Canad. Math. Bull.Vol. 34 (1), 1991 pp. 42–47

RINGS OF INVARIANTS AND p-SYLOW SUBGROUPS

H. E. A. CAMPBELL, I. HUGHES, AND R. D. POLLACK

ABSTRACT. Let V be a vector space of dimension n over a field k of characteristic p. Let $G \subseteq Gl(V)$ be a finite group with p-Sylow subgroup P. G and P act on the symmetric algebra R of V. Denote the respective rings of invariants by R^G and R^P. We show that if R^P is Cohen-Macaulay (CM) so also is R^G, generalizing a result of M. Hochster and J. A. Eagon. If P is normal in G and G is generated by P and pseudo-reflections, we show that if R^G is CM so also is R^P. However, in general, R^G may even be polynomial with R^P not CM. Finally, we give a procedure for determining a set of generators for R^G given a set of generators for R^P.

Introduction. Let V be a vector space of dimension n over a field k of characteristic $p \geq 0$ with basis $\{x_1, \ldots, x_n\}$. Suppose $G \subset Gl(V)$ is finite group with a p-Sylow subgroup P. In what follows, if $p = 0$, set $P = \{1\}$. G and P act on the symmetric algebra $R \cong k[x_1, \ldots, x_n]$ of V as algebra automorphisms. Denote the respective rings of invariants by R^G and R^P. These rings are known to be finitely generated by a fundamental result due to Hilbert, see for example the beautiful survey paper of R. P. Stanley [10].

In this paper the relations between R^G and R^P are investigated; the philosophy has been to try and locate the difficulties at R^P. For example, it is well-known that R^G is Cohen-Macaulay (CM) when $p \not| |G|$ (here $|G|$ denotes the order of G) and G is finite—see the fundamental paper of Eagon and Hochster [4]. However, when $p > 0$ and p divides the order of G, R^G need not be CM. In fact, H. Nakijima [7, example 4.1, pgs. 211–212] gives examples of elementary abelian p-groups generated by pseudo-reflections ($g \in G$ is a *pseudo-reflection* if $\operatorname{rank}(1 - g) \leq 1$) with R^G *not* CM.

In section one a proof that R^P CM forces R^G to be CM is given. First a Reynold's or averaging operator $\rho : R^P \longrightarrow R^G$ is built using the cosets of G/P and then the proof is word for word that of [10, theorem 3.2, pg. 482]. In fact, in the cases $p = 0$ or $p \not| |G|$, $P = \{1\}$, so $R^P = R$ is polynomial and the original proof in [10] is recovered. If P is normal in G, and G is generated by P and pseudo-reflections, the converse is true, see Proposition 2.

In general, R^G may even be polynomial (and so CM) with R^P not CM. See the example following the proof of Proposition 2.

In section two a procedure for determining a set of generators for R^G given any set of generators for R^P is described. In turn, this relies on the paper [1]. This is perhaps

The first author gratefully acknowledges the support of NSERC.
Key words and phrases: Invariant theory
Received by the editors June 26, 1990.
AMS subject classification: 13F20.

the most interesting result of the paper for the following reason. Invariant theorists are familiar with two cases:

(1) $p = 0$ or $p \not| |G|$, the so-called non-modular case,

(2) $p \mid |G|$, the modular case.

In the non-modular case the proofs of many classical ($p = 0$) theorems work word for word in the more general setting $p \not| |G|$. However, E. Noether (see H. Weyl's description [11, pgs. 275–276]) shows that when $p = 0$, then R^G is generated by the $\binom{|G|+n}{n}$ polynomials $\frac{1}{|G|} \sum_{g \in G} g(f)$, as f ranges over all monomials in the variables $x_1, \ldots, x_n$ of degree at most $|G|$. The procedure described below requires averaging polynomials of degree at most $max(|G|, n\binom{|G|}{2})$ to achieve a proof that works also for $p \not| |G|$, see proposition 3 in section two. Finally, an attempt is made to obtain generators for R^P.

We would like to point out that this paper relies heavily on the papers of R. P. Stanley [10] and J. A. Eagon and M. Hochster [4].

Section One. Recall that a finitely generated **N**-graded commutative k-algebra $A = \oplus_{\ell \geq 0} A_\ell$ with $A_0 = k$ has Krull dimension n if n is the maximum number of algebraically independent elements of A over k. Further, if A has Krull dimension n, then a set $f_1, \ldots, f_n$ of algebraically independent homogeneous elements of positive degree is said to be a *homogeneous system of parameters* (hsop) if A is finitely generated as a module over the polynomial subalgebra $B = k[f_1, \ldots, f_n]$. If A is a domain then the Noether normalization lemma, see [13, theorem 25, pg. 200] implies that a hsop for A exists.

Let $\{f_1, \ldots, f_n\}$ be a hsop for A. A is said to be *Cohen-Macaulay* (CM) if A is free as a module over the polynomial subalgebra $B = k[f_1, \ldots, f_n]$. In other words, A is CM if there exist homogeneous elements $g_1, \ldots, g_m$ such that $A = \oplus_{l \geq 0}^m B g_l$ as B-modules. Further, if A is CM this holds if and only if the images of $g_1, \ldots, g_m$ in A/I form a vector space basis for A/I over k, where I is the ideal of A generated by $\{f_1, \ldots, f_n\}$. Finally, a standard result is that if A is free over one hsop then it is free for every hsop, see [9,theorem 2, p.IV-20].

Now $P \subset G \subset Gl(V)$ with P a p-Sylow subgroup of the finite group G. Further R is the symmetric algebra of V, so that $R^G \subset R^P$. Suppose $[G : P] = m$ so that $p \not| m$, and let $\alpha_1, \ldots, \alpha_m$ be coset representatives, i.e. $G = \cup \alpha_\ell P$. Define $\rho : R^P \longrightarrow R^G$ by $\rho(f) = \frac{1}{m} \sum_{\ell=1}^m \alpha_\ell(f)$. It is easy to see that ρ is independent of the choice of coset representatives and that $\rho(f) \in R^G$. It is also easy to see that ρ is a map of R^G-modules, $\rho(1) = 1$ and $\rho^2 = \rho$. It follows that $R^P = R^G \oplus U$ as R^G-modules where $U = ker(\rho)$.

THEOREM 1. *If R^P is CM then so also is R^G.*

PROOF. By the Noether Normalization theorem, a hsop $f_1, \ldots, f_n$ exists for R^G since it is finitely generated. Since R is integral over R^G, so also is R^P and so both are finitely generated as R^G-modules and so R^P is finitely generated as a module over $B = k[f_1, \ldots, f_n]$. Consequently $\{f_1, \ldots, f_n\}$ is hsop for R^P. But R^P is CM and so R^P is a free module over B. R^G is projective over the polynomial algebra B since as shown above it is a direct summand in the free module R^P, so R^G is a free B-module by Quillen's or

https://doi.org/10.4153/CMB-1991-007-0 Published online by Cambridge University Press

Suslin's solutions of Serre's conjecture, see for example [5]. Alternately, the decomposition $R^P = R^G \oplus U$ yields $R^P/I \cong R^G/J \oplus U/K$ where I is the ideal of R^P generated by $\{f_1, \ldots, f_n\}$, J is the ideal of R^G generated by $\{f_1, \ldots, f_n\}$, and $K = f_1U + \cdots + f_nU$. Choose homogeneous elements $g_1, \ldots, g_r$ in R^G which project to a basis for R^G/J and homogeneous elements $g_{r+1}, \ldots, g_s$ in U which project to a basis for U/K so that R^P/I has basis $\{\bar{g}_1, \ldots, \bar{g}_s\}$. But R^P is CM and R^P/I has $\{\bar{g}_1, \ldots, \bar{g}_s\}$ as a basis so $R^P = \oplus_{l=1}^s Bg_l$ and consequently $R^G = \oplus_{l=1}^r Bg_l$ and so is a free B-module. Thus R^G is CM. ∎

PROPOSITION 2. *Suppose P is normal in G and that G is generated by P and pseudo-reflections. Then R^P is CM if and only if R^G is CM.*

PROOF. The proposition follows immediately from [4, proposition 16, pg 1035] provided we show each pseudo-reflection of G acts as a generalized reflection on R^P ($\alpha \in G$ acts as a generalized reflection on R^P if there is a homogeneous positive degree element f in R^P with $(\alpha - 1)R^P \subset fR^P$).

Let $\alpha \in G$ be a non-trivial pseudo-reflection; then there is an $x \in V$ with $(\alpha - 1)R \subset xR$. Let $\mathrm{Stab}_P(x) = \{\beta \in P \mid \beta(x) = x\}$ and let Ω be a set of left coset representatives of $\mathrm{Stab}_P(x)$ in P containing $1 \in P$. Set $f = \prod_{\beta \in \Omega} \beta(x)$ so that $f \in R^P$. If $g \in R^P$ then $\alpha(g) \in R^P$, so $(\alpha - 1)(g) \in R^P \cap xR$. But $R^P \cap xR \subset \bigcap_{\beta \in \Omega} \beta(xR) = \bigcap_{\beta \in \Omega} \beta(x)R = fR$ (the last equality since P acts unipotently on V). Thus $(\alpha - 1)g \in R^P \cap xR \subset fR^P$. ∎

In general, R^G may even be polynomial, with R^P not CM. For example, consider the symmetric group Σ_p acting on V of dimension p over k as permutations of a basis X. The subgroup P of order p generated by a fixed cyclic permutation of X is a p-Sylow subgroup of Σ_p. R^{Σ_p} is the polynomial algebra on the elementary symmetric functions $\sigma_1, \ldots, \sigma_p$ while R^P is not CM for $p > 3$ by a result of Fossum and Griffith [2, corollary 1.8, pg. 193].

Section Two. As in Section One, let $G \subset Gl(V)$ be a finite group with a p-Sylow subgroup P. Let R^P be generated as a k-algebra by $\{f_1, \ldots, f_s\}$ for some $s \geq n$. Choose a set of coset representatives of P in G, $\alpha_1, \ldots, \alpha_m$, $m = [G : P]$. Let T denote the subalgebra of R generated by the ms elements $\alpha_i(f_j)$. G acts on T, since for fixed j, the elements of G act as permutations of the $\alpha_i f_j$. Consequently, we obtain a group homomorphism $\xi : G \longrightarrow \Sigma_m$ where Σ_m denotes the symmetric group on m letters. If S is the polynomial algebra $k[z_{ij} \mid 1 \leq i \leq m, 1 \leq j \leq s]$ the algebra homomorphism $\theta : S \longrightarrow R$ defined by $\theta(z_{ij}) = \alpha_i(f_j)$ has image T. Σ_m acts on S by $\sigma(z_{ij}) = z_{\sigma(i)j}$ so G acts on S via ξ. Consequently $S^{\Sigma_m} \subset S^G \subset S$. It is not difficult to see that the map θ is G-equivariant and so there is a commutative diagram

$$\begin{array}{ccccccc} & & S & \xrightarrow{\theta} & T & \subset & R \\ & & \uparrow & & \uparrow & & \uparrow \\ S^{\Sigma_m} & \subset & S^G & \xrightarrow{\theta} & T^G & \subset R^G \subset & R^P \end{array}$$

We claim that θ restricted to S^{Σ_m} maps onto R^G. To see this take $h = h(f_1, \ldots, f_s) \in R^G \subset R^P$ and form $g \in S$ by defining

$$g = \frac{1}{m}(h(z_{11}, \ldots, z_{1s}) + \cdots + h(z_{m1}, \ldots, z_{ms}))$$

(recall $p \not| m$). It is easy to see that $g \in S^{\Sigma_m}$ since $\sigma(h(z_{i1}, \ldots, z_{is})) = h(z_{\sigma(i)1}, \ldots, z_{\sigma(i)s})$ so that $\sigma \in \Sigma_m$ simply permutes the terms of g.

Now

$$\begin{aligned}
\theta(g) &= \frac{1}{m}\left[\theta\,(h(z_{11}, \ldots, z_{1s})) + \cdots + \theta\,(h(z_{m1}, \ldots, z_{ms}))\right] \\
&= \frac{1}{m}\left[h\,(\theta\,(z_{11}), \ldots, \theta\,(z_{1s})) + \cdots + h\,(\theta\,(z_{m1}), \ldots, \theta\,(z_{ms}))\right] \\
&= \frac{1}{m}\left[h(\alpha_1(f_1), \ldots, \alpha_1(f_s)) + \cdots + h(\alpha_m(f_1), \ldots, \alpha_m(f_s))\right] \\
&= \frac{1}{m}\left[\alpha_1(h) + \cdots + \alpha_m(h)\right] \\
&= \frac{1}{m}(mh) \\
&= h.
\end{aligned}$$

Thus $\theta : S^{\Sigma_m} \longrightarrow R^G$ is onto and is a map of algebras, so if generators for S^{Σ_m} are known generators for R^G are obtained by using the map θ.

Generators for S^{Σ_m} valid over any ring are described in [1]. Here is the result. Let $I = [a_{ij}]$ be a $m \times s$ matrix of non-negative integers, and let $z^I = z_{11}^{a_{11}} \cdots z_{ms}^{a_{ms}}$ denote the corresponding monomial in S. I is said to be an *exponent matrix*. Let $O(I) = \{ J \mid \exists \alpha \in \Sigma_m$ *with* $\alpha(z^I) = z^J \}$ so that $\{ z^J \mid J \in O(I) \}$ is the orbit of z^I under the action of Σ_m given above. Then $s(I) = \sum_{J \in O(I)} z^J$ is an invariant.

Let K_{ij} be the $m \times s$ matrix which is everywhere zero except in its *jth* column $K_{ij}^j = (1, \ldots, 1, 0, \ldots, 0)$ (i ones). Denote by σ_{ij} the orbit polynomial $s(K_{ij})$. This is the i-th elementary symmetric function in the variables $z_{1j}, \ldots, z_{mj}$. Set $B = k[\sigma_{ij} \mid 1 \leq i \leq m, 1 \leq j \leq s]$.

Just for the moment view each column, I^j, of an exponent matrix, I, as a function $I^j : \{ 1, \ldots, n \} \longrightarrow \mathbf{N}$. Define $Ker(I^j) = \{ i \mid I^j(i) = 0 \}$. Let Ω be the set of exponent matrices $I = [I^1 | \ldots | I^s]$ satisfying $I = 0$ or both of

(1) the image of I is an interval in $\mathbf{N}$ and,

(2) $\{ Ker(I^j) \mid 1 \leq j \leq s \}$ has no minimum element.

THEOREM. *Let A be the B-module generated by $\{ s(I) \mid I \in \Omega \}$. Then $A = S^{\Sigma_m}$.*

PROOF. See [1, theorem 4.1] ■

Remark. This method is a generalization of Emmy Noether's method for $k = \mathbf{Q}$, $\mathbf{R}$ or $\mathbf{C}$ (see H. Weyl's description [11, pgs. 275-276]).

PROPOSITION 3. *If $p \not| |G|$ then R^G is generated by polynomials of degree at most $max(|G|, n\binom{|G|}{2})$.*

PROOF. If $n = 1$, G is a finite subgroup of k^* and hence cyclic. It follows that R^G is generated by $x_1^{|G|}$.

We take each z_{ij} to have degree 1 so that θ is degree-preserving. A is generated as an algebra by the algebra generators of B (which have degree at most $m = |G|$) and the B-module generators of A. Property (2) above guarantees that each column of an exponent matrix in Ω has a zero entry, while property (1) then implies that a maximal entry in any column is $m-1$. Hence the result. ∎

Scholium. On generators for rings of invariants of p-groups $G = P$ over a finite field of characteristic p.

The following is an attempt to obtain generators for R^P when k is a finite field of characteristic $p > 0$. Suppose $P = \{\beta_1, \ldots, \beta_r\}$ so $r = p^t$, for some t. Then P acts on itself via left multiplication and we obtain $\xi : P \longrightarrow \Sigma_r$. Fix a basis $\{x_1, \ldots, x_n\}$ for V and let U denote the upper triangular p-Sylow subgroup of $Gl(V)$. Replacing P by some conjugate of P if necessary assume that $P \subset U$. Now R^U is the polynomial algebra $k[v_1, \ldots, v_n]$ where $v_i = \prod_{\gamma \in U/\,\mathrm{Stab}_U(x_i)} \gamma(x_i)$. This result is well-known, see for example [6,theorem 3.4, pg. 328] or [8, proposition 4.1 and example 4.3, pgs.265 and 269] or [12, theorem 3.1(c), pg. 428]). Set $S = k[z_{ij} \mid 1 \leq i \leq r, 1 \leq j \leq n]$ and define $\theta(z_{ij}) = \alpha_i(x_j) \in R$. Then Σ_r acts on S by $\sigma(z_{ij}) = z_{\sigma(i)j}$, and so P acts on S via ξ, and θ is equivariant as before.

Proceeding as above obtain a map of algebras $\theta : S^{\Sigma_r} \longrightarrow R^P$. Construct a subalgebra A of R^P by adjoining the elements $v_1, \ldots, v_n$ to the subalgebra $im(\theta \mid_{S^{\Sigma_r}})$. Then $R^U \subset A \subset R^P$. Since generators for S^{Σ_r} are known (see [1]) a set of generators for A is obtained.

PROPOSITION 4. $R^P = \{f \in R \mid \exists\, \ell \in \mathbf{N}\ with\, f^{p^\ell} \in A\}$.

PROOF. For each ℓ set $B_\ell = \{f \in R \mid f^{p^\ell} \in A\}$. If $f \in B_\ell$ then $f^{p^\ell} \in A \subset R^P$ so $\alpha(f^{p^\ell}) = f^{p^\ell}$ for all $\alpha \in P$. Thus $(\alpha(f) - f)^{p^\ell} = 0$ and consequently $(\alpha - 1)f = 0$ since R is a domain. Hence $B_\ell \subset R^P$. On the other hand, if $f = f(x_1, \ldots, x_n) \in R^P$ then the element $g = \prod_{i=1}^r f(z_{i1}, \ldots, z_{in}) \in S^{\Sigma_r}$ and $\theta(g) = f^r$. ∎

Let Q(S) denote the field of fractions of a domain S.

PROPOSITION 5. $R^P = Q(A) \cap R$.

PROOF. Now $Q(R^U) \subset Q(A) \subset Q(R^P) \subset Q(R)$, and $Q(R)$ is Galois over $Q(R^U) = Q(R)^U$ with Galois group U. So $Q(A) = Q(R)^H$ for some subgroup H of U with $P \subset H$. Consider $f \in R^P$ and $h \in H$. Since $f^r \in A$ we have $((h-1)f)^r = (h-1)(f^r) = 0$ so $h(f) = f$ for $f \in R^P$. It follows that $H = P$ and $Q(R^P) = Q(A)$, hence the result. ∎

REFERENCES

1. H. E. A. Campbell, I. Hughes, R. D. Pollack, *On the vector invariants of the symmetric groups* preprint.
2. R. M. Fossum, P. A. Griffith, *Complete local factorial rings which are not Cohen-Macaulay in characteristic p*, Ann. scient. Èc. Norm. Sup. 4^e sèrie **8**(1975) 189–200.
3. M. Hochster, *The invariant theory of commutative rings*, Contemp. Math. **43**(1985) 161–179.
4. M. Hochster, J. A. Eagon, *Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci*, Amer. J. Math. **93**(1971) 1020–1058.
5. T. Y. Lam, *Serre's conjecture*, Lecture Notes in Math. **635** Springer-Verlag New York.

6. H. Mùi, *Modular invariant theory and the cohomology algebras of symmetric groups*, J. Fac. Sci., Univ. Tokyo, Sec. IA, **22** (1975) 319–369.
7. H. Nakajima, *Invariants of finite abelian groups generated by transvections*, Tokyo Journal of Math. (2)**3** (1980) 201–214.
8. ———, *Regular rings of invariants of unipotent groups*, Journal of Algebra **85**(1986) 253–286.
9. J. P. Serre, *Algèbre Locale Multiplicités*, Lecture Notes in Math. **11** Springer-Verlag, New York 1975 .
10. R. P. Stanley, *Invariants of finite groups and their applications to combinatorics*, Bull. A.M.S. (3)**1** May 1979 475–511.
11. H. Weyl, *Classical Groups*, Princeton University Press, Princeton, New Jersey, U.S.A. 1939.
12. C. Wilkerson, *A primer on the Dickson invariants*, Contemp. Math. **19**(1983) 421–434.
13. O. Zariski, P. Samuel, *Commutative Algebra,* Vol. II van Nostrand Princeton, New Jersey, U.S.A. 1960.

Department of Mathematics and Statistics
Queen's University
Kingston, Ontario, K7L 3N6