PACIFIC JOURNAL OF MATHEMATICS
Vol. 50, No. 2, 1974

THE REALIZATION OF POLYNOMIAL ALGEBRAS AS COHOMOLOGY RINGS

ALLAN CLARK AND JOHN EWING

To the memory of Norman Steenrod

We construct, for certain choices of a group G, a prime p, and a positive integer n, a space $X(G, p, n)$ whose cohomology ring mod p is a polynomial algebra, and we classify the polynomial algebras which can be realized as cohomology rings by this construction.

Let $\boldsymbol{Z}_p$ denote the ring of p-adic integers. From Sullivan's work on completions [15] it follows that the Eilenberg-MacLane space $K(\boldsymbol{Z}_p^n, 2)$ is the p-profinite completion of $K(\boldsymbol{Z}^n, 2)$, and that as a consequence of the p-analogue of [15, 3.9] we have

$$H^*(K(\boldsymbol{Z}_p^n, 2); Z_p) = \boldsymbol{Z}_p[x_1, x_2, \cdots, x_n]$$

where $\deg x_i = 2$. Now if G is a subgroup of $\mathrm{GL}(n, \boldsymbol{Z}_p)$ and finite, we have an action of G on the space $K(\boldsymbol{Z}_p^n, 2)$ which passes to its cohomology ring, and we define

$$X(G, p, n) = K(\boldsymbol{Z}_p^n, 2) \times_G EG$$

where EG is the total space of a universal bundle for G.

PROPOSITION. *If p does not divide the order of G, then $H^*(X(G, p, n); \boldsymbol{Z}_p)$ is the subalgebra of invariants of $H^*(K)(\boldsymbol{Z}_p^n, 2); \boldsymbol{Z}_p)$ under the action of G.*

Obviously the conclusions of this proposition apply as well with coefficients in the prime field $\boldsymbol{F}_p$ or in the field $\boldsymbol{Q}_p$ of p-adic numbers. For the sake of completeness we sketch a proof.

Proof. From [5, Th. 3.1] and [8] it follows that the cohomology of $X(G, p, n)$ is given by $\mathrm{Ext}_{Z_p(G)}(C_*(EG)), C^*(K(\boldsymbol{Z}_p^n, 2))$, where we let $\boldsymbol{Z}_p(G)$ denote the group ring over $\boldsymbol{Z}_p$ and C_* and C^* denote singular chains with coefficients in $\boldsymbol{Z}_p$. The Eilenberg-Moore spectral sequence associated with this Ext has E_2 term determined by

$$E_2^{r,s} = \mathrm{Ext}^r_{Z_p(G)}(\boldsymbol{Z}_p, H^s(K(\boldsymbol{Z}_p^n, 2); \boldsymbol{Z}_p))$$

and it follows that for $r > 0$, $|G| E_2^{r,s} = 0$ by the results of [3, Ch. XII, 2.5]. However, $E_2^{r,s}$ is a $\boldsymbol{Z}_p$-module and therefore can have only p-torsion. The fact that p does not divide $|G|$ implies that $E_2^{r,s} = 0$

except for $r = 0$ and the spectral sequence collapses, giving

$$E_2 = E_\infty = \mathrm{Hom}_{Z_p(G)}(\boldsymbol{Z}_p, H^*(K(\boldsymbol{Z}_p^n, 2); \boldsymbol{Z}_p))$$

which is clearly the invariant subalgebra under the action of G. Furthermore, E_∞ is a free $\boldsymbol{Z}_p$-module and as a result $H^*(X(G, p, n); \boldsymbol{Z}_p)$ is isomorphic to the invariant subalgebra as a $\boldsymbol{Z}_p$-module. This shows that the bundle projection

$$K(\boldsymbol{Z}_p^n, 2) \times EG \longrightarrow X(G, p, n)$$

induces an isomorphism from the cohomology of $X(G, p, n)$ onto the subalgebra of invariants under the action of G, and the proof is complete.

These remarks reduce the problem to the purely algebraic question of when the subalgebra of invariants of a finite group acting homogeneously on a polynomial algebra is again a polynomial algebra. This question is answered completely by the following result abstracted from Theorem 4 of [2, Ch. 2, §5].

THEOREM. *Let G be a subgroup of* $\mathrm{GL}(V)$ *where V is a vector space of dimension n over a field k with characteristic prime to the order of G or with* $\mathrm{char}\, k = 0$. *Let R denote the invariants of the action of G on $S(V)$, the symmetric algebra of V. Then R is a polynomial algebra if and only if G is a finite group generated by pseudo-reflections.*

A pseudo-reflection of V is an endomorphism s such that $1 - s$ has rank 1. $\mathrm{Ker}\,(1 - s)$ is called the hyperplane of s. We shall call a finite group generated by pseudo-reflections a *hyperplane group* of V. Of course when k is a subfield of the real numbers, pseudo-reflections are just reflections. We also observe that if we are given a basis $x_1, x_2, \cdots, x_n$ of V, that $S(V) = k[x_1, x_2, \cdots, x_n]$ and that if $R = k[u_1, u_2, \cdots, u_n]$, then the order of G is the product of the degrees of the u_i's. This is also proved in [2]. Of course we shall prefer to use topological degrees in these graded algebras rather than homogeneous degrees. As a result we obtain the following theorem about the cohomology ring of the space $X(G, p, n)$ by first applying the theorem above to the case $k = \boldsymbol{Q}_p$ and $k = \boldsymbol{F}_p$, and then lifting the result to $\boldsymbol{Z}_p$.

COROLLARY. *Let G be a finite subgroup of* $\mathrm{GL}(n, \boldsymbol{Z}_p)$ *with order prime to p which is a hyperplane group in* $\mathrm{GL}(n, \boldsymbol{Q}_p)$. *Then the cohomology ring of the space $X(G, p, n)$ with coefficients in $\boldsymbol{Z}_p$, $\boldsymbol{Q}_p$, or $\boldsymbol{F}_p$ is a polynomial algebra.*

Proof. We set $V = H^2(K(\boldsymbol{Z}_p^n, 2); \boldsymbol{Z}_p) \cong \boldsymbol{Z}_p^n$, and $V' = V \otimes \boldsymbol{Q}_p$, and $\bar{V} = V \otimes \boldsymbol{F}_p$. Then we have $S(V)$ isomorphic to the cohomology ring $H^*(K(\boldsymbol{Z}_p^n, 2); \boldsymbol{Z}_p) = \boldsymbol{Z}_p[x_1, x_2, \cdots, x_n]$ where $\deg x_i = 2$. We let R denote the invariants of $S(V)$ under the action of G, R' the invariants of $S(V') \cong S(V) \otimes \boldsymbol{Q}_p$, and $\bar{R}$ the invariants of $S(\bar{V}) \cong S(V) \otimes \boldsymbol{F}_p$ under the action of the group $\bar{G}$ obtained from G by reduction mod p. $\bar{G}$ is a hyperplane group in $\mathrm{GL}(n, \boldsymbol{F}_p)$ and is, in fact, isomorphic to G, as we shall see.

The theorem above applies directly to R' and $\bar{R}$. Clearly we have $R' = R \otimes \boldsymbol{Q}_p$. We also have $\bar{R} = R \otimes \boldsymbol{F}_p$ by the following argument. For $v \in S(V)$ and $a \in \boldsymbol{Z}_p$, $av \in R$ implies that $g(av) - av = a(gv - v) = 0$ for every $g \in G$. Since $S(V)$ is a free $\boldsymbol{Z}_p$-module, this implies that $v \in R$. Therefore, R is a direct summand of $S(V)$ and consequently we have $R \otimes \boldsymbol{F}_p$ contained in $\bar{R}$. On the other hand, given an element $\bar{u}$ of $\bar{R}$, we can always write it in the form $\bar{u} = \sum_i v_i \otimes a_i$ for some v_i's in $S(V)$ and some a_i's in $\boldsymbol{F}_p$, and furthermore, since $\bar{u}$ is an invariant we have

$$\bar{u} = \frac{1}{|\bar{G}|} \sum_{\bar{G}} \bar{g} \cdot \bar{u} = \frac{1}{|G|} \sum_i \left(\sum_G g v_i \right) \otimes a_i$$

in which the last expression obviously belongs to $R \otimes \boldsymbol{F}_p$.

Now R is a free $\boldsymbol{Z}_p$-module and consequently R' and $\bar{R}$ have the same Poincaré polynomials. Since R' and $\bar{R}$ are polynomial algebras, it follows that they have generators of the same degree. Since the product of the homogeneous degrees of these generators give the orders of the groups G and $\bar{G}$, it follows that G and $\bar{G}$ must have the same orders and are isomorphic.

It remains to show that R is a polynomial algebra. Since R' is a polynomial algebra we have $R' = S(U')$ for some graded vector subspace of $S(V')$. We let $U = U' R$. Then if $u \in R$ and $au \in U$ for some $a \in \boldsymbol{Z}_p$, we have $au \in U'$ and it follows that $u \in U'$ and hence $u \in U$. Thus R/U is torsion free and U is a direct summand of R. The inclusion of algebras $S(U) \to R$ is a monomorphism since $S(U)$ and R are free over $\boldsymbol{Z}_p$ and tensoring with $\boldsymbol{Q}_p$ yields the isomorphism $S(U') \cong R'$. Comparison of Poincaré polynomials shows that $S(U) = R$, which completes the proof.

Representations of hyperplane groups. To determine which polynomial algebras are representable as the cohomology rings of spaces $X(G, p, n)$ we need a classification of the finite subgroups of $\mathrm{GL}(n, \boldsymbol{Z}_p)$ which are generated by pseudo-reflections, and which have order prime to p. While no such classification seems to be available, a complete classification of hyperplane groups over the complex field $\boldsymbol{C}$ has been given by Shepard and Todd [12], and by using some ele-

mentary theory of group representation to shift back and forth between C-representations and Z_p-representations, we can derive the results we need. Feit's book [6] is a general reference. By the *type* of a polynomial algebra we mean the list of the degrees of the generators.

THEOREM. *Let G be a finite group with order prime to p. If G has a faithful representation ρ as a hyperplane group over $\boldsymbol{Z}_p$, then G has a faithful unitary representation σ as a hyperplane group over $\boldsymbol{C}$, such that σ affords the same character as ρ. Furthermore, the invariant algebras obtained from G acting on $S(\boldsymbol{Z}_p^n)$ and $S(\boldsymbol{C}^n)$ have the same type.*

Proof. Let χ denote the character of ρ, viewed as a $\boldsymbol{Q}_p$-representation for G. Since char $\boldsymbol{Q}_p = 0$, there is a finite extension E of the rational field Q and an E-representation σ of G which affords the same character as ρ. Since ρ and σ may be construed as K-representations for some common extension K of E and $\boldsymbol{Q}_p$, and since they afford the same character, it follows that as K-representations ρ and σ are similar by [6, I, 2.6]. Thus σ still represents G as a hyperplane group and is a unitary representation of G if we consider E a subfield of $\boldsymbol{C}$.

Let R denote the invariant subalgebra produced by the action of G on $S(\boldsymbol{Z}_p^n)$ via ρ. The argument of the preceding corollary may be repeated to show that R is a polynomial algebra. Let $\hat{R}$ denote the invariant subalgebra produced by the action of G on $S(E^n)$ via σ. The actions of G on $S(K^n)$ via ρ and σ have invariant subalgebras $R \otimes K$ and $\hat{R} \otimes K$ and these K-algebras are isomorphic since the representations are similar. The invariant subalgebra obtained from the action of G on $S(\boldsymbol{C}^n)$ via σ is clearly $\hat{R} \otimes \boldsymbol{C}$. It is obvious that all these invariant subalgebras must have the same types and the proof is finished.

This theorem shows that we can pass from hyperplane groups over $\boldsymbol{Z}_p$ to hyperplane groups over $\boldsymbol{C}$. We cannot always go in the opposite direction, but the following proposition tells us when we can.

We recall that the Schur index of a character χ is the minimum of the degrees $[F: Q(\chi)]$ taken over all the fields F for which there is an F-representation affording χ.

PROPOSITION. *If σ is an irreducible unitary representation of G with character χ whose Schur index $m_Q(\chi)$ is 1, then there is a $\boldsymbol{Z}_p$-representation of G which affords the same character χ if and only if $\boldsymbol{Q}_p$ contains a subfield isomorphic to the character field $\boldsymbol{Q}(\chi)$.*

This is obvious. We now show that for hyperplane representations

over C the Schur index is always 1. In fact we can extract most of the following theorem from the section on the Schur index in Huppert's book [7, V, §14].

THEOREM. *Let σ be an irreducible C-representation of degree n of a finite group G and let χ denote the character of σ. For $g \in G$ let $F_{\sigma(g)}$ denote the subspace of C^n left pointwise fixed by $\sigma(g)$ and let*

$$k = \max \{\dim_C F_{\sigma(g)} \mid g \in G, \sigma(g) \neq 1\} .$$

Then the Schur index $m_Q(\chi)$ is at most $n - k$.

Proof. The group algebra $Q(\chi)(G)$ is semisimple and χ is nonzero on precisely one of its constituents, call it A. A is simple and is a complete matrix algebra, by the Wedderburn theorem, of $m \times m$ matrices over D, a division ring over $Q(\chi)$. Furthermore, A is central simple over $Q(\chi)$ and we have

$$\dim_D A = m^2 \qquad \dim_{Q(\chi)} D = (m_Q(\chi))^2$$

hence

$$\dim_{Q(\chi)} A = n^2 = m^2(m_Q(\chi))^2 .$$

Let π denote the projection of the group algebra $Q(\chi)(G)$ onto A and let I denote a minimal nontrivial left ideal of A. G acts on I via the projection and, furthermore, I consists of $m \times m$ matrices over D which vanish outside one column. Therefore,

$$\dim_{Q(\chi)} I = m \cdot \dim_{Q(\chi)} D = n \cdot m_Q(\chi) .$$

In fact the action of G on I is equivalent to the representation $m_Q(\chi) \cdot \sigma$. For $g \in G$, $\pi(g)$ acts on I by left multiplication and the space $F_{\pi(g)}$ left pointwise fixed under this action is a right vector space over D. Thus when $\pi(g) \neq 1$, we have $\dim_D F_{\pi(g)} \leqq m - 1$. It follows that

$$\dim_{Q(\chi)} F_{\pi(g)} \leqq (m - 1)(m_Q(\chi))^2 = m_Q(\chi) \cdot (n - m_Q(\chi)) .$$

On the other hand,

$$\dim_{Q(\chi)} F_{\pi(g)} = \dim_{Q(\chi)} F_{m_Q(\chi)\cdot\sigma(g)} = m_Q(\chi) \dim_{Q(\chi)} F_{\sigma(g)} .$$

Consequently when $\sigma(g) \neq 1$, we also have $\pi(g) \neq 1$, and thus

$$\dim_{Q(\chi)} F_{\sigma(g)} \leqq n - m_Q(\chi) .$$

Maximizing over the g's for which $\sigma(g) \neq 1$ yields $k \leqq n - m_Q(\chi)$.

COROLLARY. *For hyperplane representations the Schur index is always* 1.

Classification of the types. To summarize the situation to this point, we know that if p does not divide the order of G, then the space $X(G, p, n)$ has polynomial cohomology mod p precisely when G is a hyperplane group over $\boldsymbol{Z}_p$. A hyperplane group over $\boldsymbol{Z}_p$ always has a representation as a unitary hyperplane group, while a given unitary hyperplane group has a $\boldsymbol{Z}_p$-representation as a hyperplane group only for some primes.

Further, we observe that while the space $X(G, p, n)$ depends on the class of the $\boldsymbol{Z}_p$-representation of G, its cohomology algebra depends only on the class of the $\boldsymbol{Q}_p$-representation, which is to say, upon the character. For this reason it turns out that the types of polynomial algebras realizable in this way are products of irreducible types, although we cannot say the same thing for the spaces involved. It may be that such a statement is true after completion.

In the table below the types are given with topological degrees and the last column gives conditions on the primes. We give the order of G as well as the rank of the algebra it determines.

THEOREM. *The types of polynomial algebras* mod p *which can be realized as the cohomology ring* $H^*(X(G, p, n); \boldsymbol{F}_p)$ *where* G *is a hyperplane group over* $\boldsymbol{Z}_p$ *with order prime to* p *are products of the irreducible types given by the following table:*

Number	Rank	Order	Type	Primes
1	n	$(n+1)!$	$[4,6,\cdots,2(n+1)]$	$p \nmid (n+1)!$
2a*	n	$qm^{n-1}n!$	$[2m,4m,\cdots,2(n-1)m,2qn]$	$p \nmid n!, p \equiv 1 \bmod m$
2b	2	$2m$	$[4,2m]$	$m > 2, p \equiv \pm 1 \bmod m$
3	1	m	$[2m]$	$p \equiv 1 \bmod m$
4	2	24	[8,12]	$p \equiv 1 \bmod 3$
5	2	72	[12,24]	$p \equiv 1 \bmod 3$
6	2	48	[8,24]	$p \equiv 1 \bmod 12$
7	2	144	[24,24]	$p \equiv 1 \bmod 12$
8	2	96	[16,24]	$p \equiv 1 \bmod 4$
9	2	192	[16,48]	$p \equiv 1 \bmod 8$
10	2	288	[24,48]	$p \equiv 1 \bmod 12$
11	2	576	[48,48]	$p \equiv 1 \bmod 24$
12	2	48	[12,16]	$p \equiv 1,3 \bmod 8,\ p \neq 3$
13	2	96	[16,24]	$p \equiv 1 \bmod 8$
14	2	144	[12,48]	$p \equiv 1,19 \bmod 24$
15	2	288	[24,48]	$p \equiv 1 \bmod 24$
16	2	600	[40,60]	$p \equiv 1 \bmod 5$
17	2	1200	[40,120]	$p \equiv 1 \bmod 20$
18	2	1800	[60,120]	$p \equiv 1 \bmod 15$

(table to be continued)

(table to be continued)

Number	Rank	Order	Type	Primes
19	2	3600	[120,120]	$p \equiv 1 \bmod 60$
20	2	360	[24,60]	$p \equiv 1,4 \bmod 15$
21	2	720	[24,120]	$p \equiv 1,49 \bmod 60$
22	2	240	[24,40]	$p \equiv 1,9 \bmod 20$
23	3	120	[4,12,20]	$p \equiv 1,4 \bmod 5$
24	3	336	[8,12,28]	$p \equiv 1,2,4 \bmod 7$
25	3	648	[12,18,24]	$p \equiv 1 \bmod 3$
26	3	1296	[12,24,36]	$p \equiv 1 \bmod 3$
27	3	2160	[12,24,60]	$p \equiv 1,4 \bmod 15$
28	4	1152	[4,12,16,24]	$p \neq 2$ or 3
29	4	7680	[8,16,24,40]	$p \equiv 1 \bmod 4,\ p \neq 5$
30	4	14,400	[4,24,40,60]	$p \equiv 1,4 \bmod 5$
31	4	64·6!	[16,24,40,48]	$p \equiv 1 \bmod 4,\ p \neq 5$
32	4	216·6!	[24,36,48,60]	$p \equiv 1 \bmod 3$
33	5	72·6!	[8,12,20,24,36]	$p \equiv 1 \bmod 3$
34	6	108·9!	[12,24,36,48,60,84]	$p \equiv 1 \bmod 3,\ p \neq 7$
35	6	72·6!	[4,10,12,16,18,24]	$p \neq 2,3,$ or 5
36	7	8·9!	[4,12,16,20,24,28,36]	$p \neq 2,3,5,$ or 7
37	8	192·10!	[4,16,24,28,36,40,48,60]	$p \neq 2,3,5,$ or 7

* where $m > 1$ and $m = qr$.

Note: The product of the entries in the type is $2^{\text{rank}} \times |G|$.

Proof. The groups on this list come from the classification of irreducible unitary hyperplane groups given by Shepard and Todd [12, p. 301]. Given a faithful representation ρ of a group G as a hyperplane group over $\boldsymbol{Z}_p$, we know that the character field $\boldsymbol{Q}(\chi)$ is contained in $\boldsymbol{Q}_p$ and, furthermore, we know that there exists a faithful unitary representation σ of G which affords the same character χ. Now σ is equivalent to a sum $\sum_i \sigma_i$ of irreducible unitary representations σ_i with characters χ_i. Let $G_i = \sigma_i(G)$. It follows from the fact that G is generated by pseudo-reflections that each G_i is an irreducible unitary hyperplane group and that G is isomorphic to the direct product of the G_i. Of course each G_i must be among the groups listed by Shepard and Todd. What is more, since G is hyperplane and the Schur index $m_Q(\chi) = 1$, we may assume that σ is a $\boldsymbol{Q}(\chi)$-representation, and consequently that the same is true of each σ_i. As a result $\boldsymbol{Q}(\chi)$ must contain the character field $\boldsymbol{Q}(\chi_i)$ for each i. (The essential step in this argument is to see that each pseudo-reflection of G must belong to one of the groups G_i, that is, must leave fixed all but one of the invariant subspaces of $\boldsymbol{C}^n$ under the action of G.) Since $\boldsymbol{Q}(\chi_i)$ is contained in $\boldsymbol{Q}(\chi)$ and hence in $\boldsymbol{Q}_p$, it follows that each G_i has a representation over $\boldsymbol{Z}_p$, say ρ_i which affords the same character χ_i as

σ_i. Consequently we have that $\sum_i \rho_i$ is a representation of G as a hyperplane group over Z_p with character $\sum_i \chi_i = \chi$, as a result of which it must be equivalent to ρ, the representation with which we started. Thus the type of G is a product of the types of the G_i, that is, of types in the list of Shepard and Todd.

It remains only to compute the primes for which various types on the list can occur. To do this we must compute the character field for each of the groups from the information of Shepard and Todd [12]. In most cases this is not difficult at all and we omit the details, simply listing the results in the table below. However, we do give the details for the groups $2a$ and $2b$, which are more difficult.

Table of Character Fields

No.	$Q(\gamma)$	No.	$Q(\chi)$	No.	$Q(\chi)$
1	Q	13	$Q(i, \sqrt{2})$	26	$Q(\omega)$
$2a$	$Q(\theta)$	14	$Q(\omega, \sqrt{-2})$	27	$Q(\omega, \sqrt{5})$
$2b$	$Q(\theta+\theta^{-1})$	15	$Q(i, \omega, \sqrt{2})$	28	Q
3	$Q(\theta)$	16	$Q(\eta)$	29	$Q(i)$
4	$Q(\omega)$	17	$Q(i, \eta)$	30	$Q(\sqrt{5})$
5	$Q(\omega)$	18	$Q(\omega, \eta)$	31	$Q(i)$
6	$Q(i, \omega)$	19	$Q(\omega, i, \eta)$	32	$Q(\omega)$
7	$Q(i, \omega)$	20	$Q(\omega, \sqrt{5})$	33	$Q(\omega)$
8	$Q(i)$	21	$Q(i, \omega, \sqrt{5})$	34	$Q(\omega)$
9	$Q(i, \sqrt{2})$	22	$Q(i, \sqrt{5})$	35	Q
10	$Q(i, \omega)$	23	$Q(\sqrt{5}$	36	Q
11	$Q(\varepsilon, \omega)$	24	$Q(\sqrt{-7})$	37	Q
12	$Q(\sqrt{-2})$	25	$Q(\omega)$		

where $i = \sqrt{-1}$, $\omega = e^{2\pi i/3}$, $\eta = e^{2\pi i/5}$, $\varepsilon = e^{2\pi i/8}$, $\theta = e^{2\pi i/m}$.

Character fields of the groups $2a$ *and* $2b$. These are the group. $G(m, r, n)$ consisting of all the transformations $x_i \to \theta^{\nu_i} \cdot x_{\sigma(i)}$, where $x_1, x_2, \cdots, x_n$ is a basis for C^n, σ is a permutation of n letters, $\theta = e^{2\pi i/m}$, and the ν_i's are integers satisfying the congruence $\sum_i \nu_i \equiv 0 \bmod r$, and where $m > 1$ and $m = qr$. The order of $G(m, r, n)$ is $qm^{n-1} \cdot n!$ as computed in [12]. Clearly $Q(\chi)$ is contained in $Q(\theta)$ and when $n > 2$, $Q(\chi) = Q(\theta)$ because $G(m, r, n)$ contains transformations of the form $x_1 \to \theta x_1$, $x_2 \to \theta^{\alpha} x_3$, $x_3 \to \theta^{\beta} x_2$, and $x_i \to x_i$ for $i > 3$. On the other hand, for $n = 2$, $G(m, r, n)$ has the transformation $x_1 \to \theta x_1$, $x_2 \to \theta^{-1} x_2$, so that $Q(\theta + \theta^{-1})$ is contained in $Q(\chi)$. To decide whether $Q(\chi)$ is $Q(\theta)$ or $Q(\theta + \theta^{-1})$ we need to look closely. We observe that when $q > 2$, we have θ^r is in $Q(\chi)$ but not in $Q(\theta + \theta^{-1})$ and therefore $Q(\chi) = Q(\theta)$ for $q > 2$. This follows because $Q(\theta)$ is a degree 2 Galois extension of $Q(\theta + \theta^{-1})$ with nontrivial automorphism $\theta \to \theta^{-1}$, and $\theta^r \in Q(\theta + \theta^{-1})$ would imply $\theta^r = \theta^{-r}$ or $m \mid 2r$, contradicting $q > 2$.

When $q = 2$, we have $\theta^r = -1$, and $G(m, r, 2)$ contains the transformations $x_1 \to \theta x_1$, $x_2 \to \pm \theta^{-1} x_2$ so that $\theta \pm \theta^{-1}$ belongs to $Q(\chi)$ and $Q(\chi) = Q(\theta)$. Finally, for $q = 1$, $G(m, m, 2)$ is the dihedral group of order $2m$ generated by the transformations $x_1 \to \theta x_1$, $x_2 \to \theta^{-1} x_2$, and $x_1 \to x_2$, $x_2 \to x_1$, from which we compute directly that $Q(\chi) = Q(\theta + \theta^{-1})$.

Determination of the primes for which a given type occurs. This is a simple matter now that the character fields are given. In the cases 1, 28, 35, 36, 37, the character field is Q and the only restriction is that p does not divide the order of G. For many of the other cases the conditions are determined by the fact that Q_p contains only the $(p-1)$st roots of unity. In the cases where square roots occur, we use the theorem that Q_p contains $\sqrt{a}$ if and only if a is a quadratic residue mod p [1, Th. 1, p. 48]. The results are obtained by routine use of quadratic reciprocity.

This completes the proof of the classification theorem.

Remarks on the primes allowable for a type. All the presently known types of polynomial algebras which can occur as the mod p cohomology of a space are given as products of the types in the list above. However, it is clear that some types occur for primes other than those listed. It turns out, however, that we are missing at most primes which divide the order of the group. To verify this it is sufficient to apply the following result [4, Th. 2].

THEOREM. *If B is an algebra over the Steenrod algebra as well as a polynomial algebra over F_p on generators of even degree, one of which occurs in degree $2m$, then either $p \mid m$ or else B has a generator in some degree $2n$ where $n \equiv 1 - p \bmod m$.*

This theorem can also be used to eliminate some of the primes dividing the order of the group. Specifically we can eliminate $p = 3$ for the groups 6, 8, 9, 13, 16, 17, 22, 23, 24, 29, 30, 31, and we can eliminate $p = 5$ for the groups 20, 21, 30, 31, 32, 33, 34. There still remain a number of cases not constructed by our method for given primes dividing the order of the group.

Final remarks. One would like to have a complete answer to the question first raised by Steenrod in [13]: *Given a graded polynomial algebra $A = F_p[x_1, x_2, \cdots, x_n]$ of rank n over the prime field F_p with generators of even degree, under what conditions does there exist a space X whose cohomology algebra $H^*(X; F_p)$ is isomorphic to A?*

The requirement that A admit an action of the Steenrod algebra,

and higher order operations, severely limits the types of polynomial algebras which can be realized. In the rank one case $\boldsymbol{F}_p[x]$ admits Steenrod operations only when $\deg x = 2\lambda p^k$ where $\lambda | (p-1)$, and secondary operations eliminate all the cases where $k \neq 0$, except the type [4] for $p = 2$ (realized by infinite quaternionic projective space). All the types $[2\lambda]$ where $\lambda | (p-1)$ are realized as shown by Sullivan [15, 4.30] and by group 3 above. In rank 2 some restrictions have been obtained by Nakagawa and Ochiai [9], but their results can be improved even by further use of primary operations. In ranks above 2 nothing whatever has been accomplished and in general it seems that we are very far from an answer.

We see no reason not to conjecture that the list of types constructed above, and their products, with the exceptional primes determined, is the complete list of polynomial algebras realizable as cohomology rings, but the evidence for this is very slender.

REFERENCES

1. Z. I. Borevich and I. R. Shafarevich, *Number Theory*, New York, Academic Press, 1966.
2. N. Bourbaki, *Groupes et Algèbres de Lie*, Paris, Hermann, 1968.
3. H. Cartan and S. Eilenberg, *Homological Algebra*, Princeton University Press, 1956.
4. A. Clark, *On π_3 of finite dimensional H-spaces*, Ann. of Math., **78** (1963), 193–196.
5. S. Eilenberg and J. C. Moore, *Homological algebra and fibrations*, Colloque de Topologie, Bruxelles, (1964), 81–90.
6. W. Feit, *Characters of Finite Groups*, New York, Benjamin and Co., 1967.
7. B. Huppert, *Endliche Gruppen I*, Berlin, Springer-Verlag, 1967.
8. J. C. Moore, *Algebre homologique et homologie des espaces classifiants*, Seminaire H. Cartan—J. C. Moore, **12** (1959/60) exposé 7.
9. R. Nakagawa and S. Ochial, *On the dimension of generators of a polynomial algebra over the* mod p *Steenrod algebra*, Proc. Japan Acad., **43** (1967), 932–936.
10. G. C. Shepard, *Unitary groups generated by reflections*, Canad. J. Math., **5** (1953), 364–383.
11. ———, *Some problems on finite reflection groups*, L'Enseignement Mathématique, II^e Série, t. **2** (1956), 42–48.
12. G. C. Shepard and J. A. Todd, *Finite unitary reflection groups*, Canad. J. Math., **6** (1954), 274–304.
13. N. E. Steenrod, *The cohomology algebra of a space*, L'Enseignement Mathématique, II^e Série, t. **7** (1961), 153–178.
14. ———, *Polynomial algebras over the algebra of cohomology operations, H-spaces*, Neuchâtel (Suisse) Août, 1970. Lecture Notes in Mathematics 196, Springer-Verlag.
15. D. Sullivan, *Geometric Topology Part I*, M. I. T., April, 1971.

Received November 11, 1972. Partially supported by the National Science Foundation.

BROWN UNIVERSITY,
DARTMOUTH COLLEGE,
AND
UNIVERSITY OF AARHUS, DENMARK