BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 1, Number 3, May 1979

INVARIANTS OF FINITE GROUPS AND THEIR APPLICATIONS TO COMBINATORICS

BY RICHARD P. STANLEY[1]

CONTENTS

1. Introduction. The theory of invariants of finite groups forms an interesting and relatively self-contained nook in the imposing edifice of commutative algebra. Moreover, there are close connections between this subject and combinatorics, for two reasons: (a) the highly combinatorial tool of *generating functions* pervades the study of invariants of finite groups, and (b) several direct applications of invariants of finite groups have recently been given to combinatorics. Here we give an exposition of the theory of invariants of finite groups with emphasis on the connections with combinatorics, which assumes a minimal background in commutative algebra and combinatorics on the part of the reader. It is hoped that such an exposition will appeal to several types of readers. (a) Those who simply wish to see a self-contained treatment of an elegant and fascinating subject. This might include coding theorists, physicists, and others who are beginning to use invariant theory as a tool in their own work. (b) Those who are interested in learning something about the revolutionary developments in present-day combinatorics. Until recently combinatorics has been regarded as a disparate collection of *ad hoc* tricks, but this picture is slowly changing under a determined effort to unify various branches of combinatorics and to understand their relationship with other branches of mathematics. (c) Finally, those who would like a relatively painless glimpse of certain topics of current interest in commutative algebra, such as the theory of Cohen-Macaulay rings and Gorenstein rings. For a really adequate understanding of these concepts it would be necessary to work in far greater generality and to introduce sophisticated machinery from

Received by the editors September 1, 1978.

AMS (*MOS*) *subject classifications* (1970). Primary 05-02, 13-02, 20-02, 05A15, 13H10, 20C99.

[1] Partially supported by NSF Grant MPS 7308445-A03.

homological algebra. Thus, while our mundane treatment should not be construed as an "introduction to contemporary commutative algebra," it should make certain interesting and useful aspects of commutative algebra accessible to a wide audience.

The paper is divided into ten sections. §1 contains the basic definitions and classical results about the ring R^G of invariants of a finite group G acting on the polynomial ring $R = \mathbf{C}[x_1, \ldots, x_m]$. §2 is devoted to Molien's theorem, which gives a simple expression for the dimension of the vector space R_n^G of forms of degree n left invariant by G. A common theme throughout this paper consists of reading off information about G and R^G from the numbers $\dim_{\mathbf{C}} R_n^G$ (or more precisely, from the generating function $F_G(\lambda) = \Sigma(\dim_{\mathbf{C}} R_n^G)\lambda^n$). In §3 we leave the classical theory and show that the elements of R^G can be written in a certain explicit canonical form. The existence of such a canonical representation is equivalent to the statement that R^G is a Cohen-Macaulay ring. §4 is devoted to groups G for which R^G is generated by algebraically independent polynomials, the "groups generated by pseudo-reflections." Many of the remarkable properties of these groups are obtained by an appeal to Molien's theorem. Such combinatorial objects as the marriage theorem, the fundamental theorem of symmetric functions, the Stirling numbers of the first kind, and standard Young tableaux make a brief appearance. In §5 we present three applications to combinatorial problems which *a priori* seem to have no connection with invariant theory. These problems concern (a) the evaluation of certain sums involving roots of unity, (b) the "weight enumerator" of a self-dual code over GF(2), and (c) the theory of "multipartite partitions" or "vector partitions." The next four sections are devoted to the homological aspects of the invariant theory of finite groups. The basic object of study is the minimal free resolution of R^G (as a module over some polynomial ring). We discuss what it means in terms of the minimal free resolution for R^G to be Cohen-Macaulay, Gorenstein, or a complete intersection, and the connection between these properties, the internal structure of R^G, the structure of G, and the generating function $F_G(\lambda)$. Proofs for the most part are omitted. Included are discussions of such recent results as the characterization of Gorenstein R^G solely in terms of $F_G(\lambda)$, and the determination of the canonical module $\Omega(R^G)$. Finally in §10 we consider the class of monomial groups and use our general theory to derive the famous Pólya enumeration theorem for groups acting on the domain of a set of functions.

The following notation is fixed throughout:

$\mathbf{N}$ nonnegative integers,
$\mathbf{P}$ positive integers,
$\mathbf{C}$ complex numbers,
$[n]$ the set $\{1, 2, \ldots, n\}$ where $n \in \mathbf{P}$,
$T \subset S$ T is a subset of S, allowing $T = \varnothing$ or $T = S$,
$V \oplus W$ direct sum of the vector spaces V and W,
$\amalg_i V_i$ direct sum of the vector spaces V_i,
$\langle y_1, \ldots, y_j \rangle$ the vector space spanned by $y_1, \ldots, y_j$.

Also throughout this paper V denotes an m-dimensional vector space over the complex numbers $\mathbf{C}$, and $x_1, \ldots, x_m$ denotes a basis for V. Let GL(V)

denote the group of all invertible linear transformations $M\colon V \to V$. Once we fix the basis $x_1, \ldots, x_m$ we may identify $\mathrm{GL}(V)$ with the multiplicative group of all nonsingular $m \times m$ matrices with entries in $\mathbf{C}$. Let R be the algebra of polynomials in the variables $x_1, \ldots, x_m$ with coefficients in $\mathbf{C}$, i.e., $R = \mathbf{C}[x_1, x_2, \ldots, x_m]$. Thus the vector space of linear forms in R is just V. The action of $M \in \mathrm{GL}(V)$ on V extends uniquely to an algebra automorphism of R, viz., if $\mathbf{x}$ denotes the column vector

$$\begin{bmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_m \end{bmatrix}$$

and $f \in R$, then $(Mf)(\mathrm{x}) = f(M\mathrm{x})$. For instance, if

$$M = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \quad \text{and} \quad f(x_1, x_2) = x_1^2 - x_2^2,$$

then

$$Mf(x_1, x_2) = \left[\frac{1}{\sqrt{2}}(x_1 + x_2)\right]^2 - \left[\frac{1}{\sqrt{2}}(-x_1 + x_2)\right]^2 = x_1^2 + 2x_1x_2.$$

Many questions in combinatorial theory and other fields can be reduced to the problem of finding all polynomials $f \in R$ satisfying $Mf = f$ for all M in some finite subgroup $G \subset \mathrm{GL}(V)$. Such a polynomial f is called an *absolute invariant*, or simply an *invariant*, of G. Clearly, the invariants of G form a subalgebra of R, which we denote by R^G and call the *algebra of invariants* of G. Thus,

$$R^G = \{f \in R\colon Mf = f \text{ for all } M \in G\}.$$

More generally, let $X = X(G)$ be the set of irreducible (complex) characters of G. (The number of such characters is equal to the number of conjugacy classes in G.) The action of G on R can be decomposed into a direct sum of irreducible representations, i.e., $R = \amalg T$, where each T is a G-invariant subspace of R on which G acts irreducibly. If $\chi \in X$, then let R_χ^G denote the direct sum of those T's which correspond to the character χ. R_χ^G is called an *isotypical* (or *isotypic*) component of the action of G on R. Although the T's are not uniquely determined, the isotypical components R_χ^G are unique. Clearly $R = \amalg_{\chi \in X} R_\chi^G$. In particular, $R^G = R_\varepsilon^G$, where ε denotes the trivial character. If T is an irreducible component and $f \in R$, then the map $T \to fT$ given by multiplication by f is clearly a G-module isomorphism. From this it follows that $R^G \cdot R_\chi^G \subset R_\chi^G$, i.e., R_χ^G is an R^G-module.

In the special case where χ is linear (i.e., χ is a homomorphism $G \to \mathbf{C} - \{0\}$), then the condition $f \in R_\chi^G$ is equivalent to $M(f) = \chi(M)f$ for all $M \in G$. A polynomial $f \in R_\chi^G$ for χ linear is called a *relative invariant*, *semi-invariant*, or *χ-invariant*. We shall extend this terminology to *any* irreducible character χ. Thus $f \in R$ is a χ-invariant if $f \in R_\chi^G$, for any $\chi \in X(G)$. Although we will be primarily interested in absolute invariants (i.e., $f \in R^G$), we will indicate to what extent the theory extends to χ-invariants.

The fundamental problem of the invariant theory of finite groups is to "determine" or "characterize" the algebra R^G of invariants. A survey of the classical approach to this subject may be found in [**Bu**, Chapter XVII]. More recent work will be quoted in the course of this paper. We also mention the survey article by Sloane [**Sl**]. There is considerable overlap between parts of this paper and of Sloane's. However, Sloane's emphasis is on applications to coding theory while we have a broader point of view. We now quote without proof two of the principal classical results concerning invariants of finite groups. For this purpose define the *degree* of $G \subset \mathrm{GL}(V)$ to be $m = \dim V$ and the *order* g of G to be the number $|G|$ of elements of G.

1.1 THEOREM. *If G has degree m, then there exist m, but not $m + 1$, algebraically independent invariants* (*over* $\mathbf{C}$). *Equivalently, R^G has Krull dimension m.* □

1.2 THEOREM. *Let G have order g and degree m. Then R^G is generated as an algebra over* $\mathbf{C}$ *by not more than $\binom{g+m}{m}$ homogeneous invariants, of degree not exceeding g.* □

A proof of Theorem 1.1 may be found in [**Bu**, §262]. It follows from the work of Hilbert that R^G is finitely generated, but the more precise Theorem 1.2 is due to Noether (see [**We**, pp. 275–276]). Noether in fact showed that R^G is generated by the $\binom{g+m}{m}$ polynomials $(1/g)\Sigma_{M \in G} Mf$, as f ranges over all $\binom{g+m}{m}$ monomials in the variables $x_1, \ldots, x_m$ of degree at most g.

For many purposes Noether's result gives a satisfactory answer to the problem of determining R^G. We can ask, however, for more precise information, viz., a complete description or enumeration, without repetitions, of all the invariants. There are two possible approaches to this problem: (a) find a canonical form for the elements of R^G, or (b) determine all the relationships among the generators of R^G. We shall discuss both of these approaches toward describing R^G.

We conclude this section by supplementing Theorems 1.1 and 1.2 with a related result which is easily proved by classical techniques, though an explicit statement is difficult to find in the literature.

1.3 THEOREM. *Let $\chi \in X(G)$. Then R_χ^G is a finitely-generated R^G-module. In fact, R_χ^G is generated by homogeneous polynomials of degree not exceeding g.* □

2. Molien's theorem. To enumerate all the invariants explicitly, it is convenient and natural to classify invariants by their *degrees* (as polynomials). More precisely, if k is a field then we define an $\mathbf{N}$-*graded k-algebra* to be a finitely generated k-algebra B (always assumed to be associative, commutative, and with identity), together with a vector space direct sum decomposition

$$B = B_0 \oplus B_1 \oplus B_2 \oplus \cdots,$$

such that $B_0 = k$ and$B_i B_j \subset B_{i+j}$. We call B_n the *nth homogeneous part* of B, and an element $f \in B_n$ is said to be *homogeneous of degree n*, denoted $\deg f = n$. Now note that the polynomial ring $R = \mathbf{C}[x_1, \ldots, x_m]$ has a familiar grading $R = R_0 \oplus R_1 \oplus R_2 \oplus \cdots$, where R_n consists of all homogeneous polynomials of degree n, in the usual sense. If $f \in R_n$ then $Mf \in R_n$ for all $M \in \mathrm{GL}(V)$. It follows that for any subgroup $G \subset \mathrm{GL}(V)$, R^G has the structure $R^G = R_0^G \oplus R_1^G \oplus \cdots$ of an $\mathbf{N}$-graded $\mathbf{C}$-algebra given by $R_n^G = R^G \cap R_n$. Hence to determine R^G it suffices to determine each R_n^G.

More generally, if B is an $\mathbf{N}$-graded k-algebra, then define a *$\mathbf{Z}$-graded B-module* to be a finitely-generated B-module Λ, together with a vector space direct sum decomposition

$$\Lambda = \coprod_{i \in \mathbf{Z}} \Lambda_i,$$

such that $B_i \Lambda_j \subset \Lambda_{i+j}$. The assumption that Λ is finitely-generated guarantees that $\Lambda = \coprod_{i \geqslant i_0} \Lambda_i$ for some $i_0 \in \mathbf{Z}$. If we set $(R_\chi^G)_n = R_\chi^G \cap R_n$, then this gives R_χ^G the structure of a $\mathbf{Z}$-graded R^G-module.

If $\Lambda = \coprod_{n \in \mathbf{Z}} \Lambda_n$ is a $\mathbf{Z}$-graded module over the $\mathbf{N}$-graded k-algebra B, then it follows that $\dim_k \Lambda_n < \infty$ since B is finitely-generated as an algebra and Λ is finitely-generated as a B-module. The *Hilbert function* $H(\Lambda, \cdot)\colon \mathbf{Z} \to \mathbf{N}$ of Λ is defined by $H(\Lambda, n) = \dim_k \Lambda_n$, and the *Hilbert series* (sometimes called the *Poincaré series*) of Λ is the formal Laurent series

$$F(\Lambda, \lambda) = \sum_{n \in \mathbf{Z}} H(\Lambda, n)\lambda^n.$$

A theorem of Hilbert, embellished by Serre, implies that $F(\Lambda, \lambda)$ is a rational function of λ. See, e.g., [**A-M**, Theorem 11.1] or [**Sm**] for further details.

When $\Lambda = R_\chi^G$ we call $\chi(1)^{-1}F(R_\chi^G, \lambda)$ the *Molien series* of the pair (G, χ) and write $F_{G,\chi}(\lambda) = \chi(1)^{-1}F(R_\chi^G, \lambda)$. When χ is trivial we call $F(R^G, \lambda)$ the *Molien series of* G and write $F_G(\lambda) = F(R^G, \lambda)$. Note that $\chi(1)$ is just the degree of the irreducible representation of G afforded by χ. Hence the coefficient of λ^n in $F_{G,\chi}(\lambda)$ is equal to the multiplicity of the character χ in the action of G on R_n. Clearly we have

$$\sum_{\chi \in X(G)} \chi(1) F_{G,\chi}(\lambda) = (1 - \lambda)^{-m}.$$

It is very helpful in analyzing R_χ^G to know the Hilbert function $H(R_\chi^G, n)$, since then we can check whether a tentative listing of invariants is complete. Often, moreover, one is only interested in the Hilbert function $H(R_\chi^G, n)$ itself, and not in the actual elements of $(R_\chi^G)_n$. A classical theorem of Molien [**Mo**], [**Bu**, §227], [**Bo**, p. 110], [**Sl**, Theorem 1] gives an explicit expression for the rational function $F_{G,\chi}(\lambda)$ and thereby ties together invariant theory with generating functions.

2.1 THEOREM. *Let G be a finite subgroup of* GL(V) *of order g, and let $\chi \in X(G)$. Then the Molien series $F_{G,\chi}(\lambda)$ is given by*

$$F_{G,\chi}(\lambda) = \frac{1}{g} \sum_{M \in G} \frac{\bar{\chi}(M)}{\det(I - \lambda M)}, \tag{1}$$

where I denotes the identity transformation and $\bar{\chi}$ is the complex conjugate character to χ.

PROOF. Let W be any finite-dimensional vector space over $\mathbf{C}$, and let H be a finite subgroup of $\mathrm{GL}(W)$ of order h. Let W_χ^H denote the isotypical component afforded by χ. Thus $\chi(1)^{-1}\dim_{\mathbf{C}} W_\chi^H$ is just the multiplicity of χ in the action of H on W. From the rudiments of the representation theory of finite groups we conclude

$$\chi(1)^{-1}\dim_{\mathbf{C}} W_\chi^H = \frac{1}{h}\sum_{M\in H}\bar{\chi}(M)(\operatorname{tr} M), \tag{2}$$

where tr denotes trace.

Now given $M \in G \subset \mathrm{GL}(V)$, let $\rho_1, \ldots, \rho_m$ be its eigenvalues. Since M has finite multiplicative order it follows that there exist m linearly independent eigenvectors $y_1, \ldots, y_m$ belonging to $\rho_1, \ldots, \rho_m$, respectively. Consider the action of G on R_n, the nth homogeneous part of R. The $\binom{n+m-1}{n}$ distinct monomials $y_1^{a_1} \ldots y_m^{a_m}$ of degree n are eigenvectors for M (acting on R_n) with corresponding eigenvalues $\rho_1^{a_1} \ldots \rho_m^{a_m}$. Hence for this action of M we have

$$\operatorname{tr} M = \sum_{a_1+\cdots+a_m=n} \rho_1^{a_1} \ldots \rho_m^{a_m}.$$

Therefore by (2),

$$\chi(1)^{-1}H(R^G, n) = \frac{1}{g}\sum_{M\in G}\bar{\chi}(M)\sum_{a_1+\cdots+a_m=n}\rho_1^{a_1}\ldots\rho_m^{a_m}, \tag{3}$$

where $\rho_1, \ldots, \rho_m$ are the eigenvalues of M acting on V. Since $1/\det(I - \lambda M) = 1/\Pi(1 - \rho_1\lambda) \ldots (1 - \rho_m\lambda)$, the right-hand of (3) is just the coefficient of λ^n in

$$\frac{1}{g}\chi(1)^{-1}\sum_{M\in G}\bar{\chi}(M)/\det(I - \lambda M),$$

and the proof follows. □

Molien's theorem breaks down over fields in which $g = 0$. In fact, the entire theory of invariants of finite groups becomes much more complicated and much less understood in characteristic p. For an inkling of the problems which can arise, see [A-F].

2.2 EXAMPLE. As a simple first application of Molien's theorem, we prove the nonobvious result that each $R_\chi^G \neq \varnothing$. In the expression (1) for $F_{G,\chi}(\lambda)$, exactly one term (corresponding to $M = I$) has a pole of order m at $\lambda = 1$, while the other terms have a pole of order $< m$. Hence $F_{G,\chi}(\lambda) \neq 0$, so $R_\chi^G \neq \varnothing$.

2.3 EXAMPLE. Let $G = \{I, M, M^2, M^3\}$, where $M = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$. The Molien series of G is given by

$$\begin{aligned} F_G(\lambda) &= \frac{1}{4}\left[\frac{1}{(1-\lambda)^2} + \frac{2}{1+\lambda^2} + \frac{1}{(1+\lambda)^2}\right] \\ &= (1+\lambda^4)/(1-\lambda^2)(1-\lambda^4). \end{aligned} \tag{4}$$

The form of this Molien series suggests that there may be invariants $\theta_1 \in R_2^G$, $\theta_2 \in R_4^G$, $\eta \in R_4^G$, such that every invariant $f \in R^G$ can be written uniquely in the form $p(\theta_1, \theta_2) + \eta \cdot q(\theta_1, \theta_2)$, where p and q belong to

$\mathbf{C}[x_1, x_2]$. More succinctly, we could write this condition as

$$R^G = \mathbf{C}[\theta_1, \theta_2] \oplus \eta \cdot \mathbf{C}[\theta_1, \theta_2] = \mathbf{C}[\theta_1, \theta_2](1 \oplus \eta) \tag{5}$$

the sum $\oplus$ being a vector space direct sum (or a $\mathbf{C}[\theta_1, \theta_2]$-module direct sum). Using (4), it is in fact not difficult to show that (5) holds for $\theta_1 = x_1^2 + x_2^2$, $\theta_2 = x_1^2x_2^2$, $\eta = x_1^3x_2 - x_1x_2^3$.

The preceding example raises many theoretical questions. Consider R^G for any finite subgroup G of $\mathrm{GL}(V)$. Suppose we can find algebraically independent homogeneous invariants $\theta_1, \theta_2, \ldots, \theta_m$ of degrees $d_1, d_2, \ldots, d_m$, respectively (i.e., $\theta_i \in R_{d_i}^G$), and a set $\eta_1, \eta_2, \ldots, \eta_t$ of homogeneous invariants of degrees $e_1, e_2, \ldots, e_t$, respectively (i.e., $\eta_i \in R_{e_i}^G$), such that if $S = \mathbf{C}[\theta_1, \theta_2, \ldots, \theta_m]$, then $R^G = \eta_1 S \oplus \eta_2 S \oplus \cdots \oplus \eta_t S$. It is then clear from the definition of $F_G(\lambda)$ that

$$F_G(\lambda) = \left(\sum_{i=1}^{t} \lambda^{e_i}\right) \Big/ \prod_{j=1}^{m} (1 - \lambda^{d_j}). \tag{4}$$

Mallows and Sloane **[M-S]** conjectured that the converse statement is true, i.e., if $F_G(\lambda)$ can be written in the form (6), then we can always find the appropriate invariants η_i and θ_j. This conjecture, however, is false, as pointed out in **[Sl**, p. 101] and **[Sta$_2$**, Ex. 3.8]. For instance, let G be the group generated by $\mathrm{diag}(-1, -1, 1)$ and $\mathrm{diag}(1, 1, i)$, where $i^2 = -1$. Thus G is abelian of order 8, and we have $F_G(\lambda) = 1/(1 - \lambda^2)^3$. However, $R^G = \mathbf{C}[x_1^2, x_2^2, x_3^4](1 \oplus x_1x_2)$, which cannot be expressed in the form $\mathbf{C}[\theta_1, \theta_2, \theta_3]$, $\theta_i \in R_2^G$.

The question then arises as to whether there is *some* way of writing $F_G(\lambda)$ in the form (6) such that

$$R^G = \coprod_{i=1}^{t} \eta_i \mathbf{C}[\theta_1, \ldots, \theta_m],$$

where $\theta_j \in R_{d_j}^G$, $\eta_i \in R_{e_i}^G$, and the θ_j's are algebraically independent over $\mathbf{C}$. In other words, do there exist m algebraically independent homogeneous elements $\theta_1, \ldots, \theta_m \in R^G$ such that R^G is a finitely-generated *free* $\mathbf{C}[\theta_1, \ldots, \theta_m]$-module? This question immediately leads to the subject of Cohen-Macaulay rings.

3. Cohen-Macaulay rings. Let $B = B_0 \oplus B_1 \oplus \cdots$ be an $\mathbf{N}$-graded k-algebra, as defined in the previous section. We denote by $\dim B$ the *Krull dimension* of B, i.e., the maximum number of elements of B which are algebraically independent over k. Equivalently, $\dim B$ is the order to which $\lambda = 1$ is a pole of the rational function $F(B, \lambda)$ **[Sm**, Theorem 5.5]. If $m = \dim B$, then a set $\theta_1, \ldots, \theta_m$ of m homogeneous elements of positive degree is said to be a *homogeneous system of parameters* (h.s.o.p.) if B is a finitely-generated module over the subalgebra $k[\theta_1, \ldots, \theta_m]$. This implies that $\theta_1, \ldots, \theta_m$ are algebraically independent. It is easy to see that $\theta_1, \ldots, \theta_m$ is an h.s.o.p. if and only if the quotient algebra $B/(\theta_1, \ldots, \theta_m)$ is a finite dimensional vector space over k. A basic result of commutative algebra, known as the *Noether normalization lemma*, implies that an h.s.o.p. for B always exists (e.g., **[A-M**, p. 69], **[Z-S**, Theorem 25, p. 200]). We now come to another standard result of commutative algebra.

3.1 Proposition. *Let B be as above, and let $\theta_1, \ldots, \theta_m$ be an h.s.o.p. for B. The following two conditions are equivalent.*

(i) *B is a free module (necessarily finitely generated) over $k[\theta_1, \ldots, \theta_m]$. In other words, there exist $\eta_1, \ldots, \eta_t \in B$ (which may be chosen to be homogeneous) such that*

$$B = \coprod_{i=1}^{t} \eta_i k[\theta_1, \ldots, \theta_m]. \tag{7}$$

(ii) *For every h.s.o.p. $\psi_1, \ldots, \psi_m$ of B, B is a free $k[\psi_1, \ldots, \psi_m]$-module.*

If condition (i) (*and therefore* (ii)) *holds, then the elements $\eta_1, \ldots, \eta_t$ of B satisfy* (7) *if and only if their images in $B/(\theta_1, \ldots, \theta_m)$ form a vector space basis for $B/(\theta_1, \ldots, \theta_m)$.* □

A proof that (i) and (ii) are equivalent can be found, e.g., in [**Se**$_2$, Theorem 2, p. IV–20] (using somewhat different terminology). The latter part of the above proposition is an easy consequence of (i). An $\mathbf{N}$-graded k-algebra B satisfying (i) and (ii) above is said to be a *Cohen-Macaulay* algebra. Hence the question raised at the end of the previous section can be rephrased: Is R^G Cohen-Macaulay for finite $G \subset \mathrm{GL}(V)$? The first explicit answer to this question appeared in [**H-E**, Proposition 13], although it was apparently part of the folklore of commutative algebra before [**H-E**] appeared.

3.2 Theorem. *For any finite $G \subset \mathrm{GL}(V)$, R^G is a Cohen-Macaulay algebra.*

Proof. We first claim that we can write $R = R^G \oplus U$, where U is an R^G-module. If $f \in R$ let $\phi(f) = (1/g)\Sigma_{M \in G} Mf$. ($\phi$ is the so-called *Reynolds operator*.) Now $\phi^2 = \phi$, and it follows that we can take $U = \{f \in R\colon \phi f = 0\} = \{f - \phi f\colon f \in R\}$.

We next claim that R is a finitely-generated R^G-module. This claim is equivalent to the classical result that R is *integral* over R^G, i.e., every element of R satisfies a monic polynomial with coefficients in R^G. (For the equivalence of finite generation to integrality, see, e.g., [**A-M**, Chapter 5].) For the sake of completeness we give the standard proof that R is integral over R^G. Let $f \in R$, and consider the polynomial $P_f(t) = \Pi_{M \in G}(t - M(f))$. The coefficients of $P_f(t)$ are symmetric functions of the $M(f)$'s, so elements of R^G. Moreover $P_f(t)$ is monic, and $P_f(f) = 0$ since $t - f$ is a factor of $P_f(t)$. Hence f is integral over R^G, as desired.

Now let $\theta_1, \ldots, \theta_m$ be an h.s.o.p. for R^G (existence guaranteed by the Noether normalization lemma). Since R^G is finite over $\mathbf{C}[\theta_1, \ldots, \theta_m]$ and R is finite over R^G, it follows that R is finite over $\mathbf{C}[\theta_1, \ldots, \theta_m]$, so $\theta_1, \ldots, \theta_m$ is an h.s.o.p. for R. Since $x_1, \ldots, x_m$ is also an h.s.o.p. for R and R is clearly a free $\mathbf{C}[x_1, \ldots, x_m]$-module, it follows from Proposition 3.1 that R is a free $\mathbf{C}[\theta_1, \ldots, \theta_m]$-module. Moreover, it follows from the decomposition $R = R^G \oplus U$ that $R/(\theta_1, \ldots, \theta_m) = R^G/(\theta_1, \ldots, \theta_m) \oplus U/(\theta_1 U + \cdots + \theta_m U)$. Choose a homogeneous $\mathbf{C}$-basis $\bar{\eta}_1, \ldots, \bar{\eta}_s$ for $R/(\theta_1, \ldots, \theta_m)$ such that $\bar{\eta}_1, \ldots, \bar{\eta}_t$ is a $\mathbf{C}$-basis for $R^G/(\theta_1, \ldots, \theta_m)$ and $\bar{\eta}_{t+1}, \ldots, \bar{\eta}_s$ is a $\mathbf{C}$-basis for $U/(\theta_1 U + \cdots + \theta_m U)$. Lift $\bar{\eta}_i$ to a homogeneous element η_i of R^G if $1 \leqslant i \leqslant t$ and to a homogeneous element η_i of U if $t + 1 \leqslant i \leqslant s$. By

Proposition 3.1 we have $R = \amalg_1^s \eta_i \mathbf{C}[\theta_1, \ldots, \theta_m]$, so $R^G = \amalg_1^t \eta_i \mathbf{C}[\theta_1, \ldots, \theta_m]$. Hence R^G is a free $\mathbf{C}[\theta_1, \ldots, \theta_m]$-module, so R^G is Cohen-Macaulay. □

We now wish to give an explicit description of a certain h.s.o.p. $\psi_1, \ldots, \psi_m$ for R^G. We will in fact show directly that R is a free $\mathbf{C}[\psi_1, \ldots, \psi_m]$-module, so it will follow from the proof of Theorem 3.2 (circumventing the use of Proposition 3.1) that R^G is a free $\mathbf{C}[\psi_1, \ldots, \psi_m]$-module. We will require the following result from commutative algebra [**H-E**, p. 1036], [**Sm**, Proposition 6.8]. Since a direct, elementary proof is lacking in the literature, we include such a proof here.

3.3 Lemma. *Let B be an $\mathbf{N}$-graded k-algebra of Krull dimension m, and let $\theta_1, \ldots, \theta_j$ be algebraically independent homogeneous elements of B of positive degree. Set $C = k[\theta_1, \ldots, \theta_j]$. Then B is a free C-module if and only if θ_{i+1} is not a zero-divisor in $B/(\theta_1, \ldots, \theta_i)$ for $0 \leqslant i \leqslant j - 1$. Moreover, given that B is a free C-module, then B is finitely-generated as a C-module if $j = m$.*

Proof. Induction on j. First assume $j = 1$, and let $\theta = \theta_1$. Let W be a vector space complement in B of the ideal θB. The statement that θ is not a zero-divisor in B is equivalent to saying $B = W + \theta W + \theta^2 W + \cdots$, i.e., B is a free $k[\theta]$-module (with basis consisting of a k-basis for W). Now assume the lemma for $j = l - 1$. It is clear that B is a free $k[\theta_1, \ldots, \theta_l]$-module if and only if B is a free $k[\theta_1, \ldots, \theta_{l-1}]$-module and $B/(\theta_1, \ldots, \theta_{l-1})$ is a free $k[\theta_l]$-module. By the induction hypothesis (including the case $j = 1$), the first assertion of the lemma follows.

Now suppose $j = m$ and let Y be a (graded) vector space complement in B to the ideal $(\theta_1, \ldots, \theta_m)$. Hence $B = \amalg_u Yu$, where u ranges over all monomials in $\theta_1, \ldots, \theta_m$. We want to show $\dim_k Y < \infty$. Linearly independent elements of Y remain linearly independent in $D = B/(\theta_1, \ldots, \theta_m)$. If $\dim_k Y = \infty$, then D contains a homogeneous element f of positive degree which isn't nilpotent. Thus the elements $f^i u$ are linearly independent in B for all $i \geqslant 0$ and all monomials u in $\theta_1, \ldots, \theta_m$, so $\theta_1, \ldots, \theta_m, f$ are algebraically independent. This contradicts the definition of m as the largest number of algebraically independent elements of B. □

Now choose linear forms $f_1, \ldots, f_m \in V$ as follows. Pick $f_1 \neq 0$. Once $f_1, \ldots, f_i$ have been chosen, pick f_{i+1} not to be in any of the i-dimensional subspaces $\langle M_1 f_1, \ldots, M_i f_i \rangle$ of V, where $M_1, \ldots, M_i \in G$. (Such a choice is always possible since V is not a set-theoretic union of finitely many proper subspaces.) Let $f_{i1}, \ldots, f_{ia_i}$ be the *distinct* images of f_i under G. (Hence if H_i is the subgroup of G fixing f_i, then $a_i = |G|/|H_i|$.) Define $\psi_i = f_{i_1} f_{i_2} \cdots f_{ia_i}$. Clearly $\psi_i \in R^G$.

3.4 Proposition. *R (and hence R^G) is a finitely-generated free $\mathbf{C}[\psi_1, \ldots, \psi_m]$-module.*

Proof (based on a letter from E. Dade to N. Sloane and on a conversation with N. Sloane). By Lemma 3.3, it suffices to prove that ψ_{i+1} is not a zero-divisor in $R/(\psi_1, \ldots, \psi_i)$. In other words, if

$$Y\psi_{i+1} = \sum_{j=1}^{i} Z_j\psi_j,$$

where $Y, Z_j \in R$, then $Y \in (\psi_1, \ldots, \psi_i)$. Now the right-hand side of the above equality belongs to the prime ideal $\mathfrak{p} = (f_{1c_1}, \ldots, f_{ic_i})$ of R for any $(c_1, \ldots, c_i)$, so therefore some factor on the left-hand side does. But by definition we have $f_{i+1,j} \in \mathfrak{p}$, so $\psi_{i+1} \notin \mathfrak{p}$. Hence $Y \in (f_{1c_1}, \ldots, f_{ic_i})$ for every $(c_1, \ldots, c_i)$, so $Y \in \bigcap (f_{1c_1}, \ldots, f_{ic_i}) = (\psi_1, \ldots, \psi_i)$. □

Proposition 3.4 shows that there exists an h.s.o.p. $\psi_1, \ldots, \psi_m$ for R^G such that deg ψ_i divides g for all i. By raising the ψ_i's to appropriate powers we get an h.s.o.p. for R^G whose elements all have degree g. Hence we can always write $F_G(\lambda)$ in the form $P_G(\lambda)/(1 - \lambda^g)^m$, where $P_G(\lambda)$ is a polynomial with nonnegative coefficients.

An interesting open problem is to determine the least possible degrees of the elements of an h.s.o.p. for R^G, in terms of the structure of G. For instance, if the elements of G (regarded as matrices) all have real entries, then there exists an h.s.o.p. $\theta_1, \ldots, \theta_m$ with deg $\theta_1 = 2$. This follows from the fact that G is equivalent to an orthogonal representation and therefore after a suitable change of basis fixes the form $x_1^2 + \cdots + x_m^2$. (In the complex case we get the invariant $x_1\bar{x}_1 + \cdots + x_m\bar{x}_m$, but this is not a *polynomial* invariant.) Conversely, if G is irreducible and has a nonzero invariant of degree 2, then G is equivalent to a real orthogonal representation [**Sp$_2$**, Lemma 4.2.15].

3.5 Example. Let $G = \{1, M, M^2\}$, where $M = \text{diag}(\omega, \omega^{-1})$, $\omega = e^{2\pi i/3}$. Then x_1^3, x_2^3 is an h.s.o.p. for R^G, corresponding to the decomposition $R^G = \mathbf{C}[x_1^3, x_2^3](1 \oplus x_1x_2 \oplus x_1^2x_2^2)$. Also $x_1x_2, x_1^3 + x_2^3$ is an h.s.o.p., corresponding to $R^G = \mathbf{C}[x_1x_2, x_1^3 + x_2^3](1 \oplus x_1^3)$. Hence

$$F_G(\lambda) = \frac{1 + \lambda^2 + \lambda^4}{(1 - \lambda^3)^2} = \frac{1 + \lambda^3}{(1 - \lambda^2)(1 - \lambda^3)}.$$

The greatest common divisor of $(1 - \lambda^3)^2$ and $(1 - \lambda^2)(1 - \lambda^3)$ is $(1 - \lambda) \cdot (1 - \lambda^3)$, so $F_G(\lambda)$ can be written with this denominator, viz., $F_G(\lambda) = (1 - \lambda + \lambda^2)/(1 - \lambda)(1 - \lambda^3)$. In this form the coefficients of the numerator and the factors of the denominator have no direct algebraic significance.

3.6 Example. Let us illustrate Proposition 3.4 with the cyclic group G of order 4 acting on $V = \langle x_1, x_2, x_3, x_4\rangle$ by $x_1 \to x_2 \to x_3 \to x_4 \to x_1$. Choose $f_1 = x_1 + x_2 + x_3 + x_4$, $f_2 = x_1 + x_3$, $f_3 = x_1 - x_3$, $f_4 = x_1 + x_2$. We get $\psi_1 = x_1 + x_2 + x_3 + x_4$, $\psi_2 = (x_1 + x_3)(x_2 + x_4)$, $\psi_3 = (x_1 - x_3)^2(x_2 - x_4)^2$, $\psi_4 = (x_1 + x_2)(x_2 + x_3)(x_3 + x_4)(x_1 + x_4)$. We cannot replace ψ_3 by $(x_1 - x_3)(x_2 - x_4)$ since this element is not an invariant. We cannot replace f_4 by x_1, since $x_1 \in \langle f_2, f_3\rangle$.

Proposition 3.4 yields information about the possible values of $d_i = \deg \theta_i$ in a decomposition $R^G = \coprod_1^t \eta_i \mathbf{C}[\theta_1, \ldots, \theta_m]$. What can be said about the numbers $e_i = \deg \eta_i$? Assume the η_i's are labeled so that $0 = e_1 \leqslant e_2 \leqslant \cdots \leqslant e_t$. We will confine ourselves here to a determination of e_t.

3.7 Lemma. *Let σ be the linear character of G given by $\sigma(M) = (\det M)^{-1}$. Then as rational functions we have*

$$F_G(1/\lambda) = (-1)^m \lambda^m F_{G,\sigma}(\lambda).$$

PROOF. By Molien's theorem, we have

$$\begin{aligned} F_G(1/\lambda) &= \frac{1}{g} \sum_{M \in G} \frac{1}{\det(I - \lambda^{-1} M)} \\ &= \frac{(-1)^m \lambda^m}{g} \sum \frac{(\det M)^{-1}}{\det(I - \lambda M^{-1})} \\ &= \frac{(-1)^m \lambda^m}{g} \sum \frac{\bar{\sigma}(M)}{\det(I - \lambda M)} \\ &= (-1)^m \lambda^m F_{G,\sigma}(\lambda). \quad \square \end{aligned}$$

3.8 PROPOSITION. *Let $R^G = \coprod_1^t \eta_i \mathbf{C}[\theta_1, \ldots, \theta_m]$, where $\deg \theta_i = d_i$, $\deg \eta_i = e_i$, $0 = e_1 \leqslant e_2 \leqslant \cdots \leqslant e_t$. Let μ be the least degree of a σ-invariant, i.e., the least degree of an $f \in R$ satisfying $Mf = (\det M)^{-1} f$ for all $M \in G$. Then*

$$e_t = \sum_1^m (d_i - 1) - \mu.$$

PROOF. We have $F_G(\lambda) = (\Sigma \lambda^{e_i}) \Pi (1 - \lambda^{d_i})^{-1}$, so

$$\begin{aligned} F_G(1/\lambda) &= (-1)^m \left(\sum \lambda^{d_1 + \cdots + d_m - e_i} \right) \prod (1 - \lambda^{d_i})^{-1} \\ &= (-1)^m \lambda^m F_{G,\sigma}(\lambda) \end{aligned}$$

by Lemma 3.7. Hence $d_1 + \cdots + d_m - e_t = m + \mu$. $\square$

3.9 COROLLARY. *With the above notation, we have $e_t \leqslant \Sigma_1^m (d_i - 1)$, with equality if and only if $G \subset \mathrm{SL}(V)$ (i.e., $\det M = 1$ for all $M \in G$).* $\square$

REMARK. Our results in this section concerning R^G can be extended straightforwardly to each R_χ^G. The basic result is the following, which is equivalent to the statement that R_χ^G is a *Cohen-Macaulay module.*

3.10 THEOREM. *Let $\theta_1, \ldots, \theta_m$ be an h.s.o.p. for R^G, and let $\chi \in X(G)$. Let $\rho_1, \ldots, \rho_\mu$ be homogeneous elements of R_χ^G whose images in the quotient module $S_\chi = R_\chi^G / (\theta_1 R_\chi^G + \cdots + \theta_m R_\chi^G)$ form a $\mathbf{C}$-basis for S_χ. Then*

$$R_\chi^G = \coprod_{i=1}^u \rho_i \mathbf{C}[\theta_1, \ldots, \theta_m].$$

PROOF. In the proof of Theorem 3.2 we obtained $R \cong R^G \oplus U$. We actually have the finer decomposition $R = \coprod R_\chi^G$. Now argue exactly as in the proof of Theorem 3.2, viz., choose a homogeneous $\mathbf{C}$-basis $\bar{\eta}_1, \ldots, \bar{\eta}_s$ for $R/(\theta_1, \ldots, \theta_m)$ such that each $\bar{\eta}_i$ lies in some S_χ. It follows as before that $R_\chi^G = \coprod \rho_i \mathbf{C}[\theta_1, \ldots, \theta_m]$, where the ρ_i's are those η_j's belonging to R_χ^G. $\square$

4. Group generated by pseudo-reflections. In light of Theorem 3.2 it is natural to ask under what circumstances does the representation $R^G = \coprod_1^t \eta_i \mathbf{C}[\theta_1, \ldots, \theta_m]$ have a particularly simple or interesting form. In this section we discuss the simplest possibility of all, viz., the case when $R^G =$

$\mathbf{C}[\theta_1, \ldots, \theta_m]$. Equivalently, R^G is generated by m elements, which are necessarily algebraically independent. The best-known case occurs when G consists of all $m \times m$ permutation matrices. An invariant is just a symmetric function of the x_i's, and the "fundamental theorem of symmetric functions" states that $R^G = \mathbf{C}[a_1, \ldots, a_n]$, where a_i is the ith *elementary symmetric function*, given by $a_i(\mathrm{x}) = \Sigma x_{j_1} x_{j_2} \cdots x_{j_i}$, where the sum is over all integers $1 \leqslant j_1 < j_2 < \cdots < j_i \leqslant m$. In order to state the fundamental result telling when $R^G = \mathbf{C}[\theta_1, \ldots, \theta_m]$, we require a definition. If G is a finite subgroup of $\mathrm{GL}(V)$ and $M \in G$, then M is called a *pseudo-reflection* if precisely one eigenvalue of M is not equal to one.

4.1 THEOREM. *Let G be a finite subgroup of* $\mathrm{GL}(V)$. *There exist m algebraically independent* (*homogeneous*) *invariants $\theta_1, \ldots, \theta_m$ such that $R^G = \mathbf{C}[\theta_1, \ldots, \theta_m]$ if and only if G is generated by pseudo-reflections.* (*Such a group will be called an f.g.g.r.*)

Theorem 4.1 was proved by Shepard and Todd **[S-T]**, Chevalley **[Ch]**, and Serre **[Se$_1$]**. Shephard and Todd explicitly determined all finite subgroups G of $\mathrm{GL}(V)$ generated by pseudo-reflections and verified the "if" part of Theorem 4.1 by the inelegant method of computing R^G explicitly for each of these G. (A modern treatment appears in **[Coh]**.) Chevalley found a "theoretical" proof of the "if" part which did not depend on knowing the groups G themselves, in the special case that G is generated by *reflections* (pseudo-reflections of determinant -1). Serre observed that Chevalley's proof is valid for groups generated by pseudo-reflections. While the "if" part of Theorem 4.1 has a purely algebraic proof, the proof of the "only if" part given in **[S-T]** has a strong combinatorial flavor so will be reproduced here (in a slightly different form).

4.2 LEMMA. *Let G be a finite subgroup of* $\mathrm{GL}(V)$ *of order g, and let r be the number of pseudo-reflections in G. Then the Laurent expansion of $F_G(\lambda)$ about $\lambda = 1$ begins*

$$F_G(\lambda) = \frac{1}{g}(1-\lambda)^{-m} + \frac{r}{2g}(1-\lambda)^{-m+1} + O((1-\lambda)^{-m+2}).$$

PROOF. By Theorem 2.1 we have

$$F_G(\lambda) = \frac{1}{g} \sum_{M \in G} \det(I - \lambda M)^{-1}.$$

The only term $\det(I - \lambda M)^{-1}$ in this sum to have a pole of order m at $\lambda = 1$ is the term $(1-\lambda)^{-m}$ corresponding to the identity element $M = I$ of G. If $\det(I - \lambda M)^{-1}$ has a pole of order $m - 1$ at $\lambda = 1$, then M is a pseudo-reflection and $\det(I - \lambda M)^{-1} = 1/(1-\lambda)^{m-1}(1-\rho\lambda)$ where $\rho = \det M$. Hence the coefficient of $(1-\lambda)^{-m+1}$ in the Laurent expansion of $F_G(\lambda)$ is $(1/g)\Sigma_P(1-\rho)^{-1}$, where P ranges over all pseudo-reflections in G and $\rho = \det P$. Now we have $(1-\rho)^{-1} + (1-\rho^{-1})^{-1} = 1$. Since P is a pseudo-reflection if and only if P^{-1} is also, we conclude

$$2\sum_P \frac{1}{1-\rho} = \sum_P \frac{1}{1-\rho} + \sum_P \frac{1}{1-\rho^{-1}} = \sum_P 1 = r,$$

completing the proof. □

4.3 COROLLARY. *For any finite $G \subset \mathrm{GL}(V)$, let $\theta_1, \ldots, \theta_m$ be an h.s.o.p. for R^G with $\deg \theta_i = d_i$. Let $R^G = \amalg_1^t \eta_i \mathbf{C}[\theta_1, \ldots, \theta_m]$, say with η_i homogeneous of degree e_i. Let $g = |G|$ and let r be the number of pseudo-reflections contained in G. Then*

$$tg = d_1 d_2 \cdots d_m,$$

$$rt + 2(e_1 + \cdots + e_t) = t(d_1 + \cdots + d_m - m).$$

PROOF. We have

$$F_G(\lambda) = \frac{\lambda^{e_1} + \cdots + \lambda^{e_t}}{\Pi(1 - \lambda^{d_i})} = \frac{t}{d_1 \ldots d_m} \frac{1}{(1-\lambda)^m}$$

$$+ \frac{1}{2d_1 \ldots d_m}\left[t(d_1 + \cdots + d_m - m) - 2(e_1 + \cdots + e_t)\right]\frac{1}{(1-\lambda)^{m-1}}$$

$$+ O\left((1-\lambda)^{-m+2}\right).$$

Comparing with Lemma 4.2 completes the proof. □

4.4 COROLLARY. *If $R^G = \mathbf{C}[\theta_1, \ldots, \theta_m]$ with $d_i = \deg \theta_i$, then $g = d_1 d_2 \ldots d_m$ and $r = \Sigma(d_i - 1)$.*

PROOF. Put $t = 1$ in Corollary 4.3 and note that we must have $e_1 = 0$. □

4.5 LEMMA. *Let $\psi_1, \ldots, \psi_n$ be homogeneous algebraically independent polynomials in $R = \mathbf{C}[x_1, \ldots, x_m]$. Let $\theta_1, \ldots, \theta_m$ be homogeneous algebraically independent polynomials in R which are polynomials in the ψ_i's (so $\theta_j \in \mathbf{C}[\psi_1, \ldots, \psi_m]$). Then there is a permutation π of $1, 2, \ldots, m$ such that $\deg \psi_i \leqslant \deg \theta_{\pi(i)}$ for all $i \in [m]$, with equality holding for all i if and only if $\mathbf{C}[\psi_1, \ldots, \psi_m] = \mathbf{C}[\theta_1, \ldots, \theta_m]$.*

FIRST PROOF. Since the ψ's and θ's are algebraically independent, the Jacobian determinant $\det(\partial\theta_i/\partial\psi_j) \neq 0$. Hence for some π we have

$$\frac{\partial\theta_{\pi(1)}}{\partial\psi_1} \cdots \frac{\partial\theta_{\pi(m)}}{\partial\psi_m} \neq 0,$$

and the proof follows (the condition for $\deg \psi_i = \deg \theta_{\pi(i)}$ being clear). □

SECOND PROOF. Define a bipartite graph Γ on the vertices $\theta_1, \ldots, \theta_m$, $\psi_1, \ldots, \psi_m$ as follows: An edge connects θ_j and ψ_i if and only if ψ_i actually appears in the polynomial $\theta_j = \theta_j(\psi_1, \ldots, \psi_m)$. It follows from the algebraic independence of the θ's that any k of the θ's are connected to at least k of the ψ's. Hence by the "marriage theorem" (e.g., **[Ry**, p. 48]) there is a permutation π such that ψ_i and $\theta_{\pi(i)}$ are connected, $i \in [m]$, and the proof follows. □

PROOF OF THE "ONLY IF" PART OF THEOREM 4.1 (assuming the validity of the "if" part). Assume $R^G = \mathbf{C}[\theta_1, \ldots, \theta_m]$ with $\deg \theta_i = d_i$. Let H be the subgroup of G generated by all pseudo-reflections in G. Then by the "if" part, we have $R^H = \mathbf{C}[\psi_1, \ldots, \psi_m]$. Clearly $R^G \subset R^H$, so each θ_i is a polynomial in the ψ's. By the previous lemma we may assume the ψ's are labeled so that $e_i = \deg \psi_i \leqslant d_i$. Let r be the number of pseudo-reflections in G and therefore in H. By Corollary 4.4 we have

$$r = \sum (d_i - 1) = \sum (e_i - 1).$$

Since $e_i \leqslant d_i$ we have $e_i = d_i$, so again by Corollary 4.4 we have $|G| = |H|$ and hence $G = H$. □

There are many other fascinating facts concerning finite groups generated by pseudo-reflections (or f.g.g.r.'s). We shall briefly discuss some of them here, referring the reader to the literature for further details. First we have the generalization of Corollary 4.4 proved by Shepard and Todd **[S-T**, Theorem 5.3] by examining all cases, and first proved uniformly by Solomon **[So$_1$]**.

4.6 Proposition. *Let $G \subset \mathrm{GL}(V)$ be an f.g.g.r., and let b_i be the number of elements $M \in G$ with exactly i eigenvalues unequal to one. Suppose $R^G = \mathbf{C}[\theta_1, \ldots, \theta_m]$ with $d_i = \deg \theta_i$. Then*

$$\sum_{i=0}^{m} b_i \lambda^i = \prod_{j=1}^{m} (1 + (d_i - 1)\lambda). \quad \square$$

If we put $\lambda = 1$ in Proposition 4.6 we get $g = \Pi d_i$, while if we compare coefficients of λ we get $r = \Sigma(d_i - 1)$. Hence Corollary 4.4 is indeed a special case.

We now turn to the consideration of the modules R^G_χ of invariants of an f.g.g.r. G relative to a linear character χ. A hyperplane $\mathcal{H} \subset V$ is called a *reflecting hyperplane* if some $I \neq P \in G$ (necessarily a pseudo-reflection) fixes $\mathcal{H}$ pointwise. The subgroup of G fixing $\mathcal{H}$ pointwise is a cyclic group $C_{\mathcal{H}}$ generated by some pseudo-reflection $P_{\mathcal{H}}$. Let $s_{\mathcal{H}}(\chi)$ be the least nonnegative integer s for which $\chi(P_{\mathcal{H}}) = (\det P_{\mathcal{H}})^s$. (It is easily seen that $s_{\mathcal{H}}(\chi)$ depends only on χ and $\mathcal{H}$, not on the choice of $P_{\mathcal{H}}$ generating $C_{\mathcal{H}}$.) Let $L_{\mathcal{H}} = L_{\mathcal{H}}(\mathbf{x})$ be the linear form which vanishes on $\mathcal{H}$, i.e., $\mathcal{H} = \{\alpha \in V\colon L_{\mathcal{H}}(\alpha) = 0\}$. Finally define $f_\chi = \Pi_{\mathcal{H}} L_{\mathcal{H}}^{s_{\mathcal{H}}(\chi)}$, where the product is over all distinct reflecting hyperplanes in V. Note that f is a homogeneous polynomial in R of degree $\Sigma_{\mathcal{H}} s_{\mathcal{H}}(\chi)$. The following result appears in **[Sp$_2$**, Theorem 4.34] and **[Sta$_1$**, Theorem 3.1]. The weaker result that R^G_χ is a free R^G-module of rank one follows immediately from **[Sp$_1$**, Proposition 2.6].

4.7 Proposition. *Let $G \subset \mathrm{GL}(V)$ be an f.g.g.r. and let χ be a linear character of G. Then R^G_χ is a free R^G-module of rank one generated by f_χ, i.e., $R^G_\chi = f_\chi \cdot R^G$.* □

In the special case $\chi(M) = (\det M)^{-1}$, there is an alternative expression for f_χ first described explicitly by Steinberg **[Ste]**.

4.8 Proposition. *Let $G \subset \mathrm{GL}(V)$ be an f.g.g.r. and let σ be the linear character given by $\sigma(M) = (\deg M)^{-1}$. Suppose $R^G = \mathbf{C}[\theta_1, \ldots, \theta_m]$ and let $J(\theta_1, \ldots, \theta_m) = (\partial\theta_i/\partial x_j)$, the Jacobian matrix of $\theta_1, \ldots, \theta_m$ (with respect to $x_1, \ldots, x_m$). Then for some $0 \neq \alpha \in \mathbf{C}$ we have $\alpha f_\sigma = \det J(\theta_1, \ldots, \theta_m)$.* □

It is interesting to check the above results for the special case where G

consists of the $m \times m$ permutation matrices. We have already mentioned that $R^G = \mathbf{C}[a_1, \ldots, a_m]$, where a_i is the ith elementary symmetric function in $x_1, \ldots, x_m$. Hence by Theorem 4.1 G is generated by pseudo-reflections, viz., the *transpositions* (permutation matrices with exactly two off-diagonal 1's). Since $\deg a_i = i$ we have by Corollary 4.4 $|G| = 1 \cdot 2 \cdots m = m!$ and $r = 0 + 1 + \cdots + (m-1) = \binom{m}{2}$. If we identify a permutation matrix $M = (m_{ij})$ with the permutation π of $\{1, 2, \ldots, m\}$ given by $\pi(i) = j$ if $m_{ij} = 1$, then the number of eigenvalues of M equal to one is the same as the number of cycles of π (when expressed as a product of disjoint cycles). Hence by Proposition 4.6 we have $\sum_{i=0}^{m} b_i\lambda^i = (1+\lambda)(1+2\lambda)\cdots(1+(m-1)\lambda)$, where b_i is the number of permutations of $\{1, 2, \ldots, m\}$ with $m - i$ cycles. This is a well-known result in combinatorics (e.g., **[Com**, p. 313]), and in fact $(-1)^{m-i}b_{m-i}$ is the Stirling number $s(m, i)$ of the first kind. Turning to Proposition 4.7, the group G has a single nontrivial linear character χ, given by $\chi(M) = \det M = (\det M)^{-1}$. A χ-invariant is the same as an *alternating polynomial* $f \in R$, i.e., $f(x_{\pi(1)}, \ldots, x_{\pi(m)}) = (\operatorname{sgn} \pi)f(x_1, \ldots, x_m)$ for all π. Proposition 4.7 implies that $R_\chi^G = \Delta(x_1, \ldots, x_m)R^G$, where $\Delta = \Pi_{i<j}(x_i - x_j)$ is the so-called *discriminant*. Hence we obtain the well-known result that an alternating polynomial is a symmetric polynomial times Δ. If instead of the a_i's we choose the polynomials $(1/i)(x_1^i + \cdots + x_m^i)$ to generate R^G, then Proposition 4.8 yields the well-known Vandermonde determinant

$$\det\left(x_j^{i-1}\right) = \Delta(x_1, \ldots, x_m).$$

The next result was proved for f.g.g.r.'s by Chevalley **[Ch]** and Serre **[Se$_1$]** using elementary Galois theory. We prove a more general result using Molien's theorem.

4.9 Proposition. *Let $\theta_1, \ldots, \theta_m$ be an h.s.o.p. for R^G, where G is any finite subgroup of* $\mathrm{GL}(V)$ *of order g. Set $d_i = \deg \theta_i$ and $t = d_1 \ldots d_m/g$. Then the action of G on the quotient ring $S = R/(\theta_1, \ldots, \theta_m)$ is isomorphic to t times the regular representation of G. (I.e., the multiplicity of χ in S is equal to $t \cdot \chi(1)$.)*

Proof. Let S_χ be the isotypical component afforded by χ of the action of G on S. Let $H_\chi(n)$ equal the multiplicity of χ in the action of G on forms of degree n in S_χ, so $\dim_{\mathbf{C}} S_\chi = \chi(1)\Sigma_n H_\chi(n)$. It follows from Theorem 3.10 that

$$\sum_{n>0} H_\chi(n)\lambda^n = \frac{1}{g}(1-\lambda^{d_1})\ldots(1-\lambda^{d_m}) \sum_{M \in G} \frac{\bar{\chi}(M)}{\det(I - \lambda M)}.$$

Putting $\lambda = 1$ yields that the multiplicity of χ in S_χ is given by

$$(1/g)(d_1, \ldots, d_m)\bar{\chi}(1) = t \cdot \chi(1). \quad \square$$

4.10 Corollary. *Let G be an f.g.g.r. with $R^G = \mathbf{C}[\theta_1, \ldots, \theta_m]$. Then the action of G on $R/(\theta_1, \ldots, \theta_m)$ is isomorphic to the regular representation of G.* $\square$

The numbers $H_\chi(n)$ occurring in the proof of Proposition 4.9 have been studied in more detail for certain groups G, especially the Weyl groups (e.g. **[B-L]**). For the benefit of readers familiar with the representation theory of the symmetric group, we state without proof the following unpublished result of Lusztig.

4.11 Proposition. *Let G be the group of all $m \times m$ permutation matrices, and let χ be the irreducible character of G corresponding to the partition μ of m. Then $H_\chi(n)$ is equal to the number of standard Young tableaux Y (with entries $1, 2, \ldots, m$) of shape μ such that n is equal to the sum of those entries i of Y for which i appears in a column to the left of $i+1$.* □

Proposition 4.9 suggests the problem of analyzing the action of G on the quotient ring $T = R/R_+^G$, where $R_+^G = R_1^G \oplus R_2^G \oplus \ldots$. The **C**-dimension of the isotypical component T_χ is equal to the minimum number of generators of R_χ^G as an R^G-module. It seems unlikely that there is a nice expression for $\dim_{\mathbf{C}} T_\chi$ or even $\dim_{\mathbf{C}} T$. If χ is a *linear* character of G then there is a condition **[Sta$_1$**, Theorem 2.3] for $\dim_{\mathbf{C}} T_\chi = 1$ (equivalently, R_χ^G is a free R^G-module, necessarily of rank one).

4.12 Proposition. *Let χ be a linear character of G, and define f_χ as preceding Proposition 4.7. (Though f_χ was defined only when G is an f.g.g.r., the definition makes sense for any G.) Then R_χ^G is a free R^G-module (of rank one) if and only if $f_\chi \in R_\chi^G$, in which case $R_\chi^G = f_\chi \cdot R^G$.* □

For further results on f.g.g.r.'s, we refer the reader to **[Bo]**, **[F]**, **[Sp$_1$]**, **[Sp$_2$]** and to the references given above. In particular **[F]** is a very readable survey paper, and **[Sp$_2$**, §4.4] applies the theory of f.g.g.r.'s to the computation of the invariants of the binary polyhedral groups.

5. Three applications. We have now developed enough theory to present three combinatorial applications.

5.1 Example. Let g be a positive integer, and define

$$S(g) = \sum_{\omega} |1 - \omega|^{-2}, \tag{8}$$

where the sum is over all $g - 1$ complex numbers ω satisfying $\omega^g = 1$ and $\omega \neq 1$. This is essentially the sum asked for in **[He]**. We show how $S(g)$ can be computed using the invariant theory of finite groups. The right-hand side of (8) is reminiscent of a Molien series (1). If we define

$$F_G(\lambda) = \frac{1}{g} \sum_{\omega} \frac{1}{(1-\omega\lambda)(1-\bar{\omega}\lambda)},$$

where ω now ranges over *all* gth roots of unity, then it is clear from Theorem 2.1 that $F_G(\lambda)$ is the Molien series corresponding to the invariants of the cyclic group G of order g generated by $\operatorname{diag}(\zeta, \zeta^{-1})$, where ζ is a primitive gth root of unity.

We then have

$$S(g) = \lim_{\lambda \to 1} \left[gF_G(\lambda) - \frac{1}{(1-\lambda)^2} \right]. \tag{9}$$

Now G is such a trivial group that $F_G(\lambda)$ can be obtained practically by inspection. Setting $x = x_1$ and $y = x_2$, the invariants of G are clearly linear combinations of monomials $x^{ag}y^{bg}x^c y^c$, where $a, b, c \in \mathbf{N}$ and $0 \leqslant c \leqslant g - 1$. Hence

$$R^G = \coprod_{c=0}^{g-1} x^c y^c \cdot \mathbf{C}[x^g, y^g].$$

(Note that we have found generators of R^G as a $\mathbf{C}[x^g, y^g]$-module which are all powers of a single element xy. For the algebraic significance of this fact, see §9.) It follows that

$$F_G(\lambda) = \frac{1 + \lambda^2 + \lambda^4 + \cdots + \lambda^{2g-2}}{(1 - \lambda^g)^2}.$$

It is now a straightforward (though somewhat tedious) task to compute $S(g)$ from (9), e.g., by l'Hôpital's rule. The final result is $S(g) = (g^2 - 1)/12$.

The reader may feel that it should be unnecessary to use the sledgehammer of invariant theory to crack the walnut of $S(g)$. One advantage of our approach is that it opens several avenues of extension. As a first such extension, the reader may wish to investigate on his own the sum

$$S_k(g) = \sum_{\omega} |1 - \omega|^{-2k}$$

where $\omega^g = 1$, $\omega \neq 1$, and $k \in \mathbf{P}$. For instance,

$$S_2(g) = (g^2 - 1)(g^2 + 11)/2^4 \cdot 3^2 \cdot 5,$$
$$S_3(g) = (g^2 - 1)(2g^4 + 23g^2 + 191)/2^6 \cdot 3^3 \cdot 5 \cdot 7,$$
$$S_4(g) = (g^2 - 1)(g^2 + 11)(3g^4 + 10g^2 + 227)/2^8 \cdot 3^4 \cdot 5^2 \cdot 7.$$

It can be shown that $S_k(g)$ is an even polynomial of degree $2k$ and that

$$\sum_{k=1}^{\infty} 4^k S_k(g) x^{2k} = 1 - \frac{gx \cot(g \sin^{-1} x)}{\sqrt{1 - x^2}}.$$

5.2 Example. Let X be the vector space of dimension n over GF(2) consisting of all n-tuples of 0's and 1's. Let C be a subspace of X of dimension l, i.e., an *error-correcting* code. Suppose that C is *self-dual*, i.e., $C = C^{\perp}$, where $C^{\perp} = \{v \in X\colon v \cdot w = 0 \text{ for all } w \in C\}$, the dot product $v \cdot w$ being taken mod 2. (It follows that $n = 2l$.) Let $A(r)$ be the number of vectors in C with exactly r ones, and set $W(x, y) = \sum_{r=0}^{n} A(r) x^{n-r} y^r$. It is known that the hypothesis that C is self-dual implies that

$$W\big((x + y)/\sqrt{2}, (x - y)/\sqrt{2}\big) = W(x, y),$$
$$W(x, -y) = W(x, y). \tag{10}$$

The first of these identities is a consequence of the well-known MacWilliams identities of coding theory [Mc], [Sl], while the second is equivalent to the fact that every $w \in C$ has an even number of ones, since $w \cdot w = 0$. Hence $W(x, y)$ is an invariant of the group G generated by $(1/\sqrt{2})\left(\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$. G is a group of order 16, and each of the preceding two generators is a pseudo-reflection. Moreover, G contains precisely eight pseudo-reflections. It follows from Theorem 4.1 and Corollary 4.4 that $R^G = \mathbf{C}[\theta_1, \theta_2]$, where $\deg \theta_1 = 2$, $\deg \theta_2 = 8$. With this information at hand, it is not hard to see that θ_1 and θ_2 may be chosen to be

$$\theta_1 = x^2 + y^2, \qquad \theta_2 = x^2y^2(x^2 - y^2)^2. \tag{11}$$

Equation (11), originally due to Gleason, together with various generalizations and modifications, has recently been applied to various problems in coding theory and to the problem of finding a projective plane of order 10. See, for example, **[M-M-S]**, **[M-S]**, and the survey paper **[Sl]**.

5.3 Example. Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_l) \in \mathbf{N}^l$, and let $P_n(\boldsymbol{\alpha})$ denote the number of ways of writing $\boldsymbol{\alpha}$ as a sum of n vectors in $\mathbf{N}^l$, *without regard to order.* For instance, $P_3(2, 1) = 4$, corresponding to $(0, 0) + (0, 0) + (2, 1)$, $(0, 0) + (1, 0) + (1, 1)$, $(0, 0) + (0, 1) + (2, 0)$, $(1, 0) + (1, 0) + (0, 1)$. The theory of the numbers $P_n(\boldsymbol{\alpha})$ belongs to the subject of "multipartite partitions", of which **[An**, Chapter 11] contains a nice survey. (It is customary not to allow $(0, 0, \ldots, 0)$ as a part, but this turns out to be irrelevant.) Let $\boldsymbol{\lambda}^{\boldsymbol{\alpha}} = \lambda_1^{\alpha_1} \ldots \lambda_l^{\alpha_l}$. It is then clear by "inspection" that

$$\sum_{n \in \mathbf{N}} \sum_{\boldsymbol{\alpha} \in \mathbf{N}^l} P_n(\boldsymbol{\alpha}) \boldsymbol{\lambda}^{\boldsymbol{\alpha}} t^n = \prod_{\boldsymbol{\beta} \in \mathbf{N}^l} (1 - \boldsymbol{\lambda}^{\boldsymbol{\beta}} t)^{-1}. \tag{12}$$

It was Solomon **[So$_2$]** who first incorporated the theory of multipartite partitions into the theory of invariants of finite groups, by interpreting the right-hand side of (12) in terms of certain generalized Molien series. Solomon's results are considerably more general, but we shall merely extract from them what is needed to prove an interesting result about the generating function (12).

Suppose $V = V_1 \oplus \cdots \oplus V_l$ and that each V_i is invariant under the finite group $G \subset GL(V)$, i.e., $Mx \in V_i$ for all $M \in G$ and $x \in V_i$. We give V the structure of an "$\mathbf{N}^l$-graded vector space" by defining $\deg x$ to be the ith unit coordinate vector $\boldsymbol{\varepsilon}_i$ in $\mathbf{N}^l$ if $x \in V_i$. Let $x_{i1}, x_{i2}, \ldots, x_{is_i}$ be a basis for V_i. Then the polynomial ring $R = \mathbf{C}[x_{ij}\colon 1 \leqslant i \leqslant l,\ 1 \leqslant j \leqslant s_i]$ has an $\mathbf{N}^l$-grading "induced" from V, i.e., $R = \amalg_{\boldsymbol{\alpha} \in \mathbf{N}^l} R_{\boldsymbol{\alpha}}$, where $R_{\boldsymbol{\alpha}}$ is spanned by all monomials $\prod_{i,j} x_{ij}^{a_{ij}}$ such that $\alpha_i = \sum_j a_{ij}$ for $1 \leqslant i \leqslant l$. Moreover, the action of G on R preserves the $\mathbf{N}^l$-grading, so R^G has the structure $R^G = \amalg_{\boldsymbol{\alpha}} R^G_{\boldsymbol{\alpha}}$ of an $\mathbf{N}^l$-graded algebra, with $R^G_{\boldsymbol{\alpha}} = R^G \cap R_{\boldsymbol{\alpha}}$. It is natural to ask for an extension of Molien's theorem which will give an expression for $F_G(\boldsymbol{\lambda}) = \sum_{\boldsymbol{\alpha}} (\dim_{\mathbf{C}} R^G_{\boldsymbol{\alpha}}) \boldsymbol{\lambda}^{\boldsymbol{\alpha}}$. In exactly the way Molien's theorem is proved one obtains

$$F_G(\boldsymbol{\lambda}) = \frac{1}{g} \sum_{M \in G} \prod_{i=1}^{l} \det(1 - \lambda_i M_i)^{-1}, \tag{13}$$

where $M_i\colon V_i \to V_i$ denotes the restriction of M to V_i.

Now let each $s_i = n$, so $R = \mathbf{C}[x_{ij}\colon 1 \leqslant i \leqslant l, 1 \leqslant j \leqslant n]$. Let the symmetric group $\mathfrak{S}_n$ of all permutations of $[n]$ act on V by $\pi x_{ij} = x_{i\pi(j)}$. This defines a certain group $\Gamma_n \subset GL(V)$ abstractly isomorphic to $\mathfrak{S}_n$. It follows from (13) that

$$F_{\Gamma_n}(\boldsymbol{\lambda}) = \frac{1}{n!} \sum_{\pi \in \mathfrak{S}_n} \prod_{C} (1 - \lambda_1^c)^{-1} \ldots (1 - \lambda_l^c)^{-1}, \tag{14}$$

where C ranges over all cycles of π, and c is the length of C. A well-known formula from enumerative combinatorics (e.g., [**Ri**, p. 68], [**Co**, pp. 134 and 247]) implies that

$$\sum_{n=0}^{\infty} F_{\Gamma_n}(\boldsymbol{\lambda})t^n = \exp \sum_{i=1}^{\infty} \frac{t^i}{i}(1-\lambda_1^i)^{-1} \dots (1-\lambda_m^i)^{-1}.$$

Writing $(1-\lambda_1^i)^{-1} \dots (1-\lambda_l^i)^{-1} = \Sigma_{\boldsymbol{\beta} \in \mathbf{N}^m} \boldsymbol{\lambda}^{i\boldsymbol{\beta}}$, we get

$$\sum_{n=0}^{\infty} F_{\Gamma_n}(\boldsymbol{\lambda})t^n = \exp \sum_{\boldsymbol{\beta}} \log(1-\boldsymbol{\lambda}^{\boldsymbol{\beta}}t)^{-1}$$

$$= \prod_{\boldsymbol{\beta}} (1-\boldsymbol{\lambda}^{\boldsymbol{\beta}}t)^{-1}. \tag{15}$$

Comparing (12) with (15), we see that $\Sigma_{\boldsymbol{\alpha} \in \mathbf{N}^l} P_n(\boldsymbol{\alpha})\boldsymbol{\lambda}^{\boldsymbol{\alpha}}$ is just the generalized Molien series for the group Γ_n.

Ira Gessel has pointed out that a simple direct argument also shows that $\Sigma P_n(\boldsymbol{\alpha})\boldsymbol{\lambda}^{\boldsymbol{\alpha}}$ is the Molien series for Γ_n. Let $\boldsymbol{\alpha} = \boldsymbol{\alpha}_1 + \cdots + \boldsymbol{\alpha}_n$ be a multipartite partition of $\boldsymbol{\alpha}$ into n parts, and let $\boldsymbol{\alpha}_j = (\alpha_{1j}, \dots, \alpha_{lj})$. Then a little thought shows that the elements $\Sigma_{M \in \Gamma_n} M(\Pi_{i,j}\, x_{ij}^{\alpha_{ij}})$, taken over all multipartite partitions of $\boldsymbol{\alpha}$ into n parts, form a $\mathbf{C}$-basis for $R_{\boldsymbol{\alpha}}^{\Gamma_n}$. Hence $\dim_{\mathbf{C}} R_{\boldsymbol{\alpha}}^{\Gamma_n} = P_n(\boldsymbol{\alpha})$, as desired.

Now in general if $l \geqslant 2$, then an $\mathbf{N}^l$-graded algebra need not have a system of parameters which is homogeneous with respect to the $\mathbf{N}^l$-grading (called an $\mathbf{N}^l$-*h.s.o.p.*). However, for the algebra R^{Γ_n} it is easy to check that the elementary symmetric functions $\theta_{ij} = a_j(x_{i1}, \dots, x_{il})$, $i \in [l]$, $j \in [n]$, do form an $\mathbf{N}^l$-h.s.o.p., with $\deg \theta_{ij} = j\boldsymbol{\varepsilon}_i$. This implies that in the decomposition $R^{\Gamma_n} = \amalg_{k=1}^{t} \eta_k \mathbf{C}[\theta_{ij}]$ we can choose each η_k to be $\mathbf{N}^l$-homogeneous, say of degree $\boldsymbol{\delta}_k \in \mathbf{N}^l$. It follows that

$$F_{\Gamma_n}(\boldsymbol{\lambda}) = \left(\sum_{k=1}^{t} \boldsymbol{\lambda}^{\boldsymbol{\delta}_k} \right) \prod_{i=1}^{l} \prod_{j=1}^{n} (1-\lambda_i^j)^{-1}.$$

Therefore we conclude:

5.4 Proposition. *We have*

$$\prod_{\boldsymbol{\beta} \in \mathbf{N}^l} (1-\boldsymbol{\lambda}^{\boldsymbol{\beta}}t)^{-1} = \sum_{n=0}^{\infty} \frac{Q_n(\boldsymbol{\lambda})t^n}{\Pi_{i=1}^{l} \Pi_{j=1}^{n} (1-\lambda_i^j)},$$

where $Q_n(\boldsymbol{\lambda})$ is a polynomial with nonnegative integer coefficients. □

The nonnegativity of the coefficients of $Q_n(\boldsymbol{\lambda})$ was conjectured by Wright [**Wr**] and first proved by Gordon [**G**] using an intricate combinatorial argument. A relatively simple combinatorial proof has recently been given in [**G-G**, Remark 2.2]. As mentioned above, the invariant theory approach is due to Solomon [**So$_2$**], and the reader is referred there for further aspects of this idea. Let us simply mention that an exact analogue of Proposition 5.4 for multipartite partitions with *distinct* parts (corresponding to the product $\Pi(1+\boldsymbol{\lambda}^{\boldsymbol{\beta}}t)$) can be obtained by considering the module $R_{\chi}^{\Gamma_n}$, where χ is the alternating character of Γ_n.

Abelian groups. Suppose that in the setup of (13) we have $\dim V_i = 1$ for all $i \in [m]$. Thus each matrix $M \in G$ is diagonal with respect to the basis $x_1, \ldots, x_m$ ($x_i \in V_i$). It is well known that a finite subgroup of $\mathrm{GL}(V)$ can be put in diagonal form if and only if it is abelian, so the case $\dim V_i = 1$ corresponds to the study of abelian groups. It is clear that as a vector space over $\mathbf{C}$, R^G has a basis consisting of all invariant monomials $\mathbf{x}^{\boldsymbol{\alpha}} = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$. The generalized Molien series (13) is given by $F_G(\boldsymbol{\lambda}) = \sum_{\boldsymbol{\alpha}} \boldsymbol{\lambda}^{\boldsymbol{\alpha}}$, where $\boldsymbol{\alpha}$ ranges over all elements of $\mathbf{N}^m$ for which $\mathbf{x}^{\boldsymbol{\alpha}}$ is invariant. Hence knowing $F_G(\boldsymbol{\lambda})$ is equivalent to knowing R^G. Equation (13) takes the form

$$F_G(\boldsymbol{\lambda}) = \frac{1}{g} \sum_{M \in G} 1/(1 - \varepsilon_1 \lambda_1) \cdots (1 - \varepsilon_m \lambda_m), \tag{16}$$

where $M = \mathrm{diag}(\varepsilon_1, \ldots, \varepsilon_m)$.

It is clear that we can choose an h.s.o.p. for R^G of the form $x_1^{d_1}, x_2^{d_2}, \ldots, x_m^{d_m}$, where $d_i \in \mathbf{P}$. In the decomposition $R^G = \amalg \eta_i \mathbf{C}[x_1^{d_1}, \ldots, x_m^{d_m}]$, we can choose the η_i's to be the set of all invariant monomials of the form $x_1^{\beta_1} \ldots x_m^{\beta_m}$ such that $0 \leqslant \beta_i < d_i$ for $i \in [m]$. In particular, we may choose each $d_i = g$. In this case a monomial $\mathbf{x}^{\boldsymbol{\alpha}}$ belongs to R^G if and only if $\boldsymbol{\alpha}$ satisfies the system of congruences

$$\boldsymbol{\delta} \cdot \boldsymbol{\alpha} \equiv 0 \pmod g$$

where $\boldsymbol{\delta}$ ranges over all vectors in $\mathbf{Z}^m$ (or $(\mathbf{Z}/g\mathbf{Z})^m$) for which $\mathrm{diag}(\zeta^{\delta_1}, \ldots, \zeta^{\delta_m}) \in G$, $\zeta = e^{2\pi i/g}$. Hence the study of R^G for G abelian is essentially equivalent to the study of linear homogeneous congruences.

5.5 Example. Let G be the group of order 3 generated by $\mathrm{diag}(\omega, \omega^2)$, where $\omega = e^{2\pi i/3}$. Then

$$\begin{aligned} F_G(\boldsymbol{\lambda}) = \frac{1}{3}\Bigg[\frac{1}{(1-\lambda_1)(1-\lambda_2)} &+ \frac{1}{(1-\omega\lambda_1)(1-\omega^2\lambda_2)} \\ &+ \frac{1}{(1-\omega^2\lambda_1)(1-\omega\lambda_2)} \Bigg] \\ = (1 + \lambda_1\lambda_2 + \lambda_1^2\lambda_2^2)/&(1-\lambda_1^3)(1-\lambda_2^3). \end{aligned}$$

It follows that $R^G = \mathbf{C}[x_1^3, x_2^3](1 \oplus x_1x_2 \oplus x_1^2x_2^2)$. In terms of congruences, we have $x_1^{\alpha_1}x_2^{\alpha_2} \in R^G$ if and only if $\alpha_1 + 2\alpha_2 \equiv 0 \pmod 3$.

6. Syzygies. Theorem 3.2 establishes the existence of a "canonical form" $\sum \eta_i p_i(\theta_1, \ldots, \theta_n)$ for elements of R^G, from which the Molien series $F_G(\lambda)$ can be obtained by inspection. (Of course the actual computation of the θ_i's and η_j's may be difficult.) We would now like to discuss a second technique for "determining" R^G and obtaining $F_G(\lambda)$–the method of *syzygies*. We begin with an informal description of this method. Take any finite set $\gamma_1, \gamma_2, \ldots, \gamma_s$ of homogeneous elements of R^G which generate R^G as a $\mathbf{C}$-algebra. (By Theorem 1.2 or 3.2, such finite generating sets always exist.) If the γ_i's were algebraically independent with $\deg \gamma_i = d_i$, then we would have $F_G(\lambda) = \Pi(1 - \lambda^{d_i})^{-1}$. In general, however, various relations will hold among the γ_i's. These relations are called *syzygies of the first kind.* A version of the Hilbert basis theorem shows that all syzygies of the first kind are consequences of finitely many of them (which we may assume to be homogeneous). Suppose $S_1 = 0, S_2 = 0, \ldots, S_w = 0$ is such a homogeneous basis for the syzygies of the first kind among the γ_i's, with $\deg S_i = f_i$. It follows that the tentative generating function $F_G(\lambda) = \Pi(1 - \lambda^{d_i})^{-1}$ must be corrected to $F_G(\lambda) = (1 - \Sigma\lambda^{f_i})/\Pi(1 - \lambda^{d_i})$ to take into account the duplications caused by the syzygies $S_i = 0$. Now, however, the syzygies $S_1 = 0, S_2 = 0, \ldots, S_w = 0$ need not themselves be independent, and relations among them are called *syzygies of the second kind.* Once again by the Hilbert basis theorem the syzygies of the second kind have a finite basis, and these will cause further corrections to $F_G(\lambda)$, resulting in expressions like $F_G(\lambda) = (1 - \Sigma\lambda^{f_i} + \Sigma\lambda^{g_i})/\Pi(1 - \lambda^{d_i})$. Continuing this process, we obtain syzygies of higher and higher kinds. The *Hilbert syzygy theorem* **[Hi]**, **[Z-S**, Chapter VII, §13**]** states that this process will terminate within s steps. Hence $F_G(\lambda)$ can be written in the form

$$F_G(\lambda) = \left(1 - \sum\lambda^{f_i} + \sum\lambda^{g_i} - \cdots \pm \sum\lambda^{k_i}\right)/\prod(1 - \lambda^{d_i}),$$

where there are at most s summation signs in the numerator. Of course if one is merely given $F_G(\lambda)$, it is impossible to determine which terms of the numerator correspond to which kind of syzygies without analyzing the algebra R^G in detail. However, knowing $F_G(\lambda)$ is a useful guide for determining all the syzygies. In general, given R^G and a choice of generators γ_i, it is extremely difficult to determine all the syzygies explicitly. A good discussion of how one can explicitly determine the invariants and syzygies for a given group G may be found in **[M-M-S**, §IV**]**. For examples of computations involving the ring R^G (such as the computation of Molien series, sets of generators, syzygies of the first kind, higher order syzygies, and the decomposition $R^G = \amalg\eta_i\mathbf{C}[\theta_1, \ldots, \theta_m]$), see **[J-B$_1$]**, **[J-B$_2$]**, **[Hu]**, **[M-S]**, **[M-B-D]**, **[Pa]**, **[Sl]**, **[Sp$_2$**, Chapter 4**]**, **[Str$_1$]**, **[Str$_2$]**, **[Str$_3$]**.

6.1 Example. Let G be as in Example 2.2. Then R^G is generated by $\gamma_1 = x_1^2 + x_2^2$, $\gamma_2 = x_1^2x_2^2$, and $\gamma_3 = x_1^3x_2 - x_1x_2^3$. A basis for the syzygies of the first kind consists of the single relation $S_1 = \gamma_3^2 - \gamma_1^2\gamma_2 + 4\gamma_2^2 = 0$. There are no higher order syzygies. Since $\deg \gamma_1 = 2$, $\deg \gamma_2 = 4$, $\deg \gamma_3 = 4$, and $\deg S_1 = 8$, we have $F_G(\lambda) = (1 - \lambda^8)/(1 - \lambda^2)(1 - \lambda^4)^2$.

Our informal description of syzygies may have sufficed to derive $F_G(\lambda)$ in Example 6.1, but in general we have not made clear precisely what is meant by a "sygygy of the kth kind." We therefore give a more formal description of the method of syzygies. Let $B = B_0 \oplus B_1 \oplus \cdots$ be an $\mathbf{N}$-graded k-algebra. Given a set $\gamma_1, \gamma_2, \ldots, \gamma_s$ of homogeneous generators for B, with $d_i = \deg \gamma_i > 0$, form new indeterminates $y_1, \ldots, y_s$ and let A denote the polynomial ring $A = k[y_1, \ldots, y_s]$ with an $\mathbf{N}$-grading $A_0 \oplus A_1 \oplus \cdots$ given by $\deg y_i = d_i$. We define an A-module structure on B by the conditions $y_i f = \gamma_i f$ for all $f \in B$. As an A-module, B is generated by the single element 1 (since $\gamma_1, \ldots, \gamma_s$ generate B as a k-algebra). Hence B is isomorphic to a quotient ring A/I of A, where I is a homogeneous ideal of A (i.e., I is generated by elements homogeneous with respect to the above $\mathbf{N}$-grading). The ideal I consists of the syzygies of the first kind. *Throughout this paper, A, I, and $B = A/I$ will retain the above meaning* (with a few obvious exceptions).

In the present context, the rigorous formulation of the Hilbert syzygy theorem implies that there is an exact sequence of A-modules,

$$0 \to M_h \xrightarrow{\rho_h} M_{h-1} \to \cdots \to M_1 \xrightarrow{\rho_1} M_0 \xrightarrow{\rho_0} B \to 0, \tag{17}$$

where $h \leqslant s$ and each M_i is a finitely-generated *free* A-module. The exact sequence (17) is called a *finite free resolution* of B (as an A-module). By an appropriate choice of the degrees of the free generators of each M_i, the M_i's become $\mathbf{Z}$-graded A-modules (as defined in §1), and the homomorphisms ρ_i can be chosen to preserve degree, i.e., will map homogeneous elements of M_i of degree d into homogeneous elements of M_{i-1} of degree d. We will always suppose that (17) has been chosen so that each ρ_i preserves degree. Suppose that M_i has a basis consisting of r_i elements of degrees $d_{1i}, d_{2i}, \ldots, d_{r_i i}$, respectively. It is a simple consequence of (17) that the Hilbert series $F(B, \lambda)$ is given by

$$F(B, \lambda) = \left[\sum_{i=0}^{h} (-1)^i \sum_{j=1}^{r_i} \lambda^{d_{ji}} \right] \prod_{i=1}^{s} (1 - \lambda^{d_i})^{-1}. \tag{18}$$

Hence $F(B, \lambda)$ can be computed once (17) is known.

The homomorphisms ρ_i in (17) may be regarded as specifying the syzygies of the ith kind. The kernel of ρ_{i-1} is the *module of syzygies of the ith kind*, for $1 \leqslant i \leqslant h$. We may think of constructing (17) by finding, $M_0, M_1, \ldots, M_h$ in turn. Once we have found M_i and ρ_i, pick any set of homogeneous generators for ker ρ_i and let a basis for M_{i+1} map onto these generators. If at each stage we choose a *minimal* set of generators for ker ρ_i, then (17) is called a *minimal free resolution* of B (as an A-module). A minimal free resolution (17) of B is *unique*, in the sense that if

$$0 \to N_j \xrightarrow{\sigma_j} N_{j-1} \to \cdots \to N_1 \xrightarrow{\sigma_1} N_0 \xrightarrow{\sigma_0} B \to 0$$

is another one, with $M_h \neq 0$ and $N_j \neq 0$, then $h = j$ and there are degree-preserving A-module isomorphisms $M_i \xrightarrow{\cong} N_i$ such that the following diagram commutes:

$$\begin{tikzcd}
0 \arrow[r] & M_h \arrow[r, "\rho_h"] \arrow[d, "\cong"] & M_{h-1} \arrow[r] \arrow[d, "\cong"] & \cdots \arrow[r] & M_1 \arrow[r, "\rho_1"] \arrow[d, "\cong"] & M_0 \arrow[r, "\rho_0"] \arrow[d, "\cong"] & B \arrow[r] \arrow[d, "\cong"] & 0 \\
0 \arrow[r] & N_h \arrow[r, "\sigma_h"] & N_{h-1} \arrow[r] & \cdots \arrow[r] & N_1 \arrow[r, "\sigma_1"] & N_0 \arrow[r, "\sigma_0"] & B \arrow[r] & 0.
\end{tikzcd}$$

In particular, the minimum number of generators of M_i and the degrees d_{ji} of these generators are uniquely determined in a minimal free resolution. The minimum number of generators (or *rank*) of M_i is called the ith *Betti number* of B (as an A-module) and is denoted $\beta_i^A(B)$. If we have chosen $\gamma_1, \gamma_2, \ldots, \gamma_s$ to be a *minimal* set of generators for B (as a k-algebra), then it turns out that $\beta_i^A(B)$ (and in fact the degrees d_{ji}) depend only on B, not on the choice of γ_i's. We write $\beta_i(B)$ for $\beta_i^A(B)$ when $\gamma_1, \ldots, \gamma_s$ is minimal. It is an interesting and difficult problem to compute the Betti numbers $\beta_i(B)$ in general, and $\beta_i(R^G)$ in particular. Note that since B is generated as an A-module by the single element 1, we always have $\beta_0(B) = 1$. A good check of one's computations is the fact that $\Sigma_i(-1)^i\beta_i(B) = 0$ unless B is a polynomial ring (i.e., unless there exist algebraically independent generators $\gamma_1, \ldots, \gamma_s$).

The least integer h for which (17) exists (equivalently, the greatest integer h for which $\beta_h^A(B) \neq 0$) is called the *homological dimension* of B (as an A-module), denoted $\operatorname{hd}_A(B)$. As before we write hd B when $\gamma_1, \ldots, \gamma_s$ is minimal. A standard result of commutative algebra (e.g., [Se$_2$, Chapter IV]) implies that if $m = \dim B$ and $B = A/I$ as above with $A = k[y_1, \ldots, y_s]$, then

$$s - m \leqslant \operatorname{hd}_A B \leqslant s.$$

The latter inequality is just the Hilbert syzygy theorem. Moreover, $\operatorname{hd}_A B = s - m$ if and only if B is Cohen-Macaulay [Se$_2$, Chapter IV]. Hence from Theorems 1.1 and 3.2 we conclude the following.

6.2 THEOREM. *Let G be a finite subgroup of* GL(V), *let $A = \mathbf{C}[y_1, \ldots, y_s]$, and let $R^G = A/I$ as above. Then*

$$\operatorname{hd}_A(R^G) = s - m. \quad \square$$

Note that Theorem 4.1 may be reformulated as follows: hd $R^G = 0$ if and only if G is generated by pseudo-reflections.

Once we have chosen (homogeneous) bases for the M_i's in (17), we may represent ρ_j ($j \geqslant 1$) as an $r \times s$ matrix, where $r = \operatorname{rank} M_j$ and $s = \operatorname{rank} M_{j-1}$, thinking of the elements of M_i as row-vectors of length equal to rank M_i. The entries of the matrix ρ_j will be homogeneous elements of A. It is easy to see that the resolution (17) is minimal if and only if all the entries of each ρ_j have positive degree (allowing the element 0 as an entry). Equivalently, no entry of any ρ_j can be a nonzero element of k.

Suppose we wish to compute the minimal free resolution of some R^G (with respect to a choice of generators $\gamma_1, \ldots, \gamma_s$). As mentioned previously, it is usually best first to compute $F_G(\lambda)$ (by Molien's theorem or otherwise) and compare with (18). This will give a useful guide to the degrees d_{ji} of the generators of the modules M_i. Unfortunately there may be cancellation between various terms in the numerator of (18) so that we cannot unequivocally deduce the d_{ji}'s from $F_G(\lambda)$. In certain very special cases there is no cancellation. Two such results (not the most general possible) will now be stated without proof. For a deeper understanding of what lies behind these results, including an explicit description of the actual resolutions, see [**Wah**].

6.3 PROPOSITION. *Suppose that the Cohen-Macaulay* $\mathbf{N}$*-graded k-algebra B is generated by elements $\gamma_1, \ldots, \gamma_{m+p}$ all of the same degree e, and that $F(B, \lambda) = (1 + p\lambda^e)(1 - \lambda^e)^{-m}$. (Thus by Lemma 4.2, we have $(1 + p)g = e^m$ when $B = R^G$.) Then in the minimal free resolution (17) of B (with respect to $\gamma_1, \ldots, \gamma_{m+p}$), we have that $h = p$ and that the module M_i for $i \in [p]$ has a basis consisting of $i\binom{p+1}{i+1}$ elements of degree $e(i + 1)$.* $\square$

6.4 PROPOSITION. *Suppose that the* $\mathbf{N}$*-graded k-algebra B is a Cohen-Macaulay integral domain generated by elements $\gamma_1, \ldots, \gamma_{m+p}$ all of the same* *degree e, and that $F(B, \lambda) = (1 + p\lambda^e + \lambda^{2e})(1 - \lambda^e)^{-m}$. (Thus by Theorem 4.2, we have $(2 + p)g = e^m$ when $B = R^G$.) Then in the minimal free resolution (17) of B (with respect to $\gamma_1, \ldots, \gamma_{m+p}$), we have that $h = p$ and that the module M_i for $i \in [p - 1]$ has a basis consisting of*

$$\frac{i(p-i)}{p+1}\binom{p+2}{i+1}$$

elements of degree $e(i + 1)$, while M_p is generated by one element of degree $e(p + 2)$. □

We now give some examples of minimal free resolutions and computation of Betti numbers.

6.5 Example. Let $G, \gamma_1, \gamma_2, \gamma_3$ be as in Example 6.1. Then $A = \mathbf{C}[y_1, y_2, y_3]$ with $\deg y_1 = 2$, $\deg y_2 = 4$, $\deg y_3 = 4$, and the results of Example 6.1 yield the minimal free resolution

$$0 \to A \xrightarrow[{[y_3^2 - y_1^2 y_2 + 4y_2^2]}]{} A \to R^G \to 0.$$

The map ρ_1 is represented by the 1×1 matrix $[y_3^2 - y_1^2 y_2 + 4y_2^2]$. The unique element in any basis for $M_0 = A$ has degree 0 (as is the case for any B) and for $M_1 = A$ has degree 8 (the degree of $y_3^2 - y_1^2 y_2 + 4y_2^2$ in A). Hence (18) yields

$$F_G(\lambda) = \frac{1 - \lambda^8}{(1 - \lambda^2)(1 - \lambda^4)^2},$$

which is exactly what we obtained in Example 6.1, essentially by the same reasoning though not quite so formally. We also see that hd $R^G = 1$, $\beta_0(R^G) = 1, \beta_1(R^G) = 1$.

6.6 Example. This example should illustrate the difficulties in computing syzygies even for very small groups. Let G be the group of order 2 and degree 3 generated by diag$(-1, -1, -1)$. Pick for generators of R^G the elements $\gamma_1 = x_1^2, \gamma_2 = x_2^2, \gamma_3 = x_3^2, \gamma_4 = x_1x_2, \gamma_5 = x_1x_3, \gamma_6 = x_2x_3$. This is a minimal set of generators all of degree 2. The Molien series is given by

$$\begin{aligned} F_G(\lambda) &= \tfrac{1}{2}\left[(1 - \lambda)^{-3} + (1 + \lambda)^{-3}\right] \\ &= (1 + 3\lambda^2)(1 - \lambda^2)^{-3}. \end{aligned}$$

Hence Proposition 6.3 applies, so we know that hd $R^G = 3$ and that M_1 is generated by 6 elements of degree 4, M_2 is generated by 8 elements of degree 6, and M_3 is generated by 3 elements of degree 8. (Note that $1 - 6 + 8 - 3 = 0$.) Even with this useful information it is not easy to compute the minimal free resolution by brute force. The resolution turns out to be

$$0 \to A^3 \xrightarrow{\rho_3} A^8 \xrightarrow{\rho_2} A^6 \xrightarrow{\rho_1} A \to R^G \to 0$$

where

$$\rho_1 = \begin{bmatrix} y_1y_2 - y_4^2 \\ y_1y_3 - y_5^2 \\ y_2y_3 - y_6^2 \\ y_4y_5 - y_1y_6 \\ y_4y_6 - y_2y_5 \\ y_5y_6 - y_3y_4 \end{bmatrix},$$

$$\rho_2 = \begin{bmatrix} y_5 & 0 & 0 & y_4 & y_1 & 0 \\ y_6 & 0 & 0 & y_2 & y_4 & 0 \\ 0 & y_4 & 0 & y_5 & 0 & y_1 \\ 0 & y_6 & 0 & y_3 & 0 & y_5 \\ 0 & 0 & y_4 & 0 & y_6 & y_2 \\ 0 & 0 & y_5 & 0 & y_3 & y_6 \\ y_3 & -y_2 & 0 & 0 & y_5 & -y_4 \\ y_3 & 0 & -y_1 & y_6 & 0 & -y_4 \end{bmatrix},$$

$$\rho_3 = \begin{bmatrix} y_6 & -y_5 & y_2 & 0 & -y_1 & 0 & y_4 & -y_4 \\ y_3 & 0 & y_6 & -y_4 & 0 & -y_1 & 0 & -y_5 \\ 0 & y_3 & 0 & -y_2 & y_5 & -y_4 & -y_6 & 0 \end{bmatrix}.$$

6.7 Example. (a) Let G be the group of order 2 and degree 4 generated by diag$(-1, -1, -1, -1)$. Then

$$F_G(\lambda) = \tfrac{1}{2}\left[(1-\lambda)^{-4} + (1+\lambda)^{-4}\right] = (1 + 6\lambda^2 + \lambda^4)(1-\lambda^2)^{-4}.$$

Moreover, R^G is minimally generated by the ten monomials x_ix_j with $1 \leqslant i \leqslant j \leqslant 4$. It follows from Proposition 6.4 that the Betti numbers of R^G (with respect to the above generators) are given by $(\beta_0, \beta_1, \ldots, \beta_6) = (1, 20, 64, 90, 64, 20, 1)$. For the algebraic significance of the symmetry $\beta_i = \beta_{6-i}$, see §8.

(b) Another group to which Proposition 6.4 applies is the group G of order 3 and degree 3 generated by diag (ω, ω, ω) where $\omega = e^{2\pi i/3}$. In this case $F_G(\lambda) = (1 + 7\lambda^3 + \lambda^6)(1 - \lambda^3)^{-3}$ and $(\beta_0, \ldots, \beta_7) = (1, 27, 105, 189, 189, 105, 27, 1)$.

Remark. Our discussion of minimal free resolutions of R^G applies equally well to the modules R_χ^G. The A-module structure of R^G gives R_χ^G the structure of an A-module, and we can define the minimal free resolution of R_χ^G (as an A-module) exactly as we did for R^G. Similarly the numbers $\beta_i(R_\chi^G)$ and hd R_χ^G can be defined. It follows from Theorem 3.7 and [Se$_2$, Chapter IV] that Theorem 6.2 extends to:

$$\mathrm{hd}_A\left(R_\chi^G\right) = s - m.$$

7. The canonical module. Let Λ be a finitely-generated free (right) module over the polynomial ring $A = k[y_1, \ldots, y_s]$. Let $\Lambda^* = \mathrm{Hom}_A(\Lambda, A)$, the set of all A-module homomorphisms $\Lambda \xrightarrow{\phi} A$. We regard ϕ as acting on the right. Then Λ^* has a natural A-module structure, given by $u(\phi + \phi') = u\phi + u\phi'$ and $u(\phi f) = (u\phi)f$ $(= (uf)\phi)$, where $u \in \Lambda$, $\phi \in \Lambda^*$, $\phi' \in \Lambda^*$, $f \in A$. If $u_1, \ldots, u_l$ is a basis for Λ, then Λ^* is a free A-module with basis $u_1^*, \ldots, u_l^*$ given by

$$u_j u_i^* = \begin{cases} 1, & i = j, \\ 0, & i \neq j. \end{cases}$$

(Since we have defined Λ^* to act on the right, $\mu_j \mu_i^*$ stands for the homomorphism μ_i^*: $\Lambda \to A$ evaluated at μ_j.) Let Λ_1 and Λ_2 be finitely-generated free A-modules, and let ρ: $\Lambda_1 \to \Lambda_2$ be an A-module homomorphism. Thus once we have fixed bases $u_1, \ldots, u_l$ of Λ_1 and $v_1, \ldots, v_q$ of Λ_2, we can represent ρ as an $l \times q$ matrix (operating on the right on row vectors of length l) with entries in A. We then have a homomorphism ρ^*: $\Lambda_2^* \to \Lambda_1^*$ given by $u(\phi\rho^*) = (u\rho)\phi$, where $\phi \in \Lambda_2^*$ and $u \in \Lambda_1$. The matrix of ρ^* with respect to the bases $v_1^*, \ldots, v_q^*$ and $u_1^*, \ldots, u_l^*$ is just the *transpose* of the matrix of ρ.

Now suppose that B is a Cohen-Macaulay $\mathbf{N}$-graded k-algebra, and let (17) be a minimal free resolution of B (with respect to some choice $\gamma_1, \ldots, \gamma_s$ of homogeneous generators, so $A = \mathbf{C}[y_1, \ldots, y_s]$). We may then "dualize" the entire resolution (17) by applying the operation (functor) *. If we assume for the present that $\gamma_1, \ldots, \gamma_s$ are not algebraically independent, i.e., $B \neq A$, then $\operatorname{Hom}_A(B, A) = 0$, so we obtain

$$0 \to M_0^* \xrightarrow{\rho_1^*} M_1^* \to \cdots \xrightarrow{\rho_h^*} M_h^* \to 0 \tag{19}$$

It is clear that (19) is a complex (i.e., $\rho_{i-1}^* \rho_i^* = 0$, since $(\rho_i \rho_{i-1})^* = \rho_{i-1}^* \rho_i^*$), but in general there is no reason to suppose that (19) is exact. However, it follows from a theorem of homological algebra (e.g., **[I**, §2.3**]**) that because B is Cohen-Macaulay, the complex (19) is exact except at M_h^*. Hence if we let $\Omega_A(B)$ denote the cokernel of ρ_h^* (i.e., $\Omega_A(B) = M_h^*/\rho_h^*(M_{h-1}^*)$), then the complex

$$0 \to M_0^* \xrightarrow{\rho_1^*} M_1^* \to \cdots \xrightarrow{\rho_h^*} M_h^* \to \Omega_A(B) \to 0 \tag{20}$$

is actually a minimal free resolution of the A-module $\Omega_A(B)$. The A-module $\Omega_A(B)$ is called the *canonical module* of B. (In the case $B = A$, we simply set $\Omega_A(A) = A$, although a uniform definition of $\Omega_A(B)$ could be given.) See **[H-K]** for a general discussion of canonical modules.

Although (20) *a priori* defines $\Omega_A(B)$ only as an A-module, it is easy to see that if $B = A/I$ then I is the annihilator of $\Omega_A(B)$. It follows that we may regard $\Omega_A(B)$ as a B-module. A theorem of homological algebra (e.g., **[H-K**, Satz 5.2**]**) implies that the B-module structure of $\Omega_A(B)$ depends only on the structure of B as a ring, not the choice $\gamma_1, \ldots, \gamma_s$ of generators defining A. Hence we write $\Omega(B)$ for $\Omega_A(B)$ regarded as a B-module.

The last nonvanishing Betti number $\beta_{s-m}^A(B)$ is equal to the minimal number of generators of $\Omega_A(B)$ as an A-module and hence also as a B-module. It follows that $\beta_{s-m}^A(B)$ depends only on B, not on A, and is called the *type* of B, denoted type B. This is an important numerical invariant of a Cohen-Macaulay $\mathbf{N}$-graded k-algebra B.

There is also an "internal" definition of $\Omega(B)$ which does not involve homological considerations. Let $\theta_1, \dots, \theta_m$ be an h.s.o.p. for B, and set $T = k[\theta_1, \dots, \theta_m]$, so $B = \amalg_1^t \eta_i T$ for some homogeneous $\eta_i \in B$. Since B is a free T-module of rank t, we have already seen that $\operatorname{Hom}_T(B, T)$ is also a free T-module of rank t, with basis $\eta_1^*, \dots, \eta_t^*$ given by $\eta_j\eta_i^* = \delta_{ij}$. We now make $\operatorname{Hom}_T(B, T)$ into a B-module by defining $g(\phi f) = (gf)\phi$ for $f \in B$, $\phi \in \operatorname{Hom}_T(B, T)$, and $g \in B$. It turns out that with this B-module structure, $\operatorname{Hom}_T(B, T)$ is isomorphic to the canonical module $\Omega(B)$ **[H-K**, Kor. 5.14]. It is by no means *a priori* evident that the B-module structure on $\operatorname{Hom}_T(B, T)$ is independent of the choice of an h.s.o.p., and it would be interesting to find a nonhomological proof of this fact. There is also an "internal" definition of the integer type B which is a simple consequence of the formulas $\Omega(B) \cong \operatorname{Hom}_T(B, T)$ and $\operatorname{Hom}_{T/T_+}(B/T_+, T/T_+) \cong (T/T_+) \otimes \operatorname{Hom}_T(B, T)$, where T_+ is the ideal of T generated by $\theta_1, \dots, \theta_m$. Namely, set $S = B/(\theta_1, \dots, \theta_m)$. Thus S is a finite-dimensional vector space with basis consisting of (the images of) $\eta_1, \dots, \eta_t$. The *socle* of S, denoted soc S, is by definition the ideal of S annihilated by all $f \in B$ of *positive* degree. It is then true that

$$\text{type } B = \dim_k \operatorname{soc} S. \tag{21}$$

We can now state the fundamental theorem which determines $\Omega(R^G)$. This result is implicit in the work of Watanabe **[Wat$_1$]**, **[Wat$_2$]** and was explicitly proved by D. Eisenbud (unpublished).

7.1 Theorem. *Let G be a finite subgroup of* $\mathrm{GL}(V)$, *and let σ be the linear character of G given by $\sigma(M) = (\det M)^{-1}$. Then $\Omega(R^G) \cong R_\sigma^G$.*

Although the proof of Theorem 7.1 is beyond the scope of this paper, we can give a simple "combinatorial" motivation for this result. An easy argument (see **[Sta$_2$**, equation (12)]) shows that when B is a Cohen-Macaulay $\mathbf{N}$-graded k-algebra of Krull dimension m, then $\Omega(B)$ has a natural $\mathbf{Z}$-grading which satisfies

$$F(\Omega(B), \lambda) = (-1)^m \lambda^q F(B, 1/\lambda) \tag{22}$$

(as rational functions) for some $q \in \mathbf{Z}$. If we compare (22) with Lemma 3.7, this certainly suggests that $\Omega(R^G) \cong R_\sigma^G$.

7.2 Example. Let G be the group of degree 2 and order 3 generated by $\operatorname{diag}(\omega, \omega)$ where $\omega = e^{2\pi i/3}$. Hence $R^G = \mathbf{C}[x^3, y^3, x^2y, xy^2] = \mathbf{C}[x^3, y^3](1 \oplus x^2y \oplus xy^2)$. We will compute $\Omega(R^G)$ in three different ways.

(a) According to Theorem 7.1, $\Omega(R^G) \cong \{f \in R\colon f(\omega x, \omega y) = \omega f(x, y)\}$. Thus $\Omega(R^G)$ has a $\mathbf{C}$-basis consisting of all monomials $x^a y^b$ with $a + b \equiv 1 \pmod 3$. It follows that $\Omega(R^G)$ is the R^G-submodule of R generated by x and y. We may write this as $\Omega(R^G) = xR^G + yR^G = \mathbf{C}[x^3, y^3](x \oplus y \oplus x^2y^2)$. Note that since $\Omega(R^G)$ has two generators, we have type $R^G = 2$. The ring $S = R^G/(x^3, y^3)$ has a $\mathbf{C}$-basis consisting of 1, x^2y, xy^2. The socle of S has the basis x^2y, xy^2, so indeed $\dim_{\mathbf{C}} \operatorname{soc} S = \text{type } R^G$.

(b) Letting $\gamma_1 = x^3$, $\gamma_2 = y^3$, $\gamma_3 = x^2y$, $\gamma_4 = xy^2$, so $A = \mathbf{C}[y_1, y_2, y_3, y_4]$, the minimal free resolution of R^G is

$$0 \rightarrow A^2 \xrightarrow[\begin{bmatrix} y_2 & y_3 & -y_4 \\ y_4 & y_1 & -y_3 \end{bmatrix}]{} A^3 \xrightarrow[\begin{bmatrix} y_1y_4-y_3^2 \\ y_2y_3-y_4^2 \\ y_1y_2-y_3y_4 \end{bmatrix}]{} A \rightarrow R^G \rightarrow 0.$$

Note that the "last" module has rank equal to $2 = \text{type } R^G$. Dualizing, we obtain the resolution

$$0 \rightarrow A \xrightarrow[[y_1y_4-y_3^2\, y_2y_3-y_4^2\, y_1y_2-y_3y_4]]{} A^3 \xrightarrow[\begin{bmatrix} y_2 & y_4 \\ y_3 & y_1 \\ -y_4 & -y_3 \end{bmatrix}]{} A^2 \rightarrow \Omega(R^G) \rightarrow 0.$$

Hence $\Omega(R^G) \cong A^2/J$, where J is the submodule of A^2 generated by (y_2, y_4), (y_3, y_1), and $(-y_4, -y_3)$. If we identify $(1, 0)$ with x and $(0, 1)$ with y, we obtain an isomorphism $\Omega(R^G) \cong R_\sigma^G$.

(c) Let $T = \mathbf{C}[x^3, y^3]$. Then $\Omega(R^G) \cong \operatorname{Hom}_T(R^G, T)$. As a T-module, $\operatorname{Hom}_T(R^G, T)$ has the basis $1^*, \gamma^*, \eta^*$ where $\gamma = xy^2$ and $\eta = x^2y$. The R^G-module structure of $\operatorname{Hom}_T(R^G, T)$ is given by

$$\begin{array}{lll} 1^*1 = 1^*, & 1^*\gamma = \eta^*x^3y^3, & 1^*\eta = \gamma^*x^3y^3, \\ \gamma^*1 = \gamma^*, & \gamma^*\gamma = 1^*, & \gamma^*\eta = \eta^*x^3, \\ \eta^*1 = \eta^*, & \eta^*\gamma = \gamma^*y^3, & \eta^*\eta = 1^*. \end{array}$$

(For instance, let us compute $\eta^*\gamma$. We have $1\eta^*\gamma = \gamma\eta^* = 0 = 1\gamma^*y^3$, $\gamma\eta^*\gamma = \gamma^2\eta^* = (x^2y^4)\eta^* = (x^2y)\eta^*y^3 = \eta\eta^*y^3 = y^3 = \gamma\gamma^*y^3$, $\eta\eta^*\gamma = (\eta\gamma)\eta^* = (x^3y^3)\eta^* = 1\eta^*x^3y^3 = 0 = \eta\gamma^*y^3$. Thus $f\eta^*\gamma = f\gamma^*y^3$ for all $f \in R^G$, so $\eta^*\gamma = \gamma^*y^3$.) Hence as an R^G-module, $\operatorname{Hom}_T(R^G, T)$ is generated by γ^* and η^* subject to the relations $\gamma^*\gamma = \eta^*\eta$, $\gamma^*\eta = \eta^*x^3$, $\eta^*\gamma = \gamma^*y^3$, which agrees with (b) above upon identifying $(1, 0)$ with γ^* and $(0, 1)$ with η^*.

REMARK. The definition and basic properties of $\Omega(R^G)$ extend without difficulty to $\Omega(R_\chi^G)$. The details are left to the reader. We simply remark that Theorem 7.1 extends to $\Omega(R_\chi^G) \cong R_{\chi\sigma}^G$.

8. Gorenstein rings. The Cohen-Macaulay $\mathbf{N}$-graded k-algebra B is said to be *Gorenstein* if type $B = 1$. Equivalently (since the annihilator of $\Omega(B)$ is I), B is Gorenstein if and only if $\Omega(B) \cong B$ (as B-modules). Hence the resolution (20) is a minimal free resolution of B. Since minimal free resolutions are unique, it follows that (17) and (20) coincide, in the sense that with the correct choice of bases for the modules M_i and M_j^*, the matrices ρ_i and ρ_{h-i+1}^* are identical, $1 \leqslant i \leqslant h$. We therefore say that the minimal free resolution of B is "self-dual." In particular, rank M_i = rank M_{h-i}^*, so we obtain the result that if B is Gorenstein, then

$$\beta_i^A(B) = \beta_{h-i}^A(B), \qquad 0 \leqslant i \leqslant h = s - m. \tag{23}$$

Note that since $1 = \beta_0^A(B)$, the condition $\beta_0^A(B) = \beta_h^A(B)$ is equivalent to our definition of Gorenstein, so the case $i = 0$ of (23) implies its validity for all i (assuming B is Cohen-Macaulay).

Since one can construct the Hilbert series $F(B, \lambda)$ from a finite free resolution of B *via* (18), one might suspect that the self-duality of (17) when B is Gorenstein would lead to a condition on $F(B, \lambda)$. Indeed, an easy argument (see [Sta$_2$, Theorem 4.1] for details) shows that when B is Gorenstein of

Krull dimension m, we have

$$F(B, 1/\lambda) = (-1)^m \lambda^l F(B, \lambda) \tag{24}$$

(as rational functions) for some $l \in \mathbf{Z}$. (In fact, (24) is a special case of (22).) Equation (24) may be restated in terms of the decomposition $B = \amalg_1^t \eta_i k[\theta_1, \ldots, \theta_m]$ as follows. Let $d_i = \deg \theta_i$ and $e_i = \deg \eta_i$, with $0 = e_1 \leqslant e_2 \leqslant \cdots \leqslant e_t$. Then

$$e_i + e_{t+1-i} = e_t, \qquad 1 \leqslant i \leqslant t.$$

Equivalently, the polynomial

$$P(\lambda) = F(B, \lambda) \prod_1^m (1 - \lambda^{d_i}) = \sum_i \lambda^{e_i}$$

satisfies $P(\lambda) = \lambda^{e_t} P(1/\lambda)$. In [Sta$_2$, Theorem 5.5], it was shown that the necessary condition (24) for B to be Gorenstein is also *sufficient*, under the assumption that B is a Cohen-Macaulay domain.

Now consider the case $B = R^G$, where G is a finite subgroup of $\mathrm{GL}(V)$. Since R^G is a Cohen-Macaulay domain, it follows that (24) is equivalent to R^G being Gorenstein. If we express $F_G(\lambda)$ by Molien's theorem (Theorem 2.1) and expand both sides of (24) in a Laurent expansion about $\lambda = 1$, then analogously to Lemma 4.2 we obtain that $l = m + r$, where $m = \dim V$ and r is the number of pseudo-reflections in G. In [Sta$_1$, Corollary 2.4] another condition was given for R^G to be Gorenstein, based on the fact that Theorem 7.1 implies that R^G is Gorenstein if and only if $R_\sigma^G = f_\sigma \cdot R^G$ for some $f_\sigma \in R$, where $\sigma = \det^{-1}$. These results are summarized by the next theorem.

8.1 THEOREM. *Let G be a finite subgroup of* $\mathrm{GL}(V)$. *Let σ be the character $\sigma(M) = (\det M)^{-1}$. Let $\mathcal{H}_1, \ldots, \mathcal{H}_\nu$ be a reflecting hyperplane in V, and define the linear form $L_{\mathcal{H}} \in R$ by $\mathcal{H} = \{\alpha \in V\colon L_{\mathcal{H}}(\alpha) = 0\}$. Let $c_{\mathcal{H}}$ be the order of the* (*cyclic*) *subgroup of G which fixes $\mathcal{H}$ pointwise, and define $f_\chi = \amalg_{\mathcal{H}} L_{\mathcal{H}}^{c_{\mathcal{H}}-1}$ the product being over all reflecting hyperplanes $\mathcal{H}$ in V.* (*This definition agrees with the one preceding Proposition* 4.7 *when $\chi = \det^{-1}$.*) *Then the following three conditions are equivalent.*

(i) *R^G is Gorenstein.*

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

where r is the number of pseudo-reflections in G.

(iii) *$f_\sigma \in R_\sigma^G$* (*in which case we have $R_\sigma^G = f_\sigma \cdot R^G$*). □

8.2 COROLLARY (WATANABE [Wat$_1$]). *If $G \subset \mathrm{SL}(V)$* (*i.e.*, $\det M = 1$ *for all $M \in G$*), *then R^G is Gorenstein.*

PROOF. If $G \subset \mathrm{SL}(V)$, then $r = 0$ and (ii) clearly holds. (This corollary also follows immediately from Theorem 7.1.) □

8.3 COROLLARY (WATANABE [Wat$_2$]). *If $r = 0$ and R^G is Gorenstein, then $G \subset \mathrm{SL}(V)$.*

PROOF. We know that (ii) holds with $r = 0$. Set $\lambda = 0$ to obtain $g = \sum_{M \in G} \det M$. Since each $\det M$ is a root of unity, we must have $\det M = 1$.

(One can also give a proof using part (iii) of Theorem 8.1, since we have $f_\sigma = 1$.) □

8.4 Example. Let G be the group of degree 3 and order 6 generated by diag$(\omega, -\omega^2, -1)$, where $\omega = e^{2\pi i/3}$. By Corollary 8.2, R^G is Gorenstein. Writing $x = x_1, y = x_2, z = x_3$, a minimal set of generators for R^G consists of $\gamma_1 = x^3$, $\gamma_2 = y^6$, $\gamma_3 = z^2$, $\gamma_4 = y^3z$, $\gamma_5 = xyz$, $\gamma_6 = xy^4$, $\gamma_7 = x^2y^2$. Hence hd $R^G = 7 - 3 = 4$. By a process of trial and error, the syzygies of the first kind are computed to be $\gamma_4^2 - \gamma_2\gamma_3$, $\gamma_5^2 - \gamma_3\gamma_7$, $\gamma_6^2 - \gamma_2\gamma_7$ $\gamma_7^2 - \gamma_1\gamma_6$, $\gamma_4\gamma_5 - \gamma_3\gamma_6$, $\gamma_4\gamma_6 - \gamma_2\gamma_5$, $\gamma_4\gamma_7 - \gamma_5\gamma_6$, $\gamma_6\gamma_7 - \gamma_1\gamma_2$, $\gamma_5\gamma_7 - \gamma_1\gamma_4$. Hence $\beta_1(R^G) = 9$. Since $\beta_i(R^G) = \beta_{4-i}(R^G)$ and $\beta_0 - \beta_1 + \beta_2 - \beta_3 + \beta_4 = 0$, it follows that $\beta_0 = 1$, $\beta_1 = 9$, $\beta_2 = 16$, $\beta_3 = 9$, $\beta_4 = 1$. One could also obtain this result from a suitable modification of Proposition 6.4.

It is instructive to derive Corollary 8.2 when G is abelian directly from (21). Assume G is diagonal, so we have an h.s.o.p. of the form $x_1^{d_1}, x_2^{d_2}, \ldots, x_m^{d_m}$. If $G \subset SL(V)$, it follows that $x_1^{d_1-1}x_2^{d_2-1} \ldots x_m^{d_m-1} \in R^G$. From this it is clear that the socle of $R^G/(x_1^{d_1}, \ldots, x_m^{d_m})$ is spanned as a vector space by $x_1^{d_1-1}x_2^{d_2-1} \ldots x_m^{d_m-1}$. Hence by (21), type $R^G = 1$, so R^G is Gorenstein.

9. Complete intersections. There is a condition on R^G stronger than being Gorenstein which implies that the minimal free resolution of R^G has a simple explicit form. This is the condition of being a "complete intersection" and is defined as follows. Let $\gamma_1, \ldots, \gamma_s$ be homogeneous generators of positive degree for the $\mathbf{N}$-graded algebra B, so $B = A/I$ where $A = k[y_1, \ldots, y_s]$ and γ_i is the image of y_i. A simple result of commutative algebra (e.g., [Se$_2$, p. III-11, Proposition 6]) implies that

$$m \geqslant s - \beta_1^A(B). \tag{25}$$

Note that $\beta_1^A(B)$ is the minimal number of generators of the ideal I. Hence (25) states that in order to reduce the Krull dimension of A from s to m, we must divide out by at least $s - m$ elements. If equality holds in (25), then we say that B is a *complete intersection*. It is not hard to show that the property of being a complete intersection does not depend on the choice of A (i.e., on $\gamma_1, \ldots, \gamma_s$) and thus is a property of B alone.

Now let $\rho_0\colon A \twoheadrightarrow B$ be the canonical surjection and let $z_1, \ldots, z_\beta$ be a minimal set of generators for ker ρ_0, so $\beta = \beta_1^A(B)$. Define a sequence

$$0 \to M_\beta \xrightarrow{\rho_\beta} \cdots \to M_3 \xrightarrow{\rho_3} M_2 \xrightarrow{\rho_2} M_1 \xrightarrow{\rho_1} M_0 \xrightarrow{\rho_0} B \to 0, \tag{26}$$

where M_i is a free A-module of rank $\binom{\beta}{i}$ with basis $\{S\colon S \subset [\beta]$ and card $S = i\}$ (so in particular $M_0 \cong A$). The maps $\rho_i\colon M_i \to M_{i-1}$ for $1 \leqslant i \leqslant \beta$ are defined by

$$\rho_i(\{a_1, \ldots, a_i\}) = \sum_{j=1}^{i} (-1)^{j+1} z_j \{a_1, \ldots, \hat{a}_j, \ldots, a_i\},$$

where $a_1 < \cdots < a_i$ and $\hat{a}_j$ denotes that a_j is missing. It is easily checked by direct calculation that (26) is a complex (i.e., $\rho_i\rho_{i-1} = 0$), called the *Koszul complex* of B with respect to the generators $z_1, \ldots, z_\beta$ of I. By definition the entries of the matrices ρ_i are 0 or $\pm z_j$, so if (26) is a resolution it is minimal.

By the definition of a complete intersection, a necessary condition for (26) to be exact is that B is a complete intersection. It follows from standard properties of the Koszul complex (e.g., [**Se**$_2$, Chapter IV(A)]) that the converse is true.

9.1 PROPOSITION. *B is a complete intersection if and only if the Koszul complex* (26) *is the minimal free resolution of B.* □

Note that Proposition 9.1 immediately implies that if B is a complete intersection, then $\mathrm{hd}_A(B) = \beta = s - \dim B$, so B is Cohen-Macaulay. We then see from Proposition 9.1 that type $B = 1$, so B is in fact Gorenstein. Examples of Gorenstein rings R^G which are not complete intersections are given in Examples 6.7 and 8.4.

As a further corollary, we can explicitly compute the Hilbert series of the complete intersection B. In order for the maps ρ_i in (26) to be degree-preserving, the basis elements S of M_i must satisfy

$$\deg S = \sum_{j \in S} e_j,$$

where $e_1, \dots, e_\beta$ are the degrees of the syzygies of the first kind, i.e., $e_j = \deg z_j$. Hence from (18) we obtain, with $d_i = \deg \gamma_i$,

$$F(B, \lambda) = \left[\sum_{S \subset [\beta]} (-1)^{\operatorname{card} S} \lambda^{\deg S} \right] \prod_1^s (1 - \lambda^{d_i})^{-1}$$

$$= \left[\prod_1^\beta (1 - \lambda^{e_i}) \right] \prod_1^s (1 - \lambda^{d_i})^{-1}. \tag{27}$$

(For a direct proof of (27) avoiding Proposition 9.1, see [**Sta**$_2$, Corollary 3.3].) We thus obtain a necessary (but not sufficient) condition for B to be a complete intersection–it must be possible to write $F(B, \lambda)$ in the form (27). In particular, when $F(B, \lambda)$ is reduced to lowest terms, then every zero of the numerator must be a root of unity.

9.2 EXAMPLE. Let G be the group of degree 3 and order 12 generated by $\operatorname{diag}(-1, \zeta, \zeta^2)$ and $\operatorname{diag}(-1, 1, -1)$, where $\zeta = e^{2\pi i/6}$. Then R^G is minimally generated by $\gamma_1 = x_1^2$, $\gamma_2 = x_2^6$, $\gamma_3 = x_3^6$, $\gamma_4 = x_2^2 x_3^2$, $\gamma_5 = x_1 x_2 x_3$. The syzygies are $\gamma_2\gamma_3 - \gamma_4^3$ and $\gamma_1\gamma_4 - \gamma_5^2$. Since there are $s - m = 5 - 3 = 2$ syzygies, it follows that R^G is a complete intersection. The minimal free resolution is given by

$$0 \to A \xrightarrow[{[-z_2\, z_1]}]{} A^2 \xrightarrow[{\begin{bmatrix} z_1 \\ z_2 \end{bmatrix}}]{} A \to R^G \to 0,$$

where $z_1 = y_2 y_3 - y_4^3$ and $z_2 = y_1 y_4 - y_5^2$. Since $\deg \gamma_1 = 2$, $\deg \gamma_2 = \deg \gamma_3 = 6$, $\deg \gamma_4 = 4$, $\deg \gamma_5 = 3$, $\deg z_1 = 12$, $\deg z_2 = 6$, it follows that

$$F_G(\lambda) = \frac{(1 - \lambda^6)(1 - \lambda^{12})}{(1 - \lambda^2)(1 - \lambda^6)^2 (1 - \lambda^4)(1 - \lambda^3)}.$$

Since G is a diagonal group, we can just as easily write down the generalized

Molien series (16), viz.,

$$F_G(\lambda) = \frac{(1-\lambda_1^2\lambda_2^2\lambda_3^2)(1-\lambda_2^6\lambda_3^6)}{(1-\lambda_1^2)(1-\lambda_2^6)(1-\lambda_3^6)(1-\lambda_2^2\lambda_3^2)(1-\lambda_1\lambda_2\lambda_3)}.$$

9.3 Example. As a somewhat more complicated example, let G be the group of degree 4 and order 32 generated by diag $(i, -i, 1, 1)$, diag $(1, 1, i, -i)$, and diag $(-1, 1, 1, -1)$. The generators are $\gamma_1 = x_1^4$, $\gamma_2 = x_2^4$, $\gamma_3 = x_3^4$, $\gamma_4 = x_4^4$, $\gamma_5 = x_1^2x_2^2$, $\gamma_6 = x_1x_2x_3x_4$, $\gamma_7 = x_3^2x_4^2$. Thus $R^G = A/I$ where $A = \mathbf{C}[y_1, \ldots, y_7]$. The ideal I is generated by $z_1 = y_5^2 - y_1y_2$, $z_2 = y_7^2 - y_3y_4$, $z_3 = y_6^2 - y_5y_7$. Since $7 - 4 = 3$, it follows that R^G is a complete intersection. The minimal free resolution is

$$0 \to A \xrightarrow[{[z_1\ -z_2\ z_3]}]{} A^3 \xrightarrow[{\begin{bmatrix} 0 & z_3 & -z_2 \\ z_3 & 0 & -z_1 \\ z_2 & -z_1 & 0 \end{bmatrix}}]{} A^3 \xrightarrow[{\begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix}}]{} A \to R^G \to 0,$$

and the Molien series is

$$F_G(\lambda) = \frac{(1-\lambda^8)^3}{(1-\lambda^4)^7} = \frac{(1+\lambda^4)^3}{(1-\lambda^4)^4}.$$

The generalized Molien series (16) is

$$F_G(\lambda) = \frac{(1+\lambda_1^2\lambda_2^2)(1+\lambda_3^2\lambda_4^2)(1+\lambda_1\lambda_2\lambda_3\lambda_4)}{(1-\lambda_1^4)(1-\lambda_2^4)(1-\lambda_3^4)(1-\lambda_4^4)}.$$

The simplest type of complete intersection (except for the "degenerate" case of a polynomial ring) is the case $s - m = 1$. This condition can only hold (assuming B is not a polynomial ring) when $\gamma_1, \ldots, \gamma_s$ are chosen to be *minimal* generators of B and therefore is equivalent to $\beta_1(B) = 1$ (or hd $B = 1$). In other words, there must be a *unique* minimal syzygy (up to scalar multiples) among the minimal generators of B. If B satisfies this condition it is called a *hypersurface*. A particularly nice structure arises when we can choose the generators $\gamma_1, \ldots, \gamma_s$ $(s = m + 1)$ so that the unique minimal syzygy has the form $\gamma_s^t = P(\gamma_1, \ldots, \gamma_s)$ where $t \geqslant 2$ and P is a polynomial in $\gamma_1, \ldots, \gamma_s$. In this case $\gamma_1, \ldots, \gamma_{s-1}$ is an h.s.o.p. and $B = \mathbf{C}[\gamma_1, \ldots, \gamma_{s-1}] \cdot (1 \oplus \gamma_s \oplus \gamma_s^2 + \cdots \oplus \gamma_s^{t-1})$. This was the situation in Example 5.1.

We now have a hierarchy of conditions,

$$\text{polynomial ring} \Rightarrow \text{hypersurface} \Rightarrow \text{complete intersection}$$
$$\Rightarrow \text{Gorenstein} \Rightarrow \text{Cohen-Macaulay}.$$

We have given necessary and sufficient conditions on G for the first, fourth, or fifth condition to hold for R^G. No such characterizations are known for hypersurfaces or complete intersections, and this remains one of the outstanding gaps in the invariant theory of finite groups. Along these lines we present the following conjecture, admittedly made on the basis of very flimsy evidence.

Conjecture. If R^G is a complete intersection, then $H' \subset G \subset H$, where H is an f.g.g.r. and H' is the commutator subgroup of H.

There are two known classes of finite groups $G \subset \mathrm{GL}(V)$ for which R^G is a complete intersection. First we give the result implicit in **[M-B-D]** (see **[Hu]** for a clearer treatment). I am grateful to Cary Huffman for checking that this result is consistent with the above conjecture.

9.4 Proposition. *Let $m = \dim V = 2$ and suppose that G is a finite subgroup of* $\mathrm{SL}(V)$. *Then R^G is a complete intersection.* □

In **[Sta$_1$]** a characterization was given of those f.g.g.r.'s $G \subset \mathrm{GL}(V)$ for which R^H is a complete intersection, where $H = G \cap \mathrm{SL}(V)$. We will merely state a special case of this characterization here. The motivation comes from the case where G consists of all $m \times m$ permutation matrices. Then R^H is generated by all symmetric and alternating polynomials $f(x_1, \ldots, x_m) \in R$. We have pointed out following Proposition 4.8 that every alternating polynomial is a product of a symmetric polynomial with the *discriminant* $\Delta = \prod_{i<j}(x_i - x_j)$. Hence R^H is generated by the elementary symmetric functions $a_1, \ldots, a_m$ together with Δ, subject to the syzygy $\Delta^2 = P(a_1, \ldots, a_m)$ for some polynomial P. Hence R^H is a hypersurface, and in fact $R^H = \mathbf{C}[a_1, \ldots, a_m](1 \oplus \Delta)$.

9.5 Proposition. *Suppose $H = G \cap \mathrm{SL}(V)$, where $G \subset \mathrm{GL}(V)$ is an f.g.g.r. If the index $[G : H]$ is a prime power, then R^H is a complete intersection. If $[G : H]$ is a prime p, then R^H is a hypersurface; indeed, if $R^G = \mathbf{C}[\theta_1, \ldots, \theta_m]$ and $\eta = f_\chi$ for the character $\chi = \det$ (as defined preceding Proposition* 4.7), *then $R^H = \mathbf{C}[\theta_1, \ldots, \theta_m](1 \oplus \eta \oplus \eta^2 \oplus \cdots \oplus \eta^{p-1})$.* □

10. Monomial groups. In Example 5.3 we considered the situation where $V = V_1 \oplus \cdots \oplus V_l$ and $M(V_i) = V_i$ for all $M \in G$. More generally we could consider the situation where each $M \in G$ permutes the V_i's, i.e., for each $M \in G$ there is a permutation $\pi = \pi_M$ of $[l]$ such that $M(V_i) = V_{\pi(i)}$. For simplicity's sake we will consider only the case where each $\dim V_i = 1$ (so $l = m$). If in this case x_i is a nonzero element of V_i, then the matrix of M with respect to the basis $x_1, \ldots, x_m$ of V is a *monomial matrix*, i.e., a matrix with one nonzero entry in every row and column. A group G of monomial matrices is called a *monomial group*. The map $M \to \pi_M$ defines a homomorphism from G to the group $\mathfrak{S}_m$ of all permutations of $[m]$.

Suppose $G \subset \mathrm{GL}(V)$ is a monomial group (with respect to the basis $x_1, \ldots, x_m$). If $M \in G$, then let C be a cycle of the permutation π_M, so $C = (a_1, \ldots, a_l)$ where $\{a_1, \ldots, a_l\} \subset [m]$ and $\pi_M(a_i) = a_{i+1}$ $(1 \leqslant i \leqslant l - 1)$, $\pi_M(a_l) = a_1$. It follows that there are nonzero complex numbers $\alpha_1, \ldots, \alpha_l$ such that $M(x_{a_i}) = \alpha_i x_{a_{i+1}}$ $(1 \leqslant i \leqslant l - 1)$ and $M(x_{a_l}) = \alpha_l x_{a_1}$. Define the complex number $\gamma_M(C)$ by $\gamma_M(C) = \alpha_1 \alpha_2 \ldots \alpha_l$, and define $|C| = l$.

If $f = x_1^{n_1} x_2^{n_2} \ldots x_m^{n_m}$ is a monomial, then the *type* of f is defined to be the sequence $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \ldots)$ where exactly σ_i of the n_j's are equal to i. Let $R_{\boldsymbol{\sigma}}$ be the subspace of $R = \mathbf{C}[x_1, \ldots, x_m]$ spanned by all monomials of type $\boldsymbol{\sigma}$. Clearly a monomial matrix M transforms a monomial of type $\boldsymbol{\sigma}$ into a scalar multiple of another such monomial. Hence $MR_{\boldsymbol{\sigma}} = R_{\boldsymbol{\sigma}}$, so $R^G = \coprod_{\boldsymbol{\sigma}} R^G_{\boldsymbol{\sigma}}$

where $R_\sigma^G = R^G \cap R_\sigma$. (Note that the decomposition $\amalg_\sigma R_\sigma^G$ only gives R^G the structure of a graded vector space and not a graded algebra, since $R_\sigma^G R_\tau^G$ is not in general contained in any R_ω^G.) It is natural to ask at this point for an analogue of Molien's theorem which tells us the integers $\dim_{\mathbf{C}} R_\sigma^G$. More concretely, we seek a formula for the generating function $L_G(\lambda)$ in infinitely many variables $\lambda = (\lambda_1, \lambda_2, \ldots)$ defined by

$$L_G(\lambda) = \sum_\sigma (\dim_{\mathbf{C}} R_\sigma^G)\lambda^\sigma,$$

where $\sigma = (\sigma_1, \sigma_2, \ldots)$ ranges over all possible types and where $\lambda^\sigma = \lambda_1^{\sigma_1}\lambda_2^{\sigma_2}\ldots$. We do not expect as simple a formula for $L(G, \lambda)$ as (13), since the grading $\amalg_\sigma R_\sigma^G$ is not "induced" from a grading of V.

10.1 Theorem. *Let $G \subset \mathrm{GL}(V)$ be a finite monomial group (with respect to a basis $x_1, \ldots, x_m$ of V) of order g. Then*

$$L_G(\lambda) = \frac{1}{g} \sum_{M \in G} \prod_C \left(1 + \gamma_M(C)\lambda_1^{|C|} + \lambda_M(C)^2\lambda_2^{|C|} + \gamma_M(C)^3\lambda_3^{|C|} + \cdots\right),$$

where C ranges over all cycles of π_M.

Proof. If $M \in G$, then let $C_1, C_2, \ldots, C_s$ be the cycles of π_M. As mentioned above, each such cycle C has the form $C = (a_1, \ldots, a_l)$ where $\pi_M(a_i) = a_{i+1}$ $(1 \leqslant i \leqslant l-1)$ and $\pi_M(a_l) = a_1$. Moreover, $M(x_{a_i}) = \alpha_i x_{a_{i+1}}$ $(1 \leqslant i \leqslant l-1)$ and $M(x_{a_l}) = \alpha_l x_{a_1}$, with $\gamma_M(C) = \alpha_1\alpha_2 \ldots \alpha_l$. Now consider the vector space R_σ in R spanned by all monomials of a given type σ. The matrix M_σ of M acting on R_σ with respect to this basis of monomials is a monomial matrix. To compute its trace we need only consider monomials $u \in R_\sigma$ for which $M(u) = \alpha u$ for some $\alpha \in \mathbf{C}$. (Only these monomials will give rise to nonzero entries on the main diagonal of M_σ.) Such a monomial has the form

$$u = \prod_{i=1}^{s}\left(\prod_{j \in C_i} x_j\right)^{t_i}$$

for some $t_i \in \mathbf{N}$. We then have $Mu = [\prod_{i=1}^{s} \gamma_M(C_i)^{t_i}]u$. Hence

$$\operatorname{tr} M_\sigma = \sum \prod_{i=1}^{s} \gamma_M(C_i)^{t_i},$$

where the sum ranges over all sequences $(t_1, t_2, \ldots, t_s)$ such that among a collection of $|C_1|$ t_1's, $|C_2|$ t_2's, $\ldots$, $|C_s|$ t_s's, there are precisely σ_1 1's, σ_2 2's, $\ldots$. This is precisely the coefficient of $\lambda_1^{\sigma_1}\lambda_2^{\sigma_2}\ldots$ in the expansion of

$$\prod_{i=1}^{s}\left(1 + \gamma_M(C_i)\lambda_1^{|C_i|} + \gamma_M(C_i)^2\gamma_2^{|C_i|} + \cdots\right),$$

and the proof follows from (2). □

Although Theorem 10.1 is apparently new, it is actually a very minor extension of the well-known Theorem 10.3 below. Moreover, the techniques of Solomon [So$_2$] also lead quickly to the statement and proof of Theorem 10.1.

10.2 Example. The group $G = \{1, M, M^2, M^3\}$ of Example 2.2 is monomial. The four terms of $L_G(\lambda)$ are:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} : (1 + \lambda_1 + \lambda_2 + \lambda_3 + \cdots)^2,$$

$$M = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} : (1 - \lambda_1^2 + \lambda_2^2 - \lambda_3^2 + \cdots),$$

$$M^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} : (1 - \lambda_1 + \lambda_2 - \lambda_3 + \cdots)^2$$

$$M^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} : (1 - \lambda_1^2 + \lambda_2^2 - \lambda_3^2 + \cdots).$$

Thus we have

$$\begin{aligned} L_G(\lambda) &= \tfrac{1}{4}\big[(1 + \lambda_1 + \lambda_2 + \lambda_3 + \cdots)^2 \\ &\quad + (1 - \lambda_1 + \lambda_2 - \cdots)^2 + 2(1 - \lambda_1^2 + \lambda_2^2 - \cdots)\big] \\ &= 1 + \sum_{i=1}^{\infty} \lambda_{2i} + \sum_{i=1}^{\infty} \lambda_{2i}^2 + \sum_{\substack{1 \leqslant i < j \\ i \equiv j \ (\mathrm{mod}\ 2)}} \lambda_i \lambda_j. \end{aligned} \tag{28}$$

It is easily seen that the term λ_{2i} in (28) corresponds to the invariant $x_1^{2i} + x_2^{2i}$, the term λ_{2i}^2 corresponds to $x_1^{2i}x_2^{2i}$, while the term $\lambda_i\lambda_j$ corresponds to $x_1^i x_2^j + x_1^j x_2^i$ if i and j are even, and to $x_1^i x_2^j - x_1^j x_2^i$ if i and j are odd.

A special class of monomial groups are the *permutation groups*, i.e., subgroups of the group of all $m \times m$ permutation matrices. In this case the homomorphism $M \to \pi_M$ is one-to-one. If $\mathcal{F}$ is the set of all functions f: $[m] \to \mathbf{N}$, then M induces a permutation $\mathcal{F} \to \mathcal{F}$, also denoted M, by the rule $(Mf)(i) = f(\pi_M(i))$. We can identify a function f: $[m] \to \mathbf{N}$ with the monomial $\mathbf{x}^f = x_1^{f(1)} \ldots x_m^{f(m)}$. Under this identification, the usual action of M on $R = \mathbf{C}[x_1, \ldots, x_m]$ satisfies $M(\mathbf{x}^f) = \mathbf{x}^{M^{-1}f}$.

Call two functions f, g, $\in \mathcal{F}$ *equivalent* (denoted $f \sim g$) if $f = Mg$ for some $M \in G$. Clearly, this defines an equivalence relation; the equivalence classes are called *patterns*. If f and g are equivalent, then the set (including repetitions) of values $f(1), \ldots, f(m)$ is identical to the set $g(1), \ldots, g(m)$. In other words $\mathbf{x}^f$ and $\mathbf{x}^g$ have the same *type*, as defined in our discussion of monomial groups. Thus we can speak of the *type* of a pattern. A fundamental question of enumeration asks for the number of patterns of a given type $\boldsymbol{\sigma}$. If E is a pattern of type $\boldsymbol{\sigma}$, then $\delta_E = \sum_{f \in E} \mathbf{x}^f$ is an invariant of G belonging to $R_{\boldsymbol{\sigma}}^G$ and it is easily seen that the δ_E's form a basis for $R_{\boldsymbol{\sigma}}^G$ as E ranges over all patterns of type $\boldsymbol{\sigma}$. Hence Theorem 10.1 tells us the number of patterns of type $\boldsymbol{\sigma}$, as follows.

10.3 Theorem (Pólya). *Let G be a permutation group of degree m and order g. Let $d(\boldsymbol{\sigma})$ be the number of patterns of mappings f: $[m] \to \mathbf{N}$ of type $\boldsymbol{\sigma}$. Define*

$$F_G(\lambda) = \sum_{\boldsymbol{\sigma}} d(\boldsymbol{\sigma})\lambda^{\boldsymbol{\sigma}}.$$

Then

$$F_G(\lambda) = \frac{1}{g} \sum_{M \in G} \prod_{C} (1 + \lambda_1^{|C|} + \lambda_2^{|C|} + \lambda_3^{|C|} + \cdots),$$

where C ranges over all cycles of the permutation π_M. □

Readers familiar with Pólya's enumeration theorem have doubtlessly recognized before now that Theorem 10.3 is just a restatement of this famous result and that Theorem 10.1 is a straightforward generalization. Pólya's theorem, originally given by Pólya in **[P]**, has been discussed in many places, of which **[dB]**, **[Com]**, **[Ri]** are a sample. In particular, Redfield **[Re]** is now realized to have anticipated Pólya's theorem prior to Pólya.

ACKNOWLEDGEMENT. I am grateful to Neil Sloane for his careful reading of an earlier version of this paper and for his many helpful comments and suggestions.

REFERENCES

[A-F]. G. Almkvist and R. Fossum, *Decompositions of exterior and symmetric powers of indecomposable* $\mathbf{Z}/p\mathbf{Z}$*-modules in characteristic p and relations to invariants*, Københavns Universitet, Matematisk Institut, Preprint Series no. 19, 1977.

[An] G. Andrews, *The theory of partitions*, Encyclopedia of Mathematics and its Applications (G.-C. Rota, ed.), vol. 2, Addison-Wesley, Reading, Mass., 1976.

[A-M] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, Reading, Mass., 1969.

[B-L] W. M. Beynon and G. Lusztig, *Some numerical results on the characters of exceptional Weyl groups*, Math. Proc. Cambridge Philos. Soc. **84** (1978), 417–426.

[B-M-S] E. R. Berlekamp, F. J. MacWilliams and N. J.·A. Sloane, *Gleason's theorem on self-dual codes*, IEEE Trans. Info. Theory **18** (1972), 409–414.

[Bo] N. Bourbaki, *Groupes et algèbres de Lie*, Ch. 4, 5 et 6, Eléments de Mathématique, Fasc. XXXIV, Hermann, Paris, 1968.

[dB] N. G. deBruijn, *Pólya's theory of counting*, Applied Combinatorial Mathematics (E. F. Beckenbach, ed.), Wiley, New York, 1964, pp. 144–184.

[Bu] W. Burnside, *Theory of groups of finite order*, 2nd ed., Cambridge Univ. Press, 1911; reprinted, Dover, New York, 1955.

[Ch] C. Chevalley, *Invariants of finite groups generated by reflections*, Amer. J. Math. **67** (1955), 778–782.

[Coh] A. M. Cohen, *Finite complex reflection groups*, Ann. Sci. École Norm. Sup. **9** (1976), 379–436.

[Com] L. Comtet, *Advanced combinatorics*, Reidel, Dordrecht and Boston, Mass., 1974.

[C-R] C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Wiley, New York, 1962.

[F] L. Flatto, *Invariants of finite reflection groups* (to appear).

[G] B. Gordon, *Two theorems on multipartite partitions*, J. London Math. Soc. **38** (1963), 459–464.

[G-G] A. M. Garsia and I. Gessel, *Permutation statistics and partitions*, Advances in Math. (to appear).

[He] J. C. Hemperly, *Problem* E2442, Amer. Math. Monthly **80** (1973), 1058; *solution*, **81** (1974), 1031–1033.

[H-K] J. Herzog and E. Kunz, ed., *Der kanonische Modul eines Cohen-Macaulay-rings*, Lecture Notes in Math., vol. 238, Springer-Verlag, Berlin, 1971.

[Hi] D. Hilbert, *Ueber die Theorie der Algebraischen Formen*, Math. Ann. **36** (1890), 473–534.

[H-E] 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.

[Hu] W. C. Huffman, *Polynomial invariants of finite linear groups of degree two* (preprint).

[I] F. Ischebeck, *Eine Dualität zwischen den Funktoren* Ext *und* Tor, J. Algebra **11** (1969), 510–531.

[J-B$_1$] M. V. Jarić and J. L. Birman, *New algorithms for the Molien function*, J. Math. Physics **18** (1977), 1456–1458.

[J-B$_2$] ______, *Calculation of the Molien generating function for invariants of space groups*, J. Math. Physics **18** (1977), 1459–1464.

[Mc] F. J. MacWilliams, *A theorem on the distribution of weights in a systematic code*, Bell System Tech. J. **42** (1963), 79–84.

[M-M-S] F. J. MacWilliams, C. L. Mallows and N. J. A. Sloane, *Generalization of Gleason's theorem on weight enumerators of self-dual codes*, IEEE Trans. Info. Theory **18** (1972), 794–805.

[M-S] C. L. Mallows and N. J. A. Sloane, *On the invariants of a linear group of order* 336, Proc. Cambridge Philos. Soc. **74** (1973), 435–440.

[M-B-D] G. A. Miller, H. F. Blichfeldt and L. E. Dickson, *Theory and application of finite groups*, Dover, New York, 1961.

[Mo] T. Molien, *Über die Invarianten der linearen Substitutionsgruppe*, Sitzungsber. König. Preuss. Akad. Wiss. (1897), 1152–1156.

[P] G. Pólya, *Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen*, Acta Math. **68** (1937), 145–254.

[P-S-W] J. Patera, R. T. Sharp and P. Winternitz, *Polynomial irreducible tensors for point groups*, J. Math. Phys. **19** (1978), 2362–2376.

[Re] J. H. Redfield, *The theory of group-reduced distributions*, Amer. J. Math. **49** (1927), 433–455.

[Ri] J. Riordan, *An introduction to combinatorial analysis*, Wiley, New York, 1958.

[Ry] H. J. Ryser, *Combinatorial mathematics*, Carus Math. Monographs, No. 14, Math. Assoc. Amer., Wiley, New York, 1963.

[Se$_1$] J.-P. Serre, *Groupes finis d'auomorphisms d'anneaux locaux régulieres*, Colloq. d'Algèbre, (Paris, 1967), Secrétariat mathématique, Paris, 1968.

[Se$_2$] ______, *Algèbre locale-multiplicitiés*, Lecture Notes in Math., vol. 11, Springer-Verlag Berlin, 1965.

[S-T] G. C. Shephard and J. A. Todd, *Finite unitary reflection groups*, Canad. J. Math. **6** (1954), 274–304.

[Sl] N. J. A. Sloane, *Error-correcting codes and invariant theory: New applications of a nineteenth-century technique*, Amer. Math. Monthly **84** (1977), 82–107.

[Sm] W. Smoke, *Dimension and multiplicity for graded algebras*, J. Algebra **21** (1972), 149–173.

[So$_1$] L. Solomon, *Invariants of finite reflection groups*, Nagoya Math. J. **22** (1963), 57–64.

[So$_2$] ______, *Partition identities and invariants of finite groups*, J. Combinatorial Theory Ser. A **23** (1977), 148–175.

[Sp$_1$] T. A. Springer, *Regular elements of finite reflection groups*, Invent. Math. **25** (1974), 159–198.

[Sp$_2$] ______, *Invariant theory*, Lecture Notes in Math., vol. 585, Springer-Verlag, Berlin, 1977.

[Sta$_1$] R. Stanley, *Relative invariants of finite groups generated by pseudo-reflections*, J. Algebra **49** (1977), 134–148.

[Sta$_2$] ______, *Hilbert functions of graded algebras*, Advances in Math., **28** (1978), 57–83.

[Ste] R. Steinberg, *Invariants of finite reflection groups*, Canad. J. Math. **12** (1960), 616–618.

[Str$_1$] C. W. Strom, *On complete systems under certain finite groups*, Bull. Amer. Math. Soc. **37** (1931), 570–574.

[Str$_2$] ______, *A complete system for the simple group G_{60}^6*, Bull. Amer. Math. Soc. **43** (1937), 438–440.

[Str$_3$] ______, *Complete systems of invariants of the cyclic groups of equal order and degree*, Proc. Iowa Acad. Sci. **55** (1948), 287–290.

[Wah] J. Wahl, *Equations defining rational singularities*, Ann. Sci. École Norm. Sup. **10** (1977), 231-264.

[Wat$_1$] K. Watanabe, *Certain invariant subrings are Gorenstein*. I, Osaka. J. Math. **11** (1974), 1–8.

[Wat$_2$] ______, *Certain invariant subrings are Gorenstein*. II, Osaka J. Math. **11** (1974), 379–388.

[We] H. Weyl, *The classical groups*, 2nd ed., Princeton Univ. Press, Princeton, N. J., 1953.

[Wu] E. M. Wright, *Partitions of multi-partite numbers*, Proc. Amer. Math. Soc. **7** (1955), 880–890.

[Z-S] O. Zariski and P. Samuel, *Commutative algebra*, vol. II, van Nostrand, Princeton, N. J., 1960.

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

Current address: Department of Mathematics, University of California, San Diego, La Jolla, California 92093