewise a polynomial algebra in the indeterminates $Z_y = X_y \otimes 1$ and $Z_y' = 1 \otimes X_y$. Any $f \in S^{p^r}(M)$ is a homogeneous polynomial in finitely many of the indeterminates, say $X_1, \ldots, X_t$; we proceed by induction on t.

The comultiplication Δ maps X_i to $Z_i + Z_i'$ for $i = 1, \ldots, t$, so we have

$$\Delta f(X_1, \ldots, X_t) = f(Z_1 + Z_1', \ldots, Z_t + Z_t').$$

On the other hand

$$f(X_1, \ldots, X_t) \otimes 1 = f(Z_1, \ldots, Z_t)$$

and

$$1 \otimes f(X_1, \ldots, X_t) = f(Z_1', \ldots, Z_t').$$

Therefore $f(X_1, \ldots, X_t)$ is primitive if and only if

$$f(Z_1 + Z_1', \ldots, Z_t + Z_t') = f(Z_1, \ldots, Z_t) + f(Z_1', \ldots, Z_t').$$

We now apply the homomorphism from $S(M) \otimes_R S(M)$ to $S(M)$ defined by the "substitutions":

$$\begin{array}{ll} Z_1 \rightarrow X_1 & Z_1' \rightarrow 0 \\ Z_i \rightarrow 0 & Z_i' \rightarrow X_i \, [i = 2, \ldots, t] \end{array}$$

obtaining the identity

$$\begin{aligned} f(X_1, \ldots, X_t) &= f(X_1, 0, \ldots, 0) + f(0, X_2, \ldots, X_t) \\ &= a_1 X_1^{p^r} + f(0, X_2, \ldots, X_t) \end{aligned}$$

for some $a_1 \in R$. Since $a_1 X_1^{p^r}$ is primitive, $f(0, X_2, \ldots, X_t)$ is also primitive. By induction, we conclude that

$$f(X_1, \ldots, X_t) = a_1 X_1^{p^r} + \ldots + a_t X_t^{p^r} \in M^{(p^r)}.$$

The preceding result can be extended to include projective modules of finite type, using the techniques of localization. For if M is such a module, then there is a family of generators $\{f_1, \ldots, f_r\}$ for R such that M_{f_i} is a free R_{f_i}-module for $i = 1, \ldots, r$. Moreover, the natural homomorphism $\phi_i : S(M) \rightarrow S(M_{f_i})$ preserves the comultiplication, so that if $x \in S^{p^r}(M)$ is primitive, $x_i = \phi_i(x)$ is also primitive. Since M_{f_i} is free over R_{f_i}, we must have $x_i \in (M_{f_i})^{(p^r)}$ for $i = 1, \ldots, r$. But

$$S(M_{f_i}) \cong S(M) \otimes_R R_{f_i} \cong S(M)_{f_i},$$

and it is easy to see that $(M_{f_i})^{(p^r)}$ corresponds to $(M^{(p^r)})_{f_i}$ in this isomorphism.

https://doi.org/10.4153/CJM-1974-037-1 Published online by Cambridge University Press

Since $f_1, \ldots, f_r$ generates the unit ideal of R, it follows that $x \in M^{(p^r)}$, which establishes the result:

COROLLARY 2. *If M is projective of finite type, then*

$$P(M) = \bigoplus_{r=0}^{\infty} M^{(p^r)}.$$

The question then arises: if R is a ring of prime characteristic p, is $P(M) = \bigoplus_{r=0}^{\infty} M^{(p^r)}$ always? Is it true if M is of finite presentation at least? We shall show that this is not generally so, by exhibiting a ring R of characteristic p and an R-module M for which $P^{p^r}(M) \neq M^{(p^r)}$ for any $r \geqq 0$. Actually, this will be done for a large class of rings.

2. Untypical Results. Henceforth we suppose that $R = k \oplus V$, where k is a field of characteristic $p > 0$ and V is a maximal ideal of R with $\dim_k(V/V^2) \geqq 2$. Choose $v_1, v_2 \in V$ so that their residues are linearly independent in V/V^2. Let F be a free R-module with R-basis $\{s_1, s_2\}$ and let $e = v_1 s_1 + v_2 s_2$. Let $M = F/Re$ and let $\pi : S(F) \to S(M)$ be the ring homomorphism (onto) induced by the module epimorphism $F \to M$. Consider the element $z = v_1 s_1^{p^r - 1} s_2 \in S^{p^r}(F)$.

THEOREM 3. *$\pi(z) \in P^{p^r}(M)$ for all choices of p and r, but $\pi(z) \notin M^{(p^r)}$ unless $p = 2$ and $r = 1$.*

Proof. We first show that $\pi(z) \in P(M) = \ker(\sigma_M)$. By the commutativity of the accompanying diagram, it suffices to show that $\sigma_F(z) \in \ker(\pi \otimes \pi)$:

$$\begin{tikzcd}
S(F) \arrow[r, "\sigma_F"] \arrow[d] & S(F) \otimes_R S(F) \arrow[d, "\pi \otimes \pi"] \\
S(M) \arrow[r, "\sigma_M"] & S(M) \otimes_R S(M) .
\end{tikzcd}$$

Straightforward computation yields:

$$\begin{aligned}
\sigma_F(z) &= \Delta(z) - z \otimes 1 - 1 \otimes z \\
&= v_1(\Delta s_1)^{p^r-1}(\Delta s_2) - v_1 s_1^{p^r-1} s_2 \otimes 1 - 1 \otimes v_1 s_1^{p^r-1} s_2 \\
&= v_1[(s_1 \otimes 1 + 1 \otimes s_1)^{p^r-1}(s_2 \otimes 1 + 1 \otimes s_2) \\
&\qquad\qquad - s_1^{p^r-1} s_2 \otimes 1 - 1 \otimes s_1^{p^r-1} s_2] \\
&= v_1 \sum_{j=1}^{p^r-1} \left[\binom{p^r - 1}{j} s_1^{j} \otimes s_1^{p^r-j-1} s_2 + \binom{p^r - 1}{j - 1} s_1^{j-1} s_2 \otimes s_1^{p^r-j} \right] \\
&= v_1 \sum_{j=1}^{p^r-1} (-1)^j [s_1^{j} \otimes s_1^{p^r-j-1} s_2 - s_1^{j-1} s_2 \otimes s_1^{p^r-j}].
\end{aligned}$$

Here we have used the binomial theorem and the fact that $\binom{p^r - 1}{j} \equiv (-1)^j$ (mod p). Now we show that each summand in this expression lies in the kernel of $\pi \otimes \pi$. If $\pi(s_1) = m_1$ and $\pi(s_2) = m_2$, we will freely use the fact that $(v_1m_1 + v_2m_2) \otimes 1 = 0$ and $1 \otimes (v_1m_1 + v_2m_2) = 0$ in $S(M) \otimes_R S(M)$. Since

$$\begin{aligned} v_1m_1{}^j \otimes m_1{}^{p^r-j-1}m_2 &= -v_2m_2m_1{}^{j-1} \otimes m_1{}^{p^r-j-1}m_2 \\ &= -m_1{}^{j-1}m_2 \otimes m_1{}^{p^r-j-1}v_2m_2 = m_1{}^{j-1}m_2 \otimes v_1m_1{}^{p^r-j} \\ &= v_1m_1{}^{j-1}m_2 \otimes m_1{}^{p^r-j} \end{aligned}$$

it follows that

$$\begin{aligned} &v_1(\pi \otimes \pi)(s_1{}^j \otimes s_1{}^{p^r-j-1}s_2 - s_1{}^{j-1}s_2 \otimes s_1{}^{p^r-j}) \\ &\quad = v_1m_1{}^j \otimes m_1{}^{p^r-j-1}m_2 - v_1m_1{}^{j-1}m_2 \otimes m_1{}^{p^r-j} = 0. \end{aligned}$$

Therefore $(\pi \otimes \pi)(\sigma_F(z)) = \sigma_M(\pi(z)) = 0$, and $\pi(z) \in P(M) \cap S^{p^r}(M) = P^{p^r}(M)$ as claimed.

It remains to show that $\pi(z) \notin M^{(p^r)}$ unless $p = 2$ and $r = 1$, in which case

$$\pi(z) = v_1m_1m_2 = -v_2m_2{}^2 \in M^{(2)}.$$

Suppose, then, that $\pi(z) = a_1m_1{}^{p^r} + a_2m_2{}^{p^r}$ for some $a_1, a_2 \in R$. It follows that $z - a_1s_1{}^{p^r} - a_2s_2{}^{p^r} \in \ker(\pi)$, or more explicitly

$$v_1s_1{}^{p^r-1}s_2 - a_1s_1{}^{p^r} - a_2s_2{}^{p^r} = g(v_1s_1 + v_2s_2)$$

for some $g \in S(F)$. Reducing all coefficients modulo V^2, we may assume $V^2 = 0$. And, since $R = k \oplus V$, we may further assume that g has all its coefficients in k. As v_1 and v_2 are linearly independent after reducing modulo V^2, there can be no cancellations in expanding the product $g(v_1s_1 + v_2s_2)$. Since at most 3 terms survive, g must be a monomial, and in fact $g = s_1{}^{p^r-2}s_2$ is the only possibility. But then $g(v_1s_1 + v_2s_2) = v_1s_1{}^{p^r-1}s_2 + v_2s_1{}^{p^r-2}s_2{}^2$, from which we see that $\pi(z) \notin M^{(p^r)}$ unless $p^r = 2$ (i.e. $p = 2$ and $r = 1$).

We have exhibited an R-module M with one relation ($e = v_1s_1 + v_2s_2$) having the property that $P^{p^r}(M) \neq M^{(p^r)}$ unless $p = 2$ and $r = 1$. It is perhaps worth mentioning that such examples are not easy to come by. In characteristic 3, for instance, if $V^2 = 0$, this is the "only" R-module defined by one relation for which $P^3(M) \neq M^{(3)}$. We use the fact, that when $V^2 = 0$, any R-module M can be uniquely represented in the form F/A where F is free and $A \subset VF$. Uniqueness means that if F/A and F'/A' are two such representations for M, there is an isomorphism $\alpha : F \to F'$ with $\alpha(A) = A'$.

THEOREM 4. *Let $R = k \oplus V$ as before, where k is a field of characteristic 3 and $V^2 = 0$. If $N = F/Re$ is an R-module defined by one relation $e \in VF$ such that $P^3(N) \neq N^{(3)}$, then $N \cong M \oplus M'$, where M is the R-module of Theorem 3 and M' is a free R-module.*

https://doi.org/10.4153/CJM-1974-037-1 Published online by Cambridge University Press

Proof. Let X be an R-basis for the free module F, and let

$$e = \sum_{i=1}^{r} v_i s_i$$

with $v_i \in V$ and $s_i \in X$ for $i = 1, \ldots, r$. We first show that W, the k-space spanned by the vectors $\{v_1, \ldots, v_r\}$, must have dimension less than three if $P^3(N) \neq N^{(3)}$. We will take advantage of the following commutative diagram:

$$\begin{tikzcd}
S^3(F) \arrow[r, "\sigma_F"] \arrow[d, "\lambda"] & \bigoplus_{i+j=3} S^i(F) \otimes_R S^j(F) \arrow[r, "\pi_F"] \arrow[d, "\mu"'] & S^2(F) \otimes_R F \arrow[d, "\nu"'] \\
S^3(N) \arrow[r, "\sigma_N"] & \bigoplus_{i+j=3} S^i(N) \otimes_R S^j(N) \arrow[r, "\pi_N"] & S^2(N) \otimes_R N .
\end{tikzcd}$$

Here λ, μ, ν are induced by the map $F \rightarrow N$ and π_F, π_N are projections onto the appropriate summands.

If

$$x = \sum_{i \leqslant j \leqslant k} a_{ijk} s_i s_j s_k \in S^3(N)$$

with $a_{ijk} \in R$ then (writing σ' for $\pi_F \circ \sigma_F$) we have

$$(1) \quad \sigma'(x) = \sum a_{ijk}(s_i s_j \otimes s_k + s_k s_i \otimes s_j + s_j s_k \otimes s_i).$$

Since the kernel of ν is generated by elements of the form $s_i e \otimes s_k$ and $s_i s_j \otimes e$, we cannot have $\lambda(x) \in P^3(N)$ unless

$$(2) \quad \sigma'(x) = \sum_{i,k} b_{ik} s_i e \otimes s_k + \sum_{i \leqslant j} c_{ij} s_i s_j \otimes e$$

for some b_{ik} and $c_{ij} \in k$.

By comparing the coefficients in expressions (1) and (2) and manipulating the resulting equations, it can be shown that $b_{ii} = 2c_{ii}$ (for $i = 1, \ldots, r$) if W has dimension $\geqq 2$, and $c_{ij} = b_{ij} = b_{ji}$ (for all $i \neq j$) if W has dimension $\geqq 3$. Thus, letting

$$y = \sum_{i \leqslant j} c_{ij} s_i s_j e,$$

we have $\sigma'(x) = \sigma'(y)$ if W has dimension $\geqq 3$. Since Δ is a cocommutative comultiplication, it follows that $\sigma(x) = \sigma(y)$ and hence $x - y \in P^3(F) = F^{(3)}$. Since $\lambda(y) = 0$, $\lambda(x) \in N^{(3)}$; this proves that $P^3(N) = N^{(3)}$ if W has dimension $\geqq 3$.

We now know that W must have dimension 2 or 1 if $P^3(N) \neq N^{(3)}$. In the first case we can write $e = v_1 f_1 + v_2 f_2$ where f_1 and f_2 are k-linear combinations of $\{s_1, \ldots, s_r\}$. If f_1 and f_2 are independent over R, we can choose a new R-basis for F of the form $\{f_1, f_2\} \cup Y$, and then we have $N = M \oplus M'$ where M is the module of Theorem 3 and M' is free with basis Y. On the other hand,

https://doi.org/10.4153/CJM-1974-037-1 Published online by Cambridge University Press

if f_1 and f_2 are not independent, then $e = (v_1 + av_2)f_1$ for some $a \in k$, and we are reduced to the second case (the dimension of W is 1). But it is easy to see that in this case $P^3(N) = N^{(3)}$ necessarily, which concludes the proof.

3. The characteristic two case. Theorem 3 leaves unanswered the question of finding an R-module M in the characteristic two case for which $P^2(M) \neq M^{(2)}$. As we shall see, if $V^2 = 0$, any such module must have at least three generators and at least three relations. Here we treat the case of a module defined by one relation.

THEOREM 5. *Let $R = k \oplus V$ as before, where k is a field of characteristic* 2 *and $V^2 = 0$. If $N = F/Re$ is an R-module defined by one relation $e \in VF$, then $P^2(N) = N^{(2)}$.*

Proof. Let $\{s_i\}_{i \in I}$ be an R-basis for F (where I is well-ordered) and let $e = \sum_{j \in J} v_j s_j$ with $0 \neq v_j \in V$ for all $j \in J \subset I$. Note that $\sigma_F(s_i s_j) = s_i \otimes s_j + s_j \otimes s_i$ for all $i, j \in I$. We will take advantage of the commutative diagram below, noting that $\ker(\pi \otimes \pi) = F \otimes_R Re + Re \otimes_R F$:

$$\begin{tikzcd}
S^2(F) \arrow[r, "\sigma_F"] \arrow[d] & F \otimes F \arrow[d, "\pi \otimes \pi"] \\
S^2(N) \arrow[r, "\sigma_N"] & N \otimes N .
\end{tikzcd}$$

Take $x = \sum_{i \leqq j} d_{ij} s_i s_j \in S^2(F)$. If $\sigma_F(x) \in \ker(\pi \otimes \pi)$ (i.e. if $\pi(x) \in P^2(M)$), we obtain an equation

$$(1) \quad \sum_{i<j} d_{ij}(s_i \otimes s_j + s_j \otimes s_i) = \sum_{i \in I} b_i(s_i \otimes e) + \sum_{i \in I} c_i(e \otimes s_i)$$

for some $b_i, c_i \in k$. For every $j \in J$, the right hand side of (1) contributes a term $(b_j + c_j)v_j(s_j \otimes s_j)$. Since no such term occurs on the left hand side and $v_j \neq 0$, we have $b_j = c_j$ for all $j \in J$.

Now let $\tau : F \otimes F \rightarrow F \otimes F$ be the "twist" map, sending $s_i \otimes s_j$ to $s_j \otimes s_i$. Applying τ to (1), we obtain

$$\sum_{i<j} d_{ij}(s_i \otimes s_j + s_j \otimes s_i) = \sum_{i \in I} b_i(e \otimes s_i) + \sum_{i \in I} c_i(s_i \otimes e)$$

which, added to (1), yields

$$(2) \quad \sum_{i \in I} (b_i + c_i)(e \otimes s_i) = \sum_{i \in I} (b_i + c_i)(s_i \otimes e).$$

If $i \notin J$ and $j \in J$, the left hand side contributes a term $(b_i + c_i)v_j(s_j \otimes s_i)$, which does not occur on the right-hand side. Thus $b_i = c_i$ for all $i \notin J$, since $v_j \neq 0$.

We have so far shown that $b_i = c_i$ for all $i \in I$, provided $J \neq \emptyset$. (If $J = \emptyset$, then $N = F$ is free and there is nothing to prove.) Substituting in (1) yields

$$\sum_{i<j} d_{ij}(s_i \otimes s_i + s_j \otimes s_i) = \sum_{i\in I} b_i(e \otimes s_i + s_i \otimes e).$$

Hence

$$\sum_{i<j} d_{ij}s_is_j - \sum_{i\in I} b_ies_i \in \ker(\sigma_F) = F^{(2)},$$

so

$$x = \sum_{i\leqq j} d_{ij}s_is_j = \sum_{i\in I} b_ies_i + \sum a_is_i^2$$

for some $a_i \in R$. It follows that $\pi(x) \in N^{(2)}$, because $\sum_{i\in I} b_ies_i \in \ker(\pi)$. Therefore $P^2(N) = N^{(2)}$ as claimed.

The question remains: if $R = k \oplus V$ where k is a field of characteristic 2 and $V^2 = 0$, does there exist an R-module M for which $P^2(M) \neq M^{(2)}$?

Let F be free with R-basis $\{s_1, \ldots, s_m\}$ and suppose there are n relations given by

$$e_i = \sum_{l=1}^{m} v_{il}s_l \quad [i = 1, \ldots, n]$$

with $v_{il} \in V$. Reformulate the problem in terms of matrices. Let W be the $n \times m$ matrix with vector entries v_{ij}, and W^t its transpose. Write

$$x = \textstyle\sum_{i\leqq j} d_{ij}s_is_j \in S^2(F)$$

as before, and let $D = (d_{ij})_{i,j}$ be the upper triangular matrix obtained by setting $d_{ij} = 0$ for $i > j$. We then have the following two results:

LEMMA 2. *$\pi(x) \in P^2(M)$ if and only if $D + D^t = W^tB^t + CW$ for some $m \times n$ matrices B and C with entries in k.*

LEMMA 3. *$\pi(x) \in M^{(2)}$ if and only if $D + D^t = W^tH^t + HW$ for some $m \times n$ matrix H with entries in k.*

These results follow by straightforward computation.

A skew-symmetric matrix in characteristic 2 is a symmetric matrix with zeros along the diagonal. The matrices B and C of Lemma 2 have the property that $W^tB^t + CW$ is skew-symmetric; conversely, if B_0 and C_0 are given matrices such that $G = W^tB_0^t + C_0W$ is skew-symmetric, then

$$x = \textstyle\sum_{i\leqq j} g_{ij}s_is_j \in S^2(F)$$

has $\sigma_F(x) \in \ker(\pi \otimes \pi)$, so that $\pi(x) \in P^2(M)$. The elements of $P^2(M)$ so obtained give a complete set of coset representatives for the module $P^2(M)/M^{(2)}$. Our problem is therefore reduced to finding matrices B, C, and W such that $W^tB^t + CW$ is skew-symmetric, but

$$W^tB^t + CW \neq W^tH^t + HW$$

https://doi.org/10.4153/CJM-1974-037-1 Published online by Cambridge University Press

for all matrices H with entries in k. If $\{x_1, \ldots, x_r\}$ is a basis for the subspace of V generated by the $\{v_{ij}\}$, we have $W = W_1x_1 + \ldots + W_rx_r$ where the W_i are uniquely determined matrices with entries in k. Our problem can now be formulated entirely in terms of linear algebra over the field k.

Question. Can we find $m \times n$ matrices $W_1{}^t, \ldots, W_r{}^t, B, C$, with entries in k, such that each $W_i{}^tB^t + CW_i$ is skew symmetric, but for which there is no matrix H satisfying the equations

$$W_i{}^tB^t + CW_i = W_i{}^tH^t + HW_i \text{ for } i = 1, \ldots, r?$$

This unusual condition is surprisingly hard to satisfy. In fact it cannot be satisfied at all unless $m \geqq 3$ and $n \geqq 3$.

LEMMA 4. *If $n \leqq 2$ or $m \leqq 2$, the answer to the Question is "no".*

The proof is left as an exercise.

COROLLARY 3. *In characteristic two, if $R = k \oplus V$ with $V^2 = 0$ as before, any R-module M for which $P^2(M) \neq M^{(2)}$ must have at least 3 generators and at least 3 independent relations.*

We now give an explicit example with $n = m = 3$ where the Question has an affirmative answer. Set

$$B = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad C = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

$$W_1 = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} \qquad W_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \qquad W_3 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}.$$

It can be seen in this case that there is no matrix H with $W_i{}^tH^t + HW_i = W_i{}^tB^t + CW_i$ for $i = 1, 2, 3$, although the right-hand sides are all skew-symmetric.

Translating this example in module terms, let k be a field of characteristic 2, V a k-space of dimension >2, and $R = k \oplus V$ where the ring structure on R is determined by the k-action on V and the requirement $V^2 = 0$.

The matrix W of Lemma 2 is then given by

$$W = \begin{bmatrix} 0 & v_2 & v_1 + v_2 \\ v_2 & v_2 & v_3 \\ v_1 & v_1 + v_3 & v_3 \end{bmatrix}$$

with v_1, v_2, v_3 linearly independent in V. Let $M = F/A$ where F is free with R-basis $\{s_1, s_2, s_3\}$ and A is the submodule of F generated by

$$e_1 = v_2s_2 + (v_1 + v_2)s_3$$
$$e_2 = v_2(s_1 + s_2) + v_3s_3$$
$$e_3 = v_1(s_1 + s_2) + v_3(s_2 + s_3).$$

https://doi.org/10.4153/CJM-1974-037-1 Published online by Cambridge University Press

Since

$$W^tB^t + CW = \begin{bmatrix} 0 & v_1 + v_2 + v_3 & v_3 \\ v_1 + v_2 + v_3 & 0 & v_1 + v_2 \\ v_3 & v_1 + v_2 & 0 \end{bmatrix},$$

it follows from Lemmas 2 and 3 that the element

$$z = (v_1 + v_2 + v_3)s_1s_2 + v_3s_1s_3 + (v_1 + v_2)s_2s_3$$

has the property that $\pi(z) \in P^2(M)$ but $\pi(z) \notin M^{(2)}$. We know of no simpler example.

THEOREM 6. *Let $R = k \oplus V$ as before, where k is a field of characteristic* 2 *and $V^2 = 0$. If V has dimension $\geqq 3$, there exists an R-module M for which $P^2(M) \neq M^{(2)}$.*

Remark. Let L be a restricted lie algebra over a ring R of prime characteristic p, and $U(L)$ its restricted universal enveloping algebra. It is well known that $U(L)$ possesses a cocommutative comultiplication, and that the lie algebra of primitive elements in $U(L)$ is isomorphic to L itself if the latter is projective of finite type as an R-module.

In particular, any R-module M can be regarded as a restricted lie algebra over R with trivial bracket $[m, m'] = 0$ and trivial p-map $m^{[p]} = 0$ for all $m, m' \in M$. As such, its restricted universal enveloping algebra is $S(M)/M^{(p)}S(M)$, and the canonical projection $S(M) \rightarrow S(M)/M^{(p)}S(M)$, preserves comultiplication. It follows that any primitive element in $S^p(M)$ which is not in $M^{(p)}$ gives rise to a nonzero primitive element of degree p in $S(M)/M^{(p)}S(M)$. The examples of Theorems 3 and 6 can accordingly be interpreted as examples of restricted lie algebras which are not projective of finite type and which cannot be recovered as the set of primitive elements in the restricted universal enveloping algebra, even though the canonical map $L \rightarrow U(L)$ is an inclusion.

University of British Columbia,
Vancouver, British Columbia

https://doi.org/10.4153/CJM-1974-037-1 Published online by Cambridge University Press