Available online at www.sciencedirect.com
SCIENCE DIRECT®

Journal of Pure and Applied Algebra 199 (2005) 219–234

JOURNAL OF PURE AND APPLIED ALGEBRA

www.elsevier.com/locate/jpaa

Inverse systems and regular representations

Mike Roth

Department of Mathematics and Statistics, Queens University, Kingston, Ont., Canada K7L 3N6

Received 16 August 2004; received in revised form 28 October 2004
Available online 28 January 2005
Communicated by A.V. Geramita

Abstract

Let G be a finite group acting on a finite-dimensional vector space V, such that the ring of invariants is polynomial. The purpose of this note is to describe exactly the finitely generated inverse systems such that the associated G-representation is the direct sum of copies of the regular representation of G. This generalizes work of Steinberg, Bergeron, Garsia, and Tesler. Related results are also recalled. All of the results are contained in the main theorem.

MSC: Primary: 13A50; secondary: 20C05

1. Introduction

1.1. Let $R = k[y_1, \ldots, y_n]$ be the polynomial ring in n-variables over a field k of characteristic zero. For any polynomial $r \in R$ let $\mathscr{L}_\partial(r)$ be the k-linear subspace of R spanned by r and its partial derivatives of all orders. Similarly, for a collection $r_1, \ldots, r_m$ of polynomials, we let $\mathscr{L}_\partial(r_1, \ldots, r_m)$ be the k-linear subspace spanned by the r_i's and all their partial derivatives of all orders.

1.2. Suppose that a finite group G acts faithfully by homogeneous linear substitutions on R. If $r_1, \ldots, r_m$ are a collection of polynomials in R such that the space they span is stable under the action of G, then the same is true for $\mathscr{L}_\partial(r_1, \ldots, r_m)$. The basic question is to

---

E-mail address: mikeroth@mast.queensu.ca (M. Roth).

0022-4049/$ - see front matter
doi:10.1016/j.jpaa.2004.12.011

connect the G-representation that arises to properties of the initial polynomials $r_1, \dots, r_m$ generating the subspace.

1.3. Let V be the k-vector space spanned by $y_1, \dots, y_n$, i.e., the ring R in degree 1. By hypothesis, G acts linearly on V. Call an element r of R a G-*alternant* if $g \cdot r = \det_g(V^*) r$ for all $g \in G$.

1.4. Suppose that V is a pseudo-reflection representation (Section 2.1) of G, and $r = \Delta_G$ is the product of the reflection vectors, each raised to the power one less than their order. Then r is a G-alternant and it follows from [11] that $\mathscr{L}_\partial(r)$ is the regular representation of G.

More generally, Bergeron et al. [1, Theorem 3.2] prove that if V is a pseudo-reflection representation of V and r is any G-alternant, then $\mathscr{L}_\partial(r)$ is a sum of copies of the regular representation of G.

The main result of this note is

Theorem. *Suppose that V is a pseudo-reflection representation of G. Then $\mathscr{L}_\partial(r_1, \dots, r_m)$ is a direct sum of copies of the regular representation of G if and only if $\mathscr{L}_\partial(r_1, \dots, r_m)$ can be generated by G-alternants.*

In other words, if $r_1, \dots, r_m$ are G-alternants, then $\mathscr{L}_\partial(r_1, \dots, r_m)$ is a sum of copies of the regular representation of G, and conversely, if $\mathscr{L}_\partial(r_1, \dots, r_m)$ is a sum of copies of the regular representation of G, then there are G-alternants $r'_1, \dots, r'_{m'}$ in $\mathscr{L}_\partial(r_1, \dots, r_m)$ such that $\mathscr{L}_\partial(r'_1, \dots, r'_{m'}) = \mathscr{L}_\partial(r_1, \dots, r_m)$.

The proof is independent of the results above, and gives a conceptual explanation for the appearance of the alternants: by Lemma 6.7 the generators of $\mathscr{L}_\partial(r_1, \dots, r_m)$ are dual to the socle of a certain module. Each $g \in G$ acts on the socle by multiplication by $\det_g(V)$, a consequence either of Grothendieck duality, or direct computation with the basic "tile" module T_G (Section 4.2); this means that the generators must also be alternates.

The hypothesis that V be a pseudo-reflection representation cannot be removed. There is simply no consistent answer possible in other cases, stemming from the fact that the relevant ring of invariants (Section 2.3) is not polynomial, and hence represents a singular variety.

1.5. A convenient way to deal with the process of taking derivatives is given by Macaulay's inverse system construction (Section 6.4). Let $A = k[x_1, \dots, x_n]$ be a polynomial ring in n variables. Let x_i act on R as the differential operator $\partial/\partial y_i$, and extend this to an action of A on R via the obvious interpretation of polynomials in A as linear differential operators.

For any collection $r_1, \dots, r_m$ of elements of R, let $I' := I'_{r_1,\dots,r_m}$ be the set of elements in A which annihilate $r_1, \dots, r_m$. Then I' is an ideal of A supported at the origin (Section 2.6). This process sets up a one-to-one correspondence between ideals I' of A supported at the origin and k-subspaces of the form $\mathscr{L}_\partial(r_1, \dots, r_m)$ of R.

From the construction, it follows that A/I' is the k-dual of $\mathscr{L}_\partial(r_1, \dots, r_m)$. If A is given the correct G-action, then this is also the dual as a G-representation. It is easier to deal with this problem by looking at A, and this leads naturally to the ring of invariants $B = A^G$.

1.6. The perspective in this note is to start with A, and construct R appropriately. In the language of inverse systems, the theorem mentioned above is parts (d) and (e) of the main theorem (Section 3).

Parts (a) and (b) of the main theorem are very well known, and certainly not new results. They are included for completeness, and since the ideas involved in their proofs lead naturally to the proofs of parts (c)–(e). Part (c) of the theorem is also useful. Although not listed in the statement of the theorem, the canonical equality in Eq. (5.3.1) is the cleanest way to understand the comparison between the socles.

Because the G-representations underlying A and R are dual, it is sometimes awkward to keep track of what G-alternant should mean in either case, and hence we will always explicitly spell out whether we are looking at elements which, when acted apon by $g \in G$, are multiplied by $\det_g(V)$ or $\det_g(V^*)$.

2. Setup and notation

2.1. Let V be an n-dimensional vector space over a field k of characteristic zero, G a finite group, and $\rho : G \to \mathrm{End}(V)$ a faithful representation of V. We further require that the representation be a pseudo-reflection representation.

A *pseudo-reflection* is an element $g \in G$ such that when diagonalized (after possibly extending scalars to the algebraic closure $\bar{k}$) $\rho(g)$ is of the form

$$\rho(g) = \begin{bmatrix} 1 & & & & \\ & 1 & & 0 & \\ & & \ddots & & \\ & 0 & & 1 & \\ & & & & \zeta \end{bmatrix},$$

where ζ is a root of unity. An ordinary reflection is the case that $\zeta = -1$. An alternate characterization of a pseudo-reflection is simply that rank $(\rho(g) - 1) \leqslant 1$. A representation ρ is called a complex reflection or pseudo-reflection representation if G is generated by elements $\{g_i\}$ such that each $\rho(g_i)$ is a pseudo-reflection.

2.2. Two examples of pseudo-reflection representations are $G = S_n$, the symmetric group, acting on an n-dimensional vector space V by the usual permutation representation, and $G = D_m$, the dihedral group of order $2m$ acting on a two-dimensional vector space V over $\mathbb{C}$ via its usual real action on a regular m-gon centered at the origin. Both of these representations are generated by genuine reflections.

2.3. Let $A = \mathrm{Sym}^{\bullet}(V^*) = \bigoplus_{d \geqslant 0} \mathrm{Sym}^d(V^*)$ be the ring of polynomial functions on V. After choosing a basis $x_1, \ldots, x_n$ for V^*, we have $A \cong k[x_1, \ldots, x_n]$.

Let $B = A^G$ be the ring of invariants of G. The condition that G be a pseudo-reflection representation is, by a well-known theorem of Shephard and Todd [8, Theorem 5.1], exactly the condition that the ring B be *polynomial*, i.e., that there exist $F_1, \ldots, F_n$ in A, invariant under G, such that every invariant is a polynomial in the F's, or in other words that

$B=k[F_1,\ldots,F_n]$. For an excellent discussion of this theorem, and certainly the most beautiful proof of it, the reader is advised to consult the lecture of Serre [7].

2.4. In the case that $G=S_n$ with the usual permutation representation, the F_i are the elementary symmetric polynomials. In case that $G=D_m$ it is convenient to first change basis so that the generating rotation σ and the generating reflection τ (satisfying $\tau\sigma\tau=\sigma^{-1}$) are of the form

$$\rho(\sigma)=\begin{bmatrix}\zeta_m & 0\\ 0 & \zeta_m^{-1}\end{bmatrix} \quad\text{and}\quad \rho(\tau)=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix},$$

where $\zeta_m=\exp(2\pi\mathrm{i}/m)$ is a primitive mth root of unity. Choosing the corresponding dual basis for V^*, the ring of invariants is generated by $F_1=x_1x_2$ and $F_2=x_1^m+x_2^m$.

2.5. It will be conceptually clearer for us to not to think of B as a subring of A, but rather as a polynomial ring $B=k[u_1,\ldots,u_n]$ in indeterminates $u_1,\ldots,u_n$, along with a ring homomorphism $B\to A$ sending each u_i to F_i.

Let d_i be the degree of F_i, $i=1,\ldots,n$. We consider the indeterminate u_i to have degree d_i, so that $B\to A$ is a graded homomorphism. All references to degrees in B will be with respect to this grading.

2.6. Let J be an ideal of B such that B/J is a finite-dimensional k-algebra, and let $I=A\cdot J$ be the ideal of A generated by J. For example, if the ideal J is the maximal homogeneous ideal $J=(u_1,\ldots,u_n)$ of B, then I would be $I=(F_1,\ldots,F_n)$, the ideal generated by the positive degree invariants. Picking $J=(u_1^2,u_2,\ldots,u_n)$ would give $I=(F_1^2,F_2,\ldots,F_n)$.

We will usually also make the restriction that B/J is “supported at the origin”, meaning that the radical of J is the ideal $(u_1,\ldots,u_n)$, and implying that the radical of I is $(x_1,\ldots,x_n)$.

2.7. If $I=A\cdot J$ as above, then I is stable under the action of G, and A/I is a finite-dimensional G-representation. The main question explored in this note is the relationship between J, the representation A/I and the inverse system M_I associated to A/I (see Section 6 for a discussion of inverse systems and the notation M_I).

The purpose of introducing the u’s is to force us to be clear about which ring we are working in. Considering B as a subring of A, an ideal written in the form $(F_1^2,\ldots,F_n)$ is ambiguous: is it an ideal of A or of B? We will also be concerned with computing the dimension (as vector spaces) of quotients B/J or A/I, and in this case the notation will also help us be clear about where we are computing the quotient.

2.8. Notation. The symbols V, G, A, B, F_i, u_i, and d_i will always have the meanings above. We will always assume that G is acting on V via a faithful pseudo-reflection representation. The symbol J will always mean an ideal of B such that the quotient B/J is a finite-dimensional vector space over k. The symbols I and I' will always denote ideals of A. The ideal I will always be an ideal of the form $I=A\cdot J$ for an ideal J of B, while I' is not necessarily an ideal of this form, although it will usually turn out to be so a posteriori. The symbol M_I will denote the inverse system (see Section 6) associated to I.

2.9. If M is a graded module, then the Hilbert series $h(M)$ of M is the formal series in t

$$h(M) := \sum_{d \geqslant 0} \dim_k(M_d)t^d,$$

where M_d is the homogeneous part of M in degree d. If M is also a finite-dimensional vector space over k then the Hilbert series is a polynomial.

Let Λ be the character ring of G, i.e., the Grothendieck group of the category of finitely generated $k[G]$ modules. For any finite-dimensional G-representation W, we denote by $[W]$ the element of Λ corresponding to the representation W.

If M is a graded A-module with G action (the action preserving the grading), then we denote by $\mathscr{F}(M)$ the *graded Frobenius Characteristic* of M, i.e., the element

$$\mathscr{F}(M) := \sum_{d \geqslant 0} [M_d]t^d$$

of $\Lambda[\![t]\!]$. If M is a finite dimensional vector space over k then $\mathscr{F}(M)$ is an element of $\Lambda[t]$.

2.10. If M is an A-module we say that M is *supported at the origin* if M is killed by a power of the maximal ideal $\mathfrak{m} = (x_1, \ldots, x_n)$. We are only considering finitely generated A modules, and so this automatically means that M is a finite-dimensional vector space over k. If M is supported at the origin then we define the *socle* $\mathrm{Soc}(M)$ of M by

$$\mathrm{Soc}(M) := \{m \in M \mid f \cdot m = 0 \text{ for all } f \in \mathfrak{m}\}.$$

We will chiefly use this for modules of the form $M = A/I$ where $\mathfrak{m}$ is the radical of I. The appeal of the socle is that

(i) It is the simplest possible kind of A-module supported at the origin.
(ii) If M is a nonzero module supported at the origin, then $\mathrm{Soc}(M) \neq 0$.

From point (ii) it follows by induction that if M is a nonzero A-module supported at the origin then there exists a filtration

$$0 = M_0 \subset M_1 \subset M_2 \subset \cdots \subset M_\ell = M$$

such that each M_i/M_{i-1} is killed by $\mathfrak{m}$ (set $M_1 = \mathrm{Soc}(M)$ and then pullback the corresponding filtration from M/M_1). Thus any module supported at the origin is filtered by submodules with the simplest possible factors. This fact plus flatness will prove part (a) of the main theorem below.

In Section 5 it will be convenient to use the identity $\mathrm{Soc}(M) = \mathrm{Hom}_A(A/\mathfrak{m}, M)$, valid for any A-module M supported at the origin.

The definitions are similar for a B-module N, but with respect to the maximal ideal $\mathfrak{n} = (u_1, \ldots, u_n)$ of B.

3. Main theorem

With the above notational conventions in place, let J be an ideal of B such that B/J is a finite-dimensional vector space over k, and let $I = A \cdot J$. For parts (c)–(e) below we also assume that B/J is supported at the origin. Then:

3.1. Theorem. (a) *A/I is a direct sum of copies of the regular representation of G. We have* $\dim_k(A/I) = |G| \dim_k(B/J)$ *so that in fact A/I is a direct sum of* $\dim_k(B/J)$ *copies of the regular representation.*

There is a fixed polynomial $H \in \mathbb{Z}[t]$ and a fixed $F \in \Lambda[t]$ such that, whenever J is a homogeneous ideal and $I = A \cdot J$, we have $h(A/I) = H \cdot h(B/J)$, and $\mathscr{F}(A/I) = F \cdot h(B/J)$ (see Section 2.9 *for notation).*

(b) *Conversely, suppose that I' is an ideal of A such that I' is stable under the action of G and A/I' is supported at the origin. If the G-representation A/I' is a direct sum of copies of the regular representation then $I' = A \cdot J'$ for some ideal J' of B.*

(c) *We have* $\dim_k \mathrm{Soc}(A/I) = \dim_k \mathrm{Soc}(B/J)$. *The socle of A/I is G-stable, and for any $\bar{a} \in \mathrm{Soc}(A/I)$, and any $g \in G$, g acts on $\bar{a}$ by multiplication by* $\det_g(V)$. *In other words,* $\mathrm{Soc}(A/I)$ *is the trivial representation of G tensored with the one-dimensional representation where G acts via* $\det(V)$. *If J is homogeneous, then degrees of* $\mathrm{Soc}(A/I)$ *are the degrees of* $\mathrm{Soc}(B/J)$ *shifted by $\delta := \sum_{i=1}^{n} (d_i - 1)$, or* $h(\mathrm{Soc}(A/I)) = h(\mathrm{Soc}(B/J)) \cdot t^{\delta}$.

(d) *If M_I is the inverse system associated to I, then M_I is generated as an A-module by elements where G acts by multiplication by* $\det(V^*)$. *That is, there is a set of A-module generators $m_1, \ldots, m_r$ for M_I such that each g in G acts on each m_i by multiplication by* $\det_g(V^*)$.

(e) *Conversely, suppose that I' is an ideal of A such that A/I' is supported at the origin, and such that its inverse system $M_{I'}$ is generated as an A-module by elements where G acts by multiplication by* $\det(V^*)$. *Then $I' = A \cdot J'$ for some ideal J' of B and hence (by part ((a)) both A/I' and $M_{I'}$ are direct sums of copies of the regular representation.*

4. Proof of (a) and (b)

4.1. Flatness. The assumption that B is polynomial implies that the inclusion $B \to A$ makes A into a flat B-module.

There are many ways to see this. For instance, since the fibres of the induced map $\mathrm{Spec}(A) \to \mathrm{Spec}(B)$ are all zero dimensional and hence Cohen–Macaulay, and since B is regular, the map must be flat, by the wonderful flatness theorem of [3, IV_2, 6.1.5] or [6, Theorem 23.1].

Alternatively, since A is a finite B-module, and A is regular, it is a well known theorem of Serre [7, 8-06, Lemma] that B is regular if and only if the map $B \to A$ is flat.

Flatness implies that the crucial case to understand is when $J = \mathfrak{n} = (u_1, \ldots, u_n)$, or equivalently when $I = (F_1, \ldots, F_n)$, sometimes called the Hilbert ideal. This particular A-module will come up several times in the proof and it is worthwhile to give it its own name. A general A/I (again with $I = A \cdot J$ for some ideal J of B) is “tiled” by copies of this module, so we will use the symbol T_G to refer to it.

4.2. Structure of T_G. Let $T_G := B/\mathfrak{n} \otimes_B A = A/(F_1, \ldots, F_n)$. Since T_G is a complete intersection, it is Gorenstein, and so has a one-dimensional socle. The Hilbert series of any complete intersection is easy to compute; since the degrees of the F_i’s are $d_1, \ldots, d_n$, we have

$$h(T_G) = \prod_{i=1}^{n} \frac{(1-t^{d_i})}{(1-t)} = \prod_{i=1}^{n} (1+t+t^2+\cdots+t^{d_i-1}).$$

In particular, T_G is one dimensional in the top degree $\delta := \sum_{i=1}^{n} (d_i - 1)$, and so the socle must be that one-dimensional subspace.

4.3. The map $\mathrm{Spec}(A) \to \mathrm{Spec}(B)$ is the geometric quotient of the affine space $\mathrm{Spec}(A)$ by G. The locus of points in $\mathrm{Spec}(A)$ with nontrivial stabilizer subgroup is a proper closed subset of $\mathrm{Spec}(A)$, so for a general point $p \in \mathrm{Spec}(B)$ the fibre will consist of a G-orbit with $|G|$ distinct points. If $p = (p_1, \ldots, p_n)$ is such a point, this implies that $B/(u_1 - p_1, u_2 - p_2, \ldots, u_n - p_n) \otimes_B A = A/(F_1 = p_1, F_2 - p_2, \ldots, F_n - p_n)$ is the regular representation of G, since this is the coordinate ring of the fibre over p.

For $t \in k$ define $I_t = (F_1 - tp_1, F_2 - tp_t, \ldots, F_n - tp_n) = A \cdot (u_1 - tp_1, u_2 - tp_t, \ldots, u_n - tp_n)$. The quotient $B/(u_1 - tp_1, u_2 - tp_2, \ldots, u_n - tp_n)$ has the same dimension (i.e., 1) for all t. Since the ring map $B \to A$ is finite and flat, this implies that quotient A/I_t has the same dimension for all $t \in k$. Since I_t is stable under G the quotient A/I_t is also a representation of G.

As t varies in k we therefore get a family of G-representations of the same dimension. Since the set of G-representations is discrete (being determined by the character) it is impossible for the representation to vary continuously, and therefore the representation is the same for all t.

In particular, $T_G = A/I_0$ is the regular representation of G, since A/I_1 is.

A shorter version of the argument is this: since $\mathrm{Spec}(A) \to \mathrm{Spec}(B)$ is a finite flat map, all scheme theoretic fibres are of the same dimension. By continuity, the G-representation on each must be the same. To see what that representation is, it suffices to take any fibre. Picking $\eta \in \mathrm{Spec}(B)$ to be the generic point, the fibre is the quotient field of A as a vector space over the quotient field of B. By the normal basis theorem in Galois theory, this is the regular representation.

4.4. We will see in Section 5 as a consequence of Grothendieck duality that the one-dimensional representation of G on the socle of T_G is multiplication by $\det(V)$. On the other hand, establishing that fact independently will allow an alternate proof of (c) avoiding duality altogether.

The determinant

$$\Delta(F_1, \ldots, F_n) := \begin{vmatrix} \dfrac{\partial F_1}{\partial x_1} & \dfrac{\partial F_2}{\partial x_1} & \cdots & \dfrac{\partial F_n}{\partial x_1} \\ \dfrac{\partial F_1}{\partial x_2} & \dfrac{\partial F_2}{\partial x_2} & \cdots & \dfrac{\partial F_n}{\partial x_2} \\ \vdots & \vdots & \ddots & \vdots \\ \dfrac{\partial F_1}{\partial x_n} & \dfrac{\partial F_2}{\partial x_n} & \cdots & \dfrac{\partial F_n}{\partial x_n} \end{vmatrix}$$

of the Jacobian matrix is a polynomial of degree $\delta = \sum_{i=1}^{n} (d_i - 1)$ in $x_1, \ldots, x_n$.

The variables $x_1, \ldots, x_n$ are a basis for V^*. The first-order differential operators $\partial/\partial x_1, \ldots, \partial/\partial x_n$ pair naturally by differentiation with these basis vectors, and so the vector space spanned by them is naturally isomorphic to V as a G-representation. Since the F_i's are invariant, it follows that G acts on $\varDelta$ by multiplication by $\det(V)$.

By Stanley [9, Proposition 4.7] the set of elements of A which are acted apon by G by multiplication by $\det(V)$ is a free module over B with generator $\varDelta$. Here $\varDelta$ is not in the Hilbert ideal I, and so gives a nonzero element of T_G. Alternatively, by Steinberg [10] δ is the smallest degree in which there is an element acted upon by multiplication by $\det(V)$, and so again $\varDelta$ cannot be in the Hilbert ideal. This shows explicitly that the socle of T_G is acted upon by G by multiplication by $\det(V)$.

For convenient reference, we summarize these facts about T_G:

4.5. Proposition. *The A-module T_G is the regular representation of G with a one-dimensional socle in degree $\delta = \sum_{i=1}^{n}(d_i - 1)$. The action of G on this one-dimensional vector space is by multiplication by* $\det(V)$.

4.6. Proof of (a). Suppose that J is an ideal of B such that B/J is supported at the origin. By Section 2.10 we can find a series of submodules

$$0 \subset N_1 \subset N_2 \subset \cdots \subset N_\ell = B/J$$

such that each N_i/N_{i-1} is killed by $\mathfrak{n} = (u_1, \ldots, u_n)$. By enlarging the filtration we can assume in addition that N_i/N_{i-1} is a one-dimensional vector space, and hence equal to $B/\mathfrak{n}$ as a B-module. With this type of filtration, it follows that $\ell = \dim_k(B/J)$.

Tensoring with A, we get a filtration

$$0 \subset N_1 \otimes_B A \subset N_2 \otimes_B A \subset \cdots \subset N_\ell \otimes_B A = A/I$$

and since A is a flat B-module, we have that

$$(N_i \otimes_B A)/(N_{i-1} \otimes_B A) = (N_i/N_{i-1}) \otimes_B A = B/\mathfrak{n} \otimes_B A = T_G.$$

This shows that A/I has a filtration by a sequence of $\ell = \dim_k(B/J)$ submodules where each quotient is isomorphic to T_G. Hence as a G-module, A/I consists of $\dim_k(B/J)$ copies of the regular representation, proving the first part of (a).

This filtration also proves the second part of (a): If J is homogeneous, then we can choose the filtration to respect the grading, so that each of the quotients N_i/N_{i-1} are graded. The filtration then shows that $H := h(T_G)$ and $F := \mathscr{F}(T_G)$ have the desired properties. $\square$

4.7. Proof of (b). Suppose that I' is an ideal of A stable under G and supported at the origin, and that A/I' is a direct sum of copies of the regular representation. Set $J = (I')^G$ and $I = A \cdot J$.

Taking G-invariants of the exact sequence

$$0 \to I' \to A \to A/I' \to 0$$

gives

$$0 \to J \to B \to (A/I')^G \to 0$$

and hence that $B/J = (A/I')^G$.

Since A/I' is a direct sum of copies of the regular representation,

$$\dim_k(B/J) = \dim_k((A/I')^G) = \frac{1}{|G|}\dim_k(A/I').$$

By part (a) of the theorem, we have

$$\dim_k(A/I) = |G|\dim_k(B/J) = \frac{|G|}{|G|}\dim_k(A/I') = \dim_k(A/I').$$

Since A/I' is a quotient of A/I this gives $A/I = A/I'$ and hence $I = I'$. $\square$

5. Proof of (c)

5.1. Grothendieck duality. We want to apply Grothendieck duality in the following extremely simple case. Suppose that A and B are regular rings and that $B \to A$ is a homomorphism of rings making A into a finitely generated B module. Under these conditions, for any A-module M and B-module N, Grothendieck duality is simply that

(5.1.1)

$$\mathrm{Hom}_A(M, A\otimes_B N)\otimes_A\omega_A = \mathrm{Hom}_B(M, N)\otimes_B\omega_B,$$

where the equality is a *canonical* equality of B-modules. Here the entire left-hand side, and the A-module M on the right-hand side are treated as B-modules via the homomorphism $B \to A$. The modules ω_A and ω_B are the canonical modules of A and B. One property of these canonical modules under our hypotheses is that they are locally free modules of rank 1 over A and B, respectively. (This form of Grothendieck duality may be extracted from the general form of duality for a finite map [4, introduction] combined with [4, V, Proposition 2.4] and the fact that A is a locally free B-module.)

5.2. For our rings $A = k[x_1, \ldots, x_n]$ and $B = k[u_1, \ldots, u_n]$, ω_A is the free A-module with generator $\mathrm{d}x_1\wedge\mathrm{d}x_2\wedge\cdots\wedge\mathrm{d}x_n$ and ω_B the free B module with generator $\mathrm{d}u_1\wedge\mathrm{d}u_2\wedge\cdots\wedge\mathrm{d}u_n$. In particular, G acts on the generator of ω_A by multiplication by $\det(V^*)$. Also, in terms of grading, the generator of ω_A has degree n which the sum of the degrees of the x_i's, and the generator of ω_B has degree $\sum_{i=1}^n d_i$ which is the sum of the degrees of the u_i's.

5.3. Given an ideal J of B such that B/J is supported at the origin, let $M = A/\mathfrak{m}$ and $N = B/J$ with $\mathfrak{m} = (x_1, \ldots, x_n)$ the graded maximal ideal of A. If $I = A \cdot J$, then

(5.1.1) gives

$$\mathrm{Hom}_A(A/\mathfrak{m}, A/I)\otimes_A\omega_A = \mathrm{Hom}_B(B/\mathfrak{n}, B/J)\otimes_B\omega_B,$$

where $\mathfrak{n}$ is the maximal ideal $\mathfrak{n} = (u_1, \ldots, u_n)$ of B.

To see that this is the conclusion of (5.1.1), we just need to note that $A\otimes_B(B/J) = A/I$, which follows from the definition of I and right exactness of the tensor product, and that $A/\mathfrak{m}$ considered as a B module is $B/\mathfrak{n}$ which follows from the fact that $A/\mathfrak{m}$ is a one-dimensional vector space over k, killed by all elements of $\mathfrak{n}$.

Using the identities in Section 2.10 this is more usefully written as

(5.3.1)

$$\mathrm{Soc}(A/I)\otimes_A\omega_A = \mathrm{Soc}(B/J)\otimes_B\omega_B.$$

5.4. Proof of (c). The equality of B-modules in (5.3.1) is canonical. Let us just check what this canonical equality implies at various level of structure on the two sides.

As vector spaces: On each side of (5.3.1) we are tensoring a finite dimensional vector space with a rank 1 free module. This does not change the dimension of the vector space, hence $\dim_k(\mathrm{Soc}(A/I)) = \dim_k(\mathrm{Soc}(B/J))$.

As G-modules: The action of G on the right-hand side of (5.3.1) is trivial, hence it must also be trivial on the left-hand side. As representations the left-hand side is $\mathrm{Soc}(A/I)$ tensored with a one-dimensional representation where G acts by multiplication by $\det(V^*)$. In order for this to be the trivial representation, G must act on all of $\mathrm{Soc}(A/I)$ by multiplication by $\det(V)$.

In the case that J is homogeneous, then both sides of the equation are graded.

As graded vector spaces: The effect of tensoring with ω_A is to shift the grading by n. The effect of tensoring with ω_B is to shift the grading by $\sum_{i=1}^n d_i$. Hence the degrees of $\mathrm{Soc}(A/I)$ are the degrees of $\mathrm{Soc}(B/J)$ shifted by $\delta = \sum_{i=1}^n (d_i - 1)$. $\square$

5.5. Alternate proof of (c). It is possible to give a proof of (c) without appealing to Grothendieck duality. Let J and I be as above, and consider the map $B/J \to \oplus_{i=1}^n B/J$ where the map to the ith factor is multiplication by u_i. By definition, the kernel of this map is exactly the socle of B/J, so that we have an exact sequence

$$0 \to \mathrm{Soc}(B/J) \to B/J \overset{[u_1,\ldots,u_n]}{\to} \oplus_{i=1}^n B/J.$$

Tensoring with A we get the sequence

$$0 \to \mathrm{Soc}(B/J)\otimes_B A \to A/I \overset{[F_1,\ldots,F_n]}{\to} \oplus_{i=1}^n A/I$$

which is still exact, since A is a flat B-module. The socle of A/I is killed by multiplication by F_1 through F_n, hence $\mathrm{Soc}(A/I) \subseteq \mathrm{Soc}(B/J)\otimes_B A$, and therefore $\mathrm{Soc}(A/I) = \mathrm{Soc}(\mathrm{Soc}(B/J)\otimes_B A)$, and so we can restrict our attention to the A-module $\mathrm{Soc}(B/J)\otimes_B A$.

As a B-module, $\mathrm{Soc}(B/J)$ is a direct sum of copies of $B/\mathfrak{n}$. It follows that $\mathrm{Soc}(B/J)\otimes_B A$ is a direct sum of copies of $B/\mathfrak{n}\otimes_B A \cong T_G$, the number of copies being equal to $\dim_k(\mathrm{Soc}(B/J))$.

We now just need to recall the properties of T_G from Section 4.2.

Each T_G has a one-dimensional socle, on which G acts by multiplication by $\det(V)$, hence we recover that $\dim_k(\mathrm{Soc}(B/J)) = \dim_k(\mathrm{Soc}(A/I))$, and that the G-action on $\mathrm{Soc}(A/I)$ is multiplication by $\det(V)$.

If J is homogeneous, then $\mathrm{Soc}(B/J)$ is graded, and so is the expression of $\mathrm{Soc}(B/J)\otimes_B A$ as a direct sum of T_G's, the grading on each T_G being shifted by the degree of the corresponding element in $\mathrm{Soc}(B/J)$. Since the socle of T_G is in degree δ, we recover the fact that the degrees of $\mathrm{Soc}(A/I)$ are the degrees of $\mathrm{Soc}(B/J)$ shifted by δ. □

We finish with an easy lemma which will be useful in the proof of (e).

5.6. Lemma. *If J is an ideal of B such that B/J is supported at the origin, and $\bar{a}$ an element of* $\mathrm{Soc}(A/I)$ *with $I = A \cdot J$, then there is a submodule T of A/I with $T \cong T_G$ and $\bar{a} \in T$.*

Proof. If $\bar{b}$ is a nonzero element of $\mathrm{Soc}(B/J)$ let $\langle\bar{b}\rangle$ be the one-dimensional subspace over k spanned by $\bar{b}$. As a B module, $\langle\bar{b}\rangle$ is isomorphic to $B/\mathfrak{n}$ and so $T := \langle\bar{b}\rangle\otimes_B A \cong T_G$ as an A-module. The socle of T_G is one-dimensional, and either of the two proofs of part (c) show that the procedures

$$\langle\bar{b}\rangle \rightsquigarrow \langle\bar{b}\rangle\otimes_B A \rightsquigarrow \mathrm{Soc}(\langle\bar{b}\rangle\otimes_B A)$$

set up a one to one correspondence:

$$\left\{\begin{array}{l}\text{One-dimensional } k\text{-}\\ \text{subspaces of } \mathrm{Soc}(B/J)\end{array}\right\} \overset{1:1}{\leftrightarrow} \left\{\begin{array}{l}A\text{-submodules } T \text{ of}\\ A/I \text{ isomorphic to } T_G\end{array}\right\} \overset{1:1}{\leftrightarrow} \left\{\begin{array}{l}\text{One-dimensional } k\text{-}\\ \text{subspaces of } \mathrm{Soc}(A/I)\end{array}\right\},$$

proving the lemma. □

6. Inverse systems

6.1. Axiomatics of the module R. Given the polynomial ring A, we want to look for a graded A-module $R = \otimes_{d\geqslant 0} R_d$ with the following properties:

(i) $\dim_k(R_d) = \dim_k(A_d)$ for all $d \geqslant 0$.
(ii) The A action *lowers* degrees: for $a \in A_i$, $r \in R_j$, then $a \cdot r \in R_{j-i}$ ($=0$ if $j-i<0$).
Since R_0 is one-dimensional, that means we have a pairing

$$\langle \cdot, \cdot \rangle_d : A_d \times R_d \to R_0 \cong k,$$

$$\langle a, r \rangle_d := a \cdot r.$$

(iii) The pairing $\langle\cdot,\cdot\rangle_d$ is perfect in all degrees $d \geqslant 0$.
This means one (and hence all) of the following equivalent statements are true:

- For each $a \in A_d$ there is an $r \in R_d$ such that $a \cdot r \neq 0$.
- For each $r \in R_d$ there is an $a \in A_d$ such that $a \cdot r \neq 0$.
- The pairing makes A_d into the dual space $(R_d)^*$ of R_d.
- The pairing makes R_d into the dual space $(A_d)^*$ of A_d.

Requirement (iii) of course implies (i), but for purposes of clarity it was listed separately. Finally, if there is a group G acting on V then we also require

(iv) The group G acts on R in such a way that the A-module action is G-equivariant:

$$(ga)\cdot(gr) = g(a\cdot r)$$

for all $g \in G$, $a \in A$, and $r \in R$.

6.2. There are three typical ways of constructing an A-module R with these properties:

(a) $R = \mathrm{Sym}^\bullet(V) = \bigoplus_{d\geqslant 0}\mathrm{Sym}^d(V)$.
(b) $R = k[y_1,\ldots,y_n]$ with x_i in A acting as the differential operator $\partial/\partial y_i$, and the action extended to polynomials in the x_i's by the obvious interpretation as differential operators with constant coefficients.
(c) $R = H^{n-1}_{\mathfrak{m}}(A)$, the top local cohomology group of A with respect to the maximal ideal $\mathfrak{m} = (x_1,\ldots,x_n)$ of A.

Choice (a) is perhaps the cleanest, the G-action is automatic, as is the operation of pairing an element of $A(=\mathrm{Sym}^\bullet(V^*))$ with an element of R ([2, III, Section 11.10] is a good reference for the pairing). Choice (b) is perhaps the most concrete, although it does not come with an intrinsic G-action. Assuming that G acts trivially on the constants $R_0 \cong k$, the only choice of G-action which satisfies (iv) is to let G act on the y's in the way dual to its action on the x's. With this G-action, (b) is the same as (a).

Choice (c) is somewhat different. It has two apparent disadvantages. First the action on the "constants" R_0 is not actually constant, it is the one-dimensional representation $\det(V^*)$. Second, R in this case is not itself a ring, although this is not usually important in applications, since only the A-module structure is typically relevant.

The two disadvantages are matched by two advantages: First, this construction also works in characteristic $p > 0$. The derivative construction in (b) and the pairing in (a) fail to be perfect pairings in positive characteristic, but, by Serre duality, the A-action on the local cohomology groups induces a perfect pairing in all characteristics. Second, if we are concerned with an algorithmic approach for going from part (e) to part (a) of the theorem, then the local cohomology construction of R is more easily compared with the corresponding module for B.

Our main concern is proving a result about inverse systems, as classically defined, and so we will stick with the more down-to-earth (a) or (b) for our choice of R.

6.3. Trivial remarks on dualizing. If W is a finite-dimensional vector space over k, and W' a subspace of W, then we have the exact sequence

$$0 \to W' \to W \to (W/W') \to 0$$

which we can dualize to get

$$0 \leftarrow (W')^* \leftarrow W^* \leftarrow (W/W')^* \leftarrow 0.$$

Dualizing reverses the arrows and interchanges injective and surjective maps. It also expresses $(W/W')^*$ as a subspace of W^*; it is exactly the subspace of linear functional annihilating W'.

6.4. Inverse systems. Suppose that I is an ideal of A such that A/I is supported at the origin (see 2.10). Looking at the exact sequence

$$0 \to I \to A \to A/I \to 0$$

and remembering that R was constructed as kind of a graded k-dual to A, we look for a subspace of R corresponding to the quotient A/I of A. By the above remarks, this is the set of elements in R which annihilate I. We therefore define

$$M_I := \mathrm{ann}_R(I) = \{r \in R \mid f \cdot r = 0 \text{ for all } f \in I\}.$$

Note that $M_I = (A/I)^*$, the dual being as a k-vector space, and that M_I is an A-submodule of R. This last observation follows from the fact that I is an A-module, and that the pairing between R and A comes from an A-module action.

The module M_I is called the *inverse system associated to* I. In light of the fact that $M_I = (A/I)^*$, it might be better to think of it as something associated to A/I instead.

6.5. The inverse system construction inherits the usual properties of dualizing, for instance, if $I \subseteq I'$ are ideals, so that the natural map $A/I \to A/I'$ is surjective, then the induced map $M_I \leftarrow M_{I'}$ is injective. Similarly, if a is any element of A then the map $A/I \to A/I$ given by multiplication by a is dual to the map $M_I \leftarrow M_I$ given by letting a act on the A-module M_I.

6.6. Suppose that A/I is supported at the origin, i.e., is killed by a power of $\mathfrak{m}$, then the inverse system M_I is as well. Nakayma's lemma tells us that the quotient $M_I/\mathfrak{m}M_I$ is of interest, for example its dimension is the minimum number of generators of M_I as an A-module.

Considering the exact sequence expressing $M_I/\mathfrak{m}M_I$ as a quotient, it is natural to ask for the submodule of A/I dual to the quotient $M_I/\mathfrak{m}M_I$.

$$\begin{array}{ccccc} 0 \to \mathfrak{m}M_I \to & M_I \to & M_I/\mathfrak{m}M_I \to 0 \\ & \updownarrow \text{dual} & \updownarrow \text{dual} \\ & (A/I) \hookleftarrow & ??? \end{array}$$

The answer is given by

6.7. Lemma (Macaulay). *If I is an ideal of A supported at the origin, and* $\mathfrak{m}=(x_1,\ldots,x_n)$ *the maximal ideal, then* $M_I/\mathfrak{m}M_I = \mathrm{Soc}(A/I)^*$.

Proof. We are looking for the subspace of A/I which annihilates $\mathfrak{m}M_I$, i.e., elements $\bar{a} \in A/I$ such that $\bar{a}\cdot(f\cdot m)=0$ for all $f\in\mathfrak{m}$ and $m\in M_I$. This is the same as asking that $(f\bar{a})\cdot m=0$ for all $f\in\mathfrak{m}$ and $m\in M_I$. But since the action of A/I on M_I makes M_I into the k-dual of A/I (that is, the pairing is perfect), we have $(f\bar{a})\cdot m=0$ for all $m\in M$ if and only if $f\bar{a}=0$. This is true for all $f\in\mathfrak{m}$ if and only if $\bar{a}\in\mathrm{Soc}(A/I)$. □

6.8. If I is a homogeneous ideal, then A/I, M_I, $\mathrm{Soc}(A/I)$, and $M_I/\mathfrak{m}M_I$ are graded A-modules. The proof shows that in this case $M_I/\mathfrak{m}M_I$ is the graded dual of $\mathrm{Soc}(A/I)$. This fact is usually used in reverse: If we want to construct a finite dimensional quotient of A with socle in certain degrees, the lemma shows that it suffices to pick elements $r_1,\ldots,r_k$ of R in those degrees, let M be the A-module generated by the r's, and I the ideal such that $M=M_I$, i.e, the ideal annihilating M. The quotient A/I will then have socle in exactly the desired degrees. The inverse system construction was first introduced by Macaulay [5, Chapter 4] for this purpose.

7. Proof of (d) and (e)

7.1. Proof of (d). By the inverse system construction, M_I is k-dual of A/I. By Lemma 6.7 and Nakayama's lemma, the generators of M_I are dual to $\mathrm{Soc}(A/I)$, the hence part (d) of the theorem follows from part (c). □

In order to prove the converse statement, we first need a small result about quotients of T_G.

7.2. Lemma. *Let T_G be the module of* §4.2, *then the only quotients T' of T_G such that the G acts on the socle of T' via* $\det(V)$ *are either $T'=T_G$ or $T'=0$.*

In other words, a quotient of T_G such that the socle is acted on by multiplication by $\det(V)$ is "all or nothing"; we either quotient out by the zero module to get T_G, or by T_G to get the zero module.

Proof. Let M be the inverse system associated to T_G. Any quotient T' of T_G corresponds to a submodule M' of M. The condition that G acts on the socle of T' via $\det(V)$ is, by Lemma 6.7 the same as the condition that M' be generated by elements where G acts by multiplication by $\det(V^*)$.

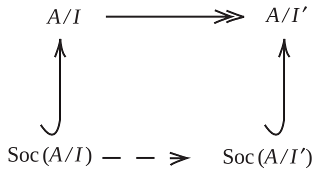
Since T_G is the regular representation of G (Proposition 4.5) M is as well, and therefore the subspace of elements of M where G acts by multiplication by $\det(V^*)$ is one dimensional. By Lemma 6.7 and part (d) of the theorem any nonzero element in this one-dimensional subspace generates M as an A-module. It follows that if M' contains a nonzero generator, it must be all of M. The only alternative is that M' is the zero module. Since M' is the k-dual of T', this proves the lemma. □

7.3. Proof of (e). Let I' be an ideal of A, supported at the origin, such that A/I' is a finite dimensional vector space and such that its inverse system $M_{I'}$ is generated by elements where G acts by multiplication by $\det(V^*)$.

Set $J = (I')^G$ and $I = A \cdot J$. Then $I \subseteq I'$ and so we have a natural surjective map $A/I \to A/I'$. Let $\bar{I}'$ be the image of I' in A/I, so that A/I' is the quotient of A/I by $\bar{I}'$. By construction, there is no nonzero element of $\bar{I}'$ invariant under G, since any such element would give an element of I' invariant under G, hence be contained in J and therefore I.

Let M_I be the inverse system of I. We have a natural inclusion $M_{I'} \hookrightarrow M_I$ dual to the surjection $A/I \to A/I'$. Using the fact that G acts on the socle of A/I by multiplication by $\det(V)$ (part (c) of the theorem), the fact that the same thing is true for A/I' (by the hypothesis about $M_{I'}$ and Lemma 6.7), and that no element of $\bar{I}'$ is invariant under G we will show that $M_{I'} = M_I$, and hence that $A/I' = A/I$, and so $I' = I$.

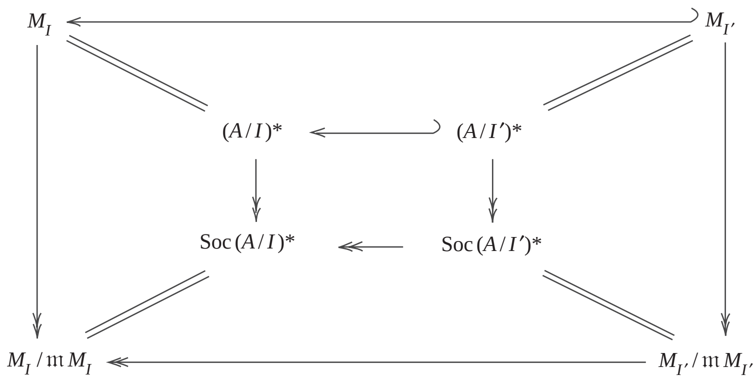
Consider the diagram



The key point is to see that the induced map $\mathrm{Soc}(A/I) \to \mathrm{Soc}(A/I')$ is injective.

Let $\bar{a}$ be any nonzero element of $\mathrm{Soc}(A/I)$. By Lemma 5.6 there is an A-submodule of A/I isomorphic to T_G containing $\bar{a}$. The image of this submodule in A/I' is a quotient of T_G, and the socle of this image will be contained in the socle of A/I'. Hence G acts on the socle of this image by multiplication by $\det(V)$ and we can apply Lemma 7.2 to conclude that the image is either all of T_G or the zero module. Since T_G contains an element invariant under G, and since no element invariant under G is in the kernel of $A/I \to A/I'$, the image cannot be the zero module. Therefore the image is all of T_G, and in particular, $\bar{a}$ is not in the kernel.

Now that we know that the map $\mathrm{Soc}(A/I) \hookrightarrow \mathrm{Soc}(A/I')$ is injective, we dualize the diagram to obtain:



The injectivity of the map between socles now becomes the surjectivity of the map $M_I/\mathfrak{m}M_I \twoheadleftarrow M_{I'}/\mathfrak{m}M_{I'}$. This shows that the submodule $M_{I'}$ contains elements which generate M_I as an A-module. Hence $M_{I'} = M_I$ and so $I' = I$, proving part (e). □

Acknowledgements

I am grateful to François Bergeron for explaining the problem to me in the first place, and for generously letting me repeat his explanations and discuss these results at the workshop on inverse systems and diagonal invariants. I am also grateful to David Pollack and especially Tony Geramita for the encouragement to write this note up, and finally to Abram Broer for pointing out that Grothendieck duality is very useful in invariant theory.

References

[1] F. Bergeron, A. Garsia, G. Tesler, Multiple left regular representations generated by alternants, J. Combin. Theory Ser. A 91 (2000) 49–83.
[2] N. Bourbaki, Algèbre I, Chapitre I à III, Nouvelle Édition, Diffusion C.C.L.S., 1970.
[3] A. Grothendieck, Éléments de Géométrie Algébrique, vol. 24, Publ. I.H.E.S., 1965.
[4] R. Hartshorne, Residues and Duality, Lecture Notes in Mathematics, vol. 20, Springer, New York, 1966.
[5] F.S. Macaulay, The Algebraic Theory of Modular Systems, Cambridge University Press, Cambridge, 1994.
[6] H. Matsumura, Commutative Ring Theory, Cambridge Studies in Advanced Mathematics, vol. 8, 1989.
[7] J.-P. Serre, Groupes finis d'automorphisms d'anneaux locaux réguliers, Colloque d'Algèbre, vol. 8, Ecole Normale Supérieure de Jeunes Filles, Paris, 1967, pp. 11.
[8] G.C. Shephard, J.A. Todd, Finite unitary reflection groups, Canad. J. Math. 6 (1954) 274–304.
[9] R. Stanley, Invariants of finite groups and their applications to combinatorics, Bull. Amer. Math. Soc. 1 (1979) 475–511.
[10] R. Steinberg, Invariants of finite reflection groups, Canad. J. Math. 12 (1960) 616–618.
[11] R. Steinberg, Differential equations invariant under finite reflection groups, Trans. Amer. Math. Soc. 112 (1964) 392–400.