JOURNAL OF ALGEBRA 49, 134–148 (1977)

Relative Invariants of Finite Groups Generated by Pseudoreflections

RICHARD P. STANLEY*

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139

Communicated by D. Buchsbaum

Received November 15, 1976

1. INTRODUCTION

Let V be an m-dimensional vector space over the complex numbers $\mathbb{C}$. Fix a basis $x_1, \ldots, x_m$ for V, and identify the polynomial ring $R = \mathbb{C}[x_1, \ldots, x_m]$ with the symmetric algebra of V in the obvious way. If $A \in GL(V)$ (the group of invertible linear transformations $V \to V$), then A extends to a $\mathbb{C}$-automorphism of R by $(Af)(x_1, \ldots, x_m) = f(Ax_1, \ldots, Ax_m)$, where $f \in R$. Suppose G is any subgroup of $GL(V)$. Denote by R^G the ring of invariants of G acting on R, i.e.,

$$R^G = \{f \in R \mid Af = f \text{ for all } A \in G\}.$$

More generally, if χ is any linear character of G, then let $R_\chi{}^G$ denote the set of invariants relative to χ, i.e.,

$$R_\chi{}^G = \{f \in R \mid Af = \chi(A)f \text{ for all } A \in G\}.$$

Elements of $R_\chi{}^G$ are sometimes known as *relative invariants*, *semiinvariants*, or *χ-invariants*. Clearly $R_\chi{}^G$ is a module over the ring R^G.

If G is finite, then it is easily seen [2, Sect. 262] that R^G contains m, but not $m + 1$, elements which are algebraically independent over $\mathbb{C}$. Equivalently, R^G has Krull dimension m. It is natural to ask when in fact we can find m such invariants which generate all of R^G as a $\mathbb{C}$-algebra, i.e., when $R^G = \mathbb{C}[\theta_1, \ldots, \theta_m]$ for some $\theta_1, \ldots, \theta_m \in R$. The answer to this question is associated with the names of Coxeter, Shephard and Todd, Chevalley, and Serre. For an exposition, see [1, Chap. 5, Sect. 5.2] or [4]. To state the result, recall that an element A of $GL(V)$ is a *pseudoreflection* if $1 - A$ has rank one. Thus if $A \in GL(V)$ has finite multiplicative order, then A is a pseudoreflection if and only if it has exactly one eigenvalue ρ not equal to one. In this case $\rho = \det A$.

* Supported in part by Bell Telephone Laboratories and by NSF Grant MCS 7308445-A04.

ISSN 0021-8693

1.1. THEOREM. *Let G be a finite subgroup of $GL(V)$. Then $R^G = \mathbb{C}[\theta_1, ..., \theta_m]$ for some $\theta_1, ..., \theta_m \in R$ if and only if G is generated by pseudo-reflections. (A classification of all such groups appears in* [7].)

Henceforth we shall call a finite subgroup of $GL(V)$ generated by pseudo-reflections an *f.g.g.r.* Our object will be to describe the modules $R_\chi{}^G$ of relative invariants of an f.g.g.r. G. As a consequence, we will obtain a fairly explicit description of the rings R^H, where H is a normal subgroup of an f.g.g.r. G such that G/H is Abelian. In particular, when $H = G \cap SL(V)$, we obtain a necessary and sufficient condition for R^H to be a complete intersection.

A fundamental tool in our work will be a result of Molien. If G is any subgroup of $GL(V)$, then R^G has the structure of a graded ring, viz., $R^G = R_0{}^G + R_1{}^G + \cdots$, where $R_n{}^G$ is the space of all homogeneous polynomials in R^G of degree n. More generally, each $R_\chi{}^G$ has in the same way the structure of a graded R^G-module, written $R_\chi{}^G = (R_\chi{}^G)_0 + (R_\chi{}^G)_1 + \cdots$. Define the *Molien series* $F_\chi(G, \lambda)$ to be the formal power series

$$F_\chi(G, \lambda) = \sum_{n=0}^{\infty} (\dim_{\mathbb{C}}(R_\chi{}^G)_n)\, \lambda^n,$$

where λ is an indeterminate. If χ is the trivial character, so that $R_\chi{}^G = R^G$, then we write $F(G, \lambda)$ for $F_\chi(G, \lambda)$.

1.2. THEOREM ([6]; see also [2, Sect. 227] and [1, Chap. V, Sect. 5.3, Lemme 3]). *If G is a finite subgroup of $GL(V)$ and χ is a linear character of G, then*

$$F_\chi(G, \lambda) = \frac{1}{|G|} \sum_{A \in G} \frac{\chi(A)^{-1}}{\det(1 - \lambda A)}.$$

If G is an f.g.g.r., then by Theorem 1.1 we have $R^G = \mathbb{C}[\theta_1, ..., \theta_m]$, for some $\theta_1, ..., \theta_m \in R$, which can be chosen to be homogeneous, say with $\deg \theta_i = d_i$. It is clear from the definition of $F(G, \lambda)$ that then

$$F(G, \lambda) = 1/(1 - \lambda^{d_1})(1 - \lambda^{d_2}) \cdots (1 - \lambda^{d_m}). \tag{1}$$

It is well known and easy to deduce from Theorem 1.2 and (1) that

$$d_1 d_2 \cdots d_m = |G|, \tag{2}$$

$$(d_1 - 1) + (d_2 - 1) + \cdots + (d_m - 1) = r, \tag{3}$$

where r denotes the number of pseudoreflections in G.

2. Free Modules of Relative Invariants

For the remainder of this paper we adopt the following terminology. G denotes a finite subgroup of $GL(V)$ (where V is as in the previous section), and χ denotes a linear character of G. A hyperplane $H \subset V$ is called a *reflecting hyperplane* if some nonidentity element A of G fixes H pointwise. It follows that A is a pseudoreflection, and conversely any pseudoreflection A fixes a unique reflecting hyperplane. Let $H_1, H_2, \ldots, H_\nu$ denote the (distinct) reflecting hyperplanes associated with G. The set of all elements of G fixing H_i pointwise forms a cyclic subgroup C_i generated by a pseudoreflection. Let c_i denote the order of C_i, and let P_i be some fixed generator of C_i. Let $L_i = L_i(x_1, \ldots, x_m)$ be the linear form defining H_i, i.e., $H_i = \{\alpha \in V \mid L_i(\alpha) = 0\}$. Thus $L_i \in R_1$, the first homogeneous part of R. For $1 \leqslant i \leqslant \nu$, define integers $s_i = s_i(\chi)$ by the condition that s_i is the least nonnegative integer satisfying $\chi(P_i) = (\det P_i)^{s_i}$. (Clearly s_i depends only on C_i, not on P_i.) Finally define $f_\chi \in R$ by $f_\chi = \prod_{i=1}^{\nu} L_i^{s_i}$. Thus f_χ is homogeneous of degree $s_1 + s_2 + \cdots + s_\nu$.

2.1. Lemma. *Let G be a finite subgroup of $GL(V)$ and χ a linear character of G. Suppose R_χ^G is a free R^G-module of rank one, so that $R_\chi^G = g_\chi \cdot R^G$ for some homogeneous $g_\chi \in R$ (uniquely determined up to multiplication by a nonzero scalar). Then* $\deg g_\chi = s_1(\chi) + s_2(\chi) + \cdots + s_\nu(\chi)$.

Proof. Let $d = \deg g_\chi$. It follows from Theorem 1.2 that

$$\sum_{A \in G} \frac{\chi(A)^{-1}}{\det(1 - \lambda A)} = \lambda^d \sum_{A \in G} \frac{1}{\det(1 - \lambda A)}. \tag{4}$$

Multiply by $(1 - \lambda)^m$ and expand both sides in a Taylor series about $\lambda = 1$. The left-hand side of (4) is given by

$$1 + (1 - \lambda) \sum_P \frac{\chi(P)^{-1}}{1 - \rho} + O((1 - \lambda)^2),$$

where P ranges over all pseudoreflections in G and where $\rho = \det P$. The right-hand side of (4) becomes

$$1 + (1 - \lambda)\left(-d + \sum_P \frac{1}{1 - \rho}\right) + O((1 - \lambda)^2).$$

It follows that

$$d = \sum_P \frac{1 - \chi(P)^{-1}}{1 - \rho}. \tag{5}$$

If we remove the identity element from each of the cyclic groups C_i defined above, we obtain a partition of the pseudoreflections of G. Hence we may rewrite (5) as

$$d = \sum_{i=1}^{\nu} \sum_{P} \frac{1 - \chi(P)^{-1}}{1 - \rho}, \tag{6}$$

where for fixed i, P ranges over all pseudoreflections in C_i (i.e., over all elements of $C_i - \{1\}$). If we let H be the subgroup of $GL(1, \mathbb{C})$ generated by the primitive c_ith root of unity $\zeta = \det P_i$, and if we let ψ be the character of H defined by $\psi(\zeta) = \chi(P_i)$, then the sum over P in (6) has exactly the same form as the right-hand side of (5), with G replaced by H and with χ replaced by ψ. Thus by what we have just proved, the sum on P in (6) is equal to the least degree of a ψ-invariant of H. But the ψ-invariants of H can be obtained by inspection; if we regard H as acting on $T = \mathbb{C}[x]$, then $T_\psi^H = x^{t_i}\mathbb{C}[x^{c_i}]$, where $\psi(\zeta) = \zeta^{t_i}$, $0 \leqslant t_i < c_i$. Thus the sum on P in (6) is equal to t_i. But since $\psi(\zeta) = \chi(P_i)$ and $\zeta = \det P_i$, we see that $t_i = s_i$, as defined above. The proof follows from (6). ∎

We remark that the above proof is reminiscent of an argument of Solomon [10, p. 279]. Other applications of Molien's theorem to invariant theory appear for instance in [1, 7, 8].

2.2. Lemma. *Let G be any finite subgroup of $GL(V)$, and let χ be a linear character of G. If $f \in R_\chi^G$, then f is divisible by $\prod_{i=1}^{\nu} L_i^{s_i(\chi)}$.*

Proof. Given i satisfying $1 \leqslant i \leqslant \nu$, choose a new basis $y_1, \ldots, y_m$ for V so that $y_1 = L_i$ and $y_2, \ldots, y_m$ spans H_i. With respect to this basis the matrix of P_i has the form

$$P_i = \begin{bmatrix} \rho & & & & & 0 \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & \ddots & \\ 0 & & & & & 1 \end{bmatrix}.$$

Thus if $f(y_1, \ldots, y_m) \in R_\chi^G$, then $f(\rho y_1, y_2, \ldots, y_m) = \rho^{s_i} f(y_1, y_2, \ldots, y_m)$. It follows that f must be divisible by $y_1^{s_i}$. Hence in terms of the x_i's, $f(x_1, \ldots, x_m)$ is divisible by $L_i^{s_i}$. ∎

The above proof is analogous to an argument of Steinberg [13].

Combining Lemmas 2.1 and 2.2, we obtain the following result.

2.3. THEOREM. *Let G be a finite subgroup of $GL(V)$ and let χ be a linear character of G. The following two conditions are equivalent.*

(i) *$R_\chi{}^G$ is a free R^G-module of rank one.*

(ii) *$f_\chi = \prod_{i=1}^{\nu} L_i^{s_i(\chi)}$ is a χ-invariant.*

If (i) *and* (ii) *hold then in fact $R_\chi{}^G = f_\chi \cdot R^G$.*

Proof. Assume (i). By Lemma 2.2, any χ-invariant f is divisible by f_χ. By Lemma 2.1, there exists a χ-invariant of degree $\sum s_i(\chi)$. It follows that f_χ is a χ-invariant.

Assume (ii). By Lemma 2.2, any χ-invariant f is divisible by f_χ. Then $f/f_\chi \in R^G$. It follows that $R_\chi{}^G = f_\chi \cdot R^G$, so (i) holds.

Note that in the course of the proof we have established the assertion $R_\chi{}^G = f_\chi \cdot R^G$. ∎

Problem. Classify all pairs (G, χ) satisfying the conditions of Theorem 2.3.

In the next section we will apply Theorem 2.3 to groups generated by pseudoreflections. First we give an application of a different nature.

2.4. COROLLARY. *Preserve the notation of this section. The following two conditions are equivalent.*

(i) *R^G is a Gorenstein ring.*

(ii) *Let χ be the character $\chi(A) = \det(A)^{-1}$. Then $L_1^{c_1-1}L_2^{c_2-1} \cdots L_\nu^{c_\nu-1}$ is a χ-invariant.*

Remark. Some conditions for R^G to be Gorenstein appear in [14, 15]. These were extended to a necessary and sufficient condition (different from (ii) above) in [12], namely, R^G is Gorenstein if and only if the following identity holds in the field $\mathbb{C}(\lambda)$, λ an indeterminate:

$$\lambda^r \sum_{A\in G} \frac{1}{\det(1-\lambda A)} = \sum_{A\in G} \frac{\det A}{\det(1-\lambda A)},$$

where r is the number of pseudoreflections in G.

Proof of Corollary 2.4. Hochster and Eagon [5, Prop. 13] (and others) have shown that R^G is a Cohen–Macaulay ring. It follows from work of Watanabe [15] (a direct proof was shown to me by Eisenbud) that if G is any finite subgroup of $GL(V)$, then $R_\chi{}^G$ is the canonical module of R^G (where $\chi = \det^{-1}$). Recall that a Cohen–Macaulay graded algebra S is Gorenstein if and only if the canonical module K_S is a free S-module of rank one. For the character $\chi = \det^{-1}$, it is clear that $s_i(\chi) = c_i - 1$. The proof now follows from Theorem 2.3. ∎

3. Relative Invariants of f.g.g.r.'s

Unless otherwise stated, for the remainder of this paper G denotes an f.g.g.r. and χ a linear character of G. Moreover, we assume that $R^G = \mathbb{C}[\theta_1, ..., \theta_m]$, where θ_i is homogeneous of degree d_i. We now show that Theorem 2.3 is applicable to this situation.

3.1. Theorem. *Let $G \subset GL(V)$ be an f.g.g.r., and let χ be a linear character of G. Then the module $R_\chi{}^G$ is a free R^G-module of rank one. Thus $R_\chi{}^G = f_\chi \cdot R^G$, where f_χ is given explicitly by Theorem* 2.3.

Proof. Chevalley [3, Thm. (B)] has shown that if G is finite and generated by reflections (i.e., pseudoreflections of determinant -1), and if F is the ideal of R generated by the homogeneous elements in R^G of positive degree, then the natural representation of G in R/F is equivalent to the regular representation. There is no difficulty in extending this result to f.g.g.r.'s. Since a linear representation of a finite group has multiplicity one in the regular representation, it follows immediately that $R_\chi{}^G$ is a cyclic R^G-module. Since $R_\chi{}^G$ is clearly torsion-free, it follows that $R_\chi{}^G$ is free of rank one, as was to be proved. ∎

An alternative proof of Theorem 3.1 can be given using the easily established result that if G is any finite subgroup of $GL(V)$ and if χ is any linear character of G, then $R_\chi{}^G$ is a Cohen–Macaulay R^G-module of Krull dimension m. The details are omitted. A result closely related to Theorem 3.1 appears in [11, Cor. 2.8].

Remarks. (1) Suppose we take χ to be the character defined by $\chi(A) = (\det A)^{-1}$. Then $s_i = c_i - 1$, so $\deg f_\chi = \sum (c_i - 1) = r$, the number of pseudoreflections in G. The formula $f_\chi = \prod L_i^{c_i - 1}$ is a known result (see [9, pp. 59–60]). We remark that an alternative expression for f_χ is known (e.g., [13, p. 616]), viz.,

$$f_\chi = \det J(\theta_1, ..., \theta_m),$$

where $R^G = \mathbb{C}[\theta_1, ..., \theta_m]$ and $J(\theta_1, ..., \theta_m) = (\partial\theta_i/\partial x_j)$, the Jacobian matrix of $\theta_1, ..., \theta_m$.

(2) Now take χ to be defined by $\chi(A) = \det A$. Then $s_i = 1$, so $\deg f_\chi = \nu$, the number of reflecting hyperplanes, and $f_\chi = \prod L_i$. From (5) we get

$$\nu = \sum_P \frac{1-\rho^{-1}}{1-\rho} = -\sum_P \rho.$$

Note also the formula

$$\frac{r}{2} = \sum_P \frac{1}{1-\rho} = -\sum_P \frac{\rho}{1-\rho}.$$

This is most easily seen from the fact that $[1/(1-\rho)] + [1/(1-\rho^{-1})] = 1$ since $|\rho| = 1$.

4. Invariants of Certain Subgroups of f.g.g.r.'s

The results of the preceding section make it possible to give a fairly explicit description of the rings R^H, where H is a normal subgroup of an f.g.g.r. G such that G/H is Abelian. We require the following lemma.

4.1. Lemma. *Let G be any finite subgroup of $GL(V)$ and let Γ be the group of all linear characters of G. (Thus $\Gamma \cong G/G'$, where G' is the commutator subgroup of G.) Let Λ be a subgroup of Γ, and let H be the normal subgroup of G defined by*

$$H = \{A \in G \mid \chi(A) = 1 \text{ for all } \chi \in \Lambda\}.$$

(Thus by the character theory for Abelian groups, $G/H \cong \Lambda$.) Then

$$R^H = \sum_{\chi \in \Lambda} R_\chi{}^G \qquad \text{(vector space direct sum).}$$

Proof. First note that the sum $\sum_{\chi\in\Lambda} R_\chi{}^G$ is indeed a direct sum, since linear representations are irreducible. Now let $R' = \sum_{\chi\in\Lambda} R_\chi{}^G$. If $A \in H$, $\chi \in \Lambda$, and $f \in R_\chi{}^G$, then $Af = \chi(A)f = f$, so $f \in R^H$. Thus $R' \subset R^H$. We prove the reverse inclusion by showing that R' and R^H have the same Hilbert function, i.e., the space $R_n{}'$ of forms in R' of a given degree n has the same dimension as the space $R_n{}^H$ of forms in R^H of degree n. If $b_n = \dim R_n{}'$, then by Theorem 1.2 we have

$$\begin{aligned}\sum_{n=0}^{\infty} b_n \lambda^n &= \sum_{\chi\in G} \frac{1}{|G|} \sum_{A\in G} \frac{\chi(A)^{-1}}{\det(1-\lambda A)} \\ &= \frac{1}{|G|} \sum_{A\in G} \frac{1}{\det(1-\lambda A)} \sum_{\chi\in\Lambda} \chi(A)^{-1}.\end{aligned}$$

Now for fixed $A \in G$ we have

$$\begin{aligned}\sum_{\chi\in\Lambda} \chi(A)^{-1} &= |\Lambda| \qquad \text{if } A \in H \\ &= 0 \qquad \text{if } A \notin H.\end{aligned}$$

Hence

$$\begin{aligned}\sum_{n=0}^{\infty} b_n \lambda^n &= \frac{|\Lambda|}{|G|} \sum_{A\in H} \frac{1}{\det(1-\lambda A)} \\ &= F(H, \lambda),\end{aligned}$$

by Theorem 1.2, since $G/H \cong \Lambda$ so $|\Lambda|/|G| = 1/|H|$. This completes the proof. ∎

4.2. COROLLARY. *In Lemma* 4.1, *let G be an f.g.g.r. Then*

$$R^H = \sum_{\chi \in A} f_\chi \cdot R^G,$$

where f_χ is given by Theorem 2.3. ∎

We have mentioned previously that R^G is a Cohen–Macaulay ring when G is a finite subgroup of $GL(V)$. This is equivalent to the assertion that there exist m homogeneous elements $\theta_1, \theta_2, ..., \theta_m \in R^G$ which are algebraically independent over $\mathbb{C}$, such that R^G is a finitely generated free module over the polynomial ring $\mathbb{C}[\theta_1, ..., \theta_m]$. In other words, there exist $\eta_1, \eta_2, ..., \eta_t \in R^G$ (which may be chosen to be homogeneous) such that every $f \in R^G$ has a *unique* representation in the form $f = \sum_1^t \eta_i \cdot p_i(\theta_1, ..., \theta_m)$, where p_i is a polynomial in $\theta_1, ..., \theta_m$ with complex coefficients. When G is an f.g.g.r. and H is a subgroup of G containing G' (the commutator subgroup of G), then Corollary 4.2 gives an explicit description of $\theta_1, ..., \theta_m$ and $\eta_1, ..., \eta_t$ for the ring R^H. Namely, the θ_i's are the polynomials guaranteed by Theorem 1.1 for which $R^G = \mathbb{C}[\theta_1, ..., \theta_m]$, and the η_i's are the f_χ's, $\chi \in A$. Moreover, implicit in Corollary 4.2 is the following simple description of the quotient ring $Q = R^H/(\theta_1, ..., \theta_m)$.

4.3. COROLLARY. *Let $G \subset GL(V)$ be an f.g.g.r., and let H be a normal subgroup of G for which G/H is Abelian. Let A be related to H as in Lemma* 4.1, *and let $R^G = \mathbb{C}[\theta_1, ..., \theta_m]$, where the θ_i's are homogeneous and algebraically independent over $\mathbb{C}$. Then $\theta_1, ..., \theta_m$ is a system of parameters* (*and a regular sequence*) *for R^H. Let $Q = R^H/(\theta_1, ..., \theta_m)$. Then as a vector space over $\mathbb{C}$, Q has as a basis the* (*images of the*) *elements f_χ, $\chi \in A$* (*given explicitly by Theorem* 2.3). *After multiplying the f_χ's by suitable nonzero complex numbers, multiplication in Q is given by*

$$f_\chi f_\psi = \begin{cases} f_{\chi\psi}, & \text{if } \deg f_{\chi\psi} = \deg f_\chi + \deg f_\psi \\ 0, & \text{otherwise.} \end{cases} \tag{7}$$

Proof. Only (7) needs to be proved. Now $f_\chi f_\psi$ is a $\chi\psi$-invariant of G, so $f_\chi f_\psi = g f_{\chi\psi}$ for some $g \in R^G$. If $\deg f_\chi + \deg f_\psi = \deg f_{\chi\psi}$, then g is a nonzero scalar. Otherwise g belongs to the ideal $(\theta_1, ..., \theta_m)$ of R^G, so it is zero in Q. Finally, it is easy to arrange that each scalar g is 0 or 1, e.g., by letting the coefficient of the lexicographically greatest nonzero term of f_χ be 1. ∎

EXAMPLE. An explicit example will be given for the sake of clarity. Suppose G has five reflecting hyperplanes H_1, H_2, H_3, H_4, H_5. Let C_j be the cyclic group fixing H_j, and let $c_j = |C_j|$. Suppose $(c_1, c_2, c_3, c_4, c_5) = (2, 3, 3, 4, 6)$. Let $\zeta = e^{2\pi i/12}$, and suppose we have chosen generators P_j of C_j so that $\det P_1 = \zeta^6 = -1$, $\det P_2 = \zeta^4$, $\det P_3 = \zeta^4$, $\det P_4 = \zeta^3$, $\det P_5 = \zeta^2$. Suppose finally that ψ is a character of G satisfying $\psi^{12} = 1$, $\psi(P_1) = \zeta^6 = -1$, $\psi(P_2) =$

ζ^4, $\psi(P_3) = \zeta^8$, $\psi(P_4) = \zeta^3$, $\psi(P_5) = \zeta^2$. Let $\Lambda = \{1, \psi, \psi^2,..., \psi^{11}\}$. The following table of the numbers $s_i = s_i(\chi)$ (as defined at the beginning of Section 2), and from this the numbers $\deg f_\chi = \sum s_i(\chi)$, is easily constructed for $\chi \in \Lambda$.

χ	s_1	s_2	s_3	s_4	s_5	$\deg f_\chi$
1	0	0	0	0	0	0
ψ	1	1	2	1	1	6
ψ^2	0	2	1	2	2	7
ψ^3	1	0	0	3	3	7
ψ^4	0	1	2	0	4	7
ψ^5	1	2	1	1	5	10
ψ^6	0	0	0	2	0	2
ψ^7	1	1	2	3	1	8
ψ^8	0	2	1	0	2	5
ψ^9	1	0	0	1	3	5
ψ^{10}	0	1	2	2	4	9
ψ^{11}	1	2	1	3	5	12

Hence Q as a vector space has a basis $1 = f_0, f_1,..., f_{11}$ with $f_i f_j = 0$ except for the following relations (and the commutative law): $f_0 f_i = f_i$ for all i, $f_1 f_6 = f_7$, $f_2 f_9 = f_{11}$, $f_3 f_8 = f_{11}$, $f_4 f_6 = f_{10}$, $f_5 f_6 = f_{11}$, $f_6 f_8 = f_2$, $f_6 f_9 = f_3$, $f_8 f_9 = f_5$. Hence $Q \cong \mathbb{C}[f_1, f_4, f_6, f_8, f_9]/(f_1^2, f_4^2, f_6^2, f_8^2, f_9^2, f_1 f_4, f_1 f_8, f_1 f_9, f_4 f_8, f_4 f_9)$.

5. A Class of Complete Intersections

Let k be a field. Recall that a graded k-algebra S is a *complete intersection* if it is isomorphic to a quotient $R/(\phi_1,..., \phi_t)$, where $R = k[x_1,..., x_m]$ and $\phi_1,..., \phi_t$ is a (homogeneous) R-sequence. If one can take $t = 1$, then S is called a *hypersurface*. It is an open problem to determine all finite $G \subset GL(V)$ such that R^G is a complete intersection or a hypersurface. Using Corollary 4.3 we can give some cases where R^G is a complete intersection.

Let $G \subset GL(V)$ be an f.g.g.r., and let Λ be the cyclic group generated by the character ψ given by $\psi(A) = \det A$. In this case the subgroup H of Lemma 4.1 is given by $H = G \cap SL(V)$. We will determine an explicit condition for R^H to be a complete intersection. Our method can be extended to subgroups H of G containing G' other than $H = G \cap SL(V)$, but we will content ourselves here with the case $H = G \cap SL(V)$.

Let $H = G \cap SL(V)$ as above; and let $c_1, c_2,..., c_v$ have the same meaning as in Section 2. Let $A = \{a_1, a_2,..., a_t\}$ be the set of *distinct* c_i's. Applying Corollary 4.3 to the case at hand (so that Λ is a cyclic group of order $a =$ l.c.m. $(a_1, a_2,..., a_t)$ generated by the character $\psi = \det$), we see that the ring $Q =$

$Q(A)$ of Corollary 4.3 has the following structure. A $\mathbb{C}$-basis for $Q(A)$ can be taken to be all sequences

$$X_i = \langle \alpha_1, \alpha_2, ..., \alpha_t \rangle, \qquad 0 \leqslant i < a, \tag{8}$$

such that $\alpha_j \equiv i \pmod{a_j}$ and $0 \leqslant \alpha_j < a_j$ for all j. Multiplication in $Q(A)$ is defined by

$$\begin{aligned} \langle \alpha_1, ..., \alpha_t \rangle \cdot \langle \beta_1, ..., \beta_t \rangle &= \langle \alpha_1 + \beta_1, ..., \alpha_t + \beta_t \rangle, \text{ if } 0 \leqslant \alpha_j + \beta_j < a_j \text{ for all } j \\ &= 0, \qquad \text{otherwise.} \end{aligned} \tag{9}$$

Now if S is a (graded) Noetherian k-algebra and $\phi_1, ..., \phi_m$ is a regular sequence, then S is a complete intersection if and only if $S/(\phi_1, ..., \phi_m)$ is a complete intersection. Hence R^H is a complete intersection if and only if $Q(A)$ is, so the question of whether or not R^H is a complete intersection is completely determined by the set A. We say that A is a *CI-set* if R^H (or $Q(A)$) is a complete intersection. Our problem is to characterize CI-sets.

In order to state our characterization, we require some additional terminology. Let π be a partition of some finite set A of positive integers. (A *partition* of a set A is a collection of nonvoid pairwise-disjoint subsets of A, called *blocks*, whose union is A.) We say that a partition σ of a set A' is an *elementary reduction* of π, written $\pi \to \sigma$, if σ can be obtained from π by one of the following two rules:

(ϵ_1) σ can be any refinement of π such that any two elements of A which are not relatively prime are in the same block of σ;

(ϵ_2) if some integer $\delta > 1$ divides every element of some block B of σ, then we may divide every element of B by δ and discard the integer 1 if it now appears.

If π has no elementary reductions, then it is called *irreducible*. If by a series of elementary reductions π can be transformed into a partition ω such that the elements of each block of ω are linearly ordered by divisibility, then we say that π is *completely reducible*. (It is evident that ω may now be further reduced to the null partition.) We identify a set A with the partition of A into one block, and therefore speak of A as being irreducible, completely reducible, etc.

For instance, suppose a, b, c, d, e are pairwise prime integers greater than one, and let $A = \{a, a^2, a^3, a^3b, ac, ac^3, d, de\}$. Then the following sequence of elementary reductions shows that A is completely reducible:

$$\begin{aligned} A &\to \{a, a^2, a^3, a^3b, ac, ac^3\}, \{d, de\} \\ &\to \{a, a^2, a^2b, c, c^3\}, \{d, de\} \\ &\to \{a, a^2, a^2b\}, \{c, c^3\}, \{d, de\}. \end{aligned}$$

We can now state the main result of this section.

5.1. THEOREM. *Let A be a finite set of integers greater than one. The following two conditions are equivalent:*

(i) *A is completely reducible,*

(ii) *A is a CI-set.*

Proof. (i) $\Rightarrow$ (ii) We have noted that a completely reducible partition π can actually be transformed into the null partition by a sequence of elementary reductions. Hence it suffices to prove that if $\pi \rightarrow \sigma$, then every block of π is a CI-set if and only if every block of σ is a CI-set. (We in fact only need the "if" part for (i) $\Rightarrow$ (ii).) Since we need consider only one block of π at a time, we may assume $\pi = A$ (the partition of A into one block).

Let $A = \{a_1, ..., a_t\}$ be the set of distinct c_i's which correspond to some f.g.g.r. $G \subset GL(V)$ and let $H = G \cap SL(V)$. Suppose that $A \rightarrow \{A_1, ..., A_q\}$ is an elementary reduction of type ϵ_1. Using the description (8) and (9) of $Q(A)$, a simple application of the Chinese Remainder Theorem shows that

$$Q(A) = Q(A_1) \otimes_k Q(A_2) \otimes_k \cdots \otimes_k Q(A_q).$$

Now $Q(A)$ is a complete intersection if and only if each factor $Q(A_i)$ is a complete intersection, so A is a CI-set if and only if each A_i is a CI-set.

Now assume that $A \rightarrow B$ is an elementary reduction of type ϵ_2. Hence $A = \{a_1, ..., a_t\}$ and $B = \{b_1, ..., b_t\}$, where $a_i = \delta b_i$ for some $\delta > 0$ and all i, except that if some $a_j = \delta$ then we discard b_j. This last step of discarding $b_j = 1$ is by (9) irrelevant in what follows, so let us ignore it. Let $X_0, ..., X_{a-1}$ be the $\mathbb{C}$-basis for $Q(A)$ defined in (8); and let $Y_0, ..., Y_{b-1}$ be the analogous basis for $Q(B)$, so $b = a/\delta = \text{l.c.m.}\ (b_1, ..., b_t)$. Every X_i can be written uniquely in the form $X_i = Y_j^{\delta} \cdot \langle h, h, ..., h\rangle$ for some j and h satisfying $0 \leqslant j < b$, $0 \leqslant h < \delta$. (Multiplication is taking place in $Q(A)$.) The subalgebra of $Q(A)$ generated by the Y_j^{δ}'s is isomorphic to $Q(B)$. The additional generator $Z = \langle 1, 1, ..., 1\rangle$ satisfies $Z^{\delta} = Y_l^{\delta}$ for some l, while every other relation involving Z is a consequence of this one. Hence $Q(A) \simeq Q(B)[Z]/(Z^{\delta} - Y_l)$, $Y_l \in Q(B)$. It follows that $Q(A)$ is a complete intersection if and only if $Q(B)$ is, so A is a CI-set if and only if B is a CI-set. This completes the proof that (i) $\Rightarrow$ (ii).

To prove that (ii) $\Rightarrow$ (i), we first require some lemmas.

5.2. LEMMA. *Suppose that the finitely generated graded k-algebra S is a complete intersection and that $S = T \oplus I$ (vector space direct sum), where T is a graded subalgebra and I is a homogeneous ideal of S. Then T is a complete intersection.*

Proof. Let the homogeneous elements $\Psi_1, ..., \Psi_r$ generate T as a k-algebra, and choose homogeneous $\Omega_1, ..., \Omega_s \in I$ so that the Ψ's and Ω's together generate S as a k-algebra. Thus $S = k[x_1, ..., x_r, y_1, ..., y_s]/J$, where $\bar{x}_i = \Psi_i$ and $\bar{y}_i = \Omega_i$ (an overhead bar denotes the image in S). Since S is a complete intersection, J is generated by a homogeneous regular sequence. We claim that we can choose this regular sequence to be of the form $\theta_1, ..., \theta_p, \eta_1, ..., \eta_q$, where $\theta_i \in k[x_1, ..., x_r]$ and $\eta_i \in (y_1, ..., y_s)$. For given any regular sequence $\omega_1, \omega_2, ..., \omega_m$, write $\omega_i = \omega_i' + \omega_i''$ where $\omega_i' \in k[x_1, ..., x_r]$ and $\omega_i'' \in (y_1, ..., y_s)$. Then $\overline{\omega_i'} \in T$ and $\overline{\omega_i''} \in I$, so $\omega_i' \in J$ and $\omega_i'' \in J$. Choose a basis for the k-vector space W generated by $\omega_1, ..., \omega_m$ consisting of various ω_i' and ω_j''. As is well known, any homogeneous basis for W is a homogeneous regular sequence, so we have found a regular sequence of the desired type. Since any nonzero polynomial in the η_i's involve y_j's, it is clear that $T = k[x_1, ..., x_r]/(\theta_1, ..., \theta_p)$. Hence T is a complete intersection. ∎

5.3. Corollary. *If A is a CI-set and $B \subset A$, then B is a CI-set.*

Proof. Consider $Q(A)$ as defined by (8) and (9). The subalgebra T generated by all $\langle \alpha_1, ..., \alpha_t \rangle$ satisfying $\alpha_i = 0$ if $\alpha_i \notin B$ is isomorphic to $Q(B)$, and the remaining $\langle \alpha_1, ..., \alpha_t \rangle$ form a k-basis of an ideal I. The proof now follows from Lemma 5.2. ∎

5.4. Lemma. *Let $A = \{a, b, c\}$ be an irreducible CI-set. Then $A' = \{(a, b)(a, c), (a, b)(b, c), (a, c)(b, c)\}$ is also an irreducible CI-set.*

Proof. It is clear that A' is irreducible. Let $[i, j]$ denote the least common multiple of i and j. Choose a set $\mathscr{G}$ of generators for $Q(A)$ (as a k-algebra), as described by (8) and (9), containing $Y_1 = X_{[a,b]}$, $Y_2 = X_{[a,c]}$, and $Y_3 = X_{[b,c]}$. Let a', b', c' be the least positive integers for which $Y_1^{c'} = Y_2^{b'} = Y_3^{a'} = 0$ in $Q(A)$. (Specifically, $c' = c/([a, b], c)$, etc., but this is irrelevant.) Since Y_1, Y_2, Y_3 have only one nonzero component (when written in the form (8)), and since no Y_i is a nontrivial power of any X_j, it follows that the relations $Y_1^{c'} = Y_2^{b'} = Y_3^{a'} = 0$ occur in some set $\mathscr{R}$ of minimal relations among the elements of $\mathscr{G}$. Since $Q(A)$ is an Artinian complete intersection, $|\mathscr{G}| = |\mathscr{R}|$. Now $Q(A') = Q(A)/(Y_1, Y_2, Y_3)$. It follows that $Q(A')$ is generated by $\mathscr{G}$ (or more precisely, the image of $\mathscr{G}$ in $Q(A')$), subject to the same relations $\mathscr{R}$ except that $Y_1^{c'} = Y_2^{b'} = Y_3^{a'} = 0$ are replaced with $Y_1 = Y_2 = Y_3 = 0$. If $\mathscr{R}'$ is this new set of relations, then $|\mathscr{G}| = |\mathscr{R}'|$, so $Q(A')$ is also a complete intersection. ∎

We now proceed to the proof that (ii) ⇒ (i) in Theorem 5.1. In view of our proof that every block of a partition π is a CI-set if and only if the same is true of an elementary reduction of π, it suffices to show that the only *irreducible* CI-set is the null set $\varnothing$. Suppose that $A = \{a_1, a_2, ..., a_t\}$ is a nonvoid irreducible CI-set with t minimal. Irreducibility implies $t \geqslant 3$. Corollary 4.3 and the minimality of t imply that every proper subset of A is completely reducible. In particular, any proper subset B of A can be partitioned into blocks δB_1, $\delta B_2, ..., \delta B_s$, where δ is a positive integer depending on B, and where every element of B_i is relatively prime to every element of B_j (denoted $(B_i, B_j) = 1$) for $i \neq j$. (Here $\delta C = \{\delta c \colon c \in C\}$.) We now will show that $t = 3$.

Case 1. For every maximal proper subset B of A, the elements of B have no common factor greater than one. In particular, this condition holds for $B = A - \{a_t\}$, so this B can be partitioned into blocks $B_1, B_2, \ldots, B_s$, $s \geqslant 2$, such that $(B_i, B_j) = 1$ for $i \neq j$, and such that s is maximal with respect to this property. Since B is completely reducible, each B_i is of the form $\delta_i B_i'$, $\delta_i > 1$. Now for any $i = 1, 2, \ldots, s$ we cannot have $(a_t, B_i) = 1$ since this would mean that $\{B_i, A - B_i\}$ is an elementary reduction of A. It follows that for $a \in B_1$, $\{B_1 - \{a\}, B_2 \cup \cdots \cup B_s \cup \{a_t\}\}$ is an elementary reduction of $A - \{a\}$. Hence if $|B_1| > 1$ then we would have $(a_t, B_1) = 1$, which cannot occur. Thus $|B_1| = 1$, and similarly $|B_i| = 1$. Since $(a_t, B_i) \neq 1$ for all i and since the elements of $B - \{a\}$ have no common factor greater than one, it follows that $A - \{a\}$ is irreducible, a contradiction. Hence Case 1 cannot occur.

Case 2. For some a_i, say a_t, the elements $a_1, a_2, \ldots, a_{t-1}$ of $A - \{a_t\}$ can be written in the form $\delta b_1, \ldots, \delta b_r$, $\delta c_1, \ldots, \delta c_s$ $(r + s = t - 1,\ r \geqslant 1,\ s \geqslant 1,\ \delta > 1)$, such that $(b_i, c_j) = 1$ for all i and j. Assume $r > 1$. The set $B = \{\delta b_1, \ldots, \delta b_{r-1}, \delta c_1, \ldots, \delta c_s, a_t\}$ is completely reducible. Since A is irreducible, $(a_t, \delta) = 1$. Then since $(b_i, c_j) = 1$ and $\delta > 1$, in order for B to be reducible we must have $(a_t, B - \{a_t\}) = 1$. Similarly if $B' = (B - \{\delta b_1\}) \cup \{\delta b_r\}$, then $(a_t, B' - \{a_t\}) = 1$. Hence $(a_t, A - \{a_t\}) = 1$, contradicting the irreducibility of A. Thus $r = 1$ and similarly $s = 1$, so $t = 3$ as was to be proved.

Therefore assume that $A = \{a, b, c\}$ is an irreducible CI-set. By Lemma 5.4, $A' = \{(a, b)(a, c), (a, b)(b, c), (a, c)(b, c)\}$ is also an irreducible CI-set. Since $(a, b, c) = 1$ because A is irreducible, A' can be written as $A' = \{\alpha\beta, \alpha\gamma, \beta\gamma\}$, where $(\alpha, \beta) = (\alpha, \gamma) = (\beta, \gamma) = 1$, and where at most one of α, β, γ is equal to one. We will now reach a contradiction by showing that A' is not a CI-set. A (minimal) set of generators for $Q(A')$ can be taken to be

$$X_1 = \langle 1, 1, 1 \rangle,$$

$$Y_1 = \langle 0, \beta_1\gamma, \gamma_1\beta \rangle, \ldots, Y_r = \langle 0, \beta_r\gamma, \gamma_r\beta \rangle,$$

$$Z_1 = \langle \alpha_1'\beta, \beta_1'\alpha, 0 \rangle, \ldots, Z_s = \langle \alpha_s'\beta, \beta_s'\alpha, 0 \rangle,$$

$$W_1 = \langle \alpha_1''\gamma, 0, \gamma_1''\alpha \rangle, \ldots, W_t = \langle \alpha_t''\gamma, 0, \gamma_t''\alpha \rangle,$$

where $r, s, t \geqslant 1$ and where $\beta_1 < \cdots < \beta_r$, $\gamma_1 > \cdots > \gamma_r$; $\alpha_1' < \cdots < \alpha_s'$, $\beta_1' > \cdots > \beta_s'$; $\alpha_1'' > \cdots > \alpha_t''$, $\gamma_1'' < \cdots < \gamma_t''$. We have relations among these generators of the form:

$$Y_i Z_j = X_1 \Phi_{ij}, \tag{a}$$

$$Y_i W_j = X_1 \psi_{ij}, \tag{b}$$

$$Z_i W_j = X_1 \Omega_{ij}; \tag{c}$$

$$Y_i^{a_i} = Z_i^{b_i} = W_i^{c_i} = 0. \tag{d}$$

These relations are easily seen to be independent. Types (a)–(c) have quadratic terms and are therefore minimal. The three relations of type (d) are minimal when we choose a_i, b_i, c_i to be minimal. Hence we have $1 + r + s + t$ generators with at least $rs + rt + st + r + s + t$ minimal relations. In order that $rs + rt + st + r + s + t \leqslant 1 + r + s + t$ we must have $rst = 0$, a contradiction. Hence $Q(A)$ has more relations than generators, so it cannot be a complete intersection. This completes the proof of Theorem 5.1. ∎

5.5. Corollary. *Let $G \subset GL(V)$ be an f.g.g.r., and let $H = G \cap SL(V)$. If $[G : H]$ is a power of a prime p, then R^H is a complete intersection.*

Proof. The set A contains only powers of p, and is therefore completely reducible. ∎

5.6. Corollary. *If in Corollary* 5.5 *$[G : H]$ is a prime p, then R^H is a hypersurface* (*i.e., there is only one relation among a minimal set of generators for R^H*).

Proof. We have $A = \{p\}$, and it is then obvious from (8) and (9) that $Q(A)$ has a single generator and is therefore a hypersurface. It is well known and easily seen that then R^H is also a hypersurface. ∎

Acknowledgment

I am grateful to B. Kostant and D. Eisenbud for their helpful comments regarding the proofs of Theorem 3.1 and Lemma 5.2, respectively.

References

1. N. Bourbaki, "Groupes et algèbres de Lie," Ch. 4, 5, et 6, Éléments de mathématique, XXXIV, Hermann, Paris, 1968.
2. W. Burnside, "Theory of Groups of Finite Order," 2nd ed., Dover, New York, 1955.
3. C. Chevalley, Invariants of finite groups generated by reflections, *Amer. J. Math.* 77 (1955), 778–782.
4. L. Flatto, Invariants of finite reflection groups, to appear.
5. M. Hochster and J. A. Eagon, Cohen–Macaulay rings, invariant theory, and the generic perfection of determinantal loci, *Amer. J. Math.* 93 (1971), 1020–1058.
6. T. Molien, Über die Invarianten der linearen Substitutionsgruppen, *Sitzungsber. König. Preuss. Akad. Wiss.* (1897), 1152–1156.
7. G. C. Shephard and J. A. Todd, Finite unitary reflection groups, *Canad. J. Math.* 6 (1954), 274–304.
8. N. J. A. Sloane, Error-correcting codes and invariant theory: New applications of a nineteenth-century technique, *Amer. Math. Monthly* 84 (1977), 82–107.
9. L. Solomon, Invariants of finite reflection groups, *Nagoya Math. J.* 22 (1963), 57–64.
10. L. Solomon, Invariants of Euclidean reflection groups, *Trans. Amer. Math. Soc.* 113 (1964), 274–286.

11. T. A. Springer, Regular elements of finite reflection groups, *Invent. Math.* **25** (1974), 159–198.
12. R. Stanley, Hilbert functions of graded algebras, *Advances in Math.*, to appear.
13. R. Steinberg, Invariants of finite reflection groups, *Canad. J. Math.* **12** (1960), 616–618.
14. K. Watanabe, Certain invariant subrings are Gorenstein, I, *Osaka J. Math.* **11** (1974), 1–8.
15. K. Watanabe, Certain invariant subrings are Gorenstein, II, *Osaka J. Math.* **11** (1974), 379–388.