

POLYNOMIAL ALGEBRAS OVER THE STEENROD ALGEBRA VARIATIONS ON A THEOREM OF ADAMS AND WILKERSON

by LARRY SMITH and R. M. SWITZER

(Received 29th September 1982)

0. Introduction

The problem of deciding which graded polynomial algebras over the field \mathbb{F}_p of p elements can occur as the \mathbb{F}_p -cohomology of a space has played a central rôle in the development of algebraic topology beginning as early as 1950. In the case where the polynomial generators do not occur in dimensions divisible by p , Adams and Wilkerson [1] have given a complete solution by showing that the spaces constructed by Clark and Ewing [3] suffice to realize all such algebras as \mathbb{F}_p -cohomology rings. The main result of Adams and Wilkerson for odd primes can be stated as follows.

Main Theorem (Adams, Wilkerson). *Let p be an odd prime and*

$$H^* \cong \mathbb{F}_p[x_1, \dots, x_n], \text{ deg } x_i = 2d_i, 1 \leq i \leq n,$$

be an unstable algebra over the Steenrod algebra, where $p \nmid d_1 d_2 \dots d_n$. Then there exists a subgroup $G < GL(n, \mathbb{F}_p)$ of order $d_1 d_2 \dots d_n$ generated by pseudoreflections such that

$$H^* \cong \mathbb{F}_p[t_1, \dots, t_n]^G, \text{ deg } t_i = 2, \quad i = 1, 2, \dots, n,$$

as algebras over the Steenrod algebra.

Note: Since t_1, \dots, t_n have degree 2, there is a unique action of the Steenrod algebra on $\mathbb{F}_p[t_1, \dots, t_n]$ making the latter into an unstable algebra over the Steenrod algebra—i.e. such that the Cartan formula holds and

$$P^k x = \begin{cases} x^p & \text{if } \text{deg } x = 2k \\ 0 & \text{if } \text{deg } x < 2k. \end{cases} \quad (1)$$

This second condition is the so-called instability condition.

For $p=2$ there is an analogous result.

The object of the present paper is to show that by rearranging the ideas of Adams and Wilkerson one can achieve a much shorter proof of the main theorem than that given in [1]. In particular we shall not need the construction of algebraic closures in the

category of unstable integral domains over the Steenrod algebra. A central ingredient here will be the Dickson algebra

$$D^*(n) = \mathbb{F}_p[t_1, \dots, t_n]^{GL(n, \mathbb{F}_p)}$$

of full invariants in $\mathbb{F}_p[t_1, \dots, t_n]$ (cf. [7]).

We wish to thank the members of the Topology Oberseminar in Göttingen for their active participation in connection with this topic in the summer semester of 1981 and Clarence Wilkerson for bringing [9] to our attention.

1. Recollections and preliminaries

We begin by recalling the salient aspects of the theory of algebraic extensions for algebras over the Steenrod algebra as developed in [1], [8] and [9]. Throughout this paper p denotes a fixed prime, which for convenience of notation and to avoid doubling the exposition we assume to be odd. \mathcal{P}^* denotes the Hopf algebra of Steenrod reduced powers (no Bockstein). By an algebra over \mathcal{P}^* we mean a graded \mathbb{F}_p -algebra which is an algebra over the Hopf algebra \mathcal{P}^* in the usual sense. We say that an algebra A^* over \mathcal{P}^* is *unstable* if (1) holds. We shall be working exclusively with *graded integral domains* over \mathcal{P}^* and we introduce the notation $\text{Un Id}/\mathcal{P}^*$ for the category of unstable graded integral domains over \mathcal{P}^* .

Note: As $p \neq 2$, a graded integral domain must be concentrated in even degrees.

An injective morphism $\varphi: A^* \hookrightarrow B^*$ in $\text{Un Id}/\mathcal{P}^*$ is called an *algebraic extension* if every element in B^* is a root of a polynomial equation with coefficients in A^* . Since we are working with graded objects, some care must be taken about the grading here. Specifically if $b \in B^{2d}$ we say b is algebraic over A^* if there is a homogeneous polynomial $p(X) \in A^*[X]$, where X is an indeterminate of degree $2d$, such that $p(b) = 0$. The element b is called *separable*, *integral*, etc. if $p(X)$ can be chosen separable, integral (i.e. leading coefficient 1), etc.

In [1] Adams and Wilkerson develop a thorough theory of algebraic closures in $\text{Un Id}/\mathcal{P}^*$. For our purposes, however, the following result of Wilkerson [9; Theorem C] building on a previous result of Serre [5] is sufficient.

Algebraic Closure Theorem (Serre, Wilkerson). *If $P^* = \mathbb{F}_p[t_1, \dots, t_n]$ is a polynomial algebra on generators t_i of degree 2 and $P^* < B^*$ is an integral extension in $\text{Un Id}/\mathcal{P}^*$, then $P^* = B^*$.*

In [8] Wilkerson shows how to extend the action of \mathcal{P}^* from an $A^* \in \text{Un Id}/\mathcal{P}^*$ to its field of fractions $F(A^*)$: if

$$P_\xi: A^* \rightarrow A^*[[\xi]], P_\xi(a) = \sum_{k=0}^{\infty} P^k(a)\xi^k$$

denotes the “giant Steenrod reduced power” and $a/b \in F(A^*)$ then

$$P_\xi\left(\frac{a}{b}\right) = \frac{P_\xi(a)}{P_\xi(b)} \in F(A^*)[[\xi]].$$

This makes sense as a formal power series in ξ since the leading coefficient of $P_\xi(b)$ is $b \neq 0$. Wilkerson further proves the

Separable Extension Lemma (Wilkerson). *Let K^* be a graded field over \mathcal{P}^* and $L^* > K^*$ a separable field extension. Then there is a unique extension to L^* of the \mathcal{P}^* -algebra structure of K^* .*

In the entire theory derivations play a major rôle (for example the primitive elements $P^{\Delta_i} \in \mathcal{P}^*$). In particular one needs the following lemma [1; 3.1].

∂ -Lemma. *Suppose $A^* \hookrightarrow B^*$ is an inclusion of graded algebras over \mathbb{F}_p and $\partial_1, \dots, \partial_n: A^* \rightarrow B^*$ are derivations. If $a_1, \dots, a_n \in A^*$ satisfy*

$$\text{Det}(\partial_i a_j) \neq 0,$$

then a_1, \dots, a_n are algebraically independent over \mathbb{F}_p .

The lemmas 5.3–5.5 of [1] can be summarized in the following

Δ -Theorem (Adams, Wilkerson). *Suppose $H^* \in \text{Un Id}/\mathcal{P}^*$ has at most a finite number of algebraically independent elements. Then there exists an integer $n \geq 0$ with the following property: any n distinct derivations $P^{\Delta_{i_1}}, \dots, P^{\Delta_{i_n}}$ are linearly independent on H^* but any $n + 1$ derivations $P^{\Delta_{i_0}}, \dots, P^{\Delta_{i_n}}$ are linearly dependent. Thus there are elements $h_0, \dots, h_n \in H^*$ all non-zero such that*

$$h_0 P^{\Delta_0} + \dots + h_n P^{\Delta_n} \equiv 0$$

vanishes identically on H^* .

Here P^{Δ_0} is the formally defined derivation with $P^{\Delta_0} x = dx$ if $x \in H^{2d}$.

2. Proof of the Main Theorem

Let n be the integer of the Δ -theorem and $h_0, \dots, h_n \in H^*$ coefficients such that the derivation $\partial = h_0 P^{\Delta_0} + \dots + h_n P^{\Delta_n}$ vanishes identically on H^* . We consider the polynomial

$$\Delta(X) = h_0 X + h_1 X^p + \dots + h_n X^{p^n} \in H^*[X]$$

(X an indeterminate of degree 2). We can also regard $\Delta(X)$ as a polynomial over the field of fractions $F(H^*)$ of H^* and take its splitting field $E^* > F(H^*)$. Since the formal derivative $\Delta'(X) = h_0 \neq 0$ does not vanish, $\Delta(X)$ is separable and $E^* > F(H^*)$ a separable extension. By the separable extension lemma there is a unique \mathcal{P}^* -algebra structure on E^* extending that on H^* .

We let $V = \{v \in E^2 \mid \Delta(v) = 0\}$. Because $\Delta(X)$ is additive, V is a vector space. In fact V is n -dimensional and consists of precisely the p^n distinct roots of $\Delta(X)$. Thus

$$\Delta(X) = h_n \prod_{v \in V} (X - v).$$

We collect some facts about V .

Proposition.

- (a) If $\{t_1, \dots, t_n\}$ is a basis for V , then t_1, \dots, t_n are algebraically independent.
- (b) The elements of V are all unstable, so

$$P^* = \mathbb{F}_p[t_1, \dots, t_n] \in \text{Un Id}/\mathcal{P}^*.$$

- (c) The action of \mathcal{P}^* on P^* commutes with the action of $GL(n, \mathbb{F}_p)$, so the Dickson algebra

$$D^*(n) = \mathbb{F}_p[t_1, \dots, t_n]^{GL(n, \mathbb{F}_p)}$$

of invariant polynomials is a \mathcal{P}^* -subalgebra.

- (d) Every $x \in P^*$ is integral over H^* .

Proof.

- (a) We can apply the ∂ -lemma. Suppose we had

$$\text{Det}(P^{\Delta_i} t_j)_{1 \leq i, j \leq n} = 0.$$

Then there would be coefficients $a_1, \dots, a_n \in E^*$ not all zero with

$$\partial' = a_1 P^{\Delta_1} + \dots + a_n P^{\Delta_n} = 0$$

on each t_i and hence on V . Hence all $v \in V$ are roots of the polynomial

$$f(X) = a_1 X^p + \dots + a_n X^{p^n}$$

and therefore

$$f(X) = a_n \prod_{v \in V} (X - v) = \frac{a_n}{h_n} \Delta(X).$$

Comparing coefficients of X gives $0 = (a_n/h_n) \cdot h_0$, so $a_n = 0$ and hence $f(X) \equiv 0$. But then $a_0 = \dots = a_n = 0$.

- (b) follows from the Lemmas 5.6–5.8 in [1].
- (c) is obvious.
- (d) The integrality of $x \in P^*$ is proved by another argument from [1]: one considers the H^* -module Q^* of all derivations $\partial: H^* \rightarrow H^*$ of the form

$$\sum_{k=0}^s a_k P^{\Delta_k}, \quad a_0, \dots, a_s \in H^*.$$

Let y_1, \dots, y_q be a finite set of generators of H^* as algebra and define

$$\phi: Q^* \rightarrow \bigoplus_{i=1}^s H^*$$

by $\phi(\partial) = \{\partial y_1, \dots, \partial y_s\}$. Then ϕ is injective, and since H^* is noetherian, Q^* must be a finitely generated H^* -module. Thus there is an m such that P^{Δ_m} is an H^* -linear combination of $P^{\Delta_0}, \dots, P^{\Delta_{m-1}}$ —say

$$d_0 P^{\Delta_0} + \dots + d_{m-1} P^{\Delta_{m-1}} + P^{\Delta_m} \equiv 0 \tag{2}$$

on H^* for suitable $d_0, \dots, d_{m-1} \in H^*$. By the uniqueness of extensions of derivations over separable extensions (2) must hold on E^* as well and thus on V . Hence each $v \in V$ satisfies

$$d_0 v + d_1 v^p + \dots + d_{m-1} v^{p^{m-1}} + v^{p^m} = 0.$$

It follows that any $x \in P^* = \mathbb{F}_p[t_1, \dots, t_n]$ is integral over H^* .

Now let A^* be the algebra obtained by adjoining t_1, \dots, t_n to H^* . Then $A^* \in \text{Un Id}/\mathcal{P}^*$ and we have inclusions

$$H^* < A^* > P^* > D^*(n).$$

Suppose we knew that $D^*(n) < A^*$ were an integral extension. Then $P^* < A^*$ would also be an integral extension in $\text{Un Id}/\mathcal{P}^*$, so by the algebraic closure theorem it follows that $A^* = P^*$ and hence $H^* < P^*$. Consider the Galois group

$$G = \mathcal{G}(E^*/F(H^*));$$

clearly $G < GL(n, \mathbb{F}_p)$, because the elements of G define linear transformations of V and an automorphism of E^* fixing $F(H^*)$ is uniquely determined by its effect on V .

We claim that

$$H^* = P^{*G} = \mathbb{F}_p[t_1, \dots, t_n]^G.$$

Evidently $H^* < P^{*G}$. On the other hand because $E^* > F(H^*)$ is a Galois extension, every $x \in P^{*G}$ lies in $F(H^*)$. Furthermore x is integral over H^* by (d) above. Now H^* is a polynomial algebra and hence integrally closed (see e.g. [4; p. 240]). Thus $x \in H^*$.

Hence our problem reduces to showing that $A^* > D^*(n)$ is an integral extension.

We recall (cf. [7]) that

$$\prod_{v \in V} (X - v)$$

is of the form $y_n X + y_{n-1} X^p + \dots + y_1 X^{p^{n-1}} + X^{p^n}$ for certain polynomials

$$y_1, \dots, y_n \in \mathbb{F}_p[t_1, \dots, t_n]$$

and in fact $D^*(n) = \mathbb{F}_p[y_1, \dots, y_n]$.

Lemma 1. *Let (y_1, \dots, y_n) denote the ideal of A^* generated by y_1, \dots, y_n and suppose $A^*/(y_1, \dots, y_n)$ is finite dimensional as a vector space over \mathbb{F}_p . Then $A^* \gg D^*(n)$ is an integral extension.*

Proof. Choose $a_1, \dots, a_m \in A^*$ such that the cosets $a_i + (y_1, \dots, y_n)$, $1 \leq i \leq m$, form a basis for $A^*/(y_1, \dots, y_n)$ over \mathbb{F}_p . Let $a \in A^*$ be arbitrary; then a can be written in the form

$$a = \sum_{i=1}^m \lambda_i a_i + \sum_{j=1}^n \gamma_j y_j \tag{3}$$

for suitable $\lambda_1, \dots, \lambda_m \in \mathbb{F}_p, \gamma_1, \dots, \gamma_n \in A^*$.

Inductive hypothesis: suppose that every $a \in A^*$ can be written in the form

$$a = \sum_{i=1}^m \sigma_i a_i + \sum_{|I|=N} \tau^I y^I \tag{B_N}$$

where $\sigma_i = \sigma_i(y_1, \dots, y_n) \in D^*(n)$ is a polynomial of degree less than N in y_1, \dots, y_n , $y^I = y_1^{i_1} \dots y_n^{i_n}$ for $I = (i_1, \dots, i_n)$, $|I| = i_1 + \dots + i_n$ and $\tau^I \in A^*$ for all I .

Then by (3) each τ^I can be written in the form

$$\tau^I = \sum_{j=1}^m \lambda_j^I a_j + \sum_{k=1}^n \mu_k^I y_k,$$

$\lambda_1^I, \dots, \lambda_m^I \in \mathbb{F}_p, \mu_k^I \in A^*, 1 \leq k \leq n$, and hence

$$\begin{aligned} a &= \sum_{j=1}^m \left(\sigma_j + \sum_I \lambda_j^I y^I \right) a_j + \sum_{I,k} \mu_k^I y^I y_k \\ &= \sum_{j=1}^m \tilde{\sigma}_j a_j + \sum_{|I|=N+1} \tilde{\mu}^I y^I, \end{aligned}$$

where

$$\tilde{\sigma}_j = \sigma_j + \sum_{|I|=N} \lambda_j^I y^I$$

is of degree less than $N + 1$ in y_1, \dots, y_n and $\tilde{\mu}^I \in A^*$.

Thus every $a \in A^*$ has a representation in the form (B_N) for N arbitrarily large. However the grading of y^I is at least $2Np^{n-1}(p-1)$ and hence τ^I has negative grading for N sufficiently large. But an unstable \mathcal{P}^* -algebra vanishes in negative gradings.

We have thus shown that a_1, \dots, a_m generate A^* as $D^*(n)$ -module. But $D^*(n)$ is noetherian, so if $a \in A^*$ and $M_k^* < A^*$ denotes the $D^*(n)$ -submodule generated by $1, a, \dots, a^k$, then for some s we must have

$$\bigcup_{i \geq 0} M_i^* = M_s^*$$

and hence $a^{s+1} \in M_s^*$ —i.e. a is integral over $D^*(n)$.

Lemma 2. $A^*/(y_1, \dots, y_n)$ is finite dimensional over \mathbb{F}_p .

Proof. If $z \in A^{2d}$ with $d \not\equiv 0 \pmod p$, then by [1; 2.3] there is an $a \in \mathcal{P}^*$ with

$$P^{\Delta n}(az) = (P^{\Delta_0 z})^{p^n} = d^{p^n} z^{p^n} = dz^{p^n}.$$

Let $b = d^{-1}a \in \mathcal{P}^*$; then $z^{p^n} = P^{\Delta n}(bz)$.

Now the derivation $y_n P^{\Delta_0} + \dots + y_1 P^{\Delta_{n-1}} + P^{\Delta_n}$ is $1/h_n(h_0 P^{\Delta_0} + \dots + h_n P^{\Delta_n}) = 1/h_n \cdot \partial$ and hence vanishes on E^* . Thus we have

$$z^{p^n} = P^{\Delta n}(bz) = -y_n P^{\Delta_0}(bz) - \dots - y_1 P^{\Delta_{n-1}}(bz) \in (y_1, \dots, y_n).$$

But A^* is generated as algebra by the algebra generators x_1, \dots, x_n of H^* and the t_1, \dots, t_n —all of which lie in gradings $\not\equiv 0 \pmod p$. If z_1, \dots, z_q denote these algebra generators for A^* , then we see that $A^*/(y_1, \dots, y_n)$ is spanned over \mathbb{F}_p by the monomials

$$z_1^{i_1} \dots z_q^{i_q}$$

with $i_k < p^n, 1 \leq k \leq q$.

This completes the proof of the main theorem.

Note. *A posteriori* one sees that the n of the Δ -theorem is the same as the number of polynomial generators of H^* .

3. Some consequences of the proof

From the proof given we can deduce the following criterion for an unstable integral domain A^* to be a ring of invariants.

Theorem. Let $A^* \in \text{UnId}/\mathcal{P}^*$ be integrally closed. The following conditions are necessary and sufficient that

$$A^* \simeq \mathbb{F}_p[t_1, \dots, t_n]^G, \text{ deg } t_i = 2, \quad i = 1, \dots, n,$$

for some group $G < GL(n, \mathbb{F}_p)$.

1. There is an element $y_1 \in A^{2(p^n - p^{n-1})}$ such that

$$P^1 P^p \dots P^{p^{n-2}} y_1 \neq 0.$$

2. If $y_i = P^{p^{n-1}} \dots P^{p^{n-2}} y_1$ for $i = 2, \dots, n$, then

$$P^{\Delta_j} y_i = \begin{cases} -y_1 y_n & j = n \\ y_n & i + j = n \\ 0 & \text{otherwise} \end{cases} \quad 1 \leq i, j \leq n.$$

3. $A^*/(y_1, \dots, y_n)$ is finite dimensional over \mathbb{F}_p .

Proof. If $A^* \simeq \mathbb{F}_p[t_1, \dots, t_n]^G$ for some $G < GL(n, \mathbb{F}_p)$, then clearly

$$A^* > \mathbb{F}_p[t_1, \dots, t_n]^{GL(n, \mathbb{F}_p)} = D^*(n) \simeq \mathbb{F}_p[y_1, \dots, y_n]$$

and this $y_1 \in D^*(n) < A^*$ satisfies 1–3 (cf. [7]).

Conversely if 1–3 hold, then the map

$$\varphi: D^*(n) \rightarrow A^*$$

given by sending the Dickson algebra generators onto the elements y_1, \dots, y_n of A^* is a morphism in $\text{Un Id}/\mathcal{P}^*$. By 2.

$$\text{Det}(P^{\Delta_i} y_j) = \begin{vmatrix} 0 & \dots & -y_n & 0 \\ \vdots & \ddots & \vdots & \vdots \\ -y_n & \dots & 0 & 0 \\ y_1 y_n & \dots & \dots & y_n y_n \end{vmatrix} = (-1)^{n+1} y_n^{n+1} \neq 0$$

and hence y_1, \dots, y_n an algebraically independent. Thus φ is injective.

If we now assume the existence of algebraic closures in $\text{Un Id}/\mathcal{P}^*$ ([1]), then the algebraic closure theorem says $D^*(n) < P^*$ is the algebraic closure of $D^*(n)$ in $\text{Un Id}/\mathcal{P}^*$, so we have

$$D^*(n) < A^* < P^*$$

since by Lemma 1 the extension

$$D^*(n) < A^*$$

is integral. Passing to the fields of fractions we have

$$F(D^*(n)) < F(A^*) < F(P^*)$$

and by [7] $F(D^*(n)) < F(P^*)$ is a Galois extension with Galois group $GL(n, \mathbb{F}_p)$. If we let $G = \mathcal{G}(F(P^*)/F(A^*)) < GL(n, \mathbb{F}_p)$, then we have

$$A^* = P^{*G}$$

as before. (Note: P^* is integral over $D^*(n)$ and hence over A^* ; and A^* is integrally closed by assumption.)

Proposition. Suppose that $H^* \in \text{Un Id}/\mathcal{P}^*$ is of the form $H^* \simeq \mathbb{F}_p[x_1, \dots, x_n]$ with $\deg x_i \not\equiv 0 \pmod p$ for $1 \leq i \leq n$. Then

$$2p^{n-1}(p-1) < \deg x_i < 2(p^n - 1), 1 \leq i \leq n.$$

Proof. We have just seen that such an H^* must contain $D^*(n)$ as subalgebra. An inclusion of the form

$$D^*(n) < \mathbb{F}_p[x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n]$$

is of course impossible, so

$$2p^{n-1}(p-1) = \deg y_1 \leq \deg x_i \leq \deg y_n = 2(p^n - 1)$$

for $1 \leq i \leq n$. Since none of the generators is in a grading congruent to zero mod p , the lower inequality must be strict. To see that the upper inequality is strict we suppose $\deg x_i = 2(p^n - 2)$ and apply the theorem of Clark [2; Thm. 2] to conclude there is a j such that with

$$\deg x_j = 2d_j$$

we have $d_j \equiv 1 - p \pmod{p^n - 1}$ and hence $p^n - 1 \mid d_j + p - 1$. Since also $d_j \leq p^n - 1$ we have $d_j + p - 1 = p^n - 1$, i.e.

$$d_j = p^n - p = p(p^{n-1} - 1)$$

contradicting the assumption $d_j \not\equiv 0 \pmod{p}$.

Of course, this result could have been obtained by appealing to the classification of finite complex hyperplane groups [6] and [3; p. 428]. From our viewpoint the result is a natural consequence of the general theory.

REFERENCES

1. J. F. ADAMS and C. W. WILKERSON, Finite H -spaces and algebras over the Steenrod algebra, *Ann. of Math.* **111** (1980), 95–143.
2. A. CLARK, On π_3 of finite dimensional H -spaces, *Ann. of Math.* **78** (1963), 193–195.
3. A. CLARK and J. EWING, The realization of polynomial algebras as cohomology rings, *Pacific J. Math.* **50** (1974), 425–434.
4. S. LANG, *Algebra* (Addison-Wesley, 1965).
5. J.-P. SERRE, Sur la dimension cohomologique des groupes profini, *Topology* **3** (1965), 413–420.
6. G. C. SHEPARD and J. A. TODD, Finite unitary reflection groups, *Canadian J. Math.* **6** (1954), 274–304.
7. L. SMITH and R. M. SWITZER, Realizability and nonrealizability of Dickson algebras as cohomology rings, *preprint*.
8. C. W. WILKERSON, Classifying spaces, Steenrod operations and algebraic closure, *Topology* **16** (1977), 227–237.
9. C. W. WILKERSON, Integral closure of unstable Steenrod algebra actions, *J. Pure and Appl. Alg.* **13** (1978), 49–55.

MATHEMATISCHES INSTITUT
 BUNSENSTRASSE 3/5
 D3400 GÖTTINGEN
 FED. REP. OF GERMANY